# Relatórios técnicos

## How to enable StorageGRID in your environment

NetApp
December 11, 2024

# Índice

# Relatórios técnicos

## Introdução aos relatórios técnicos do StorageGRID

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

O StorageGRID fornece documentação para cobrir as práticas recomendadas e recomendações para vários recursos e integrações do StorageGRID.

## NetApp StorageGRID e big data analytics

*Por Angela Cheng*

### Casos de uso do NetApp StorageGRID

A solução de storage de objetos da NetApp StorageGRID oferece escalabilidade, disponibilidade de dados, segurança e alta performance. Organizações de todos os tamanhos e em vários setores usam o StorageGRID S3 para uma ampla variedade de casos de uso. Vamos explorar alguns cenários típicos:

**Análise de big data:** o StorageGRID S3 é frequentemente usado como data Lake, onde as empresas armazenam grandes quantidades de dados estruturados e não estruturados para análise usando ferramentas como o Apache Spark, o Splunk Smartstore e o Dremio.

**Disposição em camadas de dados:** os clientes do NetApp usam o recurso FabricPool do ONTAP para mover dados automaticamente entre um nível local de alto desempenho para o StorageGRID. A disposição em camadas libera storage flash caro para dados ativos enquanto mantém os dados inativos prontamente disponíveis no storage de objetos de baixo custo. Isto maximiza o desempenho e as poupanças.

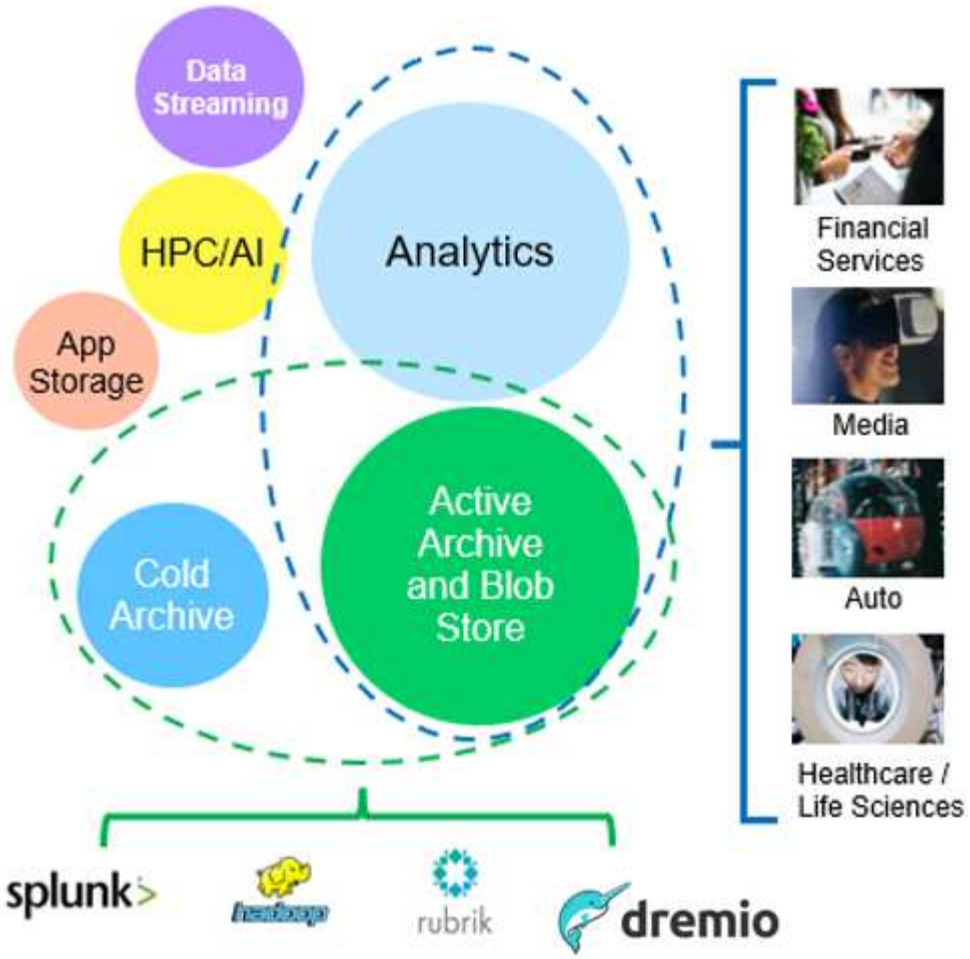
**Backup de dados e recuperação de desastres:** as empresas podem usar o StorageGRID S3 como uma solução confiável e econômica para fazer backup de dados críticos e recuperá-los em caso de desastre.

- Armazenamento de dados para aplicativos:* o StorageGRID S3 pode ser usado como um back-end de armazenamento para aplicativos, permitindo que os desenvolvedores armazenem e recuperem arquivos, imagens, vídeos e outros tipos de dados facilmente.

**Entrega de conteúdo:** o StorageGRID S3 pode ser usado para armazenar e entregar conteúdo estático do site, arquivos de Mídia e downloads de software para usuários em todo o mundo, aproveitando a distribuição geográfica e o namespace global da StorageGRID para entrega de conteúdo rápida e confiável.

**Arquivo de dados:** o StorageGRID oferece diferentes tipos de armazenamento e suporta a disposição em camadas em opções públicas de armazenamento de baixo custo a longo prazo, tornando-o uma solução ideal para arquivamento e retenção de dados a longo prazo que precisam ser mantidos para fins de conformidade ou históricos.

**Casos de uso de armazenamento de objetos**

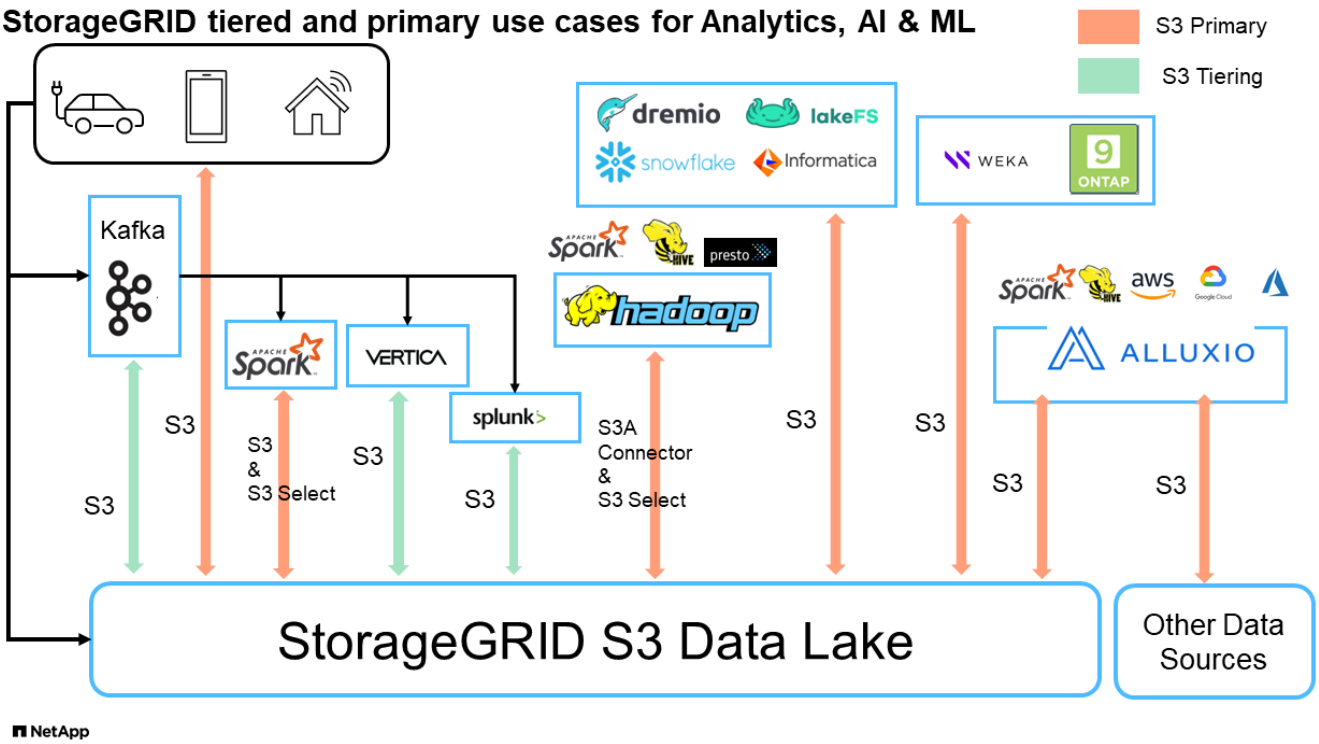



Entre as opções acima, o Big Data Analytics é um dos principais casos de uso e seu uso está em alta.

## Por que escolher a StorageGRID para data Lakes?

- Maior colaboração - enorme alocação compartilhada de vários locais e alocação a vários clientes com acesso à API padrão do setor
- Custos operacionais reduzidos: Simplicidade operacional de uma única arquitetura automatizada e com autorrecuperação
- Escalabilidade - diferentemente das soluções tradicionais de Hadoop e data warehouse, o storage de objetos StorageGRID S3 separa o storage da computação e dos dados, permitindo que as empresas escalem suas necessidades de storage à medida que crescem.
- Durabilidade e confiabilidade - o StorageGRID oferece 99,999999999% de durabilidade, o que significa que os dados armazenados são altamente resistentes à perda de dados. Ele também oferece alta disponibilidade, garantindo que os dados estejam sempre acessíveis.
- Segurança - o StorageGRID oferece vários recursos de segurança, incluindo criptografia, política de controle de acesso, gerenciamento do ciclo de vida dos dados, bloqueio de objetos e controle de versão para proteger os dados armazenados nos buckets do S3

**Lagos de dados StorageGRID S3**




## Benchmarking Data Warehouses e Lakehouses com armazenamento de objetos S3: Um estudo comparativo

este artigo apresenta uma referência abrangente de vários ecossistemas de armazenamento de dados e lakehouse usando o NetApp StorageGRID. O objetivo é determinar qual sistema tem melhor desempenho com o storage de objetos S3. Consulte isso "Apache Iceberg: O Guia definitivo" para saber mais sobre as arquiteturas datawarehous/lakehouse e o formato de tabela (Parquet e Iceberg).

- Ferramenta de benchmark - TPC-DS - https://www.tpc.org/tpcds/
- Ecossistemas de Big Data
  - Cluster de VMs, cada uma com 128G GB de RAM e 24 vCPU, armazenamento SSD para disco do sistema
  - Hadoop 3.3.5 com Hive 3.1.3 (1 nó de nome e 4 nós de dados)
  - Delta Lake com Spark 3.2.0 (1 master e 4 workers) e Hadoop 3.3.5
  - dremio V23 (1 cordinador e 5 executores)
  - Trino v438 (1 cordinador e 5 trabalhadores)
  - Starburst v453 (1 cordinador e 5 trabalhadores)
- Storage de objetos
  - NetApp StorageGRID 11,8 com 3 x SG6060 e 1x SG1000 balanceador de carga
  - Proteção de objetos - 2 cópias (o resultado é semelhante ao EC 2-1)
- Tamanho do banco de dados 1000GB
- O cache foi desativado em todos os ecossistemas para cada teste de consulta usando o formato Parquet. Para o formato Iceberg, comparamos o número de solicitações GET S3 e o tempo total de consulta entre cenários desabilitados em cache e habilitados para cache.

TPC-DS inclui 99 consultas SQL complexas projetadas para benchmarking. Medimos o tempo total necessário para executar todas as 99 consultas e realizamos uma análise detalhada examinando o tipo e o número de S3 solicitações. Nossos testes compararam a eficiência de dois formatos de tabela populares: Parquet e Iceberg.

**Resultado da consulta TPC-DS com formato de tabela Parquet**

| Ecossistema | Colmeia | Delta Lake | Dremio | Trino | Starburst |
|---|---|---|---|---|---|
| TPCDS 99 consultas e total de minutos | 1084 1 | 55 | 47 | 32 | 28 |
| S3 pedidos de divisão | OBTER | 1.117.184 | 2.074.610 | 4.414.227 | 1.504.212 |
| 1.495.039 | Observação: Toda a gama GANHA | Alcance de 80% de 2KB a 2MB de 32MB objetos, 50 a 100 solicitações/seg | Alcance de 73% abaixo de 100KB de 32MB objetos, 1000 - 1400 solicitações/seg | 90% 1M byte range get de 256MB objetos, 2000 - 2300 solicitações/seg | Alcance obter tamanho: 50% abaixo de 100KB, 16% em torno de 1MB, 27% 2MB-9MB, 3500 - 4000 solicitações/seg |
| Obter tamanho: 50% abaixo de 100KB, 16% em torno de 1MB, 27% 2MB-9MB, 4000 - 5000 solicitação/seg | Listar objetos | 312.053 | 24.158 | 240 | 509 |
| 512 | CABEÇA (objeto inexistente) | 156.027 | 12.103 | 192 | 0 |
| 0 | CABEÇA (objeto existente) | 982.126 | 922.732 | 1.845 | 0 |
| 0 | Total de solicitações | 2.567.390 | 3.033.603 | 4.416.504 | 1.504.721 |

1 não é possível concluir a consulta número 72

**Resultado da consulta TPC-DS com formato de tabela Iceberg**

| Ecossistema | Dremio | Trino | Starburst |
|---|---|---|---|
| Consultas TPCDS 99 e total de minutos (cache desativado) | 30 | 28 | 22 |
| TPCDS 99 consultas e total de minutos 2 (cache ativado) | 22 | 28 | 21,5 |
| S3 pedidos de divisão | Obter (cache desativado) | 2.154.747 | 938.639 |
| 931.582 | Obter (cache ativado) | 5.389 | 30.158 |
| 3.281 | Observação: Toda a gama GANHA | Alcance obter tamanho: 67% 1MB, 15% 100KB, 10% 500KB, 3000 - 4000 solicitações/seg | Alcance obter tamanho: 42% abaixo de 100KB, 17% em torno de 1MB, 33% 2MB-9MB, 3500 - 4000 solicitações/seg |
| Alcance obter tamanho: 43% abaixo de 100KB, 17% em torno de 1MB, 33% 2MB-9MB, 4000 - 5000 solicitações/seg | Listar objetos | 284 | 0 |
| 0 | CABEÇA (objeto inexistente) | 284 | 0 |
| 0 | CABEÇA (objeto existente) | 1.261 | 509 |
| 509 | Total de solicitações (cache desativado) | 2.156.578 | 939.148 |

2 o desempenho do Trino/Starburst é prejudicado por recursos de computação; adicionar mais RAM ao cluster reduz o tempo total de consulta.

Como mostrado na primeira tabela, o Hive é significativamente mais lento do que outros ecossistemas modernos de lakehouse de dados. Observamos que o Hive enviou um grande número de solicitações de list-objects S3, que normalmente são lentas em todas as plataformas de armazenamento de objetos, especialmente quando se trata de buckets contendo muitos objetos. Isso aumenta significativamente a duração geral da consulta. Além disso, os ecossistemas modernos do lago podem enviar um grande número de SOLICITAÇÕES GET em paralelo, variando de 2.000 a 5.000 solicitações por segundo, em comparação com as de 50 a 100 solicitações da Hive por segundo. O sistema de arquivos padrão mimetismo por Hive e Hadoop S3A contribui para a lentidão do Hive ao interagir com o armazenamento de objetos S3D.

O uso do Hadoop (em armazenamento de objetos HDFS ou S3) com o Hive ou Spark requer um amplo conhecimento do Hadoop e do Hive/Spark, bem como uma compreensão de como as configurações de cada serviço interagem. Juntos, eles têm mais de 1.000 configurações, muitas das quais estão inter-relacionadas e não podem ser alteradas independentemente. Encontrar a combinação ideal de configurações e valores requer uma quantidade enorme de tempo e esforço.

Comparando os resultados do Parquet e do Iceberg, notamos que o formato da tabela é um fator de desempenho importante. O formato da tabela Iceberg é mais eficiente do que o Parquet em termos do número de solicitações S3, com 35% a 50% menos solicitações em comparação com o formato Parquet.

O desempenho de Dremio, Trino ou Starburst é impulsionado principalmente pelo poder de computação do cluster. Embora todos os três usem o conetor S3A para conexão de armazenamento de objetos S3, eles não exigem Hadoop, e a maioria das configurações fs.s3a do Hadoop não são usadas por esses sistemas. Isso simplifica o ajuste de desempenho, eliminando a necessidade de aprender e testar várias configurações do Hadoop S3A.

A partir desse resultado de benchmark, podemos concluir que o sistema de análise de Big Data otimizado para workloads baseados em S3 é um fator de desempenho importante. As casas de repouso modernas otimizam a execução de consultas, utilizam metadados de forma eficiente e fornecem acesso contínuo a dados S3, resultando em melhor desempenho em comparação com o Hive ao trabalhar com armazenamento S3.

Consulte esta "página" secção para configurar a fonte de dados do Dremio S3 com o StorageGRID.

Visite os links abaixo para saber mais sobre como o StorageGRID e o Dremio trabalham juntos para fornecer uma infraestrutura de data Lake moderna e eficiente e como a NetApp migrou do Hive e do HDFS para o Dremio e o StorageGRID para aprimorar drasticamente a eficiência analítica de big data.

- "Aumente o desempenho para seu big data com o NetApp StorageGRID"
- "Infraestrutura de data Lake moderna, eficiente e avançada com StorageGRID e Dremio"
- "Como a NetApp está redefinindo a experiência do Cliente com a análise de produto"

# Ajuste do Hadoop S3A

*Por Angela Cheng*

O conetor Hadoop S3A facilita a interação perfeita entre aplicativos baseados em Hadoop e o armazenamento de objetos S3. Ajustar o conetor Hadoop S3A é essencial para otimizar o desempenho ao trabalhar com storage de objetos S3. Antes de entrarmos em detalhes de ajuste, vamos ter uma compreensão básica do Hadoop e de seus componentes.

## O que é Hadoop?

**Hadoop** é uma poderosa estrutura de código aberto projetada para lidar com Data Processing e armazenamento em larga escala. Ele permite o armazenamento distribuído e o processamento paralelo entre clusters de computadores.

Os três componentes principais do Hadoop são:

- **Hadoop HDFS (Hadoop Distributed File System)**: Trata o armazenamento, quebrando dados em blocos e distribuindo-os entre nós.
- **Hadoop MapReduce**: Responsável pelo processamento de dados dividindo tarefas em blocos menores e executando-as em paralelo.
- **Hadoop YARN (mais um negociador de recursos):** "Gerencia recursos e agenda tarefas de forma eficiente"

## Hadoop HDFS e conetor S3A

O HDFS é um componente vital do ecossistema do Hadoop, desempenhando um papel crítico em Big Data Processing eficientes. O HDFS permite armazenamento e gerenciamento confiáveis. Ele garante processamento paralelo e armazenamento de dados otimizado, resultando em acesso e análise mais rápidos dos dados.

No Big Data Processing, a HDFS se destaca em fornecer armazenamento tolerante a falhas para grandes conjuntos de dados. Ele consegue isso por meio da replicação de dados. Ele pode armazenar e gerenciar grandes volumes de dados estruturados e não estruturados em um ambiente de data warehouse. Além disso, ele se integra perfeitamente aos principais frameworks de Data Processing, como Apache Spark, Hive, Pig e Flink, permitindo Data Processing escalável e eficiente. Ele é compatível com sistemas operacionais baseados em Unix (Linux), tornando-o uma escolha ideal para organizações que preferem usar ambientes baseados em Linux para seus grandes Data Processing.

À medida que o volume de dados cresceu com o tempo, a abordagem de adicionar novas máquinas ao cluster Hadoop com sua própria computação e storage tornou-se ineficiente. O dimensionamento linear cria desafios para o uso eficiente de recursos e o gerenciamento da infraestrutura.

Para lidar com esses desafios, o conector Hadoop S3A oferece e/S de alto desempenho em relação ao storage de objetos S3. A implementação de um fluxo de trabalho do Hadoop com o S3A ajuda você a utilizar o storage de objetos como repositório de dados e permite separar a computação e o storage, o que, por sua vez, permite escalar a computação e o storage de forma independente. A dissociação da computação e do storage também permite que você dedique a quantidade certa de recursos para suas tarefas de computação e forneça capacidade com base no tamanho do conjunto de dados. Portanto, você pode reduzir o TCO geral para workflows do Hadoop.

## Ajuste do conetor Hadoop S3A

O S3 se comporta de forma diferente do HDFS, e algumas tentativas de preservar a aparência de um sistema de arquivos são agressivamente subótimas. Ajustes/testes/experiências cuidadosos são necessários para fazer o uso mais eficiente dos recursos do S3.

As opções do Hadoop neste documento são baseadas no Hadoop 3,3.5, "Hadoop 3.3.5 core-site.xml" consulte para obter todas as opções disponíveis.

Observação – o valor padrão de algumas configurações do Hadoop fs.s3a é diferente em cada versão do Hadoop. Certifique-se de verificar o valor padrão específico para sua versão atual do Hadoop. Se essas configurações não forem especificadas no Hadoop core-site.xml, o valor padrão será usado. Você pode substituir o valor no tempo de execução usando as opções de configuração Spark ou Hive.

Você deve ir a isso "Página do Apache Hadoop" para entender cada fs.s3a opções. Se possível, teste-os no cluster Hadoop que não é de produção para encontrar os valores ideais.

Você deve ler "Maximizar o desempenho ao trabalhar com o conetor S3A" para outras recomendações de ajuste.

Vamos explorar algumas considerações principais:

**1. Compressão de dados**

Não ative a compressão StorageGRID. A maioria dos sistemas de big data usa o intervalo de bytes get em vez de recuperar todo o objeto. Usar o intervalo de bytes Get com objetos compatados degradam significativamente o desempenho DO GET.

**2. S3A committers**

Em geral, Magic s3a committer é recomendado. Consulte isso "Página de opções comuns do committer S3A" para obter uma melhor compreensão do committer mágico e suas configurações s3a relacionadas.

Committer mágico:

O committer Magic depende especificamente do S3Guard para oferecer listas de diretórios consistentes no armazenamento de objetos S3.

Com S3 consistente (que agora é o caso), o committer Magic pode ser usado com segurança com qualquer bucket S3.

Escolha e experimentação:

Dependendo do seu caso de uso, você pode escolher entre o committer Staging (que depende de um sistema de arquivos HDFS de cluster) e o committer Magic.

Faça experimentos com ambos para determinar o que melhor se adapta à sua carga de trabalho e aos requisitos.

Em resumo, os committers S3A fornecem uma solução para o desafio fundamental do compromisso de produção consistente, de alto desempenho e confiável para S3. Seu design interno garante transferência eficiente de dados, mantendo a integridade dos dados.

| Option | Meaning | Default (Hadoop 3.3.5) |
|---|---|---|
| fs.s3a.committer.name | Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic". | file |
| fs.s3a.buffer.dir | Local filesystem directory for data being written and/or staged. | ${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a |
| fs.s3a.committer.magic.enabled | Enable “magic committer” support in the filesystem. | true |
| fs.s3a.committer.abort.pending.uploads | list and abort all pending uploads under the destination path when the job is committed or aborted. | true |
| fs.s3a.committer.threads | Number of threads in committers for parallel operations on files. | 8 |
| fs.s3a.committer.generate.uuid | Generate a Job UUID if none is passed down from Spark | false |
| fs.s3a.committer.require.uuid | Require the Job UUID to be passed down from Spark | false |
| mapreduce.fileoutputcommitter.marksuccessfuljobs | Write a _SUCCESS file on the successful completion of the job. | true |
| mapreduce.outputcommitter.factory.scheme.s3a | The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml) | org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory |

### 3. Thread, tamanhos do pool de conexão e tamanho do bloco

- Cada cliente **S3A** interagindo com um único bucket tem seu próprio pool dedicado de conexões HTTP 1,1 abertas e threads para operações de upload e cópia.
- "Você pode ajustar esses tamanhos de pool para encontrar um equilíbrio entre desempenho e uso de memória/thread".
- Ao carregar dados para S3, ele é dividido em blocos. O tamanho padrão do bloco é de 32 MB. Você pode personalizar esse valor definindo a propriedade fs.s3a.block.size.
- Tamanhos de bloco maiores podem melhorar o desempenho para grandes carregamentos de dados, reduzindo a sobrecarga de gerenciamento de peças multipeças durante o upload. O valor recomendado é de 256 MB ou superior para um conjunto de dados grande.

| Option | Meaning | Default (Hadoop 3.3.5) |
|---|---|---|
| fs.s3a.threads.max | The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*. | 64 |
| fs.s3a.connection.maximum | Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections. | 96 |
| fs.s3a.max.total.tasks | The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max. | 32 |
| fs.s3a.committer.threads | Number of threads in committers for parallel operations on files (upload, commit, abort, delete...) | 8 |
| fs.s3a.executor.capacity | The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool. | 16 |
| fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option) | Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool. | 4 |
| fs.s3a.block.size | Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value. | 32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write) |

### 4. Carregamento multipart

s3a committers **Always** Use MPU (multipart upload) para carregar dados para o bucket S3. Isso é necessário para permitir: Falha de tarefa, execução especulativa de tarefas e abortos de trabalho antes de cometer. Aqui estão algumas especificações-chave relacionadas a carregamentos de várias partes:

- Tamanho máximo do objeto: 5 TIB (terabytes).
- Número máximo de peças por upload: 10.000.
- Números de peça: Variando de 1 a 10.000 (inclusive).
- Tamanho da peça: Entre 5 MIB e 5 GiB. Notavelmente, não há limite mínimo de tamanho para a última parte do upload de várias partes.

Usar um tamanho de peça menor para uploads S3 multipart tem vantagens e desvantagens.

**Vantagens**:

- Recuperação rápida de problemas de rede: Quando você carrega partes menores, o impactos de reiniciar um upload com falha devido a um erro de rede é minimizado. Se uma peça falhar, você só precisa fazer o upload dessa peça específica em vez de todo o objeto.

- Melhor Parallelization: Mais partes podem ser carregadas em paralelo, aproveitando-se de conexões simultâneas ou multithreading. Essa paralelização melhora o desempenho, especialmente ao lidar com arquivos grandes.

**Desvantagem**:

- Sobrecarga de rede: Tamanho de peça menor significa mais partes para carregar, cada parte requer sua própria solicitação HTTP. Mais solicitações HTTP aumentam a sobrecarga de iniciar e concluir solicitações individuais. Gerenciar um grande número de peças pequenas pode afetar o desempenho.
- Complexidade: Gerenciar a ordem, rastrear peças e garantir que os uploads bem-sucedidos possam ser complicados. Se o upload precisar ser abortado, todas as peças que já foram carregadas precisam ser rastreadas e removidas.

Para Hadoop, 256MB ou acima do tamanho da peça é recomendado para fs.s3a.multipart.size. Sempre defina o valor fs.s3a.mutlipart.threshold para 2 x fs.s3a.multipart.size. Por exemplo, se fs.s3a.multipart.size for 256M, fs.s3a.mutlipart.threshold deve ser 512M.

Use um tamanho de peça maior para um conjunto de dados grande. É importante escolher um tamanho de peça que equilibre esses fatores com base em seu caso de uso específico e condições de rede.

Um upload multipart é "processo de três etapas" um :

1. O upload é iniciado, o StorageGRID retorna um ID de upload.
2. As partes do objeto são carregadas usando o upload-id.
3. Uma vez que todas as partes do objeto são carregadas, envia a solicitação de upload de várias partes completa com upload-id. O StorageGRID constrói o objeto a partir das partes carregadas, e o cliente pode acessar o objeto.

Se a solicitação completa de upload de várias peças não for enviada com sucesso, as peças permanecem no StorageGRID e não criam nenhum objeto. Isto acontece quando os trabalhos são interrompidos, falhados ou abortados. As peças permanecem na grade até que o upload de várias partes seja concluído ou abortado ou o StorageGRID apague essas peças se decorrerem 15 dias desde que o upload foi iniciado. Se houver muitos (algumas centenas de milhares a milhões) uploads em andamento em várias partes em um bucket, quando o Hadoop enviar 'list-multipart-uploads' (essa solicitação não filtra pelo ID de upload), a solicitação pode levar muito tempo para ser concluída ou, eventualmente, acabar. Você pode considerar definir fs.s3a.mutlipart.purge como true com um valor adequado fs.s3a.multipart.purge.age (por exemplo, 5 a 7 dias, não use o valor padrão de 86400 ou seja, 1 dia). Ou acione o suporte do NetApp para investigar a situação.

| Option | Meaning | Default (Hadoop 3.3.5) |
|---|---|---|
| fs.s3a.multipart.size | How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value. | 64M |
| fs.s3a.multipart.threshold | How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value. | 128M |
| fs.s3a.multipart.purge | True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations. | false |
| fs.s3a.multipart.purge.age | Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true | 86400 |

**5. Memória intermédia de gravação de dados na memória**

Para melhorar o desempenho, você pode armazenar dados de gravação em buffer na memória antes de enviá-los para S3. Isso pode reduzir o número de pequenas gravações e melhorar a eficiência.

| Option | Meaning | Default (Hadoop 3.3.5) |
|---|---|---|
| fs.s3a.fast.upload.buffer | The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items. | disk |

Lembre-se de que o S3 e o HDFS funcionam de maneiras distintas. O ajuste cuidadoso/teste/experiência é

necessário para fazer o uso mais eficiente dos recursos do S3.

# TR-4871: Configure o StorageGRID para backup e recuperação com o CommVault

## Faça backup e recupere dados usando o StorageGRID e o CommVault

A CommVault e a NetApp fizeram uma parceria para criar uma solução de proteção de dados conjunta que combina o software CommVault Complete Backup and Recovery for NetApp com o software NetApp StorageGRID para storage de nuvem. O CommVault Complete Backup and Recovery e o NetApp StorageGRID oferecem soluções exclusivas e fáceis de usar que trabalham juntas para ajudar você a atender às demandas de crescimento rápido de dados e aumento das regulamentações no mundo todo.

Muitas organizações querem migrar o storage para a nuvem, escalar os sistemas e automatizar a política para retenção de dados a longo prazo. O storage de objetos baseado em nuvem é conhecido por sua resiliência, capacidade de escala e eficiências operacionais e de custo que o tornam uma escolha natural como destino para o seu backup. A CommVault e a NetApp juntas certificaram sua solução combinada em 2014 e, desde então, desenvolveram uma integração mais profunda entre suas duas soluções. Clientes de todos os tipos em todo o mundo adotaram a solução combinada de backup e recuperação CommVault Complete e StorageGRID.

### Sobre a CommVault e o StorageGRID

O software CommVault Complete Backup and Recovery é uma solução de gerenciamento de informações e dados integrada de nível empresarial, desenvolvida do zero em uma única plataforma e com uma base de código unificada. Todas as suas funções compartilham tecnologias de back-end, trazendo vantagens e benefícios incomparáveis de uma abordagem totalmente integrada para proteger, gerenciar e acessar seus dados. O software contém módulos para proteger, arquivar, analisar, replicar e pesquisar seus dados. Os módulos compartilham um conjunto comum de serviços de back-end e recursos avançados que interagem perfeitamente uns com os outros. A solução aborda todos os aspectos do gerenciamento de dados em sua empresa, ao mesmo tempo em que oferece escalabilidade infinita e controle sem precedentes de dados e informações.

O NetApp StorageGRID como uma categoria de nuvem CommVault é uma solução empresarial de storage de objetos para nuvem híbrida. Você pode implantá-lo em vários sites, seja em um dispositivo criado sob medida ou como uma implantação definida por software. O StorageGRID permite que você estabeleça políticas de gerenciamento de dados que determinem como os dados são armazenados e protegidos. A StorageGRID coleta as informações necessárias para desenvolver e aplicar políticas. Ele examina uma ampla gama de caraterísticas e necessidades, incluindo desempenho, durabilidade, disponibilidade, localização geográfica, longevidade e custo. Os dados são totalmente mantidos e protegidos à medida que se movem entre locais e à medida que envelhecem.

O mecanismo de política inteligente StorageGRID ajuda você a escolher uma das seguintes opções:

- Usar codificação de apagamento para fazer backup de dados em vários locais para resiliência.
- Copiar objetos para locais remotos para minimizar a latência e o custo da WAN.

Quando o StorageGRID armazena um objeto, você o acessa como um objeto, independentemente de onde ele esteja ou quantas cópias existem. Esse comportamento é crucial para a recuperação de desastres, porque com ele, mesmo que uma cópia de backup de seus dados esteja corrompida, o StorageGRID é capaz de restaurar seus dados.

Reter dados de backup em seu storage primário pode ser caro. Ao usar o NetApp StorageGRID, você libera espaço no storage primário migrando dados de backup inativos para o StorageGRID, enquanto aproveita as diversas funcionalidades do StorageGRID. O valor dos dados de backup muda ao longo do tempo, assim como o custo de armazená-los. O StorageGRID pode minimizar o custo do storage primário e aumentar a durabilidade dos dados.

### Principais recursos

Os principais recursos da plataforma de software CommVault incluem:

- Uma solução completa de proteção de dados compatível com todos os principais sistemas operacionais, aplicações e bancos de dados em servidores virtuais e físicos, sistemas nas, infraestruturas baseadas em nuvem e dispositivos móveis.
- Gerenciamento simplificado por meio de um único console: Você pode visualizar, gerenciar e acessar todas as funções e todos os dados e informações da empresa.
- Vários métodos de proteção, incluindo backup e arquivamento de dados, gerenciamento de snapshot, replicação de dados e indexação de conteúdo para e-Discovery.
- Gerenciamento eficiente de storage usando deduplicação em disco e storage de nuvem.
- Integração com matrizes de armazenamento NetApp, como AFF, FAS, NetApp HCI e e-Series, e sistemas de armazenamento de escalabilidade horizontal NetApp SolidFire. Integração também com o software NetApp Cloud Volumes ONTAP para automatizar a criação de cópias NetApp Snapshot indexadas e com reconhecimento de aplicações em todo o portfólio de storage da NetApp.
- Gerenciamento completo da infraestrutura virtual compatível com os principais hypervisors virtuais no local e plataformas de hyperscaler de nuvem pública.
- Recursos avançados de segurança para limitar o acesso a dados essenciais, fornecer recursos de gerenciamento granular e fornecer acesso de logon único para usuários do ative Directory.
- Gerenciamento de dados baseado em políticas que permite gerenciar seus dados com base nas necessidades empresariais, e não no local físico.
- Uma experiência de usuário final de ponta, capacitando seus usuários a proteger, encontrar e recuperar seus próprios dados.
- Automação orientada por API, permitindo que você use ferramentas de terceiros, como o vRealize Automation ou o Service Now, para gerenciar suas operações de proteção e recuperação de dados.

Para obter detalhes sobre workloads compatíveis, visite "Tecnologias compatíveis do CommVault".

### Opções de backup

Ao implementar o software CommVault Complete Backup and Recovery com storage de nuvem, você tem duas opções de backup:

- Faça backup em um destino de disco primário e também faça backup de uma cópia auxiliar no armazenamento em nuvem.
- Fazer backup no storage de nuvem como destino principal.

No passado, o storage de objetos ou nuvem era considerado de baixa performance para ser usado no backup primário. O uso de um destino de disco primário permitiu que os clientes tivessem processos de backup e restauração mais rápidos e mantessem uma cópia auxiliar na nuvem como um backup inativo. O StorageGRID representa a próxima geração de storage de objetos. O StorageGRID oferece alta performance e taxa de transferência massiva, além de performance e flexibilidade além do que outros fornecedores de storage de objetos oferecem.

A tabela a seguir lista os benefícios de cada opção de backup com o StorageGRID:

| | **Backup primário para disco e uma cópia auxiliar para StorageGRID** | **Backup primário para StorageGRID** |
|---|---|---|
| Desempenho | Tempo de recuperação mais rápido, usando montagem em tempo real ou recuperação em tempo real: Ideal para workloads Tier0/Tier1. | Não pode ser utilizado para operações de montagem em tempo real ou de recuperação em tempo real. Ideal para operação de restauração de streaming e para retenção de longo prazo. |
| Arquitetura de implantação | Usa o all-flash ou um disco giratório como primeira camada inicial de backup. StorageGRID é usado como um nível secundário. | Simplifica a implantação usando o StorageGRID como destino de backup completo. |
| Recursos avançados (restauração ao vivo) | Suportado | Não suportado |

#### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Centro de Documentação do StorageGRID 11,9 https://docs.netapp.com/us-en/storagegrid-119/
- Documentação do produto NetApp https://docs.netapp.com
- Documentação do CommVault https://documentation.commvault.com/2024/essential/index.html

## Visão geral da solução testada

A solução testada combina as soluções CommVault e NetApp para criar uma solução conjunta poderosa.

#### Configuração da solução

Na configuração do laboratório, o ambiente StorageGRID consistia em quatro dispositivos NetApp StorageGRID SG5712, um nó de administração principal virtual e um nó de gateway virtual. O dispositivo SG5712 é a opção de nível de entrada, uma configuração de linha de base. A escolha de opções de dispositivos de maior performance, como o NetApp StorageGRID SG5760 ou o SG6060, pode fornecer benefícios significativos de performance. Consulte o arquiteto de soluções da NetApp StorageGRID para obter assistência sobre o dimensionamento.

Na política de proteção de dados, o StorageGRID usa uma política de gerenciamento de ciclo de vida integrado (ILM) para gerenciar e proteger os dados. As regras do ILM são avaliadas em uma política de cima para baixo. Implementamos a política ILM mostrada na seguinte tabela:

| Regra ILM | Qualificadores | Comportamento de ingestão |
|---|---|---|
| Codificação de apagamento 2-1 | Objetos acima de 200KB | Equilibrado |
| 2 cópia | Todos os objetos | Commit duplo |

A regra de cópia ILM 2 é a regra padrão. A regra de codificação de apagamento 2-1 foi aplicada para este teste a qualquer objeto 200KB ou maior. A regra padrão foi aplicada a objetos menores que 200KB. A aplicação das regras desta forma é uma melhor prática do StorageGRID.

Para obter detalhes técnicos sobre esse ambiente de teste, leia a seção Design da solução e práticas recomendadas no "Proteção de dados com escalabilidade horizontal do NetApp com o CommVault" relatório técnico.

### Especificações de hardware da StorageGRID

A tabela a seguir descreve o hardware NetApp StorageGRID usado neste teste. O dispositivo StorageGRID SG5712 com rede 10Gbps é a opção de nível de entrada e representa uma configuração de linha de base. Opcionalmente, o SG5712 pode ser configurado para rede 25GbpsG.

| Hardware | Quantidade | Disco | Capacidade utilizável | Rede |
|---|---|---|---|---|
| Aparelhos StorageGRID SG5712 | 4 | 48 x 4TB (HDD SAS near-line) | 136 TB | 10Gbps |

A escolha de opções de dispositivo de alta performance, como os dispositivos NetApp StorageGRID SG5760, SG6060 ou All Flash SGF6112, pode fornecer benefícios significativos de desempenho. Consulte o arquiteto de soluções da NetApp StorageGRID para obter assistência sobre o dimensionamento.

