Soluções e recursos da StorageGRID

StorageGRID solutions and resources

NetApp
July 14, 2025

Índice

Soluções e recursos da StorageGRID

Passos para aceder ao software de avaliação StorageGRID

Esta instrução destina-se a vendas, parceiros e clientes potenciais da NetApp envolvidos com a NetApp.

Registre-se para uma conta

1. Registe-se para obter uma conta no "Site de suporte da NetApp" utilizando o e-mail da sua empresa.
   a. Certifique-se de que não iniciou sessão com a conta recém-criada.
   b. Se você já tiver uma conta, certifique-se de que não está conetado e prossiga com a próxima etapa.
2. Crie um caso de suporte não técnico para elevar os níveis de acesso ao "prospect". Para fazer isso, clique no ""Relatar um problema"link " no rodapé do site.
3. Selecione "problema de registo" como a categoria de feedback.
4. Na seção de comentários, escreva: "Meu endereço de e-mail da conta é *Your-Email-Address*. Gostaria de obter acesso a potenciais clientes para transferir o software de avaliação StorageGRID."
   a. Mencione o nome da pessoa interna do NetApp que sugeriu o pedido de acesso ao cliente potencial.

Baixar StorageGRID

1. Depois que seu caso de suporte for revisado e aprovado, o suporte da NetApp notificará você por e-mail de que sua conta recebeu acesso a clientes potenciais.
2. Faça download do "Software de avaliação StorageGRID".

O arquivo de licença Eval está localizado dentro do arquivo zip. Ele é o StorageGRID-Webscale-<version> NLF000000.txt uma vez descompactado.

Baixar o software é um processo que envolve medidas de conformidade comercial para aderir aos requisitos legais. Para garantir a conformidade, os usuários precisam criar uma conta e abrir um caso de suporte antes de obter acesso. Esse processo nos ajuda a manter o controle e a documentação adequados, ao mesmo tempo em que fornece aos clientes potenciais o software pronto para a produção de que precisam.

Nós fornecemos a versão "pronta para produção" do StorageGRID, que não é uma versão de código aberto ou alternativa. É importante notar que **o suporte não é fornecido** a menos que o cliente potencial atualize para uma licença de produção.

Por favor, entre em Contato com StorageGRID.NetApp.com para qualquer problema com os passos acima.

Soluções validadas de terceiros

Soluções validadas de terceiros: Visão geral

A NetApp, em colaboração com nossos parceiros, validou essas soluções para uso com a StorageGRID. Consulte as informações nesta seção para saber quais soluções foram validadas e obter instruções adicionais, se aplicável.

Junte-se à NetApp para acelerar a inovação do portfólio, expandir o reconhecimento do mercado e aumentar as vendas ao criar soluções NetApp testadas e da melhor categoria. "Torne-se um parceiro de aliança hoje".

O StorageGRID 11,9 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,9. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Alluxio
- Apache Kafka
- Ponto de montagem da AWS
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- Collibra (versão mínima de qualidade de dados do Collibra 2024,02)
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover dados
- Dremio
- Snapshot do Elasticsearch (incluindo camada congelada)
- EMAM
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet

- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data do Microsoft SQL Server
- Model9
- Modzy
- Moonwalk Universal
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Documentum 21,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- reveille V10 Build 220706 ou superior
- CDM da Rubrik
- s3a
- Signiant
- Floco de neve
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Starburst
- Arrumação fácil
- Trino
- Verniz Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e posterior
- Vertica 10.x
- Vidisine
- Virtalica StorageFabric
- WEKA v3,10 ou posterior

Soluções de terceiros validadas no StorageGRID com bloqueio de objeto

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Recurso CommVault 11 versão 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21,4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e posterior

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Principais gerentes suportados no StorageGRID

Essas soluções foram testadas.

- Entrust KeyControl 10,2
- Hashicorp Vault 1.15.0

- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9
- Thales CipherTrust Manager 2,10
- Thales CipherTrust Manager 2,11
- Thales CipherTrust Manager 2,12
- Thales CipherTrust Manager 2,13
- Thales CipherTrust Manager 2,14

O StorageGRID 11,8 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,8. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Alluxio
- Apache Kafka
- Ponto de montagem da AWS
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- Collibra (versão mínima de qualidade de dados do Collibra 2024,02)
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover dados
- Dremio
- Snapshot do Elasticsearch (incluindo camada congelada)

- EMAM
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data do Microsoft SQL Server
- Model9
- Modzy
- Moonwalk Universal
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Documentum 21,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- reveille V10 Build 220706 ou superior
- CDM da Rubrik
- s3a
- Signiant
- Floco de neve
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Starburst
- Arrumação fácil
- Trino
- Verniz Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e posterior

- Vertica 10.x
- Vidisine
- Virtalica StorageFabric
- WEKA v3,10 ou posterior

Soluções de terceiros validadas no StorageGRID com bloqueio de objeto

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Recurso CommVault 11 versão 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21,4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e posterior

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Principais gerentes suportados no StorageGRID

Essas soluções foram testadas.

- Entrust KeyControl 10,2
- Hashicorp Vault 1.15.0
- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9
- Thales CipherTrust Manager 2,10
- Thales CipherTrust Manager 2,11
- Thales CipherTrust Manager 2,12
- Thales CipherTrust Manager 2,13
- Thales CipherTrust Manager 2,14

O StorageGRID 11,7 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,7. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Alluxio
- Apache Kafka
- Ponto de montagem da AWS
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- Collibra (versão mínima de qualidade de dados do Collibra 2024,02)
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi

- Data Dynamics StorageX
- DefendX
- Diskover dados
- Dremio
- Snapshot do Elasticsearch (incluindo camada congelada)
- EMAM
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect Plus
- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data do Microsoft SQL Server
- Model9
- Modzy
- Moonwalk Universal
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Documentum 21,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- reveille V10 Build 220706 ou superior
- CDM da Rubrik
- s3a
- Signiant
- Floco de neve
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Arrumação fácil

- Trino
- Verniz Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1 e posterior
- Vertica 10.x
- Vidisine
- Virtalica StorageFabric
- WEKA v3,10 ou posterior

Soluções de terceiros validadas no StorageGRID com bloqueio de objeto

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Recurso CommVault 11 versão 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21,4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 e posterior

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor

- SilverTrak
- SoftNAS
- QStar
- Velasea

Principais gerentes suportados no StorageGRID

Essas soluções foram testadas.

- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9

O StorageGRID 11,6 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,6. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Alluxio
- Apache Kafka
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover dados
- Dremio
- EMAM

- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Clusters de Big Data do Microsoft SQL Server
- Model9
- Modzy
- Moonwalk Universal
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Documentum 21,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- reveille V10 Build 220706 ou superior
- CDM da Rubrik
- s3a
- Signiant
- Floco de neve
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Arrumação fácil
- Trino
- Verniz Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8,0
- Vertica 10.x
- Vidisine

- Virtalica StorageFabric
- WEKA v3,10 ou posterior

Soluções de terceiros validadas no StorageGRID com bloqueio de objeto

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Recurso CommVault 11 versão 26
- IBM FileNet
- OpenText Documentum 21,4
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 e posterior

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

O StorageGRID 11,5 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,5. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Alluxio
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- Moonwalk Universal
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Documentum 21,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- CDM da Rubrik
- s3a
- Signiant
- Splunk Smartstore
- Trino
- Verniz Enterprise 6.0.4
- Veeam 11
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12

- Veritas NetBackup 8,0
- Vertica 10.x
- Vidisine
- Virtalica StorageFabric

Soluções de terceiros validadas no StorageGRID com bloqueio de objeto

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- OpenText Documentum 21,4
- Veeam 11

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

O StorageGRID 11,4 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,4. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- CDM da Rubrik
- Signiant
- Splunk Smartstore
- Verniz Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8,0
- Vertica 10.x
- Vidisine

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

O StorageGRID 11,3 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,3. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX

- DefendX
- Interica
- Komprise
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- Signiant
- Splunk Smartstore
- Verniz Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8,0
- Vidisine

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor

- SilverTrak
- SoftNAS
- QStar
- Velasea

O StorageGRID 11,2 validou soluções de terceiros

As seguintes soluções de terceiros foram validadas para uso com o StorageGRID 11,2. Se a solução que você está procurando não estiver listada, entre em Contato com o representante da sua conta NetApp.

Soluções de terceiros validadas no StorageGRID

Estas soluções foram testadas em colaboração com os respetivos parceiros.

- Actifio
- Bridgestor
- Cantemo
- Colaboração de conteúdo Citrix
- CommVault 11
- Portal Ctera 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- NICE
- Nasuni
- OpenText Documentum 16,4
- OpenText Media Management 16,5 com CyanGate Cloud
- Panzura
- Ponto Archival Gateway 2,0
- Point Storage Manager 6,4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- Signiant
- Splunk Smartstore
- Verniz Enterprise 6.0.4

- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8,0
- Vidisine

Soluções de terceiros compatíveis com o StorageGRID

Essas soluções foram testadas.

- Archiware
- Comunicações da Axis
- Congruity360
- DataFrameworks
- Plataforma ECODIGITAL DIVA
- Encoding.com
- Fujifilm Object Archive
- Arquivo GE Centricity Enterprise
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- OnSSI
- Alcance o motor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Guias de recursos do produto

Alcançar RPO zero com o StorageGRID: Um guia abrangente para replicação em vários locais

Este relatório técnico fornece um guia abrangente para implementar estratégias de replicação do StorageGRID para alcançar um objetivo de ponto de restauração (RPO) zero no caso de uma falha do local. O documento detalha várias opções de implantação para o StorageGRID, incluindo replicação síncrona de vários sites e replicação assíncrona de várias grades. Ele explica como as políticas de Gerenciamento do ciclo de vida das informações (ILM) da StorageGRID podem ser configuradas para garantir a durabilidade e a disponibilidade dos dados em vários locais. Além disso, o relatório abrange considerações de desempenho, cenários de falha e processos de recuperação para manter operações ininterruptas do cliente. O objetivo deste documento é fornecer as informações para garantir que os dados permaneçam acessíveis e consistentes, mesmo em caso de falha completa do local, utilizando técnicas de replicação síncrona e assíncrona.

Visão geral do StorageGRID

O NetApp StorageGRID é um sistema de storage baseado em objeto que dá suporte à API Amazon Simple Storage Service (Amazon S3) padrão do setor.

O StorageGRID fornece um namespace único em vários locais, com níveis de serviço variáveis orientados pelas políticas de gerenciamento do ciclo de vida das informações (ILM). Com essas políticas de ciclo de vida, você pode otimizar onde seus dados ficam ao longo de seu ciclo de vida.

O StorageGRID permite durabilidade e disponibilidade configuráveis de seus dados em soluções locais e distribuídas geograficamente. Não importa se seus dados estão no local ou em uma nuvem pública, os fluxos de trabalho de nuvem híbrida integrada permitem que sua empresa aproveite serviços de nuvem como Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch e muito mais.

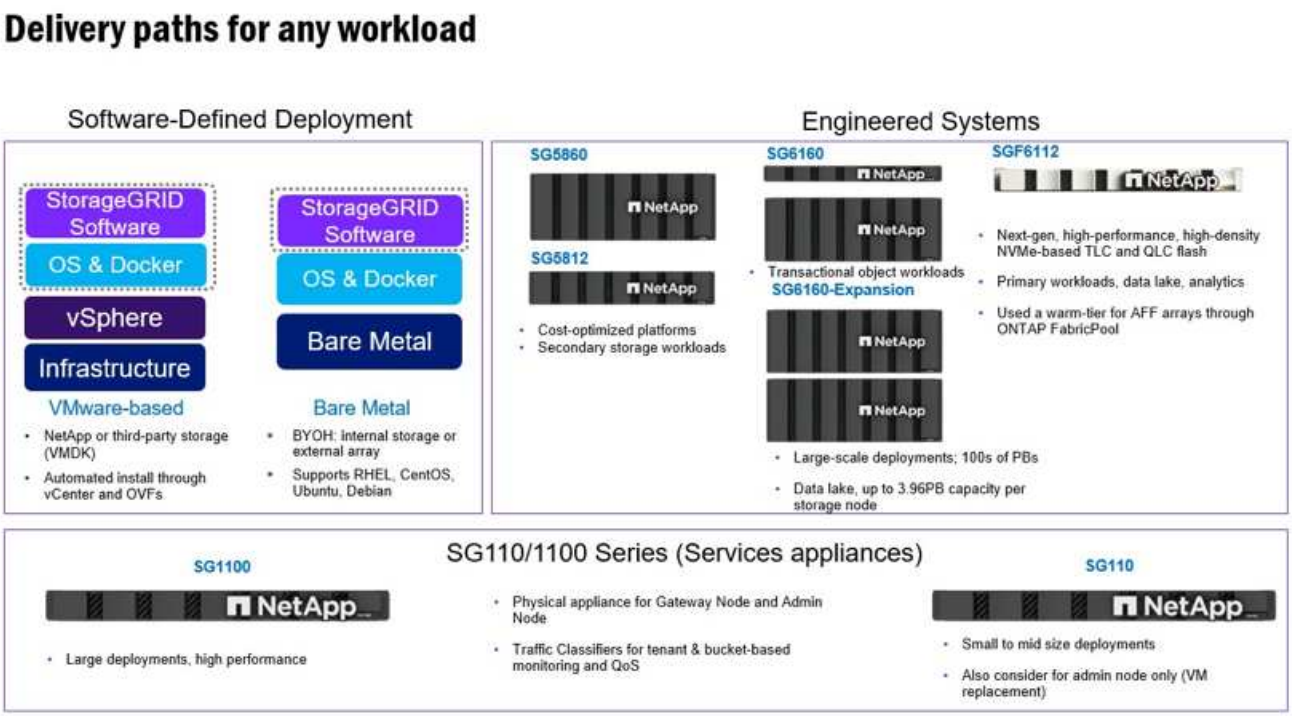
StorageGRID Scale

O StorageGRID pode ser implantado com apenas 3 nós de storage e uma única grade pode crescer até 200 nós. Uma única grade pode ser implantada como um único local ou se estender para 16 locais. Uma grade mínima consiste em um nó de administrador e 3 nós de storage em um único local. O nó de administrador contém a interface de gerenciamento, um ponto central para métricas e logs e mantém a configuração dos componentes do StorageGRID. O nó de administrador também contém um balanceador de carga integrado para acesso à API S3. O StorageGRID pode ser implantado apenas como software, como dispositivos de máquinas virtuais VMware ou como dispositivos criados sob medida.

Um nó StorageGRID pode ser implantado como:

- Um nó somente de metadados que maximiza a contagem de objetos
- Um nó de armazenamento de objetos apenas maximizando o espaço do objeto
- Um nó combinado de metadados e armazenamento de objetos que adiciona contagem de objetos e espaço de objetos

Cada nó de storage pode ser dimensionado para a capacidade de vários petabytes para armazenamento de objetos, o que possibilita um namespace único em centenas de petabytes. O StorageGRID também fornece um balanceador de carga integrado para S3 operações de API chamadas de nó de gateway.



O StorageGRID consiste em uma coleção de nós colocados em uma topologia do local. Um site no StorageGRID pode ser um local físico exclusivo ou residir em um local físico compartilhado como outros sites na grade como uma construção lógica. Um site do StorageGRID não deve abranger vários locais físicos. Um local representa uma infra-estrutura de rede local (LAN) partilhada.

Domínios de StorageGRID e falha

O StorageGRID contém várias camadas de domínios de falha a serem considerados para decidir como arquitetar sua solução, como armazenar seus dados e onde eles devem ser armazenados para reduzir os riscos de falhas.

- Nível da grade - Uma grade composta por vários locais pode ter falhas ou isolamento do local e o(s) local(s) acessível(s) pode continuar operando como a grade.
- Nível do local - falhas dentro de um local podem afetar as operações desse local, mas não afetarão o resto da grade.
- Nível do nó - Uma falha do nó não afetará a operação do local.
- Nível do disco - uma falha de disco não afetará a operação do nó.

Dados e metadados de objetos

Com o armazenamento de objetos, a unidade de armazenamento é um objeto, em vez de um arquivo ou um bloco. Ao contrário da hierarquia semelhante a uma árvore de um sistema de arquivos ou armazenamento em bloco, o armazenamento de objetos organiza os dados em um layout plano e não estruturado. O armazenamento de objetos separa a localização física dos dados do método usado para armazenar e recuperar esses dados.

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

- Os dados do objeto representam os dados subjacentes reais, por exemplo, uma fotografia, um filme ou um registo médico.
- Metadados de objetos são qualquer informação que descreva um objeto.

O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Os metadados de objeto incluem informações como as seguintes:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto, o nome do objeto, o nome do bucket do S3, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e a hora em que o objeto foi criado pela primeira vez e a data e a hora em que o objeto foi modificado pela última vez.
- O local de storage atual de cada réplica de objeto ou fragmento codificado de apagamento.
- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto
- Para objetos segmentados e objetos multipartes, identificadores de segmento e tamanhos de dados.

Os metadados de objetos são personalizáveis e expansíveis, tornando-os flexíveis para uso dos aplicativos. Para obter informações detalhadas sobre como e onde o StorageGRID armazena metadados de objetos, vá para "Gerenciar o storage de metadados de objetos".

O sistema de gerenciamento do ciclo de vida das informações (ILM) da StorageGRID é usado para orquestrar o posicionamento, a duração e o comportamento de ingestão de todos os dados de objetos em seu sistema StorageGRID. As regras do ILM determinam como o StorageGRID armazena objetos ao longo do tempo usando réplicas dos objetos ou codificando o objeto de apagamento em nós e sites. Este sistema ILM é responsável pela consistência de dados do objeto dentro de uma grade.

Codificação de apagamento

O StorageGRID permite apagar dados de código em vários níveis. Com os dispositivos StorageGRID, nós codificamos os dados armazenados em cada nó em todas as unidades com RAID, fornecendo proteção contra várias falhas de disco, causando perda ou interrupções de dados. Além disso, o StorageGRID pode usar esquemas de codificação de apagamento para armazenar dados de objetos nos nós de um site ou se espalhar por 3 ou mais sites no sistema StorageGRID por meio das regras do ILM da StorageGRID.

A codificação de apagamento fornece um layout de storage resiliente para falhas de nós com baixa sobrecarga, enquanto a replicação pode fazer o mesmo e ter mais sobrecarga. Todos os esquemas de codificação de apagamento do StorageGRID são implantáveis em um único local, desde que o número mínimo de nós necessários para armazenar os blocos de dados seja atendido. Isso significa que para um esquema EC de 4 a 2, é necessário que haja um mínimo de 6 nós disponíveis para receber os dados.

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

Consistência de metadados

No StorageGRID, os metadados geralmente são armazenados com três réplicas por local para garantir consistência e disponibilidade. Essa redundância ajuda a manter a integridade e a acessibilidade dos dados mesmo em caso de falha.

A consistência padrão é definida em um nível amplo de grade. Os usuários podem alterar a consistência no nível do balde a qualquer momento.

As opções de consistência de bucket disponíveis no StorageGRID são:

- **Todos**: Fornece o mais alto nível de consistência. Todos os nós na grade recebem os dados imediatamente, ou a solicitação falhará.
- **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-global V2**: Garante consistência de leitura-após-gravação para todas as solicitações de clientes em todos os sites. Oferece consistência para vários nós ou até mesmo uma falha do local se o quórum de réplica de metadados for possível. Por exemplo, um mínimo de 5 réplicas deve ser feito a partir de uma grade de 3 locais com um máximo de 3 réplicas dentro de um site.
- * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site.
- **Read-after-novo-write** (padrão): Fornece consistência de leitura-após-gravação para novos objetos e consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Consistência de dados do objeto

Embora os metadados sejam replicados automaticamente dentro e entre locais, cabe a você decidir sobre a disposição do storage de objetos. Os dados de objetos podem ser armazenados em réplicas dentro e entre sites, codificados para apagamento dentro ou entre sites, ou uma combinação ou réplicas e esquemas de armazenamento codificados para apagamento. As regras de ILM podem se aplicar a todos os objetos ou ser filtradas para se aplicar apenas a determinados objetos, buckets ou locatários. As regras do ILM definem como os objetos são armazenados, réplicas e/ou codificados para apagamento, quanto tempo os objetos são armazenados nesses locais, se o número de réplicas ou esquema de codificação de apagamento deve mudar ou os locais devem mudar com o tempo.

Cada regra de ILM será configurada com um dos três comportamentos de ingestão para proteger objetos: Commit duplo, balanceado ou rigoroso.

A opção de confirmação dupla fará duas cópias em quaisquer dois nós de storage diferentes na grade imediatamente e retornará a solicitação com êxito ao cliente. A seleção do nó tentará dentro do site da solicitação, mas pode usar nós de outro site em algumas circunstâncias. O objeto é adicionado à fila ILM para ser avaliado e colocado de acordo com as regras ILM.

A opção Balanced avalia o objeto em relação à política ILM imediatamente e coloca o objeto de forma síncrona antes de retornar a solicitação é bem-sucedida para o cliente. Se a regra de ILM não puder ser atendida imediatamente devido a uma interrupção ou storage inadequado para atender aos requisitos de posicionamento, a confirmação dupla será usada. Quando o problema for resolvido, o ILM colocará automaticamente o objeto com base na regra definida.

A opção strict avalia o objeto em relação à política ILM imediatamente e coloca o objeto de forma síncrona antes de retornar a solicitação é bem-sucedida para o cliente. Se a regra ILM não puder ser atendida imediatamente devido a uma interrupção ou armazenamento inadequado para atender aos requisitos de colocação, a solicitação falhará e o cliente precisará tentar novamente.

Balanceamento de carga

StorageGRID pode ser implantado com acesso de cliente através de nós de gateway integrado, um balanceador de carga externo de 3 a de terceiros, round robin DNS ou diretamente para um nó de storage. Vários nós de gateway podem ser implantados em um local e configurados em grupos de alta disponibilidade, fornecendo failover automatizado e failback no caso de uma interrupção do nó de gateway. Você pode combinar métodos de balanceamento de carga em uma solução para fornecer um único ponto de acesso para todos os sites em uma solução.

Os nós de gateway equilibrarão a carga entre os nós de storage no local onde o nó de gateway reside por padrão. O StorageGRID pode ser configurado para permitir que os nós de gateway equilibrem a carga usando nós de vários locais. Essa configuração adicionaria a latência entre esses sites à latência de resposta às solicitações do cliente. Isso só deve ser configurado se a latência total for aceitável para os clientes.

Como alcançar o RPO zero com o StorageGRID

Para alcançar o objetivo do ponto de restauração (RPO) zero em um sistema de storage de objetos, é crucial que, no momento da falha:

- Os metadados e o conteúdo do objeto estão em sincronia e são considerados consistentes
- O conteúdo do objeto permanece acessível apesar da falha.

Para uma implantação em vários locais, o strong Global V2 é o modelo de consistência preferido para garantir que os metadados sejam sincronizados em todos os locais, tornando-o essencial para atender ao requisito de

RPO zero.

Os objetos no sistema de storage são armazenados com base nas regras do Information Lifecycle Management (ILM), que determinam como e onde os dados são armazenados durante todo o ciclo de vida. Para replicação síncrona, pode-se considerar entre execução estrita ou execução equilibrada.

- A execução estrita dessas regras ILM é necessária para RPO zero, pois garante que os objetos sejam colocados nos locais definidos sem qualquer atraso ou retorno, mantendo a disponibilidade e a consistência dos dados.
- O comportamento de ingestão de equilíbrio de ILM da StorageGRID fornece um equilíbrio entre alta disponibilidade e resiliência, permitindo que os usuários continuem ingerindo dados mesmo em caso de falha do site.

Opcionalmente, garantir um rto de zero pode ser alcançado com uma combinação de balanceamento de carga local e global. Garantir o acesso ininterrupto ao cliente requer o balanceamento de carga das solicitações do cliente. Uma solução StorageGRID pode conter muitos nós de gateway e grupos de alta disponibilidade em cada local. Para fornecer acesso ininterrupto aos clientes em qualquer site, mesmo em uma falha do site, você deve configurar uma solução de balanceamento de carga externa em combinação com os nós de gateway StorageGRID. Configure grupos de alta disponibilidade de nós de gateway que gerenciam a carga em cada local e use o balanceador de carga externo para equilibrar a carga entre os grupos de alta disponibilidade. O balanceador de carga externo deve ser configurado para realizar uma verificação de integridade para garantir que as solicitações sejam enviadas apenas para os locais operacionais. Para obter mais informações sobre balanceamento de carga com o StorageGRID, consulte "Relatório técnico do balanceador de carga StorageGRID".

Implantações síncronas em vários locais

Soluções multi-site: o StorageGRID permite replicar objetos em vários locais dentro da grade de forma síncrona. Ao configurar regras de Gerenciamento do ciclo de vida da Informação (ILM) com equilíbrio ou comportamento estrito, os objetos são colocados imediatamente nos locais especificados. A configuração do nível de consistência do bucket para o Global v2 forte também garantirá a replicação síncrona de metadados. O StorageGRID usa um único namespace global, armazenando locais de posicionamento de objetos como metadados. Assim, cada nó sabe onde estão localizadas todas as cópias ou peças codificadas de apagamento. Se um objeto não puder ser recuperado do site onde a solicitação foi feita, ele será recuperado automaticamente de um site remoto sem a necessidade de procedimentos de failover.

Uma vez que a falha é resolvida, não são necessários esforços de failback manual. O desempenho da replicação depende do local com a taxa de transferência de rede mais baixa, a latência mais alta e o desempenho mais baixo. O desempenho de um site é baseado no número de nós, contagem e velocidade de núcleos da CPU, memória, quantidade de unidades e tipos de unidades.

Soluções de várias grades: a StorageGRID pode replicar locatários, usuários e buckets entre vários sistemas StorageGRID usando replicação entre grades (CGR). O CGR pode estender dados selecionados para mais de 16 locais, aumentar a capacidade utilizável do seu armazenamento de objetos e fornecer recuperação de desastres. A replicação de buckets com CGR inclui objetos, versões de objetos e metadados e pode ser bidirecional ou unidirecional. O objetivo do ponto de restauração (RPO) depende do desempenho de cada sistema StorageGRID e das conexões de rede entre eles.

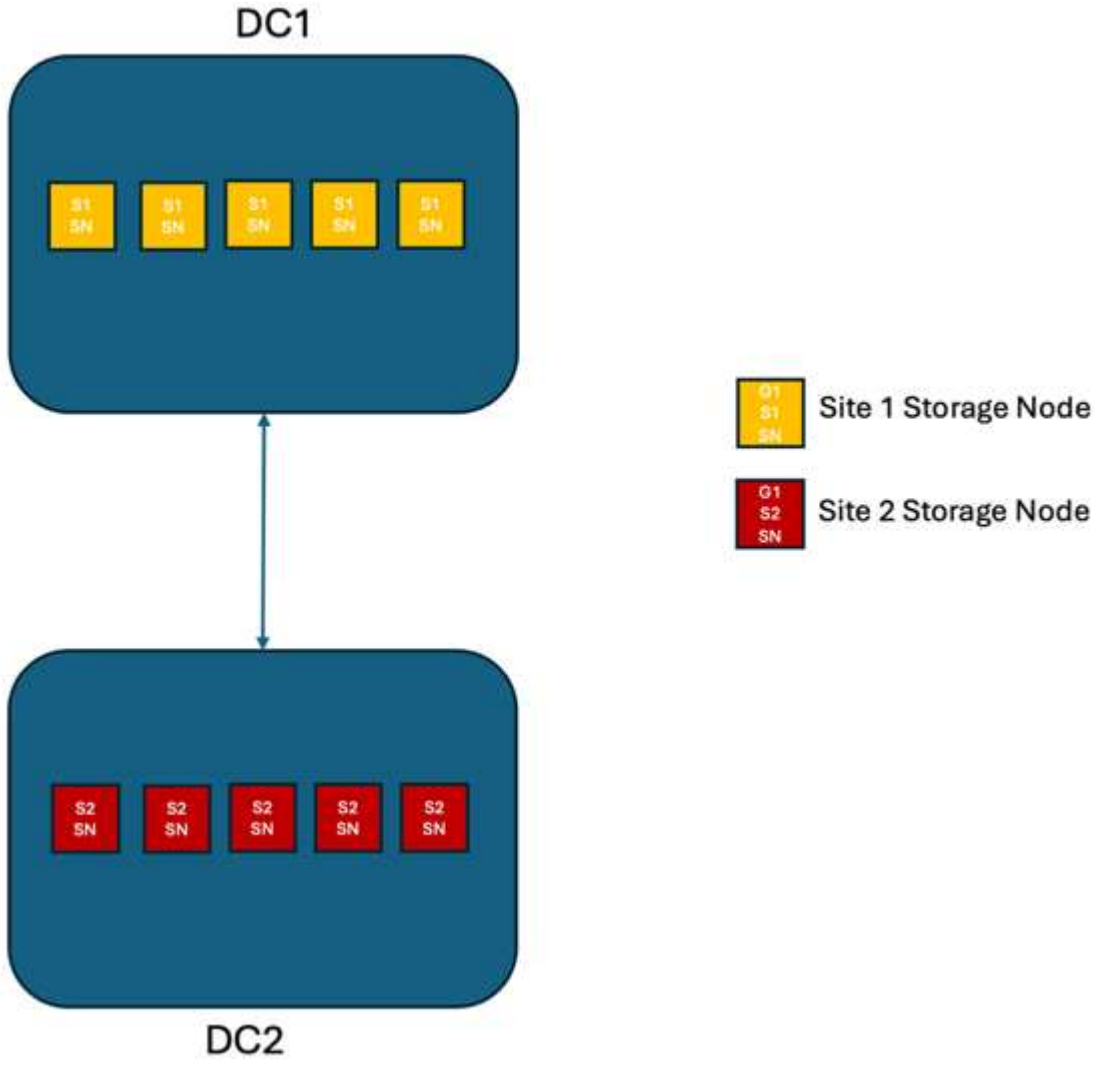
Resumo:

- A replicação intra-grade inclui replicação síncrona e assíncrona, configurável usando o comportamento de ingestão de ILM e o controle de consistência de metadados.
- A replicação inter-grid é assíncrona somente.

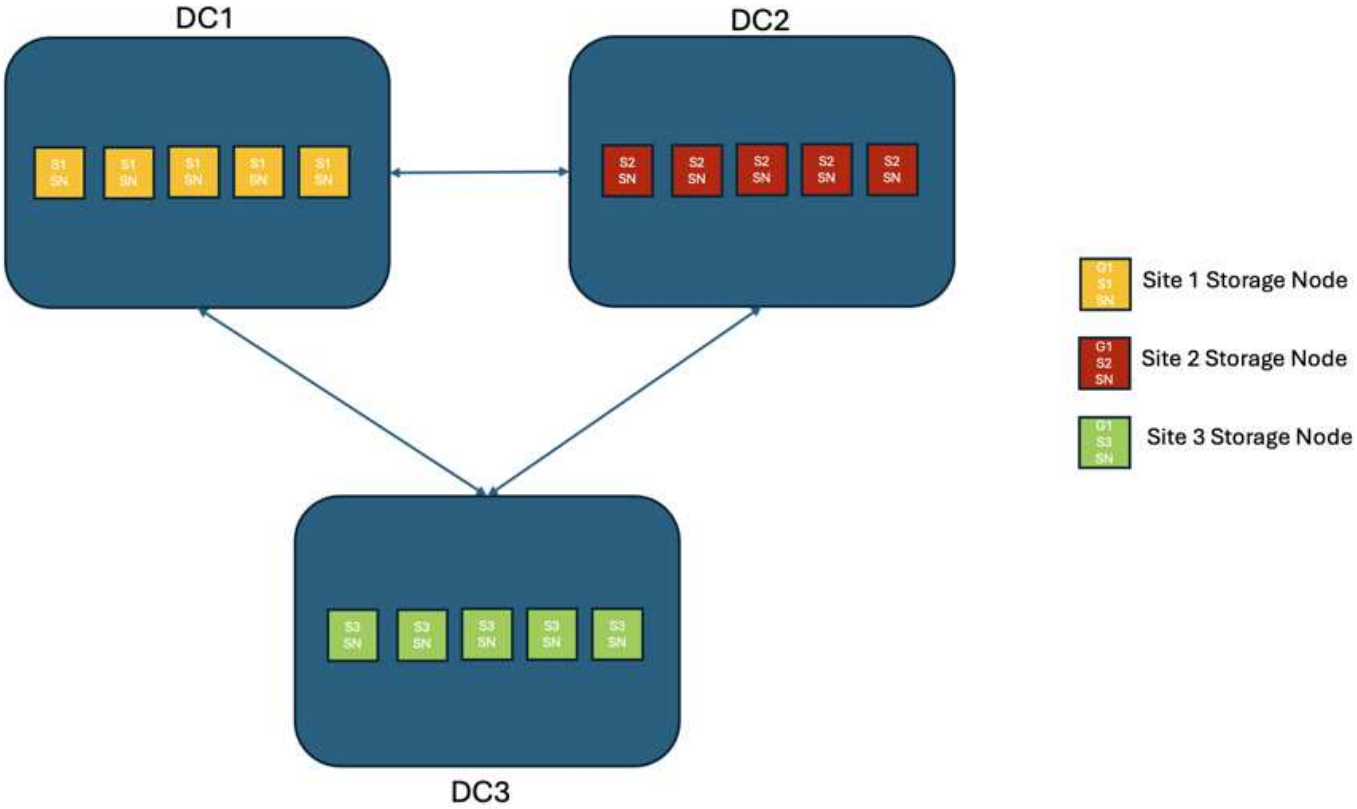
Uma implantação de Multi-site de Grade única

Nos cenários a seguir, as soluções StorageGRID são configuradas com um balanceador de carga externo opcional que gerencia solicitações aos grupos de alta disponibilidade do balanceador de carga integrado. Isso alcançará um rto zero, além de um RPO de zero. O ILM é configurado com proteção equilibrada de ingestão para colocação síncrona. Cada bucket é configurado com o forte modelo global de consistência v2 para grades de 3 ou mais locais e forte consistência Global para menos de 3 locais.

Em uma solução StorageGRID de dois sites há pelo menos duas réplicas ou 3 blocos EC de cada objeto e 6 réplicas de todos os metadados. Após a recuperação da falha, as atualizações da interrupção serão sincronizadas automaticamente com o local/nós recuperados. Com apenas 2 locais, é provável que não alcance RPO zero em cenários de falha além de uma perda total no local.



Em uma solução StorageGRID de três ou mais sites, há pelo menos 3 réplicas ou 3 blocos EC de cada objeto e 9 réplicas de todos os metadados. Após a recuperação da falha, as atualizações da interrupção serão sincronizadas automaticamente com o local/nós recuperados. Com três ou mais locais, é possível alcançar um RPO zero.



Cenários de falha em vários locais

Falha	Resultado de 2 locais	resultado de 3 ou mais sites
Falha da unidade de nó único	Cada dispositivo usa vários grupos de discos e pode sustentar uma falha de pelo menos 1 unidade por grupo sem interrupção ou perda de dados.	Cada dispositivo usa vários grupos de discos e pode sustentar uma falha de pelo menos 1 unidade por grupo sem interrupção ou perda de dados.
Falha de nó único em um local	Nenhuma interrupção das operações ou perda de dados.	Nenhuma interrupção das operações ou perda de dados.
Falha de vários nós em um local	Interrupção das operações do cliente direcionadas para este site, mas sem perda de dados. As operações direcionadas para o outro site permanecem ininterruptas e sem perda de dados.	As operações são direcionadas a todos os outros sites e permanecem ininterruptas e sem perda de dados.

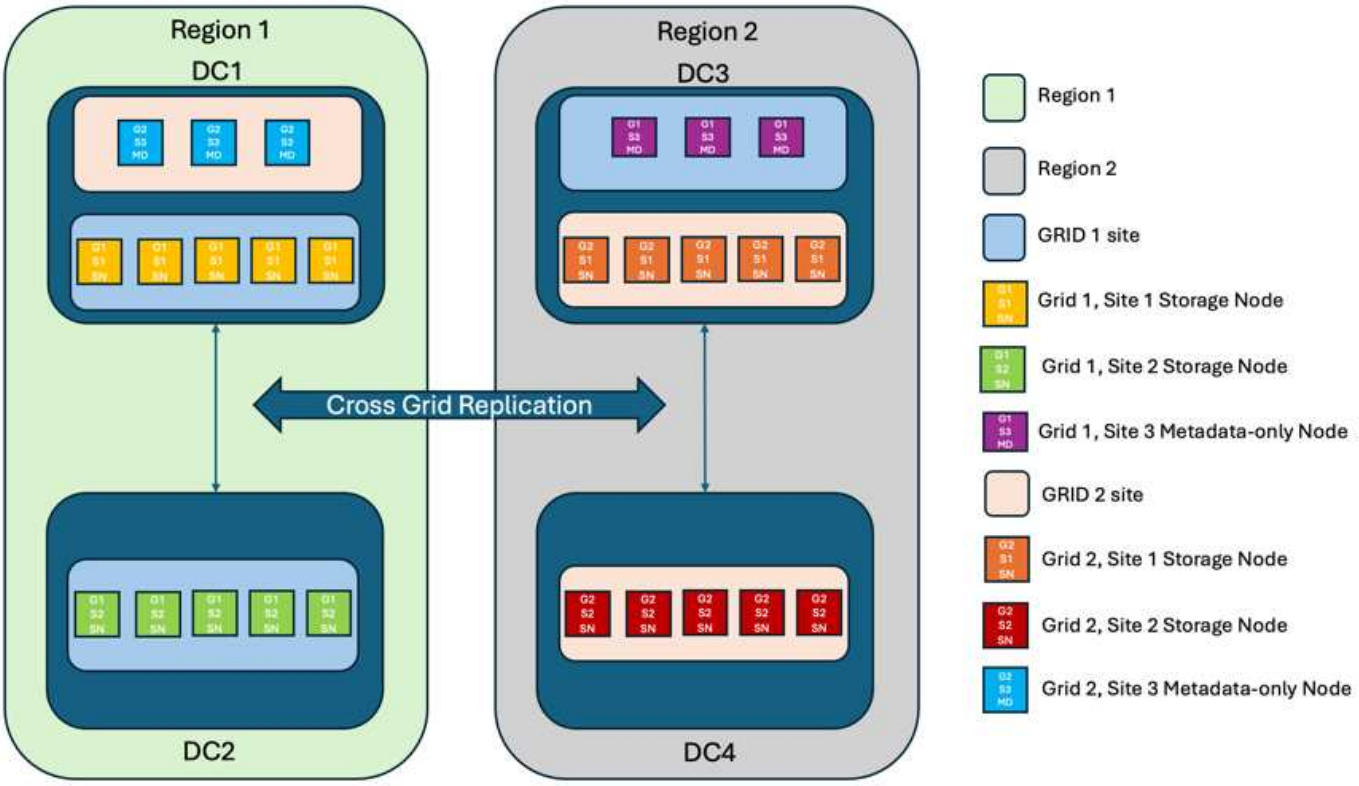
Falha	Resultado de 2 locais	resultado de 3 ou mais sites
Falha de nó único em vários locais	Sem interrupção ou perda de dados se: • Pelo menos uma única réplica existe na grade • Existem pedaços suficientes de EC na grade Operações interrompidas e risco de perda de dados se: • Não existem réplicas • Existem mandris CE insuficientes	Sem interrupção ou perda de dados se: • Pelo menos uma única réplica existe na grade • Existem pedaços suficientes de EC na grade Operações interrompidas e risco de perda de dados se: • Não existem réplicas • Existem pedaços de EC insuficientes para recuperar o objeto
Falha única de local	as operações do cliente serão interrompidas até que a falha seja resolvida, ou a consistência do bucket seja reduzida para um local forte ou menor para permitir que as operações tenham sucesso, mas sem perda de dados.	Nenhuma interrupção das operações ou perda de dados.
Um único local e falhas de nó único	as operações do cliente serão interrompidas até que a falha seja resolvida ou a consistência do bucket seja reduzida para leitura após nova gravação ou menor para permitir que as operações tenham sucesso e possível perda de dados.	Nenhuma interrupção das operações ou perda de dados.
Um único local mais um nó de cada local restante	as operações do cliente serão interrompidas até que a falha seja resolvida ou a consistência do bucket seja reduzida para leitura após nova gravação ou menor para permitir que as operações tenham sucesso e possível perda de dados.	As operações serão interrompidas se o quórum de réplica de metadados não puder ser atendido e possível perda de dados.
Falha em vários locais	Nenhum local de operações permanece os dados serão perdidos se pelo menos 1 local não puder ser recuperado em sua totalidade.	As operações serão interrompidas se o quórum de réplica de metadados não puder ser atendido. Sem perda de dados, desde que pelo menos 1 local permaneça.

Falha	Resultado de 2 locais	resultado de 3 ou mais sites
Isolamento de rede de um site	as operações do cliente serão interrompidas até que a falha seja resolvida, ou a consistência do bucket seja reduzida para um local forte ou menor para permitir que as operações tenham sucesso, mas sem perda de dados	As operações serão interrompidas para o local isolado, mas sem perda de dados Sem interrupção das operações nos locais restantes e sem perda de dados

Uma implantação multi-grade em vários locais

Para adicionar uma camada extra de redundância, esse cenário utilizará dois clusters StorageGRID e usará replicação entre grade para mantê-los sincronizados. Para essa solução, cada cluster do StorageGRID terá três locais. Dois sites serão usados para armazenamento de objetos e metadados, enquanto o terceiro site será usado apenas para metadados. Ambos os sistemas serão configurados com uma regra ILM balanceada para armazenar sincronamente os objetos usando codificação de apagamento em cada um dos dois locais de dados. Os buckets serão configurados com o forte modelo global de consistência v2. Cada grade será configurada com replicação bidirecional de grade cruzada em cada bucket. Isso fornece a replicação assíncrona entre as regiões. Opcionalmente, um balanceador de carga global pode ser implementado para gerenciar solicitações para os grupos integrados de alta disponibilidade do balanceador de carga de ambos os sistemas StorageGRID, a fim de alcançar um RPO zero.

A solução usará quatro locais divididos igualmente em duas regiões. A região 1 conterá os 2 locais de armazenamento da grade 1 como a grade primária da região e o local de metadados da grade 2. A região 2 conterá os 2 locais de armazenamento da grade 2 como a grade primária da região e o local de metadados da grade 1. Em cada região, o mesmo local pode abrigar o local de armazenamento da grade primária da região, bem como o local de metadados único da grade de outras regiões. O uso de nós somente de metadados como terceiro local fornecerá a consistência necessária para os metadados e não duplicará o storage de objetos nesse local.



Essa solução com quatro locais separados oferece redundância completa de dois sistemas StorageGRID separados que mantêm um RPO de 0 e usará a replicação síncrona de vários locais e a replicação assíncrona de várias grades. Qualquer local pode falhar, mantendo operações de cliente ininterruptas em ambos os sistemas StorageGRID.

Nessa solução, há quatro cópias codificadas de apagamento de cada objeto e 18 réplicas de todos os metadados. Isso permite vários cenários de falha sem impactos nas operações do cliente. Após a falha, as atualizações de recuperação da falha serão sincronizadas automaticamente com o local/nós com falha.

Cenários de falha multisite e de várias grades

Falha	Resultado
Falha da unidade de nó único	Cada dispositivo usa vários grupos de discos e pode sustentar uma falha de pelo menos 1 unidade por grupo sem interrupção ou perda de dados.
Falha de nó único em um local em uma grade	Nenhuma interrupção das operações ou perda de dados.
Falha de nó único em um local em cada grade	Nenhuma interrupção das operações ou perda de dados.
Falha de vários nós em um local em uma grade	Nenhuma interrupção das operações ou perda de dados.
Falha de vários nós em um local em cada grade	Nenhuma interrupção das operações ou perda de dados.
Falha de nó único em vários locais em uma grade	Nenhuma interrupção das operações ou perda de dados.

Falha	Resultado
Falha de nó único em vários locais em cada grade	Nenhuma interrupção das operações ou perda de dados.
Falha de um único local em uma grade	Nenhuma interrupção das operações ou perda de dados.
Falha de um único local em cada grade	Nenhuma interrupção das operações ou perda de dados.
Um único local e falhas de nó único em uma grade	Nenhuma interrupção das operações ou perda de dados.
Um único local mais um nó de cada local restante em uma única grade	Nenhuma interrupção das operações ou perda de dados.
Falha de local único	Nenhuma interrupção das operações ou perda de dados.
Falha de localização única em cada grade DC1 e DC3	As operações serão interrompidas até que a falha seja resolvida ou a consistência do balde seja abaixada; cada grade perdeu 2 locais Todos os dados ainda existem em 2 locais
Falha de localização única em cada grade DC1 e DC4 ou DC2 e DC3	Nenhuma interrupção das operações ou perda de dados.
Falha de localização única em cada grade DC2 e DC4	Nenhuma interrupção das operações ou perda de dados.
Isolamento de rede de um site	As operações serão interrompidas para o local isolado, mas nenhum dado será perdido Sem interrupção das operações nos locais restantes ou perda de dados.

Conclusão

Alcançar o objetivo de ponto de restauração (RPO) zero com o StorageGRID é uma meta essencial de garantir a durabilidade e a disponibilidade dos dados em caso de falhas no local. Ao aproveitar as estratégias robustas de replicação do StorageGRID, incluindo replicação síncrona em vários locais e replicação assíncrona em várias grades, as organizações podem manter operações ininterruptas dos clientes e garantir a consistência dos dados em vários locais. A implementação de políticas de Gerenciamento do ciclo de vida das informações (ILM) e o uso de nós somente metadados aumentam ainda mais a resiliência e o desempenho do sistema. Com o StorageGRID, as empresas podem gerenciar seus dados com confiança, sabendo que eles permanecem acessíveis e consistentes mesmo diante de cenários complexos de falhas. Essa abordagem abrangente para gerenciamento e replicação de dados ressalta a importância do Planejamento e execução meticulosos para alcançar RPO zero e proteger informações valiosas.

Crie o Cloud Storage Pool para AWS ou Google Cloud

Você pode usar um pool de armazenamento em nuvem se quiser mover objetos do StorageGRID para um bucket externo do S3. O bucket externo pode pertencer ao Amazon S3 (AWS) ou ao Google Cloud.

O que você vai precisar

- O StorageGRID 11,6 foi configurado.
- Você já configurou um bucket externo do S3 na AWS ou no Google Cloud.

Passos

1. No Gerenciador de Grade, navegue até **ILM** > **Storage Pools**.
2. Na seção Cloud Storage Pools da página, selecione **criar**.

   A janela pop-up Create Cloud Storage Pool (criar pool de armazenamento na nuvem) é exibida.

3. Introduza um nome de apresentação.
4. Selecione **Amazon S3** na lista suspensa tipo de provedor.

   Esse tipo de provedor funciona para AWS S3 ou Google Cloud.

5. Insira o URI para o bucket do S3 a ser usado para o pool de armazenamento em nuvem.

   Dois formatos são permitidos:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Introduza o nome do bucket S3.

   O nome especificado deve corresponder exatamente ao nome do bucket do S3; caso contrário, a criação do pool de armazenamento em nuvem falha. Você não pode alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

7. Opcionalmente, insira o ID da chave de acesso e a chave de acesso secreta.
8. Selecione **não verificar certificado** na lista suspensa.
9. Clique em **Salvar**.

Resultado esperado

Confirme se um pool de armazenamento em nuvem foi criado para o Amazon S3 ou o Google Cloud.

Por Jonathan Wong

Criar Cloud Storage Pool para Azure Blob Storage

Você pode usar um pool de storage de nuvem se quiser mover objetos do StorageGRID para um contêiner externo do Azure.

O que você vai precisar

- O StorageGRID 11,6 foi configurado.
- Você já configurou um contentor Azure externo.

Passos

1. No Gerenciador de Grade, navegue até **ILM** > **Storage Pools**.
2. Na seção Cloud Storage Pools da página, selecione **criar**.

   A janela pop-up Create Cloud Storage Pool (criar pool de armazenamento na nuvem) é exibida.

3. Introduza um nome de apresentação.
4. Selecione **armazenamento Blob Azure** na lista suspensa tipo de provedor.
5. Insira o URI para o bucket do S3 a ser usado para o pool de armazenamento em nuvem.

   Dois formatos são permitidos:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Introduza o nome do contentor Azure.

   O nome que você especificar deve corresponder exatamente ao nome do contentor do Azure; caso contrário, a criação do pool de armazenamento em nuvem falha. Você não pode alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

7. Opcionalmente, insira o nome da conta associada do Azure Container e a chave da conta para autenticação.
8. Selecione **não verificar certificado** na lista suspensa.
9. Clique em **Salvar**.

Resultado esperado

Confirme se um Cloud Storage Pool foi criado para o Azure Blob Storage.

Por Jonathan Wong

Use um Cloud Storage Pool para backup

Você pode criar uma regra ILM para mover objetos para um pool de armazenamento em nuvem para backup.

O que você vai precisar

- O StorageGRID 11,6 foi configurado.
- Você já configurou um contentor Azure externo.

Passos

1. No Gerenciador de Grade, navegue até **ILM** > **regras** > **criar**.
2. Introduza uma descrição.
3. Introduza um critério para acionar a regra.

4. Clique em **seguinte**.
5. Replique o objeto para nós de storage.
6. Adicione uma regra de colocação.
7. Replique o objeto para o Cloud Storage Pool
8. Clique em **seguinte**.
9. Clique em **Salvar**.

Resultado esperado

Confirme se o diagrama de retenção mostra os objetos armazenados localmente no StorageGRID e em um pool de storage de nuvem para backup.

Confirme que, quando a regra ILM é acionada, existe uma cópia no Cloud Storage Pool e você pode recuperar o objeto localmente sem fazer uma restauração de objeto.

Por Jonathan Wong

Configurar o serviço de integração de pesquisa StorageGRID

Este guia fornece instruções detalhadas para configurar o serviço de integração de pesquisa do NetApp StorageGRID com o serviço Amazon OpenSearch ou o Elasticsearch no local.

Introdução

O StorageGRID é compatível com três tipos de serviços de plataforma.

- **Replicação do StorageGRID CloudMirror**. Espelhe objetos específicos de um bucket do StorageGRID para um destino externo especificado.
- **Notificações**. Notificações de eventos por bucket para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (Amazon SNS) externo especificado.
- **Serviço de integração de pesquisa**. Envie metadados de objeto Simple Storage Service (S3) para um índice Elasticsearch especificado, onde você pode pesquisar ou analisar os metadados usando o serviço externo.

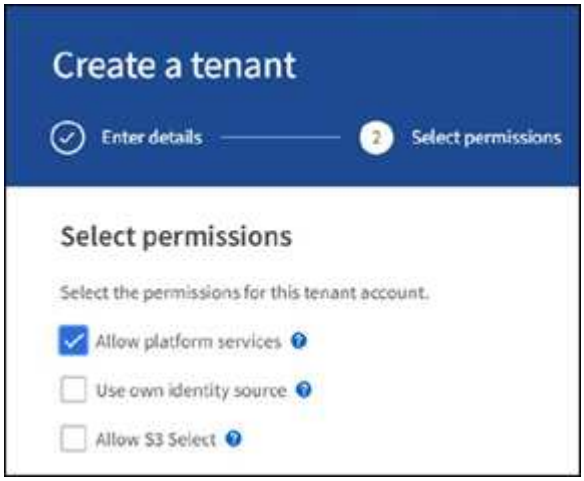
Os serviços de plataforma são configurados pelo locatário do S3 por meio da IU do Tenant Manager. Para obter mais informações, "Considerações sobre o uso de serviços de plataforma"consulte .

Este documento serve como um suplemento ao "Guia do Locatário do StorageGRID 11,6" e fornece instruções passo a passo e exemplos para a configuração de endpoint e bucket para serviços de integração de pesquisa. As instruções de configuração do Amazon Web Services (AWS) ou do Elasticsearch no local incluídas aqui são apenas para fins básicos de teste ou demonstração.

Os públicos-alvo devem estar familiarizados com o Gerenciador de Grade, o Gerenciador do Locatário e ter acesso ao navegador S3 para executar operações básicas de upload (PUT) e download (GET) para o teste de integração de pesquisa do StorageGRID.

Crie inquilino e habilite serviços de plataforma

1. Crie um locatário S3 usando o Gerenciador de Grade, insira um nome de exibição e selecione o protocolo S3.
2. Na página permissão, selecione a opção permitir Serviços de Plataforma. Opcionalmente, selecione outras permissões, se necessário.



3. Configure a senha inicial do usuário raiz do locatário ou, se a federação identificar estiver habilitada na grade, selecione qual grupo federado tem permissão de acesso raiz para configurar a conta do locatário.
4. Clique em entrar como root e selecione Bucket: Create and Manage Buckets.

   Isso o leva à página do Gerenciador de Locações.

5. No Gerenciador do Tenant, selecione Minhas chaves de acesso para criar e baixar a chave de acesso S3 para testes posteriores.

PESQUISE serviços de integração com o Amazon OpenSearch

Configuração do serviço Amazon OpenSearch (anteriormente Elasticsearch)

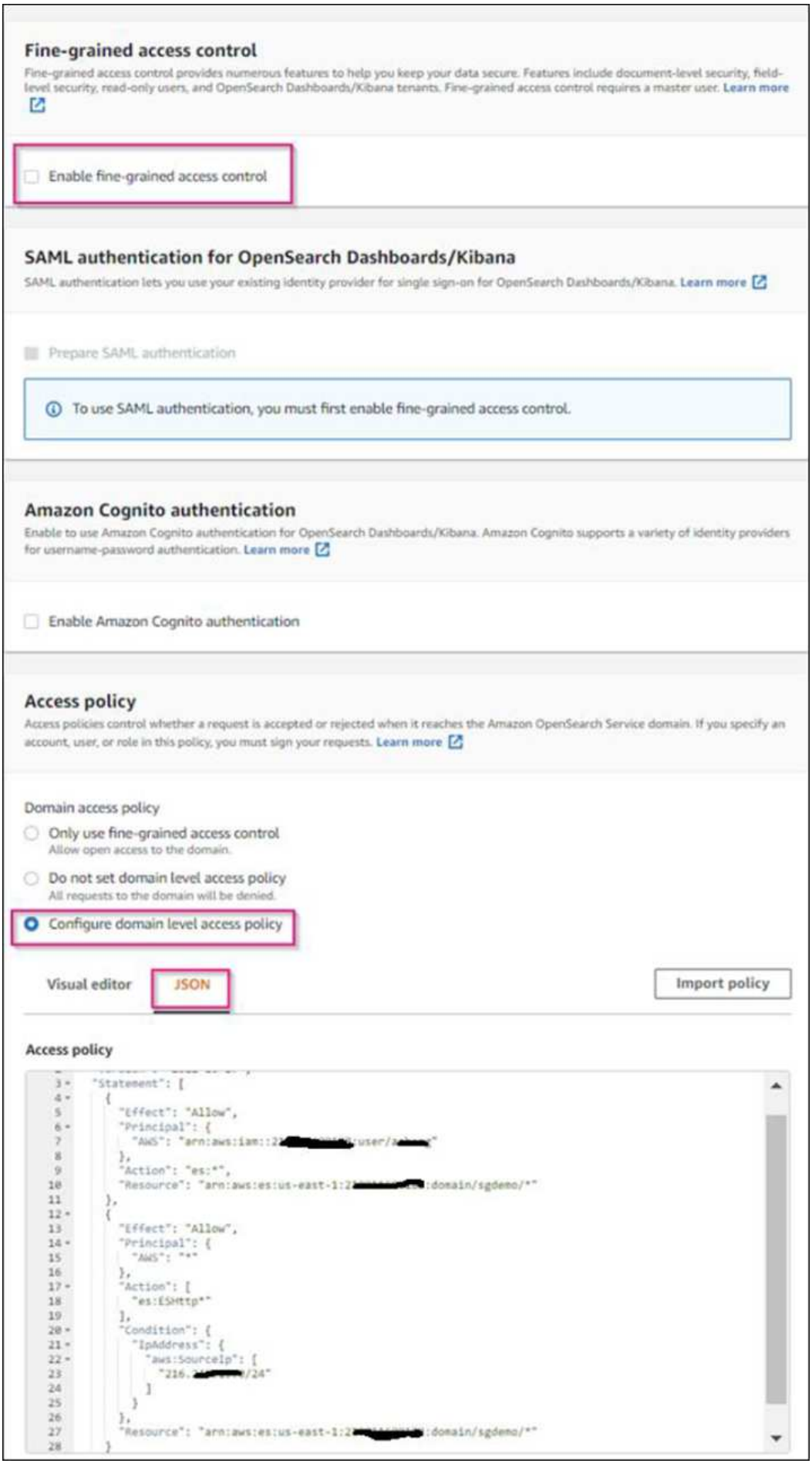
Use este procedimento para uma configuração rápida e simples do serviço OpenSearch apenas para fins de teste/demonstração. Se você estiver usando o Elasticsearch no local para serviços de integração de pesquisa, consulte a PESQUISE serviços de integração com o Elasticsearch no localseção .

> Você deve ter um login válido no console da AWS, chave de acesso, chave de acesso secreta e permissão para assinar o serviço OpenSearch.

1. Crie um novo domínio usando as instruções do "AWS OpenSearch Service Introdução ao AWS OpenSearch Service", exceto o seguinte:
   - Passo 4. Nome de domínio: Sgdemo
   - Passo 10. Controle de acesso refinado: Desmarque a opção Ativar Controle de Acesso fino com Grained.
   - Passo 12. Política de acesso: Selecione Configurar política de acesso de nível, selecione a guia JSON para modificar a política de acesso usando o exemplo a seguir:
     - Substitua o texto realçado pelo seu próprio ID e nome de usuário do AWS Identity and Access Management (IAM).

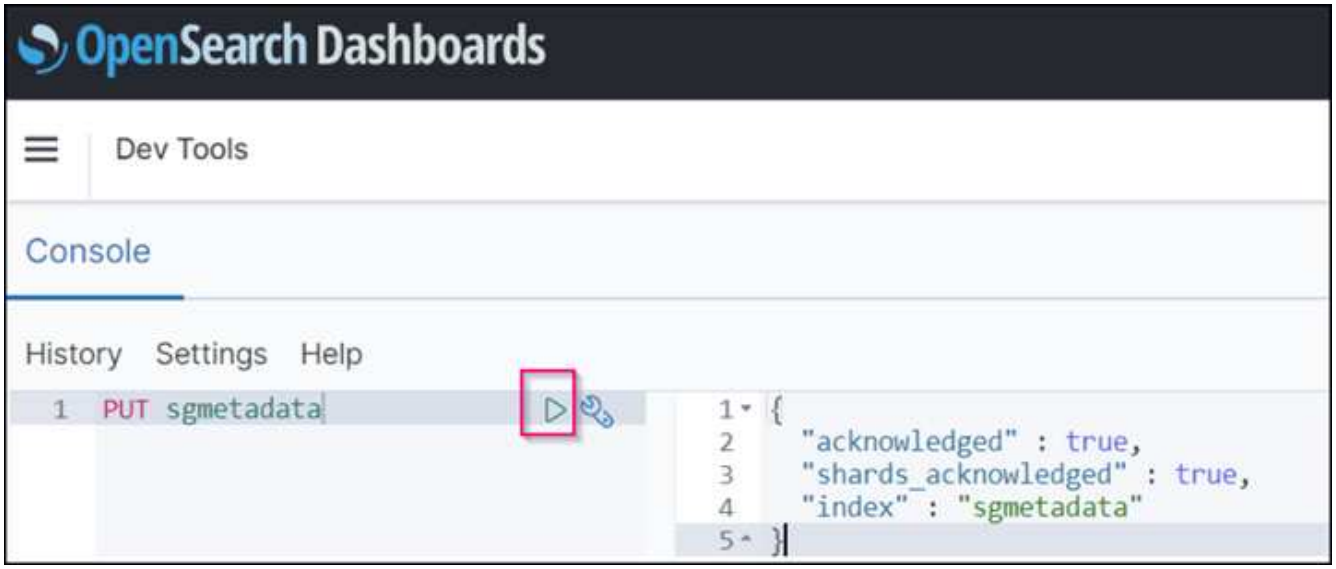
- Substitua o texto destacado (o endereço IP) pelo endereço IP público do computador local usado para acessar o console da AWS.
- Abra uma guia do navegador para "https://checkip.amazonaws.com" encontrar seu IP público.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```

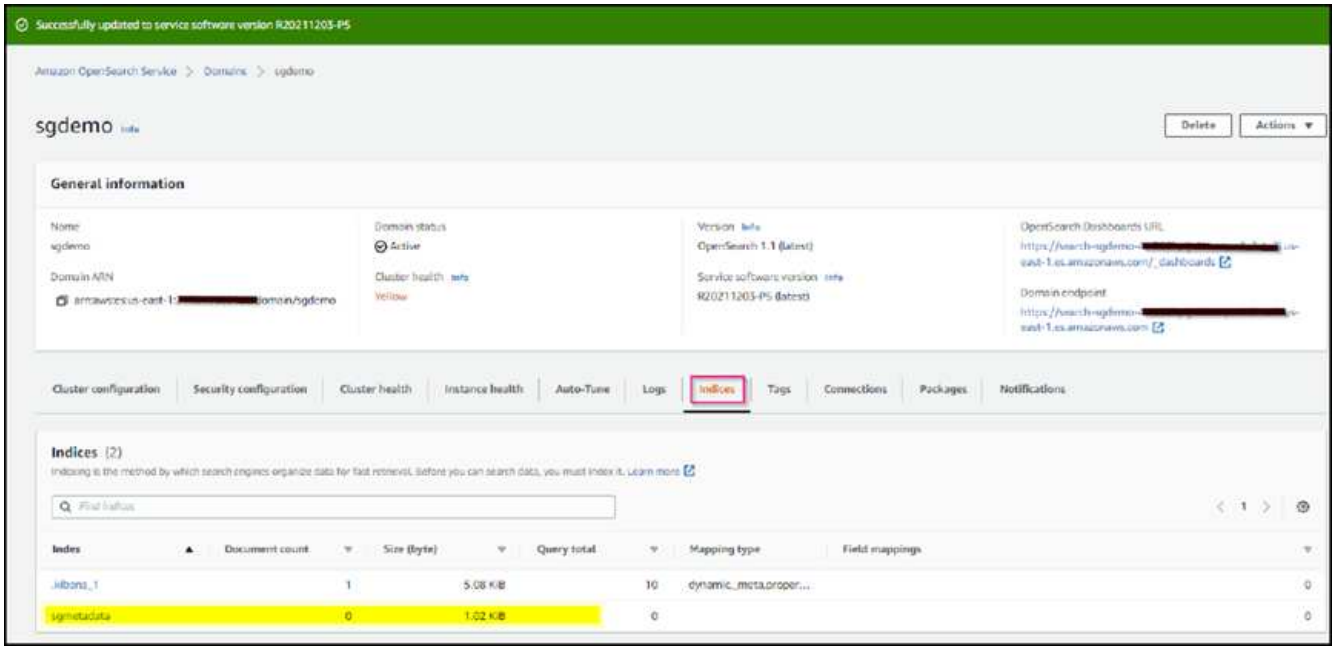

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

2. Aguarde de 15 a 20 minutos para que o domínio fique ativo.

3. Clique em OpenSearch Dashboards URL para abrir o domínio em uma nova guia para acessar o painel. Se você receber um erro de acesso negado, verifique se o endereço IP de origem da diretiva de acesso está corretamente definido para o IP público do computador para permitir o acesso ao painel do domínio.
4. Na página de boas-vindas do painel, selecione explorar por conta própria. No menu, aceda a Gestão → Ferramentas de desenvolvimento
5. Em Ferramentas de desenvolvimento → Console , digite `PUT <index>` onde você usa o índice para armazenar metadados de objetos StorageGRID. Usamos o nome do índice 'sgmetadata' no exemplo a seguir. Clique no símbolo de triângulo pequeno para executar o comando PUT. O resultado esperado é exibido no painel direito, como mostrado no exemplo de captura de tela a seguir.