### Requisitos de software CommVault e StorageGRID

As tabelas a seguir listam os requisitos de software para o software CommVault e NetApp StorageGRID instalados no software VMware para nossos testes. Quatro gerenciadores de transmissão de dados do MediaAgent e um servidor CommServe foram instalados. No teste, a rede 10GbpsG foi implementada para a infraestrutura VMware. A tabela a seguir

A tabela a seguir lista todos os requisitos de sistema do software CommVault:

| Componente | Quantidade | Armazenamento de dados | Tamanho | Total | Total de IOPS necessário |
|---|---|---|---|---|---|
| Servidor CommServe | 1 | SO | 500 GB | 500 GB | n/a. |
| | | SQL | 500 GB | 500 GB | n/a. |
| MediaAgent | 4 | CPU virtual (vCPU) | 16 | 64 | n/a. |

| Componente | Quantidade | Armazenamento de dados | Tamanho | Total | Total de IOPS necessário |
|---|---|---|---|---|---|
| | | RAM | 128 GB | 512 | n/a. |
| | | SO | 500 GB | 2 TB | n/a. |
| | | Cache de índice | 2 TB | 8 TB | Mais de 200 anos |
| | | DDB | 2 TB | 8 TB | 200-80.000K |

No ambiente de teste, um nó de administrador principal virtual e um nó de gateway virtual foram implantados no VMware em um storage array do NetApp e-Series E2812. Cada nó estava em um servidor separado com os requisitos mínimos de ambiente de produção descritos na tabela a seguir:

A tabela a seguir lista os requisitos para nós de administração virtual do StorageGRID e nós de gateway:

| Tipo de nó | Quantidade | VCPU | RAM | Armazenamento |
|---|---|---|---|---|
| Nó de gateway | 1 | 8 | 24 GB | 100GB LUN para o SO |
| Nó de administrador | 1 | 8 | 24 GB | 100GB LUN para o SO<br><br>200GB LUN para tabelas de nó Admin<br><br>200GB LUN para o log de auditoria do nó Admin |

## Orientação de dimensionamento do StorageGRID

Consulte os especialistas em proteção de dados da NetApp para obter um dimensionamento específico para o seu ambiente. Especialistas em proteção de dados da NetApp podem usar a ferramenta Calculadora de storage de CommVault Total Backup para estimar os requisitos da infraestrutura de backup. A ferramenta requer acesso ao CommVault Partner Portal. Inscreva-se para ter acesso, se necessário.

#### Entradas de dimensionamento do CommVault

As tarefas a seguir podem ser usadas para realizar a descoberta para o dimensionamento da solução de proteção de dados:

- Identifique as cargas de trabalho do sistema ou aplicativo/banco de dados e a capacidade de front-end correspondente (em terabytes [TB]) que precisarão ser protegidas.
- Identifique a carga de trabalho de VM/arquivo e a capacidade front-end (TB) semelhante que precisará ser

protegida.

- Identificar requisitos de retenção de curto e longo prazo.
- Identifique a taxa de alteração de % diária para os conjuntos de dados/workloads identificados.
- Identificar o crescimento projetado dos dados nos próximos 12, 24 e 36 meses.
- Defina o rto e o RPO para proteção/recuperação de dados de acordo com as necessidades dos negócios.

Quando essas informações estiverem disponíveis, o dimensionamento da infraestrutura de backup pode ser feito, resultando em uma repartição das capacidades de storage necessárias.

**Orientação de dimensionamento do StorageGRID**

Antes de executar o dimensionamento do NetApp StorageGRID, considere esses aspectos da sua carga de trabalho:

- Capacidade utilizável
- Modo WORM
- Tamanho médio do objeto
- Requisitos de desempenho
- Política de ILM aplicada

A quantidade de capacidade utilizável precisa acomodar o tamanho do workload de backup categorizado no StorageGRID e o cronograma de retenção.

O modo WORM será ativado ou não? Com WORM ativado no CommVault, isso configurará o bloqueio de objetos no StorageGRID. Isso aumentará a capacidade de armazenamento de objetos necessária. A quantidade de capacidade necessária varia de acordo com a duração de retenção e o número de alterações de objeto em cada backup.

O tamanho médio do objeto é um parâmetro de entrada que ajuda no dimensionamento para o desempenho em um ambiente StorageGRID. Os tamanhos médios de objetos usados para um workload do CommVault dependem do tipo de backup.

A tabela a seguir lista tamanhos médios de objetos por tipo de backup e descreve o que o processo de restauração lê do armazenamento de objetos:

| Tipo de cópia de segurança | Tamanho médio do objeto | Restaurar o comportamento |
|---|---|---|
| Faça uma cópia auxiliar no StorageGRID | 32 MB | Leitura completa do objeto 32MBD. |
| Direcionar o backup para o StorageGRID (deduplicação habilitada) | 8 MB | 1MB leitura aleatória |
| Direcionar o backup para o StorageGRID (deduplicação desativada) | 32 MB | Leitura completa do objeto 32MBD. |

Além disso, compreender os requisitos de performance para backups completos e incrementais ajuda a determinar o dimensionamento dos nós de storage da StorageGRID. Os métodos de proteção de dados da

política de gerenciamento de ciclo de vida das informações do StorageGRID (ILM) determinam a capacidade necessária para armazenar backups da CommVault e afetar o dimensionamento da grade.

A replicação StorageGRID ILM é um dos dois mecanismos usados pelo StorageGRID para armazenar dados de objetos. Quando o StorageGRID atribui objetos a uma regra de ILM que replica dados, o sistema cria cópias exatas dos dados dos objetos e armazena as cópias em nós de storage.

A codificação de apagamento é o segundo método usado pelo StorageGRID para armazenar dados de objetos. Quando o StorageGRID atribui objetos a uma regra ILM que está configurada para criar cópias codificadas de apagamento, ele segmenta dados de objeto em fragmentos de dados. Em seguida, ele 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 fragmento de dados ou um fragmento de paridade ficar corrompido ou for perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos dados restantes e fragmentos de paridade.

Os dois mecanismos exigem quantidades diferentes de armazenamento, como estes exemplos demonstram:

- Se você armazenar duas cópias replicadas, a sobrecarga de storage será duplicada.
- Se você armazenar uma 2 cópia codificada de apagamento por mais de 1 vezes, a sobrecarga de storage aumenta em 1,5 vezes.

Para a solução testada, foi usada uma implantação de StorageGRID de nível básico em um único local:

- Nó de administrador: Máquina virtual VMware (VM)
- Balanceador de carga: VM VMware
- Nós de storage: 4x SG5712 TB com 4TB unidades
- Nó de administrador principal e nó de gateway: VMs VMware com os requisitos mínimos de workload de produção

O StorageGRID também é compatível com balanceadores de carga de terceiros.

O StorageGRID normalmente é implantado em dois ou mais locais com políticas de proteção de dados que replicam dados para proteção contra falhas em nível de nó e local. Ao fazer backup dos dados no StorageGRID, os dados são protegidos por várias cópias ou por codificação de apagamento que separa e remonta os dados de forma confiável por meio de um algoritmo.

Você pode usar a ferramenta de dimensionamento "Fusion" para dimensionar sua grade.

**Dimensionamento**

Você pode expandir um sistema NetApp StorageGRID adicionando storage aos nós de storage, adicionando novos nós de grade a um local existente ou adicionando um novo local de data center. Você pode realizar expansões sem interromper a operação do seu sistema atual. O StorageGRID dimensiona a performance usando nós de performance mais alta para nós de storage ou o dispositivo físico que executa o balanceador de carga e os nós de administração ou simplesmente adicionando nós adicionais.

Para obter mais informações sobre como expandir o sistema StorageGRID, "Guia de expansão do StorageGRID 11,9" consulte .

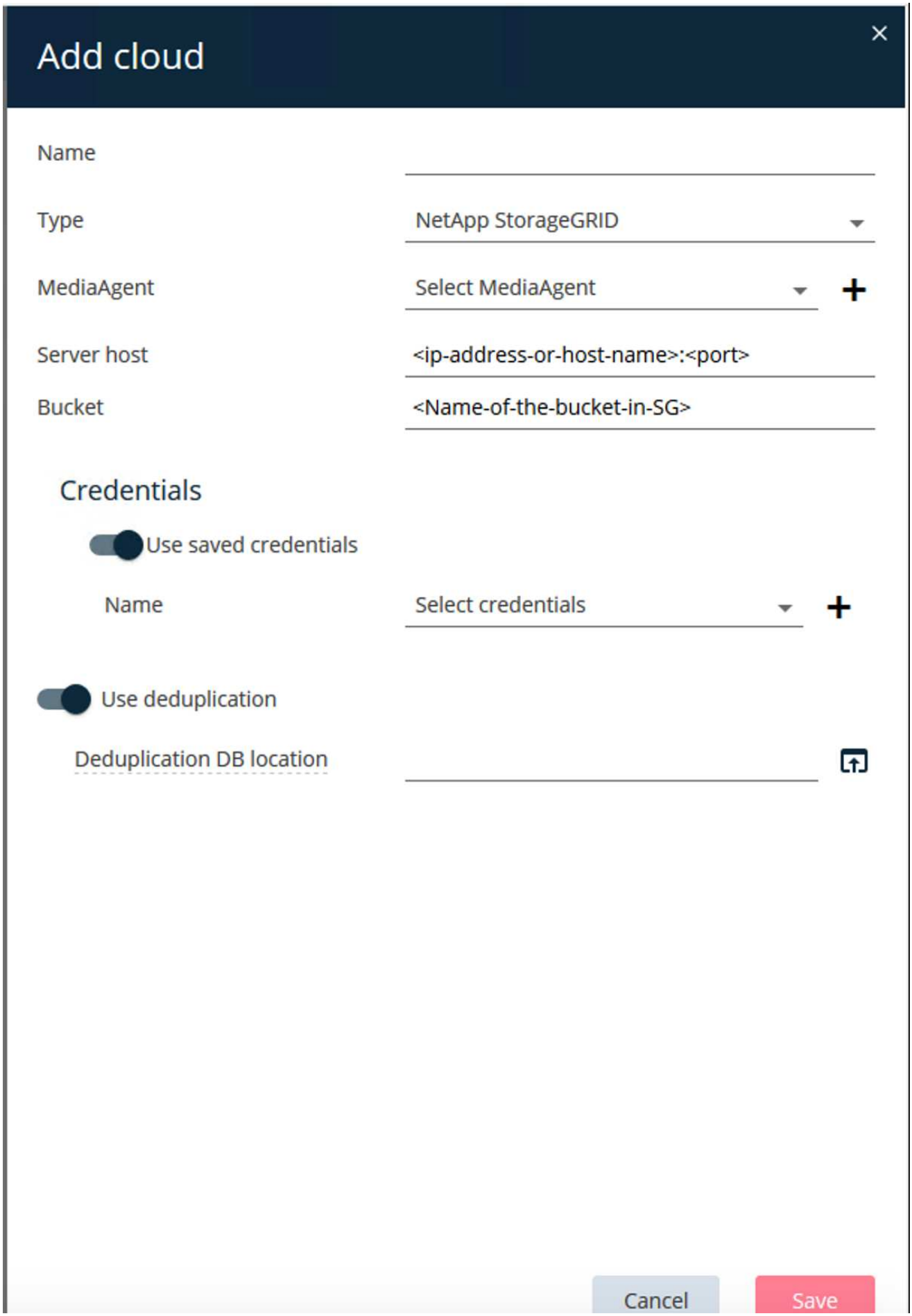
## Execute um trabalho de proteção de dados

Para configurar o StorageGRID com o CommVault Complete Backup and Recovery for NetApp, as etapas a seguir foram executadas para adicionar o StorageGRID como uma biblioteca de nuvem no software CommVault.

### Etapa 1: Configurar o CommVault com StorageGRID

**Passos**

1. Faça login no CommVault Command Center. No painel esquerdo, clique em armazenamento > nuvem > Adicionar para ver e responder à caixa de diálogo Adicionar nuvem:


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Para tipo, selecione NetApp StorageGRID.
3. No MediaAgent, selecione todos os associados à biblioteca na nuvem.
4. Para o host do servidor, insira o endereço IP ou o nome do host do endpoint do StorageGRID e o número da porta.

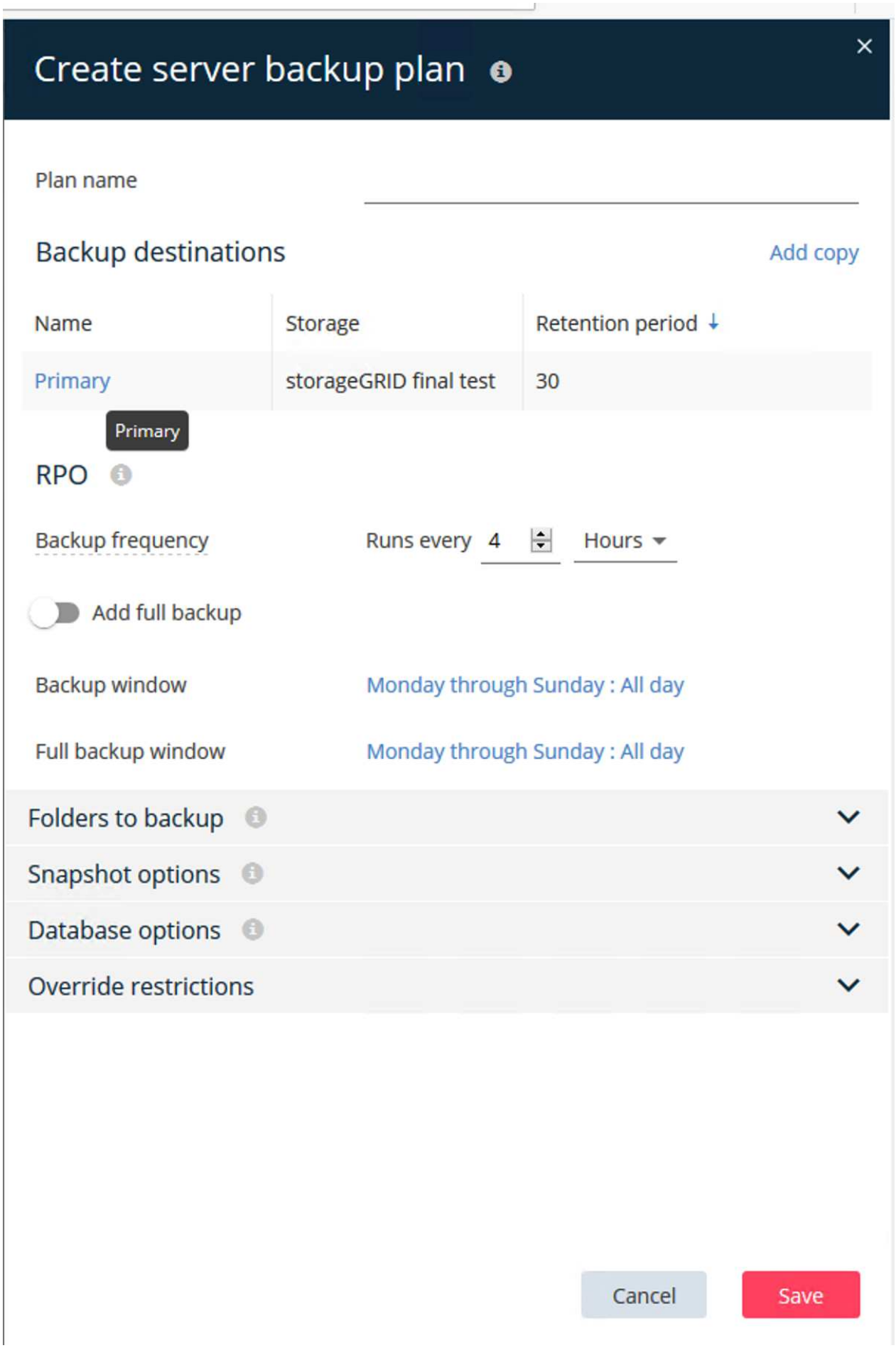
   Siga as etapas na documentação do StorageGRID no "como configurar um ponto de extremidade do balanceador de carga (porta)". Certifique-se de que tem uma porta HTTPS com um certificado auto-assinado e o endereço IP ou o nome de domínio do endpoint StorageGRID.

5. Se você quiser usar a deduplicação, ative essa opção e forneça o caminho para o local do banco de dados de deduplicação.
6. Clique em Guardar.

### Passo 2: Crie um plano de backup com o StorageGRID como destino principal

**Passos**

1. No painel esquerdo, selecione Gerenciar > planos para ver e responder à caixa de diálogo criar Plano de Backup do servidor.

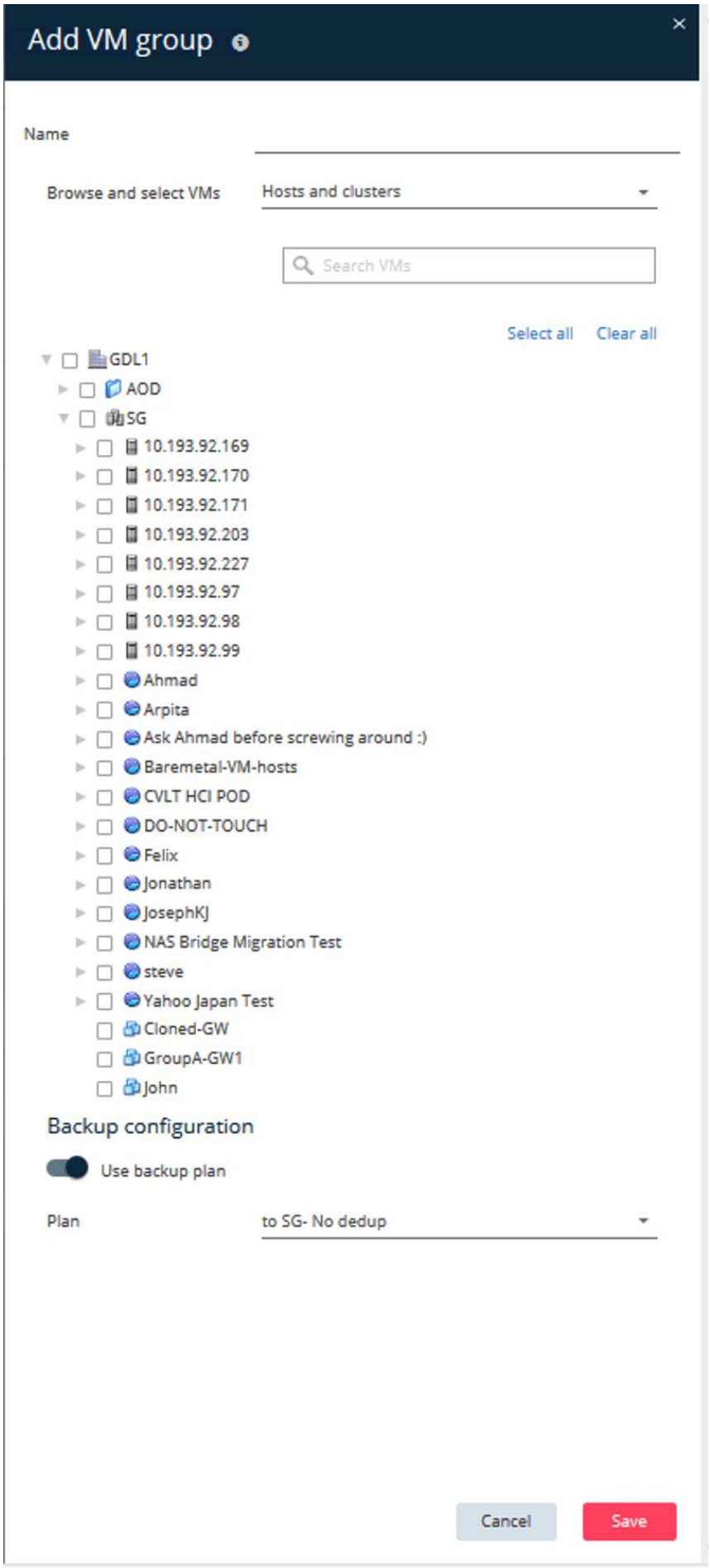

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Introduza um nome de plano.
3. Selecione o destino de backup de armazenamento do Serviço de armazenamento simples (S3) do StorageGRID que você criou anteriormente.
4. Digite o período de retenção do backup e o objetivo do ponto de restauração (RPO) que você deseja.
5. Clique em Guardar.

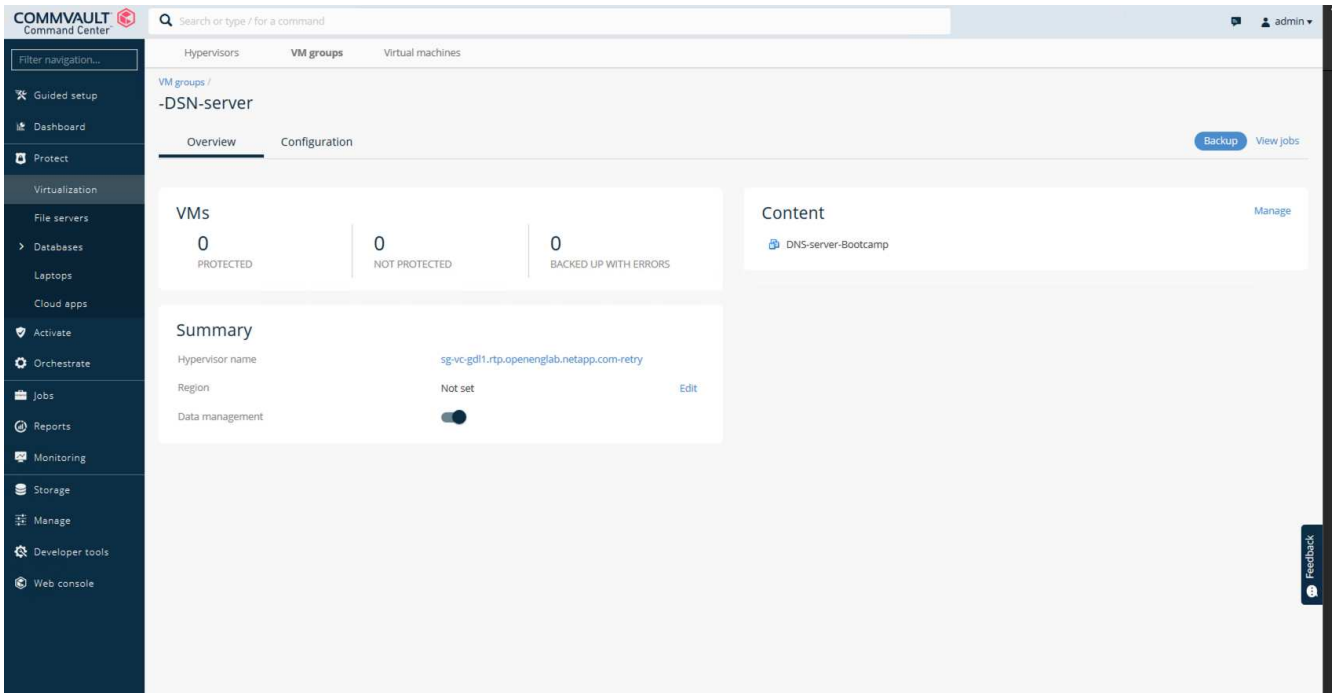
### Etapa 3: Inicie um trabalho de backup para proteger suas cargas de trabalho

**Passos**

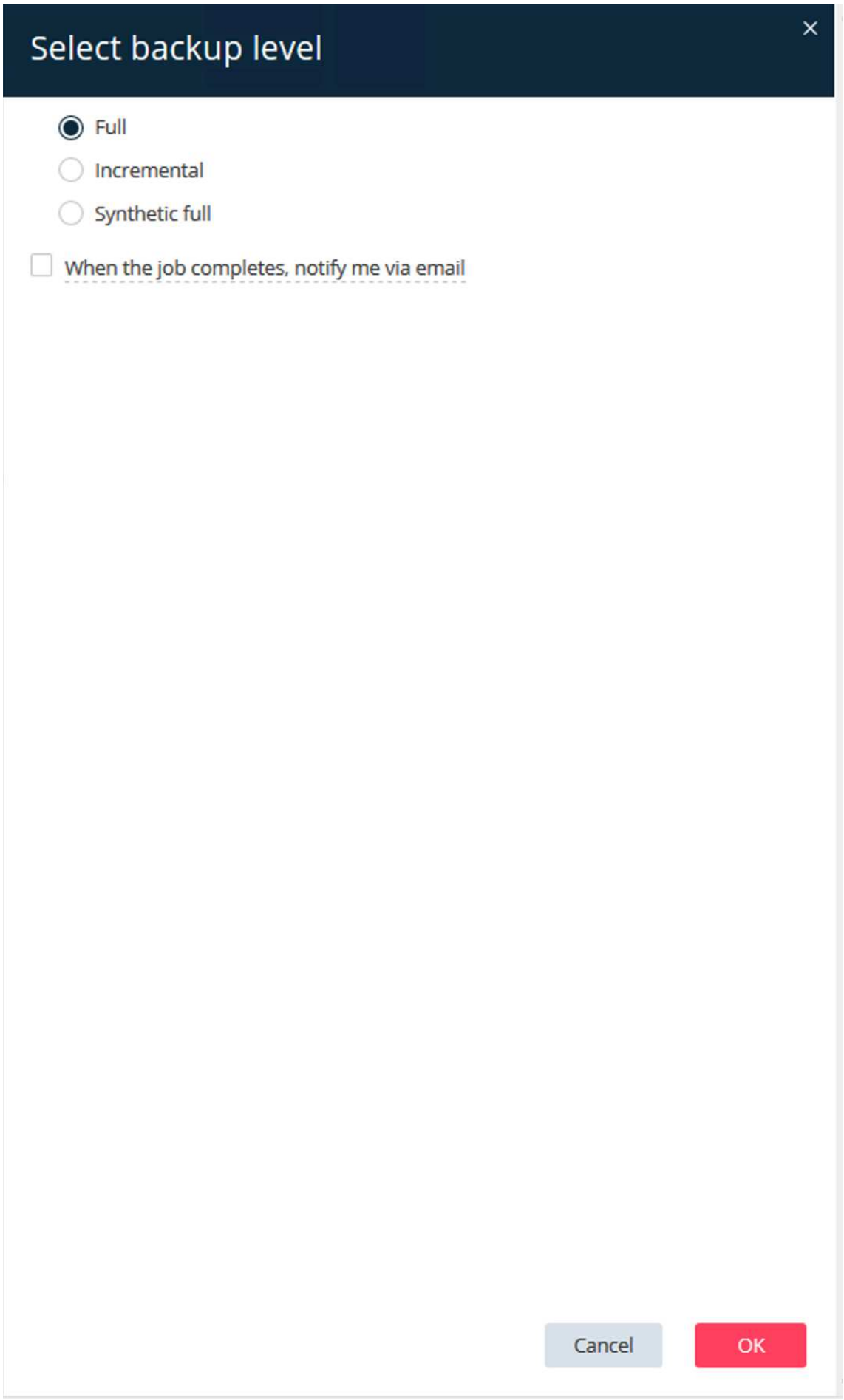
1. No CommVault Command Center, navegue para proteger > virtualização.
2. Adicione um hypervisor do VMware vCenter Server.
3. Clique no hypervisor que você acabou de adicionar.
4. Clique em Adicionar grupo VM para responder à caixa de diálogo Adicionar grupo VM para que você possa ver o ambiente do vCenter que você planeja proteger.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

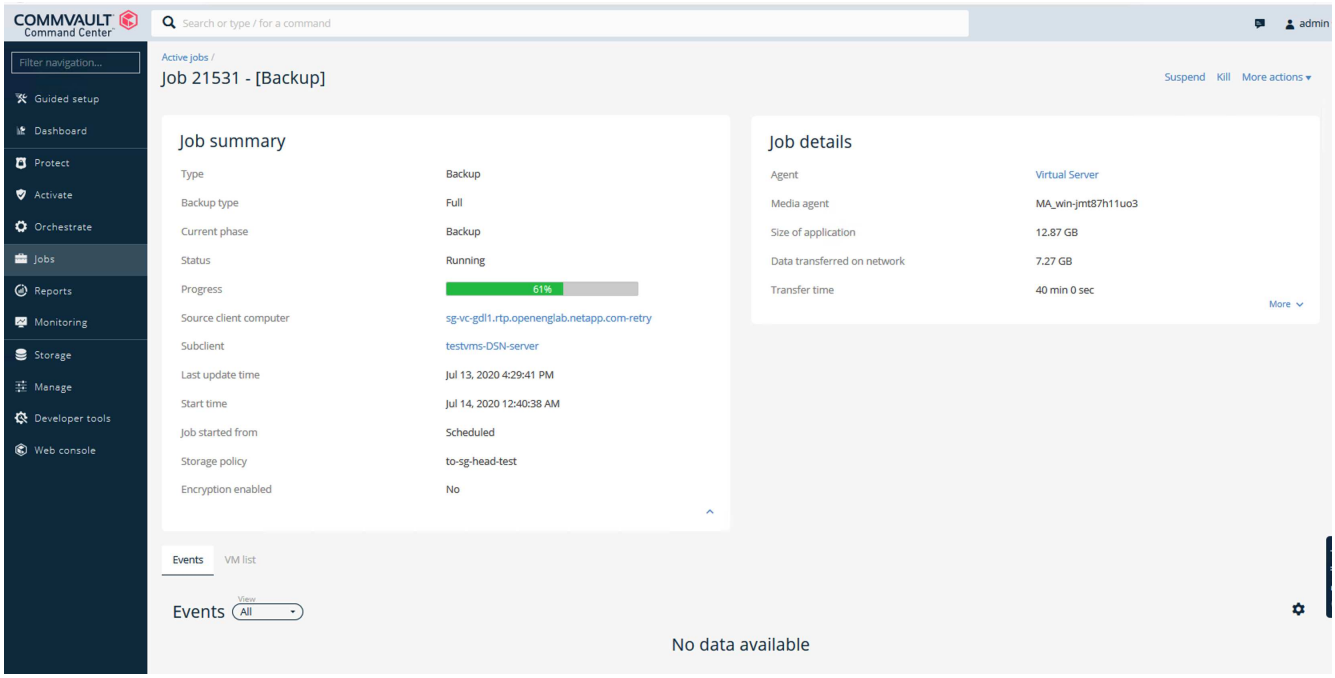
5. Selecione um datastore, uma VM ou uma coleção de VMs e insira um nome para ele.
6. Selecione o plano de cópia de segurança que criou na tarefa anterior.
7. Clique em Salvar para ver o grupo de VM que você criou.
8. No canto superior direito da janela do grupo VM, selecione Backup:




9. Selecione completo como o nível de backup, (opcionalmente) solicitar um e-mail quando o backup for concluído e clique em OK para iniciar o trabalho de backup:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Navegue até a página de resumo do trabalho para ver as métricas do trabalho:




## Reveja os testes de desempenho da linha de base

Na operação de cópia Pausa, quatro MediaAgents do CommVault fizeram backup dos dados em um sistema NetApp AFF A300 e uma cópia auxiliar foi criada no NetApp StorageGRID. Para obter detalhes sobre o ambiente de configuração de teste, leia a seção Design da solução e melhores práticas no "Proteção de dados com escalabilidade horizontal do NetApp com o CommVault" relatório técnico.

Os testes foram realizados com 100 VMs e 1000 VMs, ambos os testes com uma mistura de 50/50 VMs Windows e CentOS. A tabela a seguir mostra os resultados de nossos testes de desempenho de linha de base:

| Operação | Velocidade de cópia de segurança | Restaurar velocidade |
|---|---|---|
| Cópia AUX | 2 TB/hora | 1,27 TB/hora |
| Direto de e para objeto (deduplicação ativada) | 2,2 TB/hora | 1,22 TB/hora |

Para testar o desempenho de idade, 2,5 milhões de objetos foram excluídos. Como mostrado nas Figuras 2 e 3, a execução de exclusão foi concluída em menos de 3 horas e libertou mais de 80TBMB de espaço. O processamento de exclusão começou às 10:30 AM.

**Figura 1: Exclusão de 2,5 milhões (80TB) objetos em menos de 3 horas.**

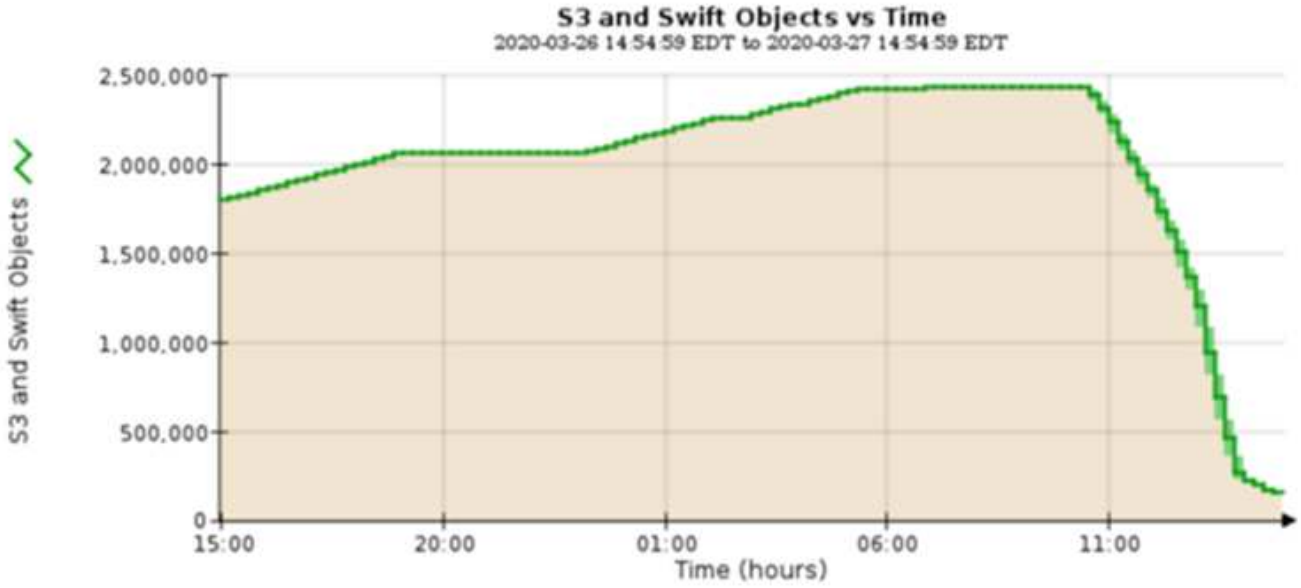
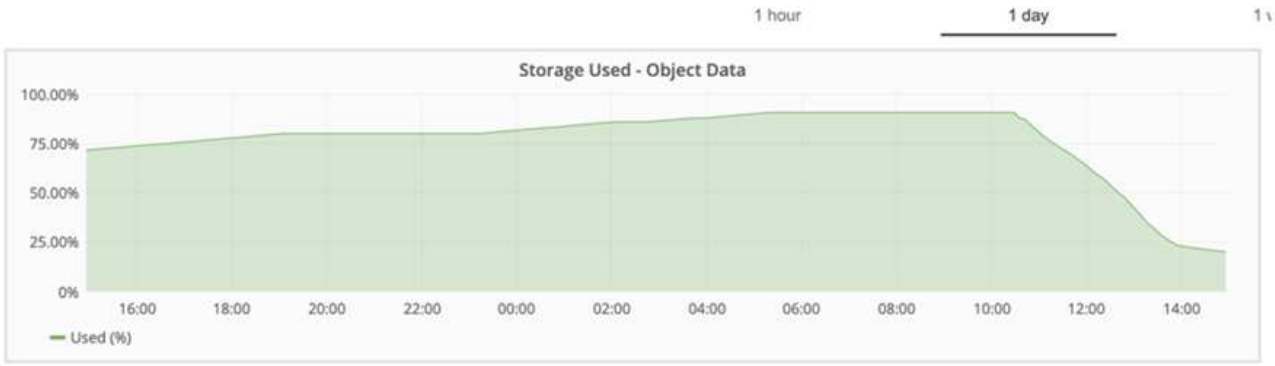



**Figura 2: Liberando 80TB TB de storage em menos de 3 horas.**




## Recomendação de nível de consistência do balde

O NetApp StorageGRID permite que o usuário final selecione o nível de consistência para operações executadas nos objetos nos buckets do Simple Storage Service (S3).

Os CommVault MediaAgents são os migradores de dados em um ambiente CommVault. Na maioria dos casos, os MediaAgents são configurados para gravar localmente em um site StorageGRID primário. Por esse motivo, recomenda-se um alto nível de consistência dentro de um local primário. Use as diretrizes a seguir quando você definir o nível de consistência nos buckets do CommVault criados no StorageGRID.

Se você tem uma versão do CommVault anterior à 11.0.0 - Service Pack 16, considere atualizar o CommVault para a versão mais recente. Se essa não for uma opção, siga as diretrizes para sua versão.

- Versões do CommVault anteriores a 11.0.0 - Service Pack 16.* Em versões anteriores a 11.0.0 - Service Pack 16, a CommVault executa S3 CABEÇAS e OBTÉM operações em objetos inexistentes como parte do processo de restauração e eliminação. Defina o nível de consistência do balde para um local seguro para obter o nível de consistência ideal para backups da CommVault para StorageGRID.
- CommVault versões 11.0.0 - Service Pack 16 e posteriores.* Nas versões 11.0.0 - Service Pack 16 e posteriores, o número de operações S3 HEAD e GET executadas em objetos inexistentes é minimizado.

Defina o nível de consistência do bucket padrão como leitura após nova gravação para garantir alto nível de consistência no ambiente CommVault e StorageGRID.

# TR-4626: Balanceadores de carga

## Use balanceadores de carga de terceiros com o StorageGRID

Saiba mais sobre o papel de balanceadores de carga globais e de terceiros em sistemas de armazenamento de objetos como o StorageGRID.

Orientação geral para a implementação do NetApp StorageGRID com balanceadores de carga de terceiros.

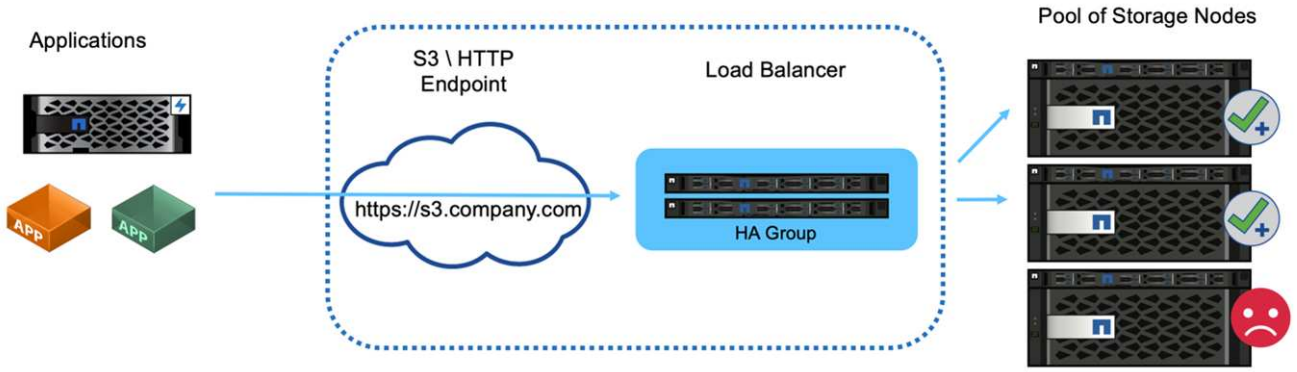
Storage de objetos é sinônimo do termo storage de nuvem e, como seria de esperar, aplicações que utilizam o storage de nuvem abordam esse storage por meio de um URL. Por trás desse URL simples, o StorageGRID pode dimensionar a capacidade, a performance e a durabilidade em um único local ou em locais distribuídos geograficamente. O componente que torna essa simplicidade possível é um balanceador de carga.

O objetivo deste documento é informar os clientes da StorageGRID sobre as opções do balanceador de carga e fornecer orientações gerais para a configuração de balanceadores de carga de terceiros.