6. Verifique se o índice está visível a partir da IU do Amazon OpenSearch em sgdomain > índices.

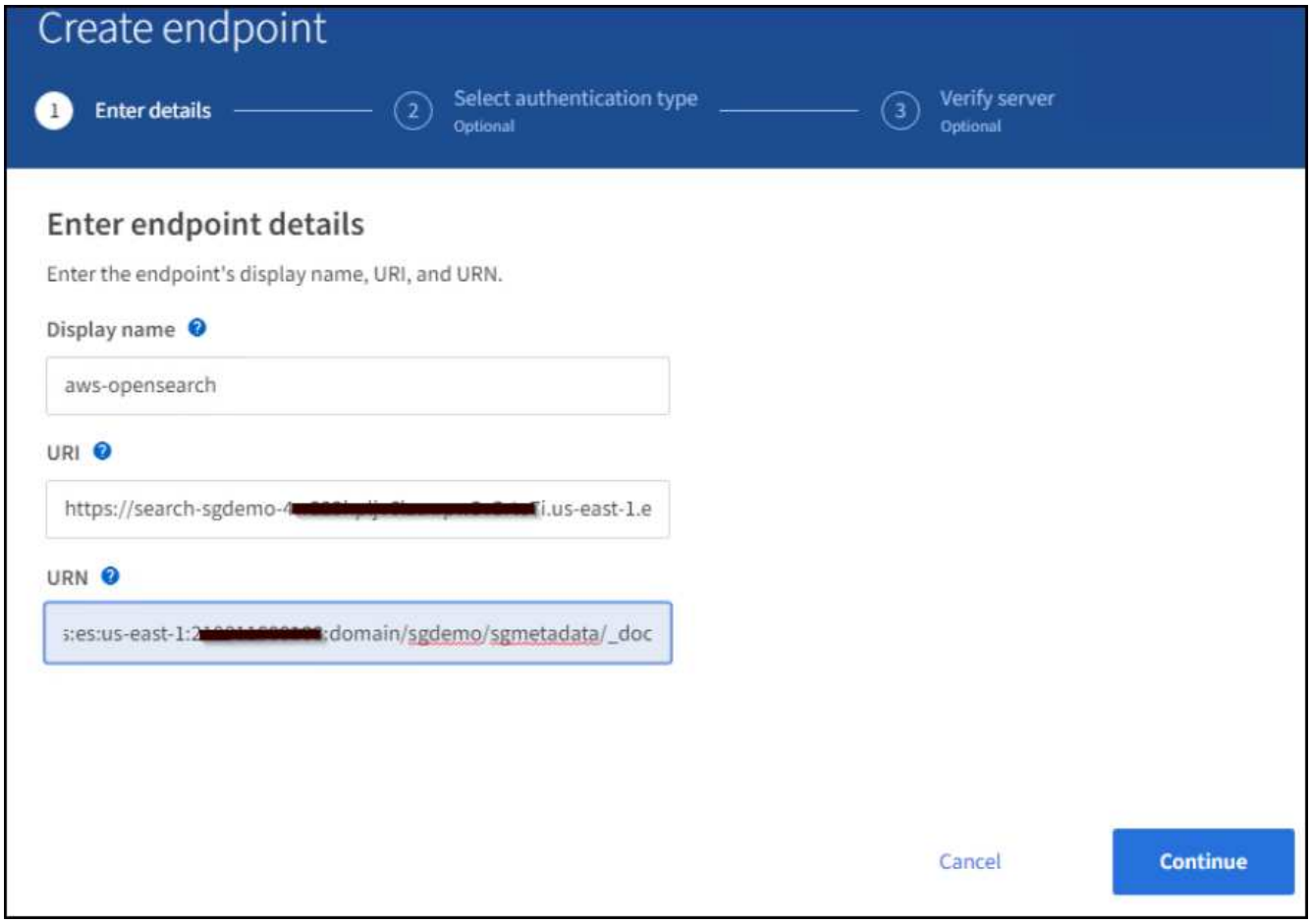


Configuração de endpoint de serviços de plataforma

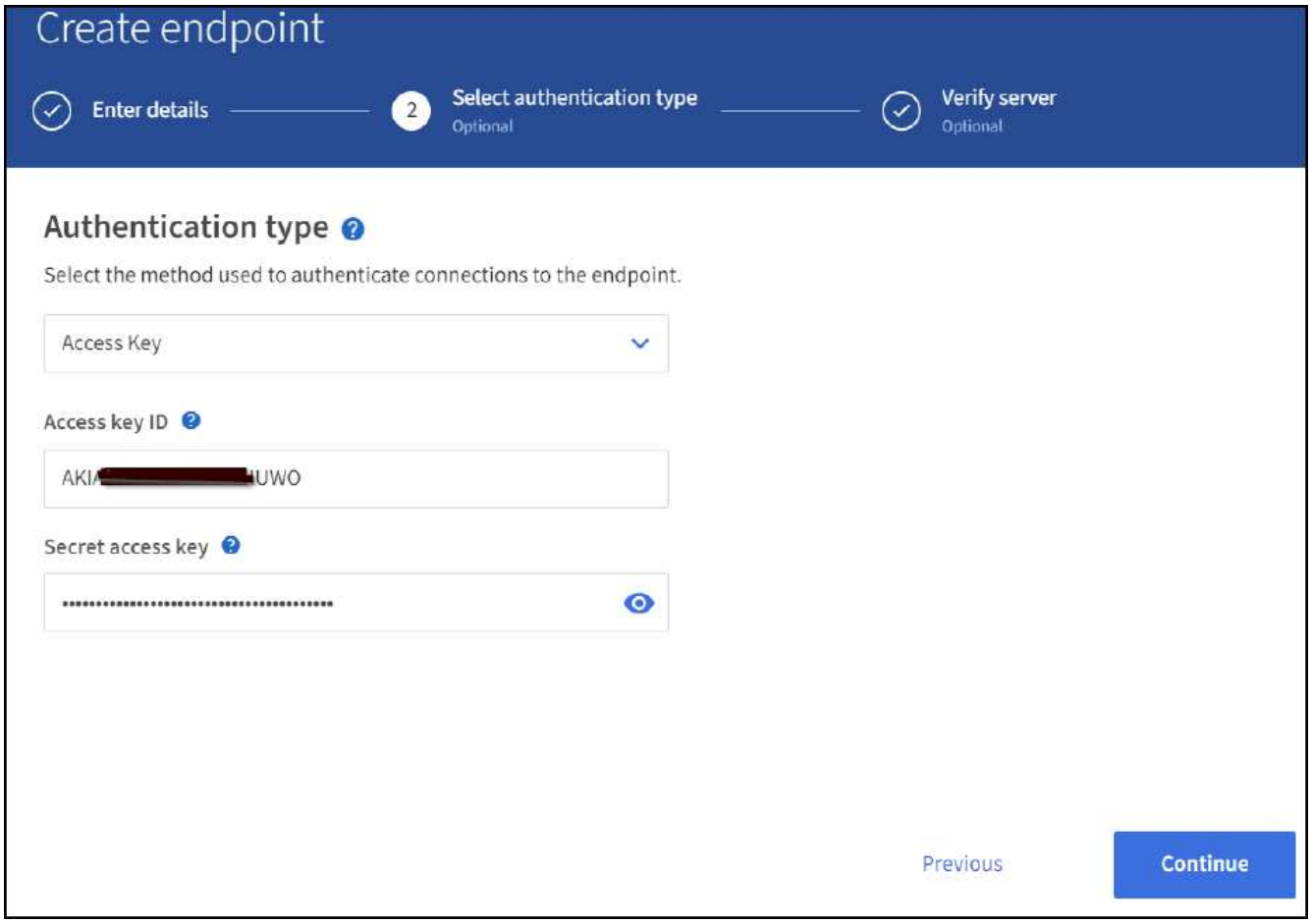
Para configurar os endpoints de serviços da plataforma, siga estas etapas:

1. No Tenant Manager, vá para STORAGE(S3) > endpoints de serviços de plataforma.
2. Clique em criar ponto final, introduza o seguinte e, em seguida, clique em continuar:
   - Exemplo de nome de exibição `aws-opensearch`
   - O endpoint do domínio na captura de tela de exemplo na Etapa 2 do procedimento anterior no campo URI.
   - O ARN de domínio utilizado na Etapa 2 do procedimento anterior no campo URNA e adicione `/<index>/_doc` ao final do ARN.

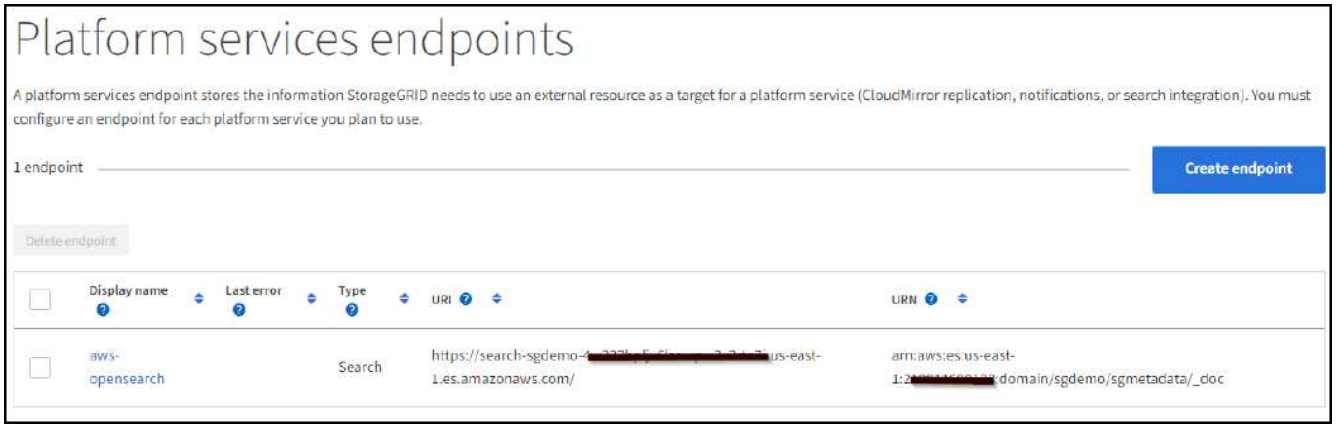
     Neste exemplo, A URNA torna `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`-se .



3. Para acessar o sgdomain do Amazon OpenSearch, escolha chave de acesso como o tipo de autenticação e insira a chave de acesso e chave secreta do Amazon S3. Para ir para a página seguinte, clique em continuar.



4. Para verificar o endpoint, selecione usar certificado e teste da CA do sistema operacional e criar endpoint. Se a verificação for bem-sucedida, é apresentado um ecrã de ponto de extremidade semelhante à figura seguinte. Se a verificação falhar, verifique se a URN inclui no final do caminho e se `/<index>/_doc` a chave de acesso da AWS e a chave secreta estão corretas.



PESQUISE serviços de integração com o Elasticsearch no local

Configuração do Elasticsearch no local

Este procedimento é para uma configuração rápida do Elasticsearch no local e do Kibana usando o docker apenas para fins de teste. Se o servidor Elasticsearch e Kibana já existir, vá para a Etapa 5.

1. Siga isso "Procedimento de instalação do Docker" para instalar o docker. Usamos o "Procedimento de instalação do Docker do CentOS"nesta configuração.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

   - Para iniciar o docker após a reinicialização, digite o seguinte:

```
sudo systemctl enable docker
```

   - Defina o `vm.max_map_count` valor como 262144:

```
sysctl -w vm.max_map_count=262144
```

   - Para manter a configuração após a reinicialização, digite o seguinte:

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. Siga a "Elasticsearch Guia de início rápido"seção autogerenciada para instalar e executar o Elasticsearch e o Kibana docker. Neste exemplo, instalamos a versão 8,1.

Observação abaixo o nome de usuário/senha e token criados pelo Elasticsearch, você precisa deles para iniciar a autenticação de endpoint da plataforma Kibana UI e StorageGRID.

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

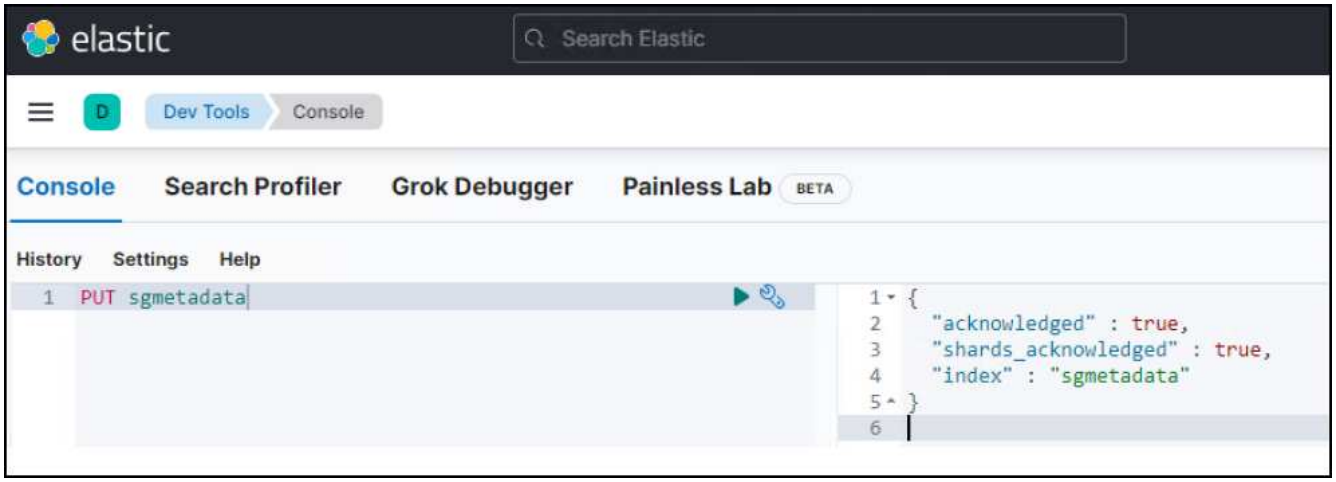
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

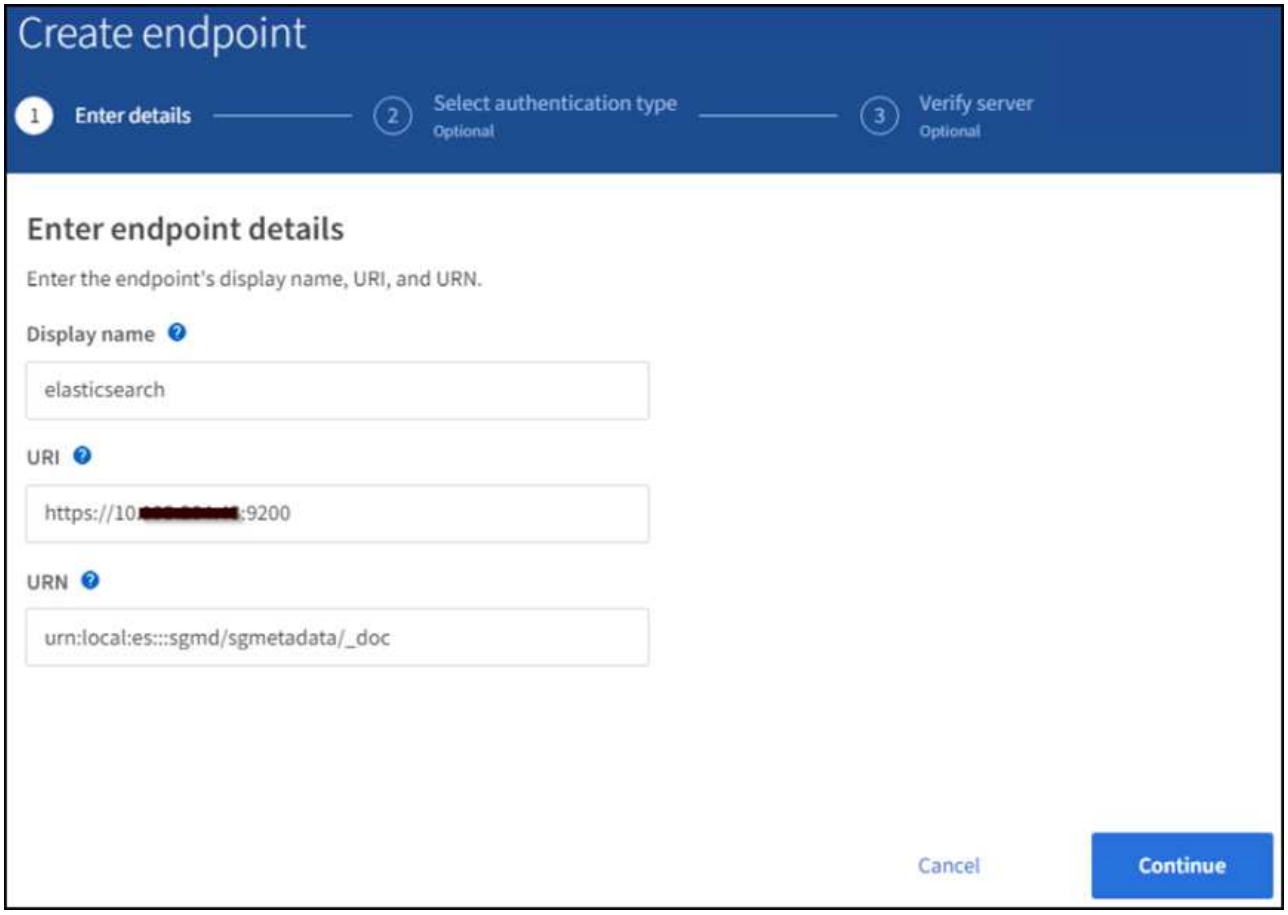
3. Depois que o contentor do Kibana docker for iniciado, o link URL `https://0.0.0.0:5601` será exibido no console. Substitua 0.0.0.0 pelo endereço IP do servidor no URL.
4. Faça login na IU do Kibana usando o nome de `elastic` usuário e a senha gerada pelo Elastic na etapa anterior.
5. Para iniciar sessão pela primeira vez, na página de boas-vindas do painel, selecione explorar por conta própria. No menu, selecione Gestão > Ferramentas de desenvolvimento.
6. Na tela Console de Ferramentas de Desenvolvimento, digite `PUT <index>` onde você usa esse índice para armazenar metadados de objetos do StorageGRID. Usamos o nome do índice `sgmetadata` neste exemplo. Clique no símbolo de triângulo pequeno para executar o comando PUT. O resultado esperado é exibido no painel direito, como mostrado no exemplo de captura de tela a seguir.



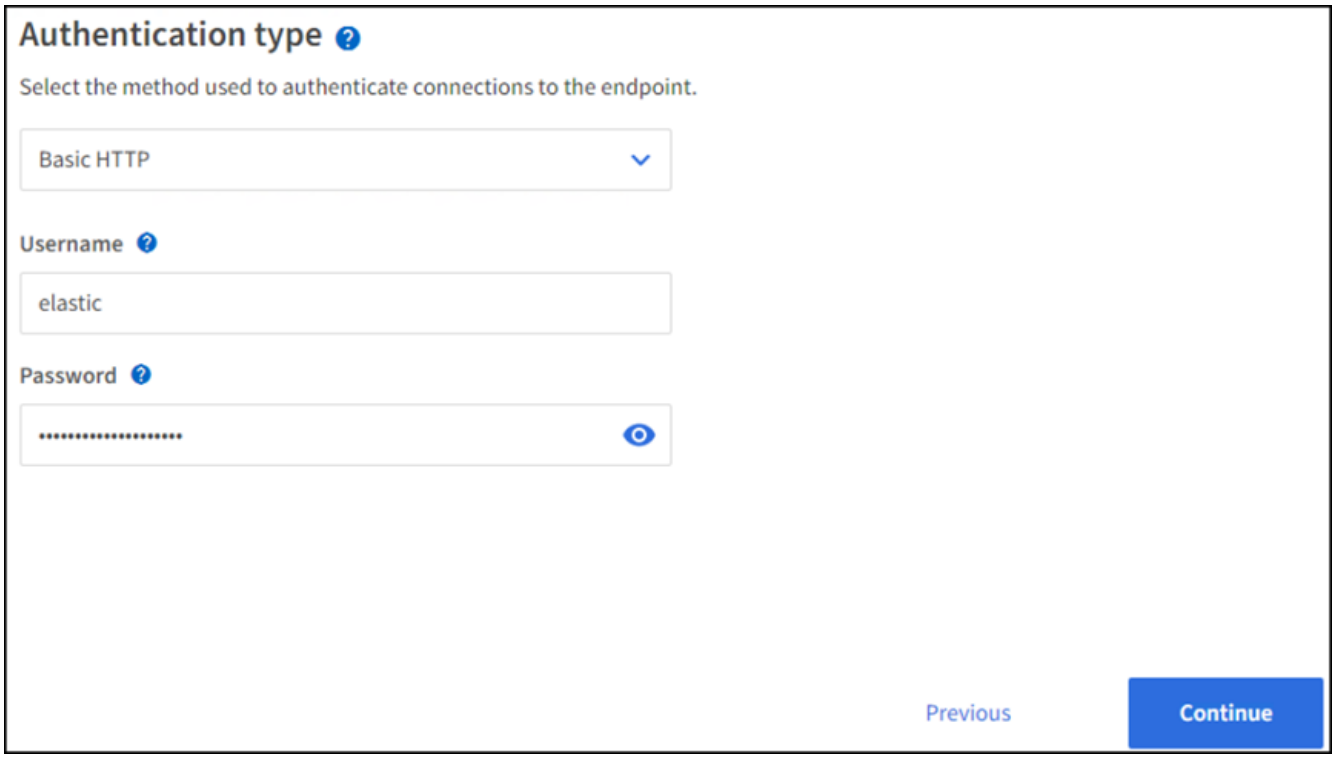
Configuração de endpoint de serviços de plataforma

Para configurar endpoints para serviços de plataforma, siga estas etapas:

1. No Tenant Manager, vá para STORAGE(S3) > endpoints de serviços de plataforma
2. Clique em criar ponto final, introduza o seguinte e, em seguida, clique em continuar:
   - Exemplo de nome de exibição: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URN: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Onde o nome do índice é o nome que você usou no console do Kibana. Exemplo: `urn:local:es:::sgmd/sgmetadata/_doc`

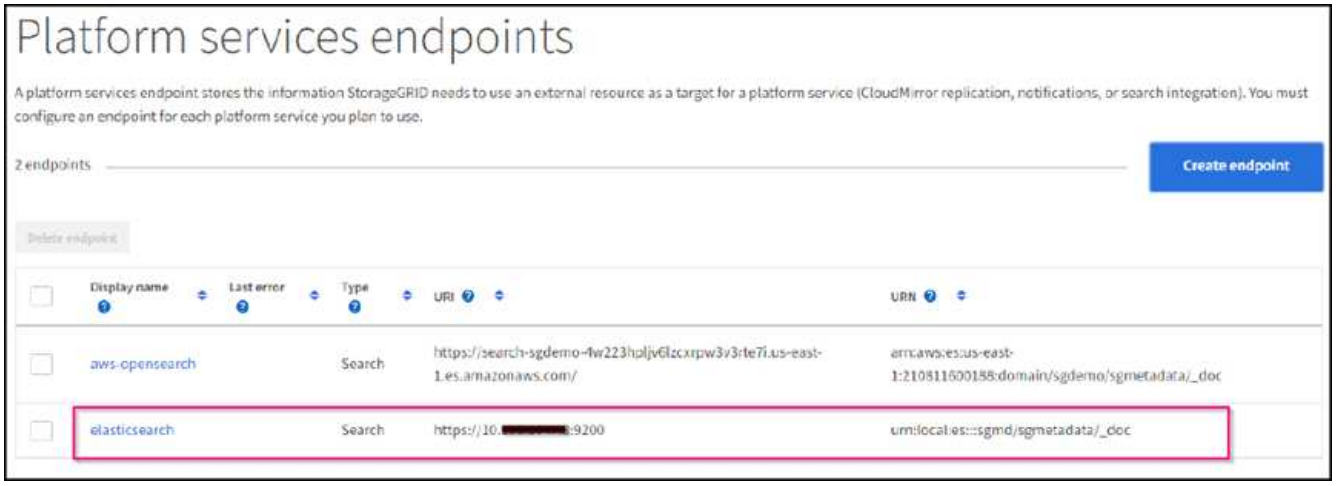


3. Selecione HTTP básico como o tipo de autenticação, insira o nome de `elastic` usuário e a senha gerados pelo processo de instalação do Elasticsearch. Para ir para a página seguinte, clique em continuar.



4. Selecione não verificar certificado e teste e criar endpoint para verificar o endpoint. Se a verificação for

bem-sucedida, uma tela de ponto final semelhante à seguinte captura de tela é exibida. Se a verificação falhar, verifique se as entradas URN, URI e nome de usuário/senha estão corretas.



Configuração do serviço de integração de pesquisa de bucket

Depois que o endpoint do serviço da plataforma é criado, a próxima etapa é configurar esse serviço no nível do bucket para enviar metadados de objeto para o endpoint definido sempre que um objeto é criado, excluído ou seus metadados ou tags são atualizados.

Você pode configurar a integração de pesquisa usando o Gerenciador do locatário para aplicar um XML de configuração StorageGRID personalizado a um bucket da seguinte forma:

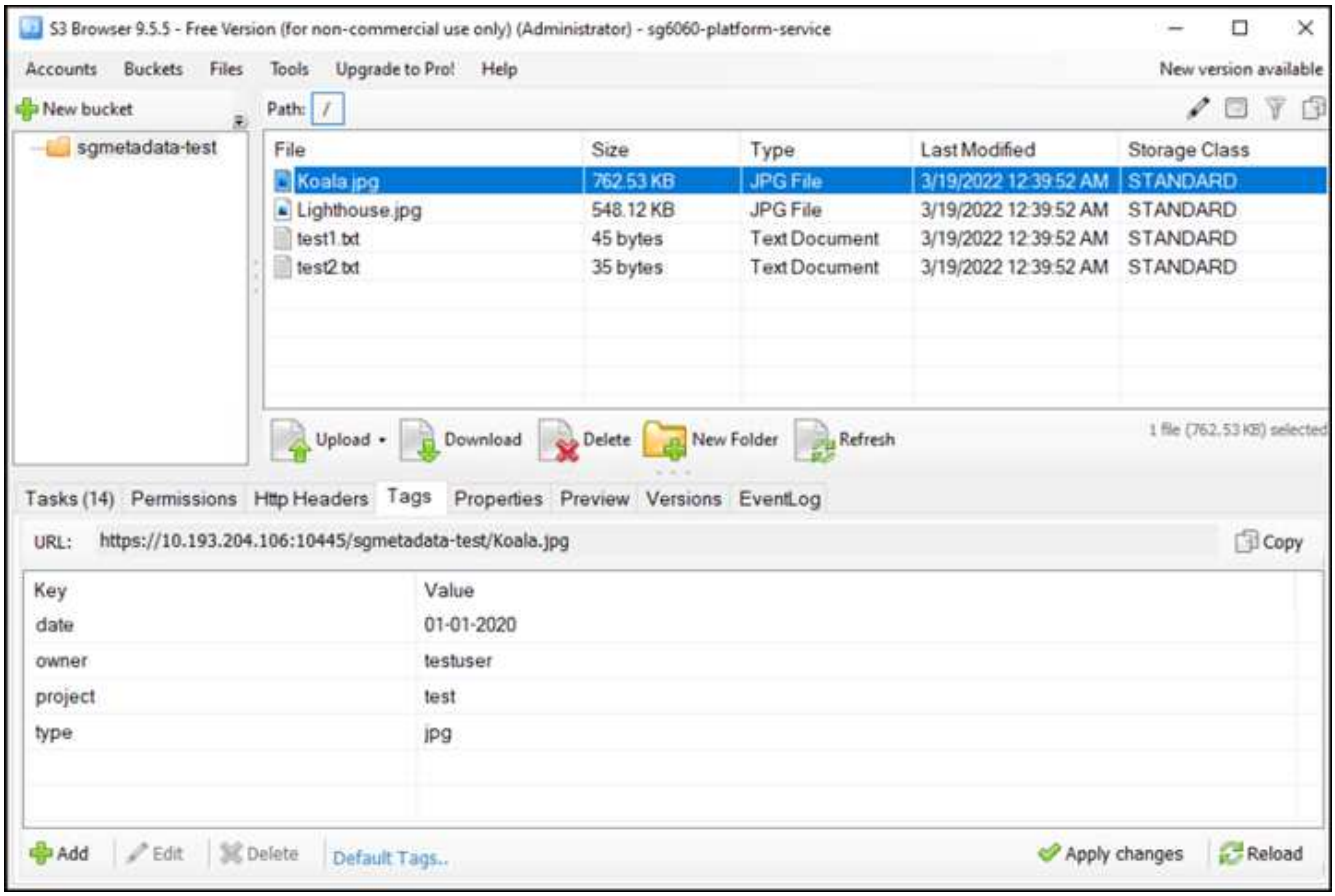
1. No Tenant Manager, aceda a STORAGE(S3) > baldes
2. Clique em criar balde, introduza o nome do balde (por exemplo, `sgmetadata-test`) e aceite a região predefinida `us-east-1`.
3. Clique em continuar > criar balde.
4. Para abrir a página Visão geral do bucket, clique no nome do bucket e selecione Serviços da plataforma.
5. Selecione a caixa de diálogo Ativar integração de pesquisa. Na caixa XML fornecida, insira o XML de configuração usando essa sintaxe.

   A URNA realçada deve corresponder ao endpoint de serviços da plataforma que você definiu. Você pode abrir outra guia do navegador para acessar o Gerenciador do Locatário e copiar a URN do endpoint de serviços da plataforma definido.

   Neste exemplo, não usamos nenhum prefixo, o que significa que os metadados de cada objeto neste intervalo são enviados para o endpoint Elasticsearch definido anteriormente.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. Use o navegador S3 para se conetar ao StorageGRID com a chave de acesso do locatário/segredo, carregue objetos de teste para `sgmetadata-test` bucket e adicione tags ou metadados personalizados a objetos.



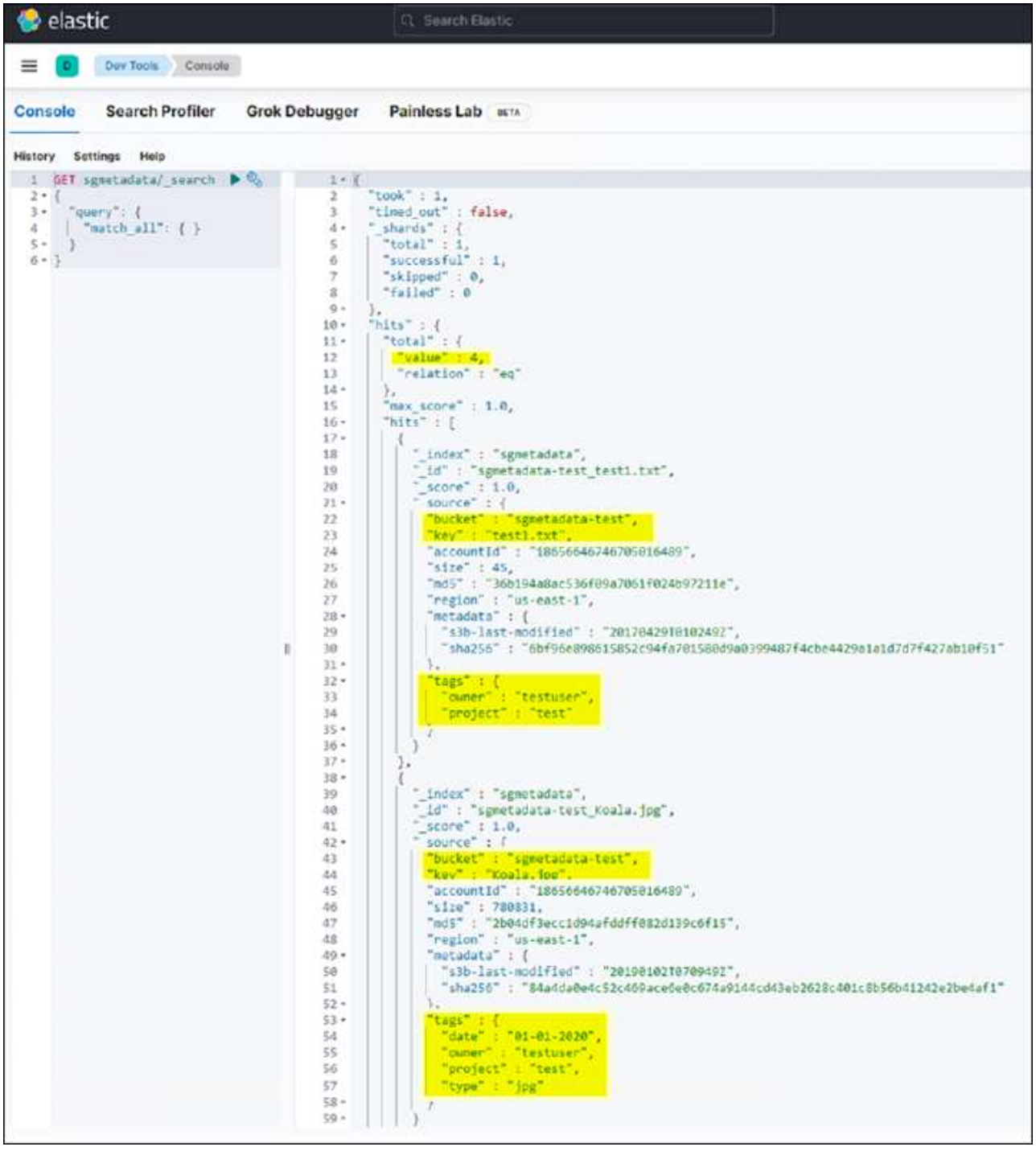
7. Use a IU do Kibana para verificar se os metadados do objeto foram carregados para o índice do sgmetadata.

   a. No menu, selecione Gestão > Ferramentas de desenvolvimento.

   b. Cole a consulta de exemplo no painel do console à esquerda e clique no símbolo do triângulo para executá-la.

      O resultado da amostra da consulta 1 na captura de tela de exemplo a seguir mostra quatro Registros. Isto corresponde ao número de objetos no balde.

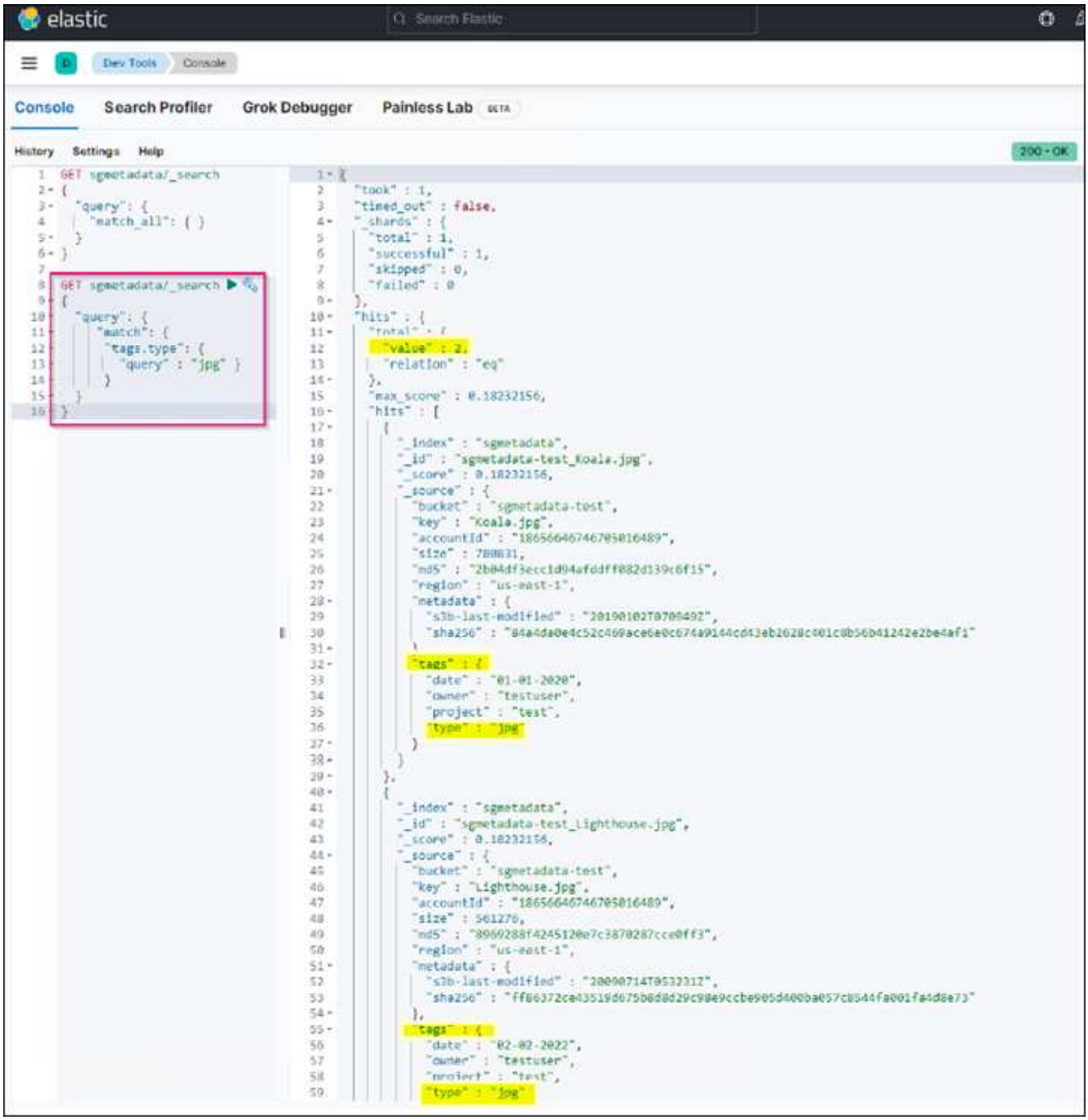
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



O resultado da amostra da consulta 2 na captura de tela a seguir mostra dois Registros com o tipo de tag jpg.

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



Onde encontrar informações adicionais

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

- "O que são serviços de plataforma"
- "Documentação do StorageGRID 11,6"

Por Angela Cheng

Clone de nó

Considerações e performance sobre o clone de nó.

Considerações sobre o clone de nó

O clone de nó pode ser um método mais rápido para substituir os nós de dispositivo existentes para uma atualização técnica, aumentar a capacidade ou aumentar a performance do seu sistema StorageGRID. O clone de nó também pode ser útil para converter para criptografia de nó com um KMS ou alterar um nó de storage de DDP8 para DDP16.

- A capacidade usada do nó de origem não é relevante para o tempo necessário para que o processo de clone seja concluído. Clone de nó é uma cópia completa do nó, incluindo espaço livre no nó.
- Os aparelhos de origem e destino devem estar na mesma versão PGE
- O nó de destino deve sempre ter capacidade maior do que a origem
  - Certifique-se de que o novo dispositivo de destino tem um tamanho de unidade maior do que a fonte
  - Se o utilitário de destino tiver unidades do mesmo tamanho e estiver configurado para DDP8, você poderá configurar o destino para DDP16. Se a origem já estiver configurada para DDP16, o clone do nó não será possível.
  - Ao passar de aparelhos SG5660 ou SG5760 para aparelhos SG6060, esteja ciente de que os SG5x60 têm unidades de capacidade de 60 TB, onde o SG6060 só tem 58 TB.
- O processo de clone de nó requer que o nó de origem fique off-line à grade durante o processo de clonagem. Se um nó adicional ficar offline durante este período, os serviços do cliente podem ser afetados.
- 11,8 e abaixo: Um nó de armazenamento só pode estar offline por 15 dias. Se a estimativa do processo de clonagem estiver próxima de 15 dias ou exceder 15 dias, use os procedimentos de expansão e desativação.
  - 11,9: O limite de 15 dias foi removido.
- Para um SG6060U ou SG6160U com compartimentos de expansão, você precisa adicionar o tempo para o tamanho correto da unidade de gaveta ao tempo do dispositivo base para obter a duração total do clone.
- O número de volumes em um dispositivo de storage de destino deve ser maior ou igual ao número de volumes no nó de origem. Você não pode clonar um nó de origem com 16 volumes de armazenamento de objetos (rangedb) para um dispositivo de storage de destino com 12 volumes de armazenamento de objetos, mesmo que o dispositivo de destino tenha maior capacidade do que o nó de origem. A maioria dos dispositivos de storage tem volumes de armazenamento de objetos de 16 TB, exceto o dispositivo de storage SGF6112 que tem apenas volumes de armazenamento de objetos de 12 TB. Por exemplo, você não pode clonar de um SG5760 para um SGF6112.

Estimativas de performance do clone de nó

As tabelas a seguir contêm estimativas calculadas para a duração do clone do nó. As condições variam assim, as entradas em **BOLD** podem correr o risco de exceder o limite de 15 dias para um nó para baixo.

DDP8

SG5612/SG5712/SG5812 → QUALQUER

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	1 dia	2 dias	2,5 dias	3 dias	4 dias	4,5 dias	5,5 dias
25 GB	1 dia	2 dias	2,5 dias	3 dias	4 dias	4,5 dias	5,5 dias

SG5660 → SG5760/SG5860

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	3,5 dia	7 dias	8,5 dias	10,5 dias	**13,5 dias**	**15,5 dias**	**18,5 dias**
25 GB	3,5 dia	7 dias	8,5 dias	10,5 dias	**13,5 dias**	**15,5 dias**	**18,5 dias**

SG5660 → SG6060/SG6160

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	2,5 dia	4,5 dias	5,5 dias	6,5 dias	9 dias	10 dias	**12 dias**
25 GB	2 dia	4 dias	5 dias	6 dias	8 dias	9 dias	10 dias

SG5760/SG5860 → SG5760/SG5860

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	3,5 dia	7 dias	8,5 dias	10,5 dias	**13,5 dias**	**15,5 dias**	**18,5 dias**

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
25 GB	3,5 dia	7 dias	8,5 dias	10,5 dias	**13,5 dias**	**15,5 dias**	**18,5 dias**

SG5760/SG5860 → SG6060/SG6160

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	2,5 dia	4,5 dias	5,5 dias	6,5 dias	9 dias	10 dias	**12 dias**
25 GB	2 dia	3,5 dias	4,5 dias	5,5 dias	7 dias	8 dias	9,5 dias

SG6060/SG6160 → SG6060/SG6160

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	2,5 dia	4,5 dias	5,5 dias	6,5 dias	8,5 dias	9,5 dias	11,5 dias
25 GB	2 dia	3 dias	4 dias	4,5 dias	6 dias	7 dias	8,5 dias

DDP16

SG5760/SG5860 → SG5760/SG5860

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	3,5 dia	6,5 dias	8 dias	9,5 dias	**12,5 dias**	**14 dias**	**17 dias**
25 GB	3,5 dia	6,5 dias	8 dias	9,5 dias	**12,5 dias**	**14 dias**	**17 dias**

SG5760/SG5860 → SG6060/SG6160

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	2,5 dia	5 dias	6 dias	7,5 dias	10 dias	11 dias	**13 dias**
25 GB	2 dia	3,5 dias	4 dias	5 dias	6,5 dias	7 dias	8,5 dias

SG6060/SG6160 → SG6060/SG6160

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	3 dia	5 dias	6 dias	7 dias	9,5 dias	10,5 dias	**13 dias**
25 GB	2 dia	3,5 dias	4,5 dias	5 dias	7 dias	7,5 dias	9 dias

Compartimento de expansão (adicione acima de SG6060/SG6160 para cada gaveta no dispositivo de origem)

Velocidade da interface de rede	4TB tamanho da unidade	8TB tamanho da unidade	10TB tamanho da unidade	12TB tamanho da unidade	16TB tamanho da unidade	18TB tamanho da unidade	22TB tamanho da unidade
10 GB	3,5 dia	5 dias	6 dias	7 dias	9,5 dias	10,5 dias	**12 dias**
25 GB	2 dia	3 dias	4 dias	4,5 dias	6 dias	7 dias	8,5 dias

Por Aron Klein

Como utilizar o remapeamento de portas

Pode ser necessário remapear uma porta de entrada ou de saída por vários motivos. Você pode estar migrando do serviço de balanceador de carga CLB legado para o endpoint de balanceador de carga de serviço nginx atual e manter a mesma porta para reduzir o impactos para os clientes, deseja usar a porta 443 para o cliente S3 em uma rede de cliente de nó de administrador ou para restrições de firewall.

Migre clientes S3 do CLB para O NGINX com o Port Remap

Em versões anteriores ao StorageGRID 11,3, o serviço de balanceamento de carga incluído nos nós de gateway é o CLB (Connection Load Balancer). No StorageGRID 11,3, o NetApp apresenta o serviço NGINX como uma solução integrada rica em recursos para balanceamento de carga de tráfego HTTP(s). Como o serviço CLB permanece disponível na versão atual do StorageGRID, não é possível reutilizar a porta 8082 na nova configuração de endpoint do balanceador de carga. Para contornar isso, a porta de entrada 8082 é

remapeada para 10443. Isso faz com que todas as solicitações HTTPS que entram na porta 8082 no gateway redirecionem para a porta 10443, ignorando o serviço CLB e, em vez disso, conetando-se ao serviço NGINX. Embora as instruções a seguir sejam para VMware, a funcionalidade port_REMAP existe para todos os métodos de instalação e você pode usar um processo semelhante para implantações e dispositivos bare metal.

Implantação do VMware Virtual Machine Gateway Node

As etapas a seguir são para uma implantação do StorageGRID em que o nó ou nós de gateway são implantados no VMware vSphere 7 como VMs usando o formato de virtualização aberta (OVF) do StorageGRID. O processo implica remover destrutivamente a VM e reimplantar a VM com o mesmo nome e configuração. Antes de ligar a VM, altere a propriedade vApp para remapear a porta, ligue a VM e siga o processo de recuperação do nó.

Pré-requisitos

- Você está executando o StorageGRID 11,3 ou posterior
- Você baixou e tem acesso aos arquivos de instalação VMware da versão do StorageGRID instalada.
- Você tem uma conta do vCenter com permissões para ligar/desligar VMs, alterar as configurações das VMs e vApps, remover VMs do vCenter e implantar VMs pelo OVF.
- Você criou um ponto de extremidade do balanceador de carga
  - A porta está configurada para a porta de redirecionamento desejada
  - O certificado SSL de endpoint é o mesmo que instalado para o serviço CLB no certificado servidor de Endpoints do Serviço de API de armazenamento de objetos ou o cliente pode aceitar uma alteração no certificado.

> ⓘ
>
> ```
> If your existing certificate is self-signed, you cannot reuse it
> in the new endpoint. You must generate a new self-signed
> certificate when creating the endpoint and configure the clients
> to accept the new certificate.
> ```

Destrua o primeiro nó de gateway

Para destruir o primeiro nó de gateway, siga estes passos:

1. Escolha o nó de gateway com o qual começar se a grade contiver mais de um.
2. Remova os IPs de nós de todas as entidades de round-robin DNS ou pools de balanceadores de carga, se aplicável.
3. Aguarde até que as sessões Time-to-Live (TTL) e Open expirem.
4. Desligue o nó da VM.
5. Remova o nó da VM do disco.

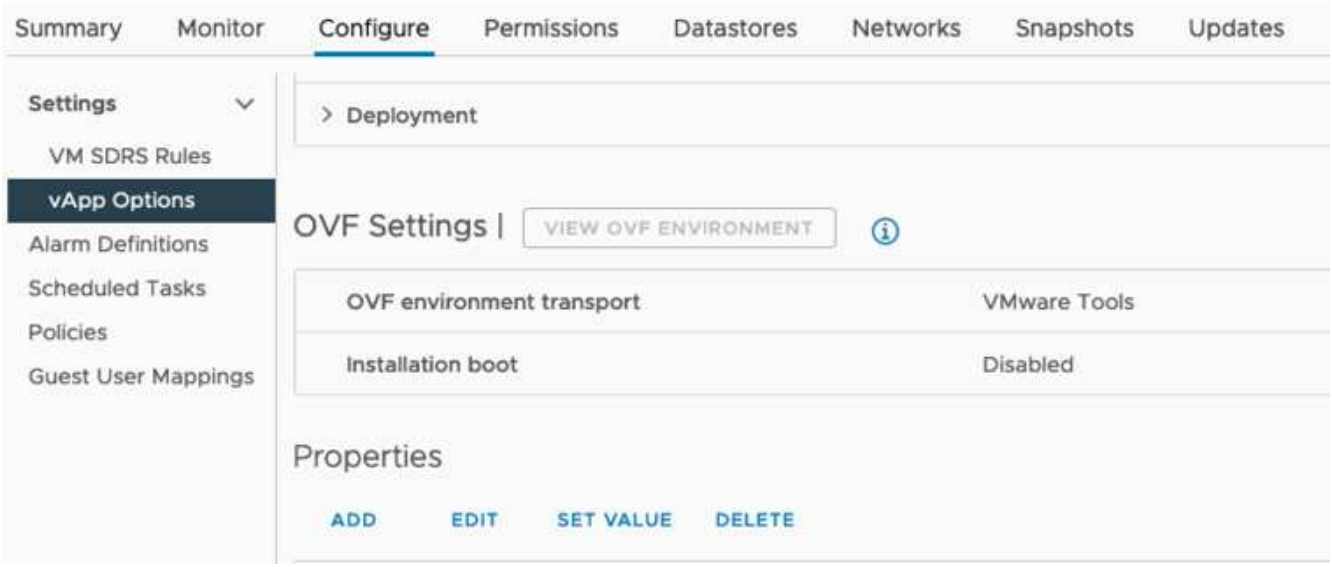
Implante o nó de gateway de substituição

Para implantar o nó de gateway de substituição, siga estas etapas:

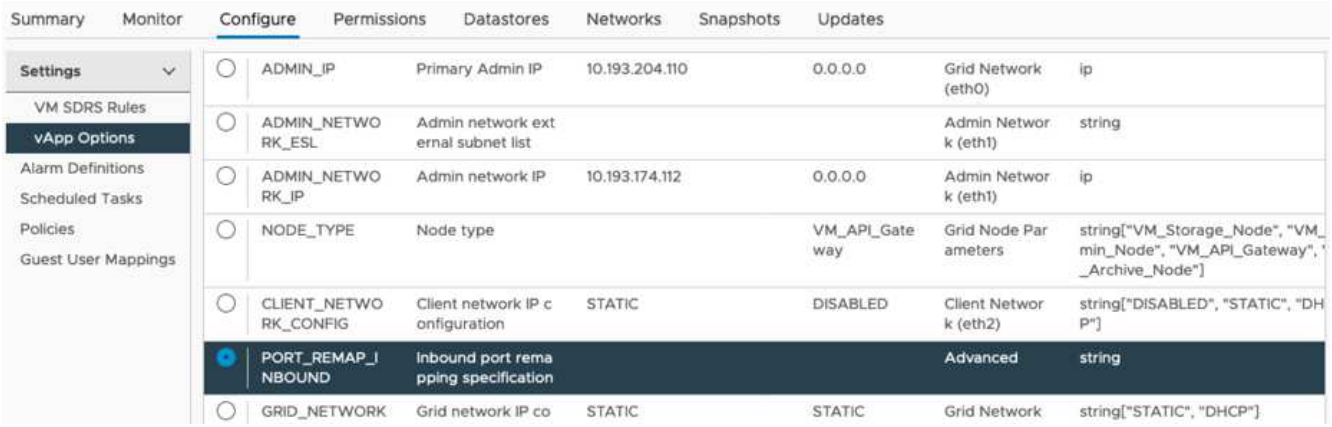
1. Implante a nova VM do OVF, selecionando os arquivos .ovf, .mf e .vmdk do pacote de instalação baixado do site de suporte:

- vsphere-gateway.mf
- vsphere-gateway.ovf
- NetApp-SG-11,4.0-20200721,1338.d3969b3.vmdk

2. Depois que a VM tiver sido implantada, selecione-a na lista de VMs, selecione a guia Configurar opções vApp.



3. Role para baixo até a seção Propriedades e selecione a propriedade PORT_REMAP_INBOUND

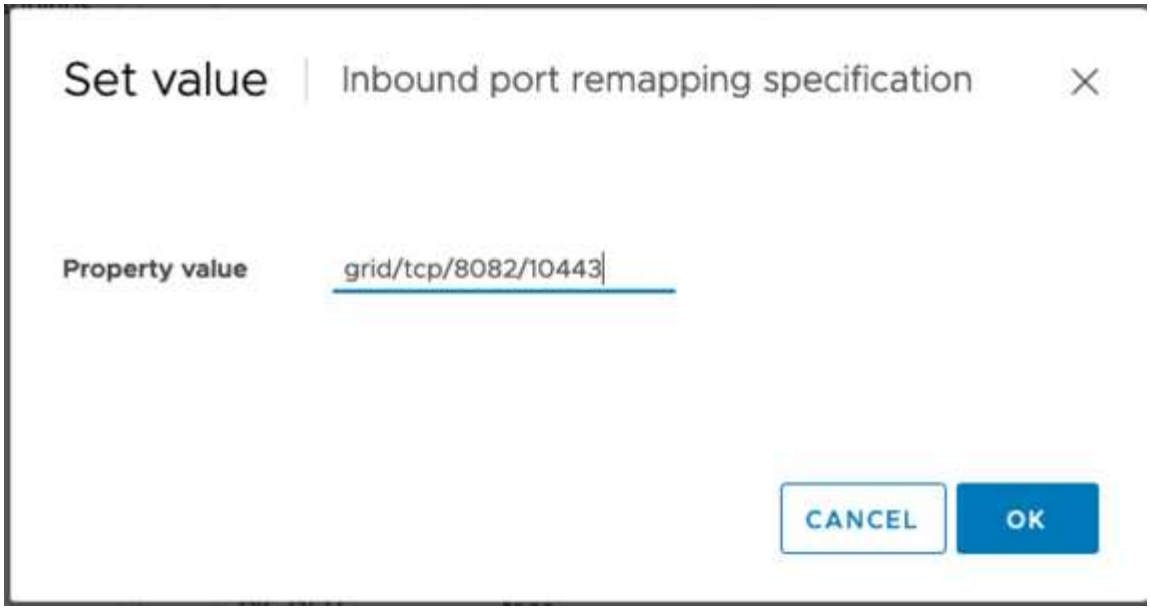


4. Role até o topo da lista Propriedades e clique em Editar

5. Selecione o separador tipo, confirme se a caixa de verificação configurável pelo utilizador está selecionada e, em seguida, clique em Guardar.

6. Na parte superior da lista Propriedades, com a propriedade "PORT_REMAP_INBOUND" ainda selecionada, clique em Definir valor.

7. No campo valor da propriedade, insira a rede (grade, administrador ou cliente), TCP, a porta original (8082) e a nova porta (10443) com "/" entre cada valor, conforme descrito a seguir.

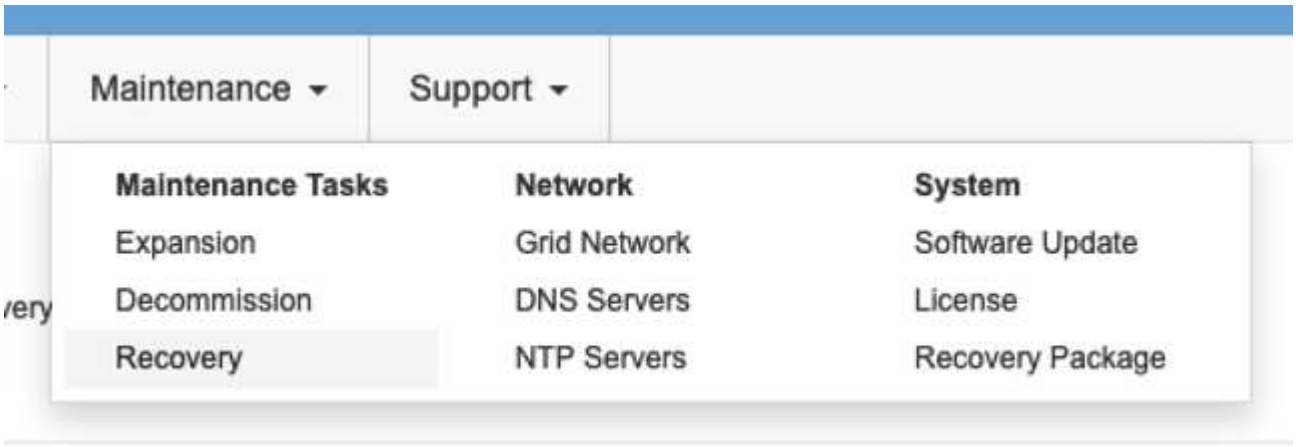


8. Se você estiver usando várias redes, use uma vírgula (,) para separar as cadeias de rede, por exemplo, Grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

Recupere o nó de gateway

Para recuperar o Gateway Node, siga estas etapas:

1. Navegue até a seção Manutenção/recuperação da IU de Gerenciamento de Grade.



2. Ligue o nó da VM e aguarde que o nó apareça na seção Maintenance/Recovery Pending Nodes da IU de Gerenciamento de Grade.

> For information and directions for node recovery, see the https://docs.netapp.com/sgws-114/topic/com.netapp.doc.sg-maint/GUID-7E22B1B9-4169-4800-8727-75F25FC0FFB1.html[Recovery and Maintenance guide]

3. Após a recuperação do nó, o IP pode ser incluído em todas as entidades de round-robin DNS ou pools de balanceadores de carga, se aplicável.

   Agora, todas as sessões HTTPS na porta 8082 vão para a porta 10443

Remapear a porta 443 para acesso ao cliente S3 em um nó Admin

A configuração padrão no sistema StorageGRID para um nó de administrador ou grupo de HA que contém um nó de administrador deve ser 443 reservada para as interfaces de usuário do gerenciador de gerenciamento e locatário e não pode ser usada para pontos de extremidade do balanceador de carga 80. A solução para isso é usar o recurso de remapeamento de portas e redirecionar a porta de entrada 443 para uma nova porta que será configurada como um ponto de extremidade do balanceador de carga. Uma vez que esse tráfego do Cliente S3 concluído será capaz de usar a porta 443, a IU de gerenciamento de grade só estará acessível através da porta 8443 e a IU de gerenciamento do locatário só estará acessível na porta 9443. O recurso de remapeamento de porta só pode ser configurado no momento da instalação do nó. Para implementar um remapeamento de portas de um nó ativo na grade, ele deve ser redefinido para o estado pré-instalado. Este é um procedimento destrutivo que inclui uma recuperação de nó uma vez que a alteração de configuração foi feita.

Backup de logs e bancos de dados

Os nós de administração contêm logs de auditoria, métricas de prometheus, bem como informações históricas sobre atributos, alarmes e alertas. Ter vários nós de administração significa que você tem várias cópias desses dados. Se você não tiver vários nós de administrador em sua grade, você deve se certificar de preservar esses dados para restaurar após o nó ter sido recuperado no final deste processo. Se você tiver outro nó de administrador na grade, você poderá copiar os dados desse nó durante o processo de recuperação. Se você não tiver outro nó de administrador na grade, você pode seguir estas instruções para copiar os dados antes de destruir o nó.

Copiar registos de auditoria

1. Faça login no nó Admin:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Criar o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado permite usar *storage_node_01*:

   a. `ssh admin@storage_node_01_IP`

   b. `mkdir -p /var/local/tmp/saved-audit-logs`

3. De volta ao nó admin, pare o serviço AMS para impedir que ele crie um novo arquivo de log: `service ams stop`

4. Renomeie o arquivo audit.log para que ele não substitua o arquivo existente quando você copiá-lo para o nó Admin recuperado.

   a. Renomeie audit.log para um nome de arquivo numerado exclusivo, como aaaa-mm-dd.txt.1. Por exemplo, você pode renomear o arquivo de log de auditoria para 2015-10-25.txt,1

```
cd /var/local/audit/export
ls -l
mv audit.log 2015-10-25.txt.1
```

5. Reinicie o serviço AMS: `service ams start`

6. Copiar todos os ficheiros de registo de auditoria: `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Copiar dados Prometheus

Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no nó Admin.

1. Crie o diretório para copiar os dados prometheus para um local temporário em um nó de grade separado, novamente utilizaremos *storage_node_01*:

   a. Faça login no nó de storage:

      i. Introduza o seguinte comando: `ssh admin@storage_node_01_IP`

      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      iii. mkdir -p /var/local/tmp/prometheus'

2. Faça login no nó Admin:

   a. Introduza o seguinte comando: `ssh admin@admin_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

3. No Admin Node, pare o serviço Prometheus: `service prometheus stop`

   a. Copie o banco de dados Prometheus do nó de administração de origem para o nó de armazenamento local de backup Node: `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" " storage_node_01_IP:/var/local/tmp/prometheus/"`

4. Reinicie o serviço Prometheus no Admin Node de origem.`service prometheus start`

Backup de informações históricas

As informações históricas são armazenadas em um banco de dados mysql. Para descarregar uma cópia do banco de dados, você precisará do usuário e da senha do NetApp. Se você tiver outro nó de administrador na grade, essa etapa não será necessária e o banco de dados poderá ser clonado de um nó de administrador restante durante o processo de recuperação.

1. Faça login no nó Admin:

   a. Introduza o seguinte comando: `ssh admin@admin_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

   f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Pare os serviços do StorageGRID no nó Admin e inicie o NTP e mysql

   a. Parar todos os serviços: `service servermanager stop`

   b. reinicie o serviço ntp: `service ntp start` ..reinicie o serviço mysql: `service mysql start`

3. Dump mi banco de dados para /var/local/tmp

   a. introduza o seguinte comando: `mysqldump –u username –p password mi > /var/local/tmp/mysql-mi.sql`

4. Copie o arquivo de despejo mysql para um nó alternativo, vamos usar *storage_node_01: scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP:/var/local/tmp/mysql-mi.sql*

a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`

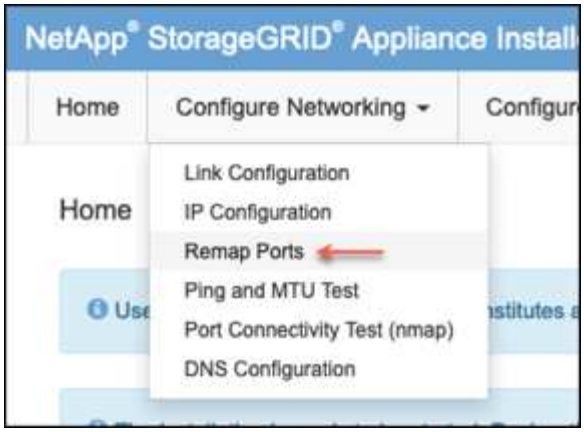
Reconstrua o nó Admin

Agora que você tem uma cópia de backup de todos os dados e logs desejados em outro nó de administrador na grade ou armazenados em um local temporário, é hora de redefinir o dispositivo para que o remapa de portas possa ser configurado.

1. A redefinição de um appliance retorna ao estado pré-instalado, onde ele só retém o nome do host, IP e configurações de rede. Todos os dados serão perdidos e é por isso que nos certificamos de ter um backup de qualquer informação importante.
   a. introduza o seguinte comando: `sgareinstall`

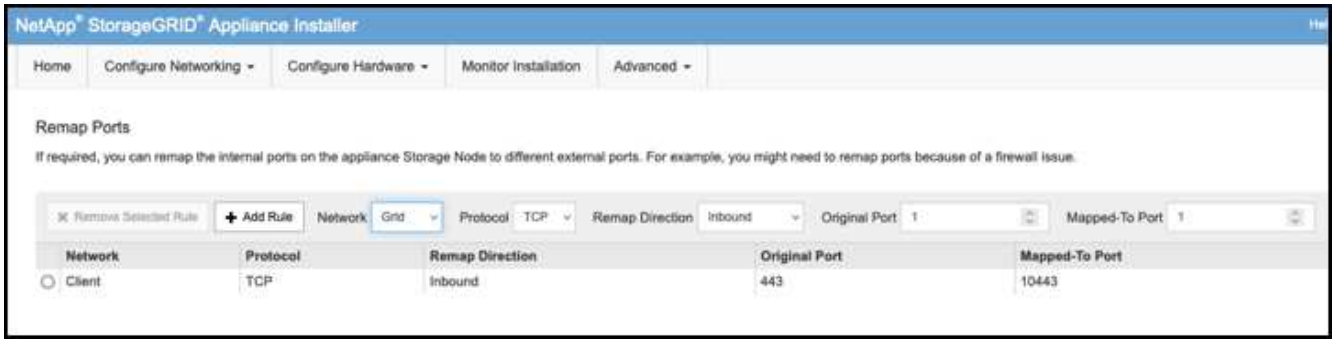
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

After running this command and waiting a few minutes for the node to
reboot,
browse to one of the following URLs to reinstall StorageGRID Webscale
on
this node:

    https://10.193.174.192:8443
    https://10.193.204.192:8443
    https://169.254.0.1:8443