### Noções básicas sobre o balanceador de carga

Balanceadores de carga são um componente essencial de um sistema de storage de objetos de nível empresarial, como o StorageGRID. O StorageGRID consiste em vários nós de storage, cada um dos quais pode apresentar todo o espaço de nomes do Simple Storage Service (S3) para uma determinada instância do StorageGRID. Os balanceadores de carga criam um ponto final altamente disponível atrás do qual podemos colocar nós de StorageGRID. O StorageGRID é exclusivo entre os sistemas de storage de objetos compatíveis com S3, pois fornece seu próprio balanceador de carga, mas também suporta balanceadores de carga de terceiros ou de uso geral, como F5, Citrix Netscaler, proxy de HA, NGINX e assim por diante.

A figura a seguir usa o exemplo URL/nome de domínio totalmente qualificado (FQDN) "s3.company.com". O balanceador de carga cria um IP virtual (VIP) que resolve para o FQDN através do DNS e, em seguida, direciona todas as solicitações de aplicativos para um pool de nós StorageGRID. O balanceador de carga realiza uma verificação de integridade em cada nó e estabelece apenas conexões com nós íntegros.




A figura mostra o balanceador de carga fornecido pelo StorageGRID, mas o conceito é o mesmo para balanceadores de carga de terceiros. Os aplicativos estabelecem uma sessão HTTP usando o VIP no balanceador de carga e o tráfego passa pelo balanceador de carga para os nós de storage. Por padrão, todo o tráfego, da aplicação ao balanceador de carga e do balanceador de carga ao nó de storage, é criptografado por meio de HTTPS. HTTP é uma opção suportada.

#### Balanceadores de carga locais e globais

Existem dois tipos de balanceadores de carga:

- **Gestores de tráfego locais (LTM)**. Espalha conexões por um pool de nós em um único local.
- **Global Service Load Balancer (GSLB)**. Distribui conexões em vários locais, equilibrando efetivamente os balanceadores de carga LTM. Pense em um GSLB como um servidor DNS inteligente. Quando um cliente solicita um URL de endpoint do StorageGRID, o GSLB resolve-lo para o VIP de um LTM com base na disponibilidade ou em outros fatores (por exemplo, qual site pode fornecer menor latência para o aplicativo). Embora um LTM seja sempre necessário, um GSLB é opcional, dependendo do número de sites da StorageGRID e dos requisitos da sua aplicação.

#### Balanceador de carga do nó de gateway StorageGRID versus balanceador de carga de terceiros

O StorageGRID é exclusivo entre os fornecedores de storage de objetos compatíveis com S3, pois fornece um balanceador de carga nativo disponível como um dispositivo, máquina virtual ou contêiner criado sob medida. O balanceador de carga fornecido pelo StorageGRID também é chamado de nó de gateway.

Para clientes que ainda não possuem um balanceador de carga como F5, Citrix e assim por diante, a implementação de um balanceador de carga de terceiros pode ser muito complexa. O balanceador de carga StorageGRID simplifica bastante as operações do balanceador de carga.

O Gateway Node é um balanceador de carga de nível empresarial, altamente disponível e de alta performance. Os clientes podem optar por implementar o Gateway Node, balanceador de carga de terceiros ou até mesmo ambos na mesma grade. O Gateway Node é um gerenciador de tráfego local versus um GSLB.

O balanceador de carga StorageGRID oferece as seguintes vantagens:

- **Simplicidade**. Configuração automática de pools de recursos, verificações de integridade, patches e manutenção, todos gerenciados pelo StorageGRID.
- **Desempenho**. O balanceador de carga do StorageGRID é dedicado ao StorageGRID. Você não compete com outros aplicativos em termos de largura de banda.
- **Custo**. As versões de máquina virtual (VM) e contentor são fornecidas sem custo adicional.
- **Classificações de tráfego**. O recurso classificação avançada de tráfego permite regras de QoS específicas do StorageGRID, juntamente com análises de carga de trabalho.
- **Recursos específicos do futuro StorageGRID**. A StorageGRID continuará a otimizar e adicionar recursos inovadores ao balanceador de carga em relação aos próximos lançamentos.

Para obter detalhes sobre como implantar o nó de gateway StorageGRID, consulte "Documentação do StorageGRID".

### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Centro de Documentação do NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Capacitação NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Considerações sobre o projeto do balanceador de carga StorageGRID F5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load equilibrando NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/

- Kemp – NetApp StorageGRID de balanceamento de carga https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

## Saiba como implementar certificados SSL para HTTPS no StorageGRID

Entenda a importância e as etapas para implementar os certificados SSL no StorageGRID.

Se você estiver usando HTTPS, você deve ter um certificado SSL (Secure Sockets Layer). O protocolo SSL identifica os clientes e endpoints, validando-os como confiáveis. O SSL também fornece criptografia do tráfego. O certificado SSL deve ser confiável pelos clientes. Para isso, o certificado SSL pode ser de uma Autoridade de Certificação (CA) globalmente confiável, como DigiCert, uma CA privada em execução em sua infraestrutura ou um certificado autoassinado gerado pelo host.

O uso de um certificado de CA globalmente confiável é o método preferido, pois não há ações adicionais no lado do cliente necessárias. O certificado é carregado no balanceador de carga ou no StorageGRID, e os clientes confiam e se conetam ao endpoint.

O uso de uma CA privada requer que a raiz e todos os certificados subordinados sejam adicionados ao cliente. O processo para confiar em um certificado de CA privado pode variar de acordo com o sistema operacional e os aplicativos do cliente. Por exemplo, no ONTAP para FabricPool, você deve carregar cada certificado na cadeia individualmente (certificado raiz, certificado subordinado, certificado de endpoint) para o cluster do ONTAP.

O uso de um certificado autoassinado exige que o cliente confie no certificado fornecido sem qualquer CA para verificar a autenticidade. Alguns aplicativos podem não aceitar certificados autoassinados e não ter capacidade de ignorar a verificação.

O posicionamento do certificado SSL no caminho StorageGRID do balanceador de carga do cliente depende de onde você precisa estar a terminação SSL. Você pode configurar um balanceador de carga para ser o ponto final do cliente e, em seguida, recriptografar ou criptografar em quente com um novo certificado SSL para o balanceador de carga para a conexão StorageGRID. Ou você pode passar pelo tráfego e deixar o StorageGRID ser o endpoint de terminação SSL. Se o balanceador de carga for o endpoint de terminação SSL, o certificado é instalado no balanceador de carga e contém o nome do assunto para o nome/URL DNS e quaisquer nomes de URL/DNS alternativos para os quais um cliente está configurado para se conetar ao destino StorageGRID através do balanceador de carga, incluindo quaisquer nomes de cartão selvagem. Se o balanceador de carga estiver configurado para passagem, o certificado SSL deve ser instalado no StorageGRID. Novamente, o certificado deve conter o nome do assunto para o nome/URL DNS e quaisquer nomes alternativos de URL/DNS para os quais um cliente está configurado para se conetar ao destino StorageGRID através do balanceador de carga, incluindo quaisquer nomes de cartão selvagem. Os nomes de nós de armazenamento individuais não precisam ser incluídos no certificado, apenas os URLs de endpoint.

## Configure o balanceador de carga de terceiros confiável no StorageGRID

Saiba como configurar o balanceador de carga de terceiros confiável no StorageGRID.

Se você estiver usando um ou mais balanceadores de carga de camada 7 externos e um bucket S3 ou políticas de grupo baseadas em IP, o StorageGRID deverá determinar o endereço IP real do remetente. Ele faz isso olhando para o cabeçalho X-Forwarded-for (XFF), que é inserido na solicitação pelo balanceador de carga. Como o cabeçalho XFF pode ser facilmente falsificado em solicitações enviadas diretamente para os nós de armazenamento, o StorageGRID deve confirmar que cada solicitação está sendo roteada por um balanceador de carga confiável da camada 7. Se o StorageGRID não puder confiar na origem da solicitação, ele ignorará o cabeçalho XFF. Há uma API de gerenciamento de grade para permitir que uma lista de balanceadores de carga externos confiáveis da camada 7 seja configurada. Essa nova API é privada e está sujeita a alterações em futuras versões do StorageGRID. Para obter as informações mais atualizadas, consulte o artigo da KB, "Como configurar o StorageGRID para funcionar com balanceadores de carga de camada 7 de terceiros".

## Saiba mais sobre balanceadores de carga do gerenciador de tráfego local

Explore as orientações para balanceadores de carga do gerenciador de tráfego local e determine a configuração ideal.

O seguinte é apresentado como orientação geral para a configuração de balanceadores de carga de terceiros. Trabalhe com o administrador do balanceador de carga para determinar a configuração ideal para o seu ambiente.

### Crie um grupo de recursos de nós de storage

Agrupe os nós de storage do StorageGRID em um pool de recursos ou grupo de serviços (a terminologia pode ser diferente com balanceadores de carga específicos). Os nós de storage do StorageGRID apresentam a API S3 nas seguintes portas:

- S3 HTTPS: 18082
- S3 HTTP: 18084

A maioria dos clientes escolhe apresentar as APIs no servidor virtual através das portas HTTPS e HTTP padrão (443 e 80).

> Cada local do StorageGRID requer um padrão de três nós de storage, dois dos quais precisam estar íntegros.

### Verificação de integridade

Balanceadores de carga de terceiros exigem um método para determinar a integridade de cada nó e sua qualificação para receber tráfego. O NetApp recomenda o método HTTP `OPTIONS` para executar a verificação de integridade. O balanceador de carga emite solicitações HTTP `OPTIONS` para cada nó de armazenamento individual e espera uma `200` resposta de status.

Se qualquer nó de storage não fornecer `200` uma resposta, esse nó não poderá atender às solicitações de storage. Seus requisitos de aplicativos e negócios devem determinar o tempo limite para essas verificações e a ação que o balanceador de carga realiza.

Por exemplo, se três de quatro nós de storage no data center 1 estiverem inoperantes, você poderá direcionar todo o tráfego para o data center 2.

O intervalo de polling recomendado é uma vez por segundo, marcando o nó off-line após três verificações falhadas.

#### S3 exemplo de verificação de integridade

No exemplo a seguir, nós enviamos `OPTIONS` e verificamos para `200 OK`. Usamos `OPTIONS` porque o Amazon S3) não oferece suporte a solicitações não autorizadas.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

#### Verificações de integridade baseadas em arquivo ou conteúdo

Em geral, o NetApp não recomenda verificações de integridade baseadas em arquivos. Normalmente, um pequeno arquivo —`healthcheck.htm`, por exemplo, é criado em um bucket com uma política somente leitura. Esse arquivo é então buscado e avaliado pelo balanceador de carga. Esta abordagem tem várias desvantagens:

- **Dependente de uma única conta.** Se a conta proprietária do arquivo estiver desativada, a verificação de integridade falhará e nenhuma solicitação de armazenamento será processada.
- **Regras de proteção de dados.** O esquema de proteção de dados padrão é uma abordagem de duas cópias. Nesse cenário, se os dois nós de storage que hospedam o arquivo de verificação de integridade não estiverem disponíveis, a verificação de integridade falhará e as solicitações de armazenamento não serão enviadas para nós de storage íntegros, tornando a grade off-line.
- * Registo de auditoria bloat.* O balanceador de carga obtém o arquivo de cada nó de storage a cada X minutos, criando muitas entradas de log de auditoria.
- **Recurso intensivo.** Buscar o arquivo de verificação de integridade de cada nó a cada poucos segundos consome recursos de rede e grade.

Se for necessária uma verificação de integridade baseada em conteúdo, use um locatário dedicado com um bucket S3 dedicado.

#### Persistência da sessão

Persistência da sessão, ou stickiness, refere-se ao tempo que uma determinada sessão HTTP é permitida para persistir. Por padrão, as sessões são descartadas pelos nós de storage após 10 minutos. Persistência mais longa pode levar a uma melhor performance porque as aplicações não precisam restabelecer as sessões para cada ação. No entanto, manter essas sessões abertas consome recursos. Se você determinar que seu workload se beneficiará, poderá reduzir a persistência da sessão em um balanceador de carga de terceiros.

### Endereçamento virtual em estilo hospedado

O estilo hospedado virtual agora é o método padrão para o AWS S3 e, embora o StorageGRID e muitos aplicativos ainda ofereçam suporte ao estilo de caminho, é prática recomendada implementar suporte virtual ao estilo hospedado. As solicitações virtuais de estilo hospedado têm o intervalo como parte do nome do host.

Para oferecer suporte ao estilo virtual hospedado, faça o seguinte:

- Suporte a pesquisas de DNS curinga: *.s3.company.com
- Use um certificado SSL com nomes alt de assunto para suportar curinga: *.s3.company.com alguns clientes expressaram preocupações de segurança em relação ao uso de certificados curinga. O StorageGRID continua a suportar o acesso ao estilo de caminho, assim como os principais aplicativos, como o FabricPool. Dito isto, certas chamadas de API do S3 falham ou se comportam de maneira inadequada sem suporte virtual hospedado.

### Terminação SSL

Há benefícios de segurança para o encerramento SSL em balanceadores de carga de terceiros. Se o balanceador de carga estiver comprometido, a grade será compartimentada.

Existem três configurações compatíveis:

- * SSL pass-through.* O certificado SSL é instalado no StorageGRID como um certificado de servidor personalizado.
- * Terminação SSL e re-criptografia (recomendado).* Isso pode ser benéfico se você já estiver fazendo gerenciamento de certificados SSL no balanceador de carga em vez de instalar o certificado SSL no StorageGRID. Essa configuração fornece o benefício de segurança adicional de limitar a superfície de ataque ao balanceador de carga.
- * Terminação SSL com HTTP.* Nesta configuração, o SSL é encerrado no balanceador de carga de terceiros e a comunicação do balanceador de carga para o StorageGRID não é criptografada para aproveitar o SSL off-load (com bibliotecas SSL incorporadas em processadores modernos, isso é de benefício limitado).

### Passe pela configuração

Se preferir configurar o balanceador de carga para passagem, instale o certificado no StorageGRID. Aceda ao **Configuração › certificados de servidor › Object Storage API Service Endpoints Server Certificate**.

### Visibilidade IP do cliente de origem

O StorageGRID 11,4 introduziu o conceito de um balanceador de carga confiável de terceiros. Para encaminhar o IP do aplicativo cliente para o StorageGRID, você deve configurar esse recurso. Para obter mais informações, consulte "Como configurar o StorageGRID para funcionar com balanceadores de carga de camada 7 de terceiros."

Para permitir que o cabeçalho XFF seja usado para exibir o IP do aplicativo cliente, siga estas etapas:

**Passos**

1. Registre o IP do cliente no log de auditoria.
2. Use `aws:SourceIp` a política de grupo ou bucket do S3.

#### Estratégias de balanceamento de carga

A maioria das soluções de balanceamento de carga oferece várias estratégias para balanceamento de carga. As seguintes estratégias são comuns:

- **Round robin.** Um ajuste universal, mas sofre com poucos nós e grandes transferências obstruindo nós únicos.
- **Menor conexão.** Uma boa opção para cargas de trabalho de objetos pequenos e mistos, resultando em uma distribuição igual das conexões para todos os nós.

A escolha do algoritmo se torna menos importante com um número cada vez maior de nós de storage para escolher.

#### Caminho de dados

Todos os dados fluem através de balanceadores de carga do gerenciador de tráfego local. O StorageGRID não suporta roteamento direto de servidor (DSR).

### Verificando a distribuição das conexões

Para verificar se seu método está distribuindo a carga uniformemente entre nós de storage, verifique as sessões estabelecidas em cada nó em um determinado local:

- **Método UI.** Aceda ao **Support › Metrics › S3 Overview › LDR HTTP Sessions**
- **Metrics API.** Utilização `storagegrid_http_sessions_incoming_currently_established`

## Saiba mais sobre alguns casos de uso para configurações do StorageGRID

Explore alguns casos de uso para configurações do StorageGRID implementadas pelos clientes e PELA TI DA NetApp.

Os exemplos a seguir ilustram as configurações implementadas pelos clientes da StorageGRID, incluindo O NetApp IT.

### F5 monitor de verificação de integridade do gestor de tráfego local de GRANDE IP para o bucket S3

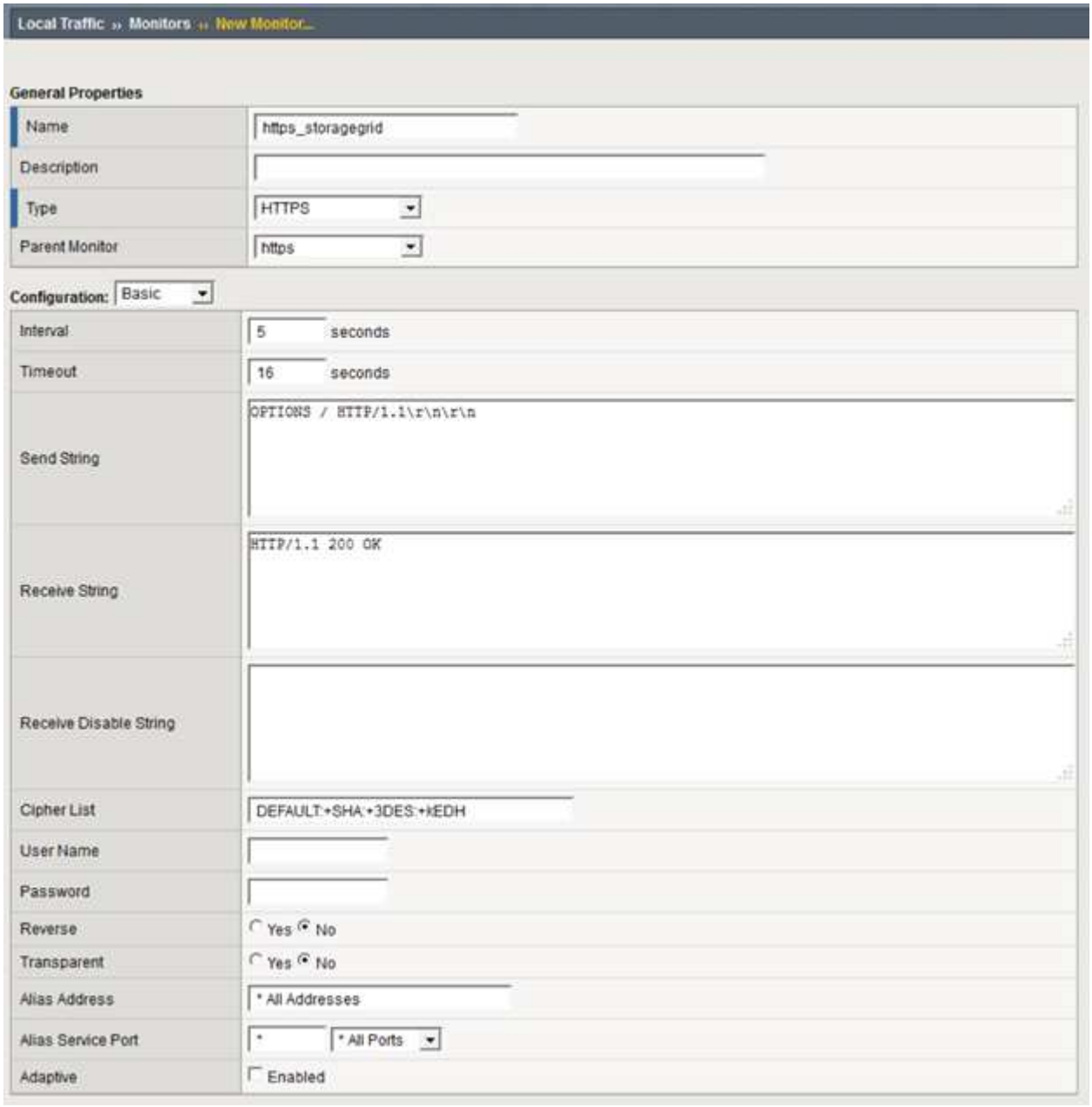
Para configurar o monitor de verificação de integridade do gerenciador de tráfego local F5 BIG-IP, siga estas etapas:

**Passos**

1. Crie um novo monitor.
   a. No campo tipo , `HTTPS` digite .
   b. Configure o intervalo e o tempo limite conforme desejado.
   c. No campo Send String (Enviar cadeia de carateres), introduza `OPTIONS / HTTP/1.1\r\n\r\n.` as

devoluções de carro; diferentes versões do software BIG-IP requerem zero, um ou dois conjuntos de sequências. Para obter mais informações, https://support.f5.com/csp/article/K10655consulte .

d. No campo receber String , digite: `HTTP/1.1 200 OK`.



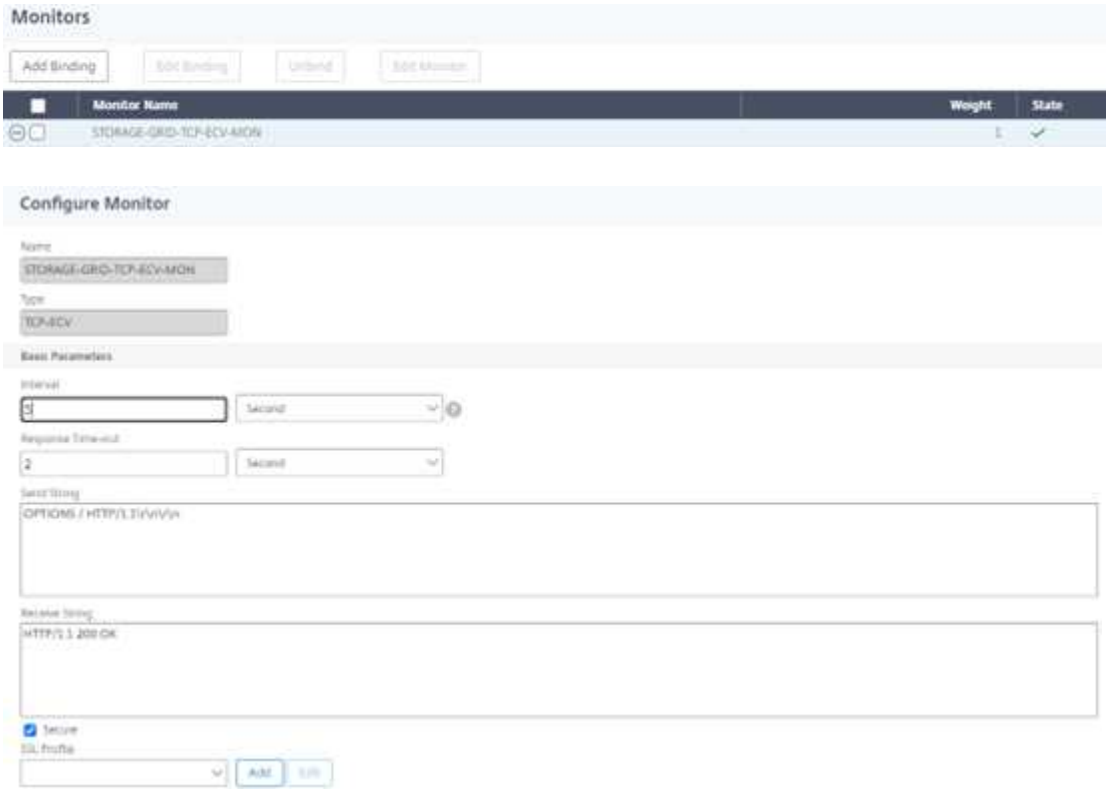

2. Em criar pool, crie um pool para cada porta necessária.
   a. Atribua o monitor de integridade que você criou na etapa anterior.
   b. Selecione um método de balanceamento de carga.
   c. Selecione a porta de serviço: 18082 (S3).
   d. Adicionar nós.

### Citrix NetScaler

O Citrix NetScaler cria um servidor virtual para o endpoint de armazenamento e se refere aos nós de armazenamento do StorageGRID como servidores de aplicativos, que são agrupados em Serviços.

Use o monitor de verificação de integridade HTTPS-ECV para criar um monitor personalizado para executar a verificação de integridade recomendada usando as OPÇÕES solicitar e receber `200`. HTTP-ECV é configurado com uma cadeia de carateres de envio e valida uma cadeia de carateres de receção.

Para obter mais informações, consulte a documentação da Citrix, "Configuração de amostra para o monitor de verificação de integridade HTTP-ECV".




### Loadbalancer.org

O Loadbalancer.org realizou seus próprios testes de integração com o StorageGRID e tem um extenso guia de configuração: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

### Kemp

A Kemp realizou seus próprios testes de integração com o StorageGRID e tem um extenso guia de configuração: https://kemptechnologies.com/solutions/netapp/.

### HAProxy

Configure o HAProxy para usar a solicitação DE OPÇÕES e verifique se há uma resposta de status 200 para a verificação de integridade no hproxy.cfg. Você pode alterar a porta de ligação no front-end para uma porta diferente, como 443.

O seguinte é um exemplo para terminação SSL no HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

O seguinte é um exemplo para a passagem SSL:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Para ver exemplos completos de configurações para o StorageGRID, "Exemplos para a Configuração HAProxy" consulte no GitHub.

## Valide a conexão SSL no StorageGRID

Saiba como validar a conexão SSL no StorageGRID.

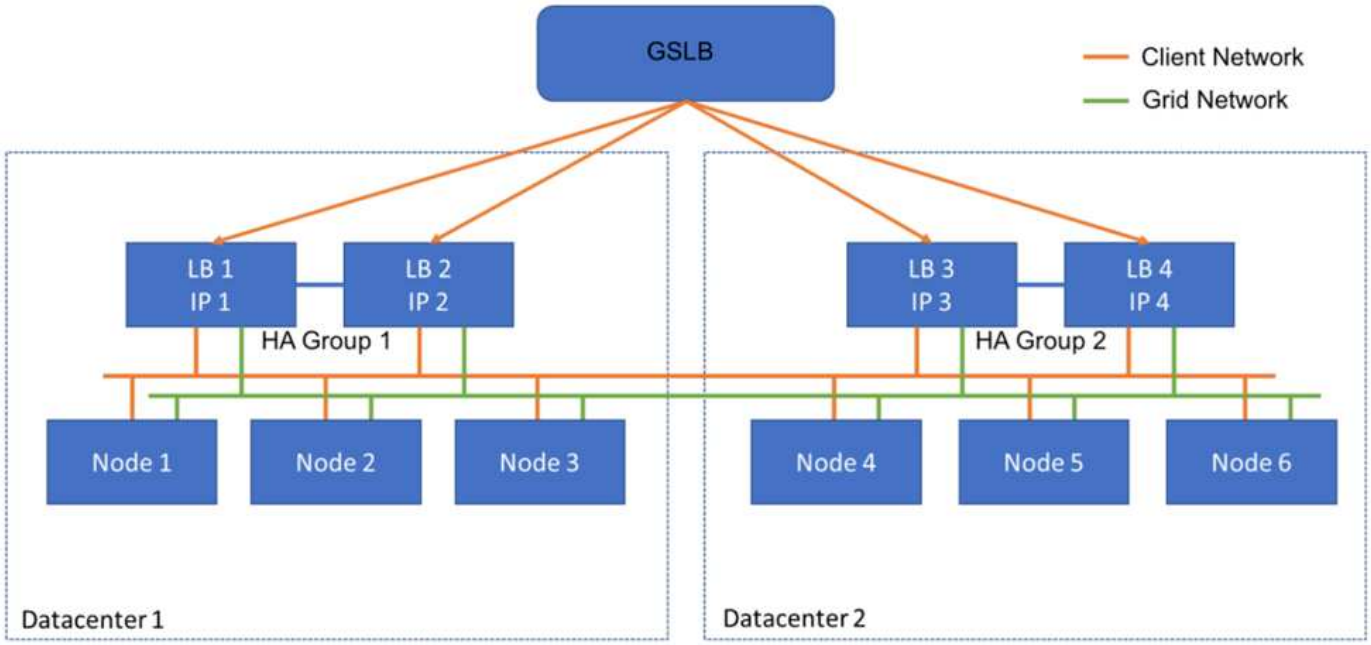
Depois que o balanceador de carga estiver configurado, você deverá validar a conexão usando ferramentas como OpenSSL e AWS CLI. Outros aplicativos, como o navegador S3, podem ignorar a configuração incorreta do SSL.

## Compreender os requisitos globais de balanceamento de carga para o StorageGRID

Explore as considerações e os requisitos de design para balanceamento de carga global no StorageGRID.

O balanceamento de carga global requer a integração com o DNS para fornecer roteamento inteligente em vários sites da StorageGRID. Essa função fica fora do domínio StorageGRID e deve ser fornecida por uma solução de terceiros, como os produtos balanceadores de carga discutidos anteriormente e/ou uma solução

de controle de tráfego DNS, como a Infoblox. Esse balanceamento de carga de nível superior fornece roteamento inteligente para o local de destino mais próximo no namespace, bem como deteção de interrupção e redirecionamento para o próximo local no namespace. Uma implementação típica do GSLB consiste no GSLB de nível superior com pools de sites contendo balanceadores de carga local. Os balanceadores de carga do local contêm pools dos nós de armazenamento do local. Isso pode incluir uma combinação de balanceadores de carga de terceiros para funções GSLB e StorageGRID fornecendo o balanceamento de carga local ou uma combinação de terceiros, ou muitos dos terceiros discutidos anteriormente podem fornecer tanto GSLB quanto balanceamento de carga local.




# TR-4645: Recursos de segurança

## Proteja os dados e metadados do StorageGRID em um armazenamento de objetos

Descubra os recursos de segurança integrais da solução de storage de objetos StorageGRID.

Esta é uma visão geral dos muitos recursos de segurança do NetApp StorageGRID, abrangendo acesso a dados, objetos e metadados, acesso administrativo e segurança da plataforma. Ele foi atualizado para incluir os recursos mais recentes lançados com o StorageGRID 11,9.

A segurança é parte integrante da solução de storage de objetos da NetApp StorageGRID. A segurança é particularmente importante porque muitos tipos de dados ricos em conteúdo que são adequados para armazenamento de objetos também são sensíveis por natureza e sujeitos a regulamentos e conformidade. À medida que os recursos do StorageGRID continuam a evoluir, o software disponibiliza muitos recursos de segurança que são inestimáveis para proteger a postura de segurança de uma organização e ajudar a organização a aderir às melhores práticas do setor.

Este documento é uma visão geral dos muitos recursos de segurança do StorageGRID 11,9, divididos em cinco categorias:

- Recursos de segurança de acesso a dados
- Recursos de segurança de objetos e metadados

- Recursos de segurança de administração
- Recursos de segurança da plataforma
- Integração com a nuvem

Este documento destina-se a ser uma folha de dados de segurança. Ele não detalha como configurar o sistema para suportar os recursos de segurança enumerados dentro que não estão configurados por padrão. O "Guia de endurecimento da StorageGRID" está disponível na página oficial "Documentação do StorageGRID".

Além dos recursos descritos neste relatório, o StorageGRID segue o "Política de notificação e resposta a vulnerabilidades de Segurança do produto NetApp". Vulnerabilidades relatadas são verificadas e respondidas de acordo com o processo de resposta a incidentes de segurança do produto.

O NetApp StorageGRID fornece recursos avançados de segurança para casos de uso de storage de objetos empresarial altamente exigentes.

### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- NetApp StorageGRID: SEC 17a-4(f), FINRA 4511(c) e CFTC 1,31(c)-(d) avaliação de conformidade https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Página de Documentação do StorageGRID 11,9 https://docs.netapp.com/us-en/storagegrid-119/
- Página de recursos da documentação do StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentação do produto NetApp https://www.netapp.com/support-and-training/documentation/

### Termos e acrônimos

Esta seção fornece definições para a terminologia usada no documento.

| Termo ou acrônimo | Definição |
|---|---|
| S3 | Simple Storage Service. |
| Cliente | Um aplicativo que pode fazer interface com o StorageGRID através do protocolo S3 para acesso a dados ou protocolo HTTP para gerenciamento. |
| Administrador do locatário | O administrador da conta de locatário do StorageGRID |
| Utilizador inquilino | Um usuário dentro de uma conta de locatário do StorageGRID |
| TLS | Segurança da camada de transporte |
| ILM | Gerenciamento do ciclo de vida da informação |
| LAN | Rede local |
| Administrador de grade | O administrador do sistema StorageGRID |
| Grelha | O sistema StorageGRID |
| Balde | Um recipiente para objetos armazenados em S3 |

| Termo ou acrônimo | Definição |
| --- | --- |
| LDAP | Lightweight Directory Access Protocol |
| SEG | Comissão de valores Mobiliários; regula os membros do câmbio, corretores ou revendedores |
| FINRA | Autoridade reguladora da indústria financeira; defensa o formato e os requisitos de Mídia da regra SEC 17a-4(f) |
| CFTC | Comissões de negociação de futuros de commodities; regula a negociação de futuros de commodities |
| NIST | Instituto Nacional de normas e tecnologia |

## Recursos de segurança de acesso a dados

Saiba mais sobre os recursos de segurança de acesso a dados no StorageGRID.

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Segurança de camada de transporte configurável (TLS) | O TLS estabelece um protocolo de handshake para comunicação entre um cliente e um nó de gateway StorageGRID, nó de armazenamento ou ponto de extremidade do balanceador de carga.<br><br>O StorageGRID suporta os seguintes conjuntos de codificação para TLS:<br><br>• TLS_AES_256_GCM_SHA384<br>• TLS_AES_128_GCM_SHA256<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• TLS_AES_256_GCM_SHA384<br>• DHE-RSA-AES128-GCM-SHA256<br>• DHE-RSA-AES256-GCM-SHA384<br>• AES256-GCM-SHA384<br>• AES128-GCM-SHA256<br>• TLS_CHACHA20_POLY1305_SHA256<br>• ECDHE-ECDSA-CHACHA20-POLY1305<br>• ECDHE-RSA-CHACHA20-POLY1305<br><br>Suporte para TLS v1,2 e 1,3.<br><br>SSLv3, TLS v1,1 e anteriores não são mais suportados. | Permite que um cliente e o StorageGRID se identifiquem e autentiquem entre si e se comuniquem com confidencialidade e integridade de dados. Garante o uso de uma versão TLS recente. As cifras agora são configuráveis nas configurações de Configuração/Segurança | — |
| | | | |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Certificado de servidor configurável (Load Balancer Endpoint) | Os administradores de grade podem configurar o Load Balancer Endpoints para gerar ou usar um certificado de servidor. | Permite o uso de certificados digitais assinados por sua autoridade de certificação confiável (CA) padrão para autenticar operações de API de objeto entre grade e cliente por ponto final do Load Balancer. | — |
| Certificado de servidor configurável (endpoint API) | Os administradores de grade podem configurar centralmente todos os endpoints da API do StorageGRID para usar um certificado de servidor assinado pela CA confiável de sua organização. | Permite o uso de certificados digitais assinados por sua CA padrão e confiável para autenticar operações de API de objeto entre um cliente e a grade. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Alocação a vários clientes | O StorageGRID dá suporte a vários locatários por grade; cada locatário tem seu próprio namespace. Um locatário fornece o protocolo S3; por padrão, o acesso a buckets/containers e objetos é restrito aos usuários dentro da conta. Os locatários podem ter um usuário (por exemplo, uma implantação corporativa, na qual cada usuário tem sua própria conta) ou vários usuários (por exemplo, uma implantação de provedor de serviços, na qual cada conta é uma empresa e um cliente do provedor de serviços). Os usuários podem ser locais ou federados; os usuários federados são definidos pelo ative Directory ou pelo LDAP (Lightweight Directory Access Protocol). O StorageGRID fornece um painel por locatário, no qual os usuários fazem login usando suas credenciais de conta local ou federada. Os usuários podem acessar relatórios visualizados sobre o uso do locatário em relação à cota atribuída pelo administrador da grade, incluindo informações de uso em dados e objetos armazenados por buckets. Os usuários com permissão administrativa podem executar tarefas de administração do sistema no nível do locatário, como gerenciar usuários e grupos e chaves de acesso. | Permite que os administradores do StorageGRID hospedem dados de vários locatários enquanto isolam o acesso do locatário e estabeleçam a identidade do usuário federando usuários com um provedor de identidade externo, como o ative Directory ou LDAP. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Não repúdio de credenciais de acesso | Cada operação do S3 é identificada e registrada com uma conta de locatário, usuário e chave de acesso exclusivos. | Permite que os administradores de Grid estabeleçam quais ações de API são executadas por quais indivíduos. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Acesso anônimo desativado | Por padrão, o acesso anônimo é desativado para contas S3. Um solicitante deve ter uma credencial de acesso válida para um usuário válido na conta do locatário para acessar buckets, contentores ou objetos dentro da conta. O acesso anônimo a buckets ou objetos do S3 pode ser habilitado com uma política explícita do IAM. | Permite que os administradores de Grade desativem ou controlem o acesso anônimo a buckets/containers e objetos. | — |
| WORM de conformidade | Projetado para atender aos requisitos da regra SEC 17a-4(f) e validado pela Cohasset. Os clientes podem habilitar a conformidade no nível do balde. As regras de gerenciamento do ciclo de vida das informações (ILM) impõem níveis mínimos de proteção de dados. | Permite que os locatários com requisitos de retenção de dados regulatórios habilitem a proteção WORM em objetos armazenados e metadados de objetos. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| WORM | Os administradores de grade podem habilitar o WORM em toda a grade ativando a opção Desativar modificação do cliente, que impede que os clientes substituam ou excluam objetos ou metadados de objetos em todas as contas de locatário.<br><br>S3 os administradores do locatário também podem habilitar WORM por locatário, bucket ou prefixo de objeto especificando a política do IAM, que inclui a permissão personalizada S3: PutOverwriteObject para substituição de objetos e metadados. | Permite que administradores de grade e administradores de locatários controlem a proteção WORM em objetos armazenados e metadados de objetos. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Gerenciamento de chaves de criptografia do servidor host KMS | Os administradores de grade podem configurar um ou mais servidores de gerenciamento de chaves externos (KMS) no Gerenciador de grade para fornecer chaves de criptografia para serviços e dispositivos de armazenamento do StorageGRID. Cada servidor host KMS ou cluster de servidor host KMS usa o KMIP (Key Management Interoperability Protocol) para fornecer uma chave de criptografia aos nós do dispositivo no site associado do StorageGRID. | A criptografia de dados em repouso é obtida. Depois que os volumes do dispositivo forem criptografados, você não poderá acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o servidor host KMS. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Failover automatizado | O StorageGRID fornece redundância incorporada e failover automatizado. O acesso a contas de locatários, buckets e objetos pode continuar mesmo que haja várias falhas, desde discos ou nós até sites inteiros. O StorageGRID tem reconhecimento de recursos e redireciona automaticamente as solicitações para nós e locais de dados disponíveis. Os locais do StorageGRID podem até operar no modo islanded; se uma interrupção da WAN desconeta um local do resto do sistema, as leituras e gravações podem continuar com os recursos locais e a replicação é retomada automaticamente quando a WAN é restaurada. | Permite que os administradores da Grid solucionem o tempo de atividade, SLA e outras obrigações contratuais e implementem planos de continuidade de negócios. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| **Recursos de segurança de acesso a dados específicos do S3** | Assinatura AWS versão 2 e versão 4 | As solicitações de API de assinatura fornecem autenticação para operações de API S3. A Amazon suporta duas versões do Signature versão 2 e versão 4. O processo de assinatura verifica a identidade do solicitante, protege os dados em trânsito e protege contra possíveis ataques de repetição. | Alinha-se à recomendação da AWS para assinatura versão 4 e permite compatibilidade com versões anteriores com aplicativos mais antigos com a assinatura versão 2. |
| — | S3 bloqueio de objetos | O recurso bloqueio de objetos S3 no StorageGRID é uma solução de proteção de objetos equivalente ao bloqueio de objetos S3 no Amazon S3. | Permite que os locatários criem buckets com o S3 Object Lock habilitado para cumprir com os regulamentos que exigem que certos objetos sejam retidos por um período fixo de tempo ou indefinidamente. |
| Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) | Armazenamento seguro de credenciais S3 | As chaves de acesso S3 são armazenadas em um formato protegido por uma função de hash de senha (SHA-2). | Permite o armazenamento seguro de chaves de acesso através de uma combinação de comprimento de chave (um número de 10 31 gerado aleatoriamente) e um algoritmo de hash de senha. |
| — | Teclas de acesso S3 com limite de tempo | Ao criar uma chave de acesso S3 para um usuário, os clientes podem definir uma data e hora de expiração na chave de acesso. | Dá aos administradores de Grade a opção de provisionar chaves de acesso S3 temporárias. |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| — | Várias chaves de acesso por conta de usuário | O StorageGRID permite que várias chaves de acesso sejam criadas e simultaneamente ativas para uma conta de usuário. Como cada ação de API é registrada com uma conta de usuário locatário e chave de acesso, a não rejeição é preservada apesar de várias chaves estarem ativas. | Permite que os clientes girem chaves de acesso sem interrupções e permite que cada cliente tenha sua própria chave, desencorajando o compartilhamento de chaves entre os clientes. |
| — | S3 Política de acesso do IAM | O StorageGRID oferece suporte a políticas do IAM S3, permitindo que os administradores de grade especifiquem o controle de acesso granular por locatário, bucket ou prefixo de objeto. O StorageGRID também suporta as condições e variáveis da política do IAM, permitindo políticas de controle de acesso mais dinâmicas. | Permite que os administradores de Grade especifiquem o controle de acesso por grupos de usuários para todo o locatário; também permite que os usuários do locatário especifiquem o controle de acesso para seus próprios buckets e objetos. |
| — | Criptografia no lado do servidor com chaves gerenciadas por StorageGRID (SSE) | O StorageGRID é compatível com SSE, permitindo a proteção de dados em repouso com chaves de criptografia gerenciadas pelo StorageGRID. | Permite que os locatários criptografem objetos. A chave de criptografia é necessária para gravar e recuperar esses objetos. |
| Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) | Criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C) | O StorageGRID oferece suporte ao SSE-C, permitindo a proteção de dados em repouso com chaves de criptografia gerenciadas pelo cliente.<br><br>Embora o StorageGRID gerencie todas as operações de criptografia e descriptografia de objetos, com o SSE-C, o cliente deve gerenciar as próprias chaves de criptografia. | Permite que os clientes criptografem objetos com as chaves que controlam. A chave de criptografia é necessária para gravar e recuperar esses objetos. |

## Segurança de objetos e metadados

Explore os recursos de segurança de objetos e metadados no StorageGRID.

| Recurso | Função | Impacto | Conformidade regulamentar |
|---|---|---|---|
| AES (Advanced Encryption Standard) encriptação de objetos no lado do servidor | O StorageGRID fornece criptografia de objetos no lado do servidor baseada em AES 128 e AES 256. Os administradores de grade podem habilitar a criptografia como uma configuração padrão global. O StorageGRID também suporta o cabeçalho de criptografia do lado do servidor x-amz S3 para permitir ou desativar a criptografia por objeto. Quando ativado, os objetos são criptografados quando armazenados ou em trânsito entre nós de grade. | Ajuda a proteger o armazenamento e a transmissão de objetos, independentemente do hardware de armazenamento subjacente. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Gerenciamento de chaves integrado | Quando a criptografia é ativada, cada objeto é criptografado com uma chave simétrica única gerada aleatoriamente, que é armazenada dentro do StorageGRID sem acesso externo. | Permite a criptografia de objetos sem exigir gerenciamento de chaves externas. | |
| Discos de criptografia compatíveis com Federal Information Processing Standard (FIPS) 140-2 | Os dispositivos StorageGRID SG5812, SG5860, SG6160 e SGF6024 oferecem a opção de discos de criptografia compatíveis com FIPS 140-2. As chaves de criptografia para os discos podem ser gerenciadas, como opção, por um servidor KMIP externo. | Permite o storage seguro de dados, metadados e objetos do sistema. Também fornece criptografia de objeto baseada em software StorageGRID, que protege o armazenamento e a transmissão de objetos. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Verificação de integridade em segundo plano e auto-cura | O StorageGRID usa um mecanismo de intertravamento de hashes, checksums e verificações de redundância cíclica (CRCs) no nível de objeto e subobjeto para proteger contra inconsistência, adulteração ou modificação de dados, tanto quando os objetos estão em armazenamento quanto em trânsito. O StorageGRID deteta automaticamente objetos corrompidos e adulterados e os substitui, enquanto coloca em quarentena os dados alterados e alerta o administrador. | Permite que os administradores de Grid cumpram SLA, regulamentos e outras obrigações em relação à durabilidade dos dados. Ajuda os clientes a detetar ransomware ou vírus que tentam criptografar, adulterar ou modificar dados. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Retenção e posicionamento de objetos baseados em políticas | O StorageGRID permite que os administradores de grade configurem regras de ILM, que especificam retenção, posicionamento, proteção, transição e expiração de objetos. Os administradores de grade podem configurar o StorageGRID para filtrar objetos por seus metadados e aplicar regras em vários níveis de granularidade, incluindo em toda a grade, locatário, bucket, prefixo de chave e pares de valor-chave de metadados definidos pelo usuário. O StorageGRID ajuda a garantir que os objetos sejam armazenados de acordo com as regras do ILM ao longo de seus ciclos de vida, a menos que sejam explicitamente excluídos pelo cliente. | Ajuda a reforçar a disposição, a proteção e a retenção dos dados. Ajuda os clientes a alcançarem o SLA para durabilidade, disponibilidade e desempenho. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Verificação de metadados em segundo plano | O StorageGRID verifica periodicamente os metadados de objetos em segundo plano para aplicar alterações no posicionamento ou proteção dos dados do objeto, conforme especificado pelo ILM. | Ajuda a descobrir objetos corrompidos. | |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Consistência ajustável | Os locatários podem selecionar níveis de consistência no nível do bucket para garantir que recursos como conectividade multisite estejam disponíveis. | Fornece a opção de confirmar gravações na grade somente quando um número necessário de sites ou recursos estiver disponível. | |

## Recursos de segurança de administração

Descubra os recursos de segurança de administração no StorageGRID.