Are you sure you want to continue (y/n)? y
Renaming SG installation flag file.
Initiating a reboot to trigger the StorageGRID Webscale appliance
installation wizard.
```

2. Após algum tempo, o aparelho reiniciará e você poderá acessar o nó PGE UI.
3. Navegue até Configurar rede



4. Selecione a rede, o protocolo, a direção e as portas pretendidas e, em seguida, clique no botão Adicionar regra.

> O remapeamento da porta de entrada 443 na REDE DE GRADE interromperá a instalação e os procedimentos de expansão. Não é recomendável remapear a porta 443 na rede DE GRADE.



5. Um dos remapas de portas desejados foi adicionado, você pode retornar à guia inicial e clicar no botão Iniciar instalação.

Pode agora seguir os procedimentos de recuperação do nó Admin no "documentação do produto"

Restaure bancos de dados e logs

Agora que o nó de administrador foi recuperado, você pode restaurar as métricas, logs e informações históricas. Se você tiver outro nó de administrador na grade, siga os "documentação do produto"scripts utilizando *prometheus-clone-dB.sh* e *mi-clone-dB.sh*. Se este for o seu único nó de administrador e você optar por fazer backup desses dados, siga as etapas abaixo para restaurar as informações.

Copiar registos de auditoria de volta

1. Faça login no nó Admin:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.
4. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado: `chown ams-user:bycast *`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

Restaurar métricas Prometheus

Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no nó Admin.

1. Faça login no nó Admin:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
   f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. No Admin Node, pare o serviço Prometheus: `service prometheus stop`
   a. Copie o banco de dados Prometheus do local de backup temporário para o nó de administrador: `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. verifique se os dados estão no caminho correto e estão completos `ls /var/local/mysql_ibdata/prometheus/data/`
3. Reinicie o serviço Prometheus no Admin Node de origem.`service prometheus start`

Restaurar informações históricas

1. Faça login no nó Admin:

a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Copie o arquivo de despejo mysql do nó alternativo: `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. Pare os serviços do StorageGRID no nó Admin e inicie o NTP e mysql
   a. Parar todos os serviços: `service servermanager stop`
   b. reinicie o serviço ntp: `service ntp start` ..reinicie o serviço mysql: `service mysql start`
4. Solte o banco de dados mi e crie um novo banco de dados vazio: `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. restaure o banco de dados mysql a partir do despejo do banco de dados: `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. Reinicie todos os outros serviços `service servermanager start`

Por Aron Klein

Procedimento de realocação do local da grade e mudança de rede em todo o local

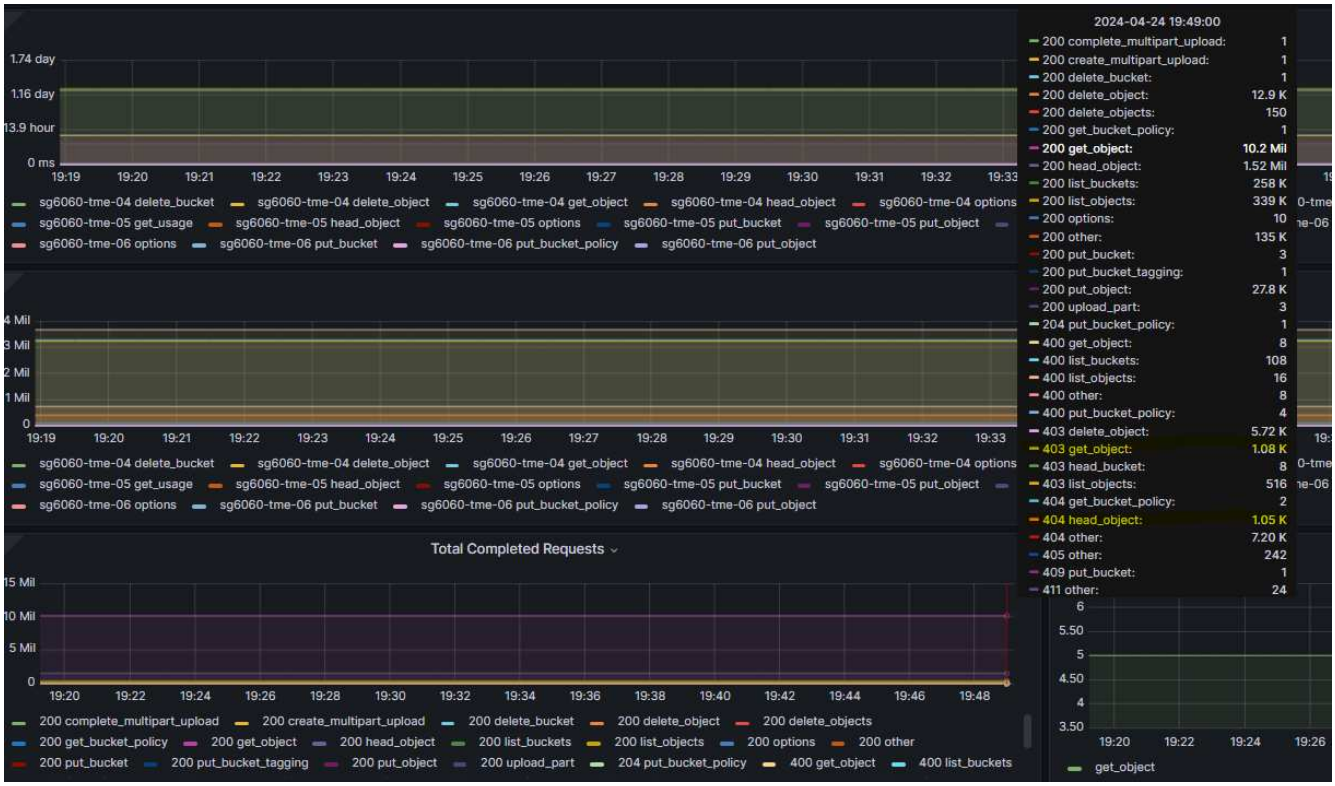
Este guia descreve a preparação e o procedimento para a realocação do local do StorageGRID em uma grade de vários locais. Você deve ter uma compreensão completa deste procedimento e Planejar com antecedência para garantir um processo suave e minimizar a interrupção para os clientes.

Se você precisar alterar a rede de Grade inteira, "Altere endereços IP para todos os nós na grade"consulte .

Considerações antes da realocação do local

- A movimentação do local deve ser concluída e todos os nós on-line em até 15 dias para evitar a reconstrução do banco de dados Cassandra. "Recupere o nó de storage abaixo mais de 15 dias"
- Se qualquer regra de ILM na política ativa estiver usando comportamento de ingestão rigoroso, considere alterá-la para equilibrar ou se o cliente quiser continuar A COLOCAR objetos na grade durante a realocação do local.
- Para dispositivos de storage com 60 unidades ou mais, nunca mova a gaveta com unidades de disco instaladas. Rotule cada unidade de disco e remova-as do compartimento de armazenamento antes de embalar/mover.

- A VLAN da rede da grade do StorageGRID pode ser executada remotamente pela rede admin ou pela rede cliente. Ou então Planeje estar no local para realizar a mudança antes ou depois da realocação.
- Verifique se o aplicativo do cliente está usando HEAD ou OBTER objeto de não existência antes DE COLOCAR. Em caso afirmativo, altere a consistência do bucket para strong-site para evitar o erro HTTP 500. Se não tiver certeza, verifique S3 visão geral gráficos Grafana **Gerenciador de Grade > suporte > métricas**, passe o Mouse sobre o gráfico 'Total Completed Request'. Se houver uma contagem muito alta de 404 Get Object ou 404 head object, provavelmente uma ou mais aplicações estão usando head ou get nonexistence object. A contagem é acumulativa, passe o Mouse sobre a linha do tempo diferente para ver a diferença.



Procedimento para alterar o endereço IP da grade antes da realocação do local

Passos

1. Se a nova sub-rede da rede Grid for usada no novo local, "Adicione a sub-rede à lista de sub-rede da rede Grid"
2. Faça login no nó de administração principal, use o Change-ip para fazer a alteração de IP de grade, deve **stage** a alteração antes de desligar o nó para realocação.
   a. Selecione 2 e, em seguida, 1 para a alteração de IP de Grade

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. selecione 5 para mostrar as alterações

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

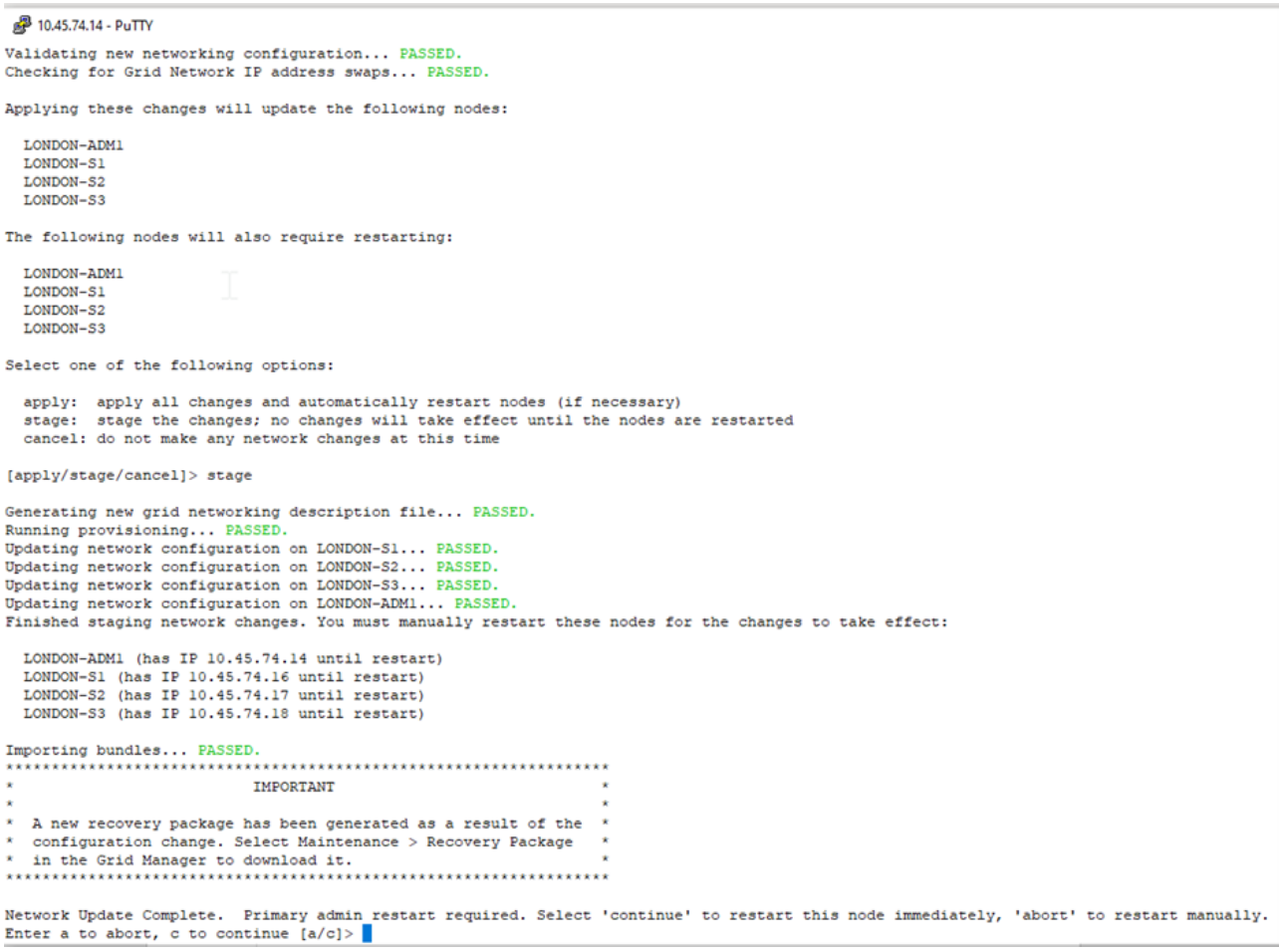
c. selecione 10 para validar e aplicar a alteração.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

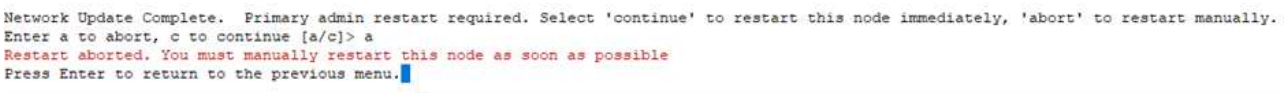
d. Deve selecionar **stage** nesta etapa.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. Se o nó de administrador principal estiver incluído na alteração acima, digite **'a' para reiniciar o nó de administrador principal manualmente**



f. Prima ENTER para regressar ao menu anterior e sair da interface Change-ip.



3. No Grid Manager, baixe o novo pacote de recuperação. **Gerenciador de grade** > **Manutenção** > **Pacote de recuperação**
4. Se a alteração de VLAN for necessária no dispositivo StorageGRID, consulte a Alteração da VLAN do dispositivoseção .
5. Encerre todos os nós e/ou dispositivos no local, rotule/remova as unidades de disco, se necessário, desprenda, embale e mova.
6. Se você planeja alterar o ip da rede de administração e/ou a VLAN do cliente e o endereço ip, poderá realizar a alteração após a realocação.

Alteração da VLAN do dispositivo

O procedimento abaixo assume que você tem acesso remoto ao administrador ou à rede cliente do StorageGRID Appliance para executar a alteração remotamente.

Passos

1. Antes de desligar o aparelho, "coloque o aparelho no modo de manutenção".
2. Usando um navegador para acessar a GUI do instalador do StorageGRID Appliance usando https://<admin-or-client-network-ip>:8443o . Não é possível usar o Grid IP como o novo Grid IP já no lugar

quando o aparelho for inicializado no modo de manutenção.

3. Altere a VLAN da rede Grid. Se você estiver acessando o dispositivo pela rede cliente, não poderá alterar a VLAN do cliente neste momento, poderá alterá-la após a movimentação.
4. ssh para o dispositivo e desligue o nó usando 'shutdoown -h now'
5. Depois que os dispositivos estiverem prontos em um novo site, acesse a GUI do instalador do StorageGRID Appliance usando https://<grid-network-ip>:8443o . Confirme se o armazenamento está em ótimo estado e conetividade de rede com outros nós de Grade usando ferramentas de ping/nmap na GUI.
6. Se pretende alterar o IP da rede do cliente, pode alterar a VLAN do cliente nesta fase. A rede do cliente não estará pronta até atualizar o ip da rede do cliente usando a ferramenta Change-ip na etapa posterior.
7. Sair do modo de manutenção. No Instalador de dispositivos StorageGRID, selecione **Avançado** > **Reiniciar controlador** e, em seguida, selecione **Reiniciar no StorageGRID**.
8. Depois que todos os nós estiverem ativos e Grid não mostrar nenhum problema de conetividade, use Change-ip para atualizar a rede de administração do dispositivo e a rede cliente, se necessário.

Migração de storage baseado em objetos do ONTAP S3 para o StorageGRID

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Demonstração de migração

Esta é uma demonstração sobre a migração de usuários e buckets do ONTAP S3 para o StorageGRID.

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

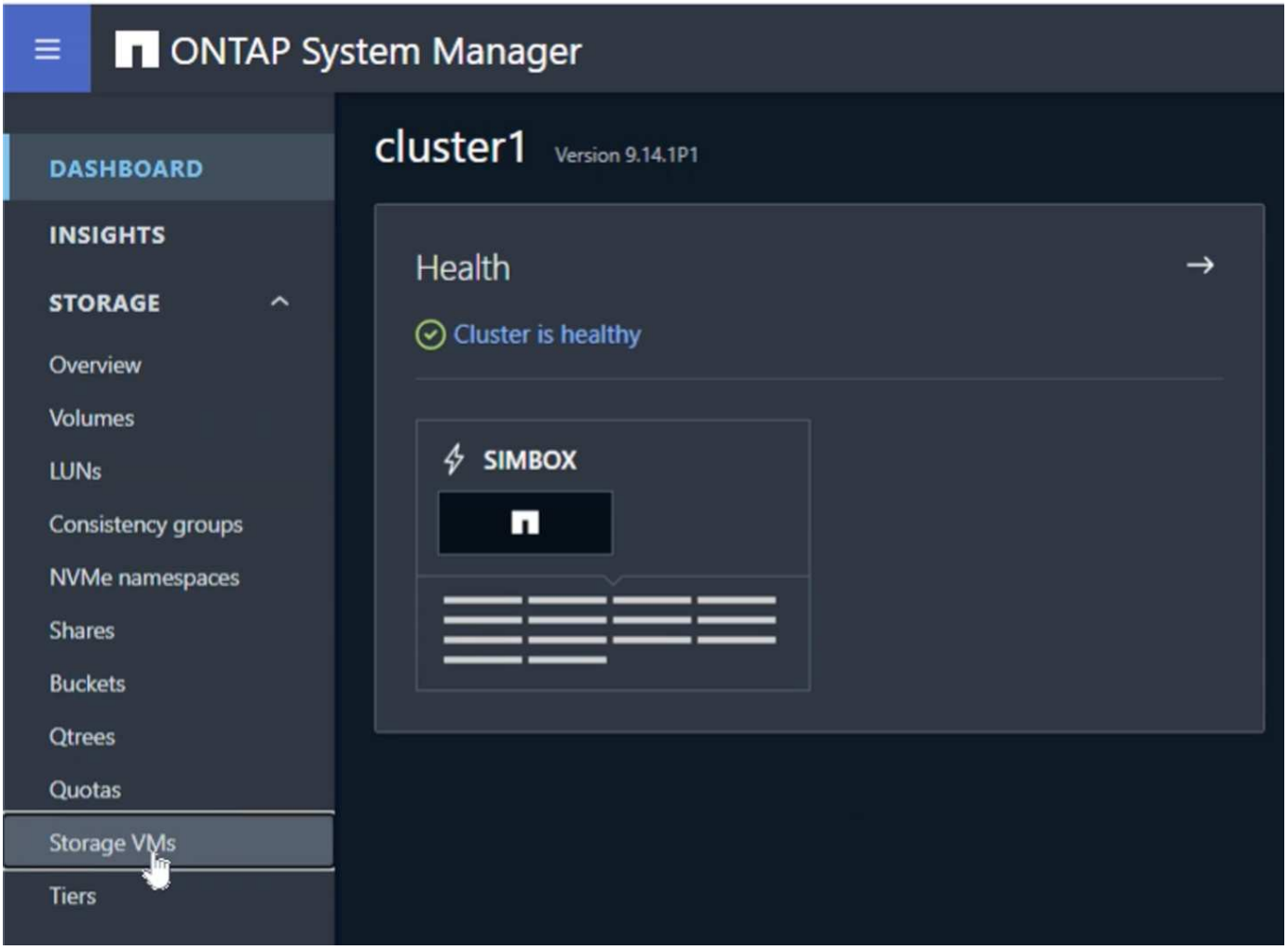
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Preparando o ONTAP

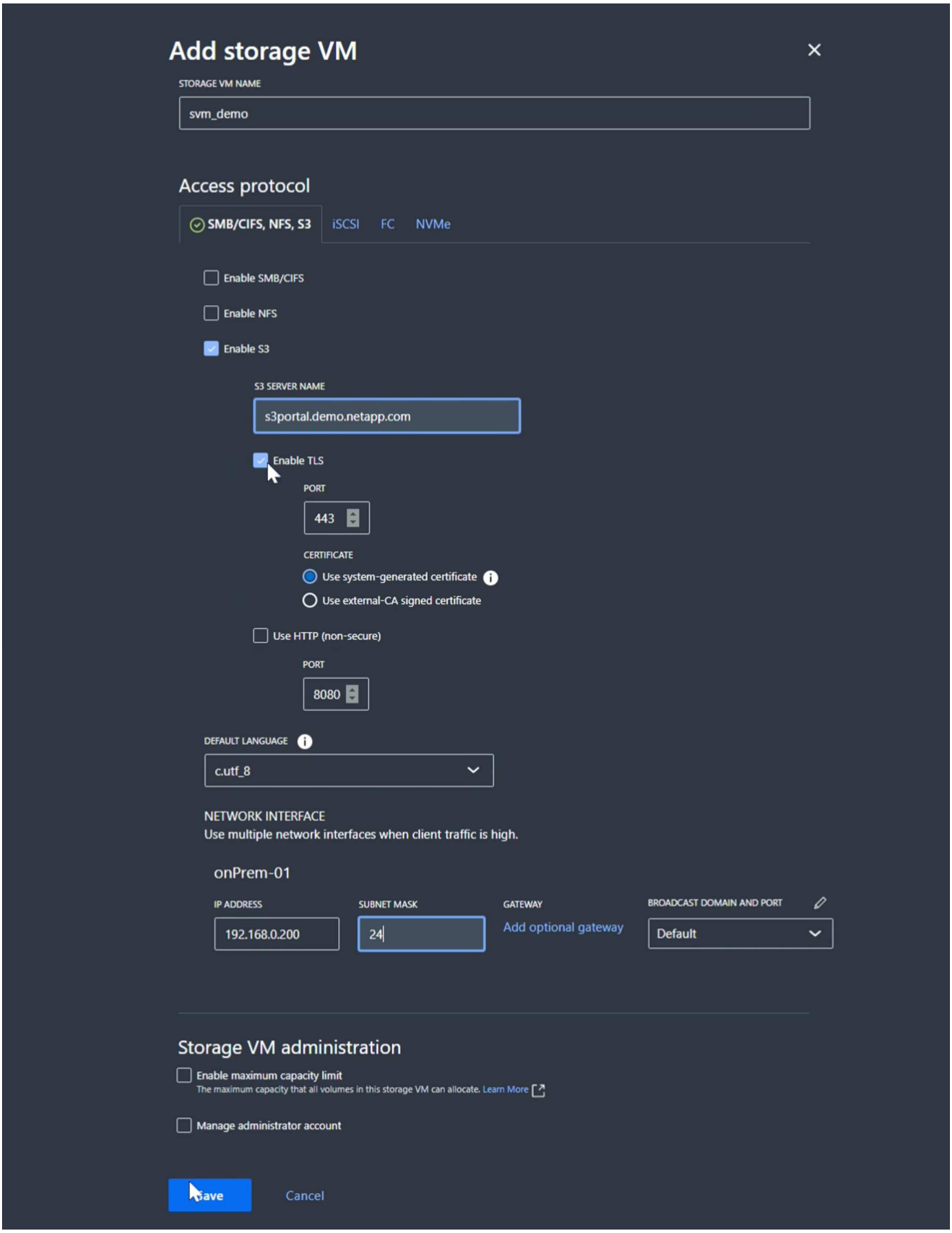
Para fins de demonstração, criaremos um servidor de armazenamento de objetos SVM, usuário, grupo, política de grupo e buckets.

Crie a Máquina Virtual de armazenamento

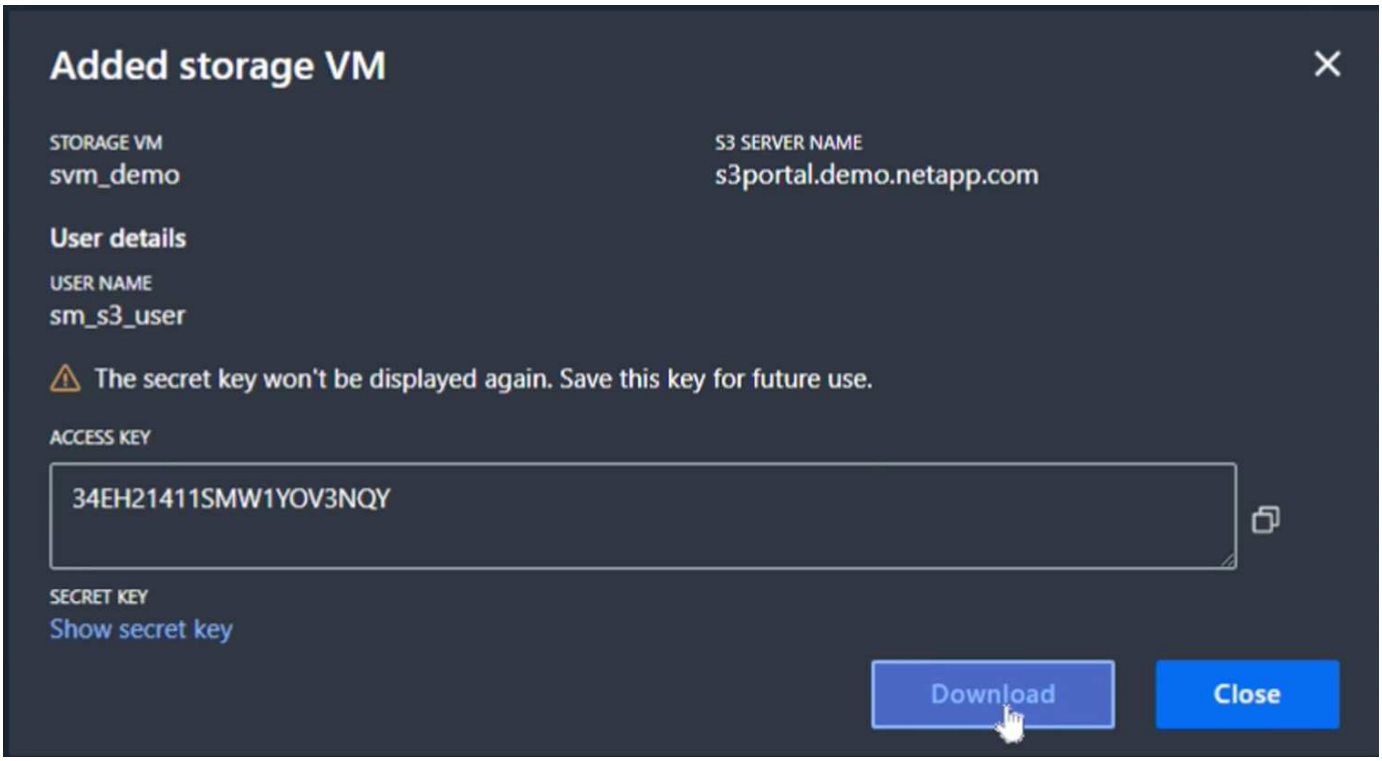
No Gerenciador de sistema do ONTAP, navegue até VMs de storage e adicione uma nova VM de storage.



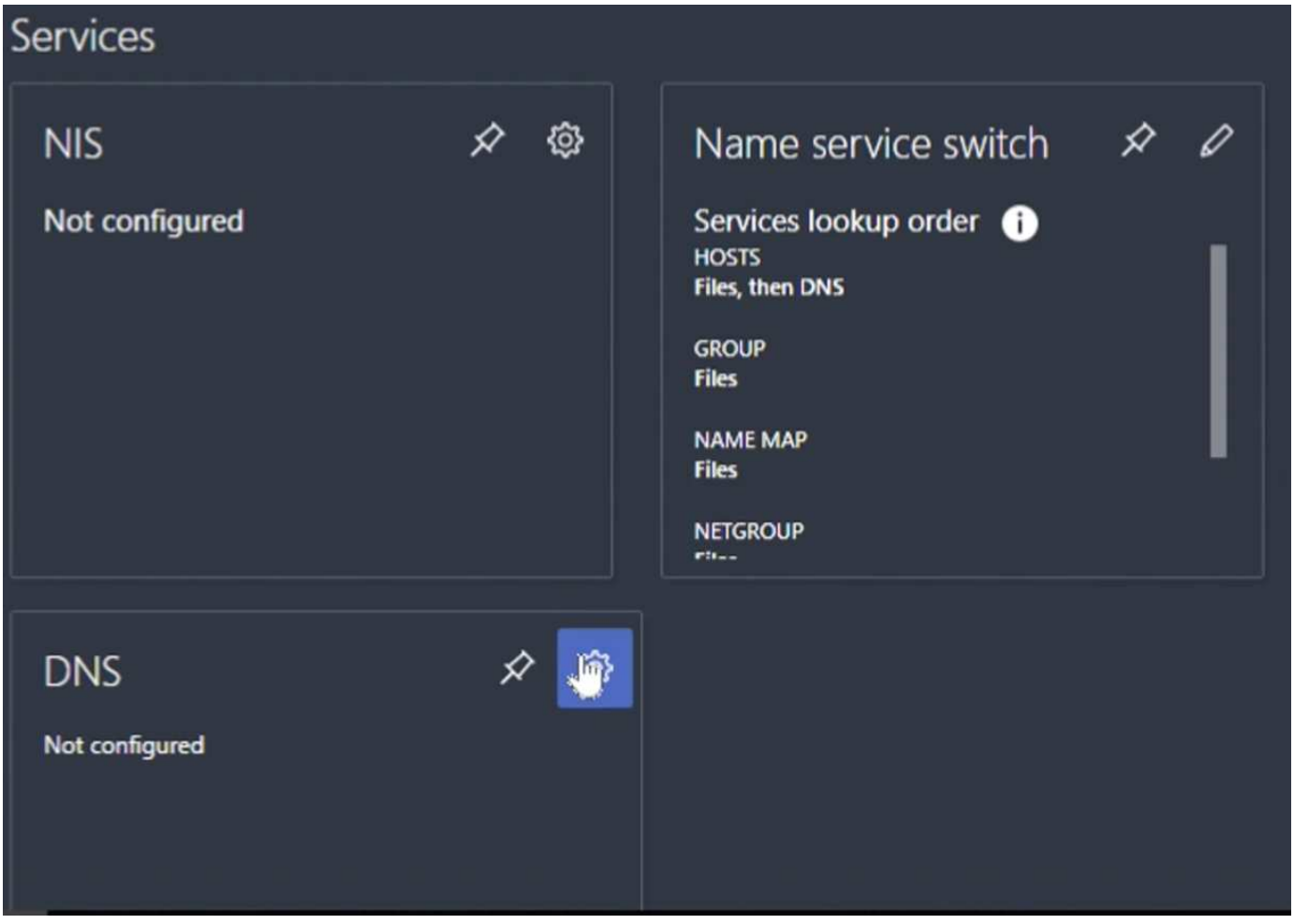
Selecione as caixas de verificação "Ativar S3" e "Ativar TLS" e configure as portas HTTP(S). Defina o IP, a máscara de sub-rede e defina o gateway e o domínio de broadcast se não estiver usando o padrão ou o necessário em seu ambiente.



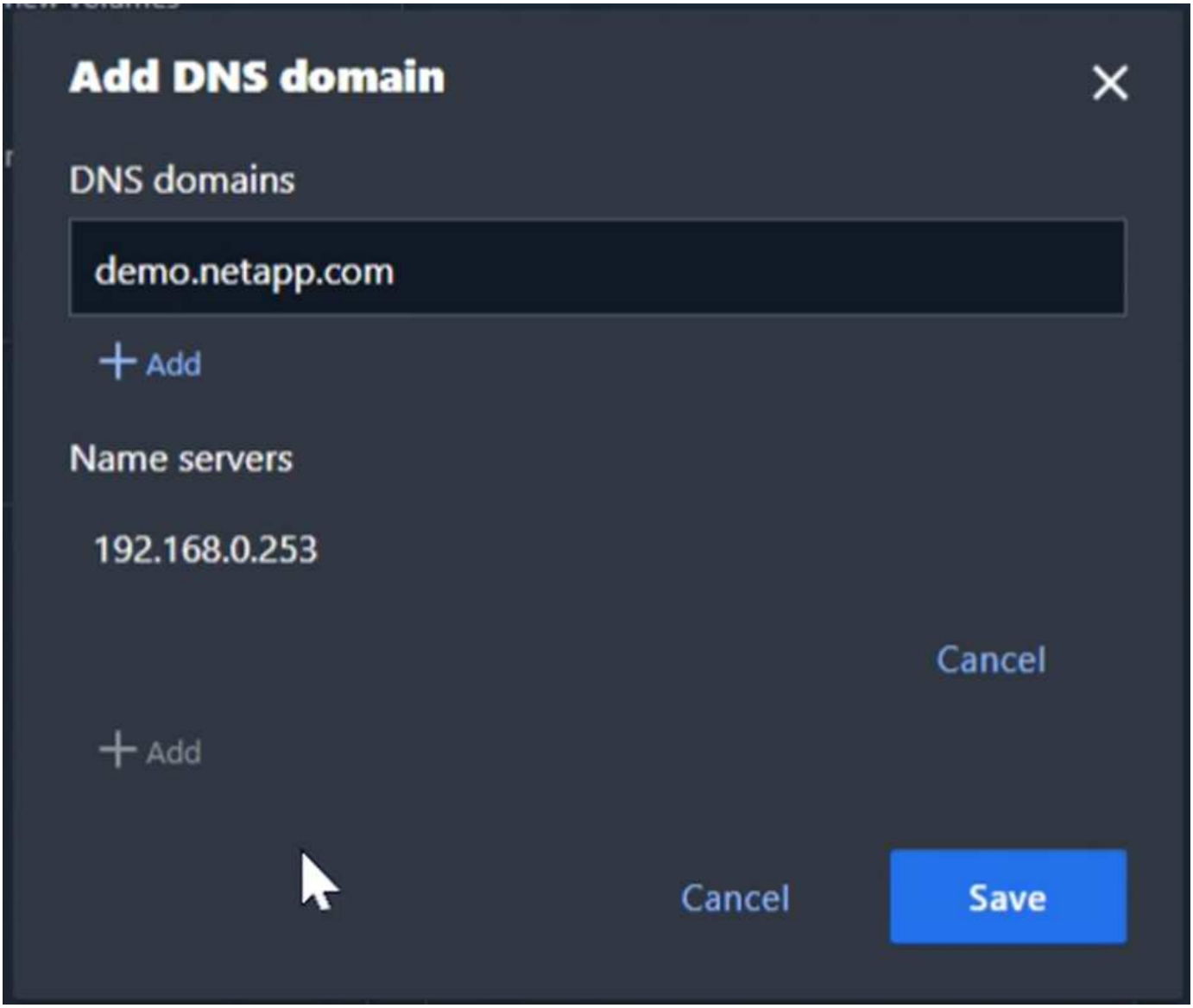
Como parte da criação do SVM, um usuário será criado. Transfira as S3 teclas para este utilizador e feche a janela.



Depois que o SVM tiver sido criado, edite o SVM e adicione as configurações de DNS.

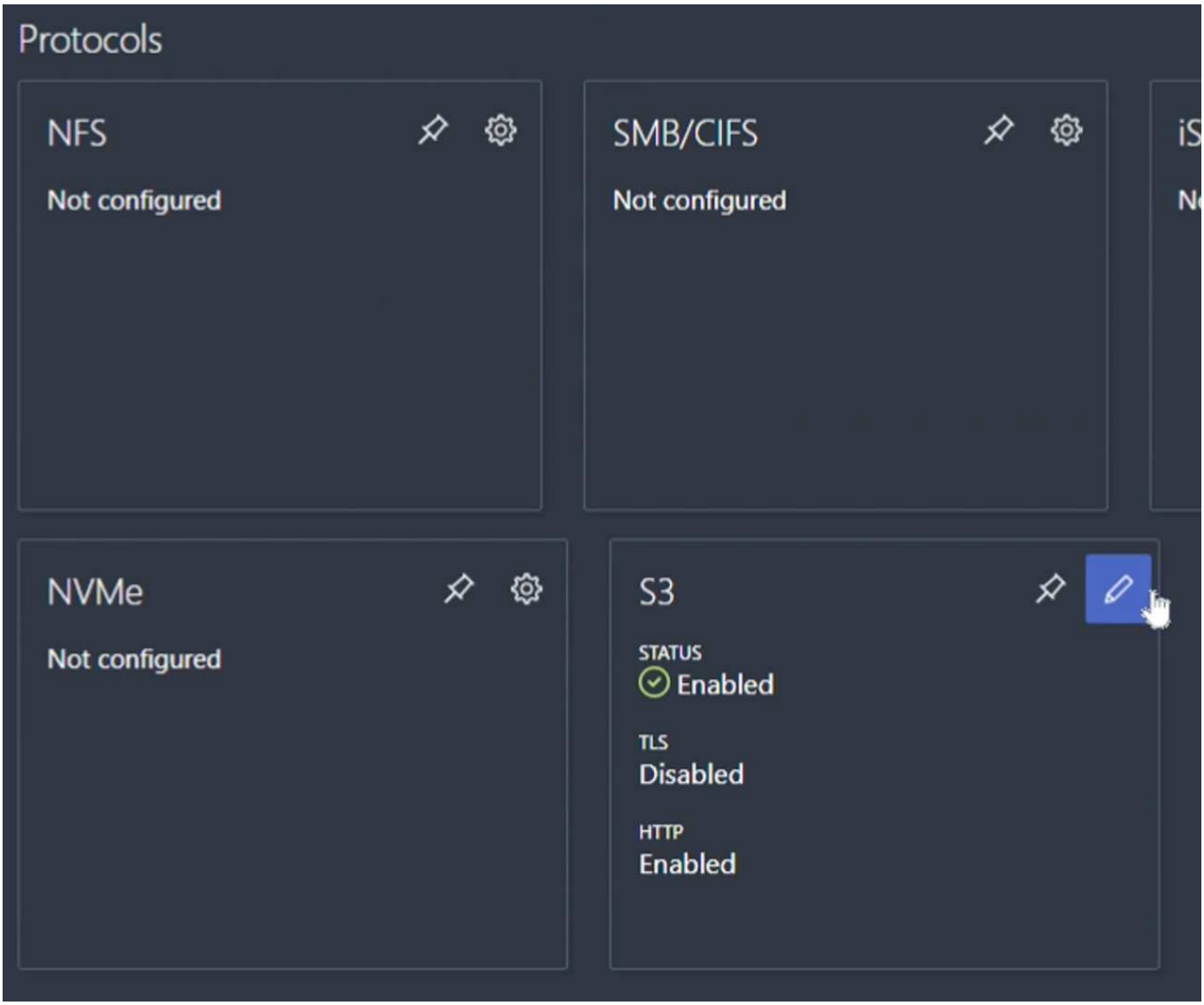


Defina o nome DNS e o IP.

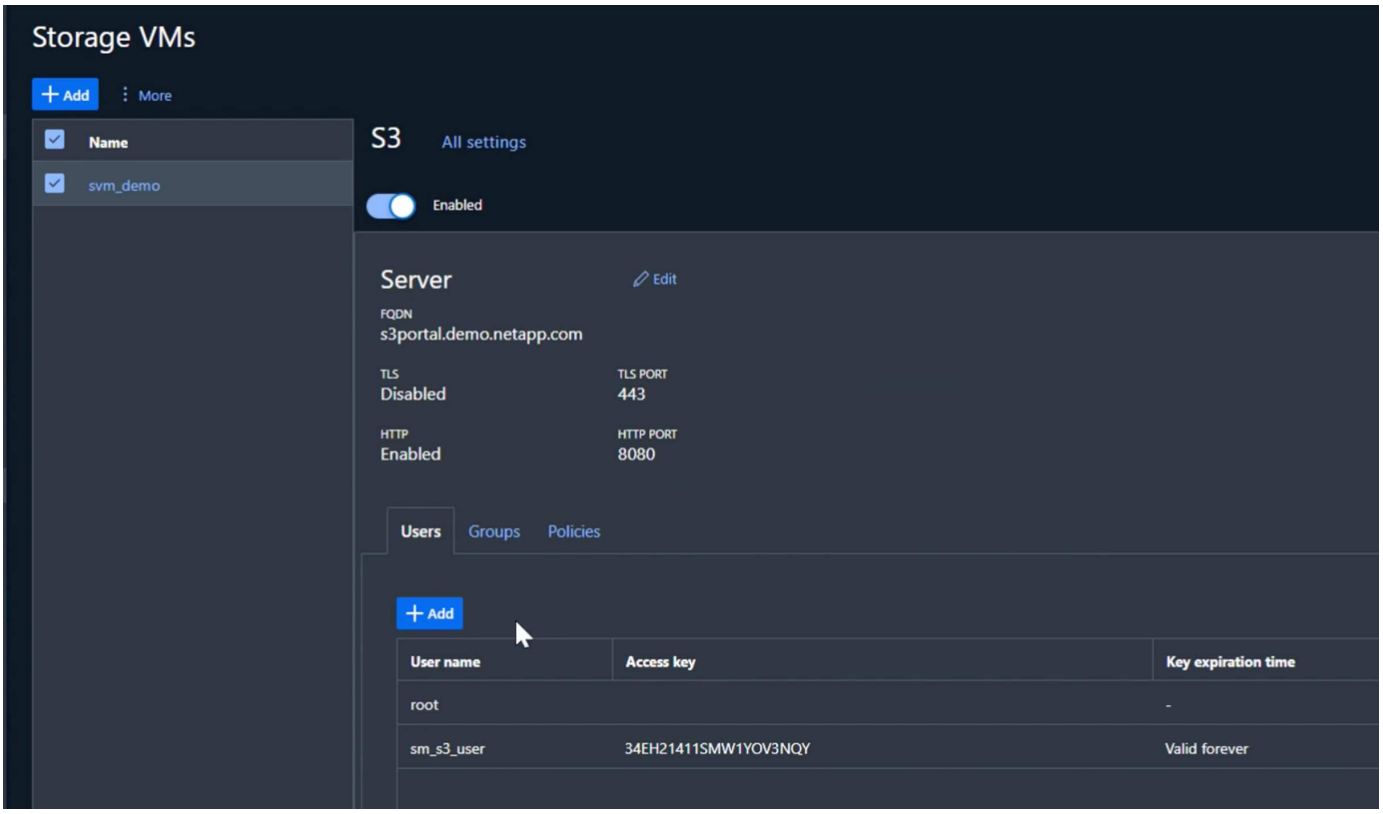


Crie o SVM S3 User

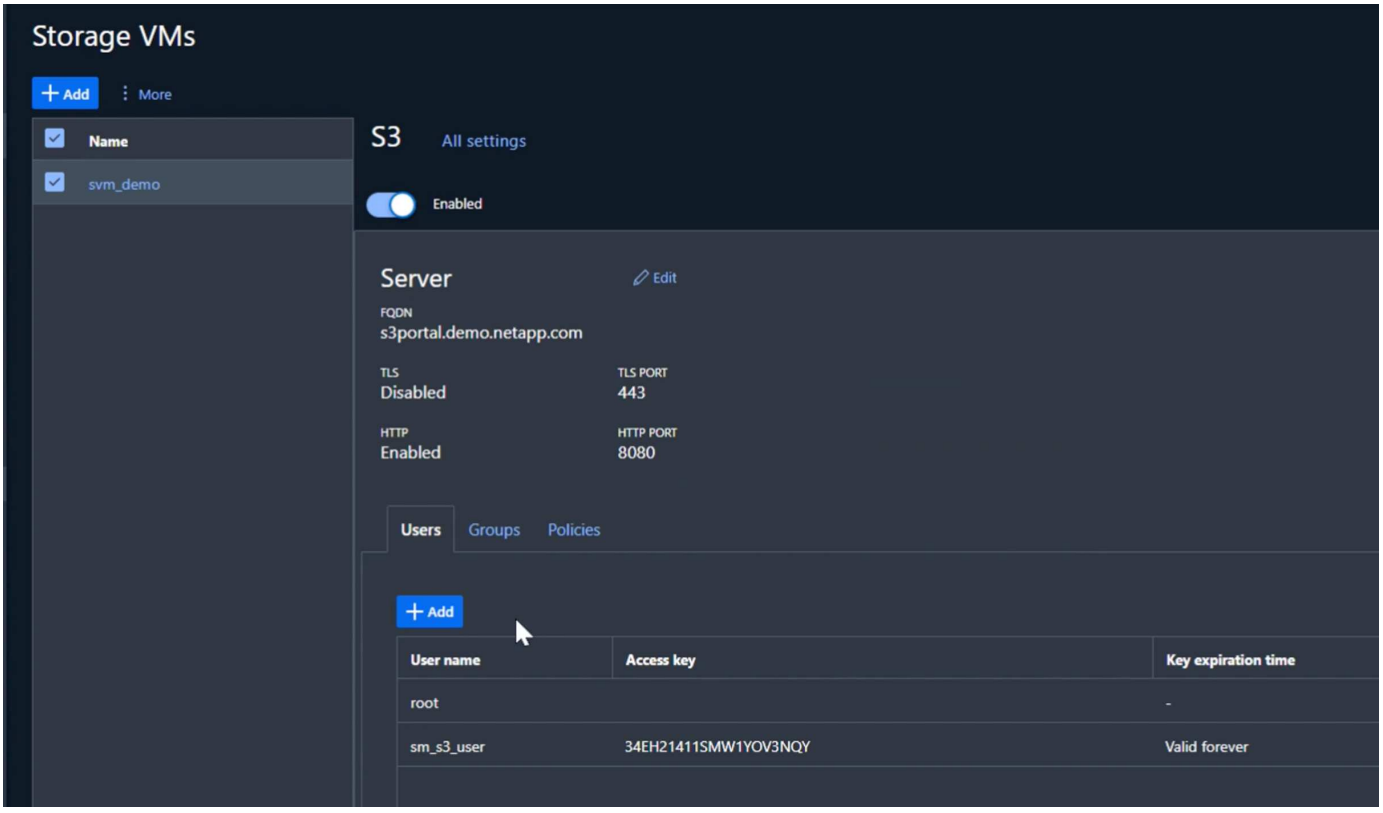
Agora podemos configurar os usuários e o grupo do S3. Edite as definições do S3.



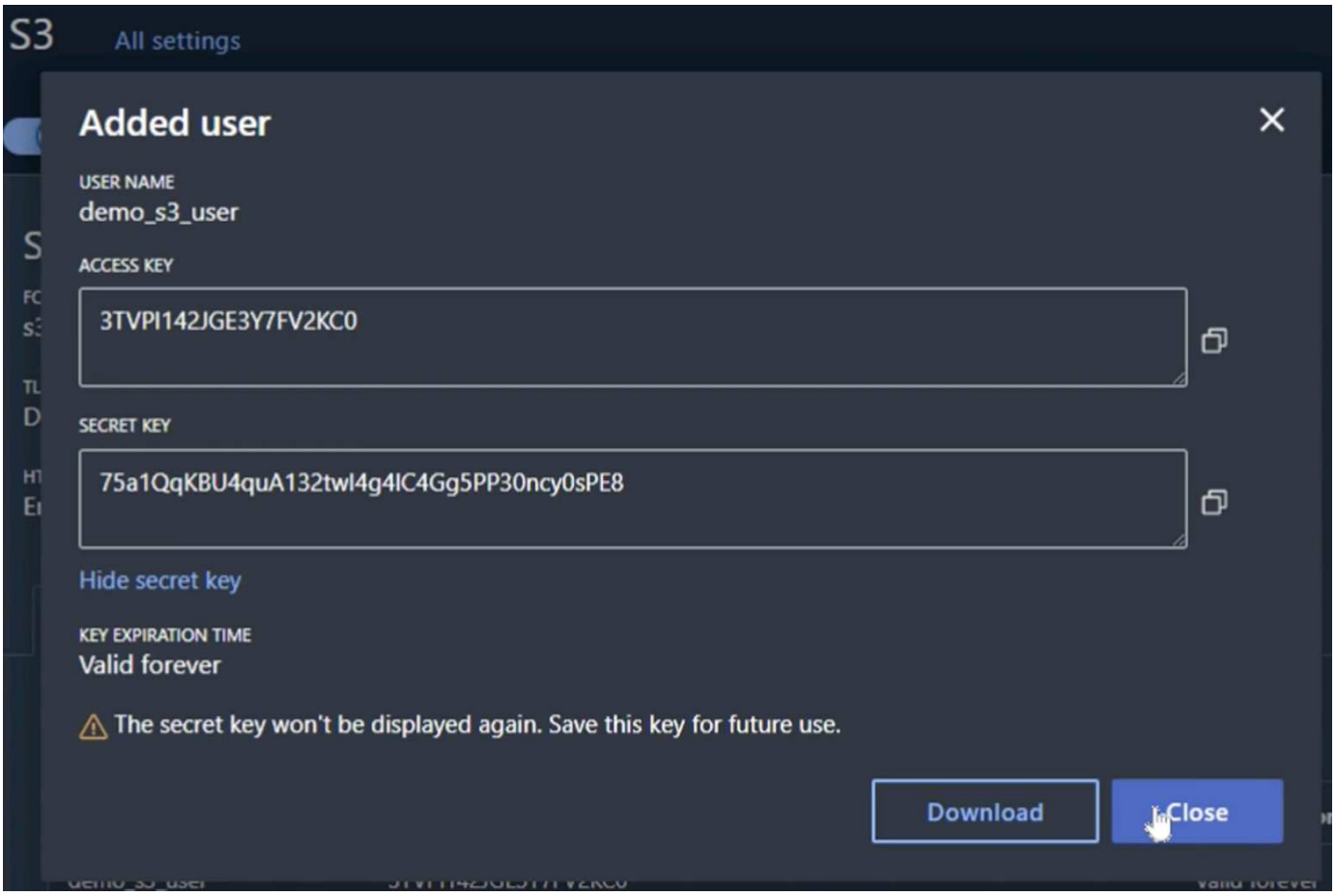
Adicionar um novo utilizador.



Introduza o nome de utilizador e a expiração da chave.

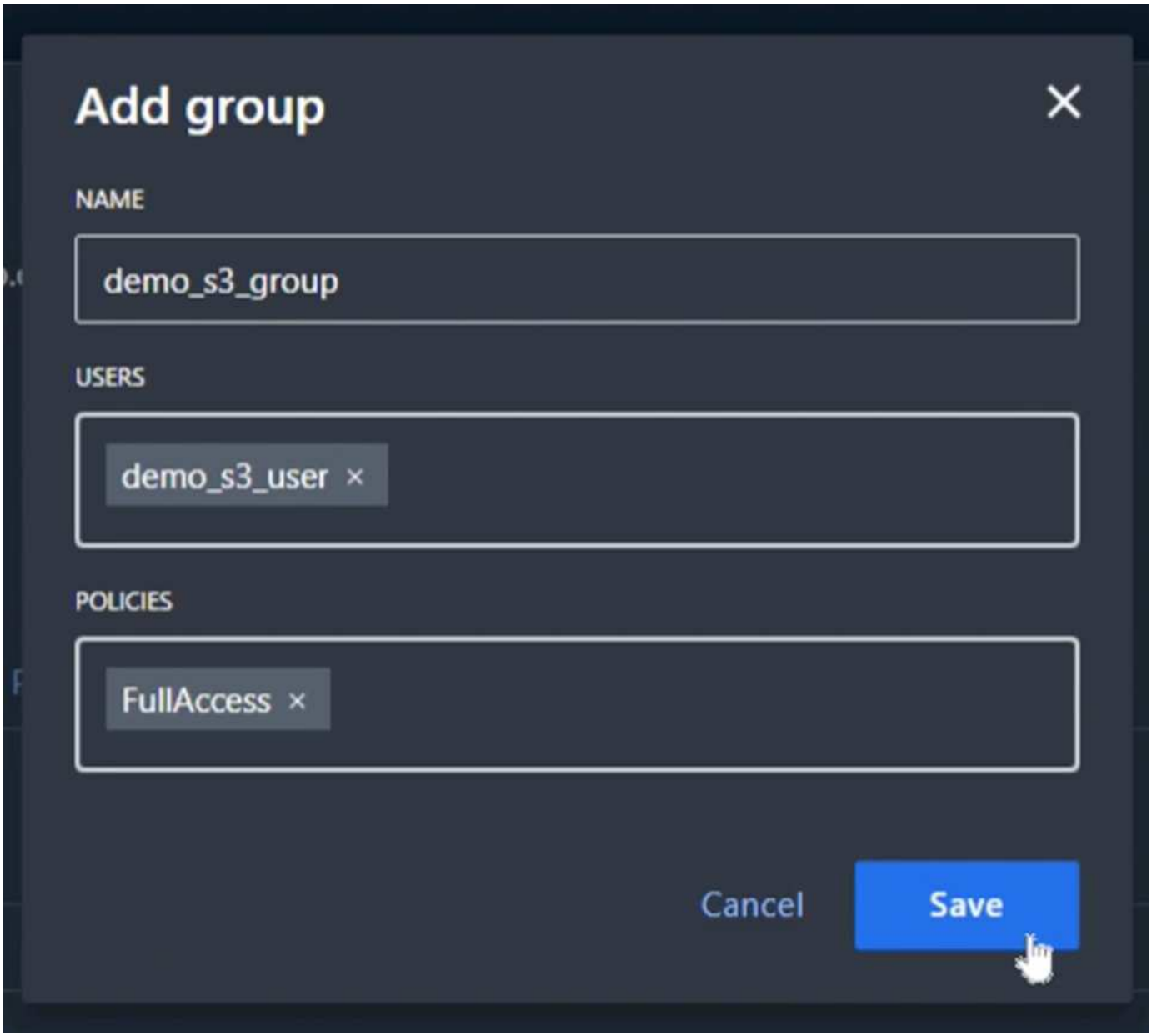


Transfira as S3 teclas para o novo utilizador.



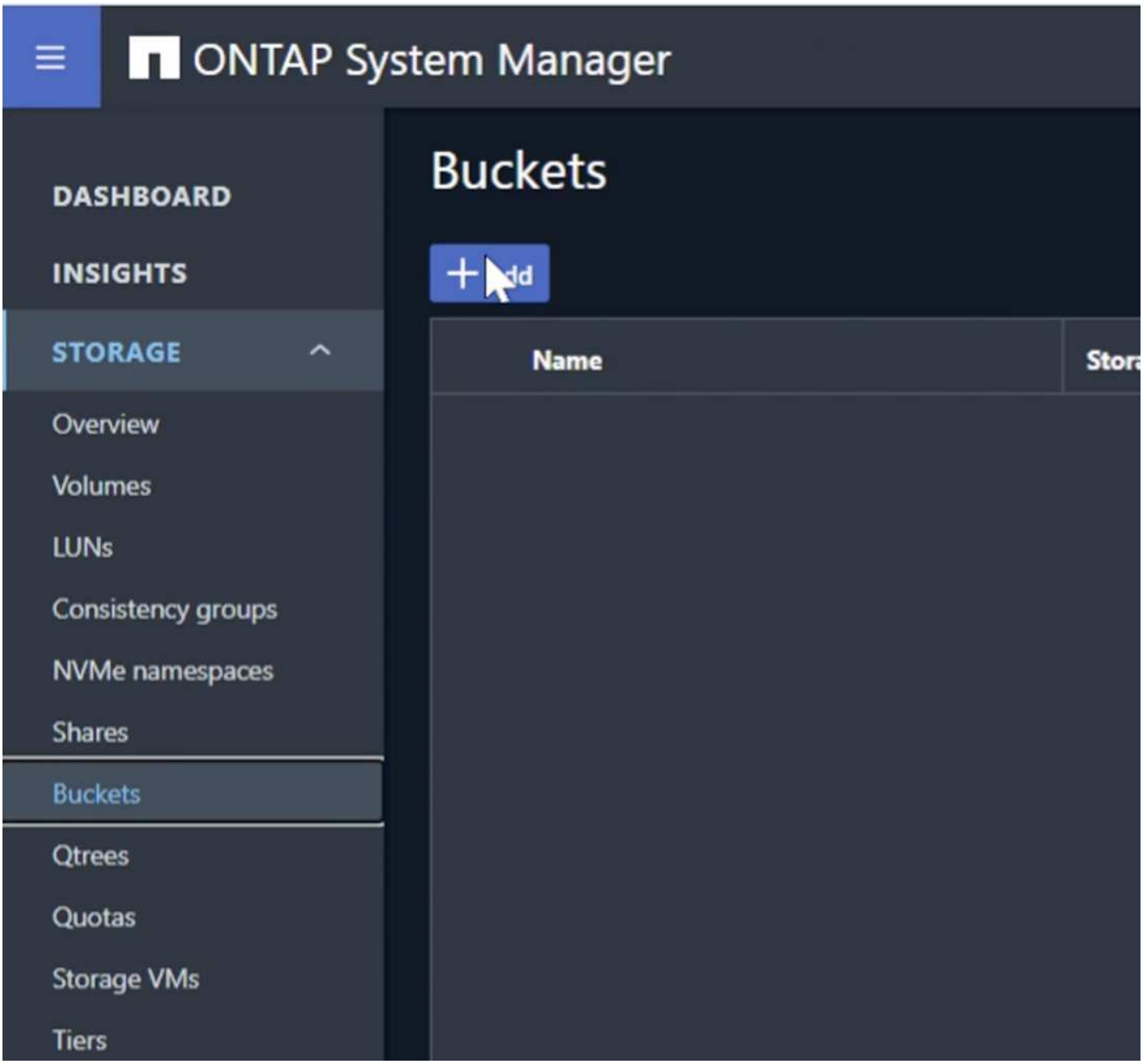
Crie o grupo SVM S3

Na guia grupos das configurações SVM S3, adicione um novo grupo com as permissões de usuário criado acima e FullAccess.

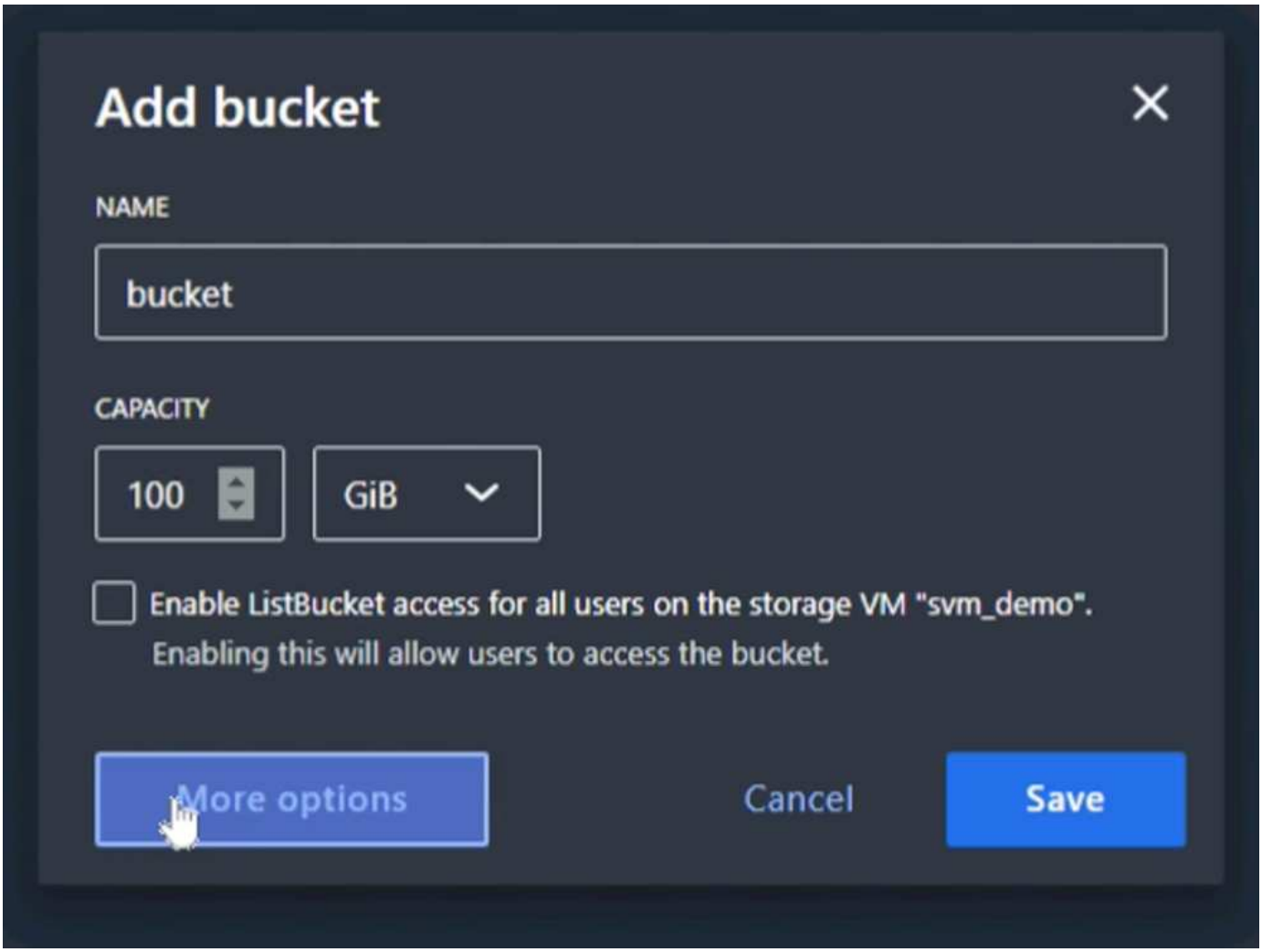


Criar buckets do SVM S3

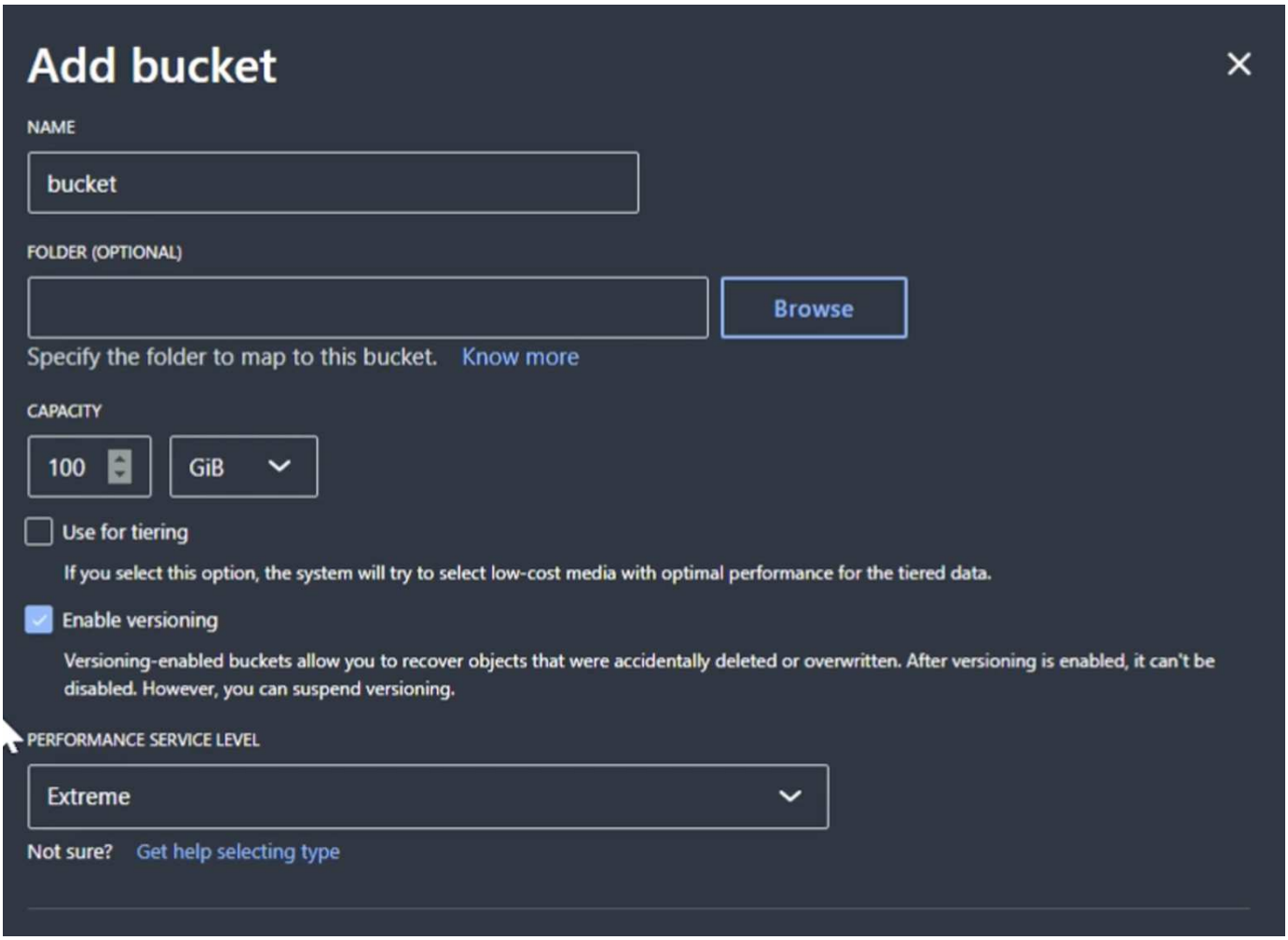
Navegue até a seção baldes e clique no botão Adicionar.



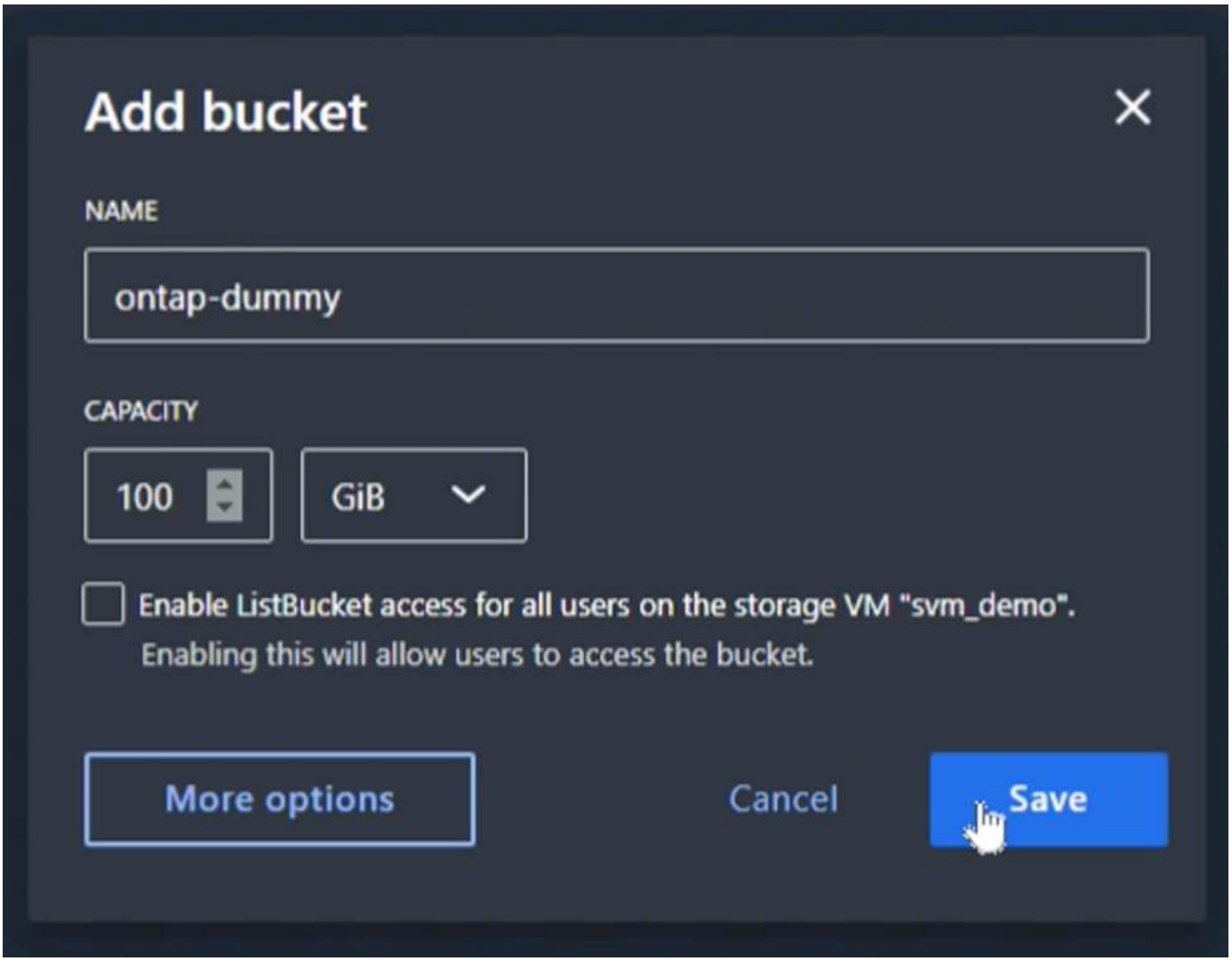
Digite um nome, capacidade e desmarque a caixa de seleção "Ativar acesso ao ListBucket…" e clique no botão "mais opções".



Na seção "mais opções", marque a caixa de seleção Ativar controle de versão e clique no botão "Salvar".



Repita o processo e crie um segundo bucket sem o controle de versão ativado. Insira um nome, a mesma capacidade que um bucket, e desmarque a caixa de seleção "Enable ListBucket Access…" e clique no botão "Save" (Salvar).



Por Rafael Guedes, e Aron Klein

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

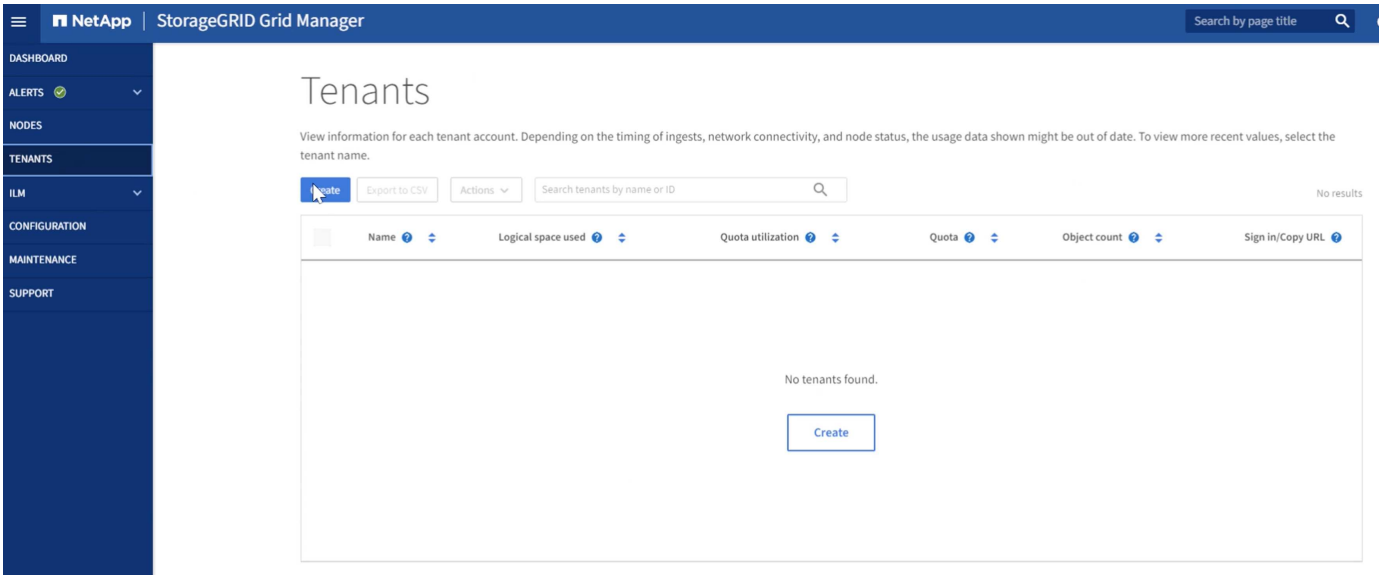
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Preparando o StorageGRID

Continuando a configuração para esta demonstração, criaremos um locatário, usuário, grupo de segurança, política de grupo e bucket.

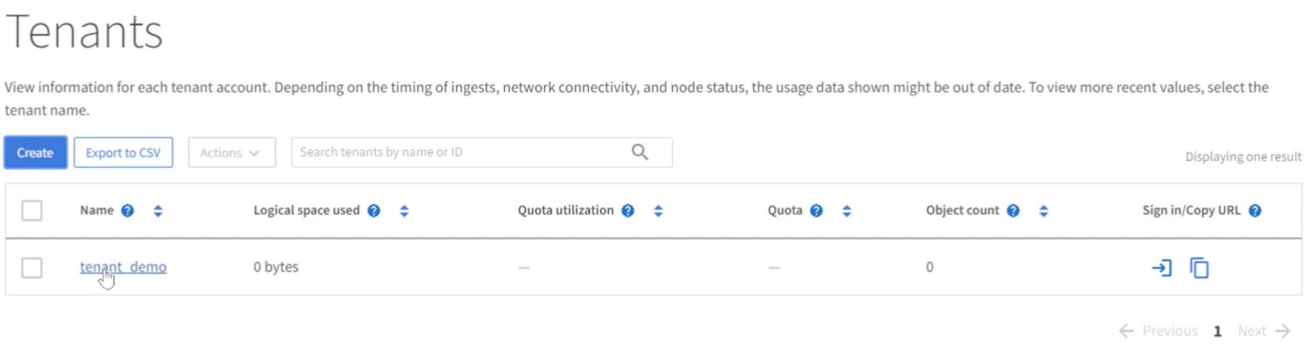
Crie o locatário

Navegue até a guia "inquilinos" e clique no botão "criar"

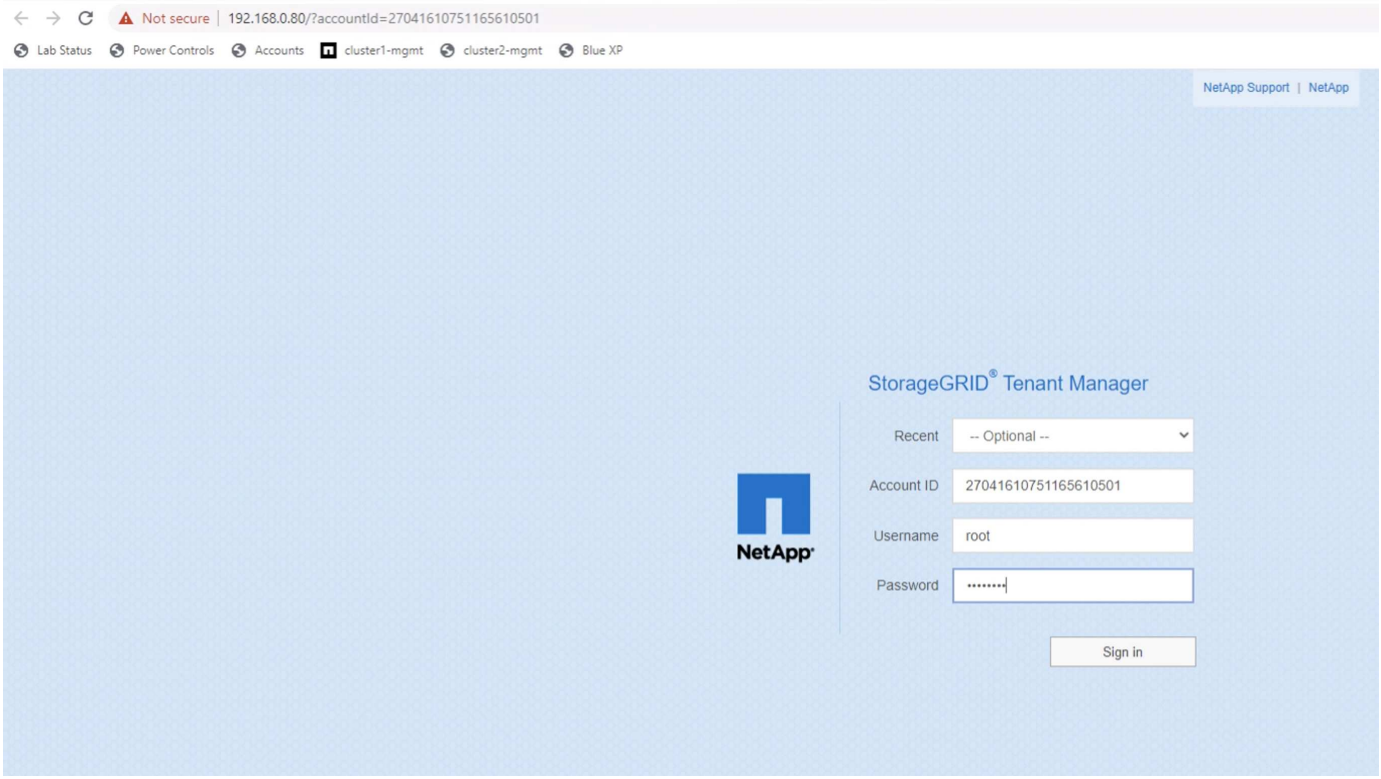


Preencha os detalhes para o locatário que fornece um nome de locatário, selecione S3 para o tipo de cliente e nenhuma cota é necessária. Não há necessidade de selecionar serviços de plataforma ou permitir S3 Select. Você pode optar por usar a própria fonte de identidade, se você escolher. Defina a senha raiz e clique no botão concluir.

Clique no nome do locatário para ver os detalhes do locatário. **Você precisará do ID do locatário mais tarde, então copie-o**. Clique no botão Iniciar sessão. Isso o levará ao login do portal do locatário. Salve o URL para uso futuro.

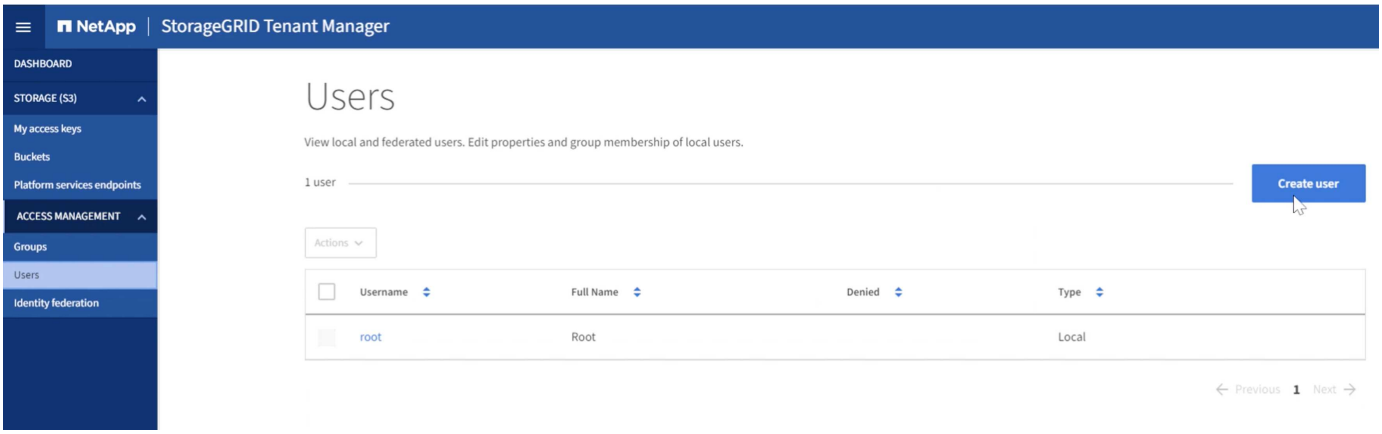


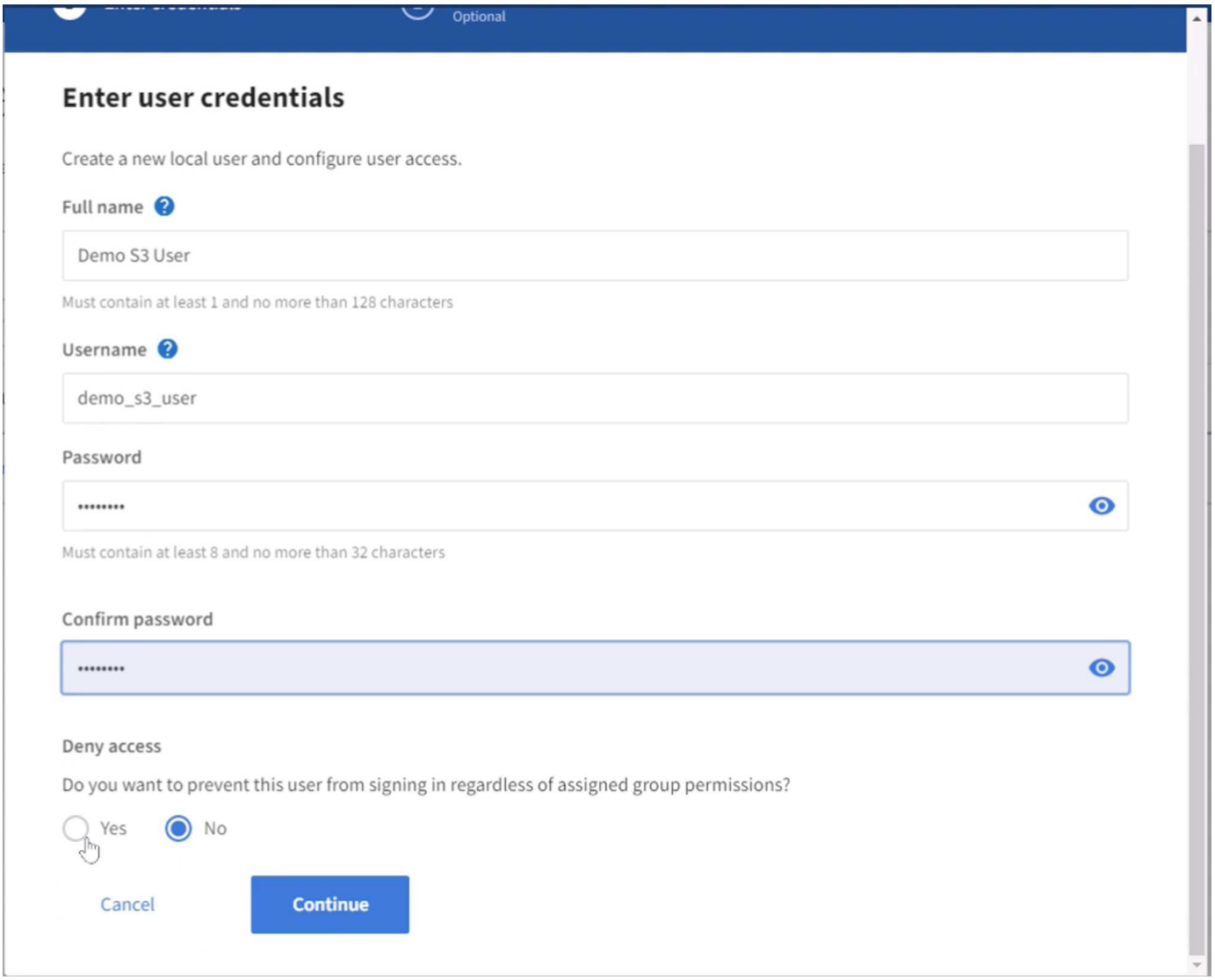
Isso o levará ao login do portal do locatário. Salve o URL para uso futuro e insira as credenciais do usuário raiz.



Crie o usuário

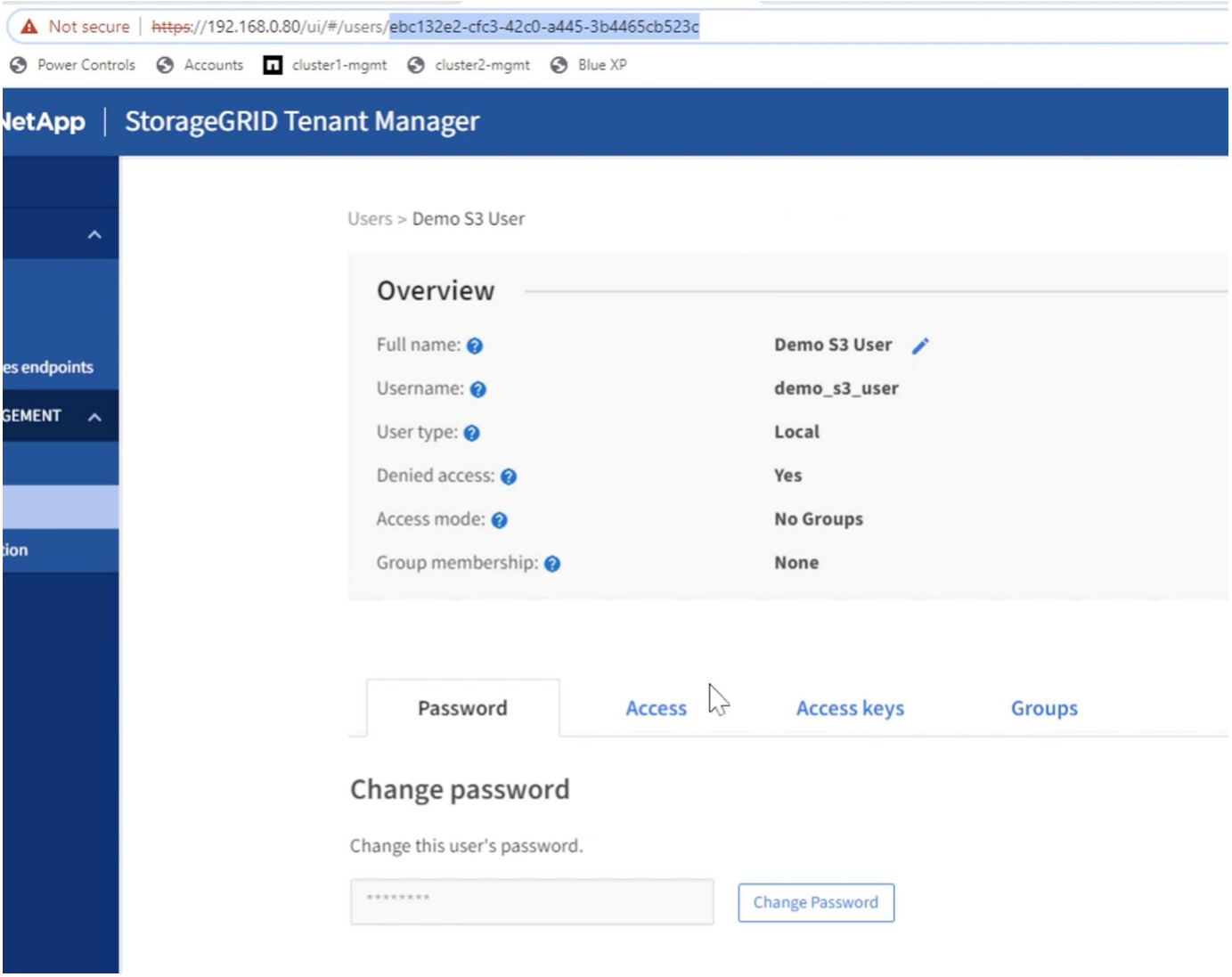
Navegue até a guia usuários e crie um novo usuário.



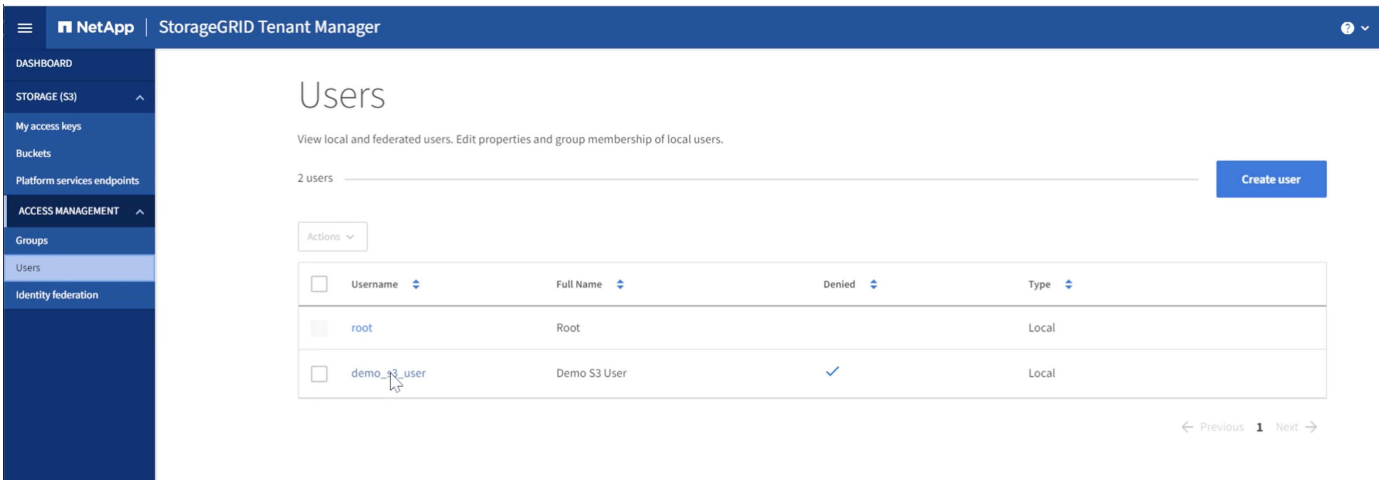


Agora que o novo usuário foi criado, clique no nome do usuário para abrir os detalhes do usuário.

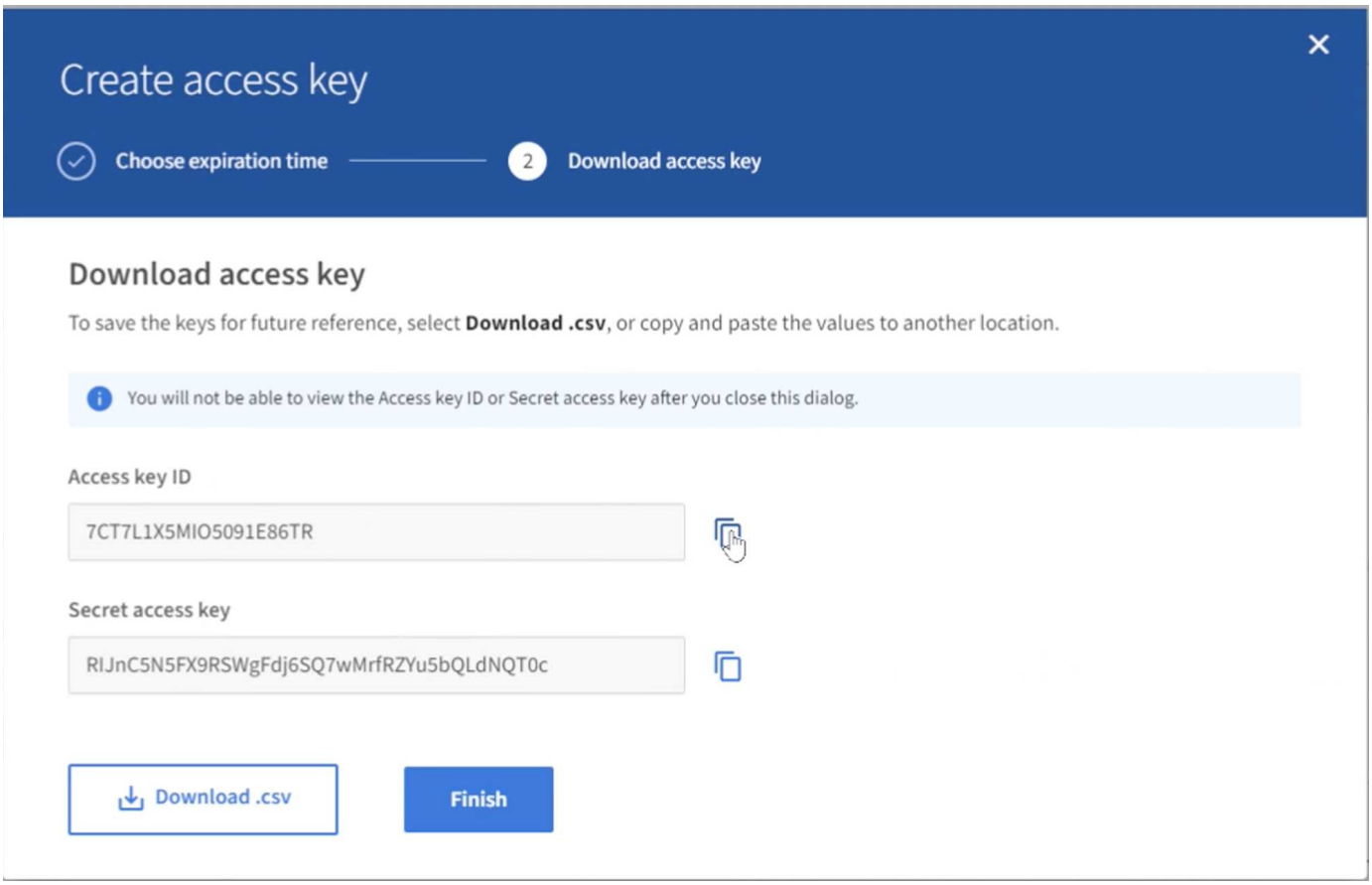
Copie o ID do usuário do URL a ser usado mais tarde.



Para criar as S3 teclas, clique no nome de usuário.

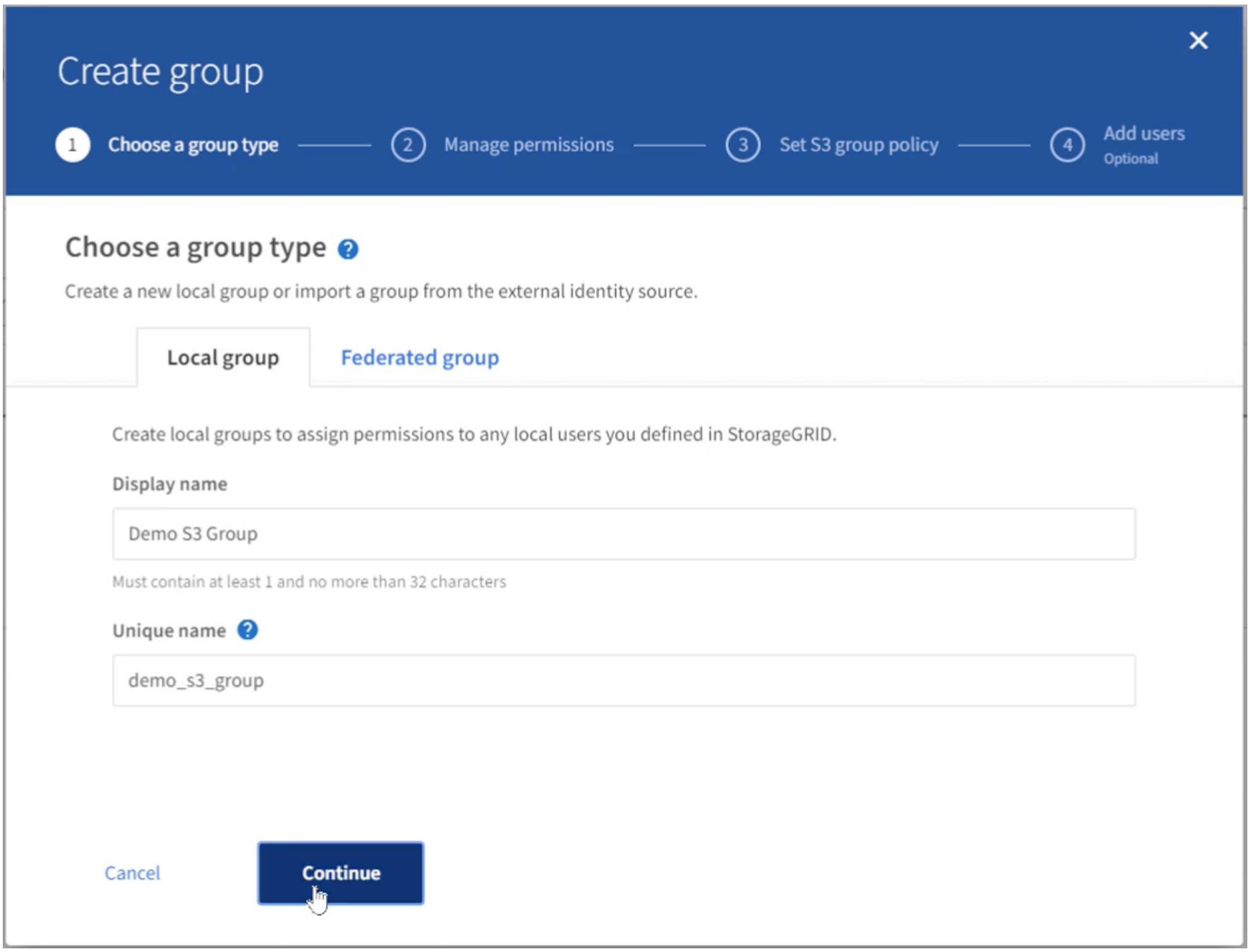


Selecione a guia "teclas de acesso" e clique no botão "criar chave". Não há necessidade de definir um tempo de expiração. Faça o download das teclas S3, pois elas não podem ser recuperadas novamente assim que a janela for fechada.

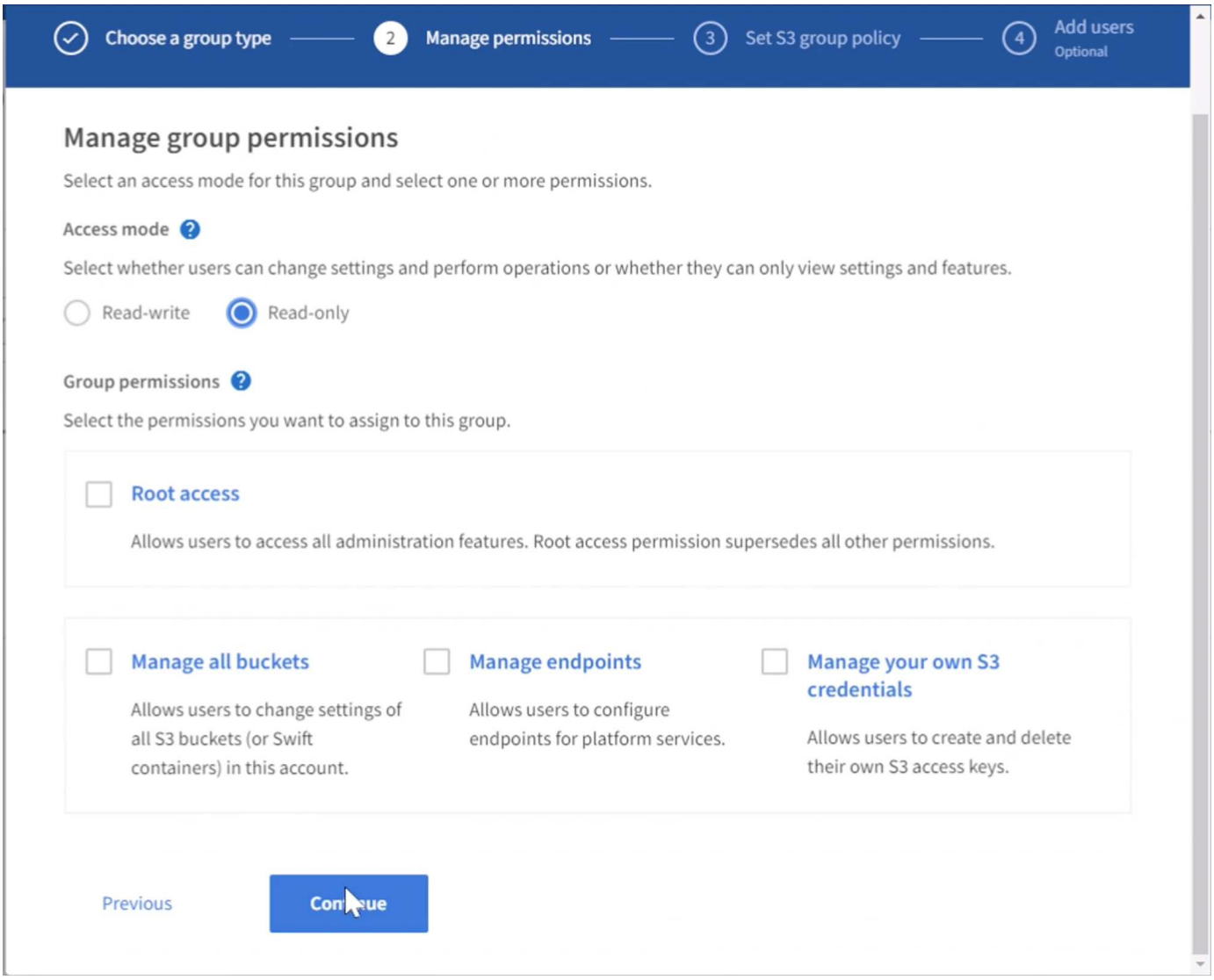


Crie o grupo de segurança

Agora vá para a página grupos e crie um novo grupo.

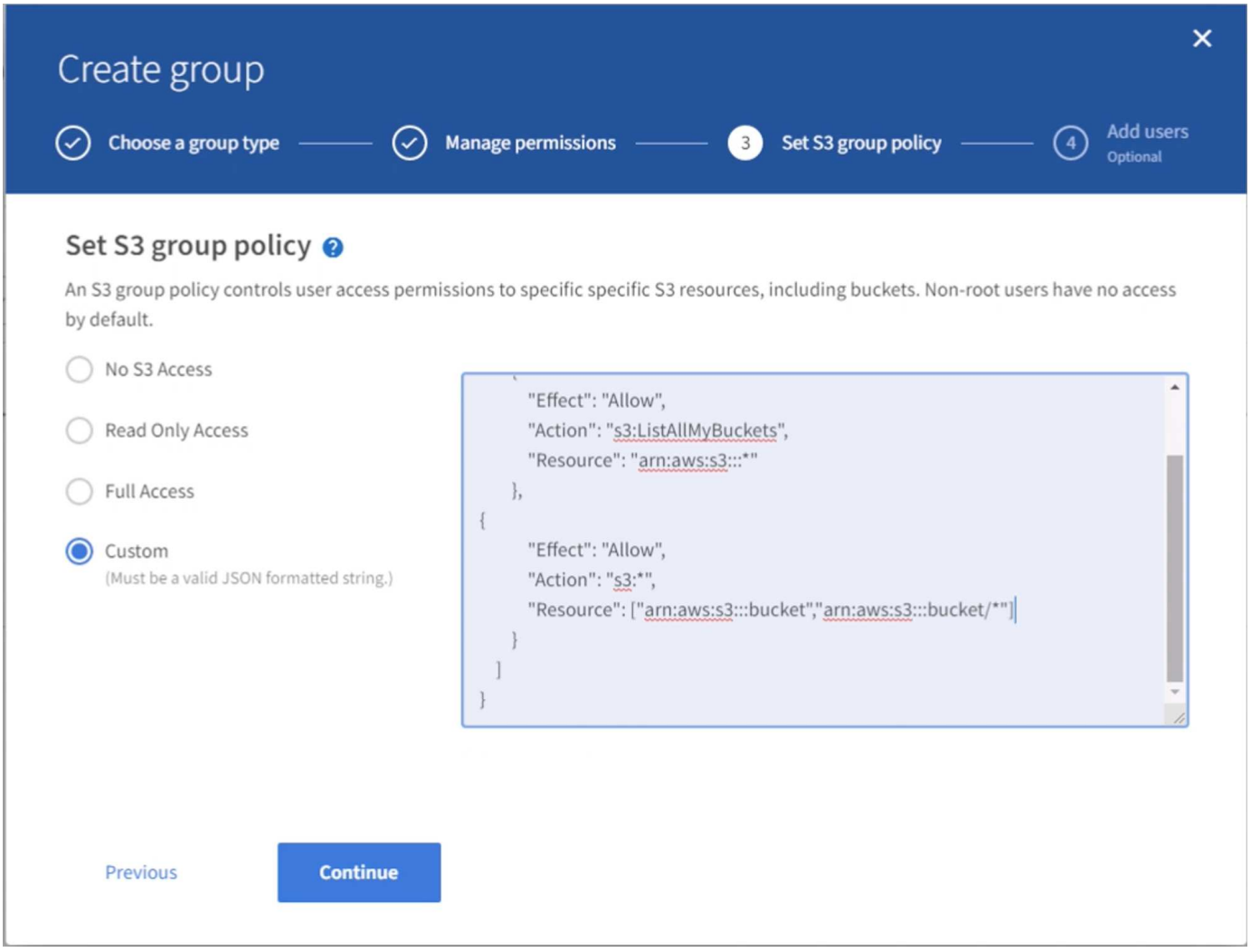


Defina as permissões do grupo como somente leitura. Estas são as permissões de IU do locatário, não as permissões S3.

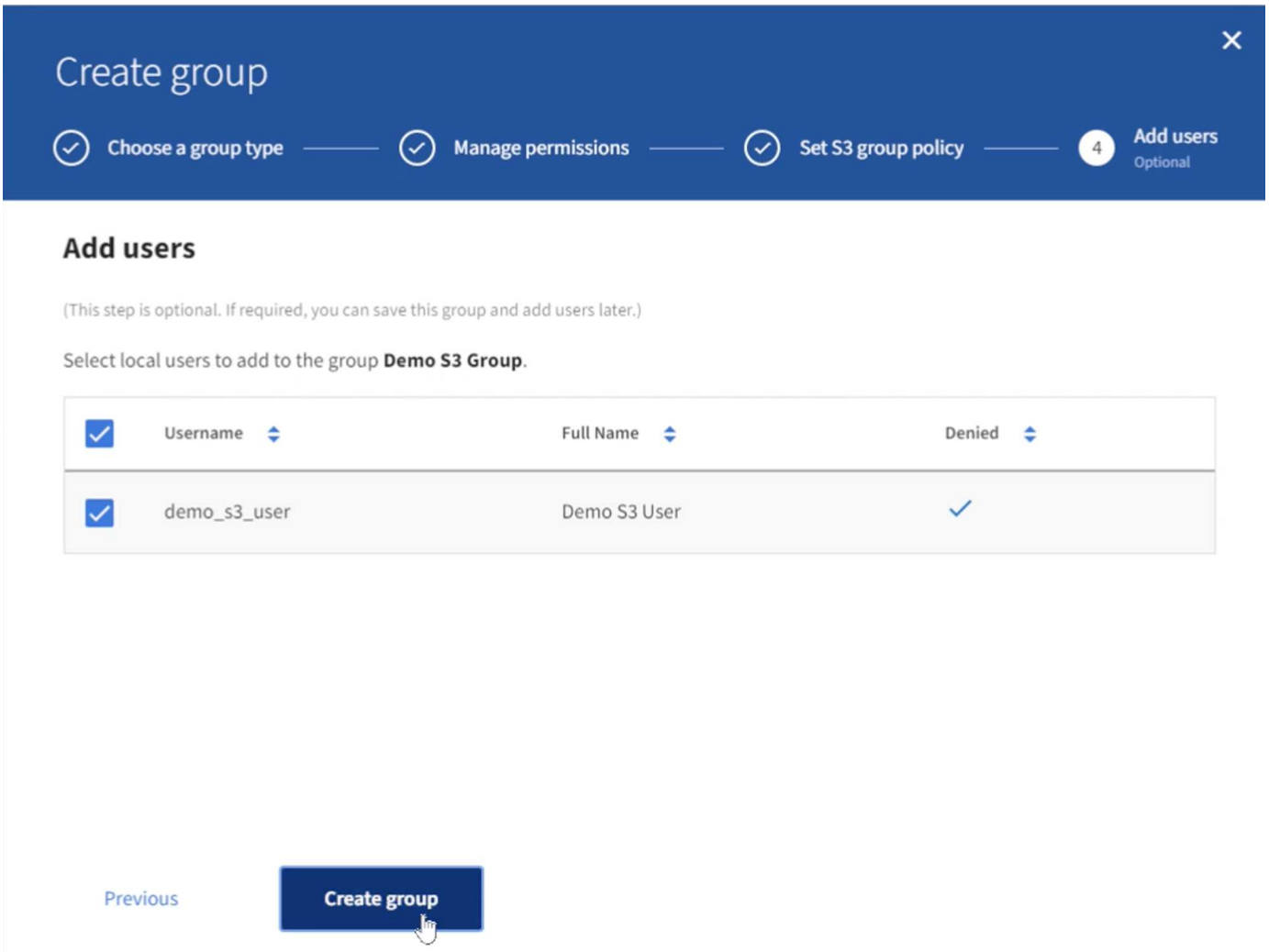


As permissões S3 são controladas com a política de grupo (diretiva IAM). Defina a política de grupo como personalizada e cole a política json na caixa. Esta política permitirá que os usuários deste grupo listem os buckets do locatário e executem quaisquer operações do S3 no bucket chamado "bucket" ou subpastas no bucket chamado "bucket".

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

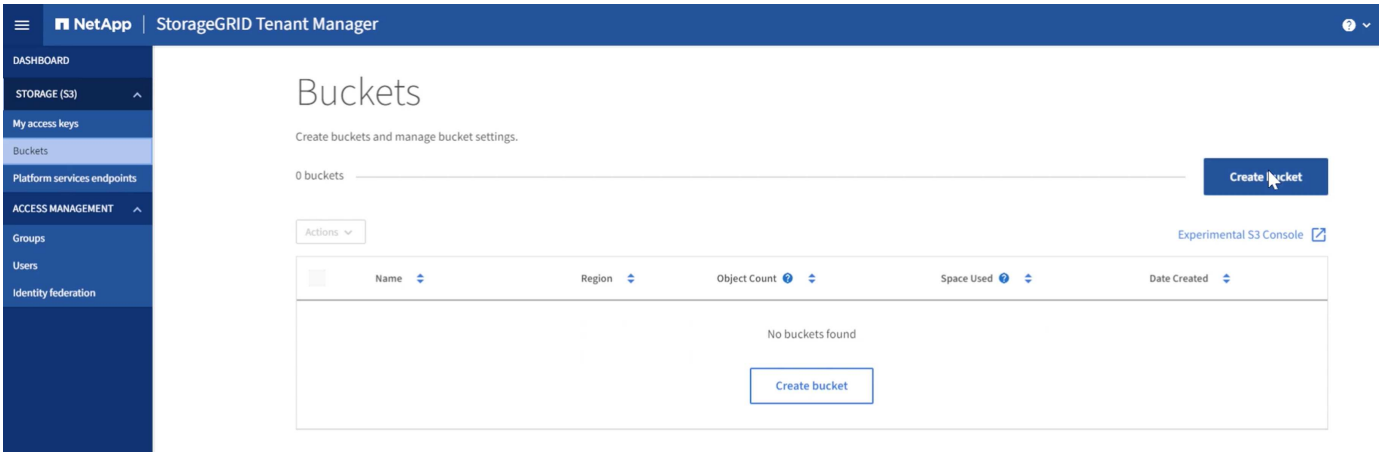


Finalmente, adicione o usuário ao grupo e termine.

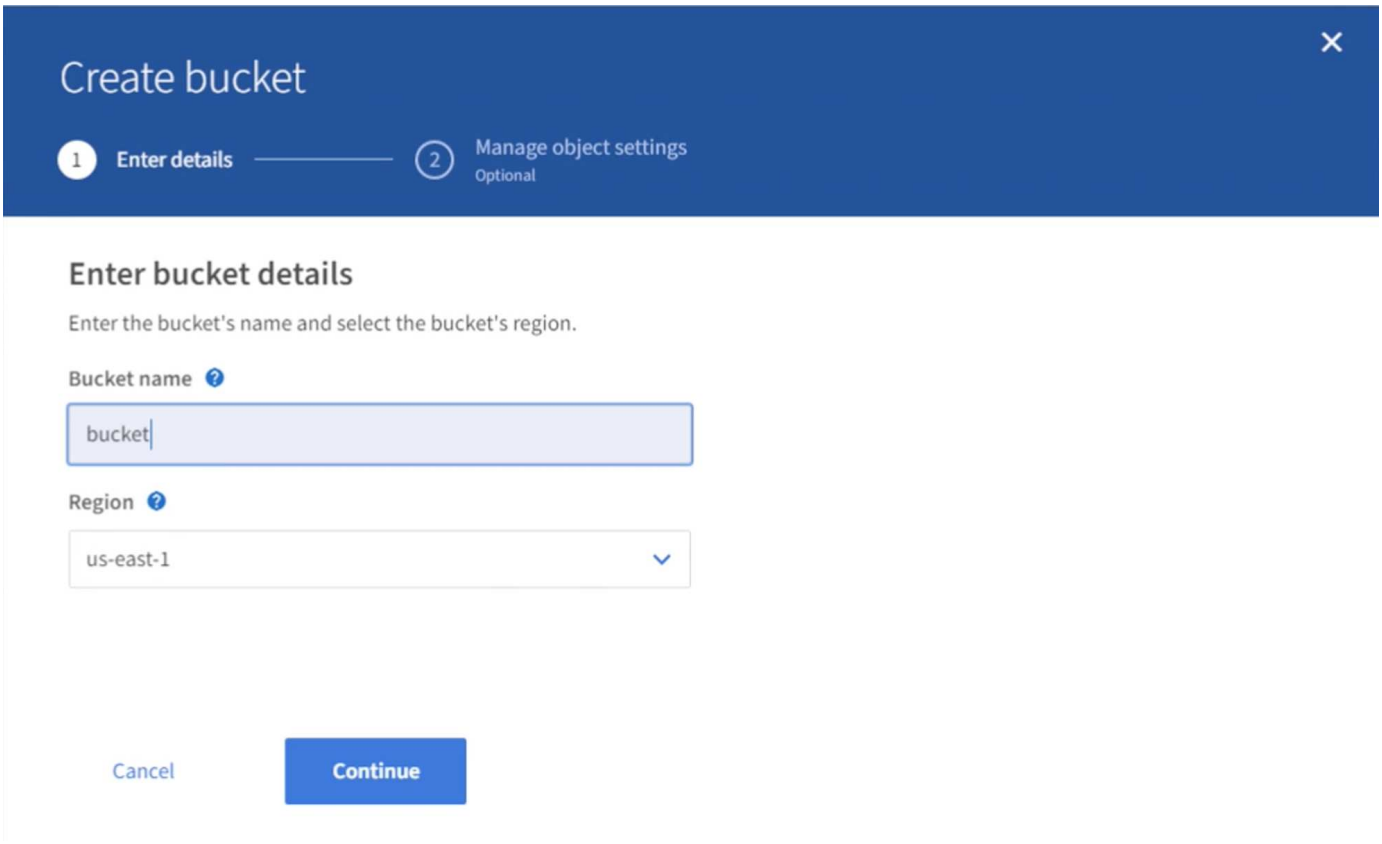


Crie dois baldes

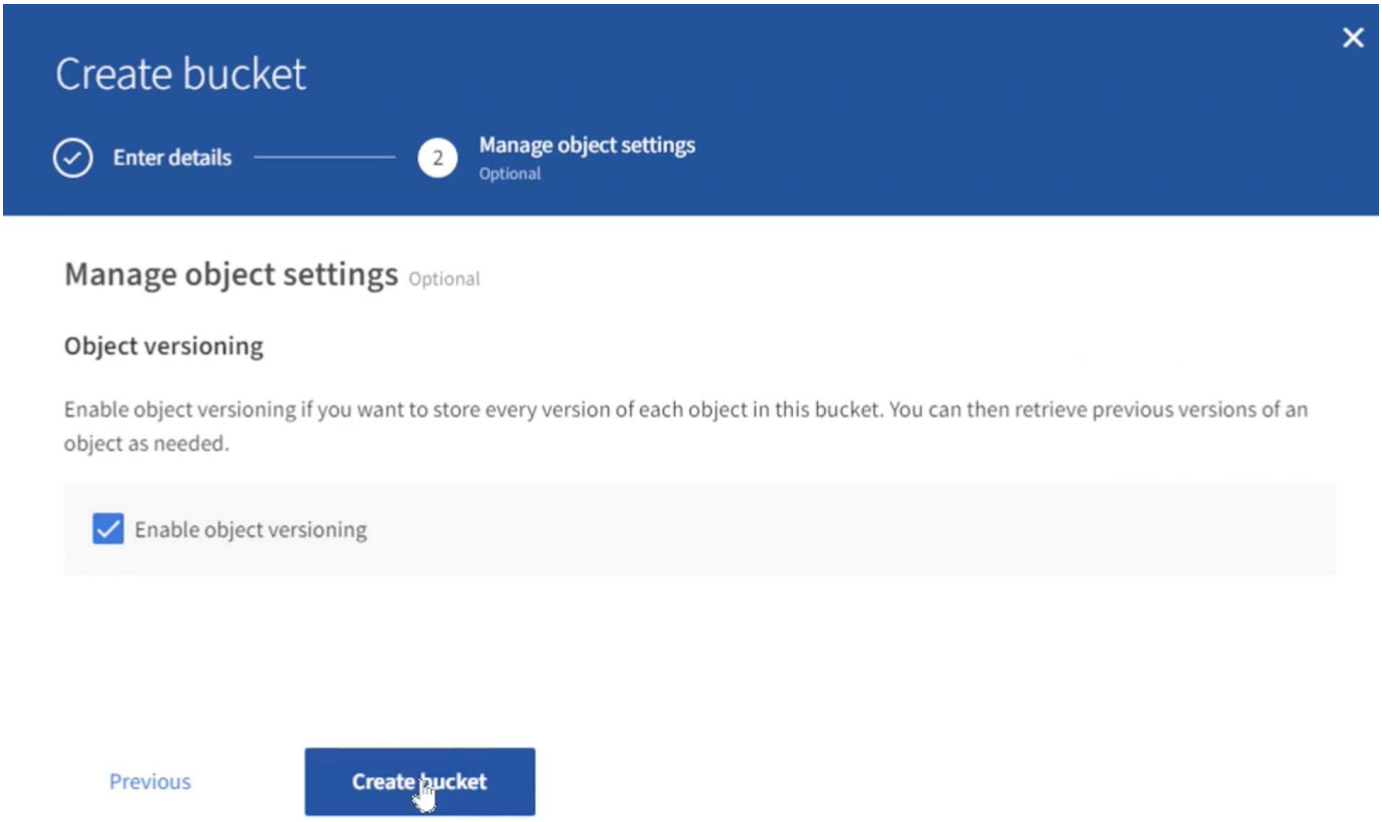
Navegue até a guia buckets e clique no botão Create bucket (criar bucket).



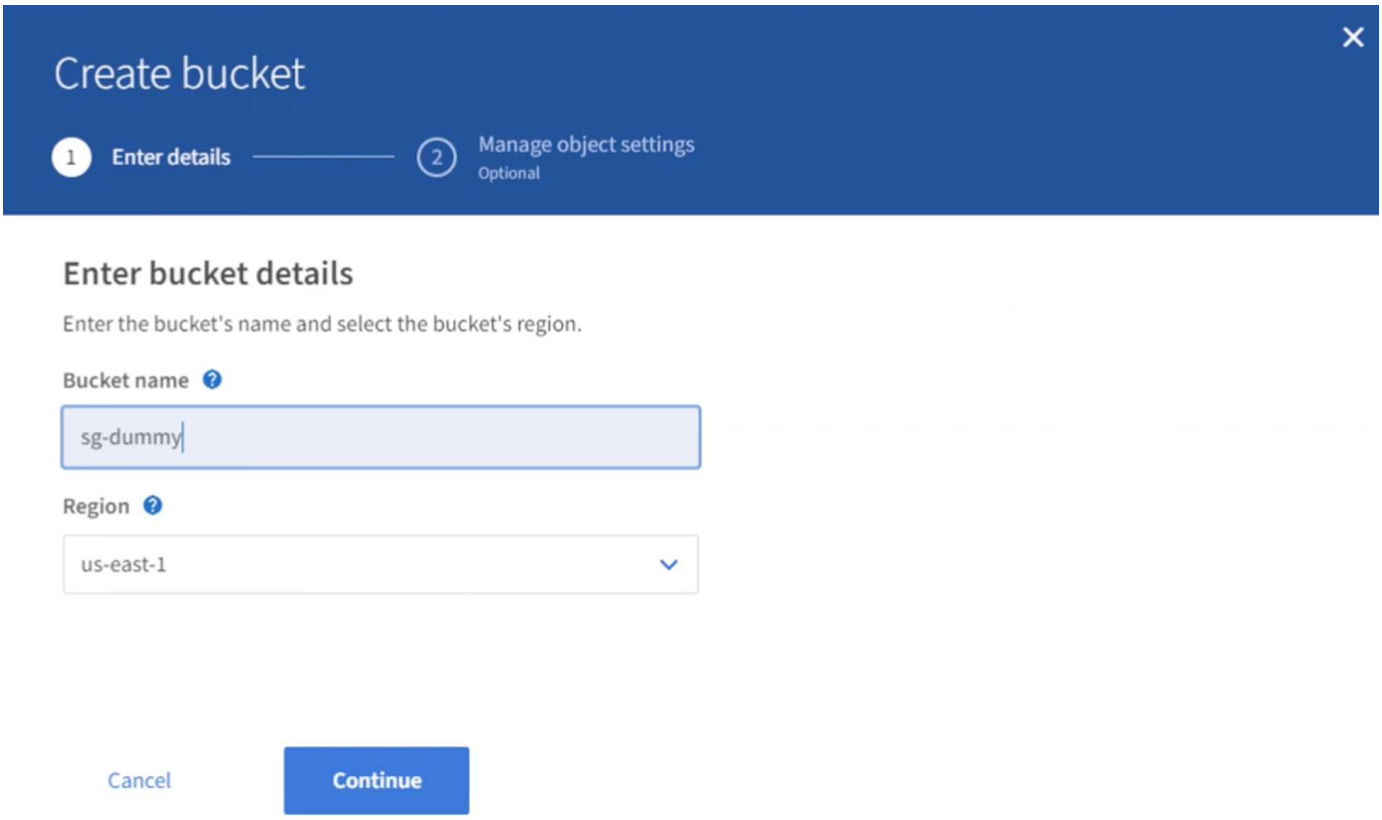
Defina o nome e a região do intervalo.



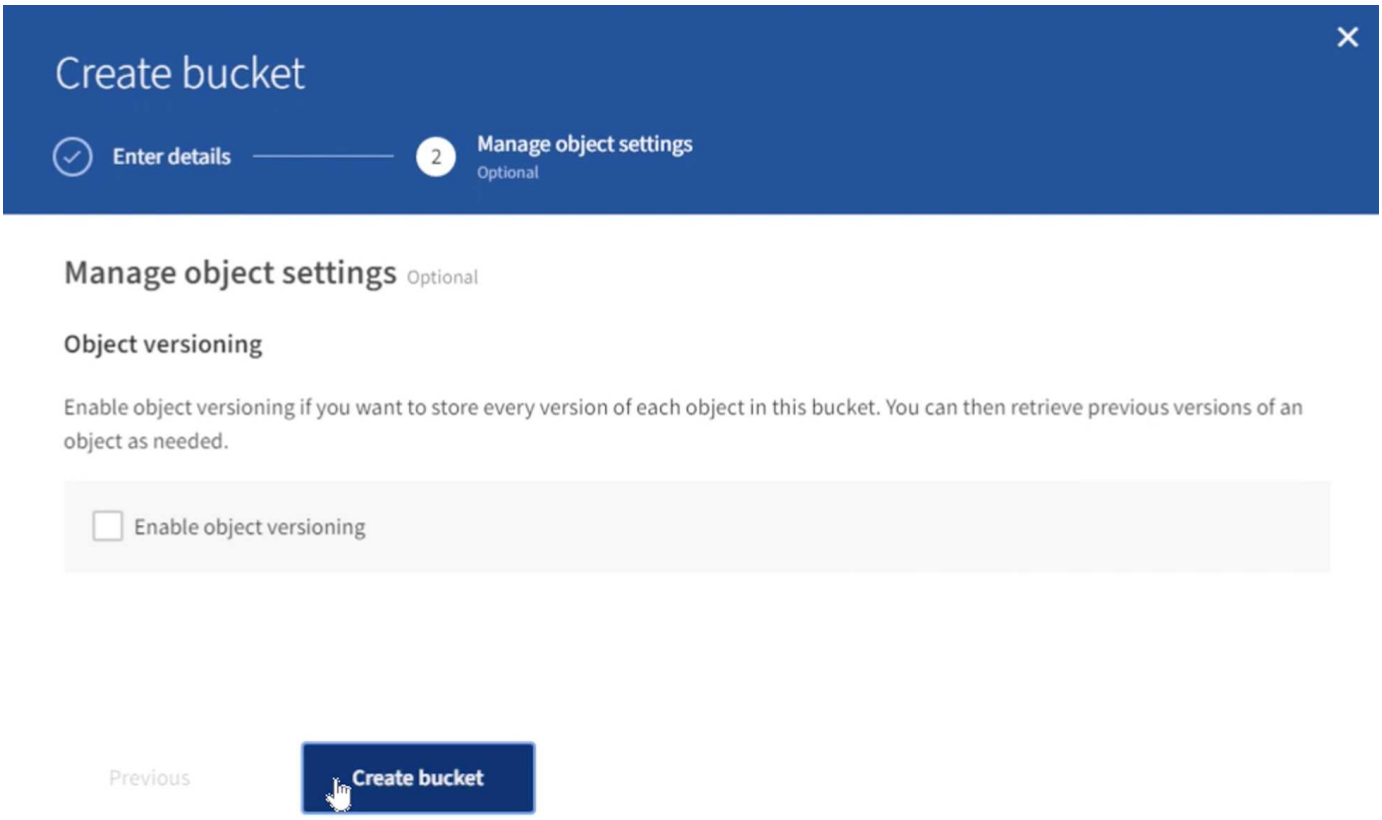
Neste primeiro bucket, ative o controle de versão.



Agora crie um segundo bucket sem o controle de versão ativado.



Não ative o controle de versão neste segundo bucket.



Por Rafael Guedes, e Aron Klein

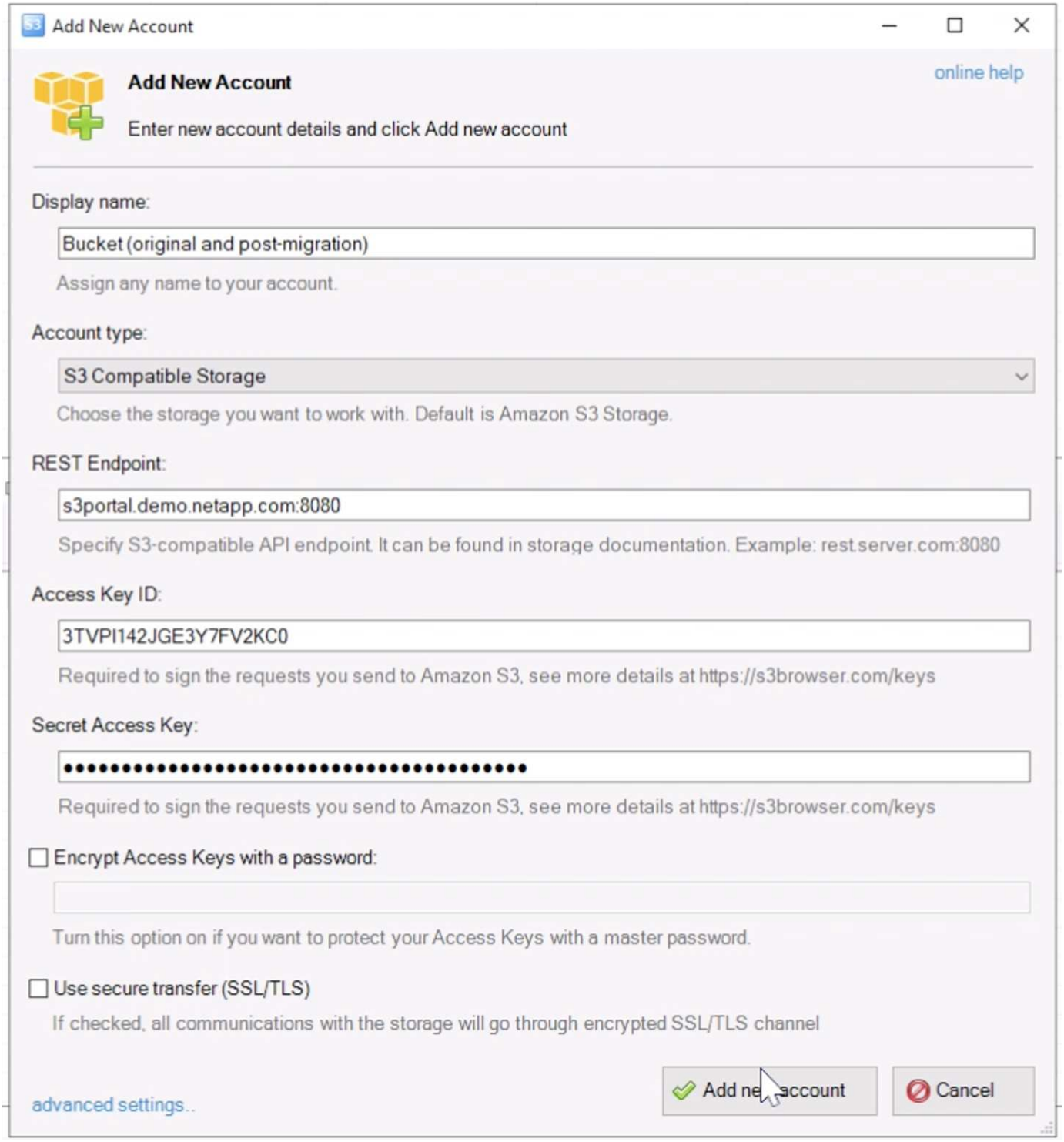
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

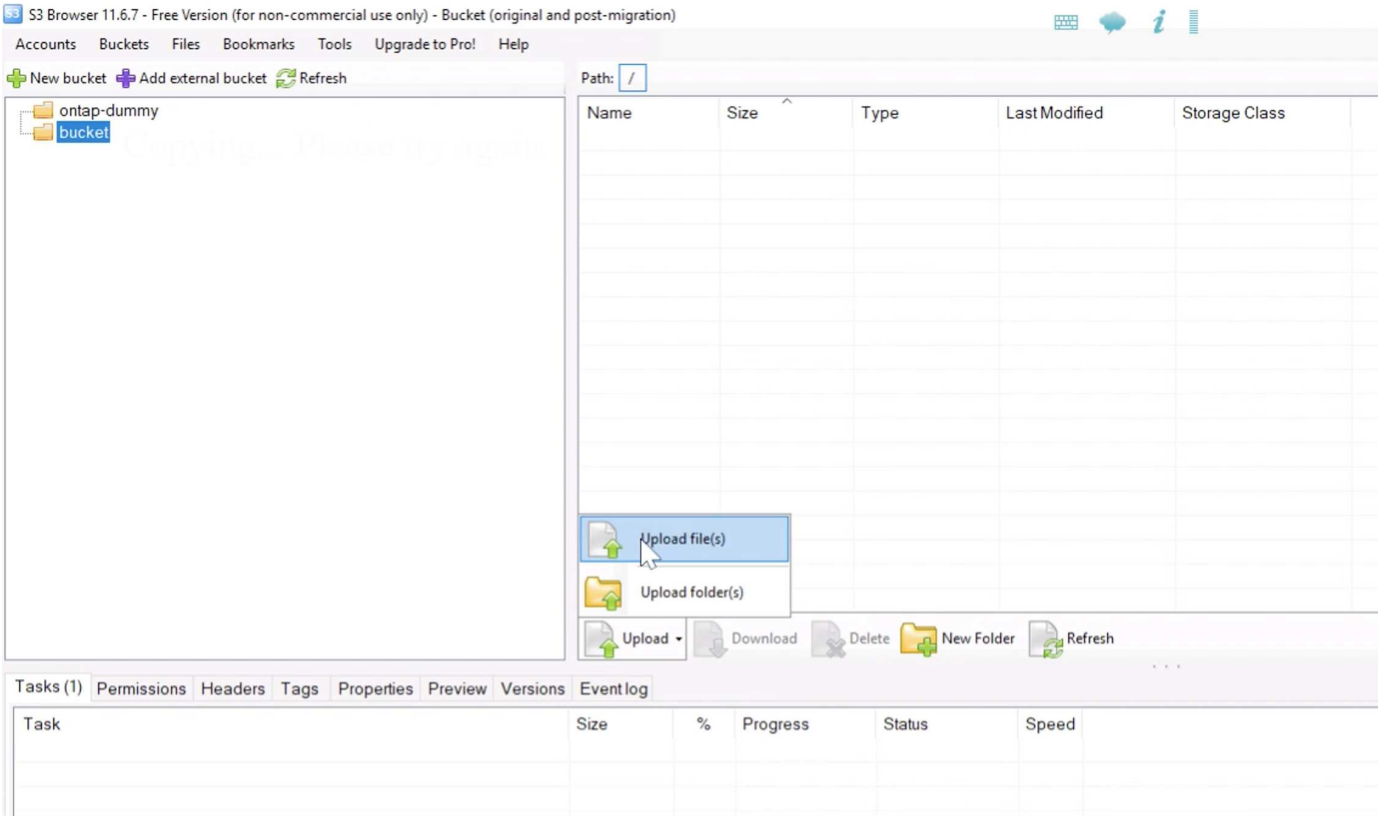
Preencha o repositório de origem

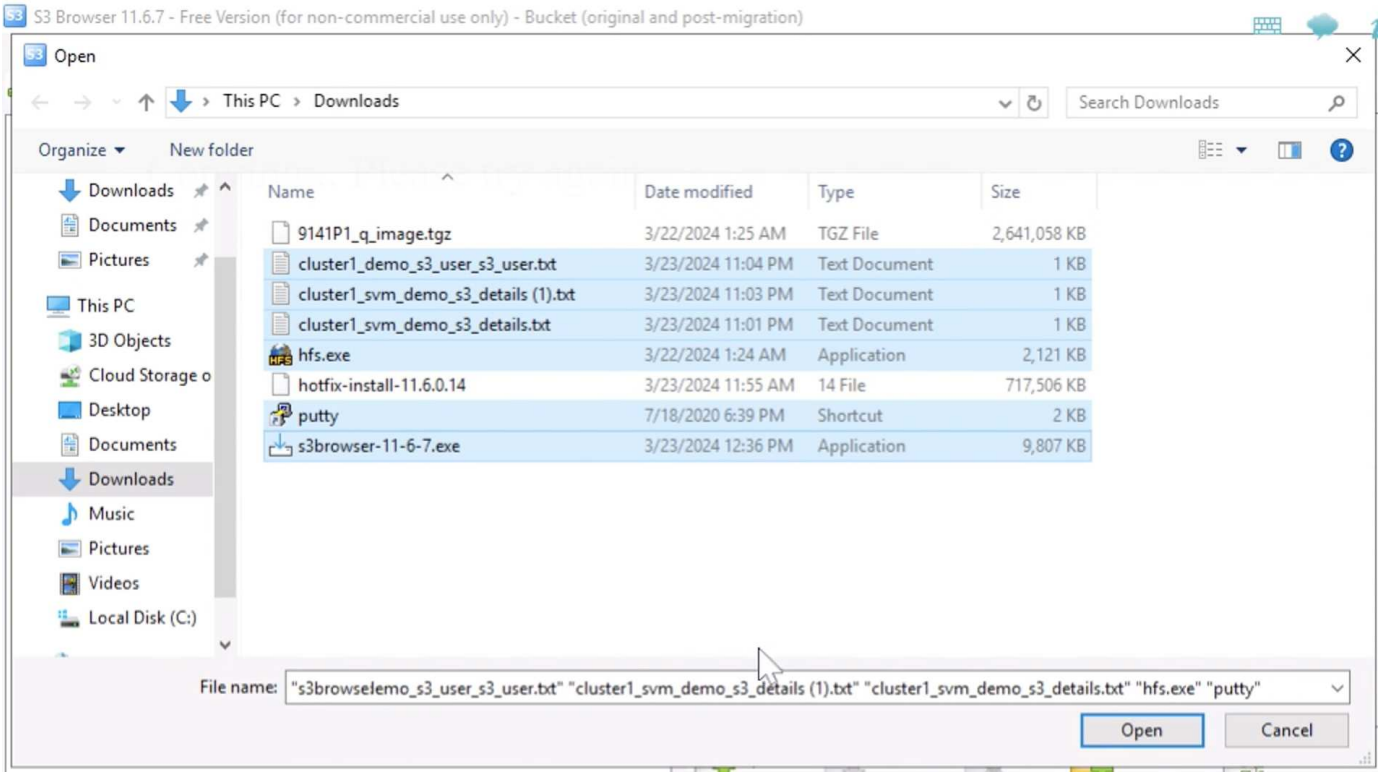
Vamos colocar alguns objetos no bucket do ONTAP de origem. Vamos usar o S3Browser para esta demonstração, mas você pode usar qualquer ferramenta com a qual você está confortável.

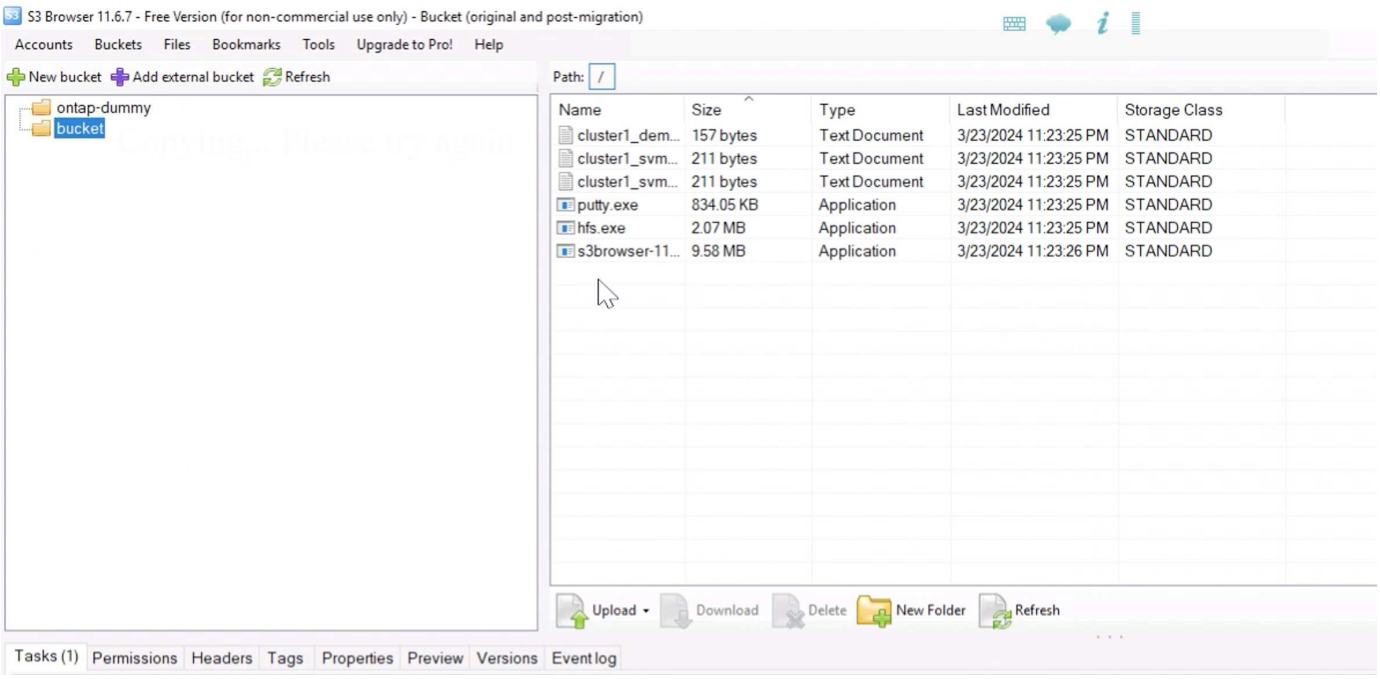
Usando as teclas do usuário ONTAP S3 criadas acima, configure o S3Browser para se conetar ao seu sistema ONTAP.



Agora permite carregar alguns arquivos para o bucket habilitado para versionamento.

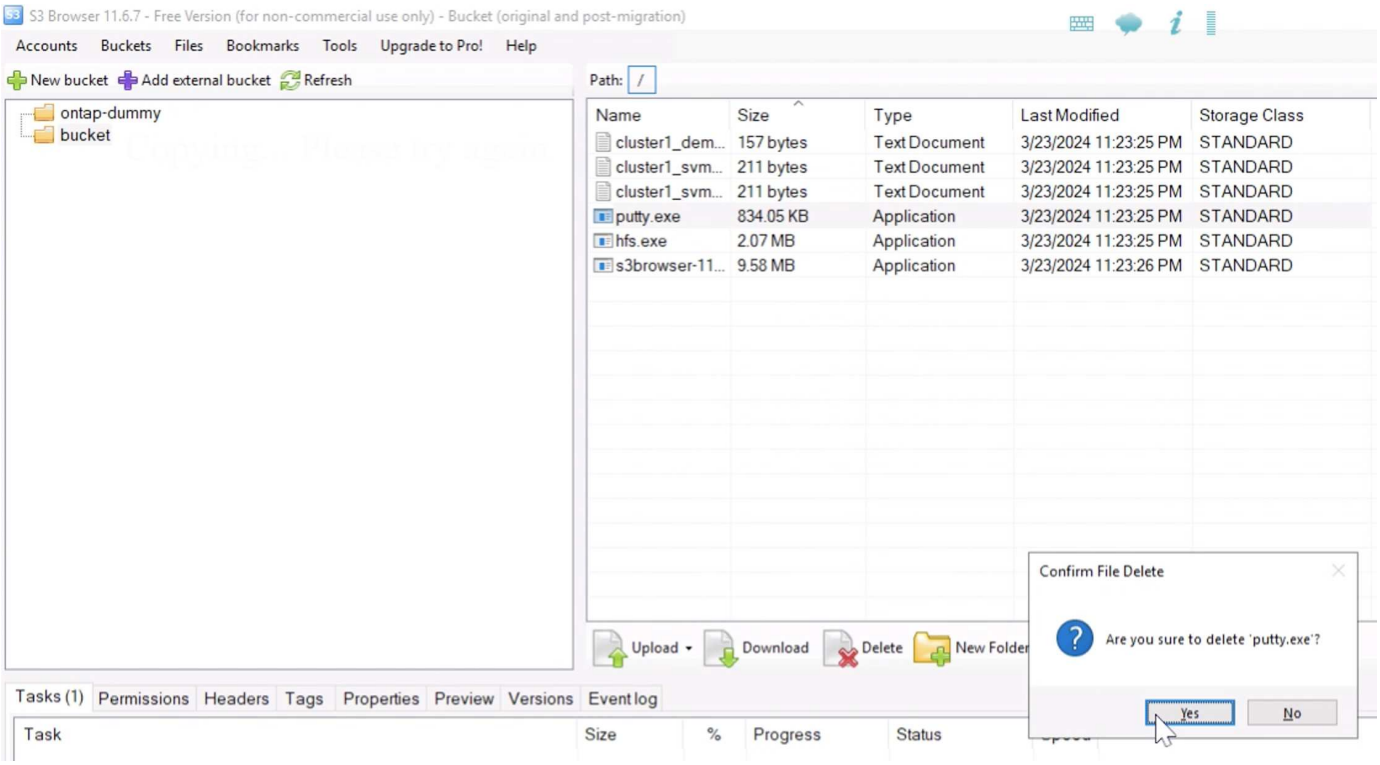

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

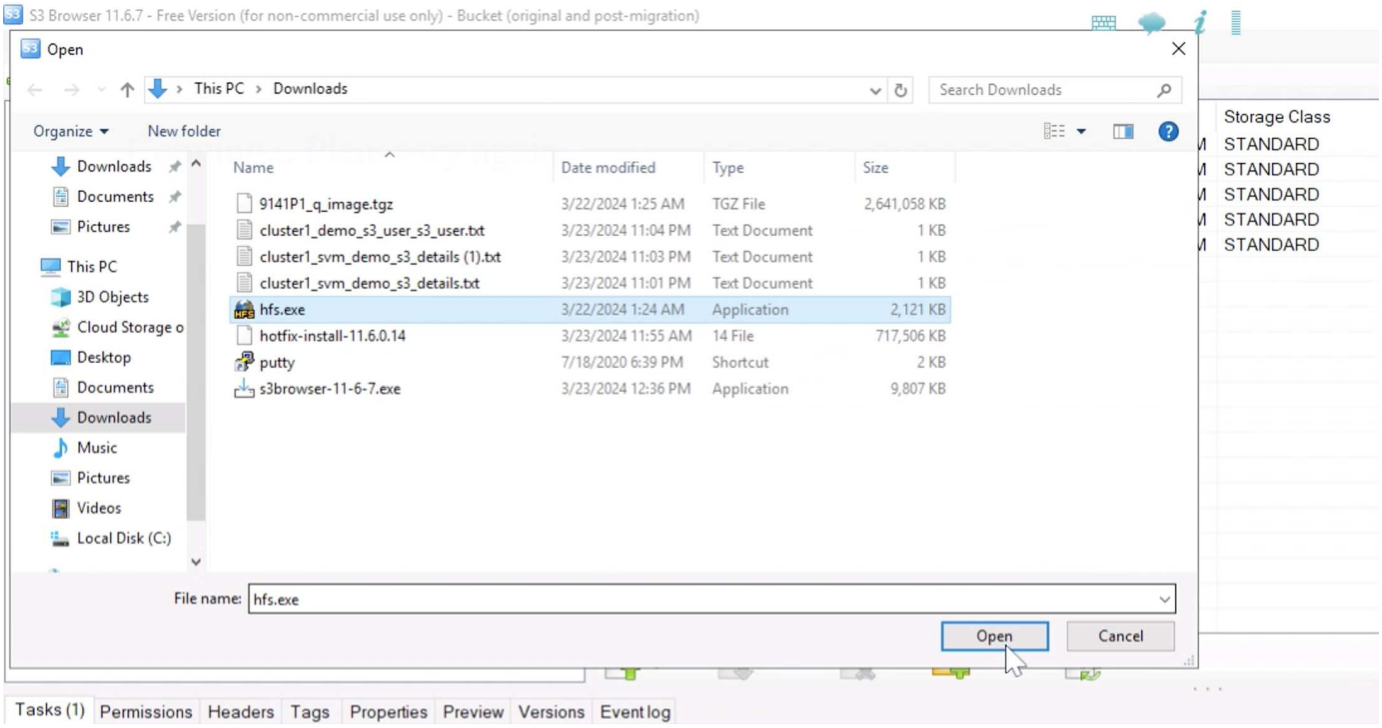


Agora vamos criar algumas versões de objetos no bucket.

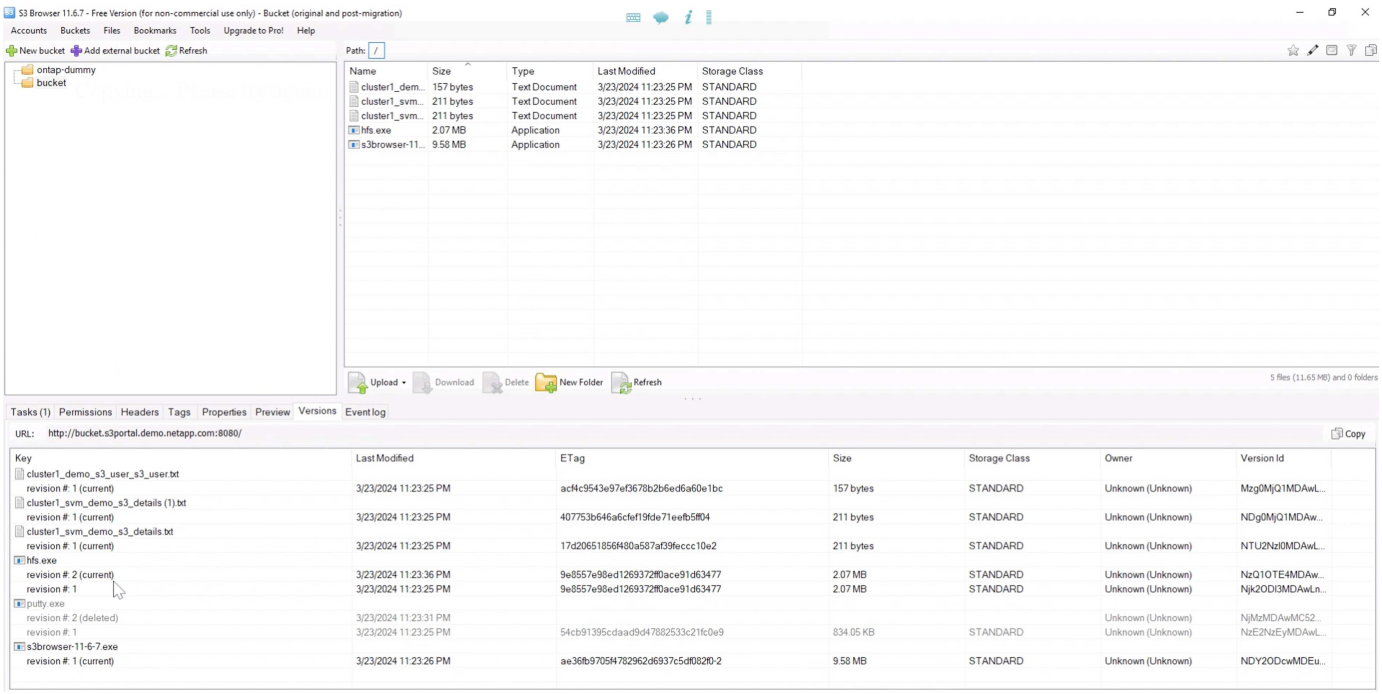
Eliminar um ficheiro.



Faça upload de um arquivo que já existe no bucket para copiar o arquivo sobre si mesmo e criar uma nova versão dele.



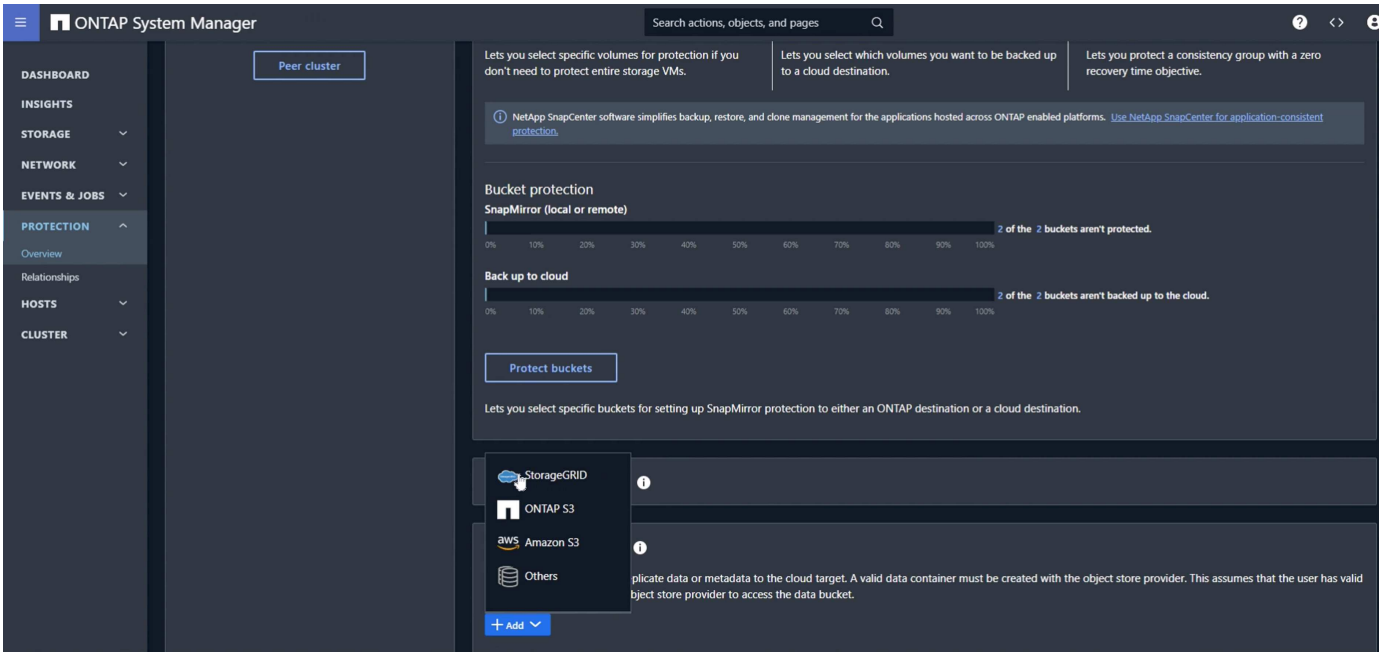
Em S3Browser podemos ver as versões dos objetos que acabamos de criar.



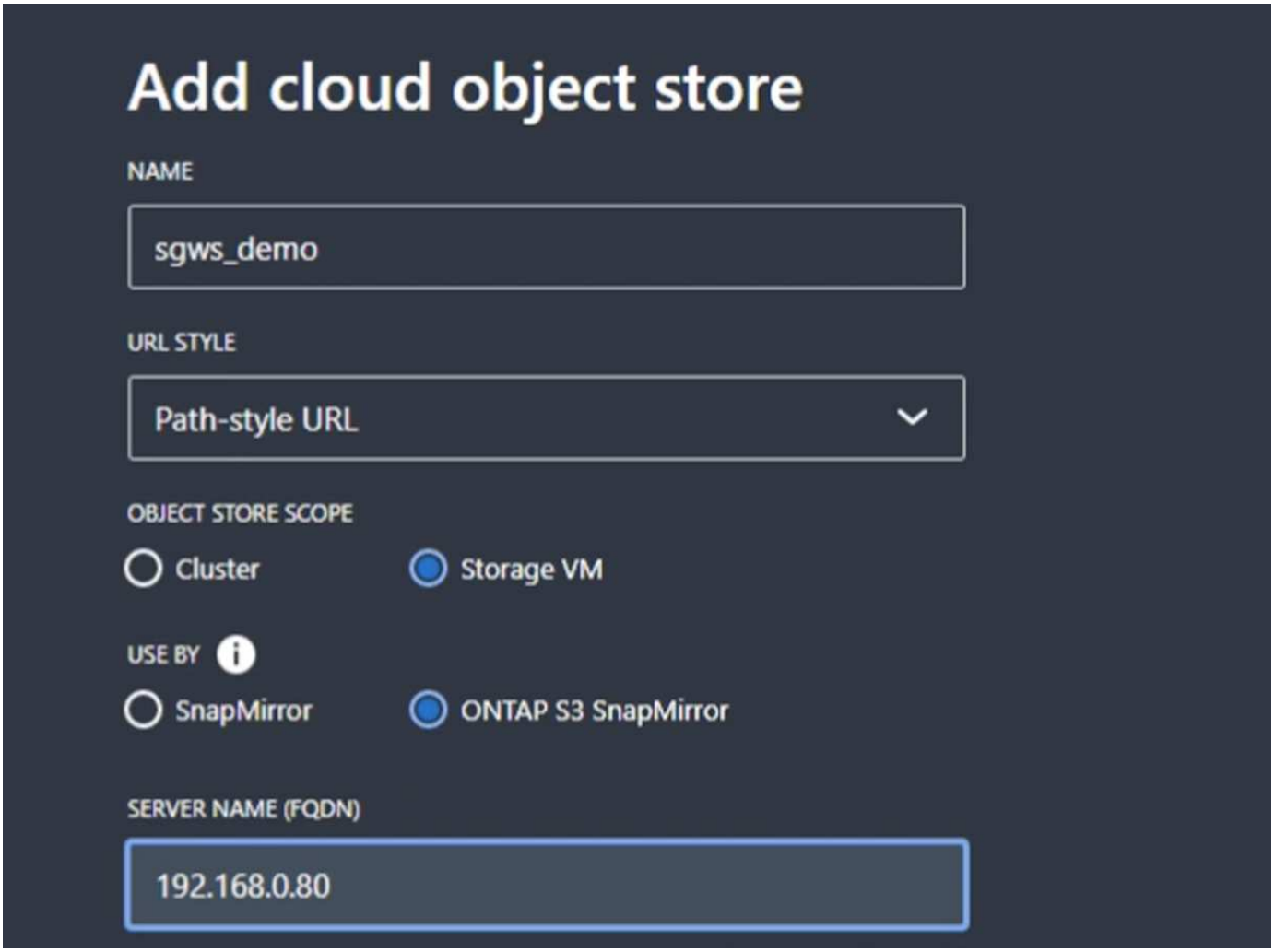
Estabeleça a relação de replicação

Vamos começar a enviar dados do ONTAP para o StorageGRID.

No Gerenciador de sistemas ONTAP, navegue até "proteção/Visão geral". Role para baixo até "Cloud object stores" e clique no botão "Adicionar" e selecione "StorageGRID".



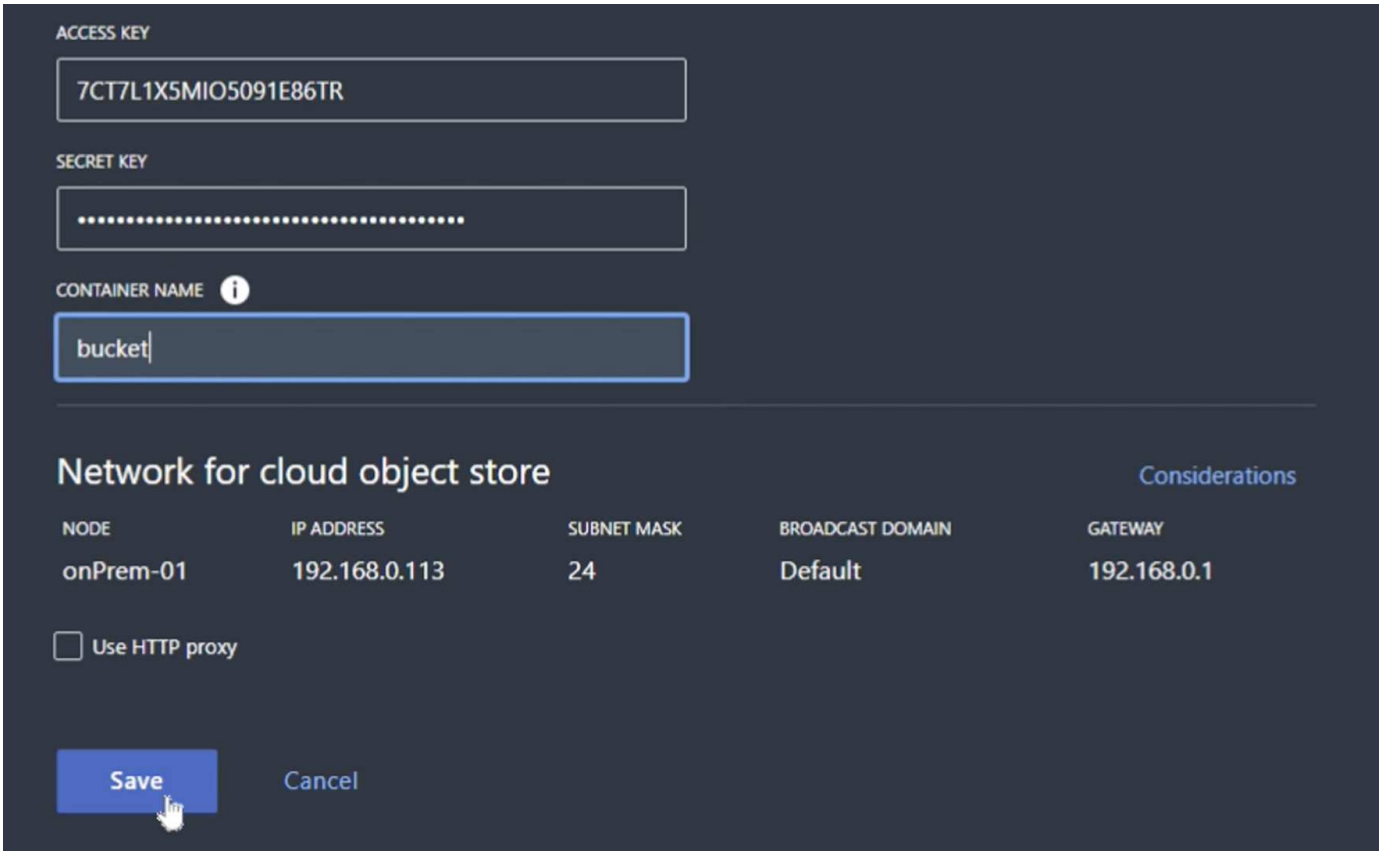
Insira as informações do StorageGRID fornecendo um nome, estilo de URL (para esta demonstração, usaremos URLs Path-styl). Defina o escopo do armazenamento de objetos como "Storage VM".



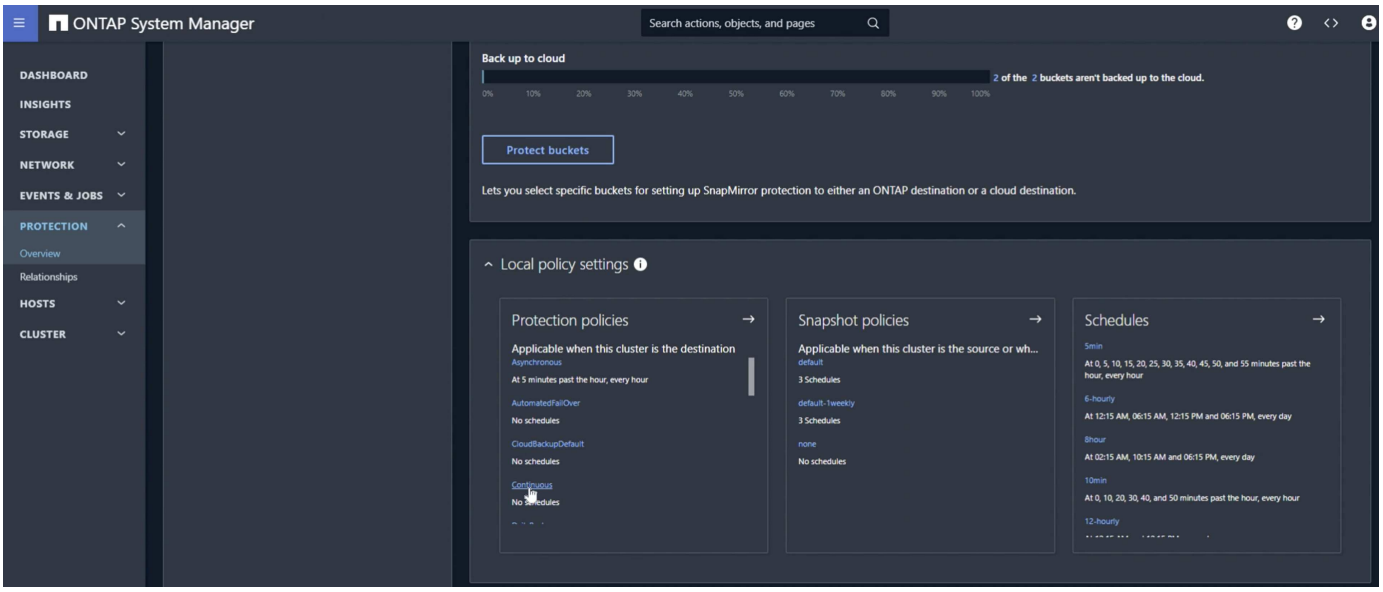
Se você estiver usando SSL, defina a porta de endpoint do balanceador de carga e copie no certificado de

endpoint do StorageGRID aqui. Caso contrário, desmarque a caixa SSL e insira a porta de endpoint HTTP aqui.

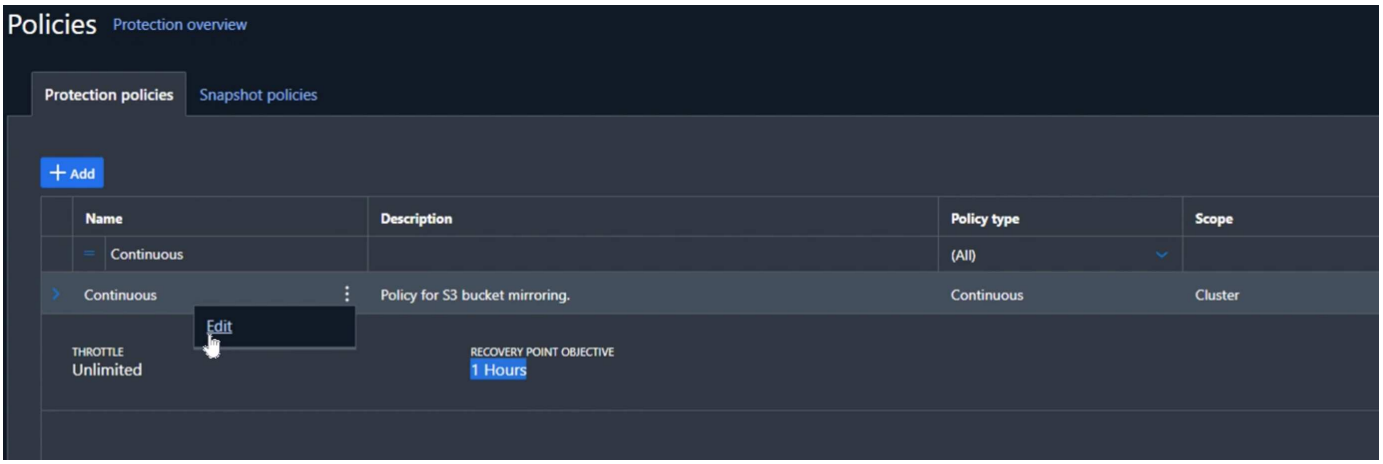
Insira as chaves S3 e o nome do bucket do usuário do StorageGRID na configuração do StorageGRID acima para o destino.



Agora que temos um destino configurado, podemos configurar as configurações de política para o destino. Expanda "local policy settings" (Definições de política local) e selecione "Continuous" (contínuo).



Edite a política contínua e altere o "objetivo do ponto de recuperação" de "1 horas" para "3 segundos".

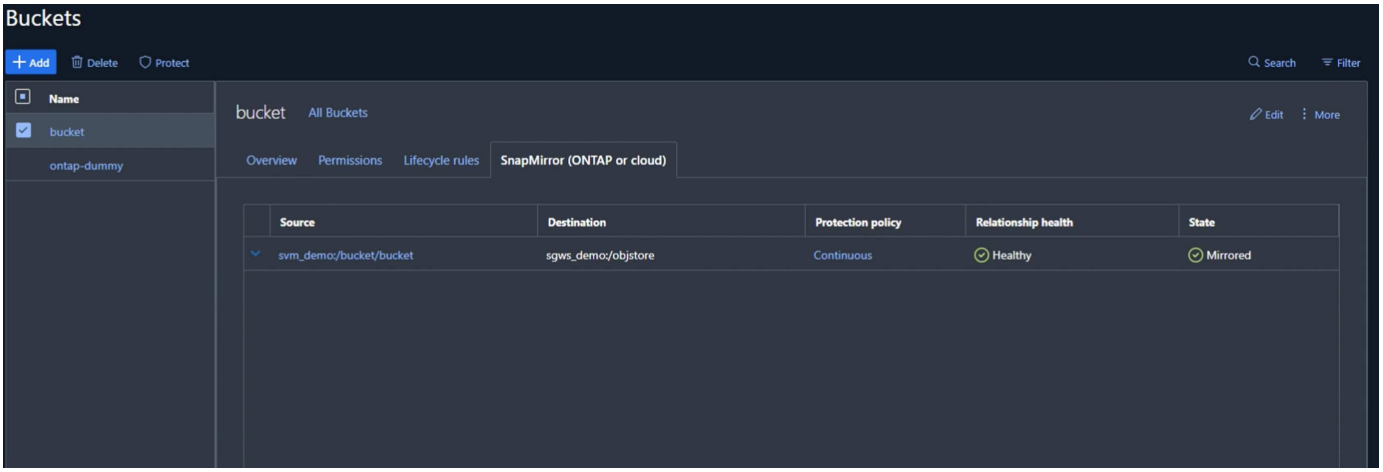


Agora podemos configurar o SnapMirror para replicar o bucket.

SnapMirror create -source-path sv_demo: /Bucket/bucket -destination-path sgws_demo: /Objstore -policy contínuo

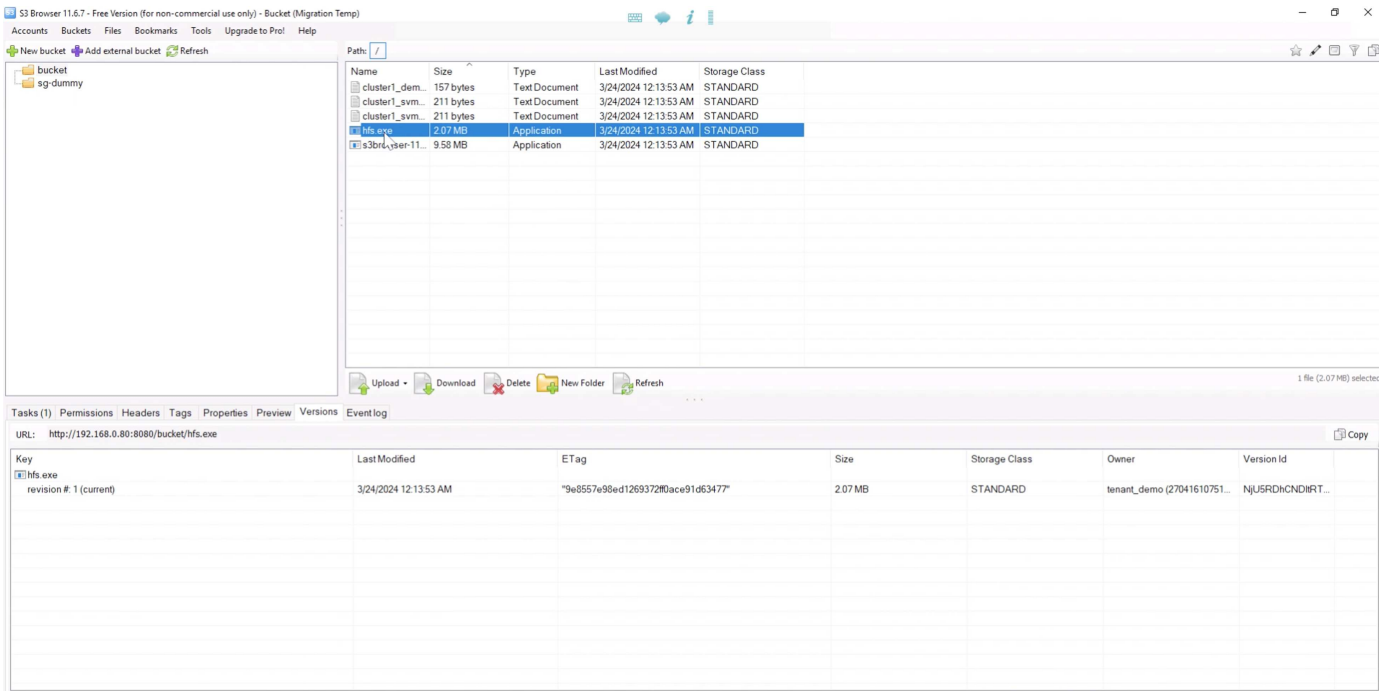
O balde agora mostrará um símbolo de nuvem na lista de buckets sob proteção.

Se selecionarmos o bucket e irmos para a guia "SnapMirror (ONTAP ou nuvem)", veremos o status do SnapMirror Repationship.

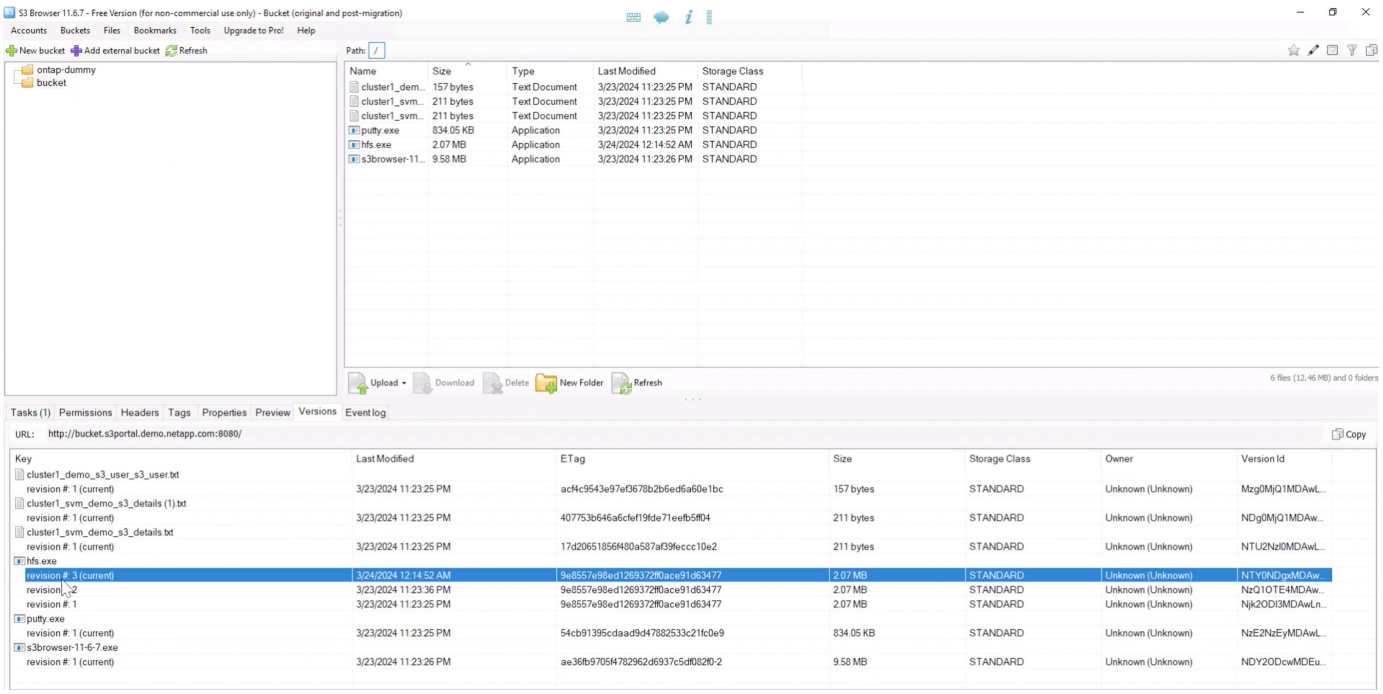


Os detalhes da replicação

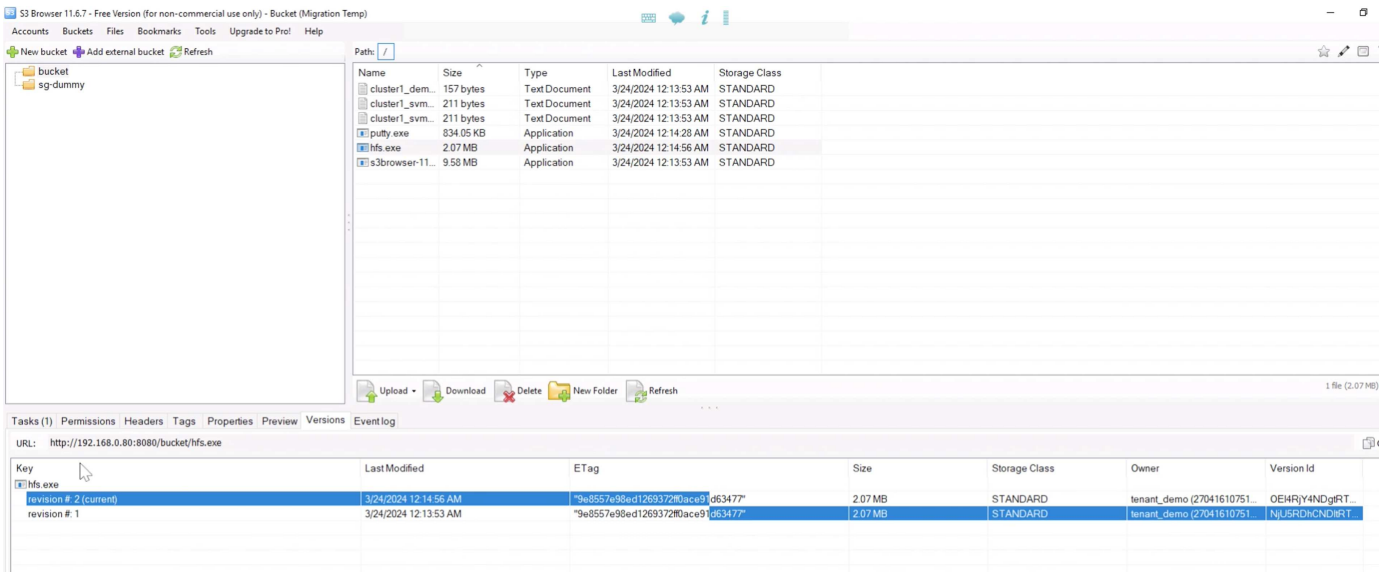
Agora temos um bucket replicando com sucesso do ONTAP para o StorageGRID. Mas o que está realmente replicando? Nossa origem e destino são ambos buckets versionados. As versões anteriores também replicam para o destino? Se olharmos para o nosso bucket do StorageGRID com S3Browser, veremos que as versões existentes não replicaram e nosso objeto excluído não existe, nem um marcador de exclusão para esse objeto. Nosso objeto duplicado tem apenas a versão 1 no bucket do StorageGRID.



Em nosso bucket do ONTAP, vamos adicionar uma nova versão ao nosso mesmo objeto que usamos anteriormente e ver como ele se replica.



Se olharmos para o lado do StorageGRID, veremos que uma nova versão foi criada neste bucket também, mas está faltando a versão inicial de antes do relacionamento do SnapMirror.



Isso ocorre porque o processo ONTAP SnapMirror S3 replica apenas a versão atual do objeto. É por isso que criamos um bucket versionado no lado StorageGRID para ser o destino. Desta forma, o StorageGRID pode manter um histórico de versões dos objetos.

Por Rafael Guedes, e Aron Klein

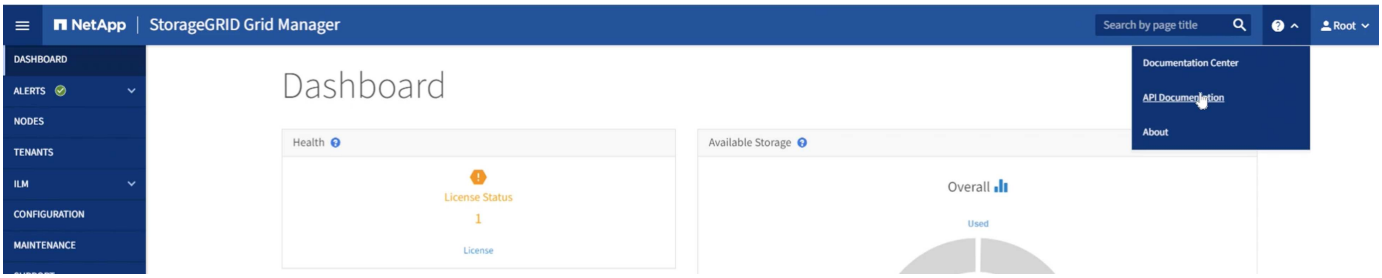
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

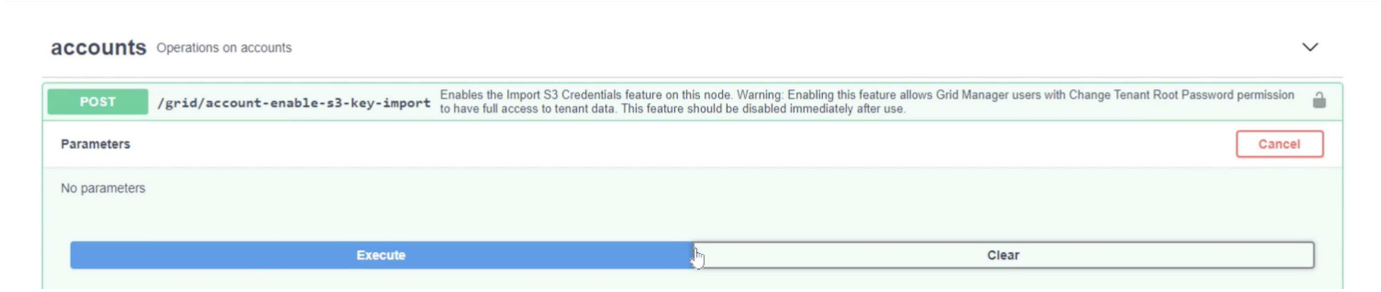
Migrar S3 chaves

Para uma migração, na maioria das vezes você vai querer migrar as credenciais para os usuários em vez de gerar novas credenciais no lado do destino. O StorageGRID fornece apis para permitir que as chaves S3 sejam importadas para um usuário.

Fazer login na IU de gerenciamento do StorageGRID (não na IU do gerenciador de locatários) abra a página do Swagger de Documentação da API.

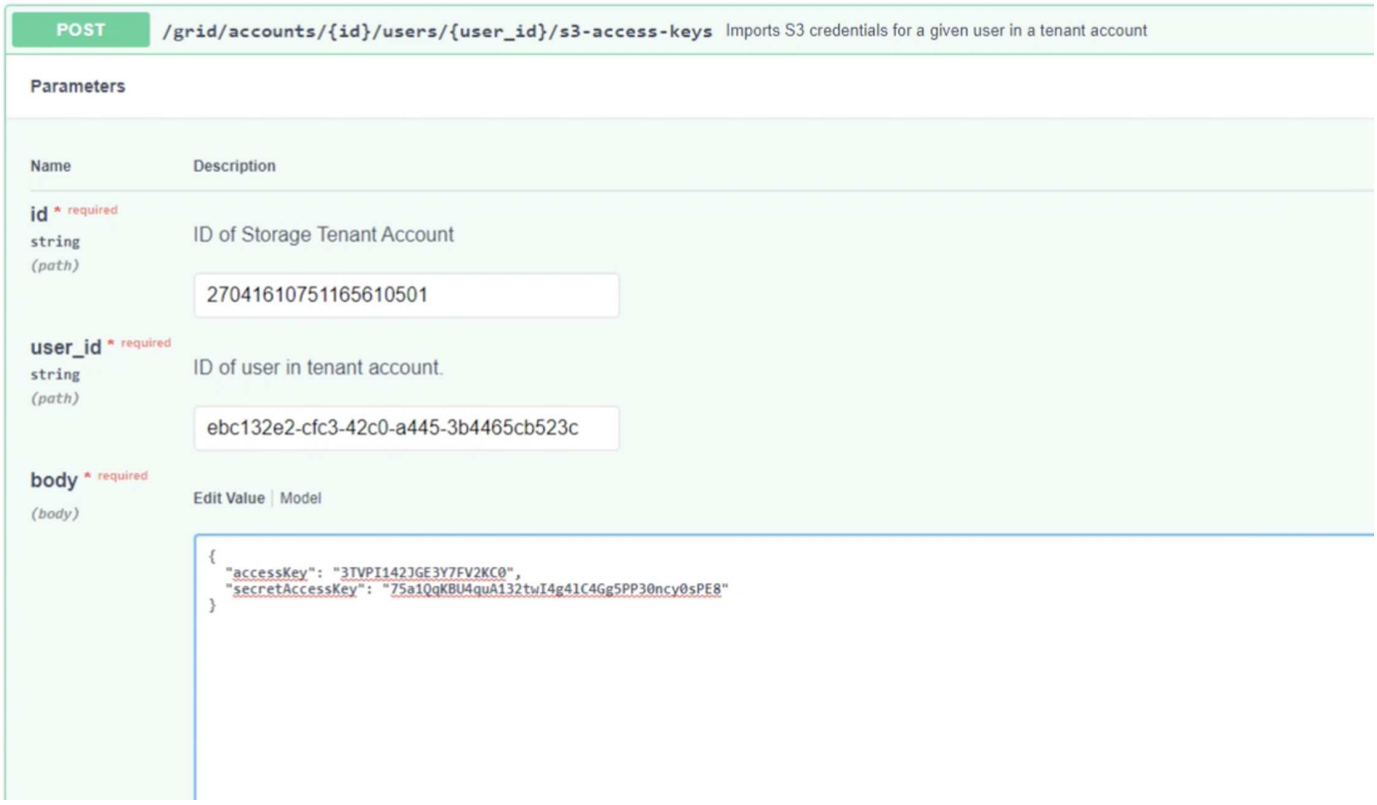


Expanda a seção "Contas", selecione o "POST /grid/account-enable-S3-key-import", clique no botão "Experimente" e clique no botão executar.

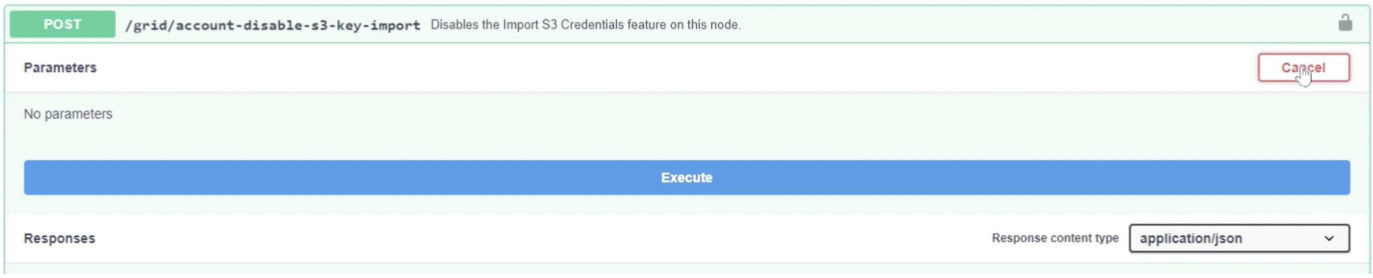


Agora role para baixo ainda em "Contas" para "POST /grid/accounts/"id"/Users/"user_id"/S3-access-keys"

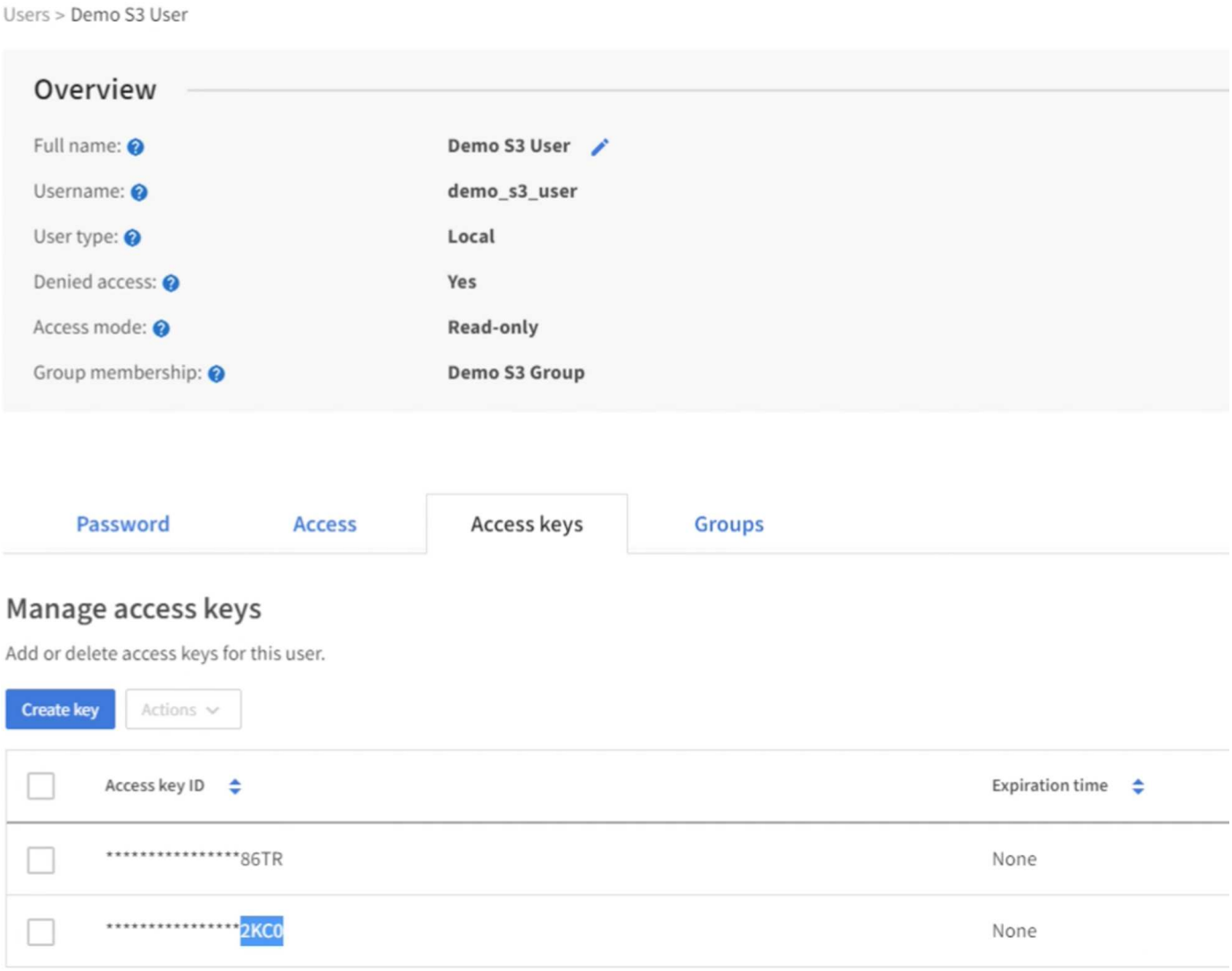
Aqui é onde vamos inserir o ID do locatário e o ID da conta de usuário que coletamos anteriormente. Preencha os campos e as chaves de nosso usuário do ONTAP na caixa json. Você pode definir a expiração das chaves ou remover o " , "expira": 123456789" e clique em executar.



Depois de concluir todas as suas importações de chave de usuário, você deve desativar a função de importação de chave em "Contas" "POST /grid/account-disable-S3-key-import"



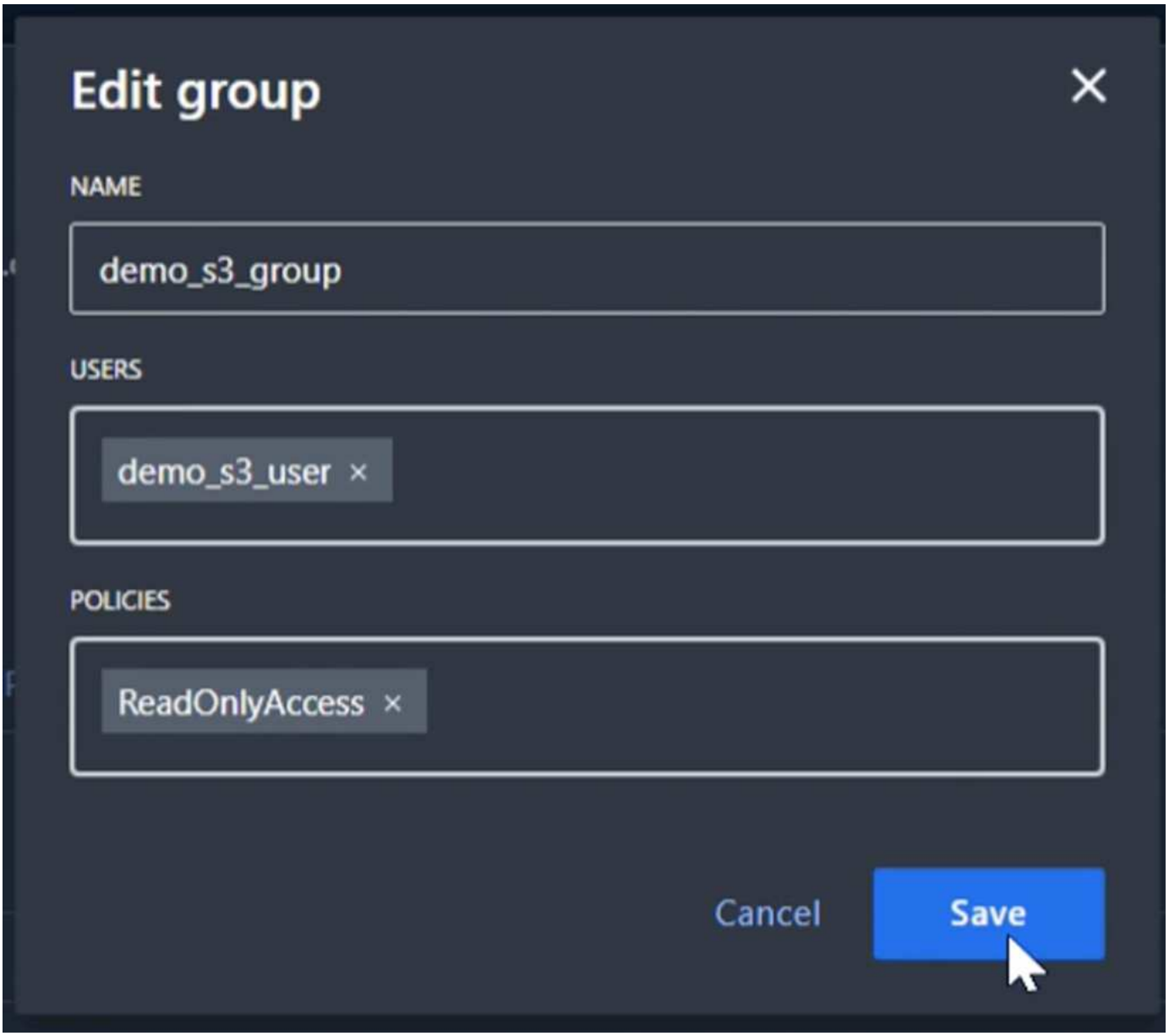
Se olharmos para a conta de usuário na IU do gerenciador de inquilinos, podemos ver a nova chave foi adicionada.



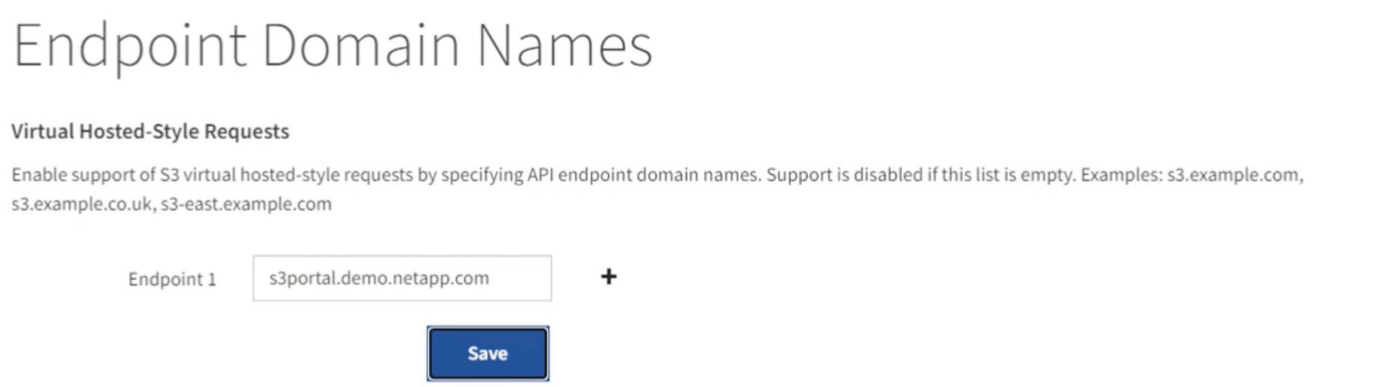
O corte final

Se a intenção é ter um bucket de replicação perpetuamente de ONTAP para StorageGRID, você pode terminar aqui. Se esta é uma migração do ONTAP S3 para o StorageGRID, então é hora de acabar com isso e cortar.

Dentro do gerenciador do sistema ONTAP, edite o grupo S3 e defina-o como "ReadOnlyAccess". Isso evitará mais que os usuários escrevam no bucket do ONTAP S3.



Tudo o que resta a fazer é configurar o DNS para apontar do cluster do ONTAP para o ponto de extremidade do StorageGRID. Certifique-se de que o seu certificado de endpoint está correto e, se você precisar de solicitações de estilo hospedadas virtuais, adicione os nomes de domínio de endpoint no StorageGRID



Seus clientes precisarão esperar que o TTL expire ou liberar DNS para resolver para o novo sistema para que você possa testar se tudo está funcionando. Tudo o que resta é limpar as chaves S3 temporárias iniciais que usamos para testar o acesso a dados StorageGRID (NÃO as chaves importadas), remover as relações SnapMirror e remover os dados ONTAP.

Por Rafael Guedes, e Aron Klein

Guias de ferramentas e aplicações

Use o conetor Cloudera Hadoop S3A com StorageGRID

Por Angela Cheng

Hadoop tem sido um favorito dos cientistas de dados há algum tempo. O Hadoop permite o processamento distribuído de grandes conjuntos de dados entre clusters de computadores usando estruturas de programação simples. O Hadoop foi projetado para escalar de servidores únicos para milhares de máquinas, com cada máquina possuindo computação e armazenamento locais.

Por que usar o S3A para fluxos de trabalho Hadoop?

À medida que o volume de dados cresceu com o tempo, a abordagem de adicionar novas máquinas 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 cliente 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.

Configure o conetor S3A para usar o StorageGRID

Pré-requisitos

- Um URL de endpoint do StorageGRID S3, uma chave de acesso do locatário S3 e uma chave secreta para o teste de conexão do Hadoop S3A.
- Um cluster Cloudera e uma permissão root ou sudo para cada host no cluster para instalar o pacote Java.

Em abril de 2022, o Java 11.0.14 com Cloudera 7.1.7 foi testado contra o StorageGRID 11,5 e 11,6. No entanto, o número da versão Java pode ser diferente no momento de uma nova instalação.

Instale o pacote Java

1. Verifique "Matriz de suporte Cloudera" se há a versão do JDK suportada.
2. Faça o download do "Pacote Java 11.x" que corresponde ao sistema operacional do cluster Cloudera. Copie este pacote para cada host no cluster. Neste exemplo, o pacote rpm é usado para o CentOS.
3. Faça login em cada host como root ou usando uma conta com permissão sudo. Execute as seguintes etapas em cada host:
   a. Instale o pacote:

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

   b. Verifique onde o Java está instalado. Se várias versões estiverem instaladas, defina a versão recém-instalada como padrão:

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. Adicione esta linha ao final `/etc/profile` do . O caminho deve corresponder ao caminho da seleção acima:

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. Execute o seguinte comando para que o perfil entre em vigor:

```
source /etc/profile
```

Configuração Cloudera HDFS S3A

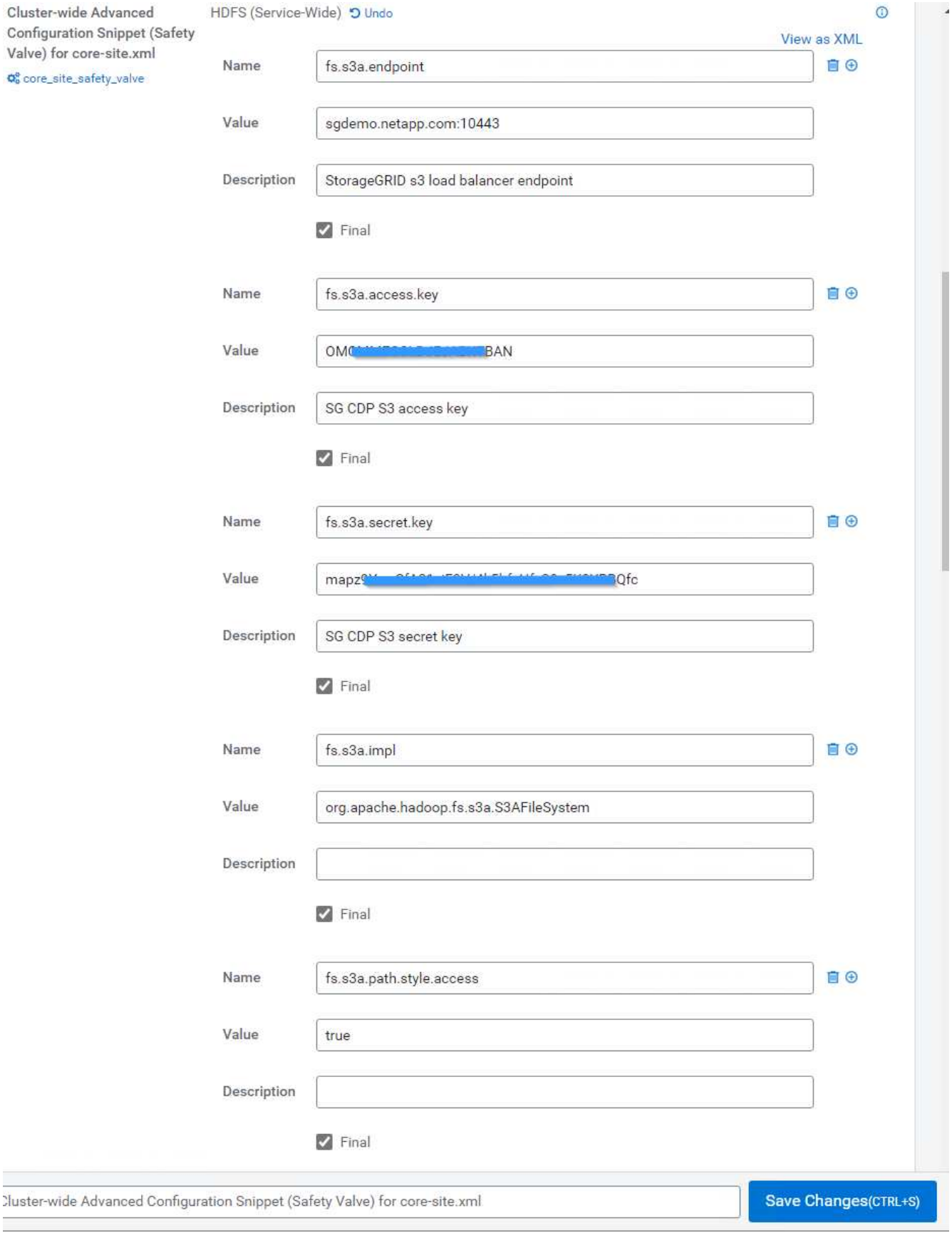
Passos

1. Na GUI do Cloudera Manager, selecione clusters > HDFS e selecione Configuração.
2. NA CATEGORIA, selecione Avançado e role para baixo para localizar `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Clique no sinal e adicione os seguintes pares de valores.

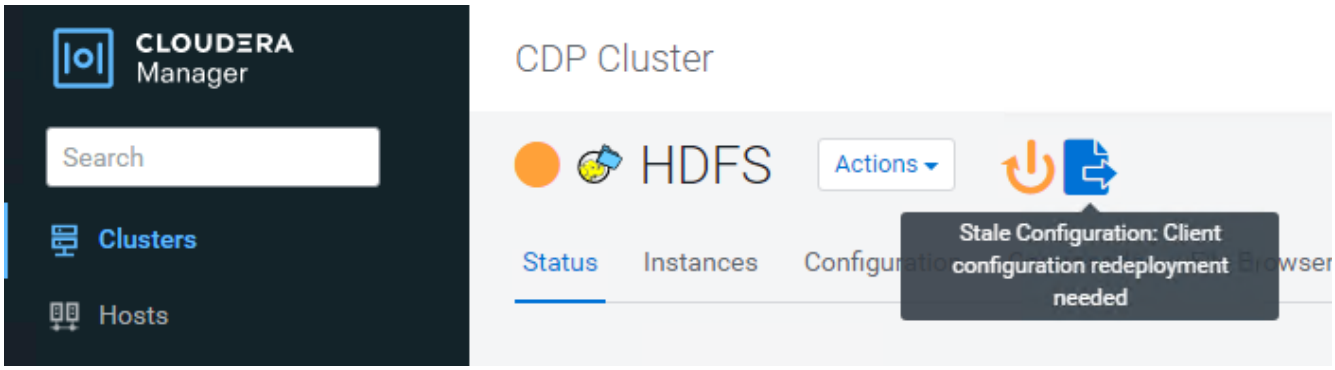
Nome	Valor
fs.s3a.access.key	_ Chave de acesso S3 do cliente a partir de StorageGRID>_
fs.s3a.secret.key	_ Chave secreta do cliente S3 da StorageGRID>_
fs.s3a.connection.ssl.enabled	[true ou false] (o padrão é https se esta entrada estiver ausente)
fs.s3a.endpoint	_ Endpoint do cliente StorageGRID S3:port>_
fs.s3a.impl	org.apache.hadoop.fs.s3a.S3AFileSystem

Nome	Valor
fs.s3a.path.style.access	[verdadeiro ou falso] (o padrão é o estilo de host virtual se essa entrada estiver ausente)

Captura de tela de amostra



4. Clique no botão Salvar alterações. Selecione o ícone Configuração obsoleta na barra de menus do HDFS, selecione Reiniciar Serviços obsoletos na próxima página e selecione Reiniciar agora.



Teste a conexão S3A com o StorageGRID

Execute o teste básico de conexão

Faça login em um dos hosts no cluster Cloudera e `hadoop fs -ls s3a://*<bucket-name>*/`digite .

O exemplo a seguir usa syle de caminho com um bucket de teste hdfs pré-existente e um objeto de teste.

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

Solução de problemas

Cenário 1

Use uma conexão HTTPS com o StorageGRID e obtenha um `handshake_failure` erro após um tempo limite de 15 minutos.

Motivo: versão antiga do JRE/JDK usando pacote de codificação TLS desatualizado ou não suportado para conexão com o StorageGRID.

- Exemplo de mensagem de erro*

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

Resolução: Certifique-se de que o JDK 11.x ou posterior esteja instalado e definido como padrão a biblioteca Java. Consulte Instale o pacote Javaa secção para obter mais informações.

Cenário 2:

Falha ao se conetar ao StorageGRID com mensagem de erro `Unable to find valid certification path to requested target`.

Razão: o certificado do servidor de endpoint StorageGRID S3 não é confiável pelo programa Java.

Exemplo de mensagem de erro:

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

Resolução: a NetApp recomenda o uso de um certificado de servidor emitido por uma autoridade pública de assinatura de certificado conhecida para garantir que a autenticação seja segura. Como alternativa, adicione uma CA personalizada ou certificado de servidor ao armazenamento de confiança Java.

Siga as etapas a seguir para adicionar uma CA personalizada do StorageGRID ou um certificado de servidor ao armazenamento de confiança do Java.

1. Faça backup do arquivo Java cacerts padrão existente.

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. Importe o cert de endpoint do StorageGRID S3 para o armazenamento de confiança Java.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

Dicas de solução de problemas

1. Aumente o nível de log do hadoop para DEPURAR.

   ```
   export HADOOP_ROOT_LOGGER=hadoop.root.logger=DEBUG,console
   ```

2. Execute o comando e direcione as mensagens de log para error.log.

   ```
   hadoop fs -ls s3a://<bucket-name>/ &>error.log
   ```

Por Angela Cheng

Use o S3cmd para testar e demonstrar o acesso S3 no StorageGRID

Por Aron Klein

S3cmd é uma ferramenta de linha de comando gratuita e cliente para operações S3. Você pode usar o s3cmd para testar e demonstrar o acesso S3 no StorageGRID.

Instale e configure o S3cmd

Para instalar o S3cmd em uma estação de trabalho ou servidor, faça o download do "Linha de comando S3 cliente". o s3cmd é pré-instalado em cada nó do StorageGRID como uma ferramenta para auxiliar na solução de problemas.

Etapas iniciais de configuração

1. s3cmd --configure
2. Forneça apenas access_key e secret_key, para que o resto mantenha os padrões.
3. Testar o acesso com as credenciais fornecidas? [Y/n]: N (ignorar o teste, pois ele falhará)
4. Guardar definições? [y/N] y
   a. Configuração guardada em '/root/.s3cfg'
5. Em .s3cfg, deixe os campos host_base e host_bucket vazios após o sinal "
   a. base_de_host
   b. host_bucket

Se você especificar host_base e host_bucket na etapa 4, não será necessário especificar um endpoint com --host na CLI. Exemplo:

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

Exemplos básicos de comandos

- **Crie um bucket:**