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Certificado do servidor (Interface de Gerenciamento de Grade) | Os administradores de grade podem configurar a interface de gerenciamento de grade para usar um certificado de servidor assinado pela CA confiável da organização. | Permite o uso de certificados digitais assinados por sua CA padrão e confiável para autenticar o acesso de UI de gerenciamento e API entre um cliente de gerenciamento e a grade. | — |
| Autenticação de usuário administrativo | Os usuários administrativos são autenticados usando nome de usuário e senha. Os usuários e grupos administrativos podem ser locais ou federados, importados do ative Directory ou LDAP do cliente. As senhas de contas locais são armazenadas em um formato protegido por bcrypt; senhas de linha de comando são armazenadas em um formato protegido por SHA-2. | Autentica o acesso administrativo à interface de usuário e às APIs de gerenciamento. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Suporte a SAML | O StorageGRID oferece suporte ao logon único (SSO) usando o padrão SAML 2,0 (Security Assertion Markup Language 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. | Permite níveis adicionais de segurança para administradores de rede e locatários, como SSO e autenticação multifator (MFA). | NIST SP800-63 |
| Controle granular de permissão | Os administradores de grade podem atribuir permissões a funções e atribuir funções a grupos de usuários administrativos, o que impõe quais tarefas os clientes administrativos podem executar usando a interface de usuário e as APIs de gerenciamento. | Permite que os administradores de Grade gerenciem o controle de acesso para usuários e grupos administrativos. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Log de auditoria distribuído | O StorageGRID fornece uma infraestrutura de log de auditoria distribuída e integrada, escalável para centenas de nós em até 16 locais. Os nós de software StorageGRID geram mensagens de auditoria, que são transmitidas por um sistema de reencaminhamento de auditoria redundante e, em última análise, capturadas em um ou mais repositórios de log de auditoria. As mensagens de auditoria capturam eventos em uma granularidade no nível do objeto, como operações de API S3 iniciadas pelo cliente, eventos de ciclo de vida do objeto pelo ILM, verificações de integridade do objeto em segundo plano e alterações de configuração feitas a partir da IU ou APIs de gerenciamento.<br><br>Os logs de auditoria podem ser exportados de nós de administração por meio de CIFS ou NFS, permitindo que as mensagens de auditoria sejam minadas por ferramentas como Splunk e ELK. Existem quatro tipos de mensagens de auditoria:<br><br>• Mensagens de auditoria do sistema<br>• Mensagens de auditoria de armazenamento de objetos<br>• Mensagens de auditoria do protocolo HTTP<br>• Mensagens de auditoria de gerenciamento | Fornece aos administradores do Grid um serviço de auditoria comprovado e escalável e permite que eles explorem dados de auditoria para vários objetivos. Tais objetivos incluem solução de problemas, auditoria do desempenho do SLA, operações da API de acesso a dados do cliente e alterações de configuração de gerenciamento. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Auditoria do sistema | As mensagens de auditoria do sistema capturam eventos relacionados ao sistema, como estados de nó de grade, deteção de objetos corrompidos, objetos comprometidos em todos os locais especificados por regra ILM e progresso das tarefas de manutenção em todo o sistema (tarefas de grade). | Ajuda os clientes a solucionar problemas do sistema e fornece a prova de que os objetos são armazenados de acordo com seu SLA. Os SLAs são implementados pelas regras do StorageGRID ILM e são protegidos por integridade. | — |
| Auditoria de storage de objetos | As mensagens de auditoria de armazenamento de objetos capturam transações de API de objetos e eventos relacionados ao ciclo de vida. Esses eventos incluem armazenamento e recuperação de objetos, transferências de nó de grade para nó de grade e verificações. | Ajuda os clientes a auditar o progresso dos dados através do sistema e se o SLA, especificado como StorageGRID ILM, está sendo entregue. | — |
| Auditoria de protocolo HTTP | As mensagens de auditoria do protocolo HTTP capturam interações do protocolo HTTP relacionadas a aplicativos clientes e nós do StorageGRID. Além disso, os clientes podem capturar cabeçalhos de solicitação HTTP específicos (como X-forwarded-for e metadados do usuário [x-amz-meta-*]) em auditoria. | Ajuda os clientes a auditar as operações da API de acesso de dados entre clientes e StorageGRID e rastrear uma ação para uma conta de usuário individual e chave de acesso. Os clientes também podem Registrar os metadados dos usuários na auditoria e usar ferramentas de log mining, como Splunk ou ELK, para pesquisar metadados de objetos. | — |
| Auditoria de gerenciamento | As mensagens de auditoria de gerenciamento Registram solicitações de usuários administradores para a interface de gerenciamento (Grid Management Interface) ou APIs. 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. | Ajuda os administradores de Grade a estabelecer um Registro das alterações de configuração do sistema feitas por qual usuário de qual IP de origem e qual IP de destino a que momento. | — |

| Recurso | Função | Impacto | Conformidade regulamentar |
|---|---|---|---|
| Suporte a TLS 1,3 para acesso à API e UI de gerenciamento | O TLS estabelece um protocolo de handshake para comunicação entre um cliente admin e um nó de administrador do StorageGRID. | Permite que um cliente administrativo e o StorageGRID se identifiquem e autentiquem-se com confidencialidade e integridade de dados. | — |
| SNMPv3 para monitorização StorageGRID | O SNMPv3 fornece segurança oferecendo autenticação forte e criptografia de dados para privacidade. Com o v3, as unidades de dados do protocolo são criptografadas, usando o CBC-DES para seu protocolo de criptografia.<br><br>A autenticação do usuário de quem enviou a unidade de dados do protocolo é fornecida pelo protocolo de autenticação HMAC-SHA ou HMAC-MD5.<br><br>SNMPv2 e v1 ainda são suportados. | Ajuda os administradores de grade a monitorar o sistema StorageGRID habilitando um agente SNMP no nó Admin. | — |
| Certificados de cliente para exportação de métricas Prometheus | Os administradores de grade podem fazer upload ou gerar certificados de cliente que podem ser usados para fornecer acesso seguro e autenticado ao banco de dados do StorageGRID Prometheus. | Os administradores de grade podem usar certificados de cliente para monitorar o StorageGRID externamente usando aplicativos como o Grafana. | — |

## Recursos de segurança da plataforma

Saiba mais sobre os recursos de segurança da plataforma no StorageGRID.

| Recurso | Função | Impacto | Conformidade regulamentar |
|---|---|---|---|
| Infraestrutura de chave pública interna (PKI), certificados de nó e TLS | O StorageGRID usa uma PKI interna e certificados de nó para autenticar e criptografar a comunicação entre nós. A comunicação entre nós é protegida por TLS. | Ajuda a proteger o tráfego do sistema pela LAN ou WAN, especialmente em uma implantação multisite. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |

| Recurso | Função | Impacto | Conformidade regulamentar |
| --- | --- | --- | --- |
| Firewall de nó | O StorageGRID configura automaticamente tabelas IP e regras de firewall para controlar o tráfego de rede de entrada e saída, bem como fechar portas não utilizadas. | Ajuda a proteger o sistema StorageGRID, os dados e os metadados contra o tráfego de rede não solicitado. | — |
| ENDURECIMENTO do SISTEMA OPERACIONAL | O sistema operacional básico de dispositivos físicos e nós virtuais do StorageGRID é endurecido; pacotes de software não relacionados são removidos. | Ajuda a minimizar potenciais superfícies de ataque. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Atualizações periódicas de plataforma e software | O StorageGRID fornece versões regulares de software que incluem sistema operacional, binários de aplicativos e atualizações de software. | Ajuda a manter o sistema StorageGRID atualizado com os binários atuais de software e aplicativos. | — |
| Login raiz desabilitado sobre Secure Shell (SSH) | O login raiz sobre SSH está desativado em todos os nós do StorageGRID. O acesso SSH usa autenticação de certificado. | Ajuda os clientes a se protegerem contra possíveis quebras de senha remota do login raiz. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Sincronização automatizada de tempo | O StorageGRID sincroniza automaticamente os relógios de sistema de cada nó com vários servidores de Protocolo de tempo de rede (NTP) externos. Pelo menos quatro servidores NTP do estrato 3 ou posterior são necessários. | Garante a mesma referência de tempo em todos os nós. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Redes separadas para o tráfego de rede de clientes, administradores e internos | Os nós de software e dispositivos de hardware da StorageGRID suportam várias interfaces de rede virtuais e físicas, para que os clientes possam separar o tráfego de rede de clientes, administração e interna em diferentes redes. | Permitir que os administradores do Grid segregem o tráfego de rede interno e externo e forneçam tráfego através de redes com diferentes SLAs. | — |
| Várias interfaces de LAN virtual (VLAN) | O StorageGRID suporta a configuração de interfaces VLAN em suas redes de cliente e grade StorageGRID. | Permita que os administradores do Grid particione e isole o tráfego do aplicativo para obter segurança, flexibilidade e desempenho. | |

| Recurso | Função | Impacto | Conformidade regulamentar |
|---|---|---|---|
| Rede cliente não confiável | A interface de rede cliente não confiável aceita conexões de entrada apenas em portas que foram explicitamente configuradas como endpoints de balanceador de carga. | Garante que as interfaces expostas a redes não confiáveis sejam protegidas. | — |
| Firewall configurável | Gerencie portas abertas e fechadas para redes Admin, Grid e cliente. | Permitir que os administradores de grade controlem o acesso nas portas e gerenciem o acesso de dispositivo aprovado às portas. | |
| Comportamento SSH aprimorado | Novos certificados de host SSH e chaves de host são gerados ao atualizar um nó para o StorageGRID 11,5. | Melhora a proteção contra ataques homem-no-meio. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |
| Criptografia de nó | Como parte do novo recurso de criptografia do servidor host KMS, uma nova configuração de criptografia de nó é adicionada ao Instalador de dispositivos StorageGRID. | Esta definição tem de ser ativada durante a fase de configuração de hardware da instalação do dispositivo. | Regra DO SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regra 4511(c) |

### Integração com a nuvem

Entenda como o StorageGRID se integra aos serviços de nuvem.

| Recurso | Função | Impacto |
|---|---|---|
| Verificação de vírus baseada em notificações | Notificações de eventos de suporte dos serviços da plataforma StorageGRID. As notificações de eventos podem ser usadas com serviços externos de computação em nuvem para acionar fluxos de trabalho de verificação de vírus nos dados. | Permite que os administradores de inquilinos acionem a verificação de vírus de dados usando serviços externos de computação em nuvem. |

# TR-4921: Defesa de ransomware

## Proteja objetos do StorageGRID S3 contra ransomware

Saiba mais sobre ataques de ransomware e como proteger dados com as práticas recomendadas de segurança da StorageGRID.

Os ataques de ransomware estão aumentando. Este documento fornece algumas recomendações sobre

como proteger seus dados de objeto no StorageGRID.

Atualmente, o ransomware é o perigo constante do data center. Ransomware é projetado para criptografar dados e torná-los inutilizáveis pelos usuários e aplicativos que dependem dele. A proteção começa com as defesas usuais de redes endurecidas e práticas sólidas de segurança do usuário, e precisamos acompanhar as práticas de segurança de acesso a dados.

O ransomware é uma das maiores ameaças à segurança de hoje. A equipe da NetApp StorageGRID está trabalhando com nossos clientes para se manterem à frente dessas ameaças. Com o uso de bloqueio de objetos e controle de versão, você pode proteger contra alterações indesejadas e recuperar de ataques maliciosos. A segurança de dados é uma aventura de várias camadas, com seu storage de objetos sendo apenas uma parte do seu data center.

#### Práticas recomendadas da StorageGRID

Para o StorageGRID, as práticas recomendadas de segurança devem incluir o uso de HTTPS com certificados assinados para gerenciamento e acesso a objetos. Crie contas de usuário dedicadas para aplicativos e indivíduos e não use as contas raiz do locatário para acesso a aplicativos ou acesso a dados do usuário. Em outras palavras, siga o princípio de menor privilégio. Use grupos de segurança com políticas definidas de gerenciamento de identidade e acesso (IAM) para governar os direitos de usuário e acessar contas específicas para os aplicativos e usuários. Com essas medidas em vigor, você ainda precisa garantir que seus dados estejam protegidos. No caso do Simple Storage Service (S3), quando os objetos são modificados para criptografá-los, ele é realizado por uma substituição do objeto original.

#### Métodos de defesa

O principal mecanismo de proteção contra ransomware na API S3 é implementar o bloqueio de objetos. Nem todos os aplicativos são compatíveis com o bloqueio de objetos, portanto, há duas outras opções para proteger os objetos descritos neste relatório: Replicação para outro bucket com o controle de versão ativado e o controle de versão com políticas do IAM.

#### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Centro de Documentação do NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Capacitação NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Página de recursos da documentação do StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentação do produto NetApp https://www.netapp.com/support-and-training/documentation/

## Defesa contra ransomware usando bloqueio de objeto

Explore como o bloqueio de objetos no StorageGRID fornece um modelo WORM para impedir a exclusão ou substituição de dados, e como ele atende aos requisitos regulatórios.

O bloqueio de objetos fornece um modelo WORM para impedir que objetos sejam excluídos ou substituídos. A implementação do StorageGRID do bloqueio de objetos "Cohasset avaliado" destina-se a ajudar a atender a requisitos regulatórios, dar suporte à retenção legal, modo de conformidade e modo de governança para retenção de objetos e políticas de retenção de buckets padrão. Você deve habilitar o bloqueio de objetos

como parte da criação e controle de versão do bucket. Uma versão específica de um objeto é bloqueada e, se nenhuma ID de versão for definida, a retenção é colocada na versão atual do objeto. Se a versão atual tiver a retenção configurada e for feita uma tentativa de excluir, modificar ou substituir o objeto, uma nova versão será criada com um marcador de exclusão ou a nova revisão do objeto como a versão atual, e a versão bloqueada será mantida como uma versão não atual. Para aplicativos que ainda não são compatíveis, talvez você ainda possa usar o bloqueio de objetos e uma configuração de retenção padrão colocada no bucket. Depois que a configuração é definida, isso aplica uma retenção de objetos a cada novo objeto colocado no bucket. Isso funciona desde que o aplicativo esteja configurado para não excluir ou substituir os objetos antes que o tempo de retenção tenha passado.

Aqui estão alguns exemplos usando a API de bloqueio de objetos:

Bloqueio de objeto retenção legal é um simples status de ligar/desligar aplicado a um objeto.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

Definir o status de retenção legal não retorna nenhum valor se bem-sucedido, portanto, ele pode ser verificado com uma operação GET.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Para desativar a retenção legal, aplique o status OFF.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

A configuração da retenção de objeto é feita com um carimbo de data/hora retent until.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Novamente, não há valor retornado no sucesso, então você pode verificar o status de retenção da mesma forma com uma chamada recebida.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

Colocar uma retenção padrão em um bucket habilitado para bloqueio de objetos usa um período de retenção em dias e anos.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Como na maioria dessas operações, nenhuma resposta é retornada com sucesso, então, podemos realizar um GET para a configuração verificar.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Em seguida, você pode colocar um objeto no bucket com a configuração de retenção aplicada.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

A OPERAÇÃO DE COLOCAÇÃO retorna uma resposta.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

No objeto de retenção, a duração de retenção definida no bucket no exemplo anterior é convertida em um carimbo de data/hora de retenção no objeto.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

## Defesa contra ransomware usando bucket replicado com controle de versão

Saiba como replicar objetos para um bucket secundário usando o StorageGRID CloudMirror.

Nem todas as aplicações e workloads serão compatíveis com o bloqueio de objetos. Outra opção é replicar os objetos para um bucket secundário na mesma grade (de preferência um locatário diferente com acesso restrito) ou qualquer outro endpoint S3 com o serviço da plataforma StorageGRID, CloudMirror.

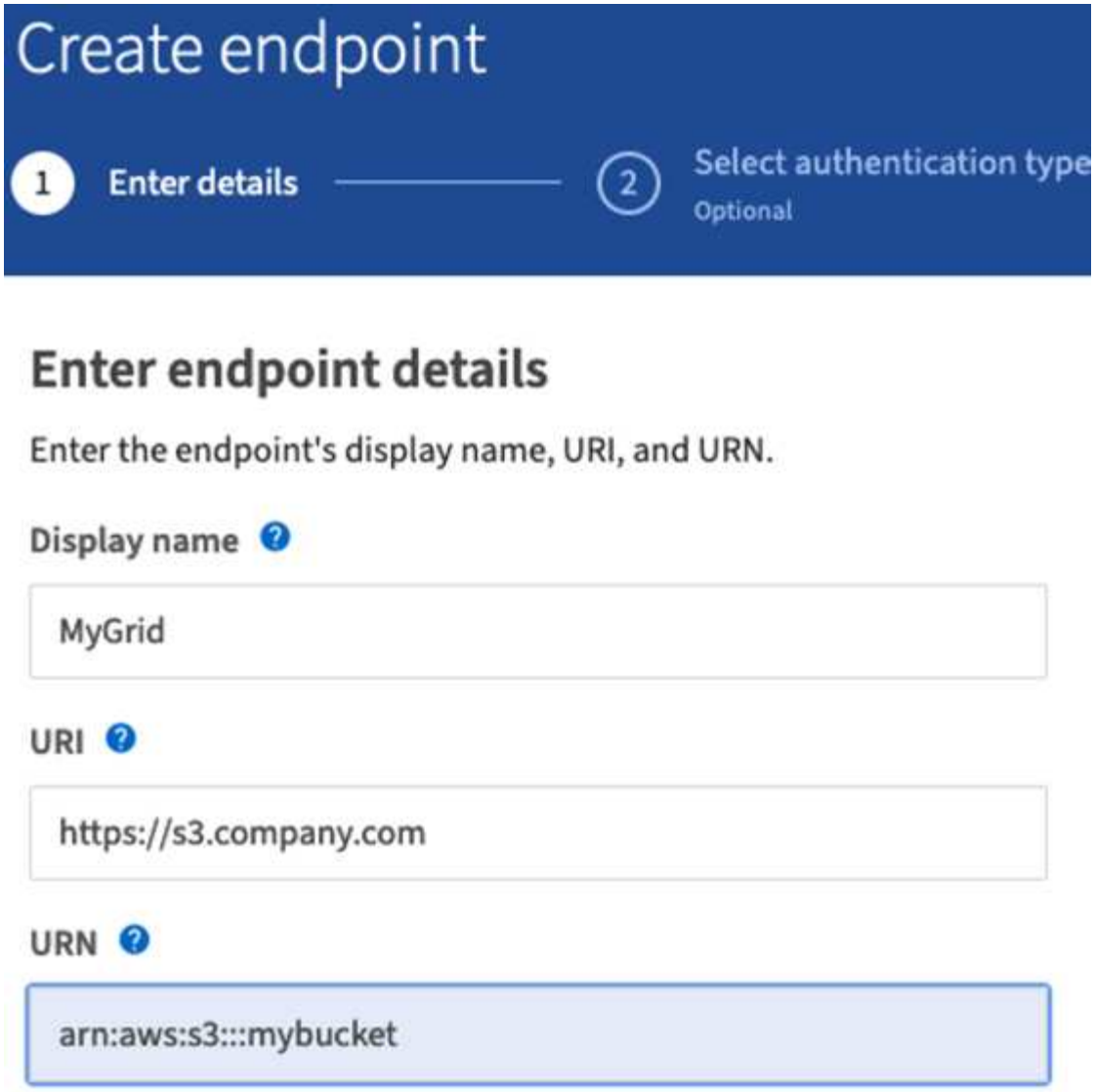
O StorageGRID CloudMirror é um componente do StorageGRID que pode ser configurado para replicar os objetos de um bucket para um destino definido à medida que são ingeridos no bucket de origem e não replica exclusões. Como o CloudMirror é um componente integrado do StorageGRID, ele não pode ser desativado ou manipulado por um ataque baseado em API S3. Você pode configurar esse bucket replicado com o controle de versão ativado. Neste cenário, você precisa de uma limpeza automatizada das versões antigas do bucket replicado que são seguras para descartar. Para isso, você pode usar o mecanismo de política StorageGRID ILM. Crie regras para gerenciar o posicionamento do objeto com base no tempo não atual por vários dias suficiente para ter identificado e recuperado de um ataque.

Uma desvantagem para essa abordagem é que ela consome mais armazenamento, tendo uma segunda cópia completa do bucket, além de várias versões dos objetos retidos por algum tempo. Além disso, os objetos que foram intencionalmente excluídos do bucket primário devem ser removidos manualmente do bucket replicado. Há outras opções de replicação fora do produto, como o NetApp CloudSync, que podem replicar exclusões para uma solução semelhante. Outra desvantagem para o bucket secundário ser o controle de versão ativado e não o bloqueio de objetos ativado é que existe uma série de contas privilegiadas que podem ser usadas para causar danos no local secundário. A vantagem é que ela deve ser uma conta exclusiva para esse bucket de endpoint ou locatário e o compromisso provavelmente não inclui acesso a contas no local primário ou vice-versa.

Depois que os buckets de origem e destino forem criados e o destino for configurado com controle de versão, você poderá configurar e ativar a replicação da seguinte forma:

**Passos**

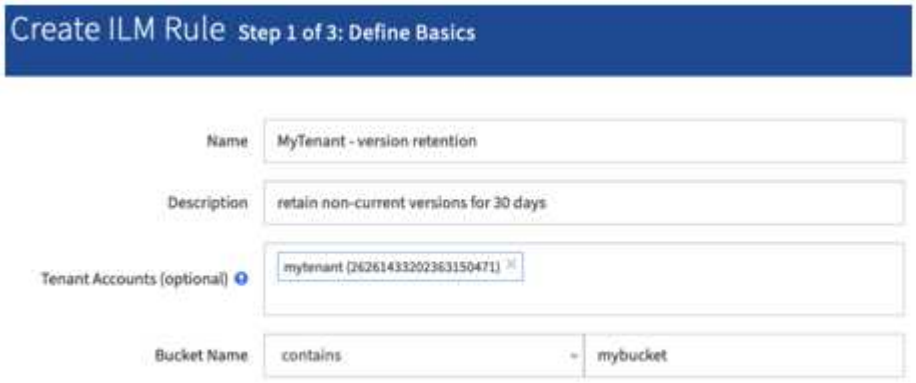
1. Para configurar o CloudMirror, crie um endpoint de serviços de plataforma para o destino S3.

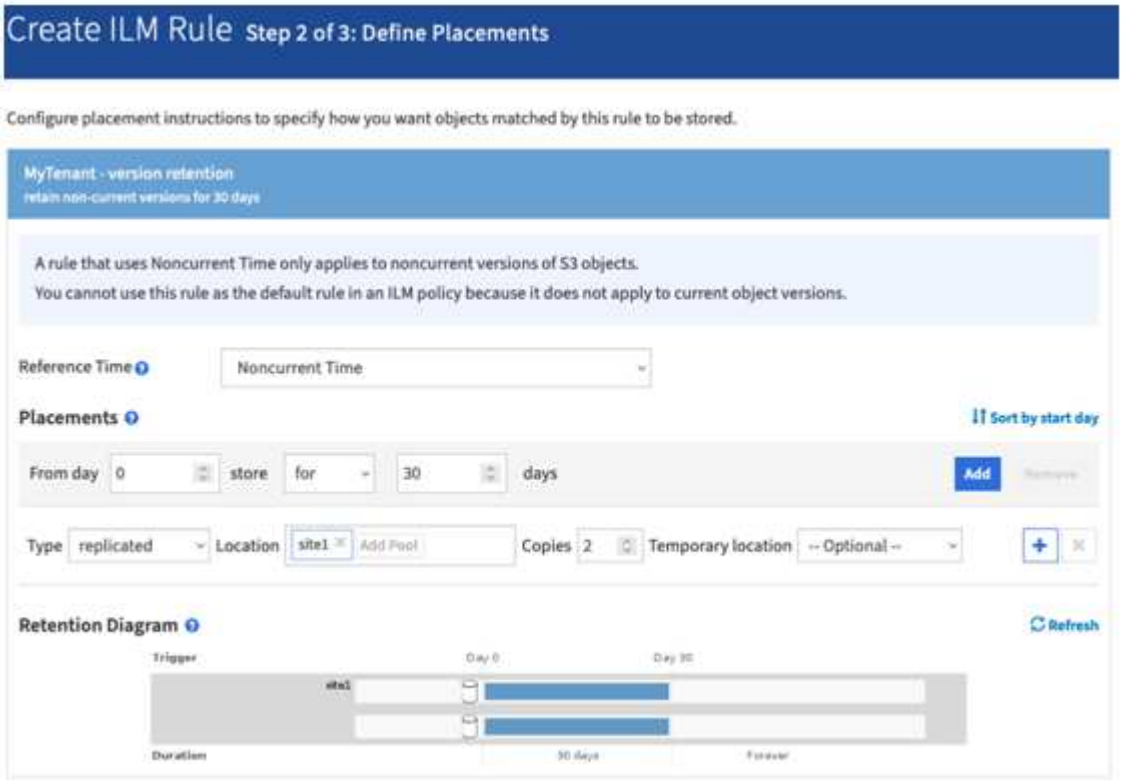



2. No intervalo de origem, configure a replicação para usar o ponto de extremidade configurado.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Crie regras ILM para gerenciar o posicionamento de armazenamento e o gerenciamento da duração do armazenamento de versão. Neste exemplo, as versões não atuais dos objetos a armazenar são configuradas.




Há duas cópias no local 1 por 30 dias. Você também configura as regras para a versão atual dos objetos com base no uso do tempo de ingestão como tempo de referência na regra ILM para corresponder à duração de armazenamento do bucket de origem. O posicionamento do storage para as versões do objeto pode ser codificado ou replicado para apagamento.

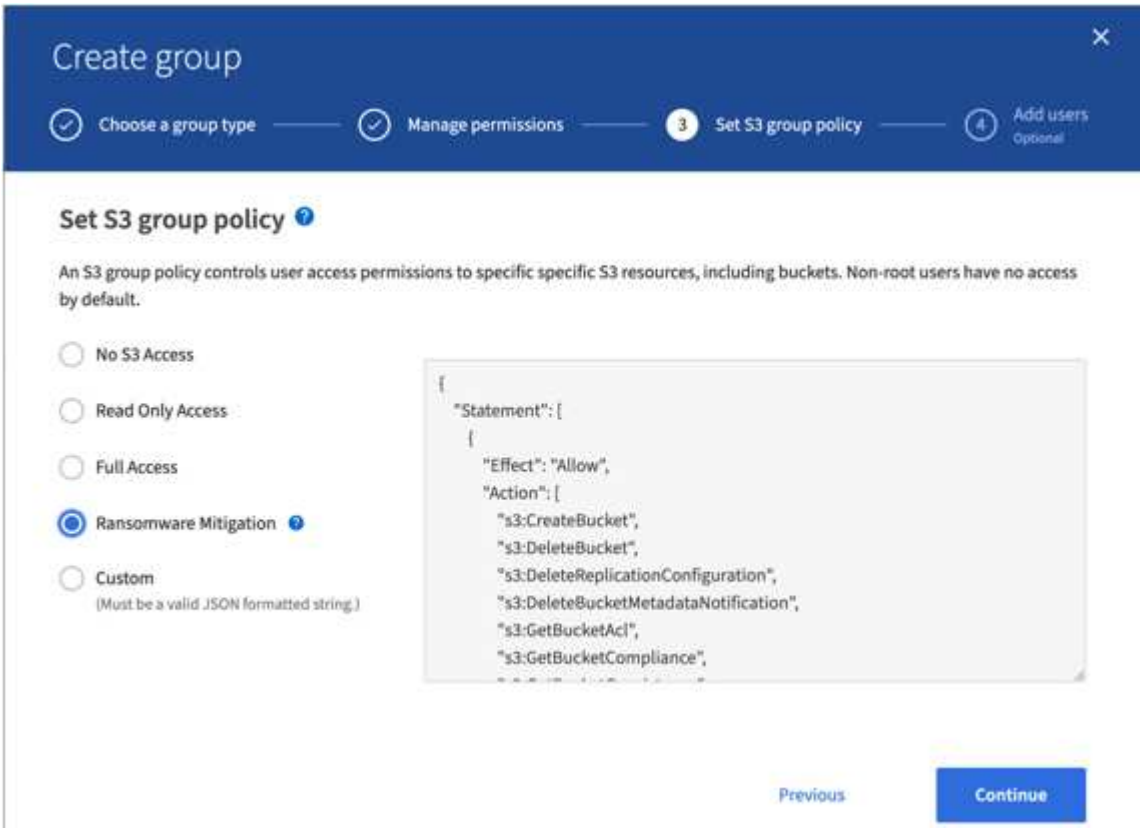
## Defesa contra ransomware usando o controle de versão com a política protetora do IAM

Saiba como proteger seus dados habilitando o controle de versão no bucket e implementando políticas do IAM em grupos de segurança de usuários no StorageGRID.

Um método para proteger seus dados sem usar bloqueio de objeto ou replicação é habilitar o controle de versão no bucket e implementar políticas do IAM nos grupos de segurança de usuários para limitar a capacidade dos usuários de gerenciar versões dos objetos. No caso de um ataque, novas versões ruins dos dados são criadas como a versão atual, e a versão não atual mais recente são os dados limpos e seguros. As

contas comprometidas para obter acesso aos dados não têm acesso para excluir ou alterar a versão não atual, protegendo-os para operações de restauração posteriores. Assim como no cenário anterior, as regras do ILM gerenciam a retenção das versões não atuais com uma duração de sua escolha. A desvantagem é que ainda há a possibilidade de contas privilegiadas existentes para um ataque de ator ruim, mas todas as contas de serviço de aplicativos e usuários devem ser configurados com um acesso mais restritivo. A política de grupo restritiva deve permitir explicitamente que cada ação que você deseja que os usuários ou aplicativos sejam capazes e negar explicitamente quaisquer ações que você não deseja que eles sejam capazes. O NetApp não recomenda o uso de uma permissão curinga porque uma nova ação pode ser introduzida no futuro e você vai querer controlar se ela é permitida ou negada. Para essa solução, a lista Negar deve incluir DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration e PutBucketversionamento para proteger a configuração de controle de versão das versões do bucket e do objeto de alterações programáticas ou do usuário.

No StorageGRID 11,7, uma nova opção de política de grupo S3 "mitigação de ransomware" foi introduzida para facilitar a implementação desta solução. Ao criar um grupo de usuários no locatário, depois de selecionar as permissões do grupo, você pode ver essa nova política opcional.




A seguir está o conteúdo da política de grupo que inclui a maioria das operações disponíveis explicitamente permitidas e o mínimo necessário negado.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
```

```
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
```

```
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

# TR-4765: Monitor StorageGRID

## Introdução ao monitoramento StorageGRID

Saiba como monitorar seu sistema StorageGRID usando aplicativos externos, como o Splunk.

O monitoramento eficaz do storage baseado em objeto do NetApp StorageGRID permite que os administradores respondam rapidamente a problemas urgentes e adicionem recursos proativamente para lidar com workloads crescentes. Este relatório fornece orientações gerais sobre como monitorar as principais métricas e como aproveitar os aplicativos de monitoramento externos. Destina-se a complementar o guia de monitorização e resolução de problemas existente.

Uma implantação do NetApp StorageGRID geralmente consiste em vários locais e muitos nós que operam para criar um sistema de storage de objetos distribuído e tolerante a falhas. Em um sistema de storage distribuído e resiliente, como o StorageGRID, é normal que existam condições de erro enquanto a grade continua operando normalmente. O desafio para você, como administrador, é entender o limite no qual as condições de erro (como nós para baixo) apresentam um problema que deve ser imediatamente resolvido versus informações que devem ser analisadas. Ao analisar os dados que o StorageGRID apresenta, você entende seu workload e toma decisões informadas, como quando adicionar mais recursos.

O StorageGRID fornece uma excelente documentação que se aprofunda no assunto do monitoramento. Este relatório pressupõe que você está familiarizado com o StorageGRID e que você revisou a documentação sobre ele. Em vez de repetir essas informações, nos referimos à documentação do produto ao longo deste

guia. A documentação do produto StorageGRID está disponível online e em formato PDF.

O objetivo deste documento é complementar a documentação do produto e discutir como monitorar o sistema StorageGRID usando aplicativos externos, como o Splunk.

#### Fontes de dados

Para monitorar com sucesso o NetApp StorageGRID, é importante saber onde coletar dados sobre a integridade e as operações do seu sistema StorageGRID.

- * Interface Web e Painel de Controle.* O Gerenciador de Grade do StorageGRID apresenta uma visualização de nível superior das informações que você, como administrador, precisa ver em uma apresentação lógica. Como administrador, você também pode aprofundar as informações de nível de serviço para solução de problemas e coleções de log.
- **Logs de auditoria.** O StorageGRID mantém logs de auditoria granular de ações de locatários, como COLOCAR, OBTER e EXCLUIR. Você também pode rastrear o ciclo de vida de um objeto desde a ingestão até a aplicação de regras de gerenciamento de dados.
- **Metrics API.** Subjacente ao StorageGRID GMI estão APIs abertas, já que a IU é orientada pela API. Essa abordagem permite extrair dados usando ferramentas externas de monitoramento e análise.

#### Onde encontrar informações adicionais

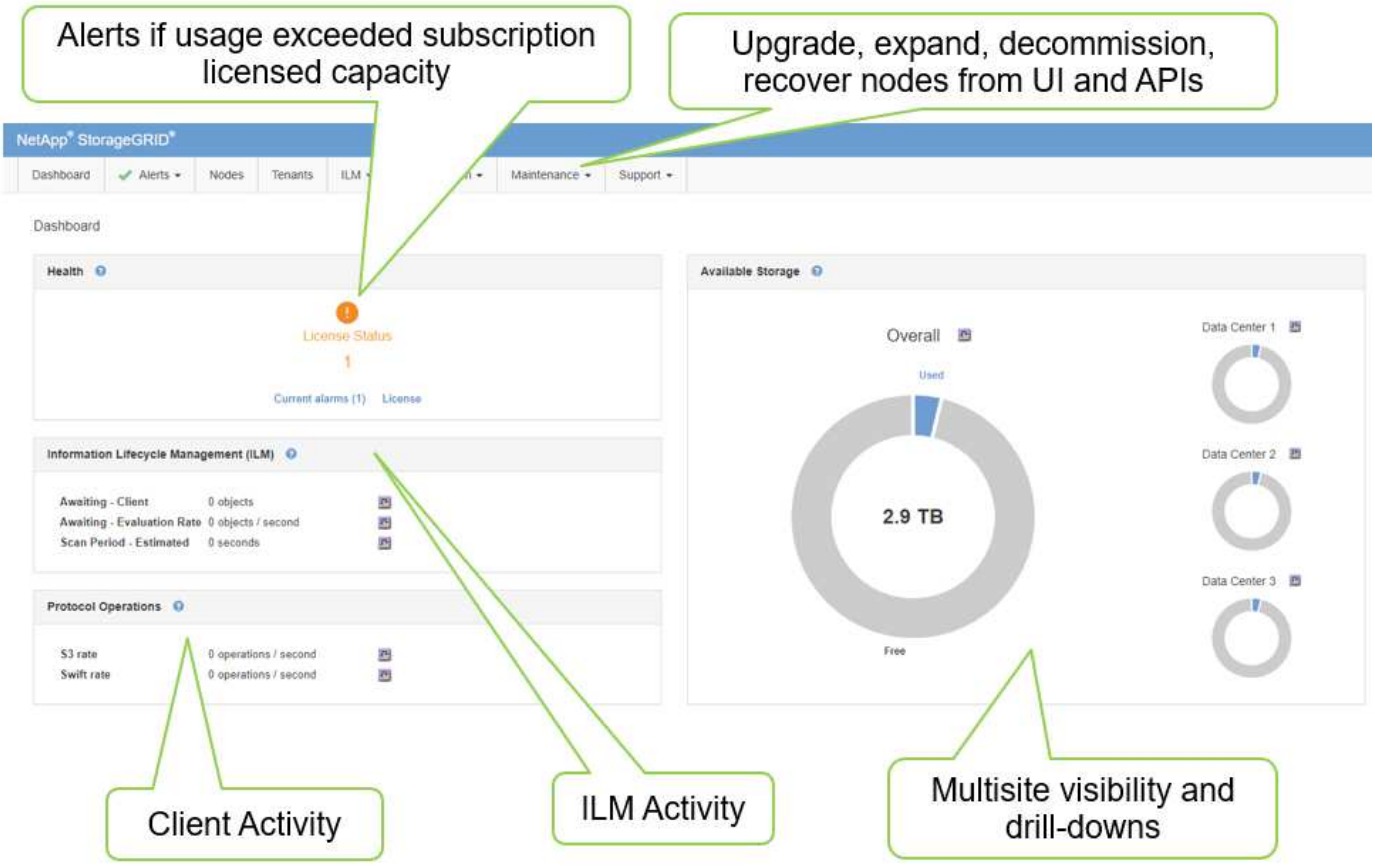
Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Centro de Documentação do NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Capacitação NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Página de recursos da documentação do StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentação do produto NetApp https://www.netapp.com/support-and-training/documentation/
- Aplicação NetApp StorageGRID para Splunk https://splunkbase.splunk.com/app/3898/#/details

## Use o painel do GMI para monitorar o StorageGRID

O dashboard da StorageGRID Grid Management Interface (GMI) fornece uma visão centralizada da infraestrutura do StorageGRID, permitindo que você supervisione a integridade, o desempenho e a capacidade de toda a grade.

Use o painel do GMI para examinar cada componente principal da grade.




**Informações que você deve monitorar regularmente**

Uma versão anterior deste relatório técnico listou as métricas para verificar periodicamente versus tendências. Essa informação está agora incluída no "Guia de monitorização e resolução de problemas".

**Monitorar o armazenamento**

Uma versão anterior deste relatório técnico listou onde monitorar métricas importantes, como espaço de armazenamento de objetos, espaço de metadados, recursos de rede e assim por diante. Essa informação está agora incluída no "Guia de monitorização e resolução de problemas".

## Use alertas para monitorar o StorageGRID

Saiba como usar o sistema de alertas no StorageGRID para monitorar problemas, gerenciar alertas personalizados e estender notificações de alerta usando SNMP ou e-mail.

Os alertas fornecem informações críticas que lhe permitem monitorizar os vários eventos e condições no seu sistema StorageGRID.

O sistema de alertas foi projetado para ser a principal ferramenta para monitorar quaisquer problemas que possam ocorrer em seu sistema StorageGRID. O sistema de alertas se concentra em problemas acionáveis no sistema e fornece uma interface fácil de usar.

Fornecemos uma variedade de regras de alerta padrão que visam ajudar a monitorar e solucionar problemas do seu sistema. Você pode gerenciar ainda mais alertas criando alertas personalizados, editando ou desativando alertas padrão e silenciando notificações de alerta.

Os alertas também são extensíveis através de notificações SNMP ou por e-mail.

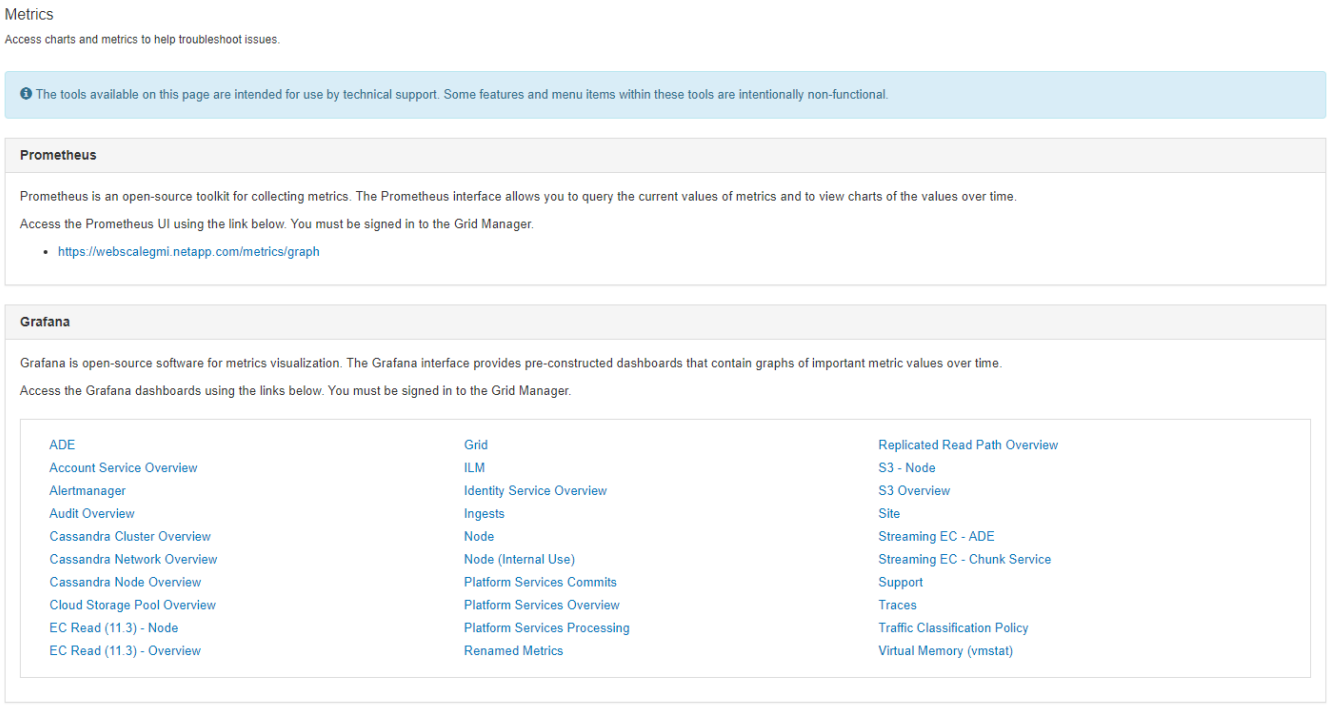
Para obter mais informações sobre alertas, consulte o "documentação do produto" disponível on-line e em formato PDF.

## Monitoramento avançado em StorageGRID

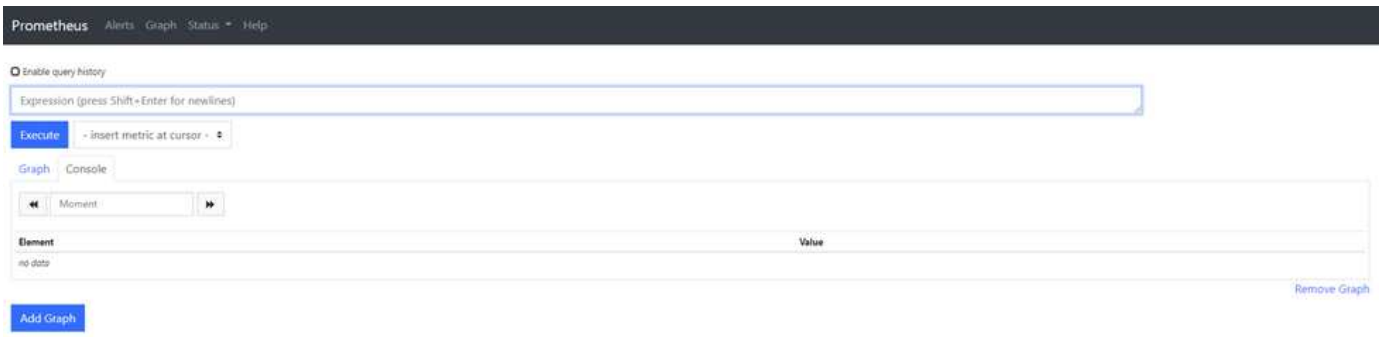
Saiba como acessar e exportar métricas para ajudar a solucionar problemas.

### Visualize a API de métricas por meio de uma consulta Prometheus

Prometheus é um software de código aberto para coletar métricas. Para acessar o Prometheus incorporado do StorageGRID através do GMI, vá para **suporte › métricas**.




Como alternativa, você pode navegar diretamente para o link.



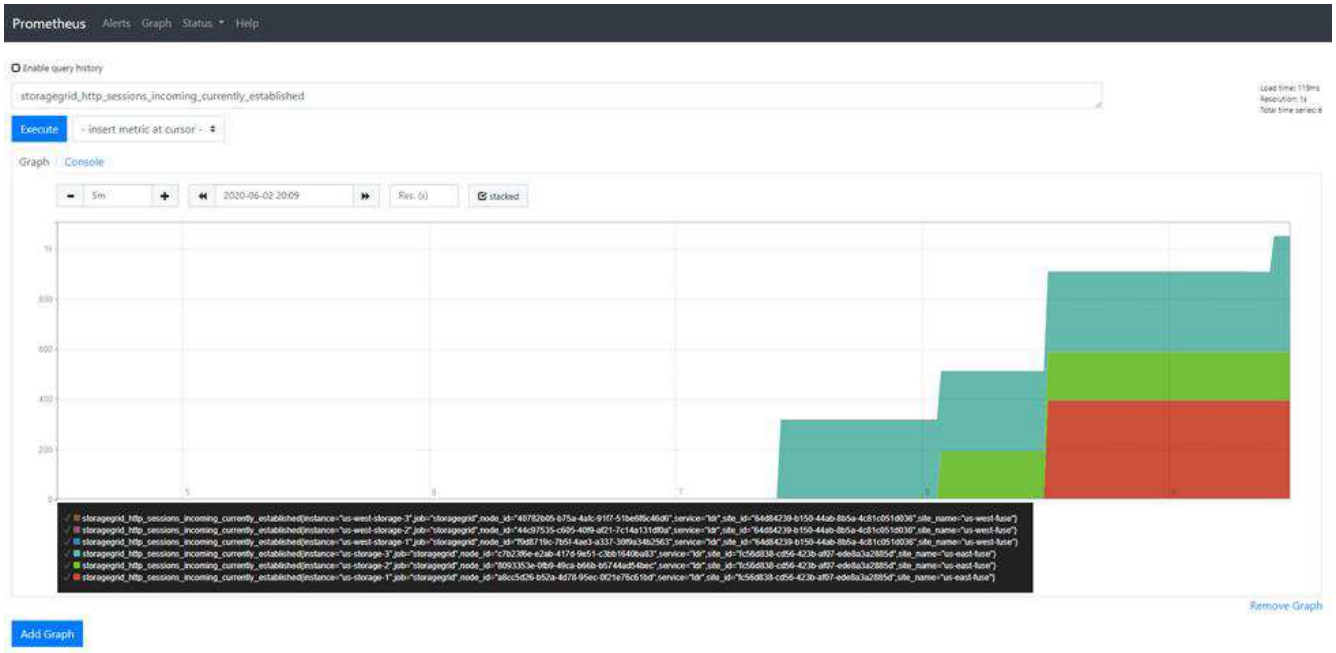

Com essa visualização, você pode acessar a interface Prometheus. A partir daí, você pode pesquisar as

métricas disponíveis e até mesmo experimentar com consultas.

Para fazer uma consulta de URL Prometheus, siga estas etapas:

**Passos**

1. Comece a digitar na caixa de texto da consulta. À medida que você digita, as métricas são listadas. Para nossos propósitos, apenas métricas que começam com StorageGRID e Node são importantes.
2. Para ver o número de sessões HTTP para cada nó, digite `storagegrid_http` e `storagegrid_http_sessions_incoming_currently_established` selecione . Clique em Executar e exiba as informações em um formato de gráfico ou console.




As consultas e gráficos que você cria através deste URL não persistem. Consultas complexas consomem recursos no nó de administração. A NetApp recomenda que você use essa visualização para explorar as métricas disponíveis.

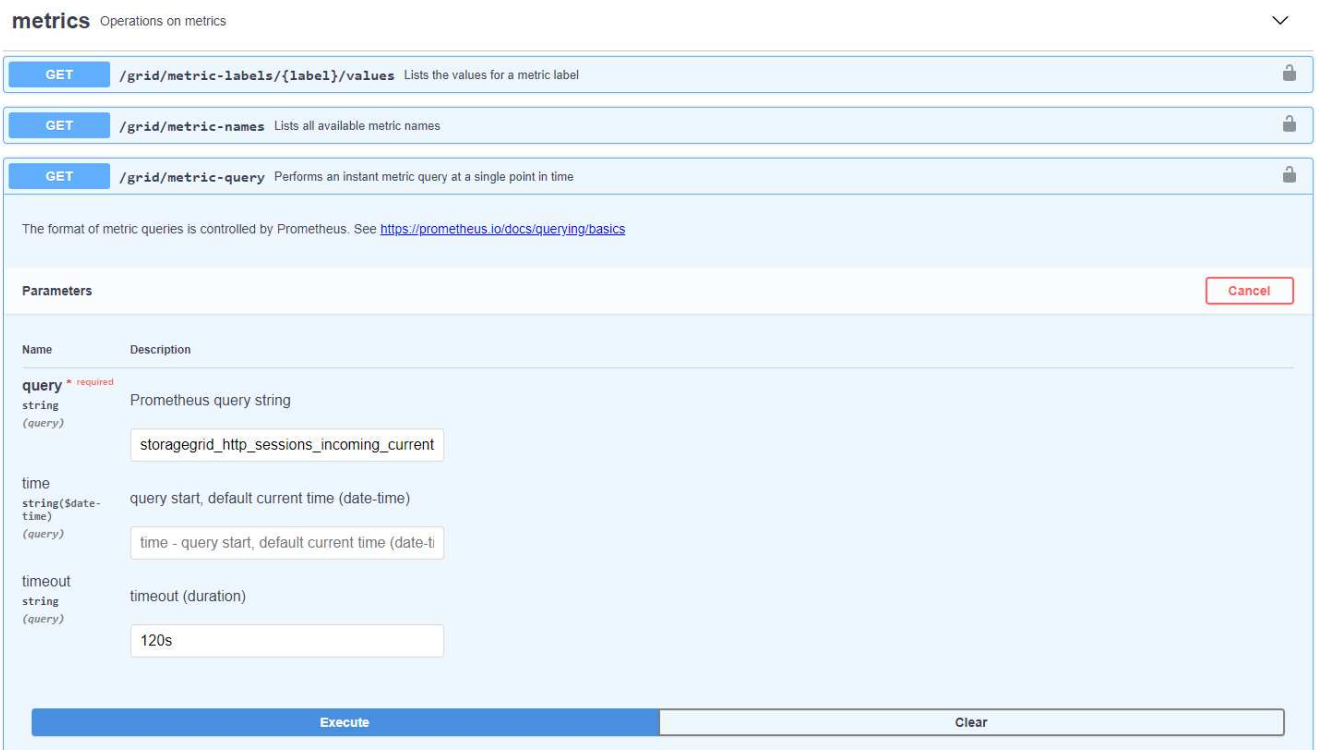
Não é recomendado fazer uma interface direta com nossa instância Prometheus porque isso requer a abertura de portas adicionais. Acessar métricas por meio de nossa API é o método recomendado e seguro.

### Exportar métricas por meio da API

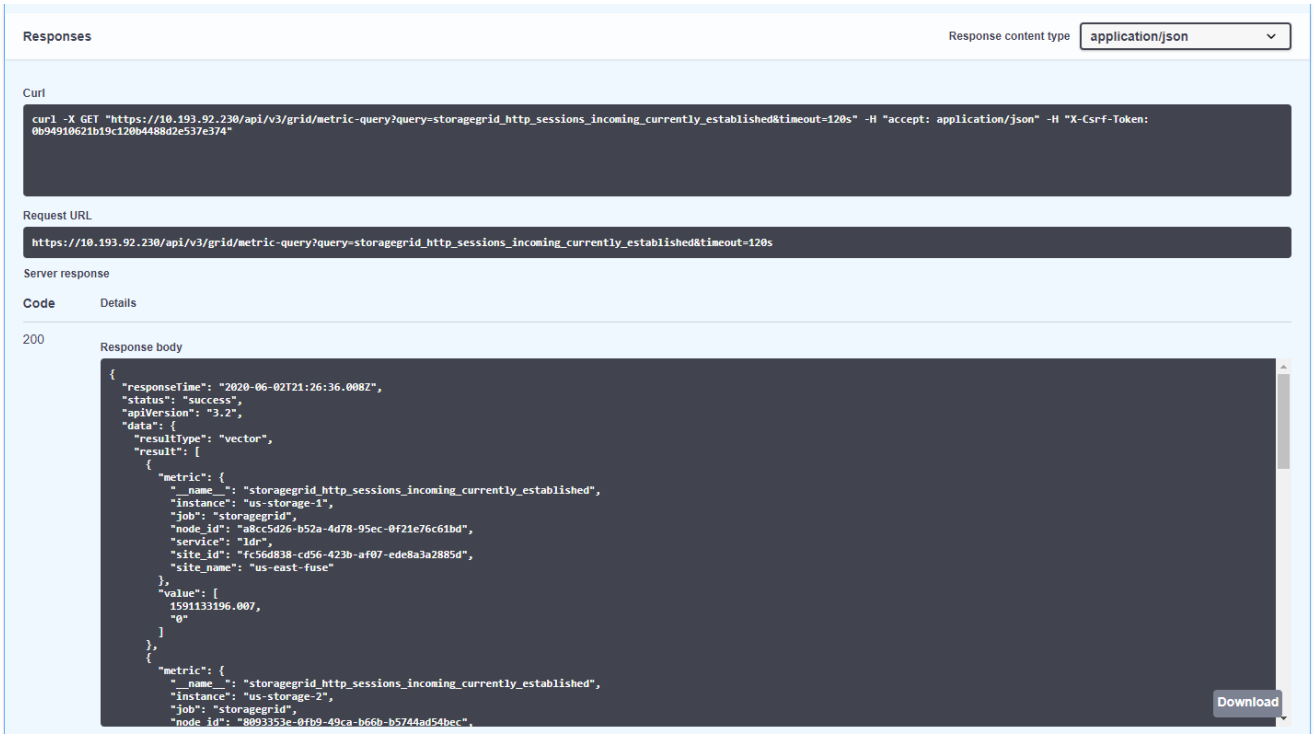
Você também pode acessar os mesmos dados por meio da API de gerenciamento do StorageGRID.

Para exportar métricas por meio da API, siga estas etapas:

1. No GMI, selecione **Ajuda › Documentação da API**.
2. Role para baixo até Metrics e SELECIONE GET /grid/metric-query.




A resposta inclui as mesmas informações que você pode obter através de uma consulta de URL Prometheus. Você pode ver novamente o número de sessões HTTP que estão atualmente estabelecidas em cada nó de armazenamento. Você também pode baixar a resposta em formato JSON para legibilidade. A figura a seguir mostra exemplos de respostas de consulta do Prometheus.




A vantagem de usar a API é que ela permite que você execute consultas autenticadas

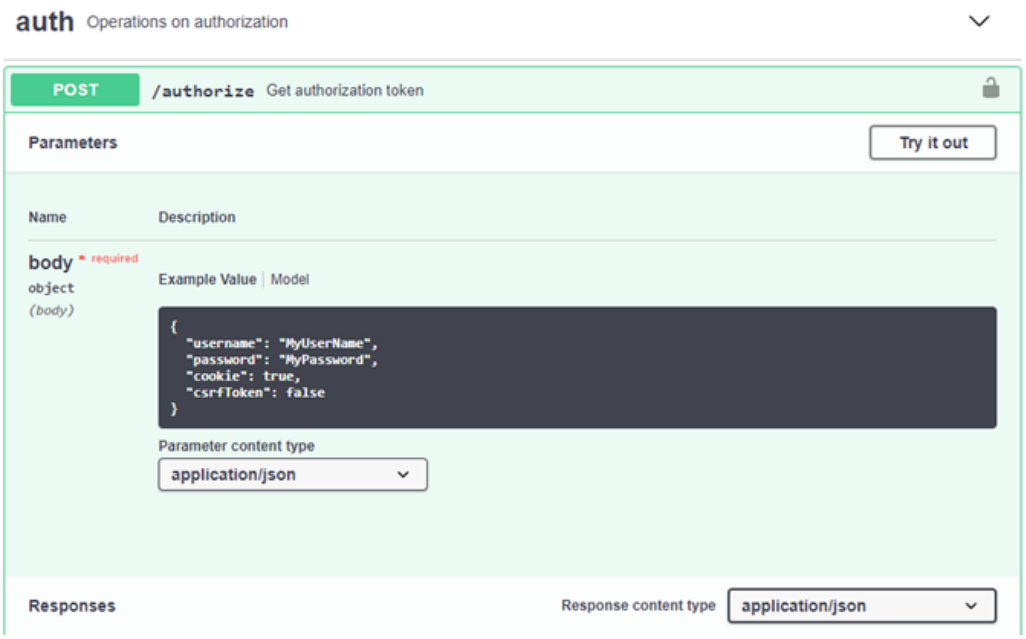
## Acesse métricas usando curl no StorageGRID

Saiba como acessar métricas por meio da CLI usando curl.

Para executar esta operação, você deve primeiro obter um token de autorização. Para solicitar um token, siga estas etapas:

**Passos**

1. No GMI, selecione **Ajuda › Documentação da API**.
2. Role para baixo até Auth para encontrar operações na autorização. A captura de tela a seguir mostra os parâmetros para o MÉTODO POST.




3. Clique em Experimente e edite o corpo com seu nome de usuário e senha do GMI.
4. Clique em Executar.
5. Copie o comando curl fornecido na seção curl e cole-o em uma janela de terminal. O comando se parece com o seguinte:

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Se sua senha do GMI contiver carateres especiais, lembre-se de usar para escapar de carateres especiais. Por exemplo, substitua ! por!

6. Depois de executar o comando curl anterior, a saída fornece um token de autorização como o exemplo a seguir:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Agora você pode usar a string de token de autorização para acessar métricas por meio do curl. O processo de acesso às métricas é semelhante às etapas da "Monitoramento avançado em StorageGRID"seção . No entanto, para fins de demonstração, mostramos um exemplo com GET /grid/metric-labels/(label)/values selecionados na categoria Metrics.

7. Como exemplo, o seguinte comando curl com o token de autorização anterior listará os nomes de sites no StorageGRID.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

O comando curl gerará a seguinte saída:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

## Visualize métricas usando o painel Grafana no StorageGRID

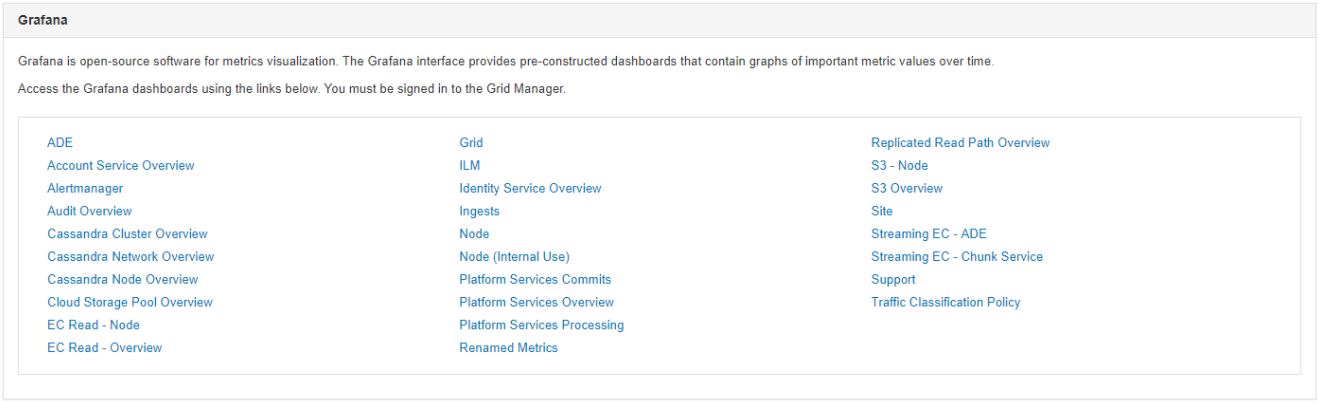
Saiba como usar a interface Grafana para visualizar e monitorar seus dados do StorageGRID.

Grafana é um software de código aberto para visualização de métricas. Por padrão, temos painéis pré-construídos que fornecem informações úteis e poderosas sobre seu sistema StorageGRID.

Esses painéis pré-construídos não são apenas úteis para monitoramento, mas também para solução de problemas. Alguns destinam-se a ser utilizados pelo suporte técnico. Por exemplo, para exibir as métricas de um nó de storage, siga estas etapas.

**Passos**

1. No GMI, **Support › Metrics**.
2. Na seção Grafana, selecione o painel nó.




3. No Grafana, defina os hosts para qualquer nó no qual você deseja exibir as métricas. Nesse caso, um nó de storage é selecionado. Mais informações são fornecidas do que as capturas de tela a seguir.


## Use políticas de classificação de tráfego no StorageGRID

Saiba como configurar e configurar políticas de classificação de tráfego para gerenciar e otimizar o tráfego de rede no StorageGRID.

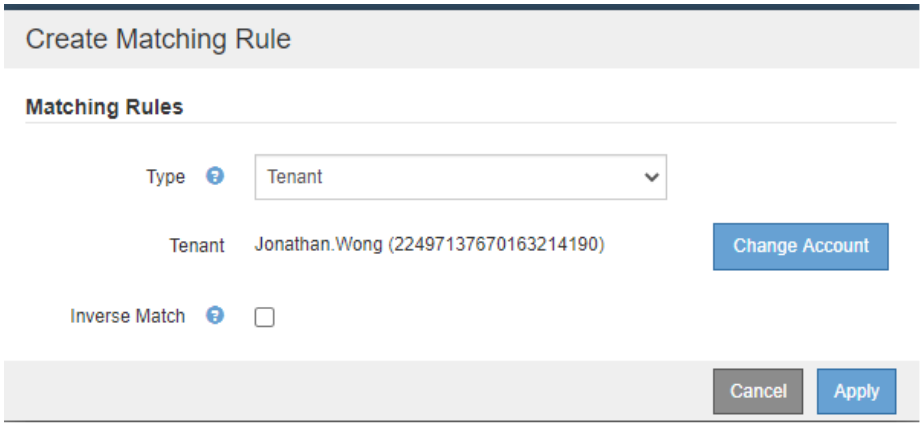
As políticas de classificação de tráfego fornecem um método para monitorar e/ou limitar o tráfego com base em um locatário específico, buckets, sub-redes IP ou pontos de extremidade do balanceador de carga. A conetividade de rede e a largura de banda são métricas especialmente importantes para o StorageGRID.

Para configurar uma Política de classificação de tráfego, siga estes passos:

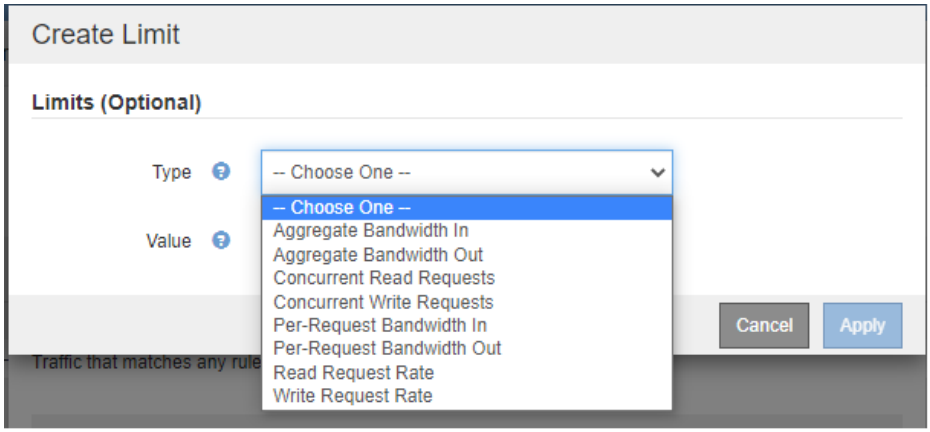
**Passos**

1. No GMI, navegue para o menu:Configuration [System Settings > Traffic Classification] (Configuração do sistema > classificação de trânsito).
2. Clique em criar
3. Introduza um nome e uma descrição para a sua política.

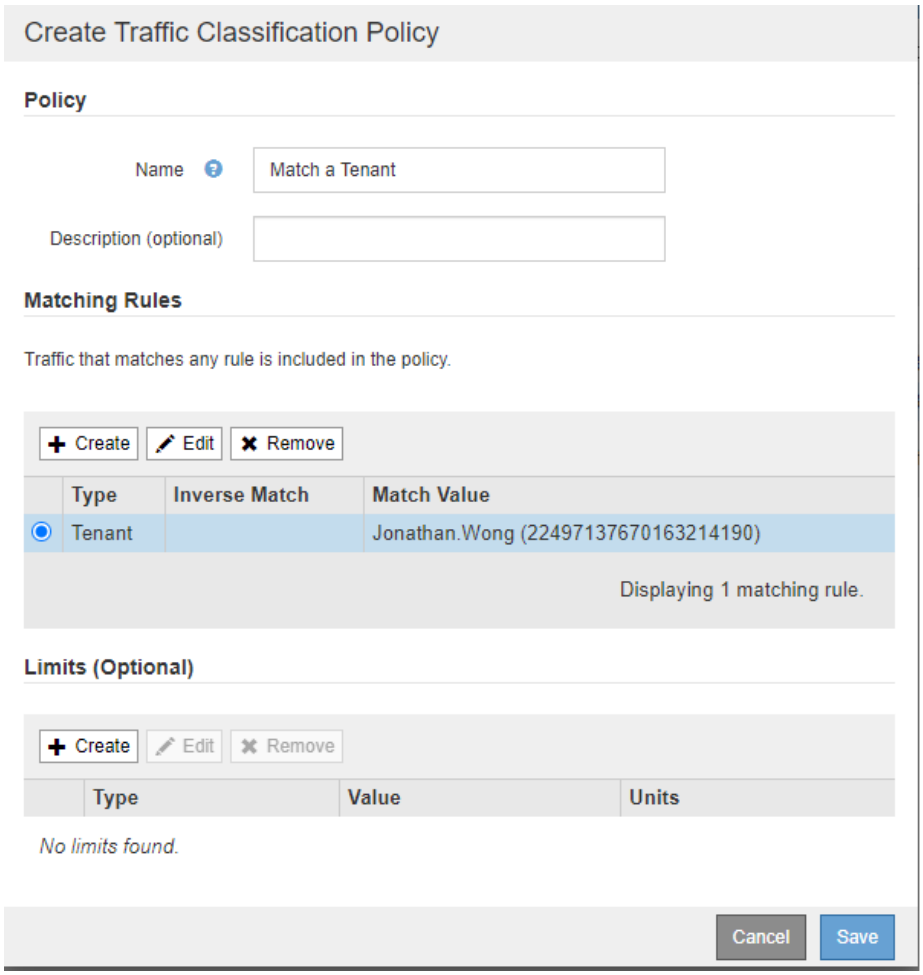
4. Crie uma regra correspondente.




5. Defina um limite (opcional).




6. Guarde a sua política




Para visualizar as métricas associadas à sua Política de classificação de tráfego, selecione a sua política e clique em métricas. Um painel do Grafana é gerado exibindo informações como tráfego de solicitação do Load Balancer e duração média da solicitação.

### Use logs de auditoria para monitorar o StorageGRID

Saiba como usar o log de auditoria do StorageGRID para obter informações detalhadas sobre as atividades do locatário e da grade e como usar ferramentas como o Splunk para análise de logs.

O log de auditoria do StorageGRID permite que você colete informações detalhadas sobre a atividade do locatário e da grade. O log de auditoria pode ser exposto para análises por meio do NFS. Para obter instruções detalhadas sobre como exportar o log de auditoria, consulte o Guia do Administrador.

Depois que a auditoria for exportada, você poderá usar ferramentas de análise de log, como Splunk ou Logstash Elasticsearch, para entender a atividade do locatário ou criar relatórios detalhados de cobrança e chargeback.

Detalhes sobre mensagens de auditoria estão incluídos na documentação do StorageGRID. "Auditar mensagens"Consulte .

### Use o aplicativo StorageGRID para Splunk

Saiba mais sobre o aplicativo NetApp StorageGRID para Splunk que permite monitorar e analisar seu ambiente do StorageGRID na plataforma.

O Splunk é uma plataforma de software que importa e indexa dados de máquina para fornecer recursos avançados de pesquisa e análise. O aplicativo NetApp StorageGRID é um complemento para Splunk que importa e enriquece os dados utilizados do StorageGRID.

As instruções sobre como instalar, atualizar e configurar o complemento StorageGRID podem ser encontradas aqui: https://splunkbase.splunk.com/app/3895/#/details

# TR-4882: Instale uma grade de metal nu StorageGRID

### Introdução à instalação do StorageGRID

Saiba como instalar o StorageGRID em hosts bare metal.

TR-4882 fornece um prático conjunto de instruções passo a passo que produz uma instalação funcional do NetApp StorageGRID. A instalação pode ser em bare metal ou em máquinas virtuais (VMs) em execução no Red Hat Enterprise Linux (RHEL). A abordagem é executar uma instalação "opinativa" de seis serviços em contêiner do StorageGRID em três máquinas físicas (ou virtuais) em um layout sugerido e configuração de storage. Alguns clientes podem achar mais fácil entender o processo de implantação seguindo o exemplo de implantação neste TR.

Para obter uma compreensão mais aprofundada sobre o StorageGRID e o processo de instalação, https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html consulte [Instalar, atualizar e hotfix StorageGRID] na documentação do produto.

Antes de iniciar a implantação, vamos examinar os requisitos de computação, storage e rede do software NetApp StorageGRID. O StorageGRID é executado como um serviço em contentor dentro do Podman ou do Docker. Neste modelo, alguns requisitos referem-se ao sistema operacional host (o SO que hospeda o Docker, que está executando o software StorageGRID). E alguns dos recursos são alocados diretamente para os contentores Docker em execução dentro de cada host. Nesta implantação, a fim de maximizar o uso de hardware, estamos implantando dois serviços por host físico. Para obter mais informações, continue para a

próxima seção, "Pré-requisitos para instalar o StorageGRID".

As etapas descritas neste TR resultam em uma instalação do StorageGRID em funcionamento em seis hosts de metal nu. Agora você tem uma rede de trabalho e uma rede de clientes, que são úteis na maioria dos cenários de teste.

### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste TR, consulte os seguintes recursos de documentação:

- Centro de Documentação do NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Capacitação NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Página de recursos da documentação do StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentação do produto NetApp https://www.netapp.com/support-and-training/documentation/

## Pré-requisitos para instalar o StorageGRID

Saiba mais sobre os requisitos de computação, armazenamento, rede, docker e nó para implantar o StorageGRID.

### Requisitos de computação

A tabela abaixo lista os requisitos mínimos de recursos suportados para cada tipo de nó StorageGRID. Esses são os recursos mínimos necessários para os nós do StorageGRID.

| Tipo de nó | Núcleos de CPU | RAM |
|---|---|---|
| Administrador | 8 | 24 GB |
| Armazenamento | 8 | 24 GB |
| Gateway | 8 | 24 GB |

Além disso, cada host Docker físico deve ter um mínimo de 16GB GB de RAM alocado para ele para operação adequada. Então, por exemplo, para hospedar quaisquer dois dos serviços descritos na tabela juntos em um host Docker físico, você faria o seguinte cálculo:

24 24GB RAM 64GBGB e 8GB RAM 8GB 16 núcleos

Como muitos servidores modernos excedem esses requisitos, combinamos seis serviços (contentores StorageGRID) em três servidores físicos.

### Requisitos de rede

Os três tipos de tráfego StorageGRID incluem:

- **Tráfego de grade (obrigatório).** O tráfego StorageGRID interno que viaja entre todos os nós na grade.
- **Admin traffic (opcional).** O tráfego utilizado para a administração e manutenção do sistema.
- **Tráfego do cliente (opcional).** O tráfego que viaja entre aplicativos clientes externos e a grade, incluindo todas as solicitações de armazenamento de objetos de clientes S3 e Swift.

Pode configurar até três redes para utilização com o sistema StorageGRID. Cada tipo de rede deve estar em

uma sub-rede separada sem sobreposição. Se todos os nós estiverem na mesma sub-rede, não será necessário um endereço de gateway.

Para esta avaliação, vamos implantar em duas redes, que contêm a grade e o tráfego do cliente. É possível adicionar uma rede de administração mais tarde para servir essa função adicional.

É muito importante mapear as redes de forma consistente para as interfaces em todos os hosts. Por exemplo, se houver duas interfaces em cada nó, ens192 e ens224, todas elas devem ser mapeadas para a mesma rede ou VLAN em todos os hosts. Nesta instalação, o instalador os mapeia para os contentores Docker como eth0 a if2 e eth2 a if3 (porque o loopback é if1 dentro do contentor), e, portanto, um modelo consistente é muito importante.

#### Nota sobre a rede Docker

O StorageGRID usa a rede de forma diferente de algumas implementações de contentor Docker. Ele não usa a rede fornecida pelo Docker (ou Kubernetes ou Swarm). Em vez disso, o StorageGRID realmente gera o contentor como none para que o Docker não faça nada para colocar em rede o contentor. Depois que o contentor tiver sido gerado pelo serviço StorageGRID, um novo dispositivo macvlan é criado a partir da interface definida no arquivo de configuração do nó. Esse dispositivo tem um novo endereço MAC e atua como um dispositivo de rede separado que pode receber pacotes da interface física. O dispositivo macvlan é então movido para o namespace de contentor e renomeado para ser um dos eth0, eth1 ou eth2 dentro do contentor. Nesse ponto, o dispositivo de rede não está mais visível no sistema operacional do host. Em nosso exemplo, o dispositivo de rede de grade é eth0 dentro dos contentores Docker e a rede de cliente é eth2. Se tivéssemos uma rede de administração, o dispositivo seria eth1 no contentor.