```
s3cmd mb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Liste todos os baldes:**

```
s3cmd ls --host=<endpoint>:<port> --no-check-certificate
```

- **Liste todos os baldes e seus conteúdos:**

```
s3cmd la --host=<endpoint>:<port> --no-check-certificate
```

- **Liste objetos em um bucket específico:**

```
s3cmd ls s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Excluir um balde:**

```
s3cmd rb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Coloque um objeto:**

```
s3cmd put <file> s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Obter um objeto:**

```
s3cmd get s3://<bucket>/<object> <file> --host=<endpoint>:<port> --no-check
-certificate
```

- **Excluir um objeto:**

```
s3cmd del s3://<bucket>/<object> --host=<endpoint>:<port> --no-check
-certificate
```

Banco de dados do modo Eon usando NetApp StorageGRID como armazenamento comunitário

Por Angela Cheng

Este guia descreve o procedimento para criar um banco de dados do modo Vertica Eon com armazenamento comunitário no NetApp StorageGRID.

Introdução

Vertica é um software de gerenciamento de banco de dados analítico. É uma plataforma de armazenamento colunar projetada para lidar com grandes volumes de dados, o que permite um desempenho de consulta muito rápido em um cenário tradicionalmente intensivo. Um banco de dados Vertica é executado em um dos dois modos: EON ou Enterprise. Você pode implantar os dois modos no local ou na nuvem.

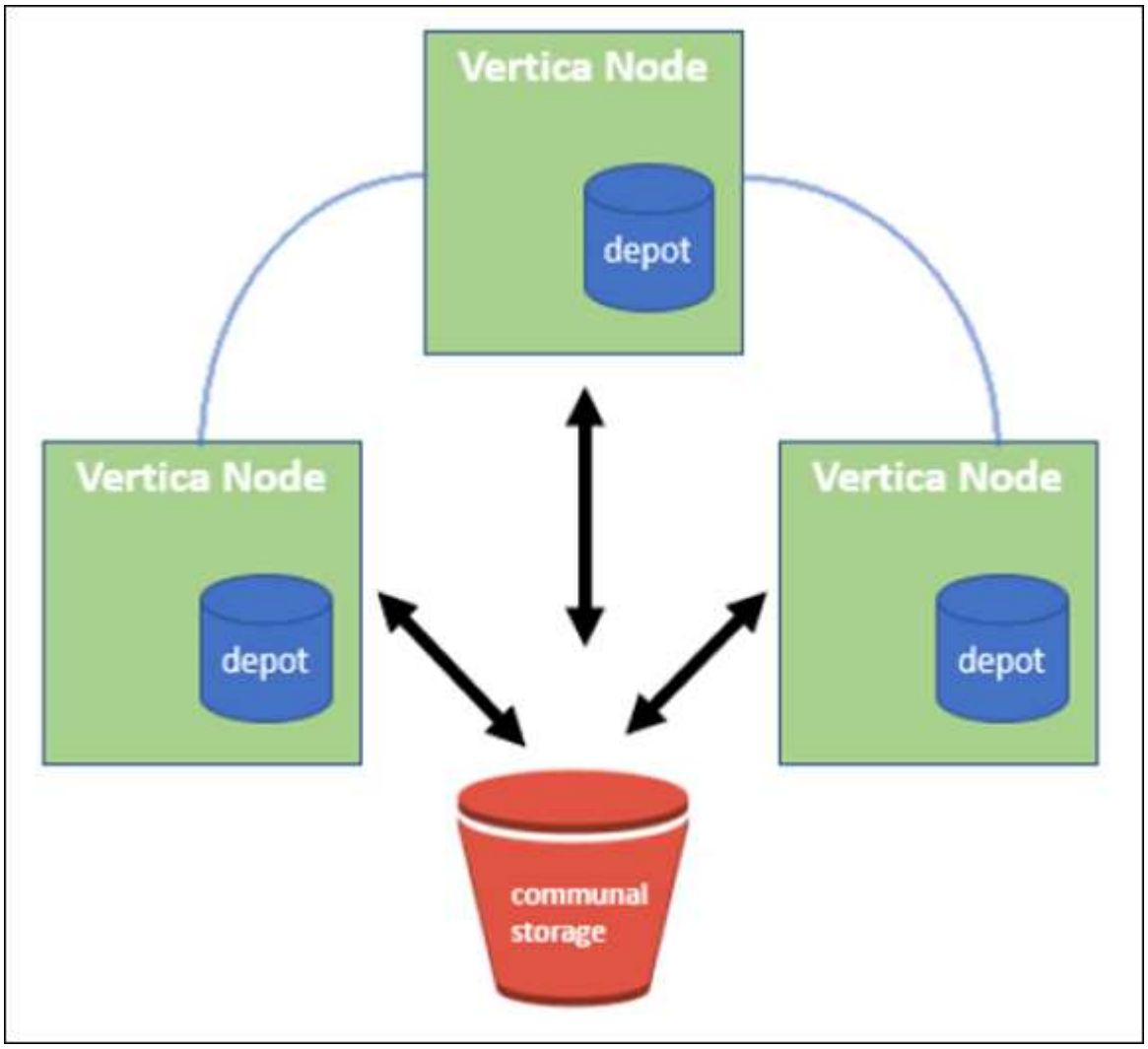
Os modos EON e Enterprise diferem principalmente no local onde armazenam dados:

- As bases de dados do modo EON utilizam armazenamento comunitário para os seus dados. Isso é recomendado pela Vertica.
- Os bancos de dados do modo empresarial armazenam dados localmente no sistema de arquivos de nós que compõem o banco de dados.

Arquitetura do modo EON

O modo EON separa os recursos computacionais da camada de armazenamento comum do banco de dados, o que permite que a computação e o armazenamento sejam dimensionados separadamente. O Vertica no modo Eon é otimizado para lidar com cargas de trabalho variáveis e isolá-las umas das outras usando recursos de computação e armazenamento separados.

O modo EON armazena dados em um armazenamento de objetos compartilhado chamado armazenamento comunitário - um bucket do S3, hospedado no local ou no Amazon S3.



Armazenamento comunitário

Em vez de armazenar dados localmente, o modo Eon usa um único local de armazenamento comunitário para todos os dados e o catálogo (metadados). O armazenamento comum é o local de armazenamento centralizado do banco de dados, compartilhado entre os nós do banco de dados.

O armazenamento comunitário tem as seguintes propriedades:

- O armazenamento comum na nuvem ou no local de objetos é mais resiliente e menos suscetível à perda de dados devido a falhas de armazenamento do que armazenamento em disco em máquinas individuais.
- Todos os dados podem ser lidos por qualquer nó usando o mesmo caminho.
- A capacidade não é limitada pelo espaço de disco nos nós.
- Como os dados são armazenados em comunidade, você pode dimensionar elasticamente seu cluster para atender às demandas em constante mudança. Se os dados fossem armazenados localmente nos nós, adicionar ou remover nós exigiria a movimentação de quantidades significativas de dados entre nós para movê-los dos nós que estão sendo removidos ou para nós recém-criados.

O depósito

Uma desvantagem do armazenamento comunitário é a sua velocidade. Acessar dados de um local compartilhado na nuvem é mais lento do que lê-los a partir do disco local. Além disso, a conexão com o armazenamento comunitário pode se tornar um gargalo se muitos nós estiverem lendo dados de uma só vez. Para melhorar a velocidade de acesso aos dados, os nós em um banco de dados do modo Eon mantêm um cache de dados de disco local chamado de depósito. Ao executar uma consulta, os nós primeiro verificam se os dados de que precisam estão no depósito. Se for, então ele termina a consulta usando a cópia local dos dados. Se os dados não estiverem no depósito, o nó buscará os dados do armazenamento comunitário e salvará uma cópia no depósito.

Recomendações do NetApp StorageGRID

Vertica armazena dados de banco de dados para armazenamento de objetos como milhares (ou milhões) de objetos compatados (o tamanho observado é de 200 a 500MB por objeto. Quando um usuário executa consultas de banco de dados, o Vertica recupera o intervalo de dados selecionado desses objetos compatados em paralelo usando a chamada DE RECEBIMENTO DE intervalo de bytes. Cada intervalo de bytes GET é de aproximadamente 8KB.

Durante o teste de consultas de usuários do 10TBo depósito do banco de dados, 4.000 a 10.000 solicitações GET (byte-range GET) por segundo foram enviadas para a grade. Ao executar esse teste usando dispositivos SG6060, embora a % de utilização de CPU por nó de appliance seja baixa (cerca de 20% a 30%), 2/3x do tempo de CPU está aguardando a e/S. Uma porcentagem muito pequena (0% a 0,5%) de espera de e/S é observada no SGF6024.

Devido à alta demanda de IOPS pequenos com requisitos de latência muito baixos (a média deve ser inferior a 0,01 segundos), a NetApp recomenda o uso do SFG6024 para serviços de storage de objetos. Se o SG6060 for necessário para tamanhos de banco de dados muito grandes, o cliente deve trabalhar com a equipe de contas Vertica no dimensionamento do depósito para oferecer suporte ao conjunto de dados ativamente consultado.

Para o nó Admin e o nó API Gateway, o cliente pode usar o SG100 ou o SG1000. A escolha depende do número de solicitações de consulta dos usuários em paralelo e tamanho do banco de dados. Se o cliente preferir usar um balanceador de carga de terceiros, a NetApp recomenda um balanceador de carga dedicado para workloads de demanda de alta performance. Para dimensionamento do StorageGRID, consulte a equipe de conta do NetApp.

Outras recomendações de configuração do StorageGRID incluem:

- **Topologia de grade**. Não misture o SGF6024 com outros modelos de dispositivos de armazenamento no mesmo local da grade. Se você preferir usar o SG6060 para proteção de arquivo de longo prazo, mantenha o SGF6024 com um balanceador de carga de grade dedicado em seu próprio local de grade (local físico ou lógico) para um banco de dados ativo para melhorar o desempenho. Misturar diferentes modelos de aparelho no mesmo local reduz o desempenho geral no local.

- **Proteção de dados**. Use cópias replicadas para proteção. Não use codificação de apagamento para um banco de dados ativo. O cliente pode usar a codificação de apagamento para proteção a longo prazo de bancos de dados inativos.
- **Não ative a compressão da grade**. Vertica compacta objetos antes de armazenar em armazenamento de objetos. Ativar a compressão de grade não economiza ainda mais o uso de armazenamento e reduz significativamente o desempenho DA faixa de bytes.
- * Conexão de endpoint HTTP versus HTTPS S3*. Durante o teste de benchmark, observamos uma melhoria de desempenho de cerca de 5% ao usar uma conexão HTTP S3 do cluster Vertica para o ponto de extremidade do balanceador de carga StorageGRID. Esta escolha deve basear-se nos requisitos de segurança do cliente.

As recomendações para uma configuração Vertica incluem:

- **As configurações padrão do depósito do banco de dados Vertica estão ativadas (valor de 1) para operações de leitura e gravação**. A NetApp recomenda fortemente que essas configurações do depósito estejam ativadas para aprimorar o desempenho.
- **Desativar limitações de streaming**. Para obter detalhes de configuração, consulte a secção Desativação das limitações de streaming.

Instalação do modo Eon no local com armazenamento comunitário no StorageGRID

As seções a seguir descrevem o procedimento para instalar o modo Eon no local com armazenamento comunitário no StorageGRID. O procedimento para configurar o armazenamento de objetos compatível com o Simple Storage Service (S3) no local é semelhante ao procedimento no guia Vertica, "Instale um banco de dados do modo Eon no local".

A seguinte configuração foi usada para o teste funcional:

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Três máquinas virtuais (VMs) com CentOS 7.x os para nós Vertica formarem um cluster. Esta configuração é apenas para o teste funcional, não para o cluster de banco de dados de produção Vertica.

Esses três nós são configurados com uma chave Secure Shell (SSH) para permitir SSH sem uma senha entre os nós dentro do cluster.

Informações necessárias da NetApp StorageGRID

Para instalar o modo Eon no local com armazenamento comunitário no StorageGRID, você deve ter as seguintes informações pré-requisitos.

- Endereço IP ou nome de domínio totalmente qualificado (FQDN) e número da porta do endpoint StorageGRID S3. Se você estiver usando HTTPS, use uma autoridade de certificação personalizada (CA) ou um certificado SSL autoassinado implementado no endpoint do StorageGRID S3.
- Nome do intervalo. Ele deve pré-existir e estar vazio.
- Acesse o ID da chave e a chave de acesso secreta com acesso de leitura e gravação ao bucket.

Criando um arquivo de autorização para acessar o endpoint S3

Os pré-requisitos a seguir se aplicam ao criar um arquivo de autorização para acessar o endpoint S3:

- Vertica está instalado.
- Um cluster está configurado, configurado e pronto para criação de banco de dados.

Para criar um arquivo de autorização para acessar o endpoint S3, siga estas etapas:

1. Faça login no nó Vertica onde você será executado `admintools` para criar o banco de dados do modo Eon.

   O usuário padrão é `dbadmin`, criado durante a instalação do cluster Vertica.

2. Use um editor de texto para criar um arquivo sob o `/home/dbadmin` diretório. O nome do arquivo pode ser o que você quiser, por exemplo `sg_auth.conf`, .
3. Se o endpoint S3 estiver usando uma porta HTTP 80 padrão ou uma porta HTTPS 443, ignore o número da porta. Para usar HTTPS, defina os seguintes valores:

   ◦ `awsenablehttps = 1`, caso contrário, defina o valor como `0`.

   ◦ `awsauth = <s3 access key ID>:<secret access key>`

   ◦ `awsendpoint = <StorageGRID s3 endpoint>:<port>`

   Para usar uma CA personalizada ou um certificado SSL autoassinado para a conexão HTTPS de endpoint do StorageGRID S3, especifique o caminho completo do arquivo e o nome do arquivo do certificado. Esse arquivo deve estar no mesmo local em cada nó Vertica e ter permissão de leitura para todos os usuários. Ignore esta etapa se o certificado SSL do StorageGRID S3 for assinado pela CA publicamente conhecida.

   - `awscafile = <filepath/filename>`

   Por exemplo, veja o seguinte arquivo de exemplo:

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

> Em um ambiente de produção, o cliente deve implementar um certificado de servidor assinado por uma CA publicamente conhecida em um endpoint do balanceador de carga do StorageGRID S3.

Escolhendo um caminho de depósito em todos os nós Vertica

Escolha ou crie um diretório em cada nó para o caminho do storage de depósito. O diretório que você fornece para o parâmetro caminho do storage de depósito deve ter o seguinte:

- O mesmo caminho em todos os nós do cluster (por exemplo, `/home/dbadmin/depot`)
- Seja legível e gravável pelo usuário dbadmin

- Armazenamento suficiente

  Por padrão, o Vertica usa 60% do espaço do sistema de arquivos que contém o diretório para armazenamento de depósito. Você pode limitar o tamanho do depósito usando o `--depot-size` argumento no `create_db` comando. "Dimensionamento do seu cluster Vertica para um banco de dados do modo Eon"consulte o artigo para obter diretrizes gerais de dimensionamento Vertica ou consulte o seu gerente de conta Vertica.

  A `admintools create_db` ferramenta tenta criar o caminho do depósito para você se não existir um.

Criando o banco de dados Eon on-premises

Para criar o banco de dados Eon on-premises, siga estas etapas:

1. Para criar o banco de dados, use a `admintools create_db` ferramenta.

   A lista a seguir fornece uma breve explicação dos argumentos usados neste exemplo. Consulte o documento Vertica para obter uma explicação detalhada de todos os argumentos necessários e opcionais.

   - -x caminho/nome do ficheiro de autorização criado em "Criando um arquivo de autorização para acessar o endpoint S3" >.

     Os detalhes da autorização são armazenados no banco de dados após a criação bem-sucedida. Você pode remover esse arquivo para evitar expor a chave secreta S3.

   - --communal-storage-localização inferior a s3://StorageGRID bucketname>
   - Lista separada por vírgulas de nós Vertica a serem usados para este banco de dados>
   - -d nome do banco de dados a ser criado>
   - a palavra-passe a ser definida para esta nova base de dados>. Por exemplo, veja o seguinte comando de exemplo:

     ```
     admintools -t create_db -x sg_auth.conf --communal-storage
     -location=s3://vertica --depot-path=/home/dbadmin/depot --shard
     -count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
     '<password>'
     ```

     A criação de um novo banco de dados leva vários minutos de duração, dependendo do número de nós para o banco de dados. Ao criar banco de dados pela primeira vez, você será solicitado a aceitar o Contrato de Licença.

Por exemplo, veja o seguinte arquivo de autorização de exemplo e `create db` comando:

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
```

```
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
```

```
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
61	s3://vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07_0_0.dfs
145	s3://vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d_0_0.dfs
146	s3://vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d_0_0.dfs
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs
34	s3://vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25_0_0.dfs
41	s3://vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d_0_0.dfs
61	s3://vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d_0_0.dfs
131	s3://vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19_0_0.dfs
91	s3://vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11_0_0.dfs
118	s3://vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15_0_0.dfs
115	s3://vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61_0_0.dfs
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs
38	s3://vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49_0_0.dfs
38	s3://vertica/eba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0_0.dfs
21521920	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2.tar
6865408	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar
53947904	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba.tar
44932608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de.tar
256306688	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e.tar
8062464	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34.tar
20024832	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70.tar
10444	s3://vertica/metadata/VMart/cluster_config.json
823266	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/chkpt_1.cat.gz
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/completed
822521	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/completed
746513	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
2596	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
8518	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Tamanho do objeto (byte)	Caminho completo da chave do balde/objeto
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Desativação das limitações de streaming

Este procedimento é baseado no guia Vertica para outro armazenamento de objetos no local e deve ser

aplicável ao StorageGRID.

1. Depois de criar o banco de dados, desative o `AWSStreamingConnectionPercentage` parâmetro de configuração definindo-o como `0`. Esta configuração é desnecessária para uma instalação no local do modo Eon com armazenamento comunitário. Este parâmetro de configuração controla o número de conexões ao armazenamento de objetos que o Vertica usa para leituras de streaming. Em um ambiente de nuvem, essa configuração ajuda a evitar que os dados de streaming do armazenamento de objetos usem todas as alças de arquivo disponíveis. Ele deixa algumas alças de arquivo disponíveis para outras operações de armazenamento de objetos. Devido à baixa latência de armazenamentos de objetos no local, essa opção é desnecessária.
2. Use uma `vsql` instrução para atualizar o valor do parâmetro. A senha é a senha do banco de dados que você definiu em "criando o banco de dados on-premises Eon". Por exemplo, veja a seguinte saída de amostra:

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

Verificando as configurações do depósito

As configurações padrão de depósito do banco de dados Vertica são ativadas (valor de 1) para operações de leitura e gravação. A NetApp recomenda fortemente que essas configurações do depósito estejam ativadas para aprimorar o desempenho.

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

Carregamento de dados de amostra (opcional)

Se este banco de dados for para teste e será removido, você pode carregar dados de amostra para este banco de dados para teste. O Vertica vem com um conjunto de dados de amostra, VMart, encontrado em `/opt/vertica/examples/VMart_Schema/` cada nó Vertica. Você pode encontrar mais informações sobre este conjunto de "aqui"dados de amostra .

Siga estes passos para carregar os dados de amostra:

1. Faça login como dbadmin em um dos nós Vertica: cd /opt/vertica/examples/VMart_Schema/
2. Carregue dados de amostra para o banco de dados e insira a senha do banco de dados quando solicitado nas subetapas c e d:
   a. `cd /opt/vertica/examples/VMart_Schema`

b. `./vmart_gen`

c. `vsql < vmart_define_schema.sql`

d. `vsql < vmart_load_data.sql`

3. Existem várias consultas SQL predefinidas, você pode executar algumas delas para confirmar que os dados de teste são carregados com sucesso no banco de dados. Por exemplo: `vsql < vmart_queries1.sql`

Onde encontrar informações adicionais

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

- "Documentação do produto NetApp StorageGRID 11,7"
- "Folha de dados do StorageGRID"
- "Documentação do produto Vertica 10,1"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Setembro de 2021	Lançamento inicial.

Por Angela Cheng

Análises de log do StorageGRID usando o ELK stack

Por Angela Cheng

Com o recurso de encaminhamento de syslog do StorageGRID, você pode configurar um servidor syslog externo para coletar e analisar mensagens de log do StorageGRID. ELK (Elasticsearch, Logstash, Kibana) tornou-se uma das soluções de análise de logs mais populares. Assista ao "Análise de log do StorageGRID usando o vídeo ELK" para exibir uma configuração DO ELK de exemplo e como ele pode ser usado para identificar e solucionar problemas de solicitações S3 com falha. O StorageGRID 11,9 suporta a exportação de log de acesso de endpoint do balanceador de carga para o servidor syslog externo. Assista a isso "Vídeo do YouTube" para saber mais sobre esse novo recurso. este artigo fornece arquivos de exemplo de configuração do Logstash, consultas do Kibana, gráficos e painel para dar a você um início rápido para o gerenciamento e análise de logs do StorageGRID.

Requisitos

- StorageGRID 11.6.0.2 ou superior
- ELK (Elasticsearch, Logstash e Kibana) 7,1x ou superior instalado e em operação

Arquivos de exemplo

- "Faça o download do pacote de arquivos de amostra Logstash 7.x" **md5 checksum** 148c23d0021d9a4bb4a6c0287464deab e **sha256 checksum** f51ec9e2e3f842d5a7861566b167a561b4373038b4e7bb3c8b8be3d522adf2d6

- "Faça o download do pacote de arquivos de amostra Logstash 8.x" **md5 checksum** e11bae3a662f87c310ef363d0fe06835 e **sha256 checksum** 5c670755742cfdfd5aa723a596ba087e0153a65bcaef3934afdb682f6cd278d
- "Faça o download do pacote de arquivos de amostra Logstash 8.x para o StorageGRID 11,9" **md5 checksum** 41272857c4a54600f95995f6ed74800d e **sha256 checksum** 67048e8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

Suposição

Os leitores estão familiarizados com a terminologia e operações do StorageGRID e ELK.

Instrução

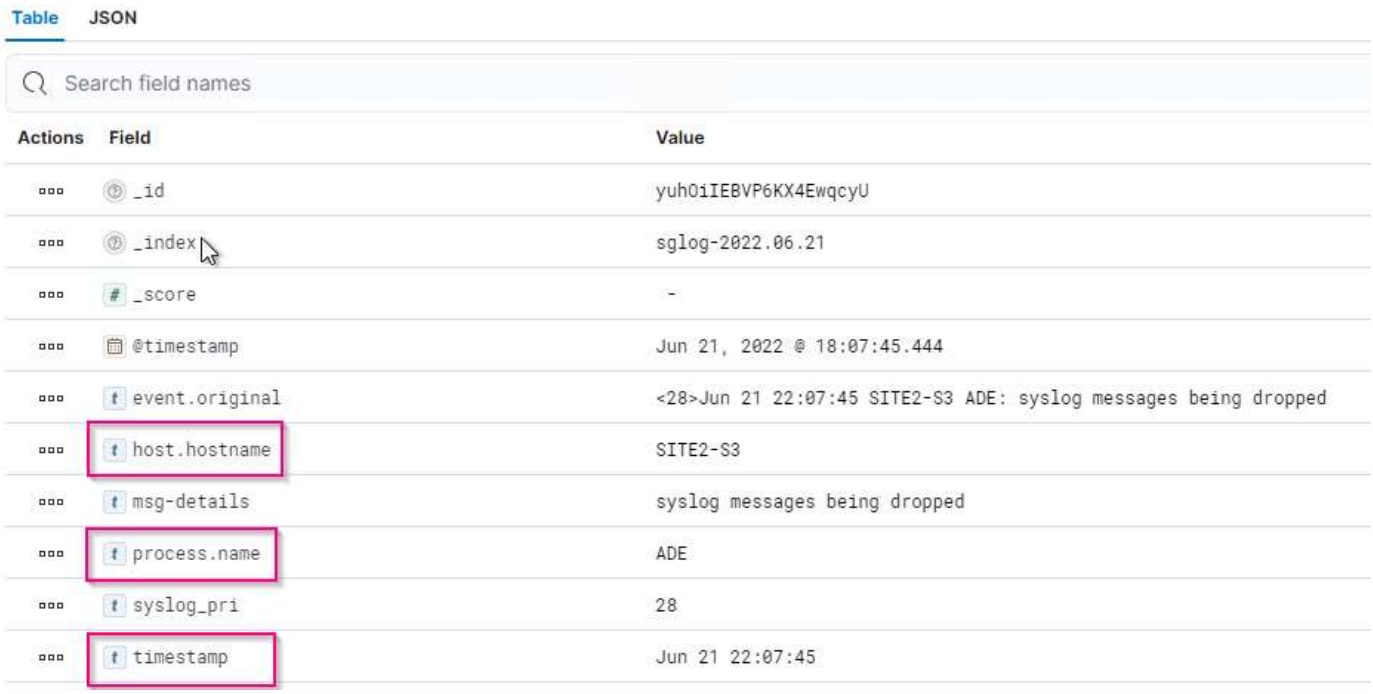
Duas versões de amostra são fornecidas devido a diferenças nos nomes definidos pelos padrões de grok. Por exemplo, o padrão de grok SYSLOGBASE no arquivo de configuração Logstash define nomes de campo de forma diferente, dependendo da versão instalada do Logstash.

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

- Logstash 7,17 amostra*

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

- Logstash 8,23 amostra*



Passos

1. Descompacte a amostra fornecida com base na versão ELK instalada. * Sglog-2-file.conf:* este arquivo de configuração envia mensagens de log do StorageGRID para um arquivo no Logstash sem transformação de dados. Você pode usar isso para confirmar que o Logstash está recebendo mensagens do StorageGRID ou para ajudar a entender os padrões de log do StorageGRID. **Sglog-2-es.conf:** este arquivo de configuração transforma mensagens de log do StorageGRID usando vários padrões e filtros. Ele inclui exemplos de instruções drop, que deixam cair mensagens com base em padrões ou filtros. A saída é enviada ao Elasticsearch para indexação. Personalize o arquivo de configuração selecionado de acordo com a instrução dentro do arquivo.
2. Teste o arquivo de configuração personalizado:

   ```
   /usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-path/file>
   ```

   Se a última linha retornada for semelhante à linha abaixo, o arquivo de configuração não tem erros de sintaxe:

   ```
   [LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
   ```

3. Copie o arquivo conf personalizado para a configuração do servidor Logstash: /Etc/logstash/conf.d se você não tiver habilitado o config.reload.automatic em /etc/logstash/logstash.yml, reinicie o serviço Logstash. Caso contrário, aguarde até que o intervalo de recarga da configuração passe.

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

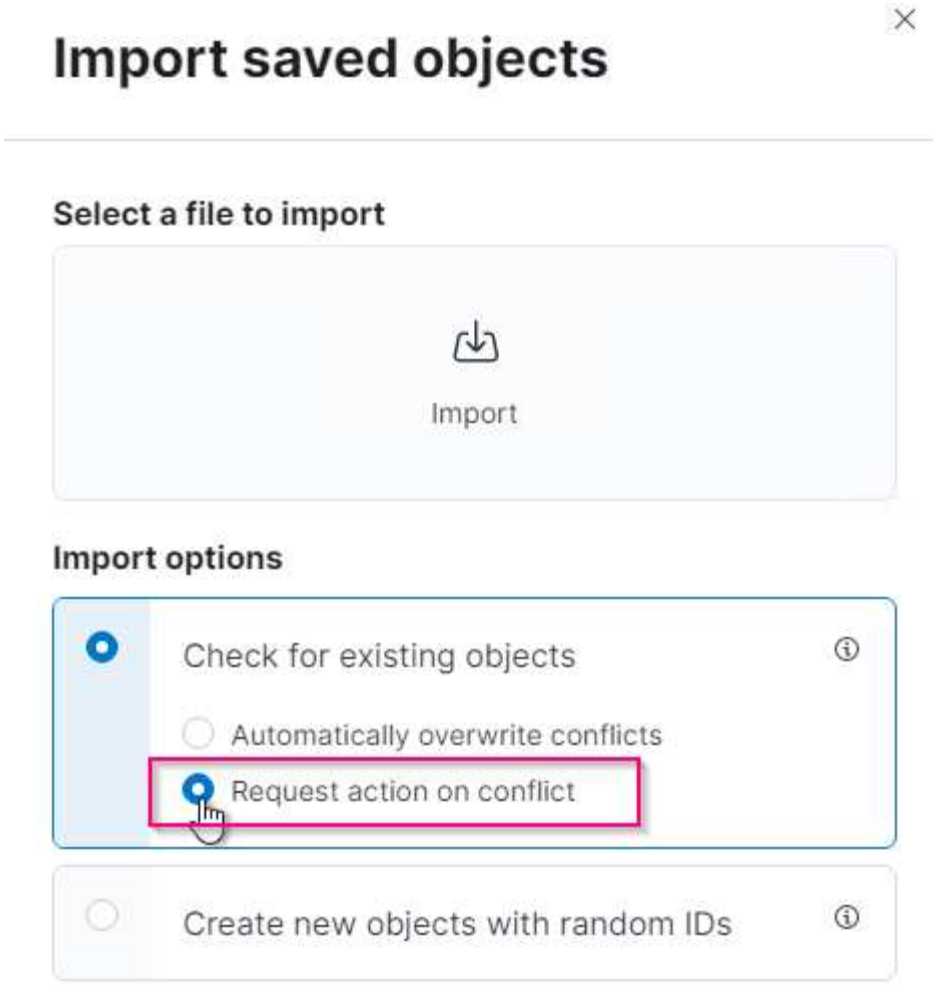
4. Verifique /var/log/logstash/logstash-plain.log e confirme que não há erros iniciando o Logstash com o novo arquivo de configuração.
5. Confirme se a porta TCP foi iniciada e escutada. Neste exemplo, a porta TCP 5000 é usada.

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

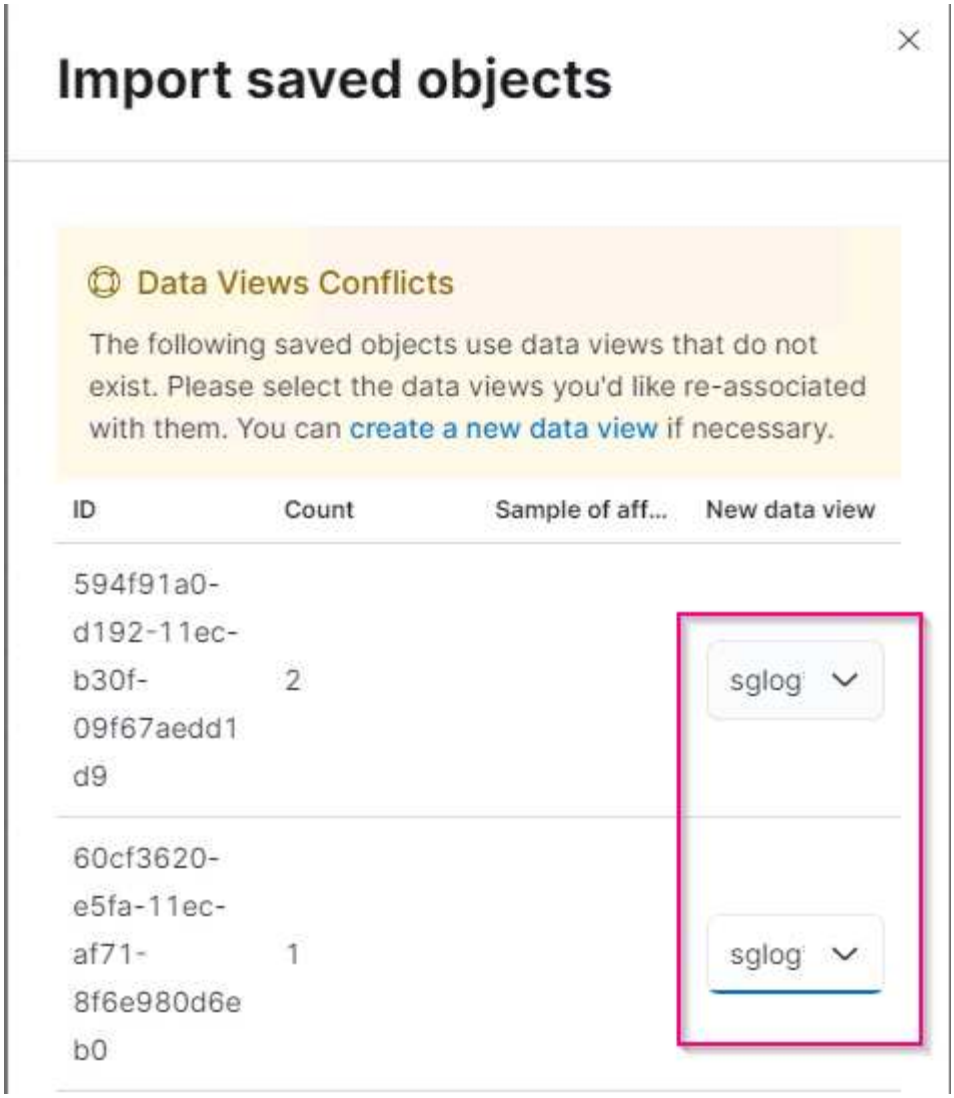
6. A partir da GUI do gerenciador do StorageGRID, configure o servidor syslog externo para enviar mensagens de log para o Logstash. Consulte "vídeo de demonstração" para obter mais informações.
7. Você precisa configurar ou desativar o firewall no servidor Logstash para permitir a conexão de nós StorageGRID à porta TCP definida.
8. Na GUI do Kibana, selecione Gerenciamento → Ferramentas de desenvolvimento. Na página Console, execute este comando GET para confirmar que novos índices são criados no Elasticsearch.

```
GET /_cat/indices/*?v=true&s=index
```

9. A partir do Kibana GUI, crie um padrão de índice (ELK 7.x) ou visualização de dados (ELK 8.x).
10. Na GUI do Kibana, digite 'objetos salvos' na caixa de pesquisa que está localizada no centro superior. Na página objetos salvos, selecione Importar. Em Opções de importação, selecione "solicitar ação em conflito"



Importe elk<version>-query-chart-sample.ndjson. Quando solicitado a resolver o conflito, selecione o padrão de índice ou a exibição de dados que você criou na etapa 8.



Os seguintes objetos Kibana são importados: * Consulta * * * auditoria-msg-s3rq S3-orlm * Registro de bycast S3 S3 mensagens relacionadas com * aviso de nível de log ou acima * evento de segurança com falha * nginx-gw Registro de acesso de endpoint (disponível apenas em elk8-sample-for-sg119.zip) * Gráfico * S3 pedidos contam com base em bycast.log * Código de status HTTP *

Agora você está pronto para executar a análise de log do StorageGRID usando o Kibana.

Recursos adicionais

- "syslog101"
- "O que é a pilha ELK"
- "Lista de padrões Grok"
- "Um guia para iniciantes para Logstash: Grok"
- "Um guia prático para o Logstash: Syslog Deep Dive"
- "Guia Kibana – explore o documento"
- "Referência de mensagens de log de auditoria do StorageGRID"

Use Prometheus e Grafana para estender a retenção de métricas

Por Aron Klein

Este relatório técnico fornece instruções detalhadas para configurar o NetApp StorageGRID 11,6 com serviços externos do Prometheus e Grafana.

Introdução

O StorageGRID armazena métricas usando Prometheus e fornece visualizações dessas métricas por meio de dashboards Grafana integrados. As métricas Prometheus podem ser acessadas com segurança a partir do StorageGRID configurando certificados de acesso de cliente e habilitando o acesso prometheus para o cliente especificado. Hoje, a retenção desses dados métricos é limitada pela capacidade de storage do nó de administração. Para obter uma duração mais longa e uma capacidade de criar visualizações personalizadas dessas métricas, implantaremos um novo servidor Prometheus e Grafana, configuraremos nosso novo servidor para raspar as métricas da instância StorageGRIDs e construir um painel com as métricas que são importantes para nós. Você pode obter mais informações sobre as métricas do Prometheus coletadas no "Documentação do StorageGRID".

Federado Prometheus

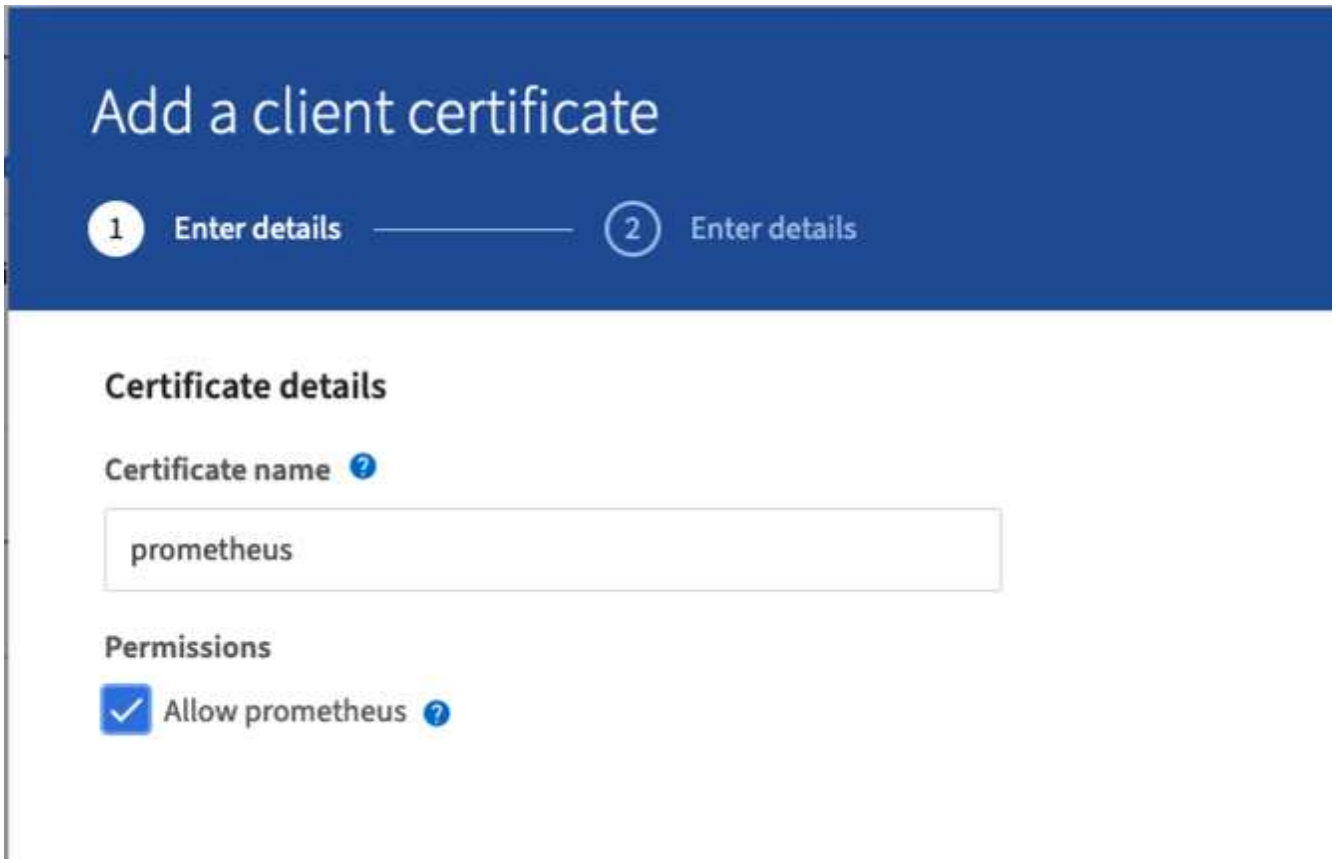
Detalhes do laboratório

Para os propósitos deste exemplo, eu vou usar todas as máquinas virtuais para nós StorageGRID 11,6 e um servidor Debian 11. A interface de gerenciamento do StorageGRID é configurada com um certificado de CA publicamente confiável. Este exemplo não passará pela instalação e configuração do sistema StorageGRID ou instalação do Debian linux. Você pode usar qualquer versão do Linux que desejar que seja suportada por Prometheus e Grafana. Tanto o Prometheus quanto o Grafana podem instalar como contentores docker, compilar a partir de fontes ou binários pré-compilados. Neste exemplo eu estarei instalando ambos binários Prometheus e Grafana diretamente no mesmo servidor Debian. Faça o download e siga as instruções básicas de instalação https://prometheus.io de e https://grafana.com/grafana/, respetivamente.

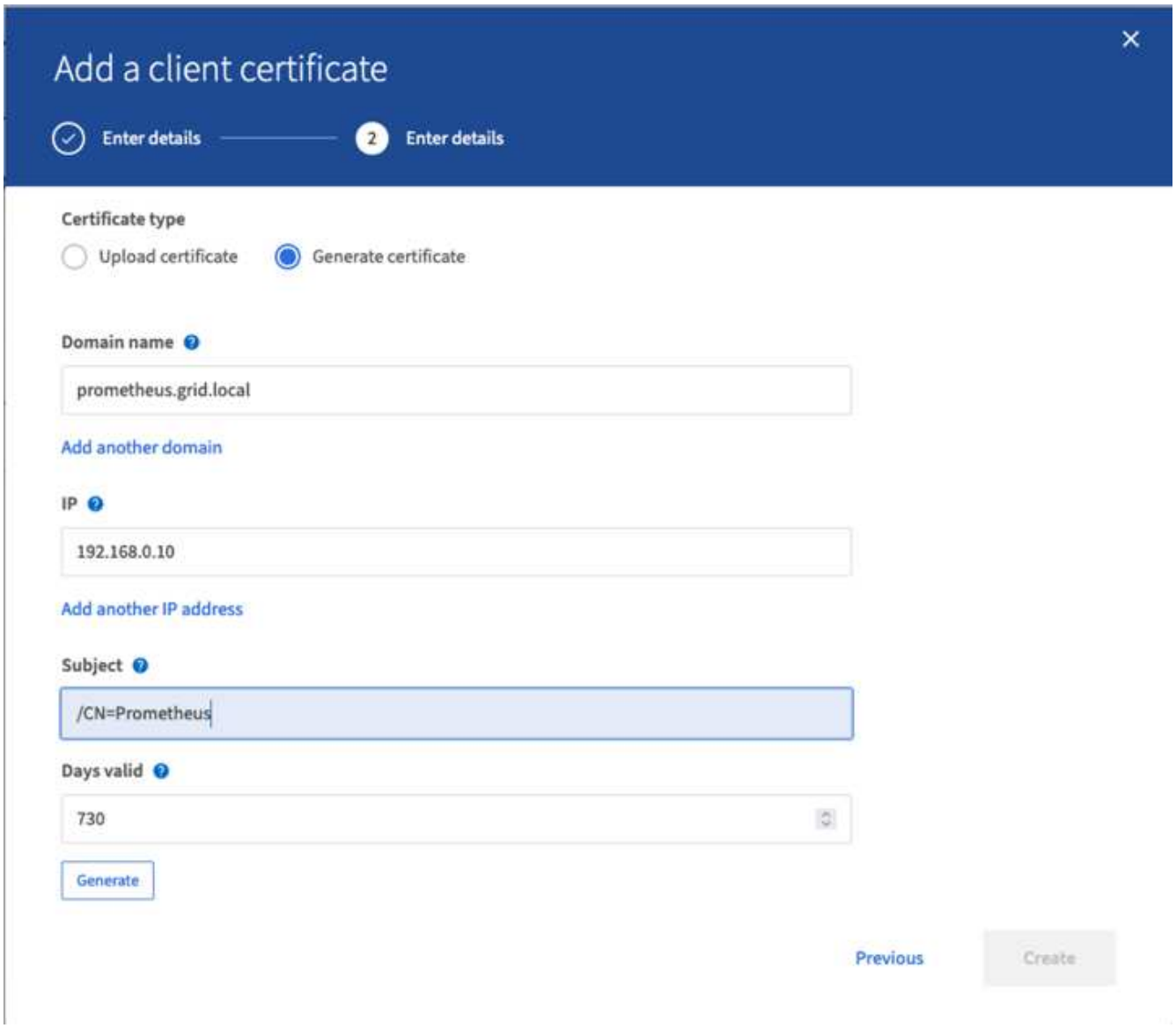
Configurar o StorageGRID para acesso ao cliente Prometheus

Para obter acesso às métricas do prometheus armazenadas pelo StorageGRIDs, você deve gerar ou carregar um certificado de cliente com chave privada e habilitar a permissão para o cliente. A interface de gerenciamento do StorageGRID deve ter um certificado SSL. Esse certificado deve ser confiável pelo servidor prometheus por uma CA confiável ou manualmente confiável se ele for autoassinado. Para ler mais, visite o "Documentação do StorageGRID".

1. Na interface de gerenciamento do StorageGRID, selecione "CONFIGURAÇÃO" no lado inferior esquerdo e, na segunda coluna em "Segurança", clique em certificados.
2. Na página certificados, selecione a guia "Cliente" e clique no botão "Adicionar".
3. Forneça um nome para o cliente que será concedido acesso e use este certificado. Clique na caixa em "permissões", na frente de "permitir Prometheus" e clique no botão continuar.

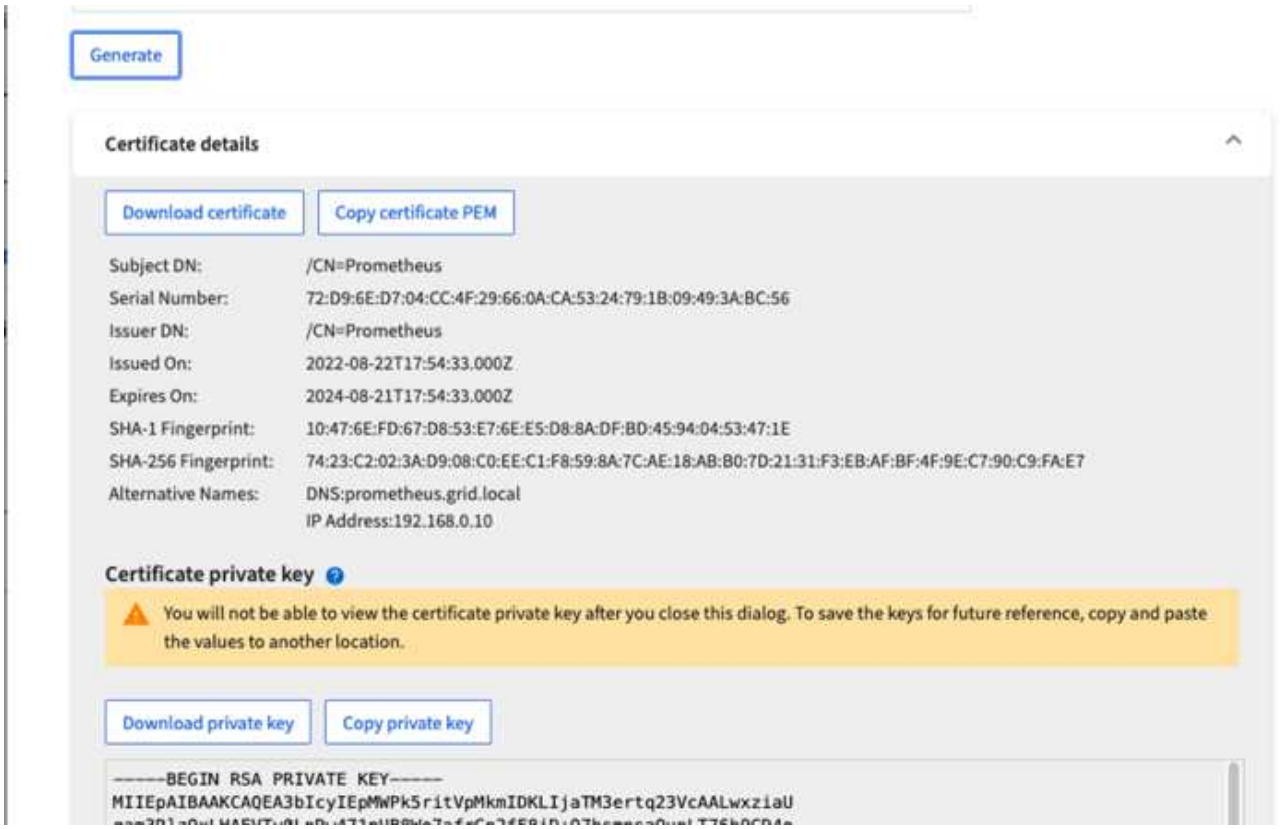


4. Se você tiver um certificado assinado pela CA, você pode selecionar o botão de opção "carregar certificado", mas, no nosso caso, vamos permitir que o StorageGRID gere o certificado do cliente selecionando o botão de opção "gerar certificado". Os campos obrigatórios serão exibidos para serem preenchidos. Insira o FQDN para o servidor cliente, o IP do servidor, o assunto e dias válidos. Em seguida, clique no botão "gerar".



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. Baixe o arquivo pem de certificado e o arquivo pem de chave privada.



> This is the only time you can download the private key, so make sure you do not skip this step.

Prepare o servidor Linux para a instalação do Prometheus

Antes de instalar o Prometheus, eu quero preparar meu ambiente com um usuário Prometheus, a estrutura de diretórios e configurar a capacidade para o local de armazenamento de métricas.

1. Crie o usuário Prometheus.

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Crie os diretórios para Prometheus, certificado de cliente e dados de métricas.

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. Formatei o disco que estou usando para retenção de métricas com um sistema de arquivos ext4.

```
mkfs -t ext4 /dev/sdb
```

4. Eu então montei o sistema de arquivos para o diretório de métricas do Prometheus.

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. Obtenha o uuid do disco que você está usando para seus dados de métricas.

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. Adicionando uma entrada em /etc/fstab/ fazendo com que a montagem persista em reinicializações usando o uuid de /dev/sdb.

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Instale e configure Prometheus

Agora que o servidor está pronto, posso iniciar a instalação do Prometheus e configurar o serviço.

1. Extraia o pacote de instalação do Prometheus

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. Copie os binários para /usr/local/bin e altere a propriedade para o usuário prometheus criado anteriormente

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. Copie os consoles e bibliotecas para /etc/prometheus

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. Copie o certificado do cliente e os arquivos pem de chave privada baixados anteriormente do StorageGRID para /etc/prometheus/certs
5. Crie o arquivo yaml de configuração prometheus

```
sudo nano /etc/prometheus/prometheus.yml
```

6. Insira a seguinte configuração. O nome do trabalho pode ser qualquer coisa que você desejar. Altere o "-targets: ["]" para o FQDN do nó admin e, se você alterou os nomes dos nomes dos arquivos de certificado e chave privada, atualize a seção tls_config para corresponder. Em seguida, salve o arquivo. Se sua interface de gerenciamento de grade estiver usando um certificado autoassinado, baixe o certificado e coloque-o com o certificado de cliente com um nome exclusivo, e na seção tls_config adicione CA_file: /Etc/prometheus/cert/UIcert.pem

   a. Neste exemplo, estou coletando todas as métricas que começam com alertmanager, cassandra, node e StorageGRID. Você pode ver mais informações sobre as métricas do Prometheus no "Documentação do StorageGRID".

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

> Se a interface de gerenciamento de grade estiver usando um certificado autoassinado, baixe o certificado e coloque-o com o certificado do cliente com um nome exclusivo. Na seção tls_config adicione o certificado acima do certificado do cliente e das linhas de chave privada
>
> ```
> ca_file: /etc/prometheus/cert/UIcert.pem
> ```

1. Altere a propriedade de todos os arquivos e diretórios em /etc/prometheus e /var/lib/prometheus para o usuário prometheus

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. Crie um arquivo de serviço prometheus em /etc/systemd/system

```
sudo nano /etc/systemd/system/prometheus.service
```

3. Insira as linhas a seguir, observe o número—storage.tsdb.retension.time.1y que define a retenção dos dados métricos para 1 ano. Como alternativa, você pode usar 300GiB para basear a retenção nos limites de armazenamento. Este é o único local para definir a retenção de métricas.

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. Recarregue o serviço systemd para Registrar o novo serviço prometheus. Em seguida, inicie e ative o serviço prometheus.

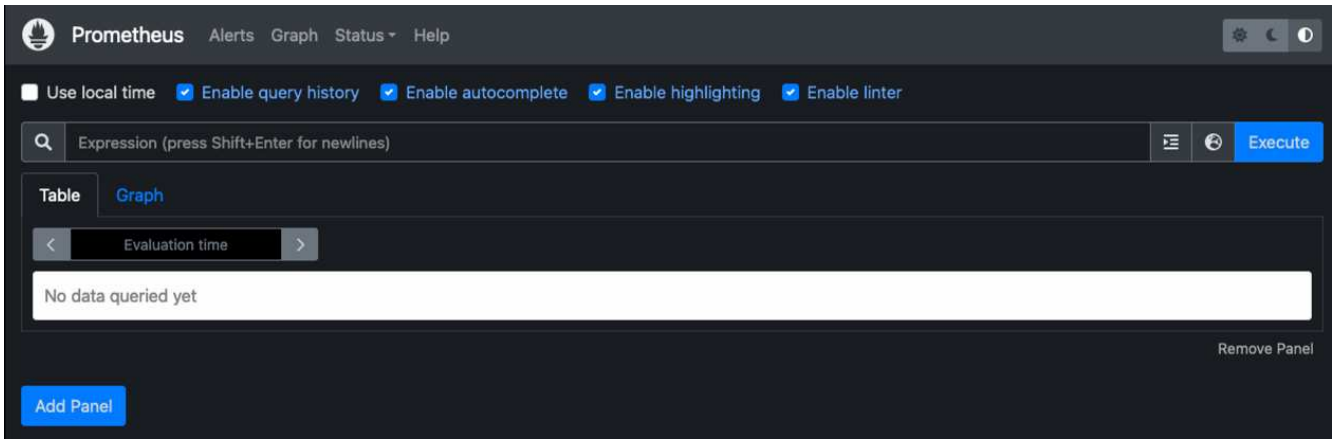
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Verifique se o serviço está funcionando corretamente

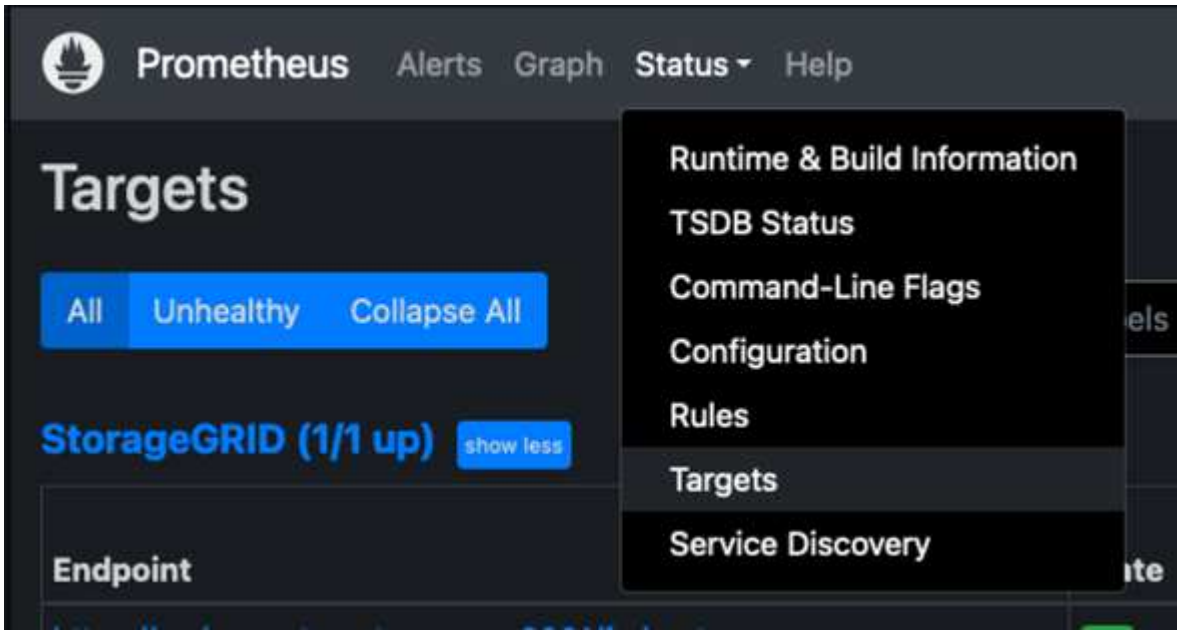
```
sudo systemctl status prometheus
```

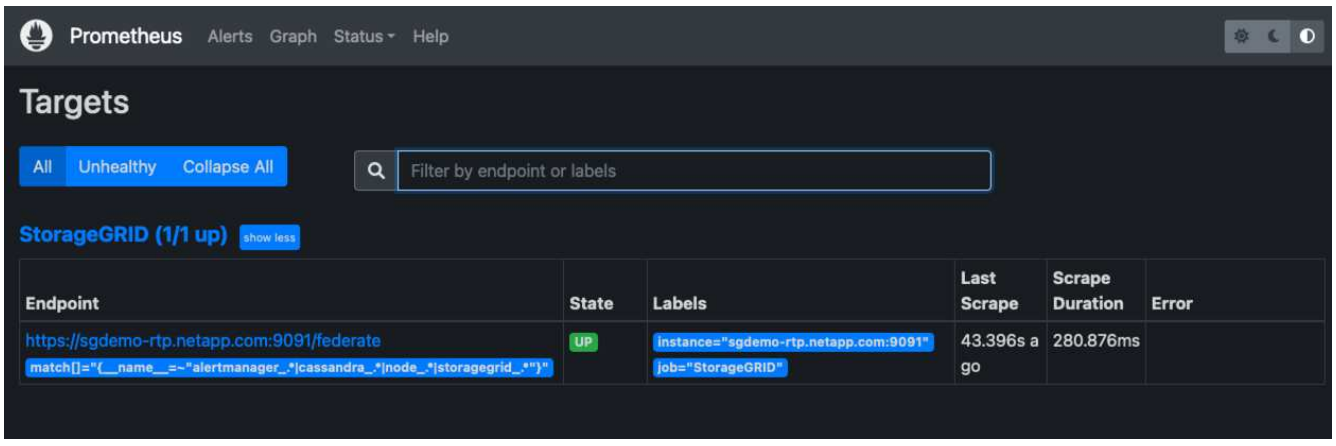
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. Agora você deve ser capaz de navegar até a IU do seu servidor prometheus http://Prometheus-server:9090 e ver a IU

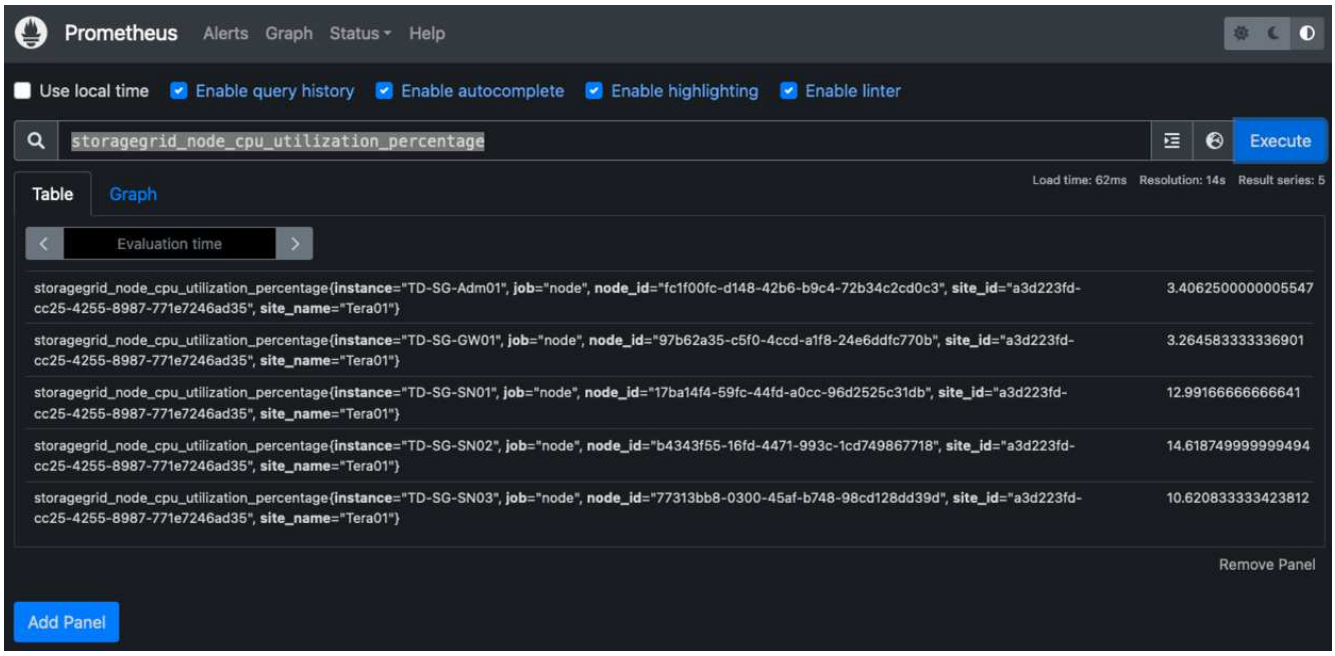


7. Em destinos "Status", você pode ver o status do endpoint do StorageGRID que configuramos em prometheus.yml





8. Na página Gráfico, você pode executar uma consulta de teste e verificar se os dados estão sendo raspados com sucesso. Por exemplo, digite "StorageGRID_node_cpu_utilization_percentage" na barra de consulta e clique no botão Executar.



Instale e configure o Grafana

Agora que o prometheus está instalado e funcionando, podemos passar para a instalação do Grafana e configurar um dashboard

Instalação do Grafana

1. Instale a mais recente edição corporativa do Grafana

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. Adicione este repositório para versões estáveis:

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. Depois de adicionar o repositório.

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. Recarregue o serviço systemd para Registrar o novo serviço grafana. Em seguida, inicie e ative o serviço Grafana.

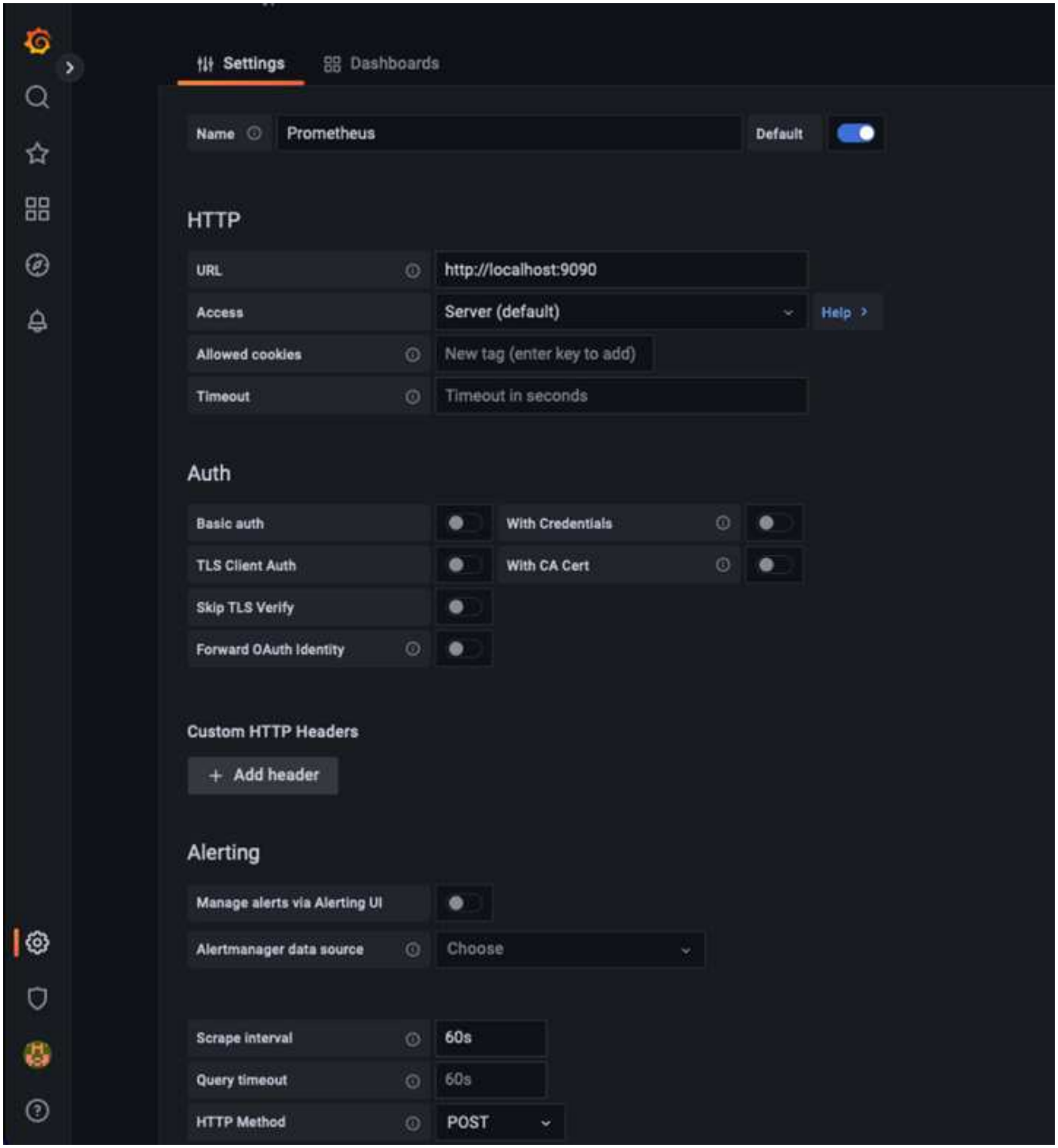
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. O Grafana agora está instalado e em execução. Quando você abre um navegador para HTTP://Prometheus-server:3000 você será recebido com a página de login do Grafana.
6. As credenciais de login padrão são admin/admin, e você deve definir uma nova senha como ela solicita.

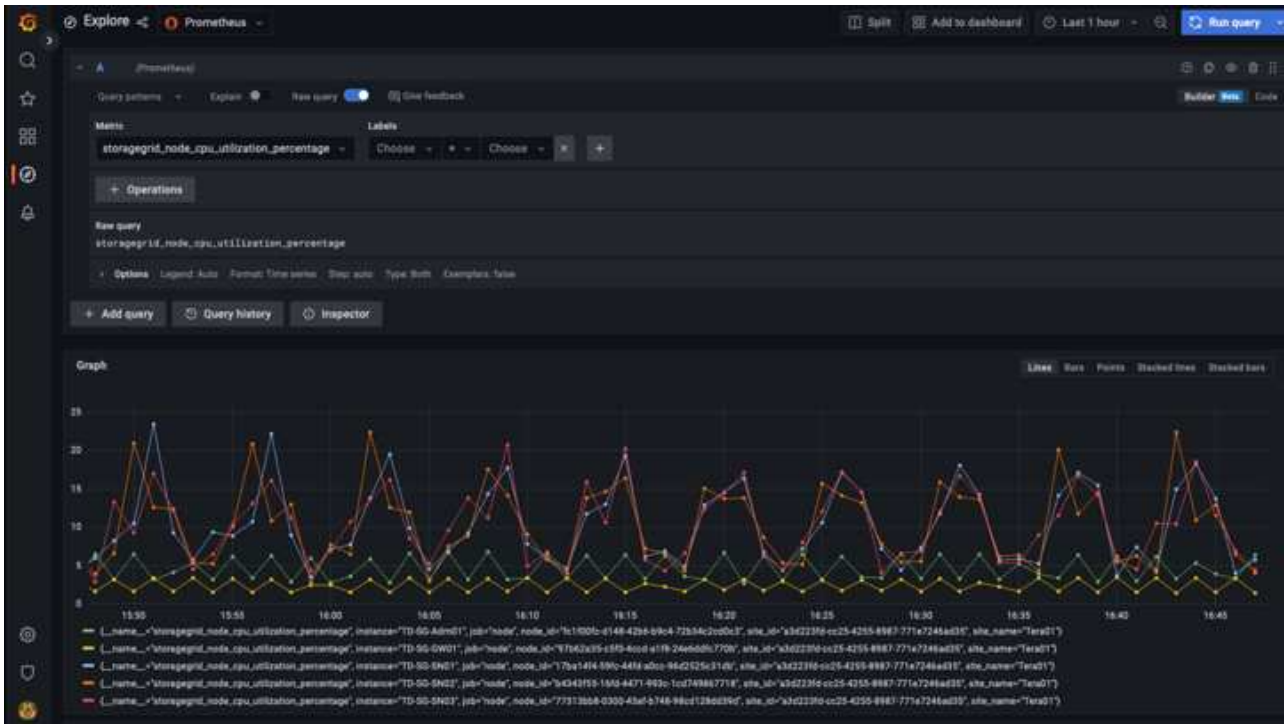
Crie um painel Grafana para StorageGRID

Com Grafana e Prometheus instalados e em execução, agora é hora de conetar os dois criando uma fonte de dados e construindo um painel

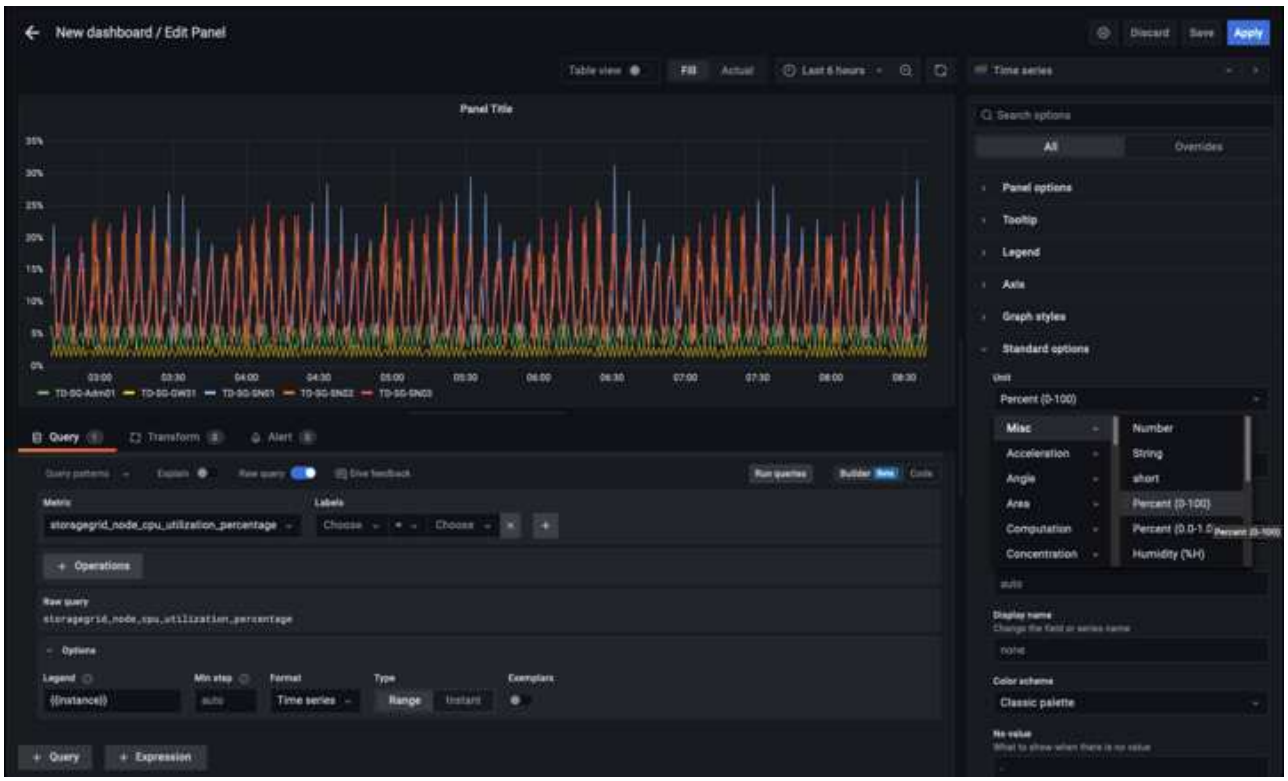
1. No painel esquerdo, expanda "Configuration" (Configuração) e selecione "Data Sources" (fontes de dados) e, em seguida, clique no botão "Add Data source" (Adicionar fonte de dados)
2. Prometheus será uma das principais fontes de dados para escolher. Se não estiver, use a barra de pesquisa para localizar "Prometheus"
3. Configure a fonte Prometheus inserindo o URL da instância prometheus e o intervalo de raspagem para corresponder ao intervalo Prometheus. Eu também desabilitei a seção de alerta, pois não configurei o gerenciador de alertas no prometheus.



4. Com as configurações desejadas inseridas, role para baixo até a parte inferior e clique em "Salvar e testar"
5. Depois que o teste de configuração for bem-sucedido, clique no botão explorar.
    a. Na janela explorar você pode usar a mesma métrica que testamos Prometheus com "StorageGRID_node_cpu_utilization_percentage" e clicar no botão "Executar consulta"



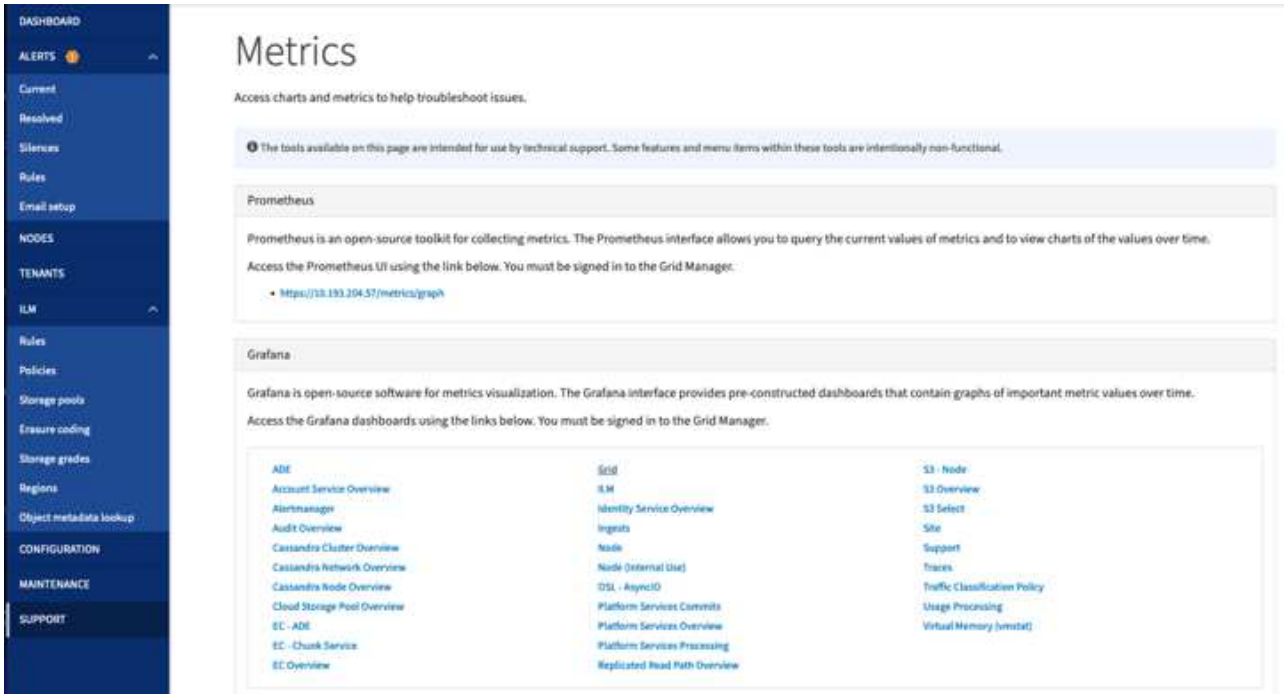
6. Agora que temos a fonte de dados configurada, podemos criar um dashboard.
   a. No painel esquerdo, expanda "Dashboards" e selecione "novo painel"
   b. Selecione "Adicionar um novo painel"
   c. Configure o novo painel selecionando uma métrica, novamente vou usar "StorageGRID_node_cpu_utilization_percentage", digite um título para o painel, expanda "Opções" na parte inferior e para a legenda mudar para personalizado e digite "_instância" para definir os nomes dos nós" e no painel direito em "Opções padrão" defina "Unidade" para "Misc/percent(0-100)". Em seguida, clique em "aplicar" para salvar o painel no painel.



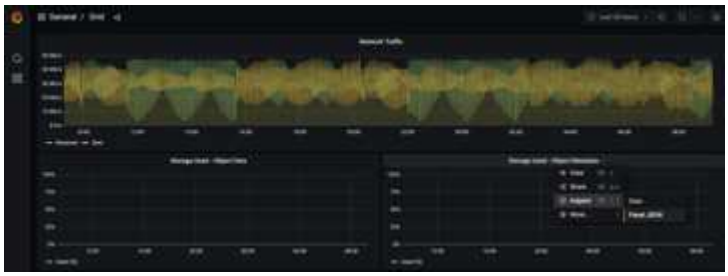
7. Poderíamos continuar a construir nosso painel como esse para cada métrica que quisermos, mas felizmente o StorageGRID já tem painéis com painéis que podemos copiar em nossos painéis personalizados.

   a. No painel esquerdo da interface de gerenciamento do StorageGRID, selecione "suporte" e, na parte inferior da coluna "Ferramentas", clique em "métricas".

   b. Dentro das métricas, vou selecionar o link "Grid" na parte superior da coluna do meio.

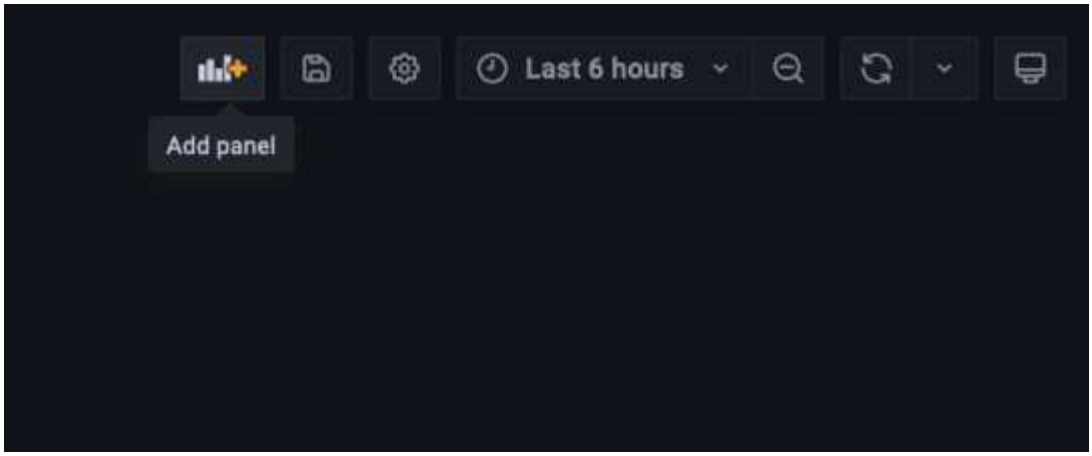


   c. No painel Grid, permite selecionar o painel "Storage Used - Object Metadata" (armazenamento usado - metadados de objetos). Clique na pequena seta para baixo e no final do título do painel para soltar um menu. Neste menu, selecione "Inspecionar" e "Painel JSON".



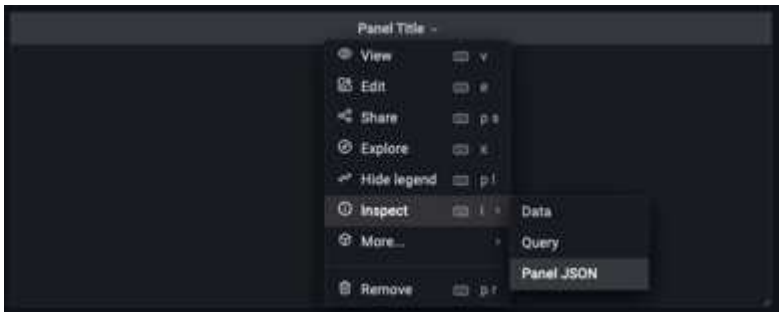
   d. Copie o código JSON e feche a janela.

e. No nosso novo painel, clique no ícone para adicionar um novo painel.

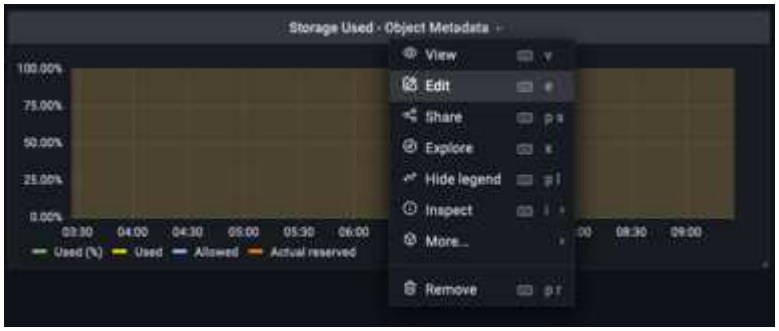


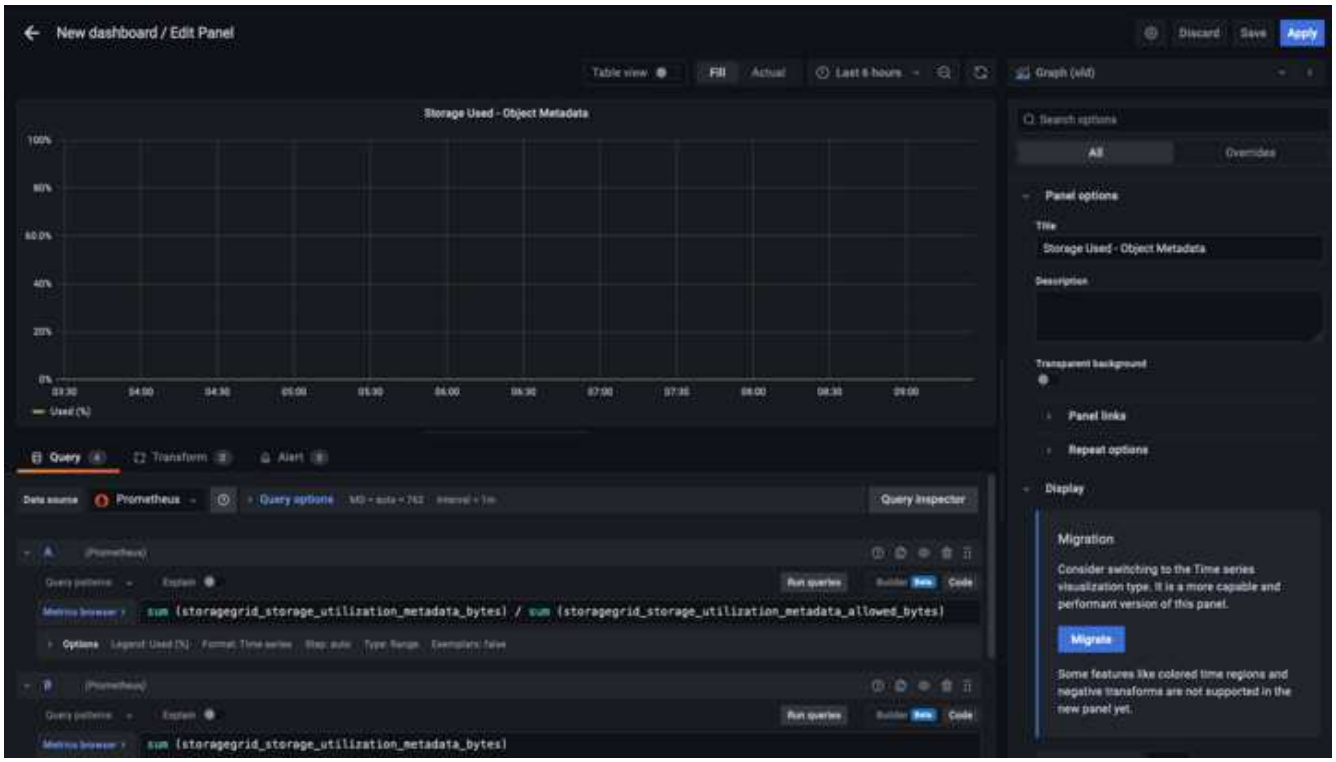
f. Aplique o novo painel sem fazer alterações

g. Assim como no painel StorageGRID, inspecione o JSON. Remova todo o código JSON e substitua-o pelo código copiado do painel StorageGRID.



h. Edite o novo painel e, no lado direito, você verá uma mensagem de migração com um botão "migrar". Clique no botão e, em seguida, clique no botão "aplicar".





8. Depois de ter todos os painéis no lugar e configurado como quiser. Salve o painel clicando no ícone do disco no canto superior direito e dê um nome ao painel.

Conclusão

Agora temos um servidor Prometheus com capacidade de armazenamento e retenção de dados personalizáveis. Com isso, podemos continuar construindo nossos próprios painéis com as métricas mais relevantes para nossas operações. Você pode obter mais informações sobre as métricas do Prometheus coletadas no "Documentação do StorageGRID".

Configuração SNMP do Datadog

Por Aron Klein

Configure o Datadog para coletar métricas e traps do StorageGRID snmp.

Configurar Datadog

O Datadog é uma solução de monitoramento que fornece métricas, visualizações e alertas. A seguinte configuração foi implementada com o agente linux versão 7.43.1 em um host Ubuntu 22.04.1 implantado local no sistema StorageGRID.

Arquivos de Perfil e Trap gerados a partir do arquivo MIB do StorageGRID

O Datadog fornece um método para converter arquivos MIB do produto em arquivos de referência de datadog necessários para mapear as mensagens SNMP.

Este arquivo StorageGRID yaml para mapeamento de resolução de armadilha Datadog gerado após a instrução encontrada "aqui". Coloque este arquivo em /etc/datadog-Agent/conf.d/snmp.d/traps_dB/

- "Baixe o arquivo trap yaml" E
  - **soma de verificação md5** 42e27e4210719945a46172b98c379517
  - **soma de verificação sha256** d0fe5c8e6ca3c902d054f854b70a85f928cba8b7c76391d356f05d2cf7b6887 e

Este arquivo yaml de perfil do StorageGRID para mapeamento de métricas do Datadog gerado após a instrução encontrada "aqui". Coloque este arquivo em /etc/datadog-Agent/conf.d/snmp.d/profiles/

- "Baixe o arquivo yaml de perfil" E
  - **md5 checksum** 72bb7784f4801adda4e0c3ea77df19aa
  - **sha256 checksum** b6b7fadd33063422a8bb8e39b3ead8ab38349ee0229926eadc85f0087b8cee

Configuração de dados SNMP para métricas

A configuração do SNMP para métricas pode ser gerenciada de duas maneiras. Você pode configurar para deteção automática fornecendo um intervalo de endereços de rede contendo o(s) sistema(s) StorageGRID ou definir os IP dos dispositivos individuais. A localização da configuração é diferente com base na decisão tomada. A descoberta automática é definida no arquivo yaml do agente de dados. Definições explícitas de dispositivo são configuradas no arquivo yaml de configuração snmp. Abaixo estão exemplos de cada um para o mesmo sistema StorageGRID.

Descoberta automática

configuração localizada em /etc/datadog-agent/datadog.yaml

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

Dispositivos individuais

/etc/datadog-agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

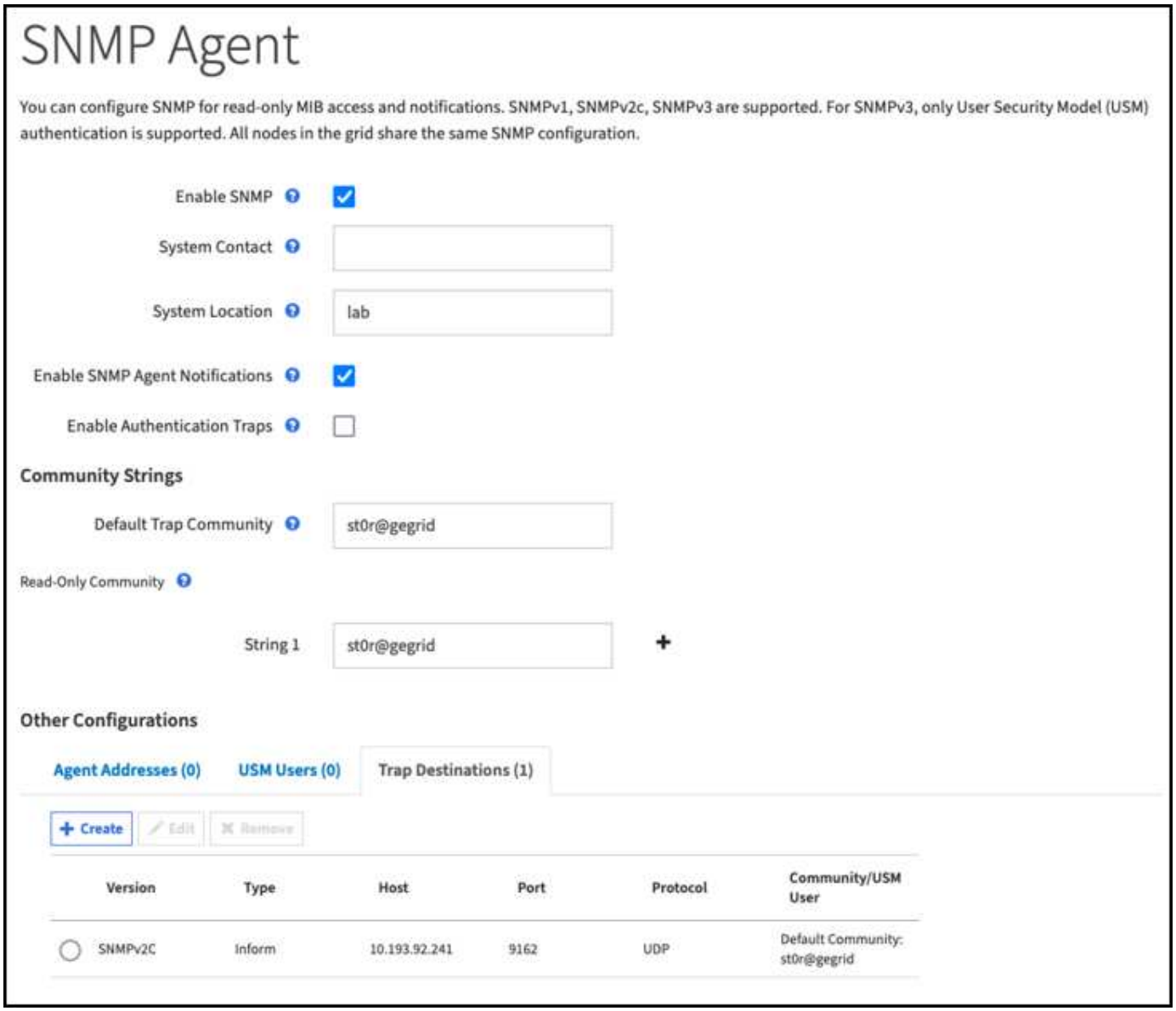
Configuração SNMP para traps

A configuração para traps SNMP é definida no arquivo yaml de configuração de dados /etc/datadog-Agent/datadog.yaml

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

Exemplo de configuração StorageGRID SNMP

O agente SNMP no seu sistema StorageGRID está localizado na guia configuração, coluna Monitoramento. Ative o SNMP e introduza as informações pretendidas. Se você deseja configurar traps, selecione "traps Destinations" e crie um destino para o host do agente Datadog que contém a configuração de traps.



Use rclone para migrar, COLOCAR e EXCLUIR objetos no StorageGRID

Por Siegfried Hepp e Aron Klein

Rclone é uma ferramenta de linha de comando gratuita e cliente para operações S3. Você pode usar o rclone para migrar, copiar e excluir dados de objetos no StorageGRID. O rclone inclui a capacidade de excluir buckets mesmo quando não estiver vazio com uma função de "purga", como visto em um exemplo abaixo.

Instalar e configurar o rclone

Para instalar o rclone em uma estação de trabalho ou servidor, baixe-o em "rclone.org".

Etapas iniciais de configuração

1. Crie o arquivo de configuração rclone executando o script de configuração ou criando manualmente o arquivo.

2. Para este exemplo, vou usar o sgdemo para o nome do endpoint StorageGRID S3 remoto na configuração rclone.
   a. Crie o arquivo de configuração -/.config/rclone/rclone.conf

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. Execute o rclone config

n rclone config

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

Exemplos básicos de comandos

- **Crie um bucket:**

  `rclone mkdir remote:bucket`

  ```
  rclone mkdir sgdemo:test01
  ```

  Use --no-check-certificate se você precisar ignorar certificados SSL.

- **Liste todos os baldes:**

```
rclone lsd remote:
```

n rclone lsd sgdemo:

- **Liste objetos em um bucket específico:**

```
rclone ls remote:bucket
```

n rclone ls sgdemo:test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- **Excluir um balde:**

```
rclone rmdir remote:bucket
```

rclone rmdir sgdemo:test02

- **Coloque um objeto:**

```
rclone copy filename remote:bucket
```

cópia rclone/test/testfile.txt sgdemo:test01

- **Obter um objeto:**

```
rclone copy remote:bucket/objectname filename
```

Cópia rclone sgdemo:TEST01/testfile.txt/test/testfileS3.txt

- **Excluir um objeto:**

```
rclone delete remote:bucket/objectname
```

n rclone delete sgdemo:test01/testfile.txt

- **Migrar objetos em um bucket**

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

n rclone sync sgdemo:test01 sgdemo:clone01 --progress

```
Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

Use --progress ou -P para exibir o progresso da tarefa. Caso contrário, não há saída.

- **Excluir um bucket e todo o conteúdo do objeto**

```
rclone purge remote:bucket --progress
```