> ⓘ O novo endereço MAC do dispositivo de rede de contentores pode exigir que o modo promíscuo seja ativado em alguns ambientes de rede e virtuais. Este modo permite que o dispositivo físico receba e envie pacotes para endereços MAC diferentes do endereço MAC físico conhecido. Se estiver em execução no VMware vSphere, você deve aceitar o modo promíscuo, alterações de endereço MAC e transmissões forjadas nos grupos de portas que servirão ao tráfego StorageGRID ao executar o RHEL. Ubuntu ou Debian funciona sem essas alterações na maioria das circunstâncias. Mais uma vez

### Requisitos de storage

Cada um dos nós requer dispositivos de disco locais ou baseados em SAN dos tamanhos mostrados na tabela a seguir.

> ⓘ Os números na tabela são para cada tipo de serviço StorageGRID, não para a grade inteira ou cada host físico. Com base nas opções de implantação, calcularemos os números para cada host físico no "Layout e requisitos físicos do host", mais adiante neste documento. Os caminhos ou sistemas de arquivos marcados com um asterisco serão criados no próprio contentor StorageGRID pelo instalador. Nenhuma configuração manual ou criação do sistema de arquivos é exigida pelo administrador, mas os hosts precisam de dispositivos de bloco para satisfazer esses requisitos. Em outras palavras, o dispositivo de bloco deve aparecer usando o comando `lsblk`, mas não ser formatado ou montado dentro do sistema operacional do host. Mais uma vez

| Tipo de nó | Finalidade do LUN | Número de LUNs | Tamanho mínimo de LUN | É necessário um sistema de ficheiros manual | Entrada de configuração do nó sugerida |
|---|---|---|---|---|---|
| Tudo | Espaço do sistema do nó de administração `/var/local` (SSD útil aqui) | Um para cada nó de administração | 90 GB | Não | `BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL` |
| Todos os nós | Pool de armazenamento do Docker em `/var/lib/docker for container pool` | Um para cada host (físico ou VM) | 100GB kg por recipiente | Sim – etx4 | NA – formate e monte como sistema de arquivos host (não mapeado no contentor) |
| Administrador | Logs de auditoria do Admin Node (dados do sistema no Admin Container) `/var/local/audit/export` | Um para cada nó de administração | 200 GB | Não | `BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS` |
| Administrador | Tabelas do Admin Node (dados do sistema no Admin Container) `/var/local/mysql_ibdata` | Um para cada nó de administração | 200 GB | Não | `BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL` |
| Nós de storage | Armazenamento de objetos (dispositivos de bloco `/var/local/rangedb0`) (SSD útil aqui) `/var/local/rangedb1` `/var/local/rangedb2` | Três para cada contêiner de storage | 4000 GB | Não | `BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02` |

Neste exemplo, os tamanhos de disco mostrados na tabela a seguir são necessários por tipo de contentor. Os requisitos por host físico são descritos em "Layout e requisitos físicos do host", mais adiante neste documento.

### Tamanhos de disco por tipo de contentor

#### Contêiner de administração

| Nome | Tamanho (GiB) |
|---|---|
| Docker-Store | 100 kg (por recipiente) |

| Nome | Tamanho (GiB) |
| --- | --- |
| ADM-os | 90 |
| ADM-Auditoria | 200 |
| ADM-MySQL | 200 |

#### Contêiner de storage

| Nome | Tamanho (GiB) |
| --- | --- |
| Docker-Store | 100 kg (por recipiente) |
| SN-OS | 90 |
| Rangedb-0 | 4096 |
| Rangedb-1 | 4096 |
| Rangedb-2 | 4096 |

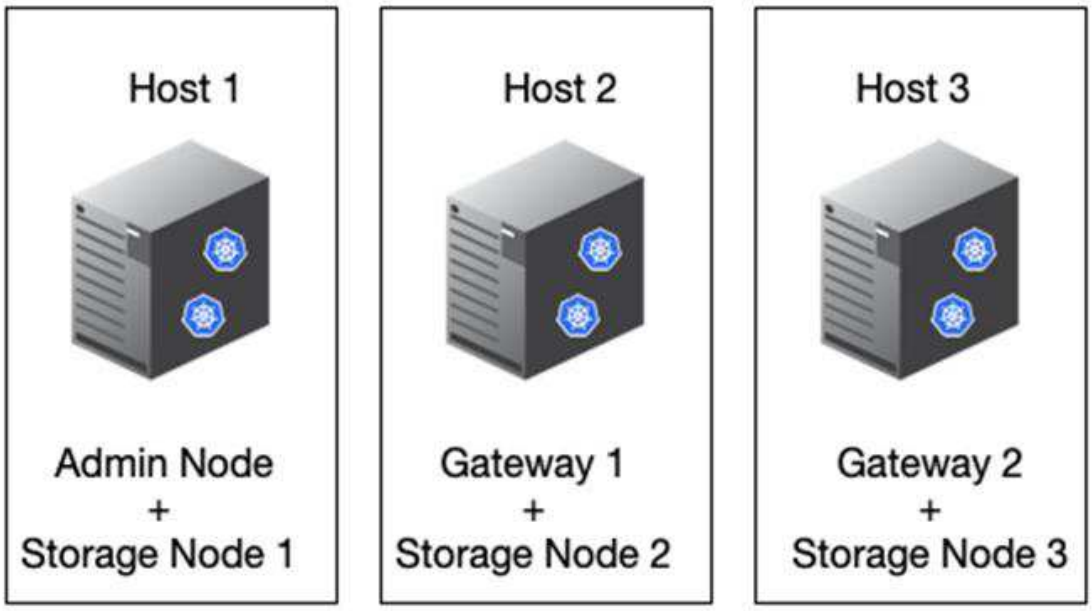
#### Contêiner do gateway

| Nome | Tamanho (GiB) |
| --- | --- |
| Docker-Store | 100 kg (por recipiente) |
| /var/local | 90 |

### Layout e requisitos físicos do host

Combinando os requisitos de computação e rede mostrados na tabela acima, você pode obter um conjunto básico de hardware necessário para essa instalação de três servidores físicos (ou virtuais) com 16 núcleos, 64GB GB de RAM e duas interfaces de rede. Se for desejado um throughput mais alto, é possível vincular duas ou mais interfaces na rede Grid ou Client Network e usar uma interface VLAN-tagged como bond0,520 no arquivo de configuração do nó. Se você espera cargas de trabalho mais intensas, mais memória para o host e os contêineres é melhor.

Como mostrado na figura a seguir, esses servidores hospedarão seis contentores Docker, dois por host. A RAM é calculada fornecendo 24GB GB por contentor e 16GB GB para o próprio sistema operacional host.




A RAM total necessária por host físico (ou VM) é 24 x 2 e 16 x 64GB. As tabelas a seguir listam o armazenamento de disco necessário para os hosts 1, 2 e 3.

| **Host 1** | **Tamanho (GiB)** |
|---|---|
| **Docker Store** | `/var/lib/docker` (Sistema de ficheiros) |
| 200 (100 x 2) | **Admin Container** |
| `BLOCK_DEVICE_VAR_LOCAL` | 90 |
| `BLOCK_DEVICE_AUDIT_LOGS` | 200 |
| `BLOCK_DEVICE_TABLES` | 200 |
| **Recipiente de armazenamento** | SN-os<br>`/var/local` (dispositivo) |
| 90 | Rangedb-0 (dispositivo) |
| 4096 | Rangedb-1 (dispositivo) |
| 4096 | Rangedb-2 (dispositivo) |

| **Host 2** | **Tamanho (GiB)** |
|---|---|
| **Docker Store** | `/var/lib/docker` (Partilhado) |
| 200 (100 x 2) | **Gateway Container** |
| GW-OS */`var/local` | 100 |

| Host 2 | Tamanho (GiB) |
| --- | --- |
| **Recipiente de armazenamento** | */var/local |
| 100 | Rangedb-0 |
| 4096 | Rangedb-1 |
| 4096 | Rangedb-2 |

| Host 3 | Tamanho (GiB) |
| --- | --- |
| **Docker Store** | /var/lib/docker (Partilhado) |
| 200 (100 x 2) | **Gateway Container** |
| */var/local | 100 |
| **Recipiente de armazenamento** | */var/local |
| 100 | Rangedb-0 |
| 4096 | Rangedb-1 |
| 4096 | Rangedb-2 |

O Docker Store foi calculado permitindo 100GB por /var/local (por contentor) x dois contentores de 200GB.

**Preparando os nós**

Para se preparar para a instalação inicial do StorageGRID, primeiro instale o RHEL versão 9,2 e habilite o SSH. Configure interfaces de rede, Network Time Protocol (NTP), DNS e o nome do host de acordo com as práticas recomendadas. Você precisa de pelo menos uma interface de rede habilitada na rede de grade e outra para a rede de cliente. Se você estiver usando uma interface com VLAN, configure-a de acordo com os exemplos abaixo. Caso contrário, uma configuração de interface de rede padrão simples será suficiente.

Se você precisar usar uma tag VLAN na interface de rede de grade, sua configuração deve ter dois arquivos no /etc/sysconfig/network-scripts/ seguinte formato:

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

Este exemplo assume que o dispositivo de rede física para a rede de grade é enp67s0. Ele também pode ser um dispositivo ligado, como bond0. Se você estiver usando a ligação ou uma interface de rede padrão, você deve usar a interface VLAN-tagged em seu arquivo de configuração de nó se sua porta de rede não tiver uma VLAN padrão ou se a VLAN padrão não estiver associada à rede de grade. O contentor StorageGRID em si não desmarca quadros Ethernet, portanto, ele deve ser Tratado pelo sistema operacional pai.

#### Configuração de armazenamento opcional com iSCSI

Se não estiver a utilizar armazenamento iSCSI, tem de garantir que o host1, o host2 e o host3 contêm dispositivos de bloco de tamanho suficiente para satisfazer os seus requisitos. "Tamanhos de disco por tipo de contentor"Consulte para obter informações sobre os requisitos de armazenamento host1, host2 e host3.

Para configurar o armazenamento com iSCSI, execute as seguintes etapas:

**Passos**

1. Se você estiver usando armazenamento iSCSI externo, como o software de gerenciamento de dados NetApp e-Series ou NetApp ONTAP, instale os seguintes pacotes:

   ```
   sudo yum install iscsi-initiator-utils
   sudo yum install device-mapper-multipath
   ```

2. Encontre o ID do iniciador em cada host.

   ```
   # cat /etc/iscsi/initiatorname.iscsi
   InitiatorName=iqn.2006-04.com.example.node1
   ```

3. Usando o nome do iniciador da etapa 2, mapeie LUNs no dispositivo de armazenamento (do número e tamanho mostrados na "Requisitos de storage" tabela) para cada nó de armazenamento.
4. Descubra os LUNs recém-criados com `iscsiadm` e inicie sessão neles.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

Para obter detalhes, consulte "Criando um iniciador iSCSI" no Portal do Cliente Red Hat.

5. Para mostrar os dispositivos multipath e seus WWIDs de LUN associados, execute o seguinte comando:

```
# multipath -ll
```

Se você não estiver usando iSCSI com dispositivos multipath, basta montar o dispositivo por um nome de caminho exclusivo que irá persistir as alterações e reinicializações do dispositivo.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

O simples uso `/dev/sdx` de nomes de dispositivos pode causar problemas mais tarde se os dispositivos forem removidos ou adicionados. Se você estiver usando dispositivos multipath, modifique o `/etc/multipath.conf` arquivo para usar aliases da seguinte forma. Mais uma vez

Esses dispositivos podem ou não estar presentes em todos os nós, dependendo do layout.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

Antes de instalar o Docker no sistema operacional do host, formate e monte o suporte de LUN ou disco `/var/lib/docker` . Os outros LUNs são definidos no arquivo de configuração do nó e são usados diretamente pelos contêineres do StorageGRID. Ou seja, eles não aparecem no sistema operacional do host; eles aparecem nos próprios contentores, e esses sistemas de arquivos são manipulados pelo instalador.

Se você estiver usando um LUN com suporte iSCSI, coloque algo semelhante à seguinte linha em seu arquivo fstab. Como observado, os outros LUNs não precisam ser montados no sistema operacional do host, mas

devem aparecer como dispositivos de bloco disponíveis.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

### Preparando-se para a instalação do Docker

Para se preparar para a instalação do Docker, execute as seguintes etapas:

**Passos**

1. Crie um sistema de arquivos no volume de armazenamento do Docker em todos os três hosts.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Se estiver a utilizar dispositivos iSCSI com multipath, `/dev/mapper/Docker-Store` utilize o .

2. Crie o ponto de montagem do volume de armazenamento do Docker:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Adicione uma entrada semelhante para o dispositivo docker-storage-volume ao `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   A seguinte `_netdev` opção é recomendada apenas se estiver a utilizar um dispositivo iSCSI. Se você estiver usando um dispositivo de bloco local `_netdev` não é necessário e `defaults` é recomendado.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Monte o novo sistema de arquivos e visualize o uso do disco.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Desative a swap e desative-a por motivos de desempenho.

   ```
   $ sudo swapoff --all
   ```

6. Para persistir as configurações, remova todas as entradas de swap do /etc/fstab, como:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

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

7. Execute uma reinicialização de teste do nó para garantir que o `/var/lib/docker` volume seja persistente e que todos os dispositivos de disco voltem.

## Instale o Docker para StorageGRID

Saiba como instalar o Docker para StorageGRID.

Para instalar o Docker, execute as seguintes etapas:

**Passos**

1. Configure o repositório yum para Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Instale os pacotes necessários.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Inicie o Docker.

```
sudo systemctl start docker
```

4. Testar Docker.

```
sudo docker run hello-world
```

5. Certifique-se de que o Docker seja executado no início do sistema.

```
sudo systemctl enable docker
```

## Prepare arquivos de configuração de nós para o StorageGRID

Saiba como preparar os arquivos de configuração do nó para o StorageGRID.

Em um nível alto, o processo de configuração do nó inclui as seguintes etapas:

**Passos**

1. Crie o `/etc/storagegrid/nodes` diretório em todos os hosts.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Crie os arquivos necessários por host físico para corresponder ao layout do tipo container/nó. Neste exemplo, criamos dois arquivos por host físico em cada máquina host.

> O nome do arquivo define o nome do nó real para instalação. Por exemplo, `dc1-adm1.conf` torna-se um nó `dc1-adm1` chamado .

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— Host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

**Preparando os arquivos de configuração do nó**

Os exemplos a seguir usam o `/dev/disk/by-path` formato. Você pode verificar os caminhos corretos executando os seguintes comandos:

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

E estes comandos:

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

**Exemplo para nó Admin principal**

Exemplo de nome de arquivo:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Exemplo de conteúdo do arquivo:

> Os caminhos de disco podem seguir os exemplos abaixo ou usar `/dev/mapper/alias` nomes de estilo. Não use nomes de dispositivos de bloco, como por exemplo `/dev/sdb`, porque eles podem mudar na reinicialização e causar grandes danos à sua grade.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

**Exemplo para um nó de storage**

Exemplo de nome de arquivo:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

**Exemplo para nó de gateway**

Exemplo de nome de arquivo:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

## Instale dependências e pacotes do StorageGRID

Saiba como instalar dependências e pacotes do StorageGRID.

Para instalar as dependências e pacotes do StorageGRID, execute os seguintes comandos:

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

## Valide os arquivos de configuração do StorageGRID

Saiba como validar o conteúdo dos arquivos de configuração do StorageGRID.

Depois de criar os arquivos de configuração em `/etc/storagegrid/nodes` para cada um dos seus nós do StorageGRID, é necessário 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:

```
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
```

Se os arquivos de configuração estiverem incorretos, os problemas serão exibidos como AVISO e ERRO. Se forem encontrados quaisquer erros de configuração, é necessário corrigi-los antes de continuar com a instalação.

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

## Inicie o serviço de host do StorageGRID

Saiba como iniciar o serviço de host do StorageGRID.

Para iniciar os nós do StorageGRID e garantir que eles sejam reiniciados após uma reinicialização do host, você deve ativar e iniciar o serviço de host do StorageGRID.

Para iniciar o serviço de host StorageGRID, execute as etapas a seguir.

**Passos**

1. Execute os seguintes comandos em cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

   O processo de início pode demorar algum tempo na execução inicial.

2. Execute o seguinte comando para garantir que a implantação está em andamento:

```
sudo storagegrid node status node-name
```

3. Para qualquer nó que retorna um status de `Not-Running` ou `Stopped`, execute o seguinte comando:

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

   Por exemplo, dada a seguinte saída, você iniciaria o `dc1-adm1` nó:

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

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

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

## Configure o Gerenciador de Grade no StorageGRID

Saiba como configurar o Gerenciador de Grade no StorageGRID no nó de administrador principal.

Conclua a instalação configurando o sistema StorageGRID a partir da interface de usuário do Gerenciador de

Grade no nó Admin principal.

### Degraus de alto nível

Configurar a grade e concluir a instalação envolve as seguintes tarefas:

**Passos**

1. Navegue até Grid Manager
2. "Especifique as informações da licença do StorageGRID"
3. "Adicione sites ao StorageGRID"
4. "Especifique sub-redes de rede de grade"
5. "Aprovar nós de grade pendentes"
6. "Especifique as informações do servidor NTP"
7. "Especifique as informações do servidor do sistema de nomes de domínio"
8. "Especifique as senhas do sistema StorageGRID"
9. "Revise sua configuração e conclua a instalação"

### Navegue até Grid Manager

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

Antes de começar, o nó Admin principal deve ser implantado e ter concluído a sequência inicial de inicialização.

Para usar o Gerenciador de Grade para definir informações, execute as etapas a seguir.

**Passos**

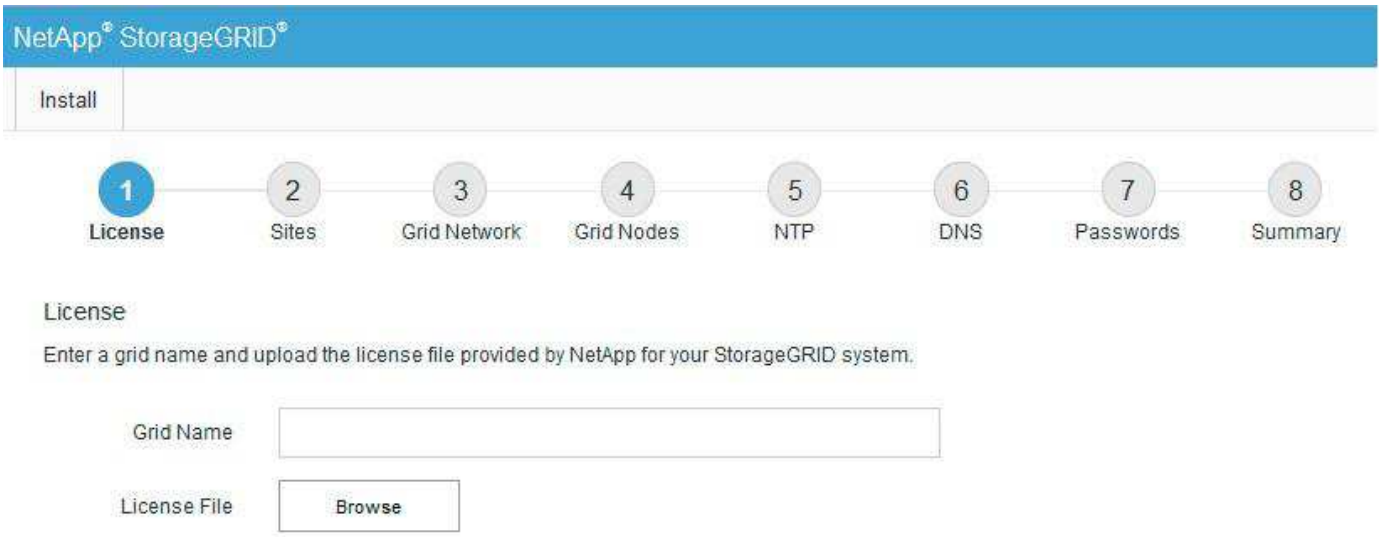
1. Acesse o Grid Manager no seguinte endereço:

   ```
   https://primary_admin_node_grid_ip
   ```

   Alternativamente, você pode acessar o Grid Manager na porta 8443.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Clique em Instalar um sistema StorageGRID. É apresentada a página utilizada para configurar uma grelha StorageGRID.




## Adicione detalhes da licença do StorageGRID

Saiba como carregar o ficheiro de licença do StorageGRID.

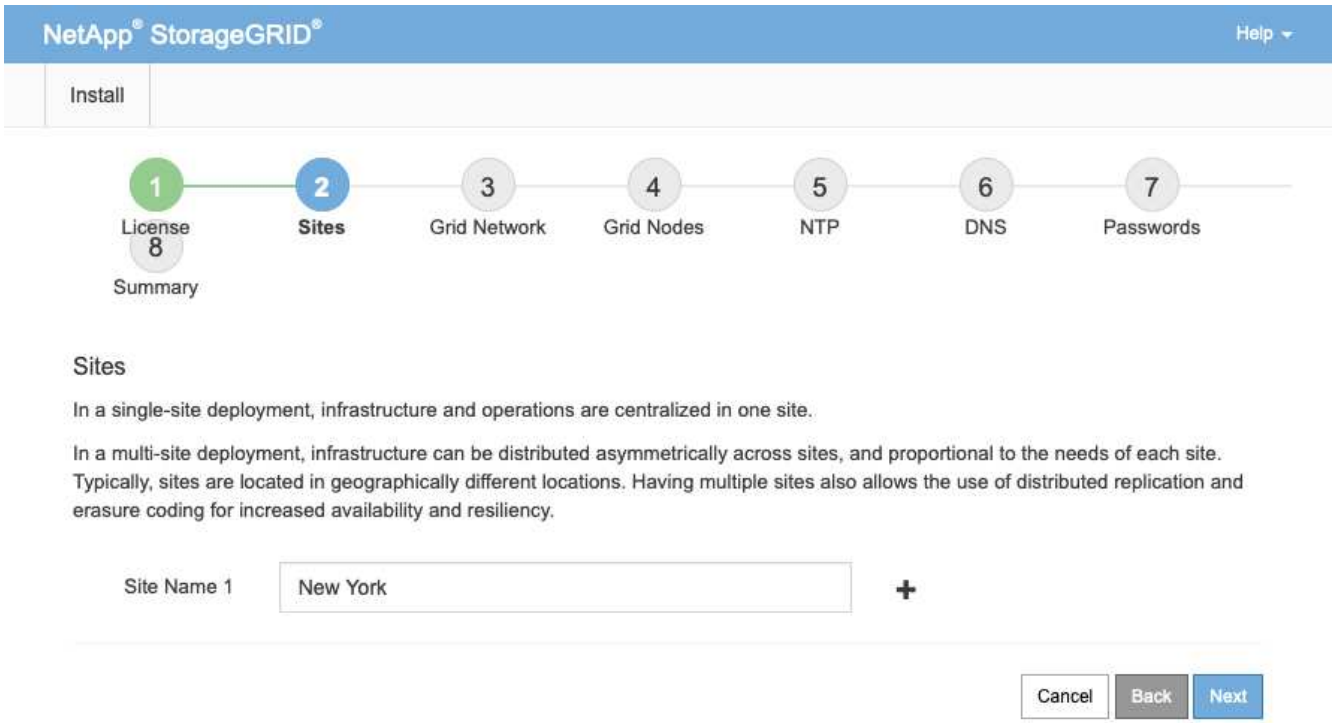
Você deve especificar o nome do seu sistema StorageGRID e fazer o upload do arquivo de licença fornecido pelo NetApp.

Para especificar as informações da licença do StorageGRID, execute as seguintes etapas:

**Passos**

1. Na página Licença, no campo Nome da Grade, digite um nome para o sistema StorageGRID. Após a instalação, o nome é exibido como o nível superior na árvore de topologia da grade.
2. Clique em Procurar, localize o ficheiro de licença do NetApp (`NLF-unique-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.

## Adicione sites ao StorageGRID

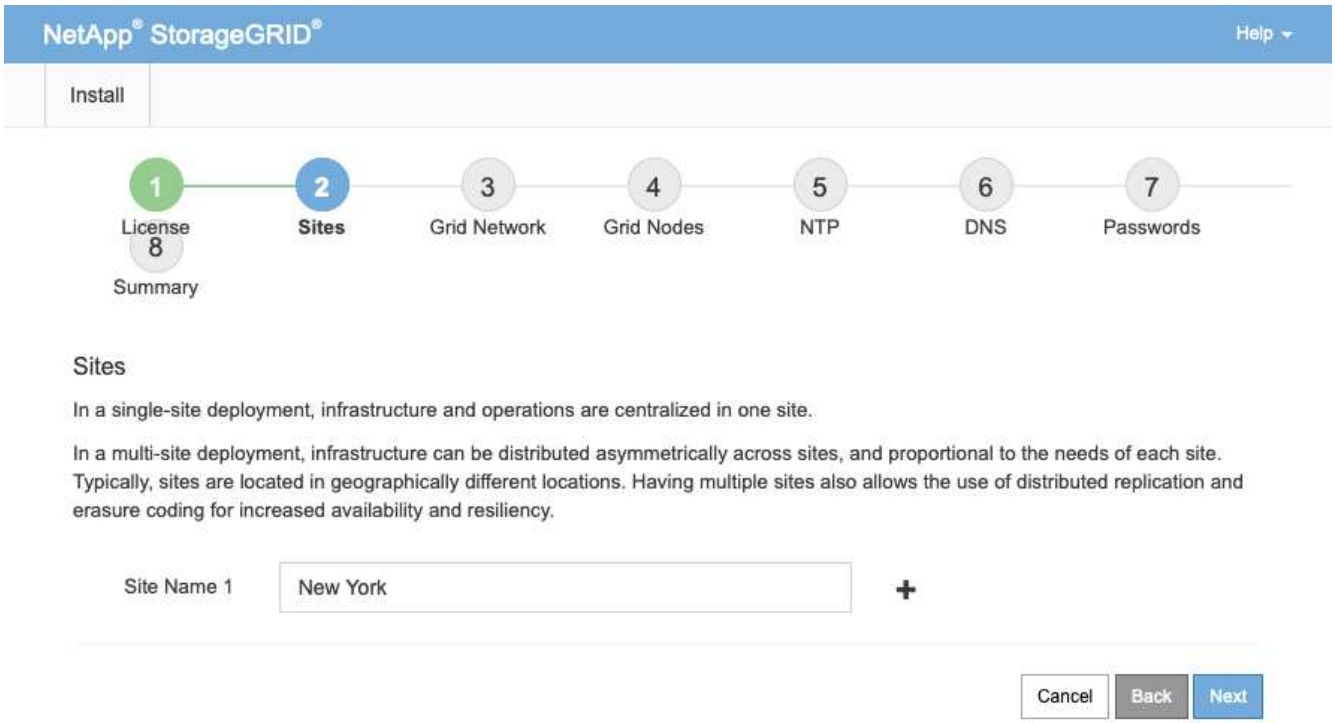
Saiba como adicionar sites ao StorageGRID para aumentar a confiabilidade e a capacidade de armazenamento.

Ao instalar o StorageGRID, você deve criar pelo menos um site. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de storage do seu sistema StorageGRID.

Para adicionar sites, execute as seguintes etapas:

**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 caixa de texto novo Nome do site. Adicione tantos locais adicionais quanto necessário para a topologia da grade. Você pode adicionar até 16 sites.




3. Clique em seguinte.

## Especifique sub-redes de rede de grade para StorageGRID

Saiba como configurar as sub-redes de rede de grade para StorageGRID.

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

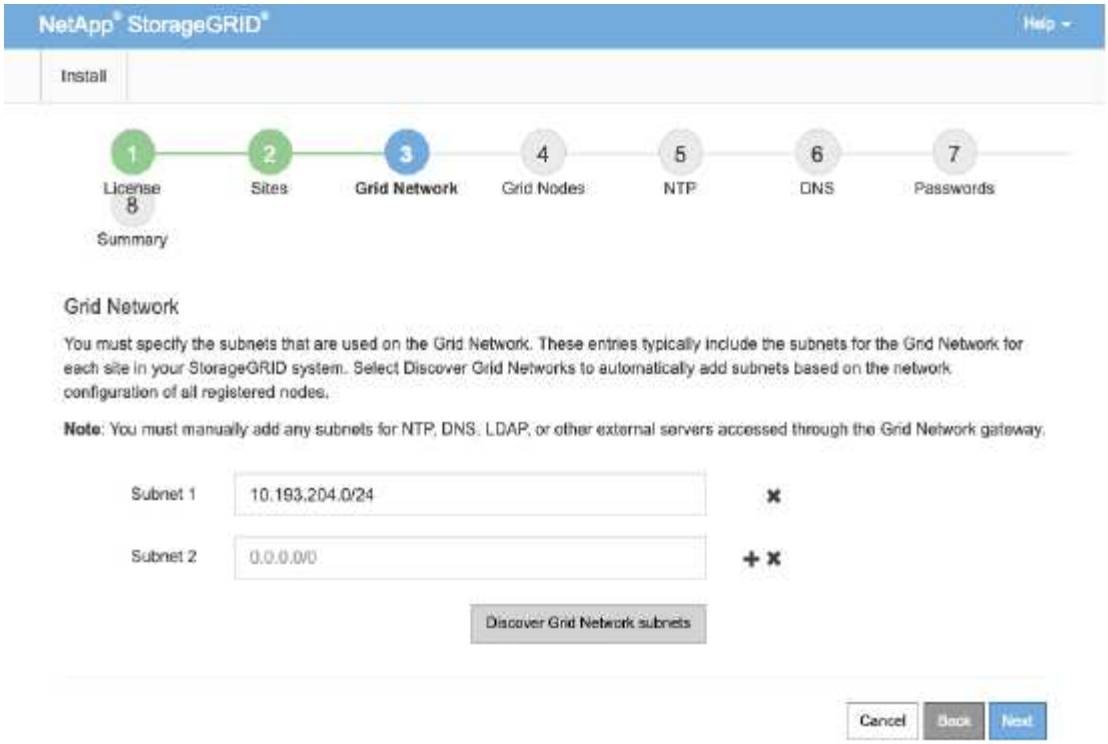
As entradas de sub-rede incluem as sub-redes para a rede de grade para cada site em seu sistema StorageGRID, além de quaisquer sub-redes que devem ser acessíveis através da rede de grade (por exemplo, as sub-redes que hospedam seus servidores NTP).

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.

Para especificar sub-redes de rede de grade, execute as seguintes etapas:

**Passos**

1. Na caixa de texto Subnet 1 , especifique o endereço de rede CIDR para pelo menos uma rede de grade.
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.

## Aprovar nós de grade para StorageGRID

Saiba como analisar e aprovar quaisquer nós de grade pendentes que se juntem ao sistema StorageGRID.

Você deve aprovar cada nó de grade antes que ele se junte ao sistema StorageGRID.

> Antes de começar, todos os nós de grade de dispositivos virtuais e StorageGRID devem ser implantados.

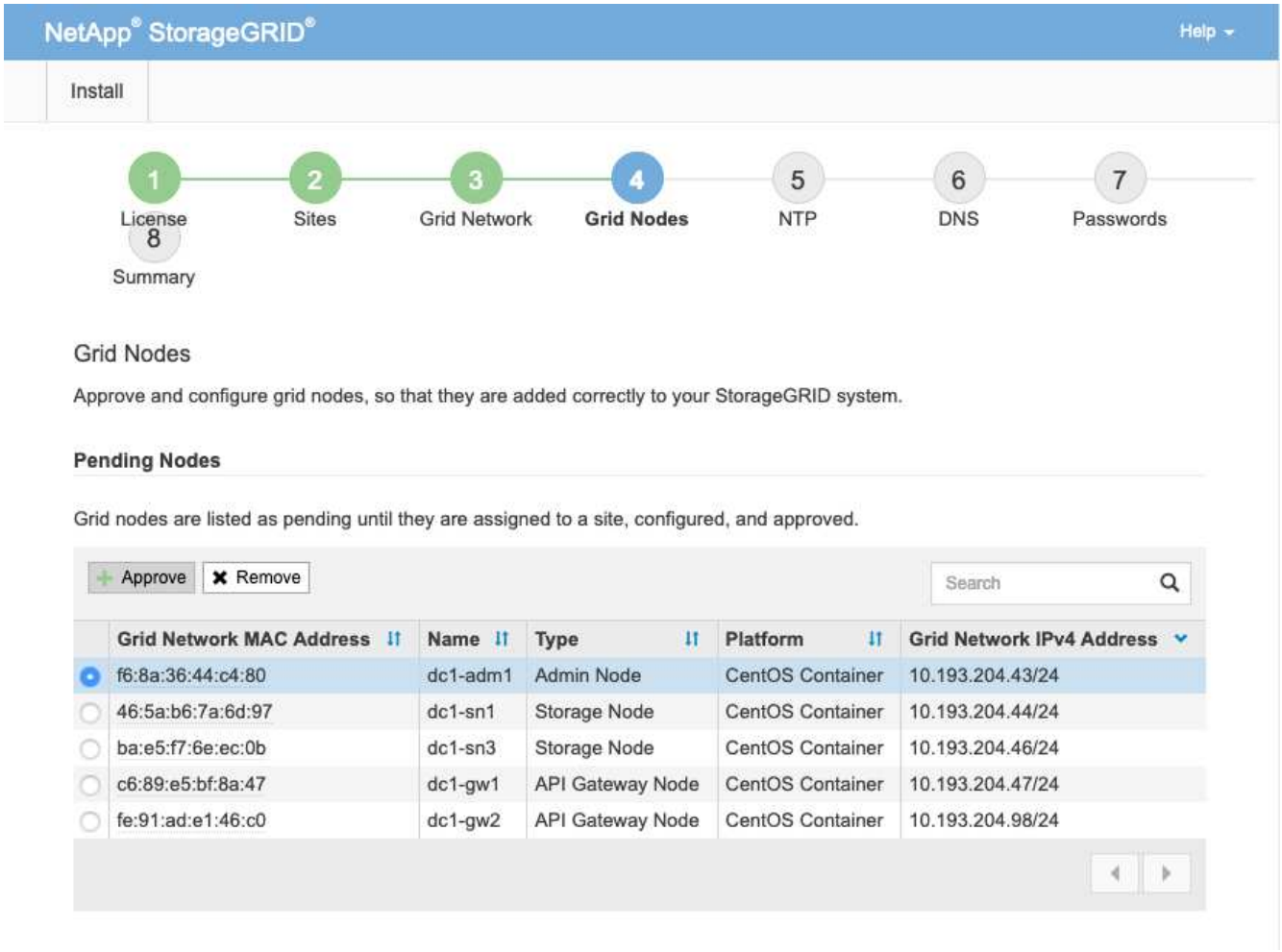
Para aprovar nós de grade pendentes, execute as seguintes etapas:

**Passos**

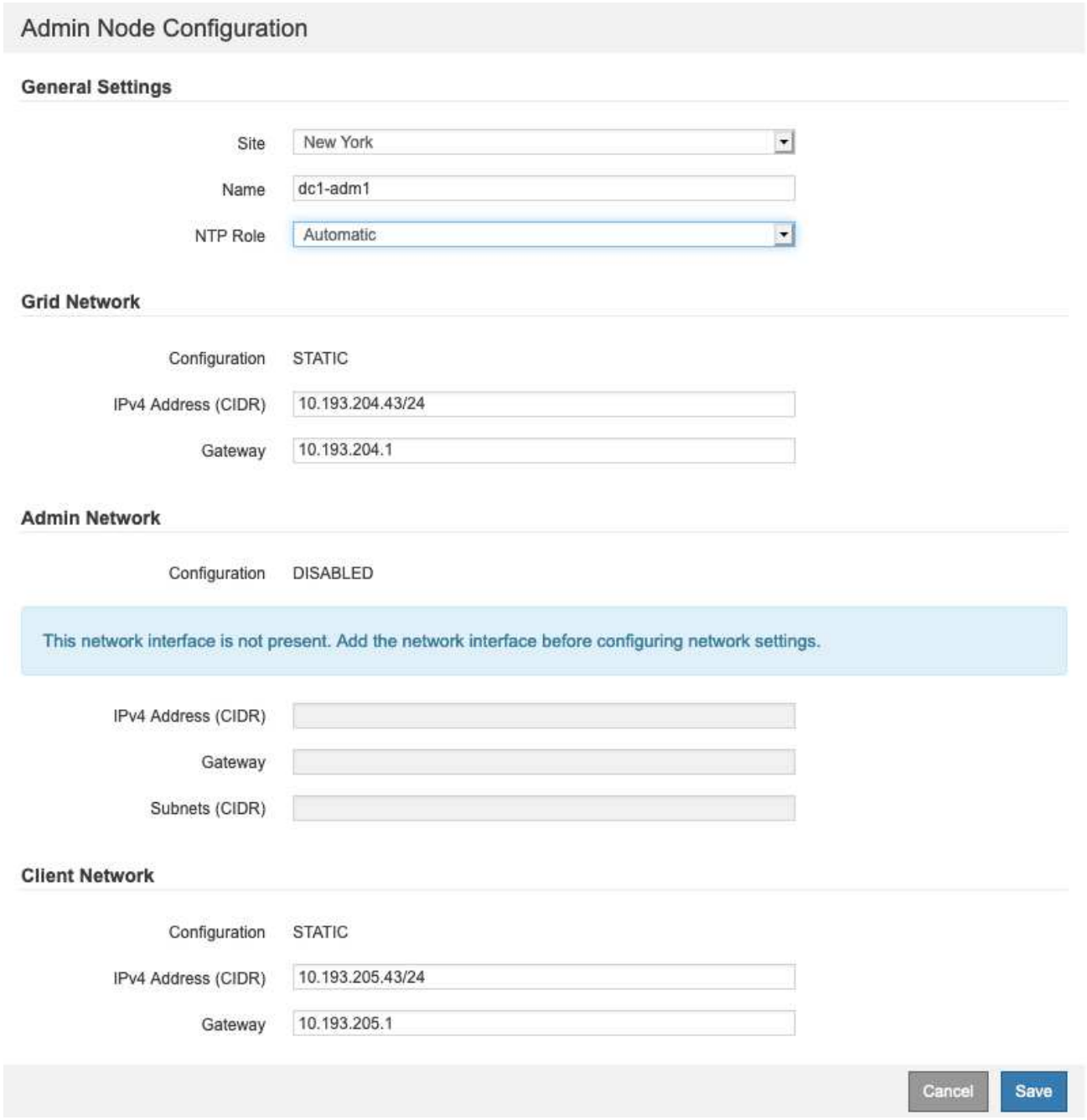
1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

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

2. Clique no botão de opção ao lado de um nó pendente que você deseja aprovar.




3. Clique em aprovar.
4. Em Configurações gerais, modifique as configurações para as seguintes propriedades, conforme necessário.




— **Site**: O nome do sistema do site para este nó de grade.

— **Nome**: O nome do host que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade. O nome padrão é o nome especificado durante a implantação do nó, mas você pode alterar o nome conforme necessário.

— **função NTP**: A função NTP do nó de grade. As opções são Automático, Principal e Cliente. A seleção da opção Automático atribui a função primária a nós de administração, nós de armazenamento com serviços de controlador de domínio administrativo (ADC), nós de gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós de grade recebem a função de 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.

— **Serviço ADC (somente nós de storage)**: Selecione Automático para permitir que o sistema determine se o nó requer o serviço 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 de rede de grade (eth0 dentro do contentor). Por exemplo, `192.168.1.234/24`.

— **Gateway**: O gateway de rede de grade. Por exemplo, `192.168.0.1`.

Se houver várias sub-redes de grade, o gateway é necessário.