n rclone purge sgdemo:test01 --progress

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:         10.2s
```

n rclone ls sgdemo:test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

Práticas recomendadas do StorageGRID para implantação com o Veeam Backup and Replication

Por Oliver Haensel e Aron Klein

Este guia concentra-se na configuração do NetApp StorageGRID e, em parte, no Veeam Backup and Replication. Este documento foi criado para administradores de storage e rede que estão familiarizados com os sistemas Linux e têm a tarefa de manter ou implementar um sistema NetApp StorageGRID em combinação com o Veeam Backup and Replication.

Visão geral

Os administradores de storage buscam gerenciar o crescimento de seus dados com soluções que atendam às metas de disponibilidade, recuperação rápida, escalabilidade para atender às suas necessidades e automatizar suas políticas de retenção de dados a longo prazo. Essas soluções também devem fornecer proteção contra perdas ou ataques mal-intencionados. Juntas, a Veeam e a NetApp fizeram uma parceria para criar uma solução de proteção de dados que combina o Veeam Backup & Recovery com o NetApp StorageGRID para storage de objetos no local.

A Veeam e a NetApp StorageGRID fornecem uma solução fácil de usar que trabalham juntas para ajudar a atender às demandas do rápido crescimento de dados e do aumento das regulamentações em todo o mundo. O storage de objetos baseado em nuvem é conhecido por sua resiliência, capacidade de escala, eficiências operacionais e de custo que o tornam uma escolha natural como destino para seus backups. Este documento fornecerá orientações e recomendações para a configuração de sua solução Veeam Backup e do sistema StorageGRID.

A carga de trabalho de objetos da Veeam cria um grande número de operações simultâneas DE PUT, DELETE e LIST DE objetos pequenos. A ativação da imutabilidade será adicionada ao número de solicitações ao armazenamento de objetos para definir versões de retenção e listagem. O processo de uma tarefa de backup inclui a gravação de objetos para a alteração diária, então depois que as novas gravações forem concluídas, a tarefa excluirá quaisquer objetos com base na política de retenção do backup. O agendamento de trabalhos de cópia de segurança quase sempre se sobrepõe. Essa sobreposição resultará em uma grande parte da janela de backup que consiste em 50/50 COLOCAR/EXCLUIR carga de trabalho no armazenamento de objetos. Fazer ajustes na Veeam ao número de operações simultâneas com a configuração de slot de tarefa, aumentar o tamanho do objeto aumentando o tamanho do bloco de tarefas de backup, reduzir o número de objetos nas solicitações de exclusão de vários objetos e escolher a janela de tempo máximo para

as tarefas serem concluídas otimizará a solução para desempenho e custo.

Certifique-se de ler a documentação do produto para "Veeam Backup and Replication" e "StorageGRID" antes de começar. A Veeam fornece calculadoras para entender o dimensionamento dos requisitos de infraestrutura e capacidade da Veeam que devem ser usados antes de dimensionar sua solução StorageGRID. Verifique sempre as configurações validadas do Veeam-NetApp no site do Programa Pronto para a Veeam para "Veeam Ready Object, Object imutabilidade e Repository".

Configuração da Veeam

Versão recomendada

É sempre recomendável manter-se atualizado e aplicar os hotfixes mais recentes para o seu sistema Veeam Backup & Replication 12 ou 12,1. Atualmente, recomendamos, no mínimo, a instalação do Veeam 12 patch P20230718.

S3 Configuração do repositório

Um repositório de backup com escalabilidade horizontal (SOBR) é a camada de capacidade do storage de objetos S3. A camada de capacidade é uma extensão do repositório principal que fornece períodos de retenção de dados mais longos e uma solução de storage de baixo custo. A Veeam oferece a capacidade de fornecer imutabilidade por meio da API S3 Object Lock. O Veeam 12 pode usar vários buckets em um repositório com escalabilidade horizontal. O StorageGRID não tem um limite para o número de objetos ou capacidade em um único bucket. O uso de vários buckets pode melhorar o desempenho ao fazer backup de conjuntos de dados muito grandes, onde os dados de backup podem chegar à escala de petabytes em objetos.

A limitação de tarefas simultâneas pode ser necessária dependendo do dimensionamento de sua solução e requisitos específicos. As configurações padrão especificam um slot de tarefa do repositório para cada núcleo da CPU e para cada slot de tarefa um limite de slot de tarefa concorrente de 64. Por exemplo, se o servidor tiver 2 núcleos de CPU, um total de 128 threads simultâneos será usado para o armazenamento de objetos. Isso inclui o PUT, GET e Batch Delete. É recomendável selecionar um limite conservador para os slots de tarefa para começar e ajustar esse valor depois que os backups da Veeam atingirem um estado estável de novos backups e expirarem os dados de backup. Trabalhe com sua equipe de conta do NetApp para dimensionar o sistema StorageGRID de forma adequada para atender às janelas de tempo e desempenho desejados. Ajustar o número de slots de tarefa e o limite de tarefas por slot pode ser necessário para fornecer a solução ideal.

Configuração do trabalho de cópia de segurança

As tarefas de backup da Veeam podem ser configuradas com diferentes opções de tamanho de bloco que devem ser consideradas cuidadosamente. O tamanho padrão do bloco é 1MB e, com as eficiências de storage oferecidas pela Veeam, a deduplicação e a compactação criam tamanhos de objetos de aproximadamente 500KB TB para o backup completo inicial e objetos 100-200kB TB para as tarefas incrementais. Podemos aumentar bastante o desempenho e reduzir os requisitos do armazenamento de objetos escolhendo um tamanho maior de bloco de backup. Embora o tamanho de bloco maior faça grandes melhorias no desempenho de armazenamento de objetos, ele vem com o custo do requisito de capacidade de storage primário potencialmente maior devido à performance de eficiência de storage reduzida. Recomenda-se que as tarefas de backup sejam configuradas com um tamanho de bloco 4MB que cria aproximadamente 2MB objetos para os backups completos e tamanhos de objetos 700kB-1MB para incrementos. Os clientes podem até mesmo configurar tarefas de backup usando tamanho de bloco de 8 MB, que podem ser habilitadas com a ajuda do suporte da Veeam.

A implementação de backups imutáveis faz uso do bloqueio de objetos S3 no armazenamento de objetos. A

opção imutabilidade gera um número maior de solicitações para o armazenamento de objetos para listar e reter atualizações nos objetos.

À medida que as retenções de cópia de segurança expiram, os trabalhos de cópia de segurança processarão a eliminação de objetos. A Veeam envia as solicitações de exclusão para o armazenamento de objetos em solicitações de exclusão multiobjetos de 1000 objetos por solicitação. Para soluções pequenas, isso pode precisar ser ajustado para reduzir o número de objetos por solicitação. A redução desse valor terá o benefício adicional de distribuir mais uniformemente as solicitações de exclusão entre os nós no sistema StorageGRID. Recomenda-se usar os valores na tabela abaixo como ponto de partida para configurar o limite de exclusão de vários objetos. Multiplique o valor na tabela pelo número de nós para o tipo de dispositivo escolhido para obter o valor para a configuração no Veeam. Se este valor for igual ou superior a 1000, não será necessário ajustar o valor predefinido. Se esse valor precisar ser ajustado, trabalhe com o suporte da Veeam para fazer a mudança.

Modelo do aparelho	S3MultiObjectDeleteLimit PB por nó
SG5712	34
SG5760	75
SG6060	200

Trabalhe com sua equipe de conta do NetApp para obter a configuração recomendada com base em suas necessidades específicas. As recomendações de configurações da Veeam incluem:

- Tamanho do bloco de trabalho de backup: 4MB
- Limite de slot de tarefa SOBR 2-16
- Limite de exclusão de objetos múltiplos: 34-1000

Configuração do StorageGRID

Versão recomendada

O NetApp StorageGRID 11,7 ou 11,8 com o hotfix mais recente são as versões recomendadas para implantações da Veeam. É sempre recomendável manter-se atualizado e aplicar os hotfixes mais recentes para o seu sistema StorageGRID.

Balanceador de carga e configuração de endpoint S3

A Veeam exige que o endpoint seja conetado somente via HTTPS. Uma conexão não criptografada não é suportada pela Veeam. O certificado SSL pode ser um certificado auto-assinado, uma autoridade de certificação privada confiável ou uma autoridade de certificação pública confiável. Para garantir o acesso contínuo ao repositório S3, é recomendável usar pelo menos dois balanceadores de carga em uma configuração de HA. Os balanceadores de carga podem ser um serviço de balanceador de carga integrado fornecido pela StorageGRID localizado em cada nó de administrador e nó de gateway ou solução de terceiros, como F5, Kemp, HAproxy, Loadbalancer.org, etc. o uso de um balanceador de carga StorageGRID fornecerá a capacidade de definir classificadores de tráfego (regras de QoS) que podem priorizar a carga de trabalho da Veeam ou limitar a não impactar cargas de trabalho de alta prioridade no sistema StorageGRID.

S3 balde

O StorageGRID é um sistema seguro de storage de alocação a vários clientes. É recomendável criar um locatário dedicado para a carga de trabalho da Veeam. Uma cota de armazenamento pode ser atribuída

opcionalmente. Como prática recomendada, habilite "usar origem de identidade própria". Proteja o usuário de gerenciamento de raiz do locatário com uma senha apropriada. O Veeam Backup 12 requer uma forte consistência para buckets do S3. O StorageGRID oferece várias opções de consistência configuradas no nível do bucket. Para implantações em vários locais, com a Veeam acessando os dados de vários locais, selecione "forte global". Se os backups e restaurações da Veeam acontecerem apenas em um único local, o nível de consistência deve ser definido como "local forte". Para obter mais informações sobre os níveis de consistência do balde, consulte o "documentação". Para usar o StorageGRID para backups da imutabilidade da Veeam, o bloqueio de objetos S3 deve ser ativado globalmente e configurado no bucket durante a criação do bucket.

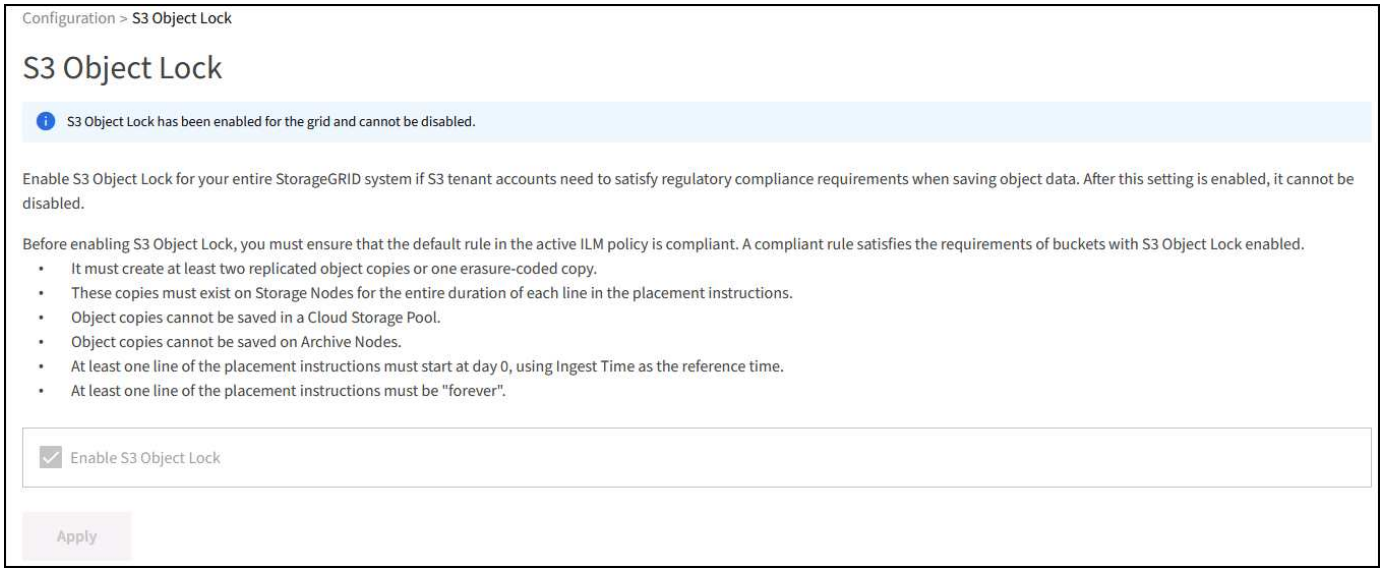
Gerenciamento de ciclo de vida

O StorageGRID é compatível com replicação e codificação de apagamento para proteção no nível de objeto em nós e sites da StorageGRID. A codificação de apagamento requer pelo menos um tamanho de objeto 200kB. O tamanho padrão do bloco para Veeam de 1MB produz tamanhos de objetos que geralmente podem estar abaixo desse tamanho mínimo recomendado de 200kB MB após as eficiências de storage da Veeam. Para o desempenho da solução, não é recomendável usar um perfil de codificação de apagamento abrangendo vários sites, a menos que a conetividade entre os sites seja suficiente para não adicionar latência ou restringir a largura de banda do sistema StorageGRID. Em um sistema StorageGRID multi-site, a regra ILM pode ser configurada para armazenar uma única cópia em cada local. Para uma durabilidade máxima, uma regra poderia ser configurada para armazenar uma cópia codificada de apagamento em cada local. O uso de duas cópias locais para os servidores do Veeam Backup é a implementação mais recomendada para essa carga de trabalho.

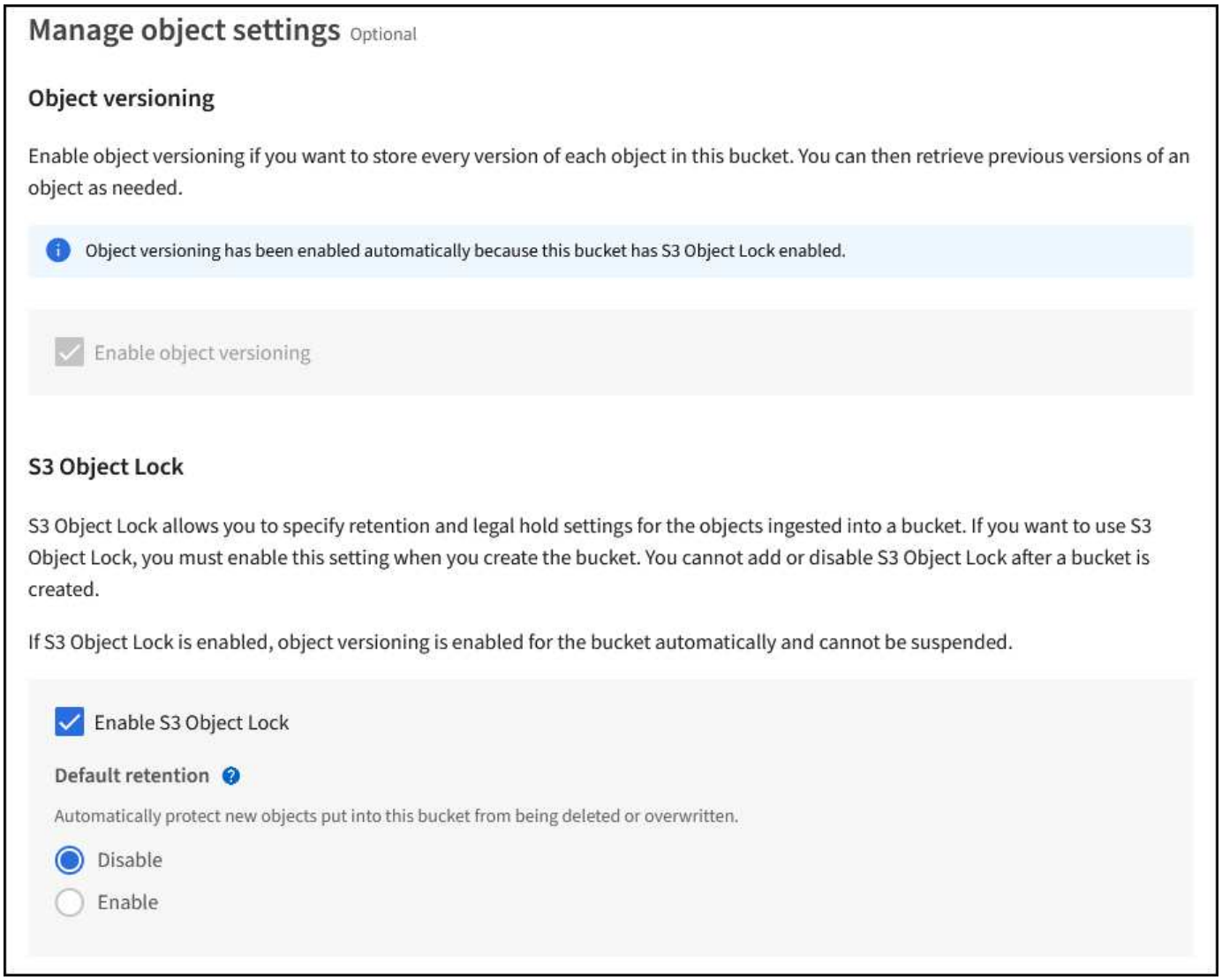
Pontos-chave de implementação

StorageGRID

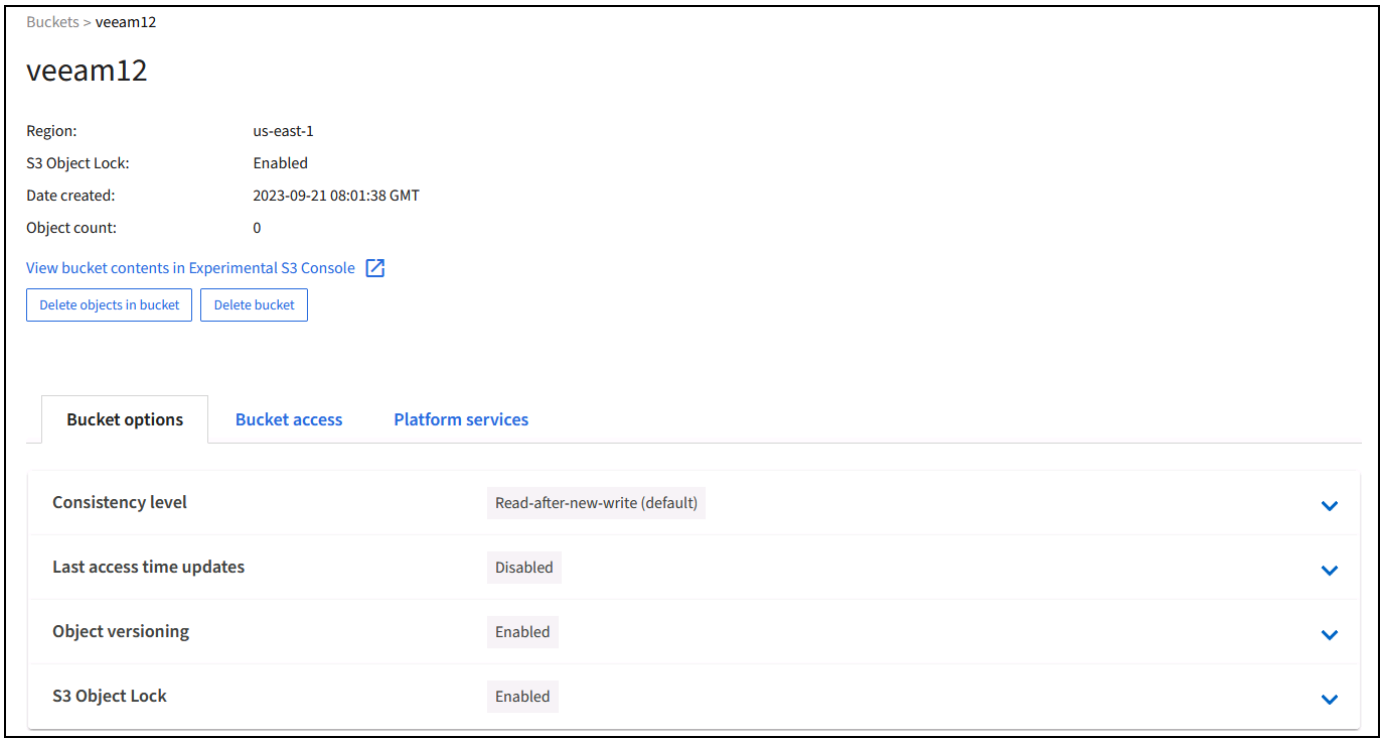
Certifique-se de que o bloqueio de objetos está ativado no sistema StorageGRID se a imutabilidade for necessária. Encontre a opção na IU de gerenciamento em Configuration/S3 Object Lock.



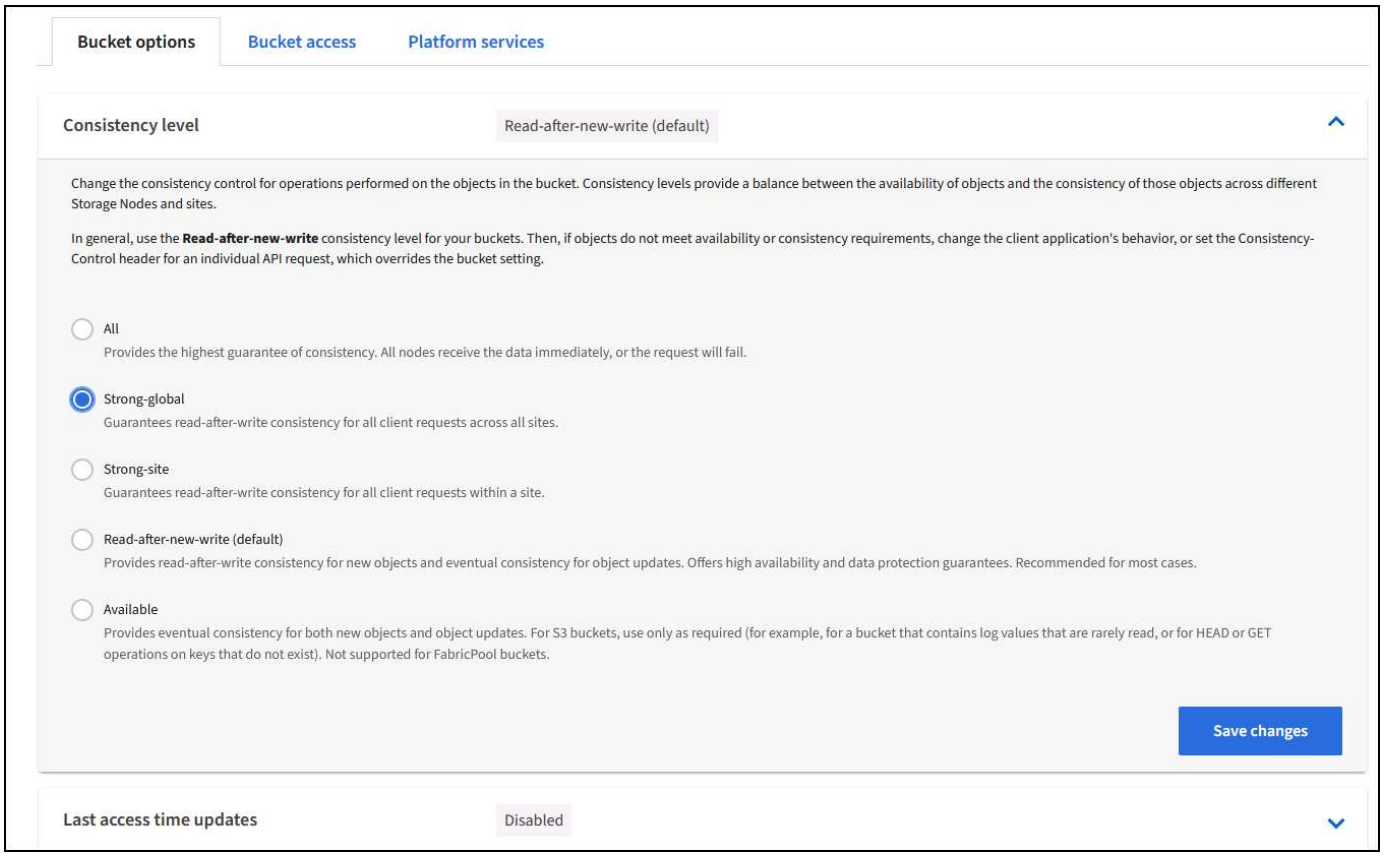
Ao criar o bucket, selecione "Ativar bloqueio de objetos S3" se esse bucket for usado para backups de imutabilidade. Isso habilitará automaticamente o controle de versão do bucket. Deixe a retenção padrão desativada, pois a Veeam definirá a retenção de objetos explicitamente. Controle de versão e bloqueio de objetos S3 não devem ser selecionados se a Veeam não estiver criando backups imutáveis.



Quando o bucket for criado, vá para a página de detalhes do bucket criado. Selecione o nível de consistência.



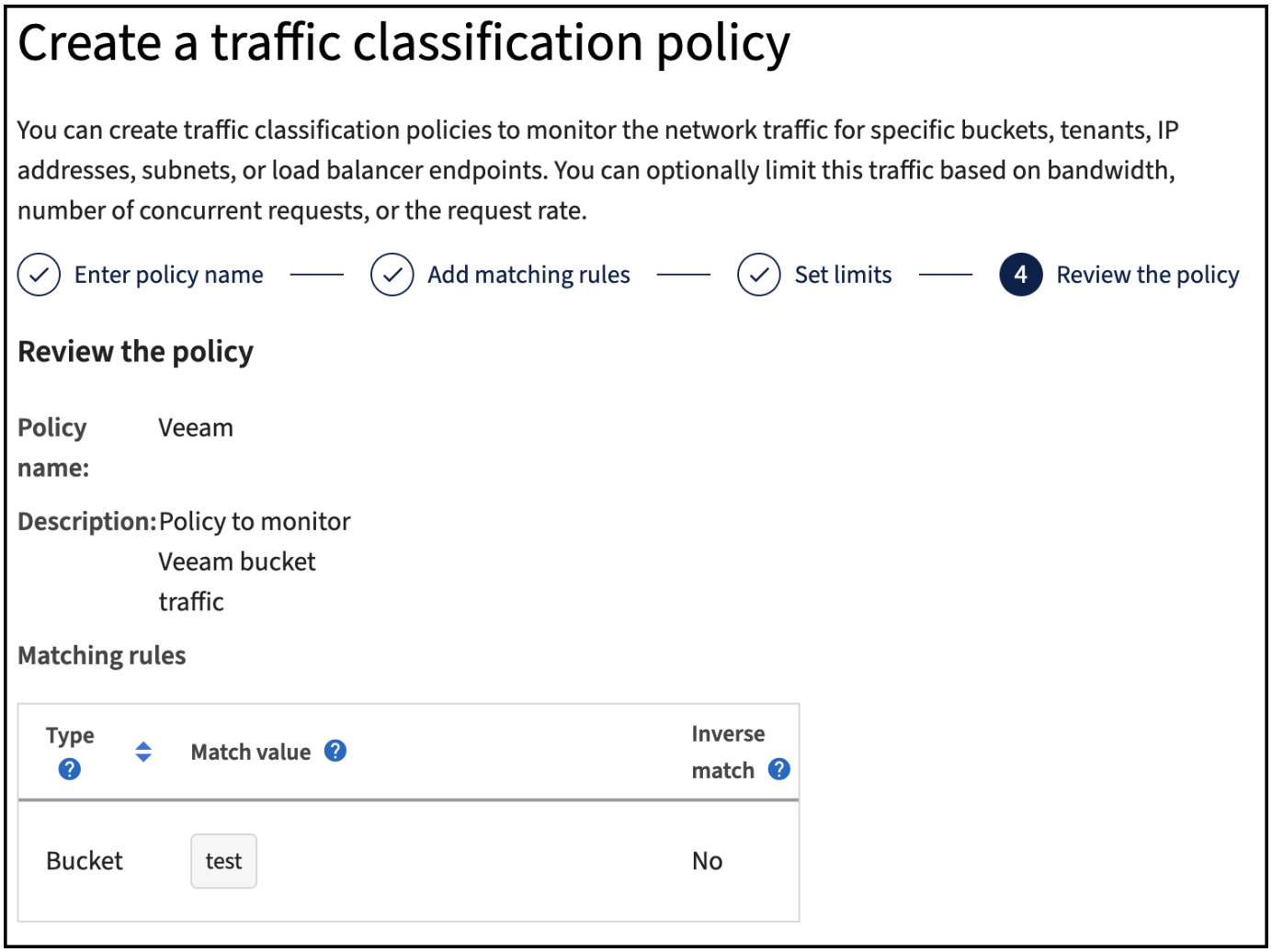
A Veeam requer uma forte consistência para buckets do S3. Então, para implantações em vários locais com a Veeam acessando os dados de vários locais, selecione "forte global". Se os backups e restaurações da Veeam acontecerem apenas em um único local, o nível de consistência deve ser definido como "local forte". Salve as alterações.



O StorageGRID fornece um serviço de balanceador de carga integrado em todos os nós de administração e

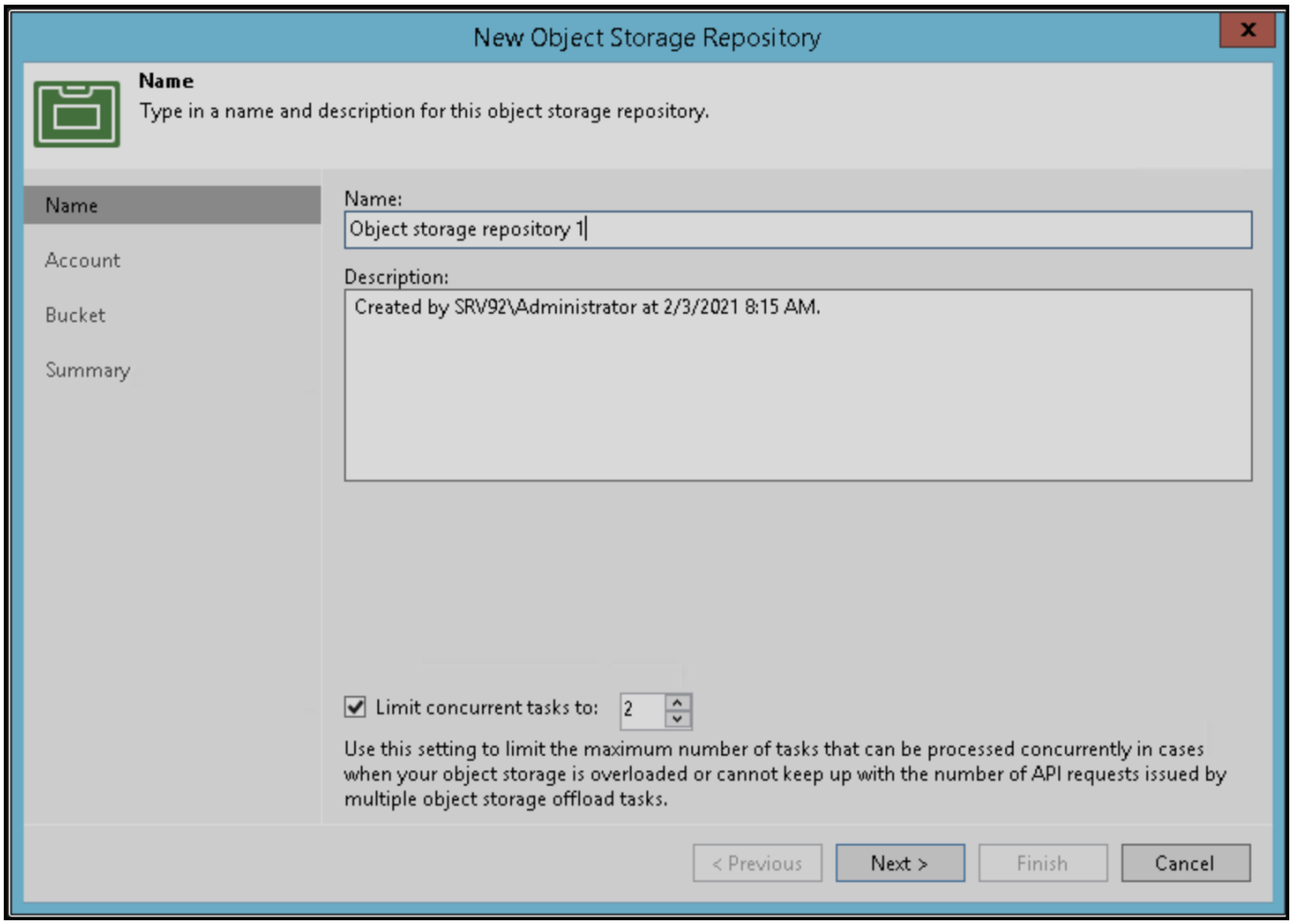
de gateway dedicados. Uma das muitas vantagens de usar este balanceador de carga é a capacidade de configurar as políticas de classificação de tráfego (QoS). Embora eles sejam usados principalmente para limitar o impactos de aplicativos em outras cargas de trabalho de clientes ou priorizar uma carga de trabalho sobre outras, eles também fornecem um bônus de coleta de métricas adicionais para ajudar no monitoramento.

No separador de configuração, selecione "classificação de tráfego" e crie uma nova política. Nomeie a regra e selecione o(s) intervalo(s) ou o locatário como o tipo. Introduza o(s) nome(s) do(s) bucket(s) ou inquilino(s). Se a QoS for necessária, defina um limite, mas para a maioria das implementações, queremos apenas adicionar os benefícios de monitoramento que isso proporciona, portanto, não defina um limite.

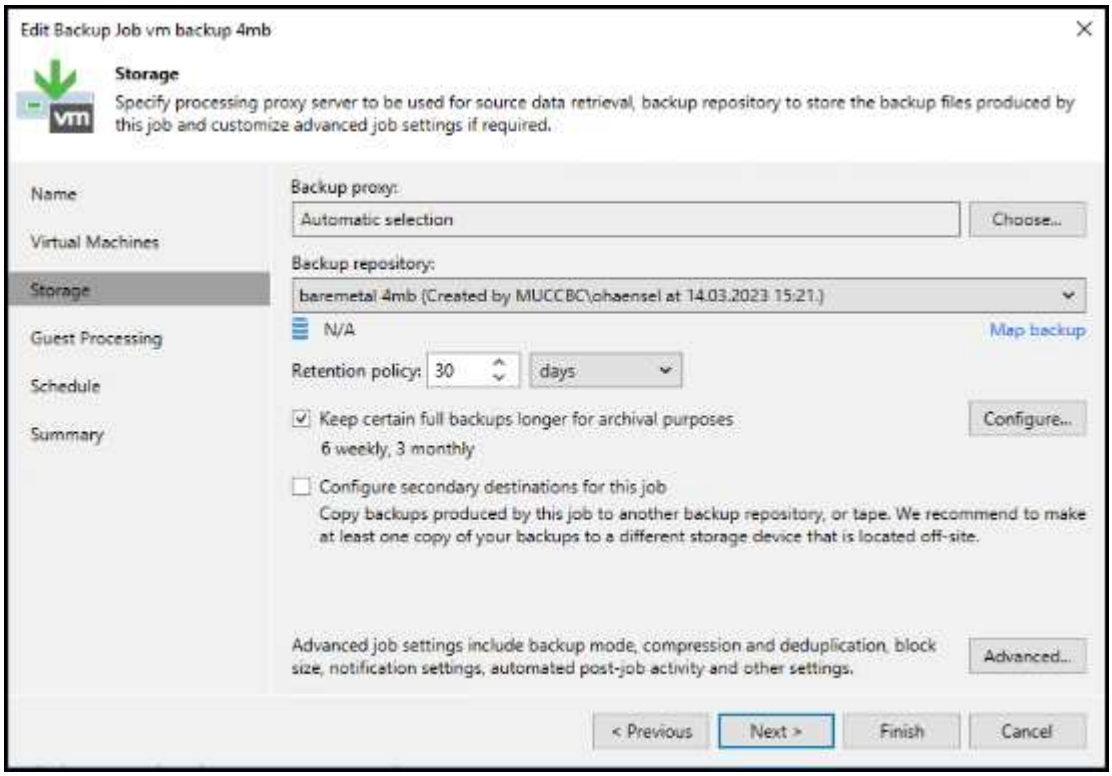


Veeam

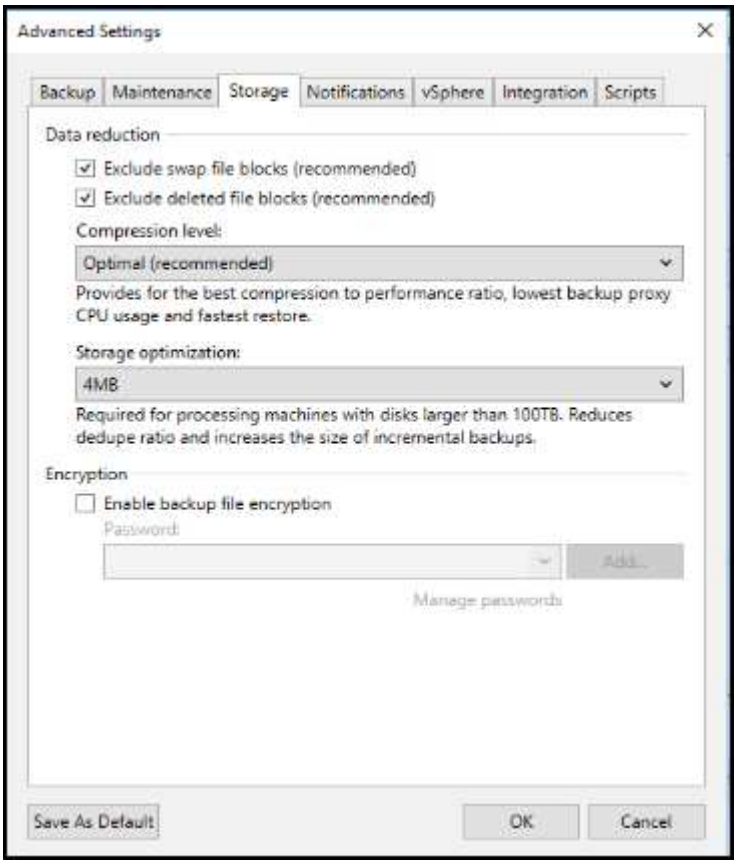
Dependendo do modelo e da quantidade de dispositivos StorageGRID, pode ser necessário selecionar e configurar um limite para o número de operações simultâneas no bucket.



Siga a documentação da Veeam sobre a configuração da tarefa de backup no console da Veeam para iniciar o assistente. Depois de adicionar VMs, selecione o repositório SOBR.



Clique em Configurações avançadas e altere as configurações de otimização de armazenamento para 4 MB ou mais. A compactação e a deduplicação devem ser habilitadas. Altere as configurações do convidado de acordo com seus requisitos e configure o agendamento do trabalho de backup.



Monitorização do StorageGRID

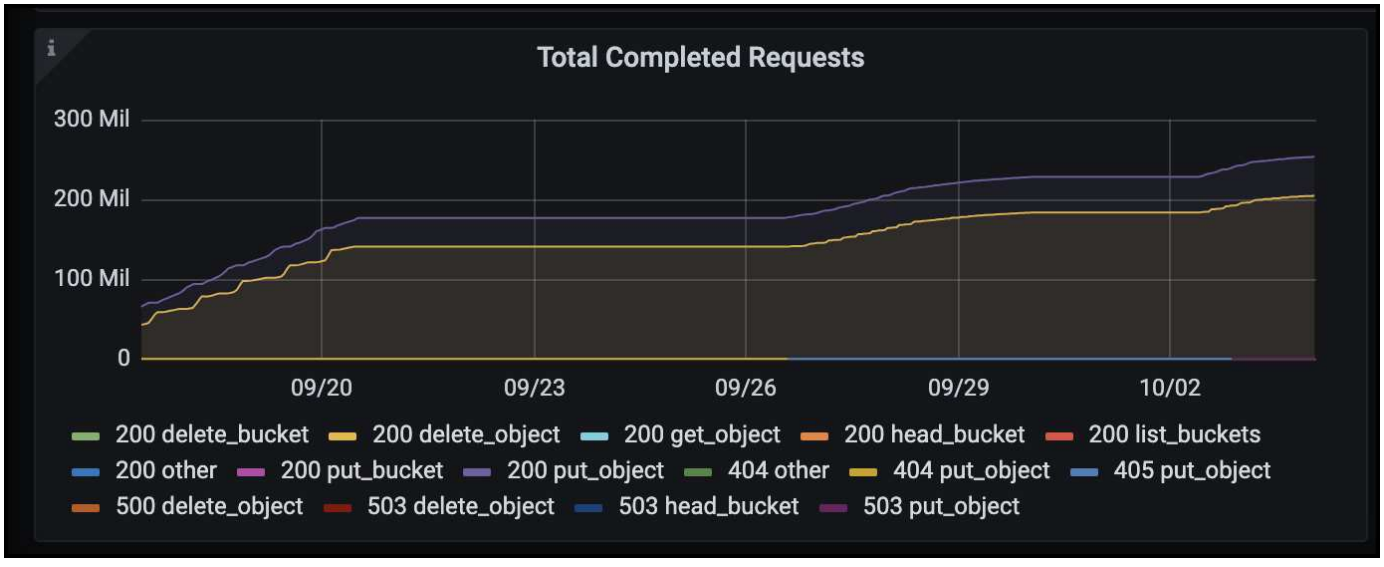
Para ter uma visão completa de como a Veeam e o StorageGRID estão funcionando juntos, você precisará esperar até que o tempo de retenção dos primeiros backups expire. Até esse ponto, a carga de trabalho da Veeam consiste principalmente em operações PUT e não ocorreram exclusões. Uma vez que os dados de backup expiram e as limpezas estão ocorrendo, você pode agora ver o uso consistente completo no armazenamento de objetos e ajustar as configurações no Veeam, se necessário.

O StorageGRID fornece gráficos convenientes para monitorar o funcionamento do sistema localizado na página métricas do separador suporte. Os principais painéis a serem analisados serão a Visão geral do S3, ILM e a Política de classificação de tráfego, se uma política foi criada. No painel Visão geral do S3, você encontrará informações sobre as taxas de operação, latências e respostas de solicitações do S3.

Olhando para as taxas do S3 e as solicitações ativas, você pode ver quanto da carga cada nó está lidando e o número total de solicitações por tipo.

O gráfico de duração média mostra o tempo médio que cada nó está tomando para cada tipo de solicitação. Esta é a latência média da solicitação e pode ser um bom indicador de que ajustes adicionais podem ser necessários, ou há espaço para o sistema StorageGRID assumir mais carga.

No gráfico Total de solicitações concluídas, você pode ver as solicitações por tipo e códigos de resposta. Se você vir respostas diferentes de 200 (OK) para as respostas, isso pode indicar um problema como o sistema StorageGRID está recebendo fortemente carregado enviando respostas 503 (lento) e alguma sintonização adicional pode ser necessária, ou chegou a hora de expandir o sistema para a carga aumentada.



No Painel ILM, você pode monitorar o desempenho de exclusão do seu sistema StorageGRID. O StorageGRID usa uma combinação de exclusões síncronas e assíncronas em cada nó para tentar otimizar o desempenho geral de todas as solicitações.

Com uma Política de classificação de tráfego, podemos visualizar métricas sobre a taxa de transferência de solicitação do balanceador de carga, taxas, duração, bem como os tamanhos de objeto que a Veeam está enviando e recebendo.

Onde encontrar informações adicionais

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

- "Documentação do produto NetApp StorageGRID 11,9"
- "Veeam Backup and Replication"

Configure a fonte de dados do Dremio com o StorageGRID

Por Angela Cheng

O Dremio dá suporte a uma variedade de fontes de dados, incluindo armazenamento de objetos baseado na nuvem ou no local. Você pode configurar o Dremio para usar o StorageGRID como fonte de dados de armazenamento de objetos.

Configurar a fonte de dados do Dremio

Pré-requisitos

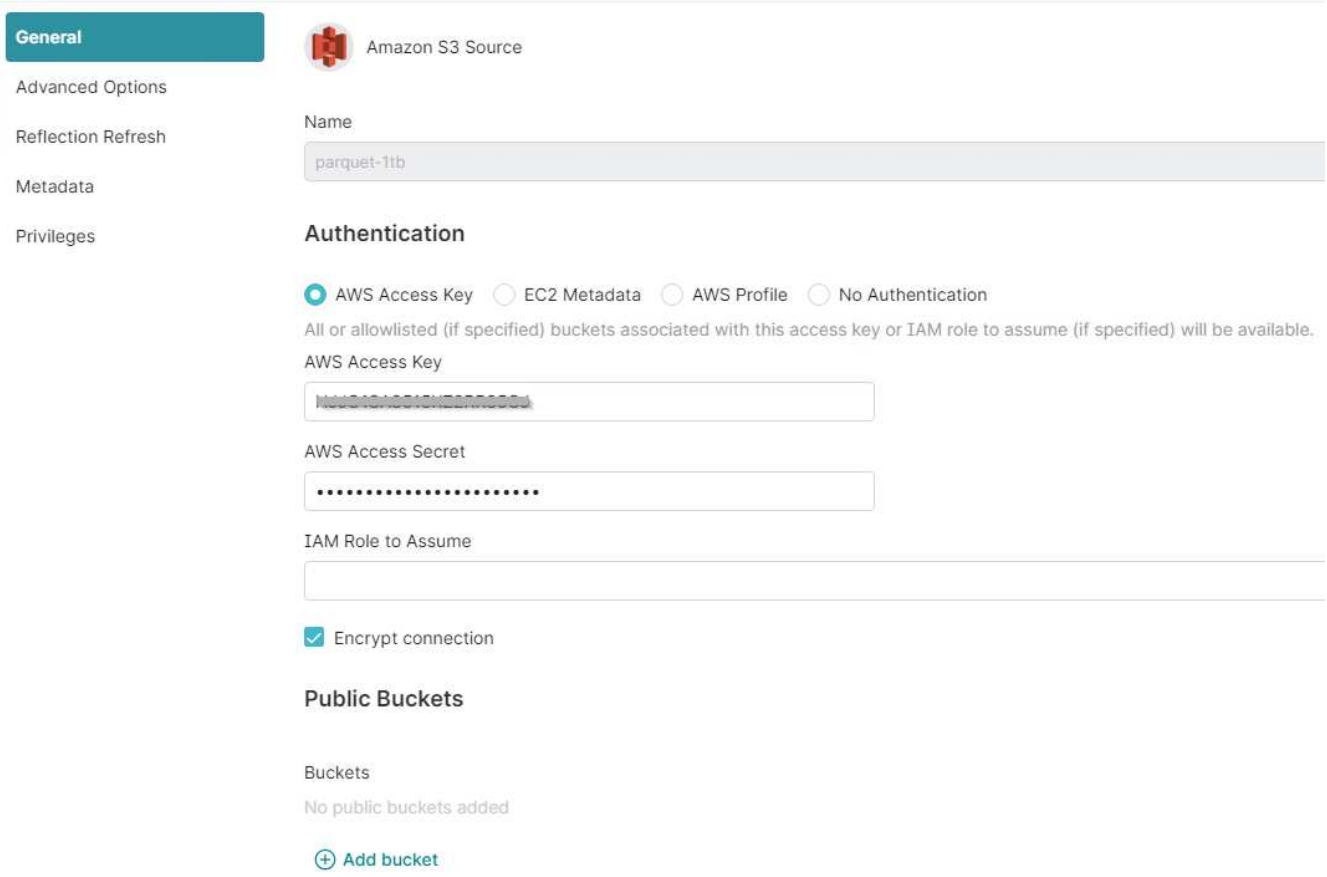
- Um URL de endpoint do StorageGRID S3, um ID de chave de acesso do locatário S3 e chave de acesso secreta.
- Recomendação de configuração do StorageGRID: Desativar a compactação (desativada por padrão). Dremio usa o intervalo de bytes get para buscar diferentes intervalos de bytes dentro do mesmo objeto simultaneamente durante a consulta. O tamanho típico para solicitações de intervalo de bytes é 1MB. O objeto comprimido degrada a gama de bytes OBTENHA desempenho.

Guia de Dremio

"Conetando ao Amazon S3 - Configurando o armazenamento compatível com S3".

Instrução

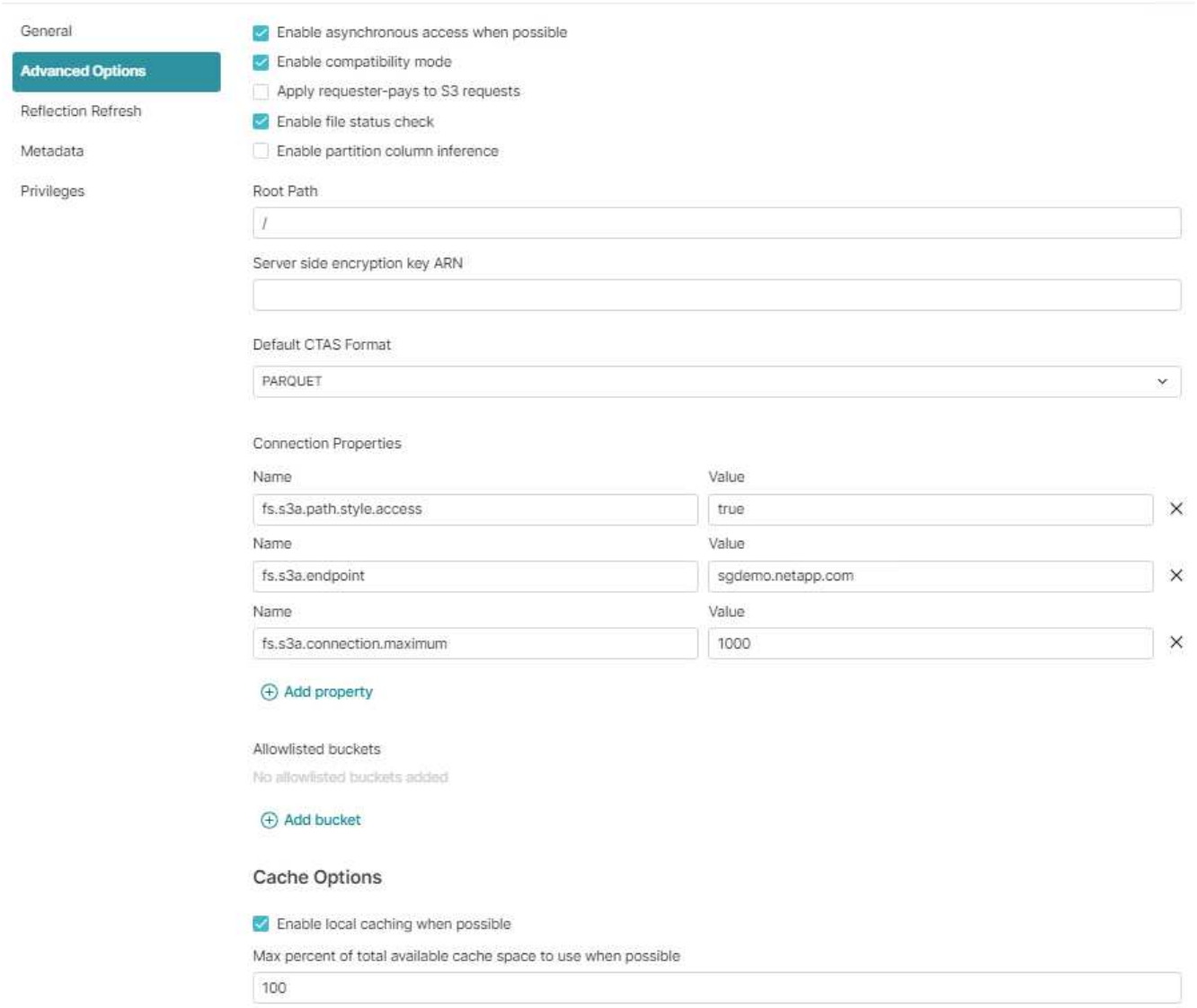
1. Na página Datasets do Dremio, clique em assinar para adicionar uma fonte, selecione 'Amazon S3'.
2. Insira um nome para esta nova fonte de dados, ID da chave de acesso ao locatário do StorageGRID S3 e chave de acesso secreto.
3. Marque a caixa 'criptografar conexão' se estiver usando https para conexão com o endpoint StorageGRID S3. Se estiver usando CA cert autoassinado para este endpoint S3, siga a instrução de guia Dremio para adicionar este CA cert no servidor Dremio <JAVA_HOME>/jre/lib/security **sample screenshot**



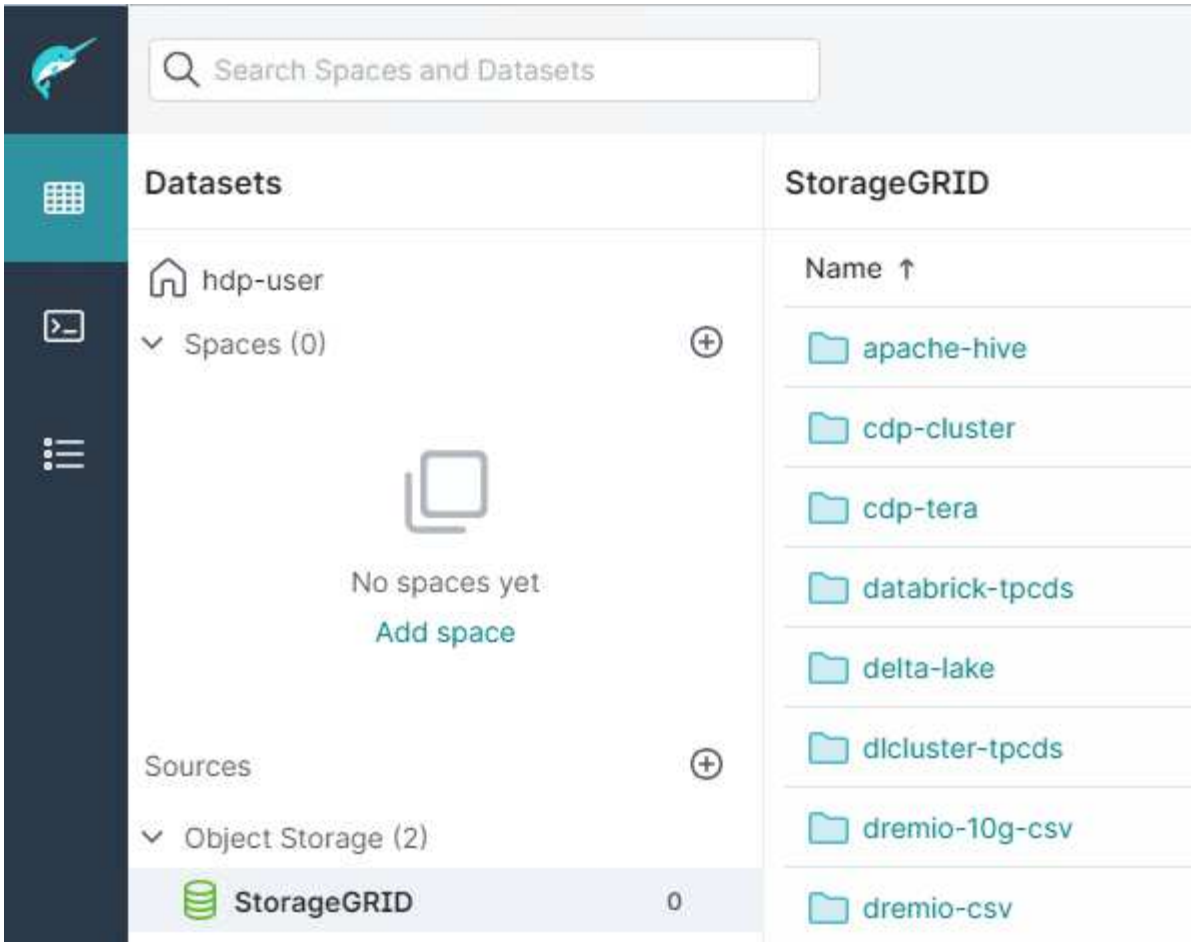
4. Clique em "Opções avançadas", verifique "Ativar modo de compatibilidade"
5. Em Propriedades de conexão, clique em Adicionar propriedades e adicione essas s3a propriedades.
6. fs.s3a.connection.o padrão máximo é 100. Se os conjuntos de dados do S3 incluírem ficheiros Parquet grandes com 100 ou mais colunas, tem de introduzir um valor superior a 100. Consulte o guia Dremio para obter esta definição.

Nome	Valor
fs.s3a.endpoint	_ Endpoint do cliente StorageGRID S3:port>_
fs.s3a.path.style.access	verdadeiro
fs.s3a.connection.maximum	_ valor de cliente maior que 100>_

Captura de tela de amostra



7. Configure outras opções do Dremio de acordo com os requisitos da sua organização ou aplicação.
8. Clique no botão Salvar para criar esta nova fonte de dados.
9. Depois que a fonte de dados StorageGRID for adicionada com sucesso, uma lista de buckets será exibida no painel esquerdo. * Captura de tela de amostra*



NetApp StorageGRID com GitLab

Por Angela Cheng

A NetApp testou o StorageGRID com o GitLab. Veja exemplo de configuração do GitLab abaixo. "Guia de configuração de armazenamento de objetos GitLab"Consulte para obter detalhes.

Exemplo de conexão de armazenamento de objetos

Para instalações do pacote Linux, este é um exemplo `connection` da configuração na forma consolidada. Edite `/etc/gitlab/gitlab.rb` e adicione as seguintes linhas, substituindo os valores desejados:

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

Procedimentos e exemplos de API

Teste e demonstre as opções de criptografia S3 no StorageGRID

Por Aron Klein

O StorageGRID e a API S3 oferecem várias maneiras diferentes de criptografar seus dados em repouso. Para saber mais, "Reveja os métodos de encriptação StorageGRID" consulte .

Este guia demonstrará os métodos de criptografia da API S3.

Criptografia do lado do servidor (SSE)

O SSE permite que o cliente armazene um objeto e criptografe-o com uma chave única que é gerenciada pelo StorageGRID. Quando o objeto é solicitado, o objeto é descriptografado pela chave armazenada no StorageGRID.

Exemplo SSE

- COLOQUE um objeto com SSE

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- DIRIJA o objeto para verificar a criptografia

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- OBTENHA o objeto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

SSE permite que o cliente armazene um objeto e criptografe-o com uma chave única que é fornecida pelo cliente com o objeto. Quando o objeto é solicitado, a mesma chave deve ser fornecida para descriptografar e retornar o objeto.

Exemplo SSE-C.

- Para fins de teste ou demonstração, você pode criar uma chave de criptografia
  - Crie uma chave de criptografia

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- Coloque um objeto com a chave gerada

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- Cabeça o objeto

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:20:02+00:00",
    "ContentLength": 47,
    "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
    "ContentType": "binary/octet-stream",
    "Metadata": {},
    "SSECustomerAlgorithm": "AES256",
    "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
}
```

Se você não fornecer a chave de criptografia, você receberá um erro "ocorreu um erro (404) ao chamar a operação HeadObject: Not found"

- Obtenha o objeto

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

Se você não fornecer a chave de criptografia, você receberá um erro "ocorreu um erro (InvalidRequest) ao chamar a operação GetObject: O objeto foi armazenado usando uma forma de criptografia do lado do servidor. Os parâmetros corretos devem ser fornecidos para recuperar o objeto."

Criptografia do lado do servidor do bucket (SSE-S3)

O SSE-S3 permite que o cliente defina um comportamento de criptografia padrão para todos os objetos armazenados em um bucket. Os objetos são criptografados com uma chave exclusiva que é gerenciada pelo StorageGRID. Quando o objeto é solicitado, o objeto é descriptografado pela chave armazenada no StorageGRID.

Exemplo SSE-S3 do bucket

- Crie um novo intervalo e defina uma política de criptografia padrão
  - Crie um novo balde

    ```
    aws s3api create-bucket --bucket <bucket> --region us-east-1
    --endpoint-url https://s3.example.com
    ```

  - Coloque criptografia de bucket

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- Coloque um objeto no balde

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Cabeça o objeto

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- OBTENHA o objeto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Teste e demonstre o bloqueio de objetos S3D no StorageGRID

Por Aron Klein

O Object Lock fornece um modelo WORM para impedir que objetos sejam excluídos ou substituídos. A implementação do StorageGRID do bloqueio de objetos é avaliada pela Cohasset para ajudar a atender aos requisitos regulatórios, oferecendo suporte à retenção legal e ao modo de conformidade para retenção de objetos e políticas de retenção de buckets padrão.

Este guia demonstrará a API S3D Object Lock.

Guarda legal

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

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- Verifique-o com uma operação GET.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Desligue a retenção legal

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- Verifique-o com uma operação GET.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Modo de conformidade

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

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- Verifique o status de retenção

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

Retenção padrão

- Defina o período de retenção em dias e anos versículos a data de retenção até definida com a api per object.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- Verifique o status de retenção

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- Coloque um objeto no balde

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- A duração de retenção definida no bucket é convertida em um carimbo de data/hora de retenção no objeto.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Teste a exclusão de um objeto com uma retenção definida

O bloqueio de objetos é construído sobre o controle de versão. A retenção é definida em uma versão do objeto. Se uma tentativa for feita para excluir um objeto com uma retenção definida e nenhuma versão for especificada, um marcador de exclusão será criado como a versão atual do objeto.

- Exclua o objeto com retenção definida

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- Liste os objetos no intervalo

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - Observe que o objeto não está listado.

- Liste versões para ver o marcador de exclusão e a versão original bloqueada

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Exclua a versão bloqueada do objeto

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

Políticas e permissões no StorageGRID

Aqui estão exemplos de políticas e permissões no StorageGRID S3.

A estrutura de uma política

No StorageGRID, as políticas de grupo são as mesmas que as políticas de serviço do AWS user (IAM) S3.

As políticas de grupo são necessárias no StorageGRID. Um usuário com S3 chaves de acesso, mas não atribuído a um grupo de usuários, ou atribuído a um grupo sem uma política que conceda algumas permissões, não poderá acessar nenhum dado.

As políticas de bucket e grupo compartilham a maioria dos mesmos elementos. As políticas são construídas no formato json e podem ser geradas usando o. "Gerador de políticas da AWS"

Todas as políticas definirão o efeito, a(s) ação(ões) e o(s) recurso(s). As políticas de bucket também definirão um principal.

O **efeito** será permitir ou negar o pedido.

O **principal**

- Aplica-se apenas a políticas de bucket.
- O principal é a(s) conta(s)/usuário(s) que está sendo concedido(s) ou negado(s) as permissões.
- Pode ser definido como:
  - Um curinga

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - Um ID de locatário para todos os usuários em um locatário (equivalente à conta da AWS)

```
"Principal": { "AWS": "27233906934684427525" }
```

- Um usuário (local ou federado de dentro do locatário o bucket reside, ou outro locatário na grade)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

- Um grupo (local ou federado de dentro do locatário o bucket reside, ou outro inquilino na grade).

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

A **Ação** é o conjunto de S3 operações que estão sendo concedidas ou negadas ao(s) usuário(s).

> Para políticas de Grupo, a ação S3:ListBucket permitida é necessária para que os usuários executem quaisquer ações S3D.

O **recurso** é o bucket ou buckets em que os princípios estão sendo concedidos ou negados a capacidade de executar as ações. Opcionalmente, pode haver uma **condição** para quando a ação da política é válida.

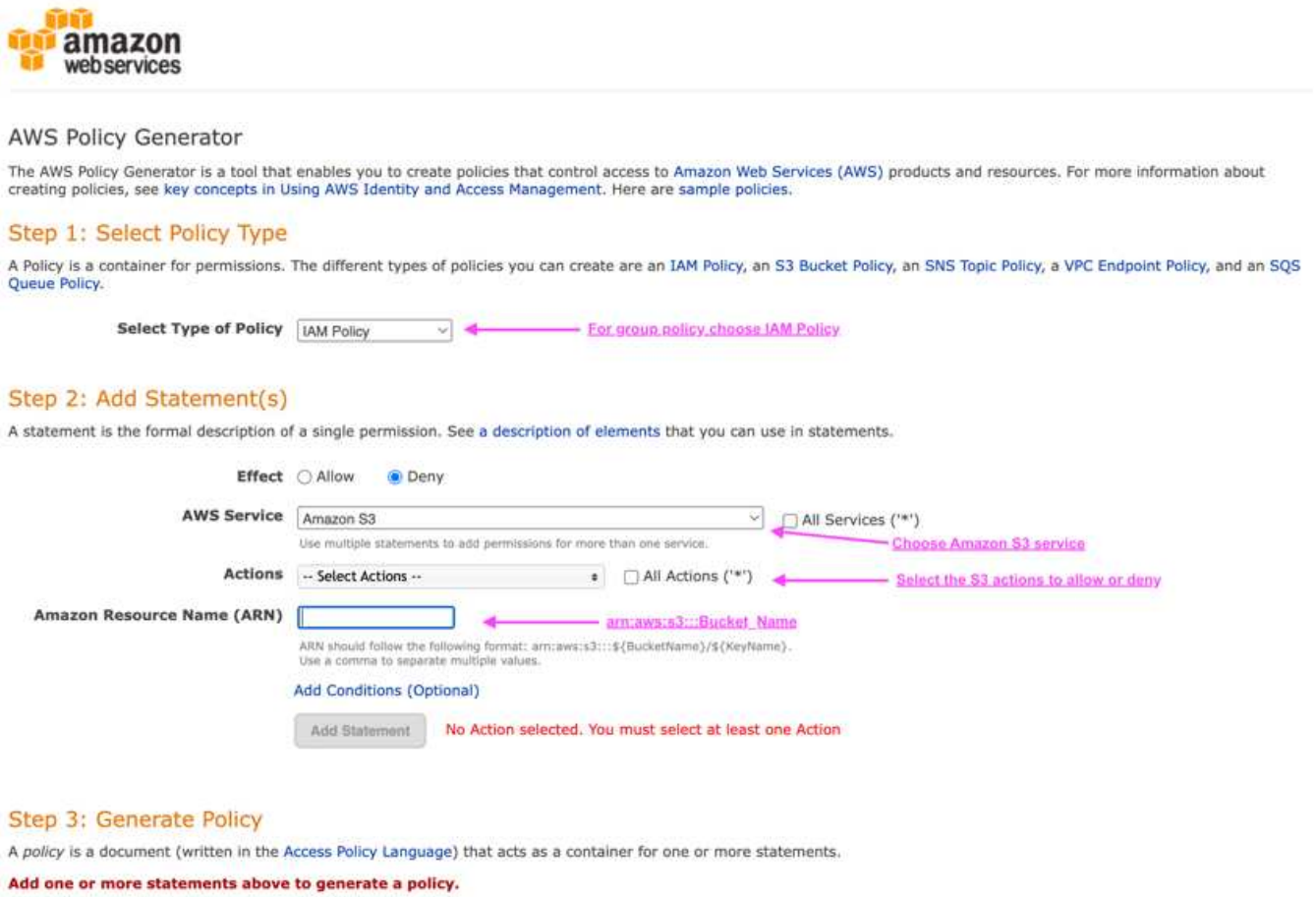
O formato da política JSON será assim:

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

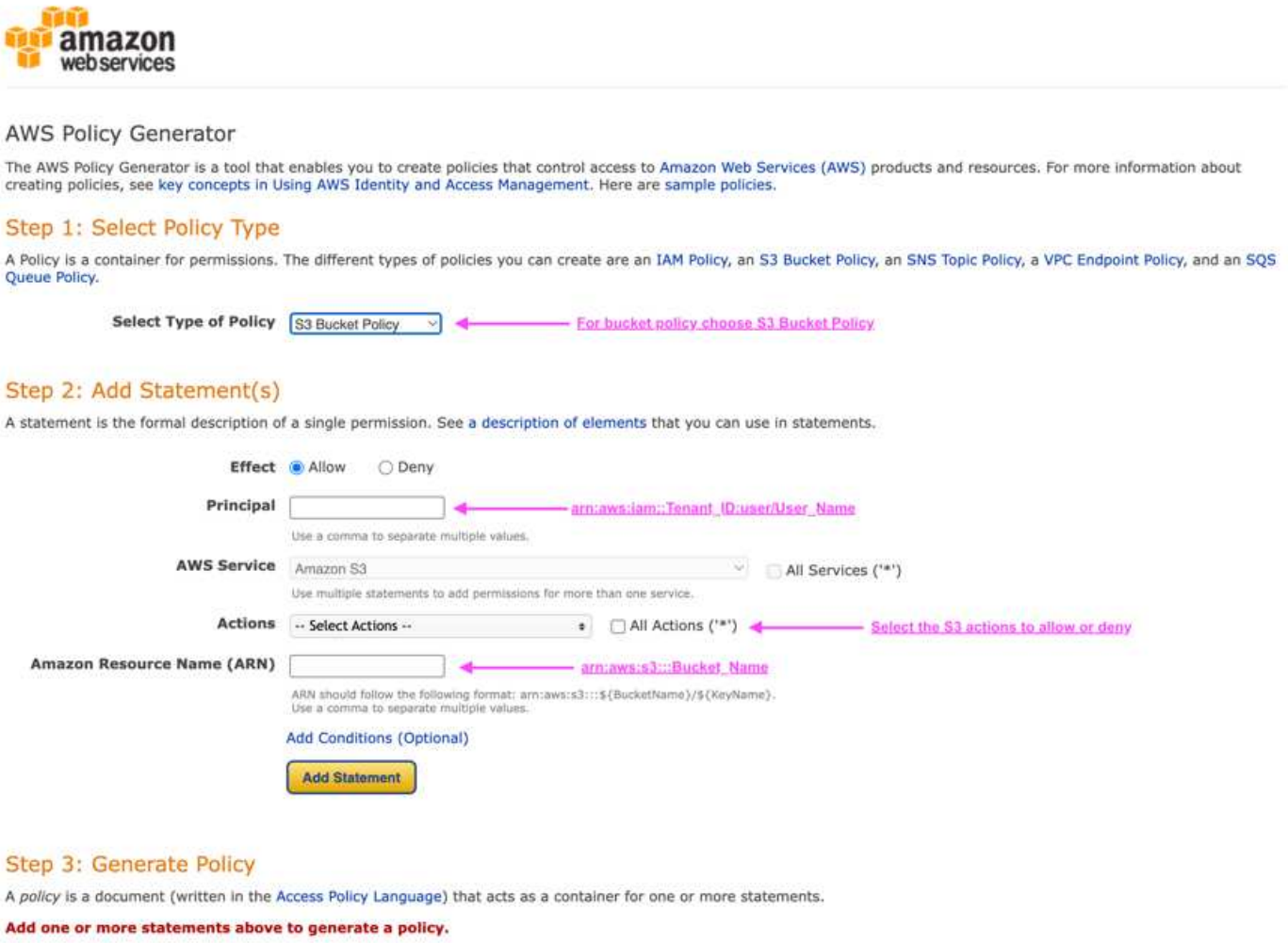
Usando o gerador de políticas da AWS

O gerador de políticas da AWS é uma ótima ferramenta para ajudar a obter o código json com o formato correto e as informações que você está tentando implementar.

Para gerar as permissões para uma política de grupo do StorageGRID: * Escolha a política do IAM para o tipo de política. * Selecione o botão para o efeito desejado - permitir ou negar. É uma boa prática iniciar suas políticas com as permissões de negação e, em seguida, adicionar as permissões de permissão * na caixa suspensa ações clique na caixa ao lado de quantas das ações S3 que você deseja incluir nesta permissão ou na caixa "todas as ações". * Digite os caminhos de intervalo na caixa Nome de recurso do Amazon (ARN). Inclua "ARN:aws:S3:::" antes do nome do intervalo. Ex. "arn:aws:s3:::example_bucket"

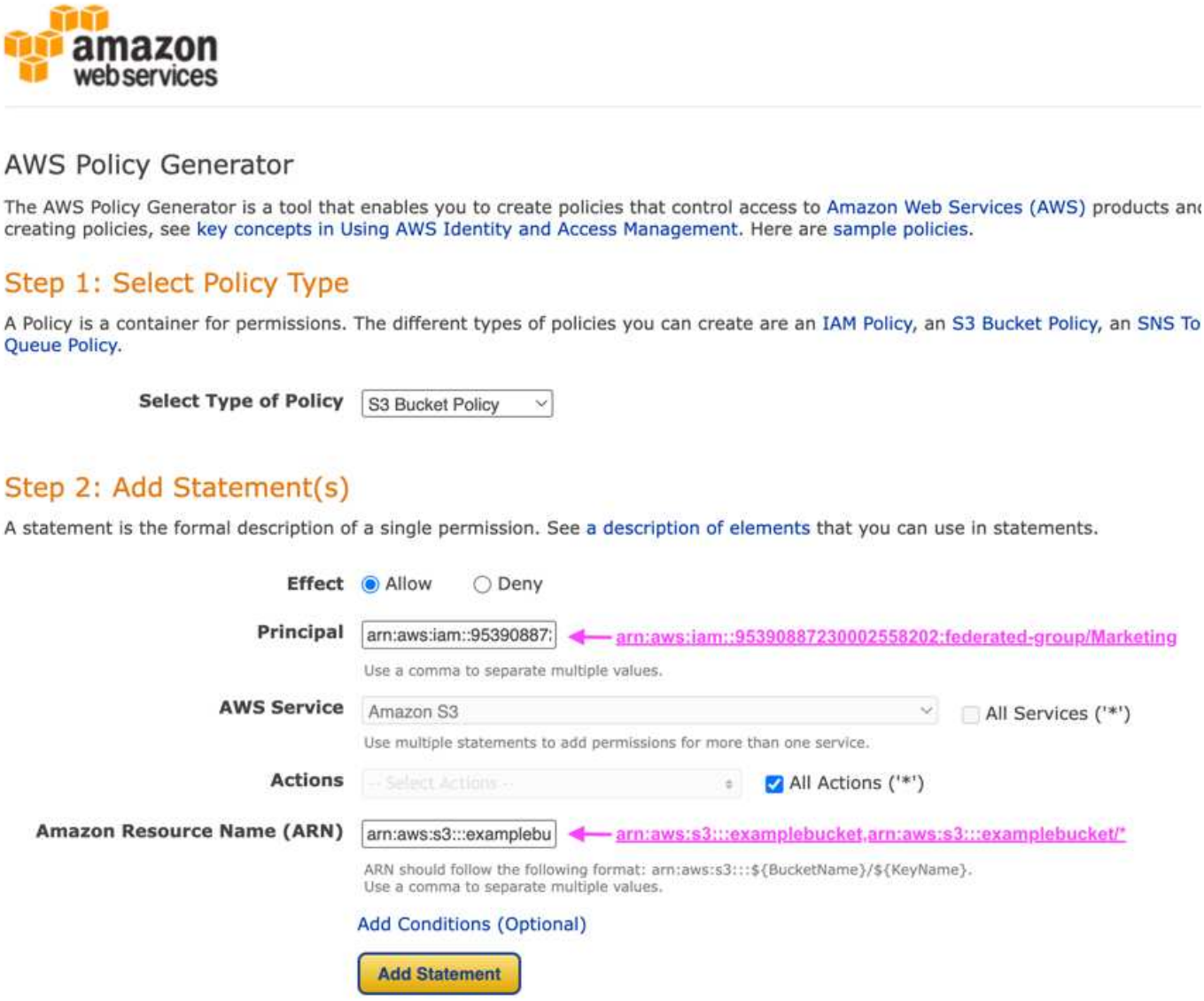


Para gerar as permissões para uma política de bucket: * Escolha a Política de bucket do S3 para o tipo de diretiva. * Selecione o botão para o efeito desejado - permitir ou negar. É uma boa prática iniciar suas políticas com as permissões de negação e, em seguida, adicionar as permissões de permissão * tipo nas informações de usuário ou grupo para o principal. * Na lista suspensa ações, clique na caixa ao lado de tantas das S3 ações que você deseja incluir nesta permissão ou na caixa "todas as ações". * Digite os caminhos de intervalo na caixa Nome de recurso do Amazon (ARN). Inclua "ARN:aws:S3:::" antes do nome do intervalo. Ex. "arn:aws:s3:::example_bucket"



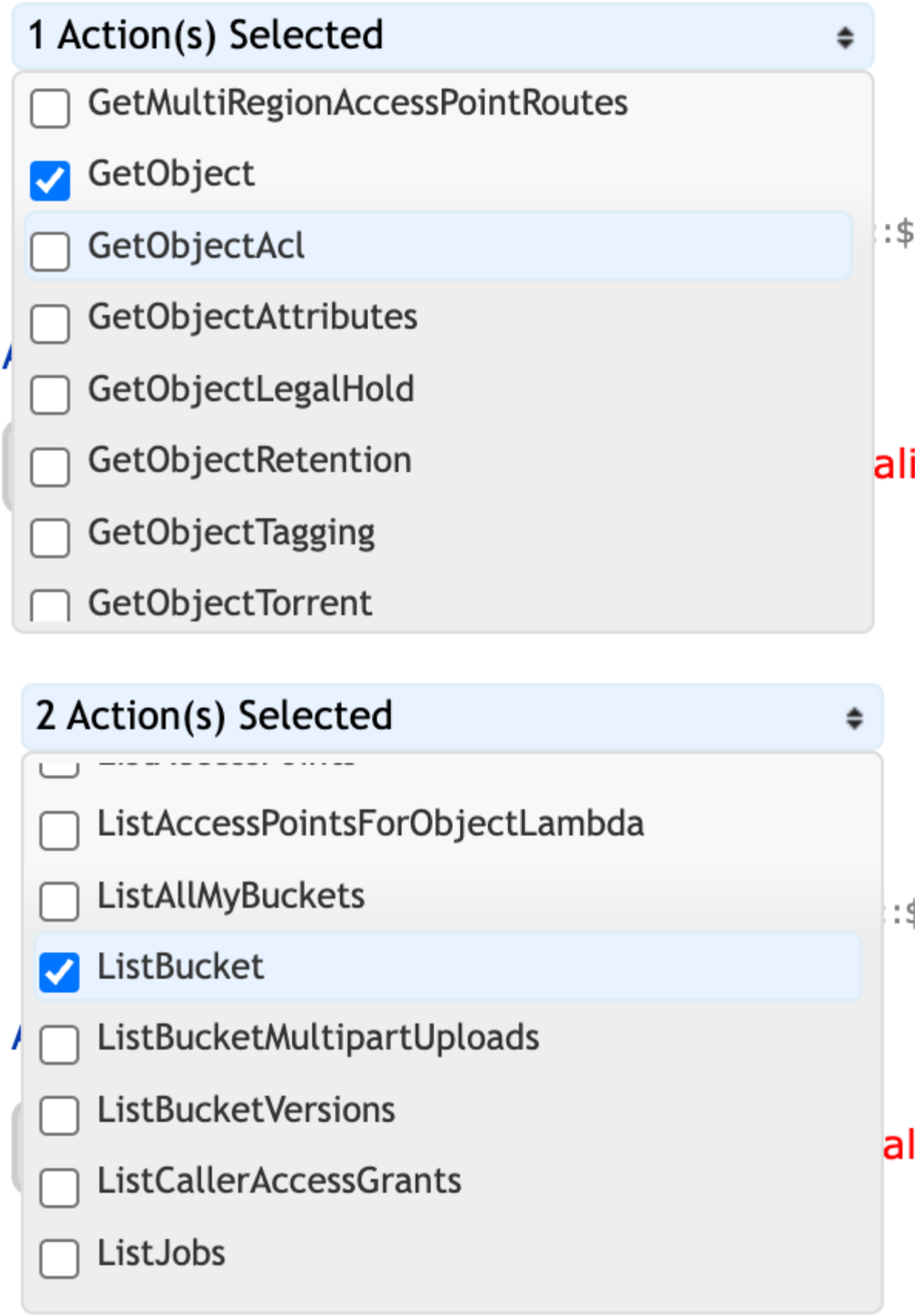
Por exemplo, se você quiser gerar uma política de bucket para permitir que todos os usuários executem operações GetObject em todos os objetos no bucket, enquanto somente os usuários pertencentes ao grupo "Marketing" na conta especificada terão acesso total.

- Selecione S3 Bucket Policy como o tipo de política.
- Escolha o efeito permitir
- Insira as informações do grupo Marketing - ARN:aws:iam::95390887230002558202:grupo federado/Marketing
- Clique na caixa "todas as ações"
- Insira as informações do bucket - ARN:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*

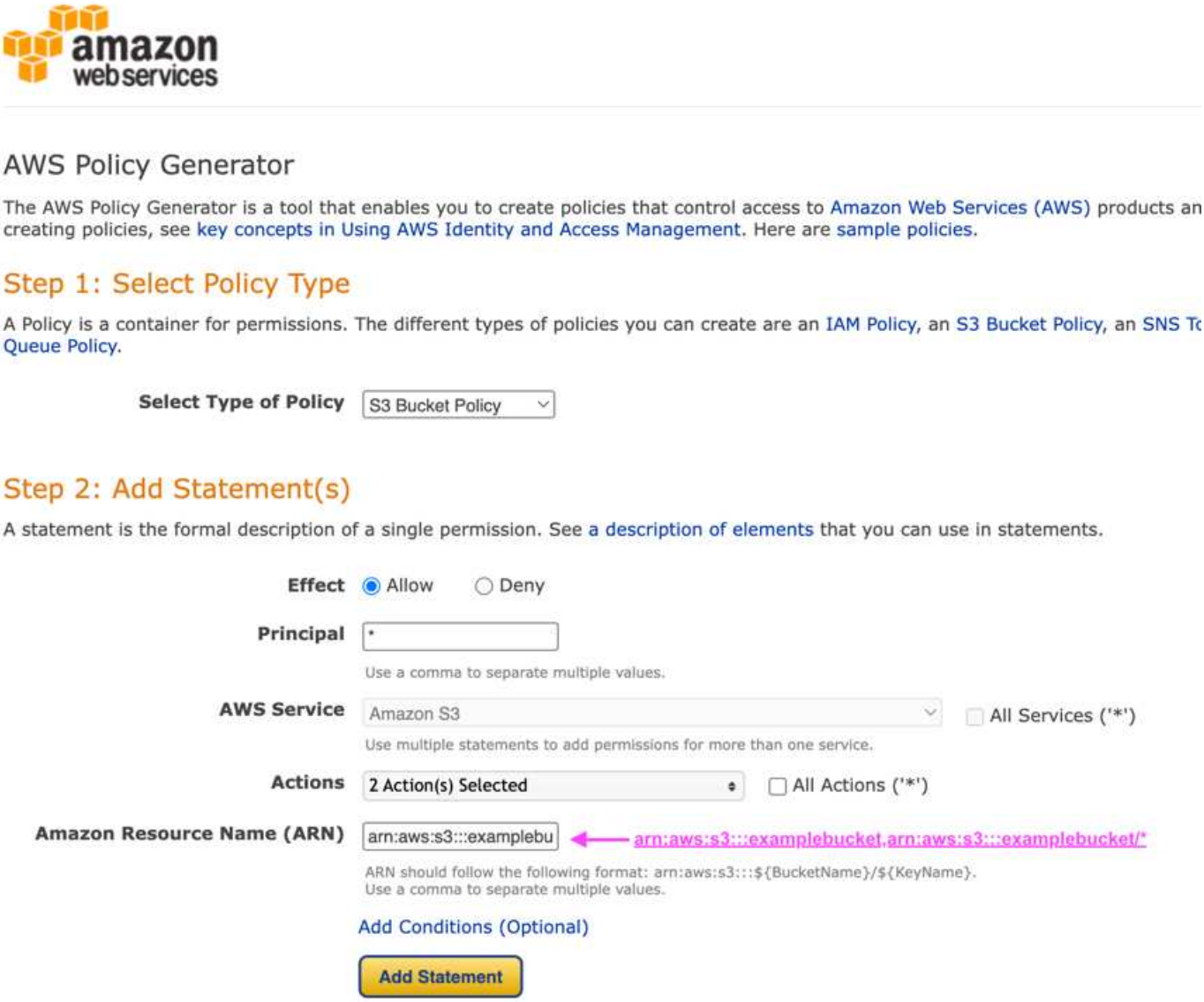


- Clique no botão "Adicionar declaração"

- Escolha o efeito permitir
- Digite o asterisco (*) para todos
- Clique na caixa ao lado de ações GetObject e ListBucket"