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. Certifique-se de que o endereço IP resultante não esteja em um pool de endereços DHCP.

6. Para configurar a rede de administração para o nó de grade, adicione ou atualize as configurações na seção 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 de administração, o gateway de administração é necessário.

Se você selecionou DHCP para a configuração da rede de administração e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Certifique-se de que o endereço IP resultante não esteja em 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:

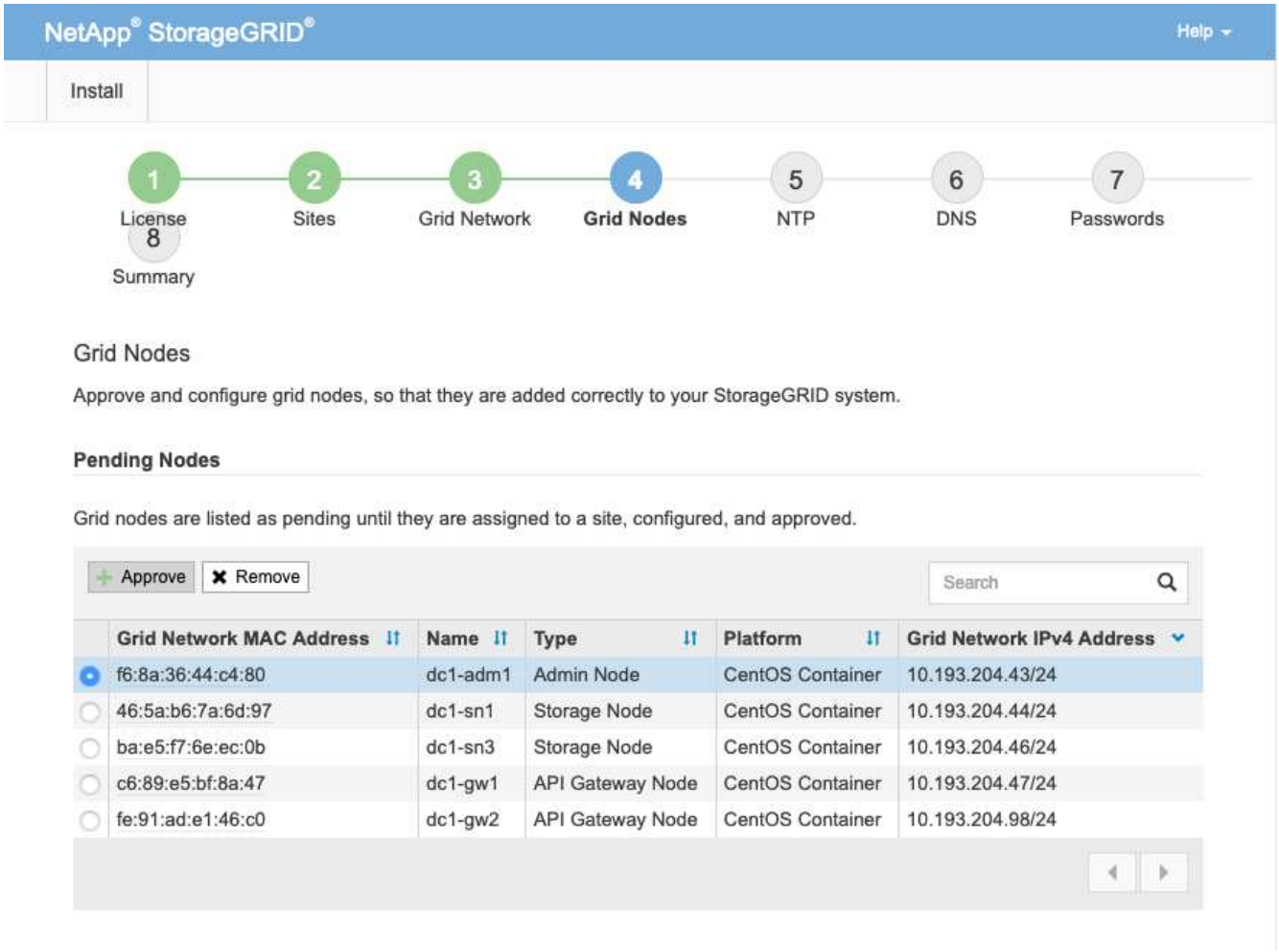
a. Reinicie o aparelho: No Instalador de aparelhos, selecione **Avançado › Reboot**. A reinicialização pode levar vários minutos.
b. Selecione **Configurar rede › Link Configuration** e ative as redes apropriadas.
c. Selecione **Configurar rede › Configuração IP** e configure as redes ativadas.
d. Volte à página inicial e clique em Iniciar instalação.
e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, 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.

   **Appliances**: Para um appliance StorageGRID, se a rede cliente não tiver sido configurada durante a instalação inicial usando o Instalador de dispositivos 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 aparelhos, selecione **Avançado › Reboot**. A reinicialização pode levar vários minutos.
   b. Selecione **Configurar rede › Link Configuration** e ative as redes apropriadas.
   c. Selecione **Configurar rede › Configuração IP** e configure as redes ativadas.
   d. Volte à página inicial e clique em Iniciar instalação.
   e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, 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 Guardar. A entrada do nó de grade se move para a lista de nós aprovados.



9. Repita as etapas 1-8 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. Para modificar as propriedades de um nó de grade aprovado, clique no botão de opção e clique em Editar.

10. Quando terminar de aprovar nós de grade, clique em Avançar.

## Especifique os detalhes do servidor NTP para o StorageGRID

Saiba como especificar as informações de configuração do NTP para o seu sistema StorageGRID para que as operações realizadas em servidores separados possam ser mantidas sincronizadas.

Para evitar problemas com o desvio de tempo, você deve especificar quatro referências externas de servidor NTP do estrato 3 ou superior.

> 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 exigentes como o StorageGRID.

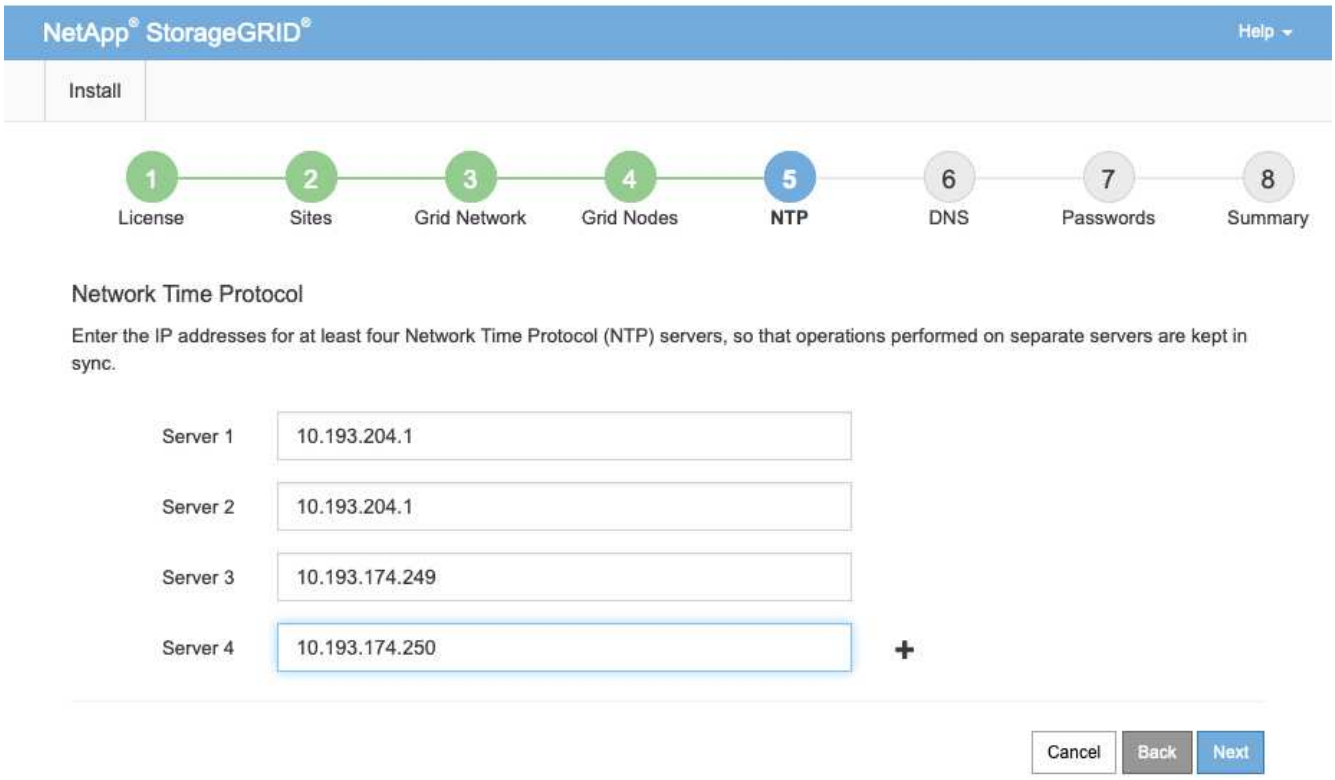
Os servidores NTP externos são usados pelos nós aos quais você atribuiu anteriormente as funções NTP principais.

> A rede do cliente não está ativada cedo o suficiente no processo de instalação para ser a única fonte de servidores NTP. Certifique-se de que pelo menos um servidor NTP pode ser alcançado através da rede de grade ou da rede de administração.

Para especificar informações do servidor NTP, execute as seguintes etapas:

**Passos**

1. Nas caixas de texto Server 1 to Server 4, especifique os endereços IP para pelo menos quatro servidores NTP.
2. Se necessário, clique no sinal de adição ao lado da última entrada para adicionar mais entradas de servidor.




3. Clique em seguinte.

## Especifique os detalhes do servidor DNS para o StorageGRID

Saiba como configurar o servidor DNS para StorageGRID.

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

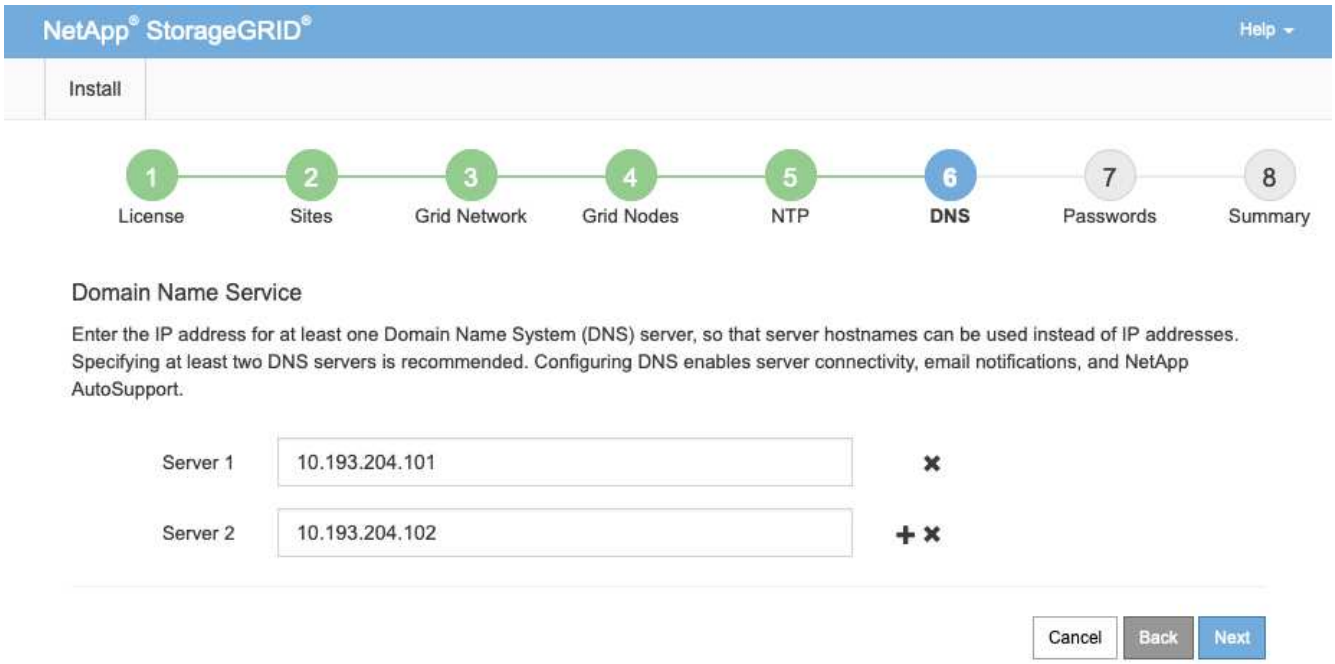
Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificado (FQDN) em vez de endereços IP para notificações de e-mail e mensagens NetApp AutoSupport. A NetApp recomenda especificar pelo menos dois servidores DNS.

> Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada.

Para especificar informações do servidor DNS, execute as seguintes etapas:

**Passos**

1. Na caixa de texto Server 1, especifique o endereço IP de um servidor DNS.
2. Se necessário, clique no sinal de adição ao lado da última entrada para adicionar mais servidores.




3. Clique em seguinte.

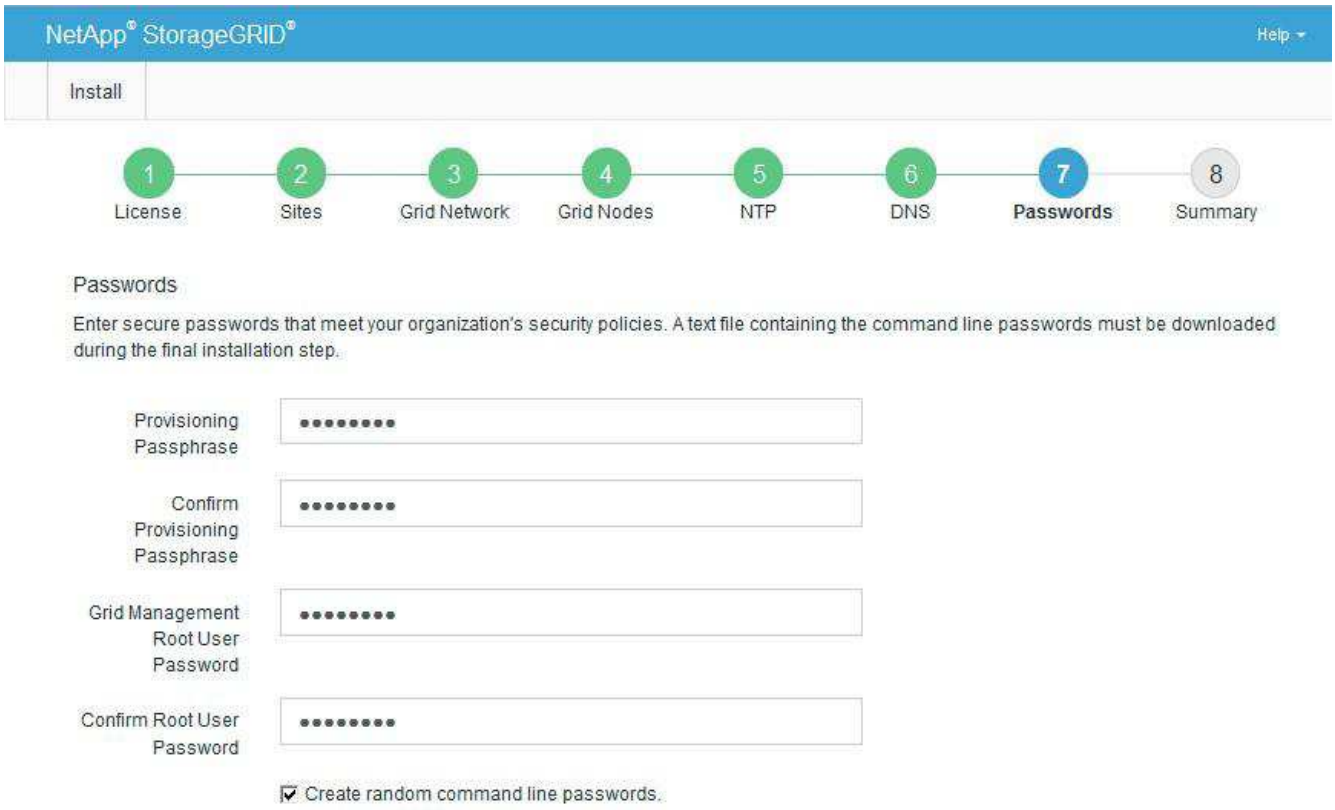
## Especifique as senhas do sistema para o StorageGRID

Saiba como proteger seu sistema StorageGRID definindo a senha de provisionamento e a senha de usuário raiz de gerenciamento de grade.

Para inserir as senhas a serem usadas para proteger seu sistema StorageGRID, siga estas etapas:

**Passos**

1. Em frase-passe de aprovisionamento, introduza a frase-passe de aprovisionamento que será necessária para efetuar alterações à topologia de grelha do seu sistema StorageGRID. Você deve gravar essa senha em um lugar seguro.
2. Em Confirm Provisioning Passphrase (confirmar frase-passe de aprovisionamento), volte a introduzir a frase-passe
3. Na Senha de usuário raiz do Gerenciamento de Grade, insira a senha a ser usada para acessar o Gerenciador de Grade como usuário raiz.
4. Em Confirm root User Password (confirmar palavra-passe de utilizador raiz), introduza novamente a palavra-passe do Grid Manager




5. Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, desmarque a opção criar senhas de linha de comando aleatória.

   Para implantações de produção, senhas aleatórias devem sempre ser usadas por razões de segurança. Desmarque a opção criar senhas de linha de comando aleatória somente para grades de demonstração se você quiser usar senhas padrão para acessar nós de grade a partir da linha de comando usando a conta de root ou de administrador.

   > Quando você clica em Instalar na página Resumo, você será solicitado a baixar o arquivo do pacote de recuperação (`sgws-recovery-packageid-revision.zip`). Tem de transferir este ficheiro para concluir a instalação. As senhas para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

6. Clique em seguinte.

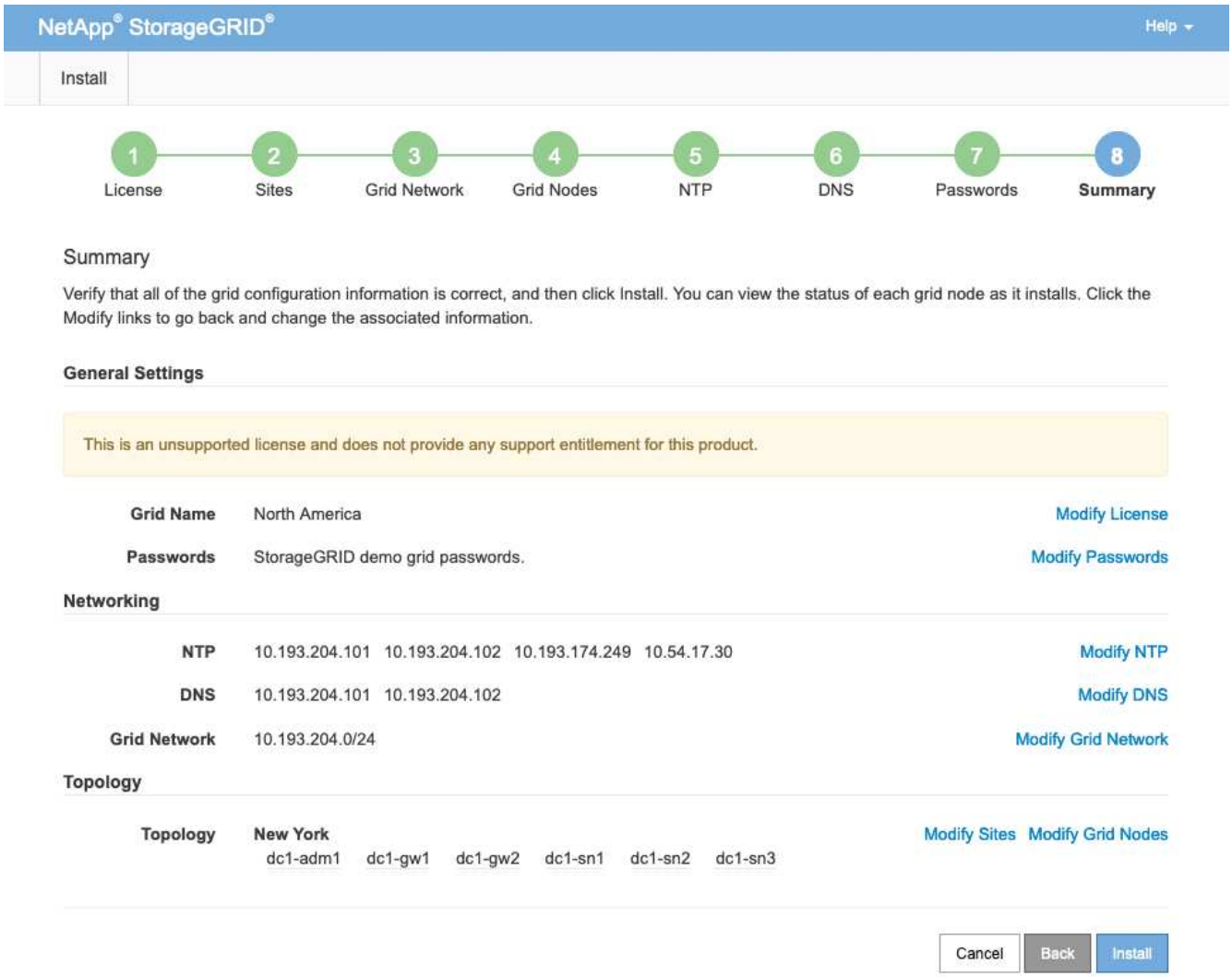
## Revise a configuração e conclua a instalação do StorageGRID

Saiba como validar as informações de configuração da grade e concluir o processo de instalação do StorageGRID.

Para se certificar de que a instalação foi concluída com êxito, reveja cuidadosamente as informações de configuração que introduziu. Siga estes passos.

**Passos**

1. Veja a página Resumo.




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 de grade para a rede do cliente quando você clica em Instalar. Se você perder a conetividade, certifique-se de que você está acessando o nó de administração principal por meio de uma sub-rede acessível. Para obter mais informações, consulte "Instalação e provisionamento de rede".

4. Clique em Download Recovery Package.

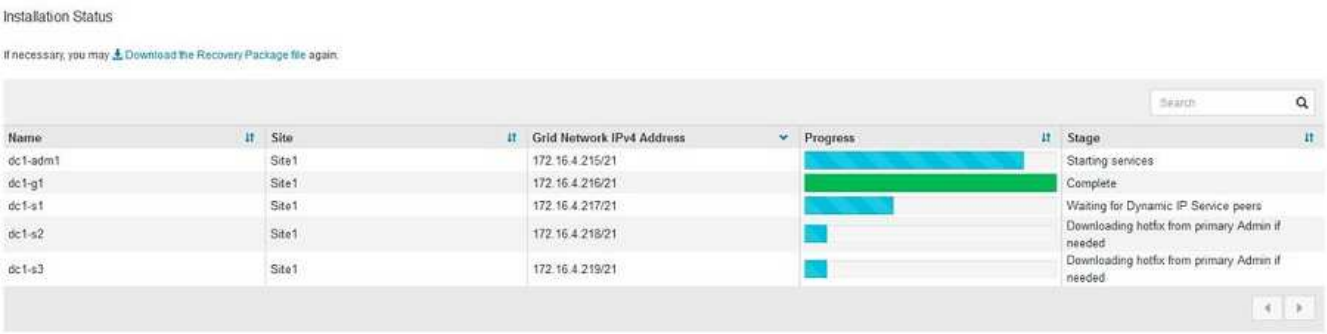
   Quando a instalação progride até o ponto em que a topologia da grade é definida, você será solicitado a baixar o arquivo do Pacote de recuperação (`.zip`) e confirmar que você pode acessar o conteúdo desse arquivo. Você deve baixar o arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID no caso de um ou mais nós de grade falharem.

   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.

5. Selecione a opção Eu fiz o download e verifiquei com êxito o arquivo do pacote de recuperação e clique em Avançar.


Se a instalação ainda estiver em andamento, a página Status da instalação será aberta. 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 será aberta.

6. Inicie sessão no Grid Manager como utilizador raiz com a palavra-passe especificada durante a instalação.

## Atualizar nós bare-metal no StorageGRID

Saiba mais sobre o processo de atualização para nós bare-metal no StorageGRID.

O processo de atualização para nós bare-metal é diferente do que para dispositivos ou nós VMware. Antes de executar uma atualização de um nó bare-metal, você deve primeiro atualizar os arquivos RPM em todos os hosts antes de executar a atualização através da GUI.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

Agora você pode prosseguir para a atualização de software através da GUI.

# TR-4907: Configure o StorageGRID com o veritas Enterprise Vault

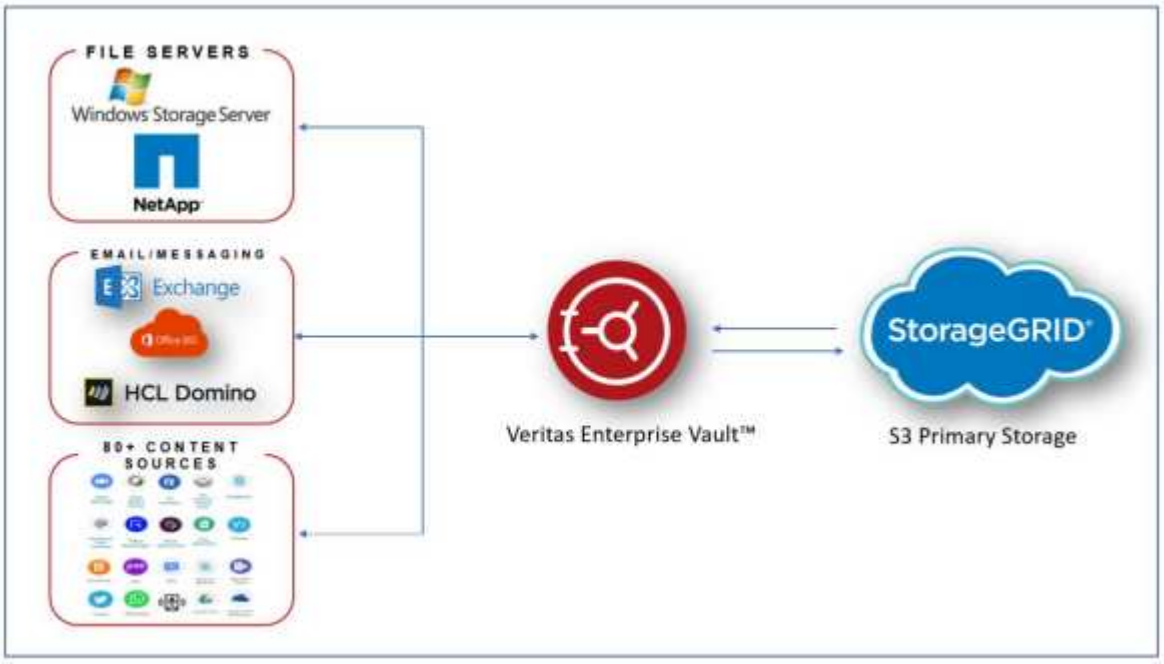
## Introdução à configuração do StorageGRID para failover de site

Saiba como o veritas Enterprise Vault usa o StorageGRID como um destino de armazenamento primário para recuperação de desastres.

Este guia de configuração fornece as etapas para configurar o NetApp StorageGRID como um destino de armazenamento primário com o veritas Enterprise Vault. Ele também descreve como configurar o StorageGRID para failover de local em um cenário de recuperação de desastres (DR).

### Arquitetura de referência

O StorageGRID fornece um destino de backup em nuvem compatível com S3 no local para o veritas Enterprise Vault. A figura a seguir ilustra a arquitetura do veritas Enterprise Vault e do StorageGRID.




### Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Centro de Documentação do NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Capacitação NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/

- Página de recursos da documentação do StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentação do produto NetApp https://www.netapp.com/support-and-training/documentation/

## Configure o StorageGRID e o veritas Enterprise Vault

Saiba como implementar configurações básicas para o StorageGRID 11,5 ou superior e o Veritas Enterprise Vault 14,1 ou superior.

Este guia de configuração é baseado no StorageGRID 11,5 e no Enterprise Vault 14,1. Para armazenamento em modo WORM (uma gravação, muitas leituras) usando o bloqueio de objetos S3, o StorageGRID 11,6 e o Enterprise Vault 14.2.2 foram usados. Para obter informações mais detalhadas sobre essas diretrizes, consulte a "Documentação do StorageGRID" página ou entre em Contato com um especialista da StorageGRID.

### Pré-requisitos para configurar o StorageGRID e o veritas Enterprise Vault

- Antes de configurar o StorageGRID com o veritas Enterprise Vault, verifique os seguintes pré-requisitos:

> Para storage WORM (bloqueio de objetos), é necessário StorageGRID 11,6 ou superior.

- o Veritas Enterprise Vault 14,1 ou posterior está instalado.

> Para storage WORM (Object Lock), é necessário o Enterprise Vault versão 14.2.2 ou superior.

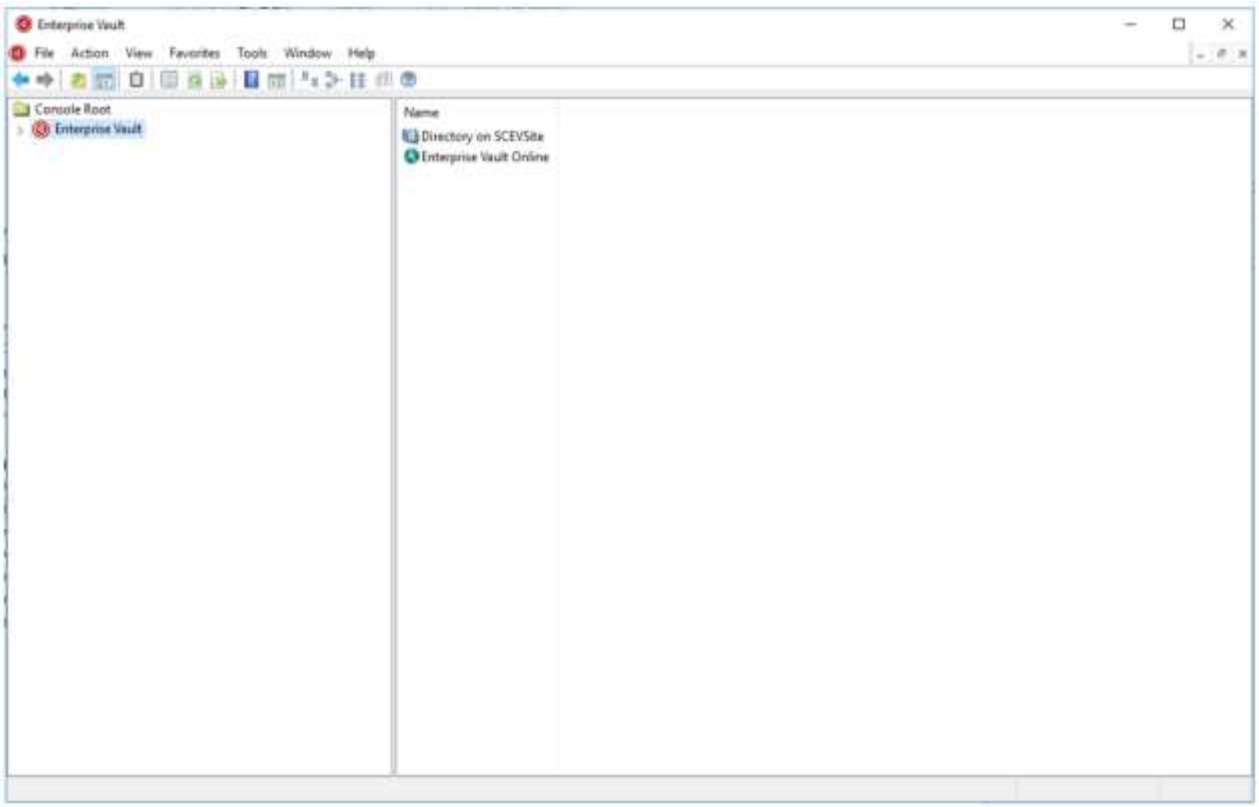
- Foram criados grupos de armazenamento de cofre e uma loja de cofre. Para obter mais informações, consulte o veritas Enterprise Vault Administration Guide.
- Um locatário, chave de acesso, chave secreta e bucket do StorageGRID foram criados.
- Foi criado um ponto de extremidade do balanceador de carga StorageGRID (HTTP ou HTTPS).
- Se estiver usando um certificado autoassinado, adicione o certificado de CA autoassinado do StorageGRID aos servidores de cofre empresarial. Para obter mais informações, consulte este "artigo da base de dados de Conhecimento da veritas".
- Atualize e aplique o arquivo de configuração mais recente do Enterprise Vault para habilitar soluções de armazenamento suportadas, como o NetApp StorageGRID. Para obter mais informações, consulte este "artigo da base de dados de Conhecimento da veritas".

### Configure o StorageGRID com o veritas Enterprise Vault

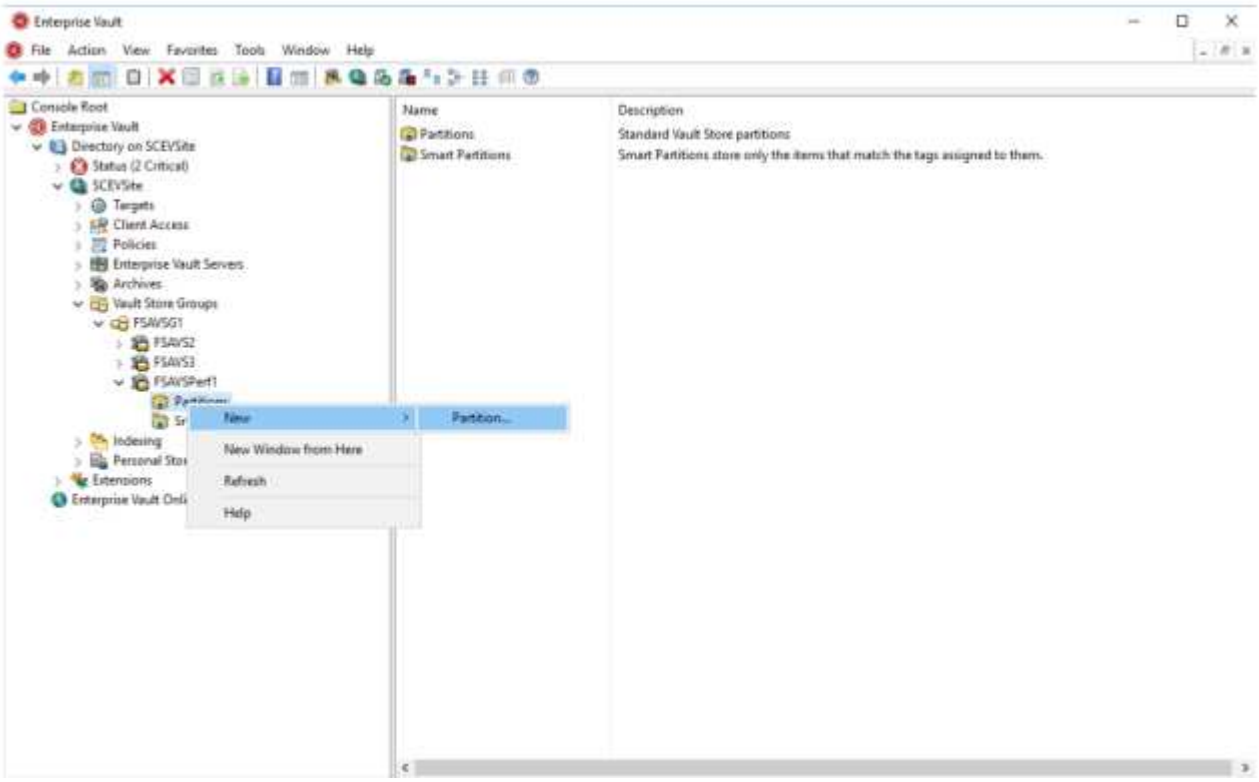
Para configurar o StorageGRID com o veritas Enterprise Vault, execute as seguintes etapas:

#### Passos

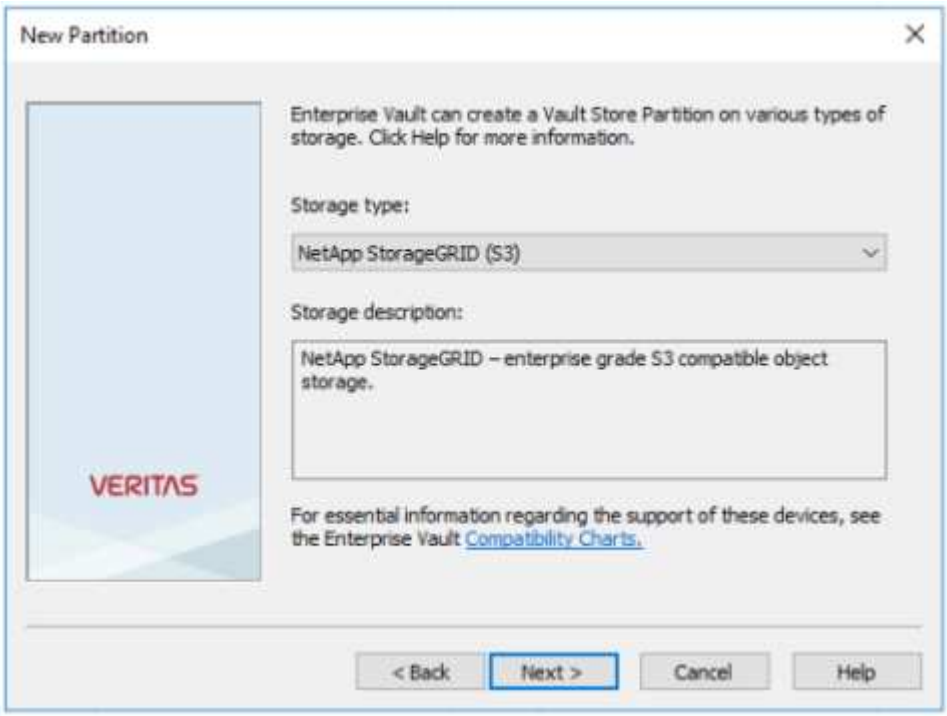
1. Inicie o console Enterprise Vault Administration.



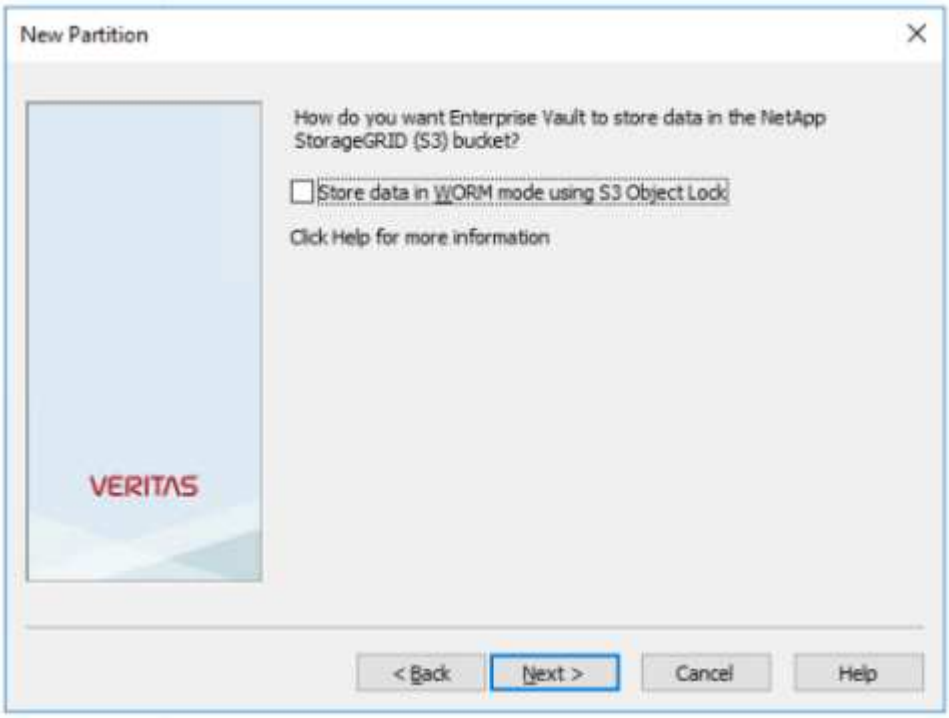

2. Crie uma nova partição de armazenamento do Vault no armazenamento apropriado do Vault. Expanda a pasta grupos do Vault Store e, em seguida, o armazenamento apropriado do Vault. Clique com o botão direito em partição e selecione **Nova › partição**.




3. Siga o assistente de criação de novas partições. No menu suspenso tipo de armazenamento, selecione NetApp StorageGRID (S3). Clique em seguinte.

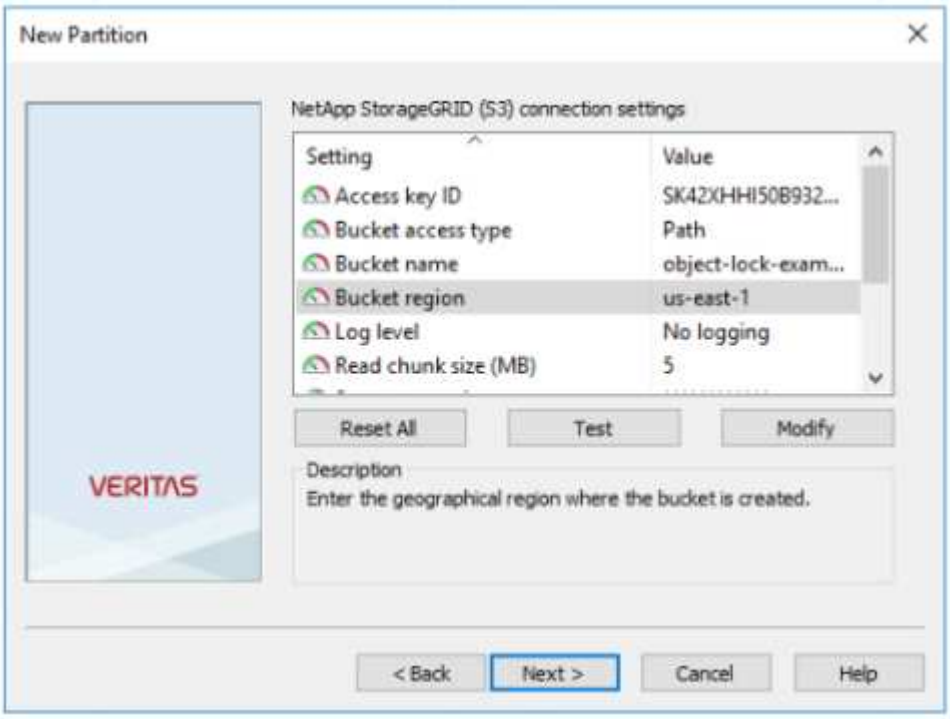



4. Deixe a opção armazenar dados no modo WORM usando S3 Object Lock desmarcada. Clique em seguinte.

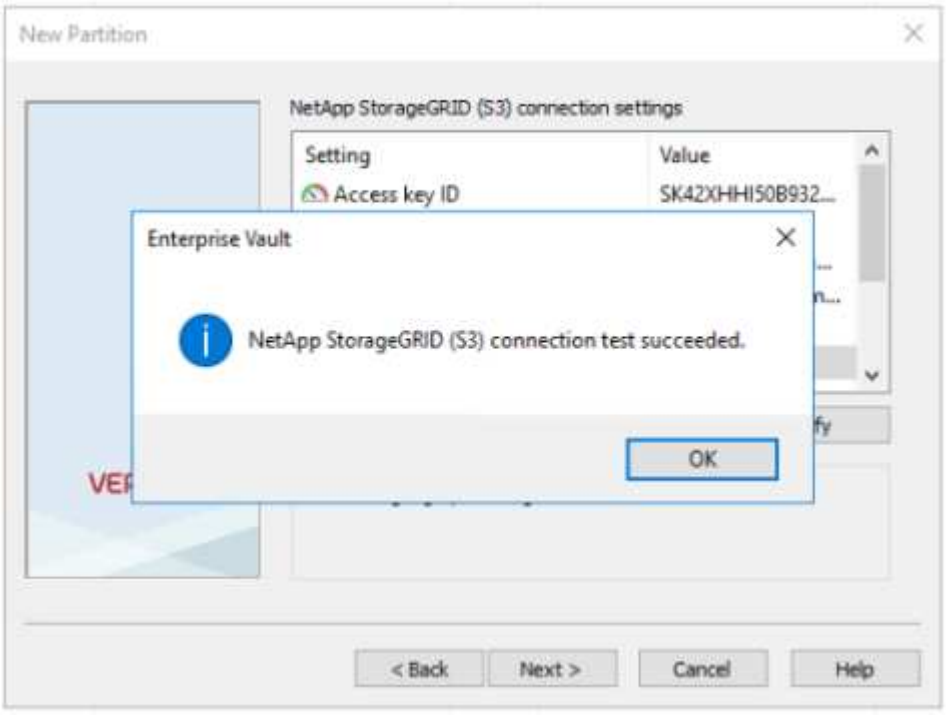



5. Na página de configurações de conexão, forneça as seguintes informações:
   - ID da chave de acesso
   - Chave de acesso secreto
   - Nome do host de serviço: Certifique-se de incluir a porta de endpoint do balanceador de carga (LBE) configurada no StorageGRID (como <a href="https://<hostname>:<LBE_port&gt" class="bare">https://<hostname>:<LBE_port&gt</a>;)

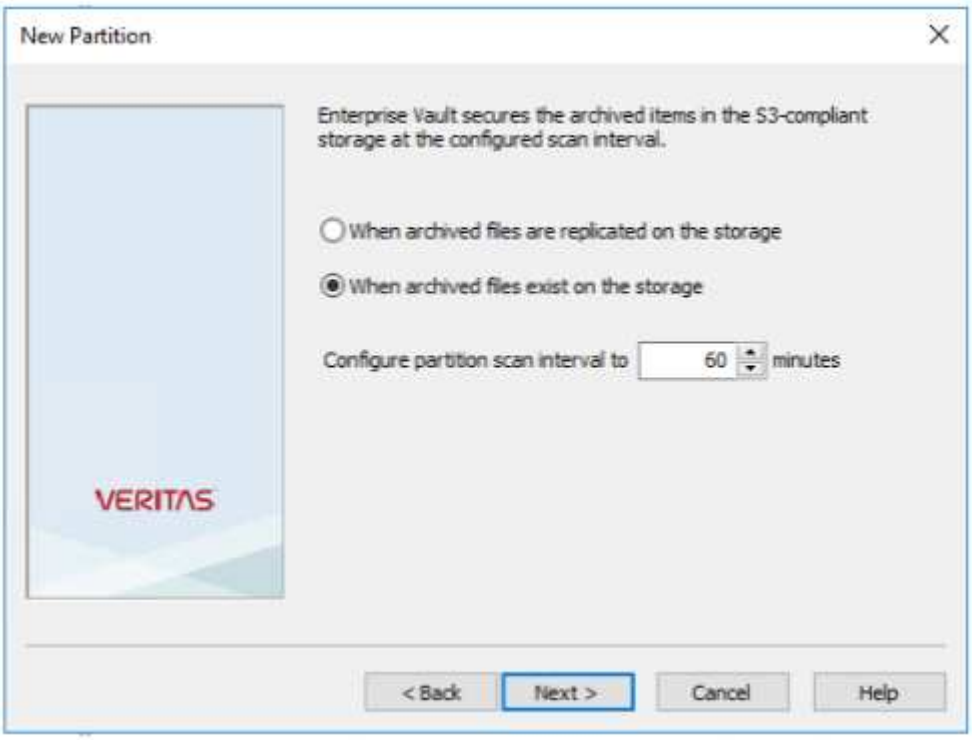
- Nome do bucket: Nome do bucket de destino pré-criado. o veritas Enterprise Vault não cria o bucket.
- Região do balde: `us-east-1` É o valor predefinido.



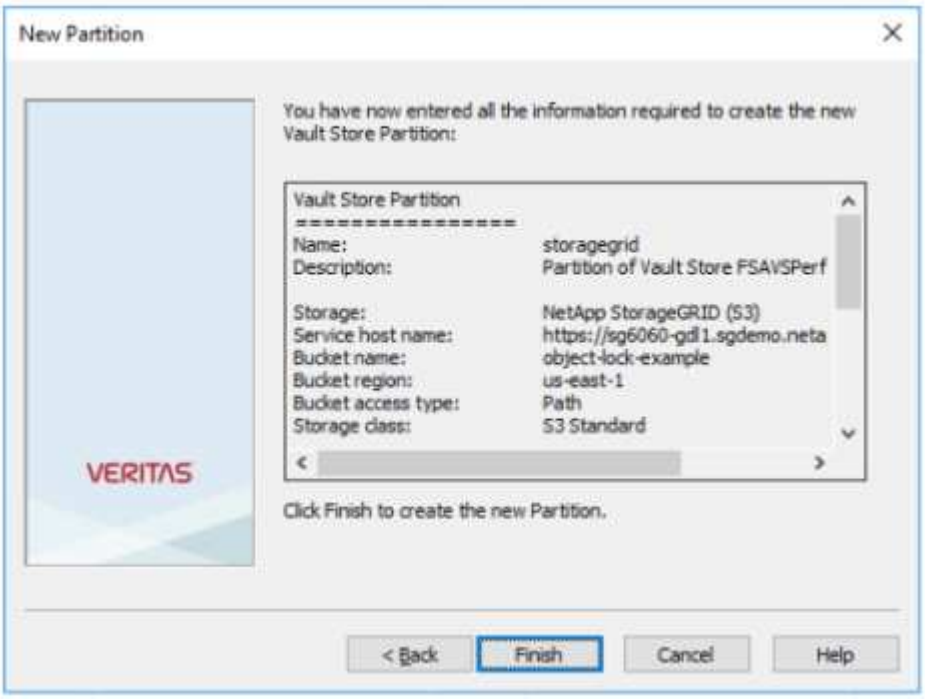

6. Para verificar a conexão com o bucket do StorageGRID, clique em testar. Verifique se o teste de conexão foi bem-sucedido. Clique em OK e em Avançar.



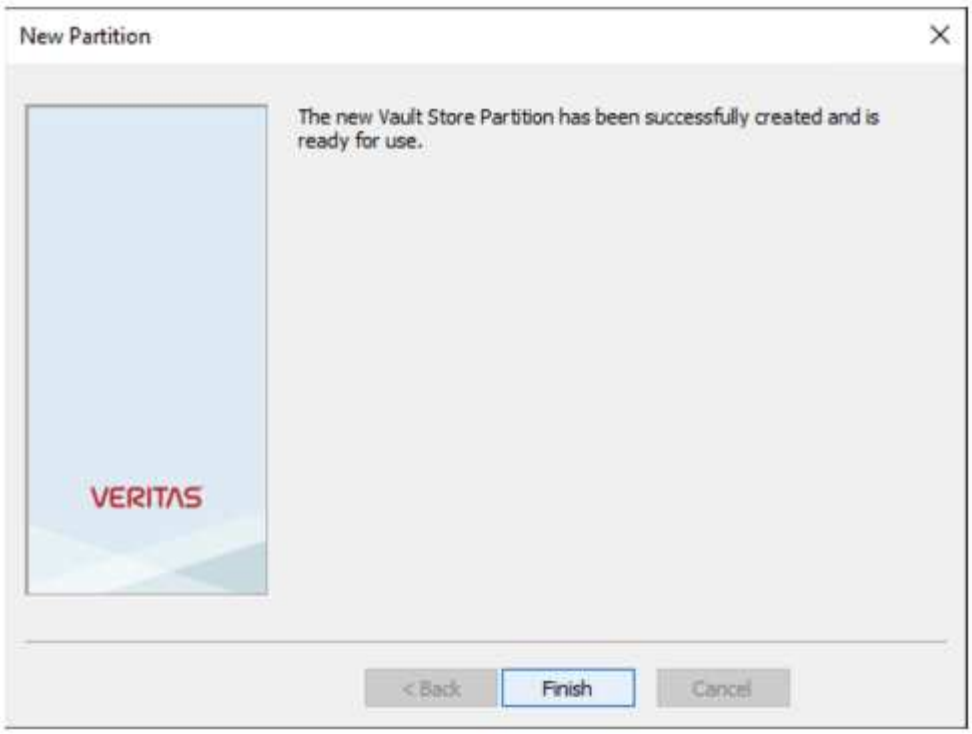

7. O StorageGRID não suporta o parâmetro de replicação S3. Para proteger seus objetos, o StorageGRID usa regras de gerenciamento do ciclo de vida das informações (ILM) para especificar esquemas de proteção de dados - várias cópias ou codificação de apagamento. Selecione a opção quando existirem ficheiros arquivados na opção armazenamento e clique em seguinte.




8. Verifique as informações na página de resumo e clique em concluir.




9. Depois que a nova partição de armazenamento do Vault tiver sido criada com sucesso, você pode arquivar, restaurar e pesquisar dados no Enterprise Vault com o StorageGRID como o armazenamento primário.




## Configurar o bloqueio de objetos StorageGRID S3 para storage WORM

Saiba como configurar o StorageGRID para armazenamento WORM usando o bloqueio de objetos S3.

### Pré-requisitos para configurar o StorageGRID para storage WORM

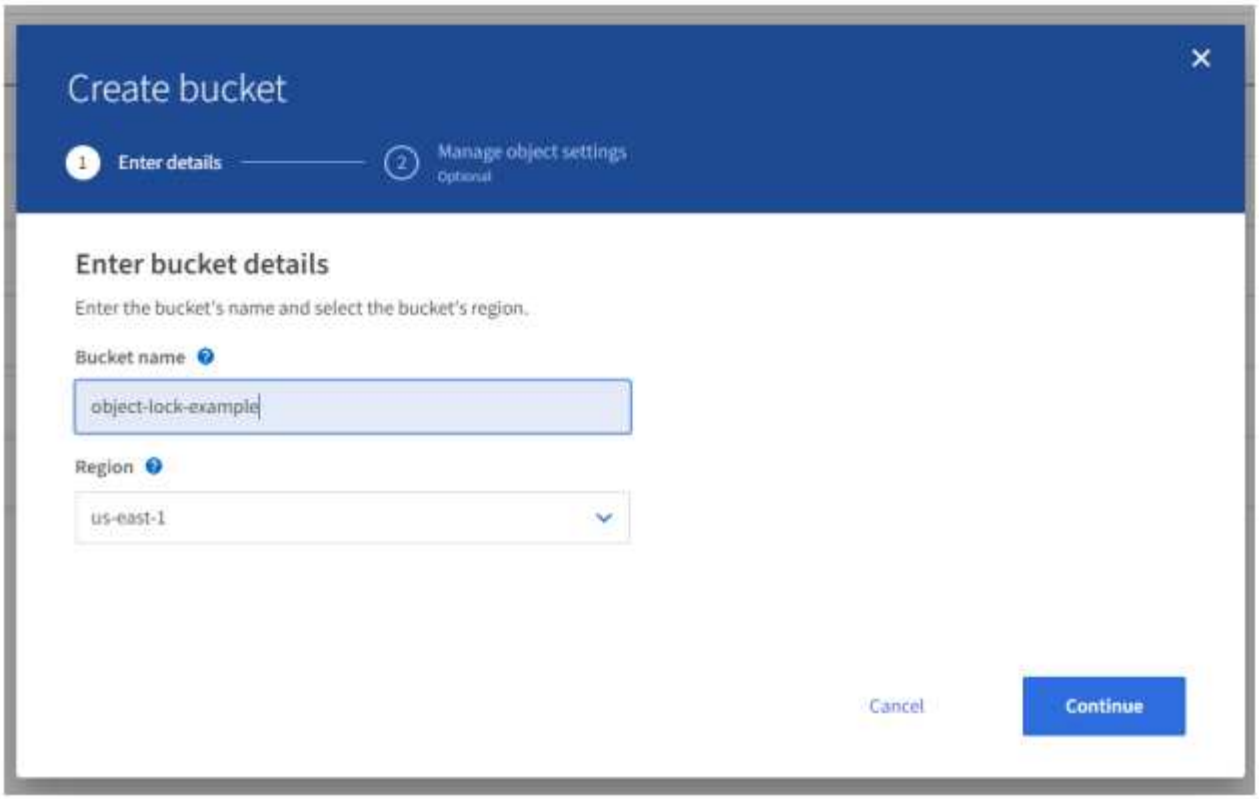
Para storage WORM, o StorageGRID usa o bloqueio de objetos S3 para reter objetos para conformidade. Isso requer o StorageGRID 11,6 ou superior, onde a retenção padrão do bucket do bloqueio de objetos S3 foi introduzida. O Enterprise Vault também requer a versão 14.2.2 ou superior.

### Configurar a retenção padrão do bucket do bloqueio de objetos do StorageGRID S3

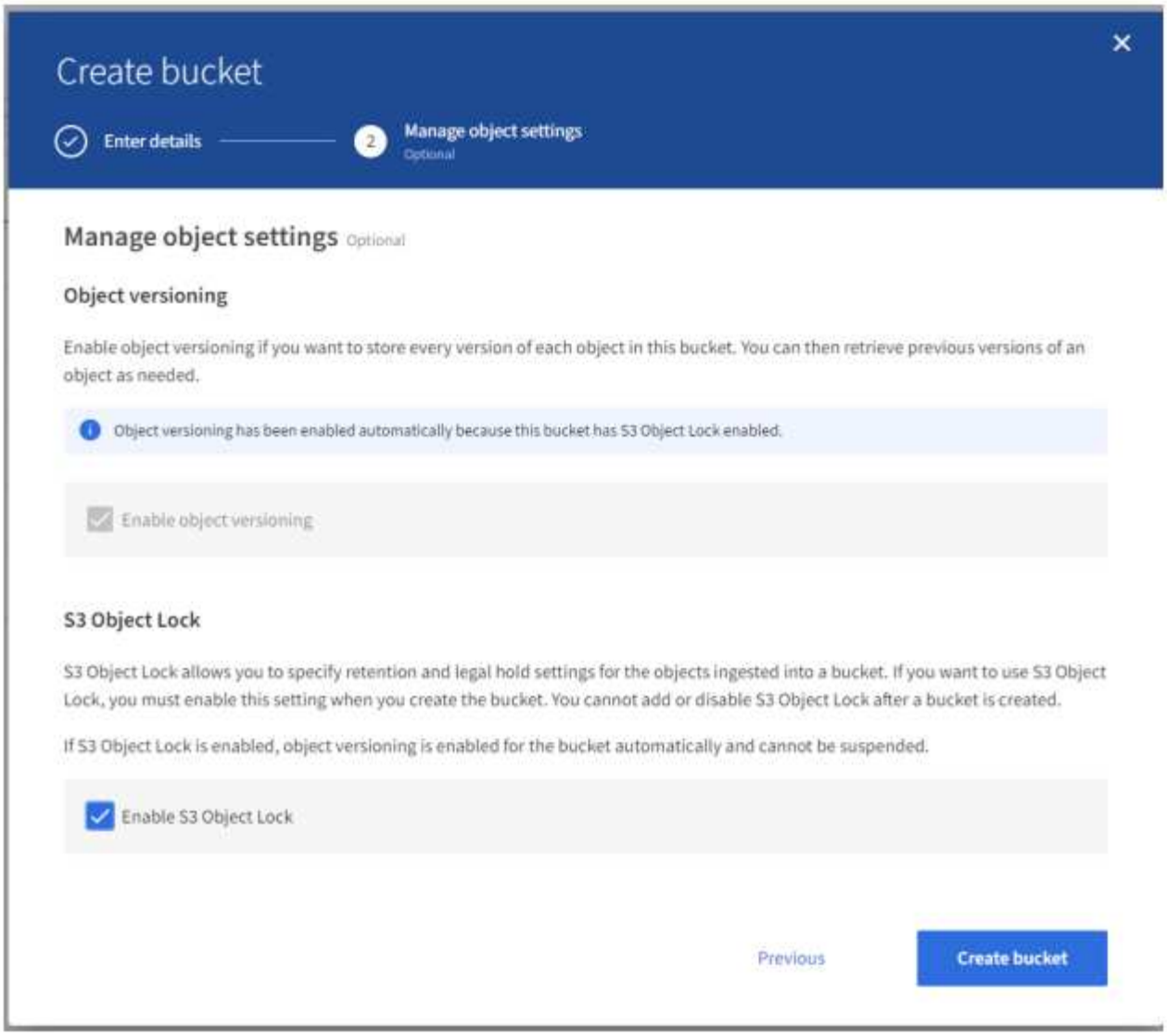
Para configurar a retenção padrão do bucket do bloqueio de objetos do StorageGRID S3, execute as seguintes etapas:

**Passos**

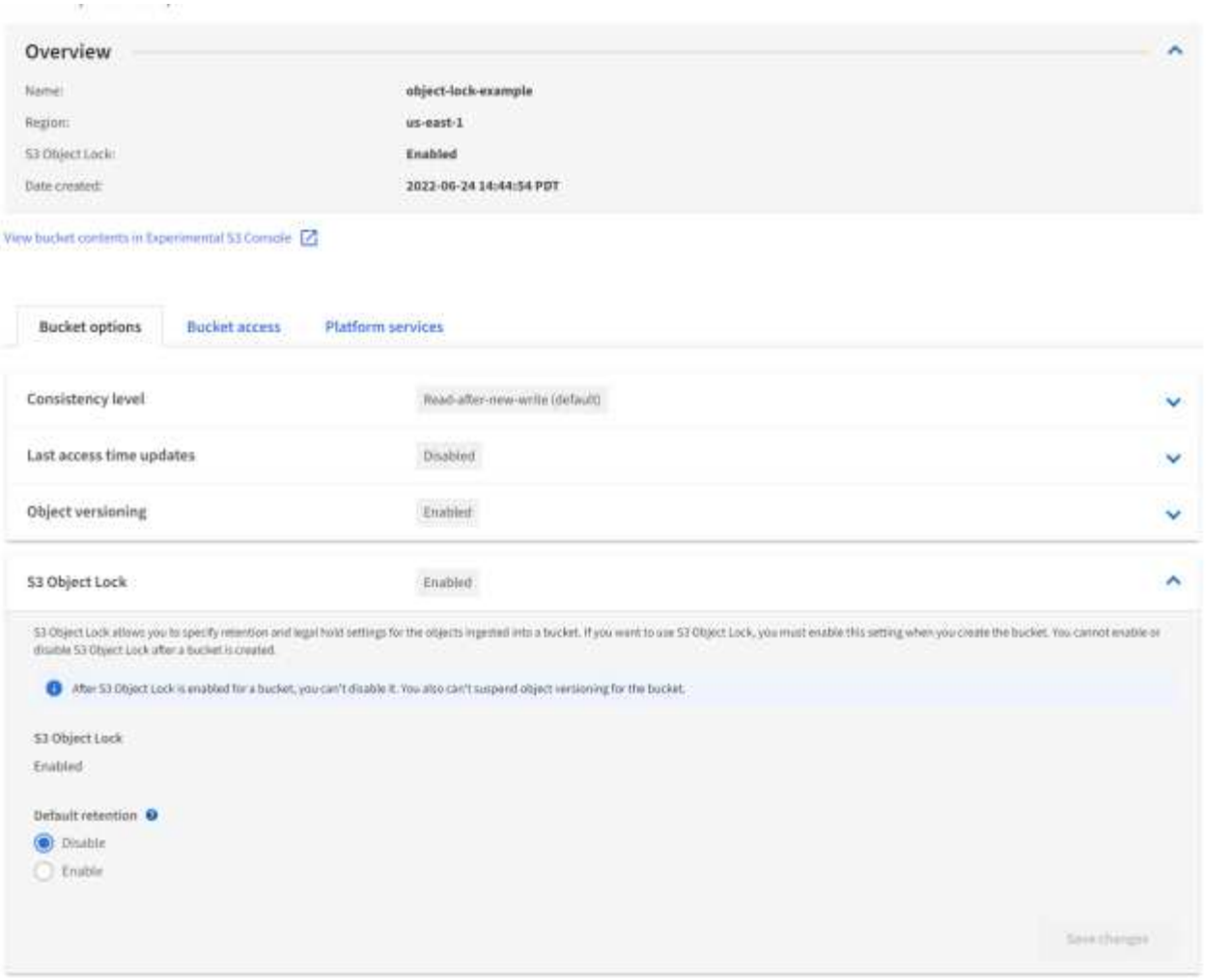
1. No Gerenciador do Locatário do StorageGRID, crie um bucket e clique em continuar



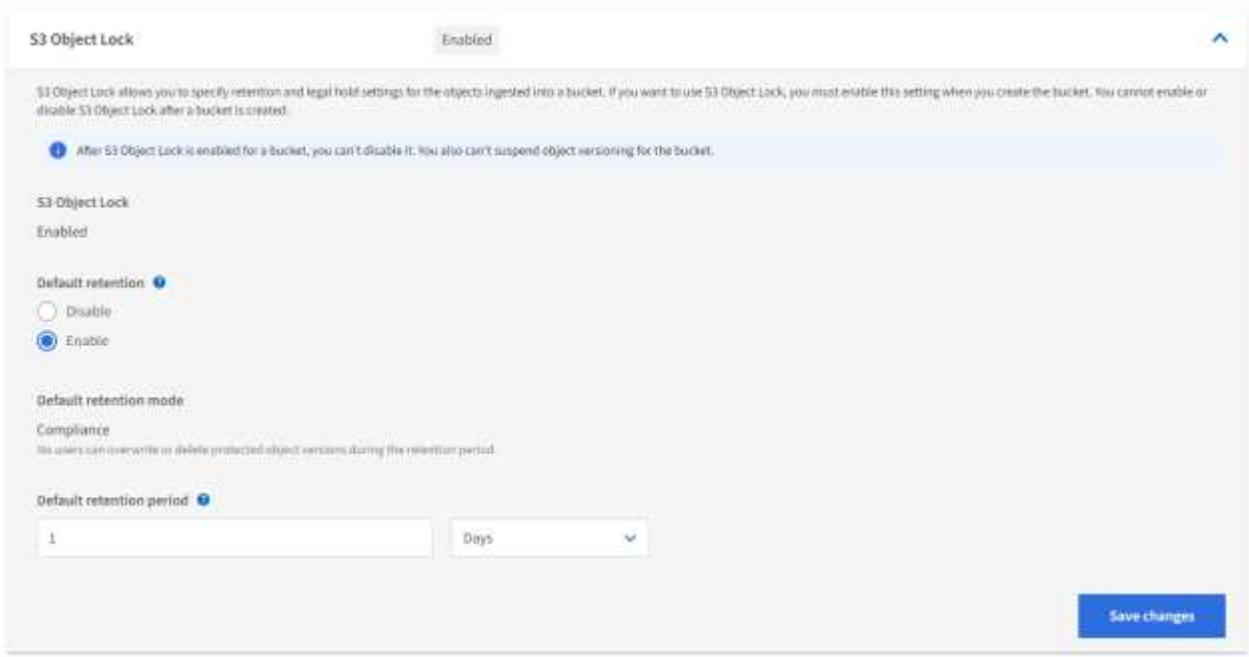

2. Selecione a opção Ativar bloqueio de objetos S3D e clique em criar balde.




3. Depois que o balde for criado, selecione o balde para visualizar as opções do balde. Expanda a opção suspensa S3 Object Lock.




4. Em retenção padrão, selecione Ativar e defina um período de retenção padrão de 1 dia. Clique em Salvar alterações.



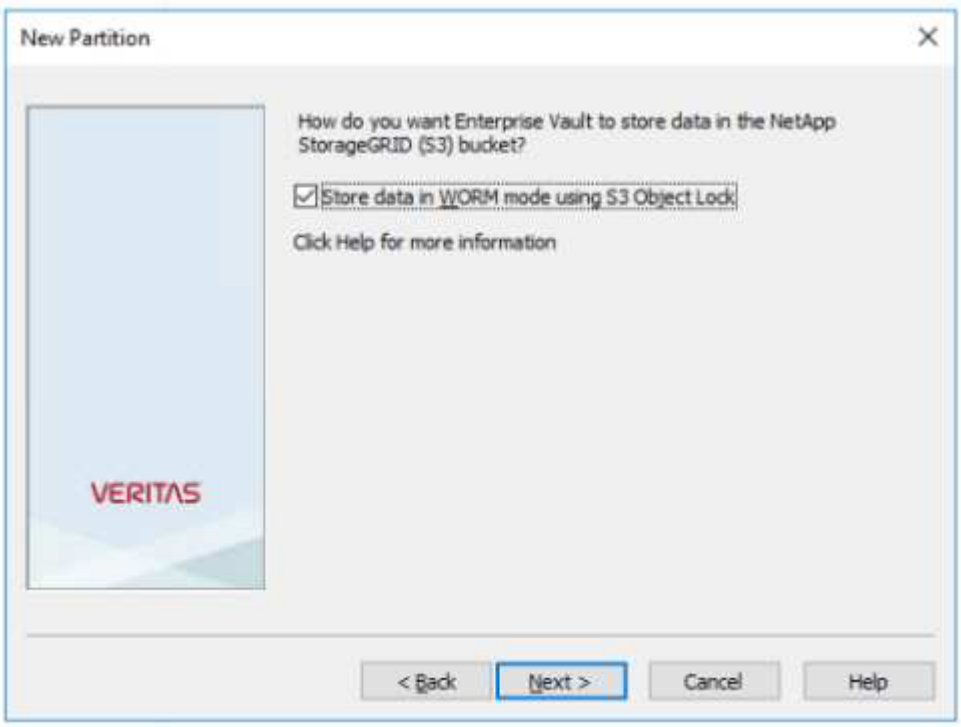
O bucket agora está pronto para ser usado pelo Enterprise Vault para armazenar dados WORM.

### Configure o Enterprise Vault

Para configurar o Enterprise Vault, execute as seguintes etapas:

**Passos**

1. Repita as etapas 1-3 na "Configuração básica" seção, mas desta vez selecione a opção armazenar dados no modo WORM usando o bloqueio de objeto S3. Clique em seguinte.




2. Ao inserir as configurações de conexão do bucket S3, verifique se você está inserindo o nome de um bucket S3 que tem a retenção padrão do bloqueio de objetos S3 ativada.
3. Teste a conexão para verificar as configurações.

## Configurar o failover de local do StorageGRID para recuperação de desastres

Saiba como configurar o failover de site do StorageGRID em um cenário de recuperação de desastres.

É comum que uma implantação de arquitetura StorageGRID seja multisite. Os locais podem ser ativo-ativo ou ativo-passivo para DR. Em um cenário de DR, certifique-se de que o veritas Enterprise Vault possa manter a conexão com seu storage primário (StorageGRID) e continuar a obter e obter dados durante uma falha no local. Esta seção fornece orientações de configuração de alto nível para uma implantação ativa-passiva de dois locais. Para obter informações detalhadas sobre essas diretrizes, consulte a "Documentação do StorageGRID" página ou entre em Contato com um especialista da StorageGRID.

### Pré-requisitos para configurar o StorageGRID com o veritas Enterprise Vault

Antes de configurar o failover de site do StorageGRID, verifique os seguintes pré-requisitos:

- Há uma implantação de StorageGRID de dois locais; por exemplo, site1 e site2.
- Um nó de administrador executando o serviço de balanceador de carga ou um nó de gateway, em cada local, para balanceamento de carga foi criado.
- Um ponto de extremidade do balanceador de carga StorageGRID foi criado.

### Configurar failover de site do StorageGRID

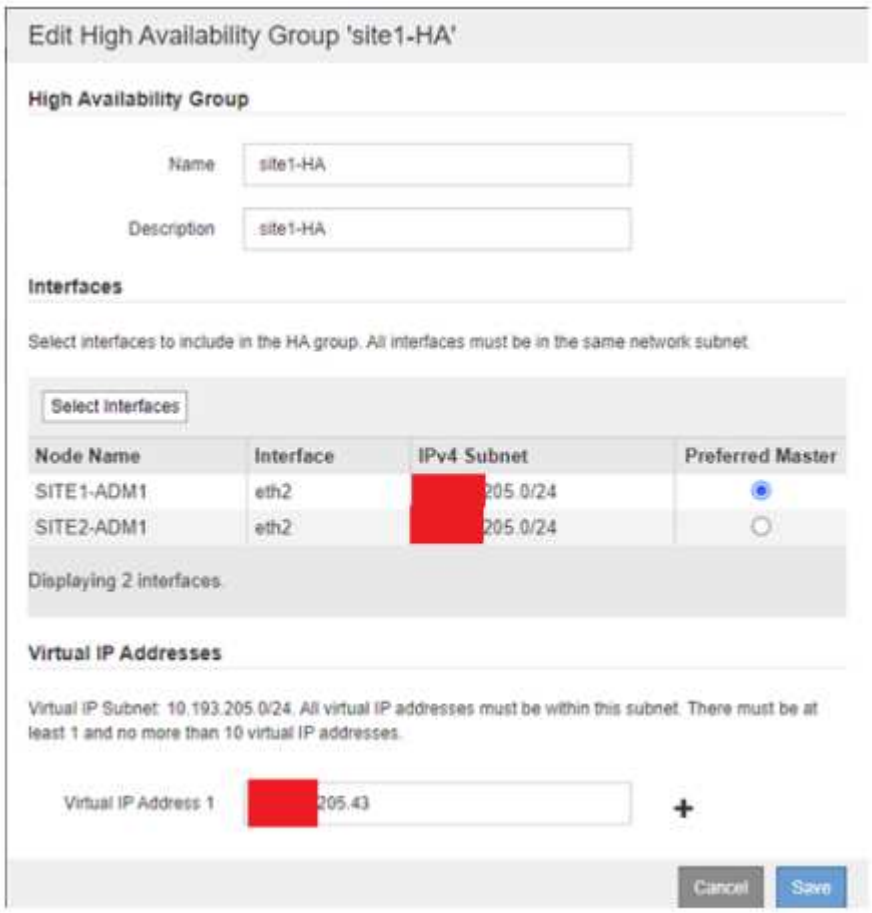
Para configurar o failover do site do StorageGRID, execute as seguintes etapas:

**Passos**

1. Para garantir a conetividade com o StorageGRID durante falhas no local, configure um grupo de alta disponibilidade (HA). Na interface do Gerenciador de Grade do StorageGRID (GMI), clique em Configuração, grupos de alta disponibilidade e criar.

   [perguntas/veritas-create-high-availability-group]

2. Introduza as informações necessárias. Clique em Selecionar interfaces e inclua as interfaces de rede DO site1 e DO site2 em que O site1 (o site principal) é o mestre preferido. Atribua um endereço IP virtual dentro da mesma sub-rede. Clique em Guardar.

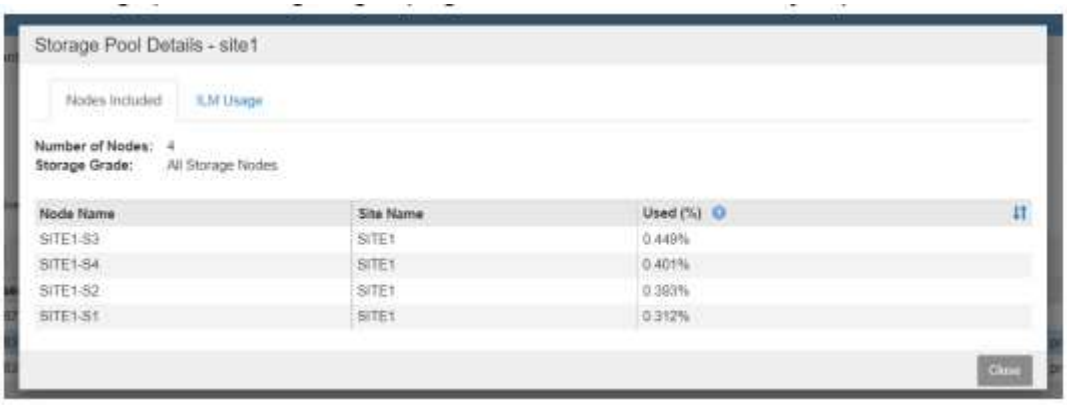


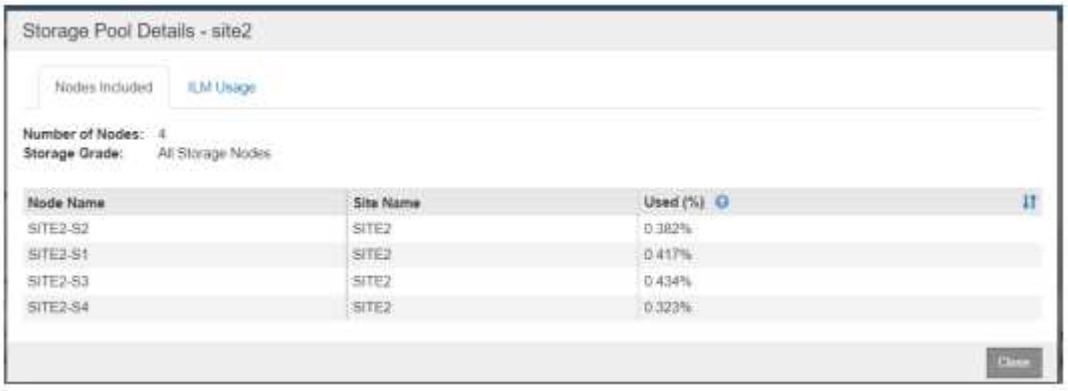

3. Esse endereço IP virtual (VIP) deve ser associado ao nome de host S3 usado durante a configuração de partição do veritas Enterprise Vault. O endereço VIP resolve o tráfego para O site1 e, durante A falha DO site1, o endereço VIP redireciona o tráfego para O site2 de forma transparente.
4. Certifique-se de que os dados sejam replicados para site1 e site2. Dessa forma, se O site1 falhar, os

dados do objeto ainda estarão disponíveis em site2. Isso é feito configurando primeiro os pools de armazenamento.

No StorageGRID GMI, clique em ILM, pools de armazenamento e, em seguida, crie. Siga o assistente para criar dois pools de armazenamento: Um para site1 e outro para site2.

Os pools de storage são agrupamentos lógicos de nós usados para definir o posicionamento do objeto




5. No StorageGRID GMI, clique em ILM, regras e, em seguida, criar. Siga o assistente para criar uma regra ILM especificando uma cópia a ser armazenada por local com um comportamento de ingestão de balanceado.

6. Adicione a regra ILM a uma política ILM e ative a política.

Esta configuração resulta no seguinte resultado:

- Um IP de endpoint virtual S3 onde site1 é o primário e site2 é o endpoint secundário. Se site1 falhar, o VIP

falhará para site2.

- Quando os dados arquivados são enviados do veritas Enterprise Vault, o StorageGRID garante que uma cópia seja armazenada NO site1 e que outra cópia DR seja armazenada no site2. Se O site1 falhar, o Enterprise Vault continuará a ingerir e recuperar do site2.

> Ambas as configurações são transparentes para o veritas Enterprise Vault. O endpoint S3, o nome do bucket, as chaves de acesso e assim por diante são os mesmos. Não há necessidade de reconfigurar as configurações de conexão S3 na partição veritas Enterprise Vault.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais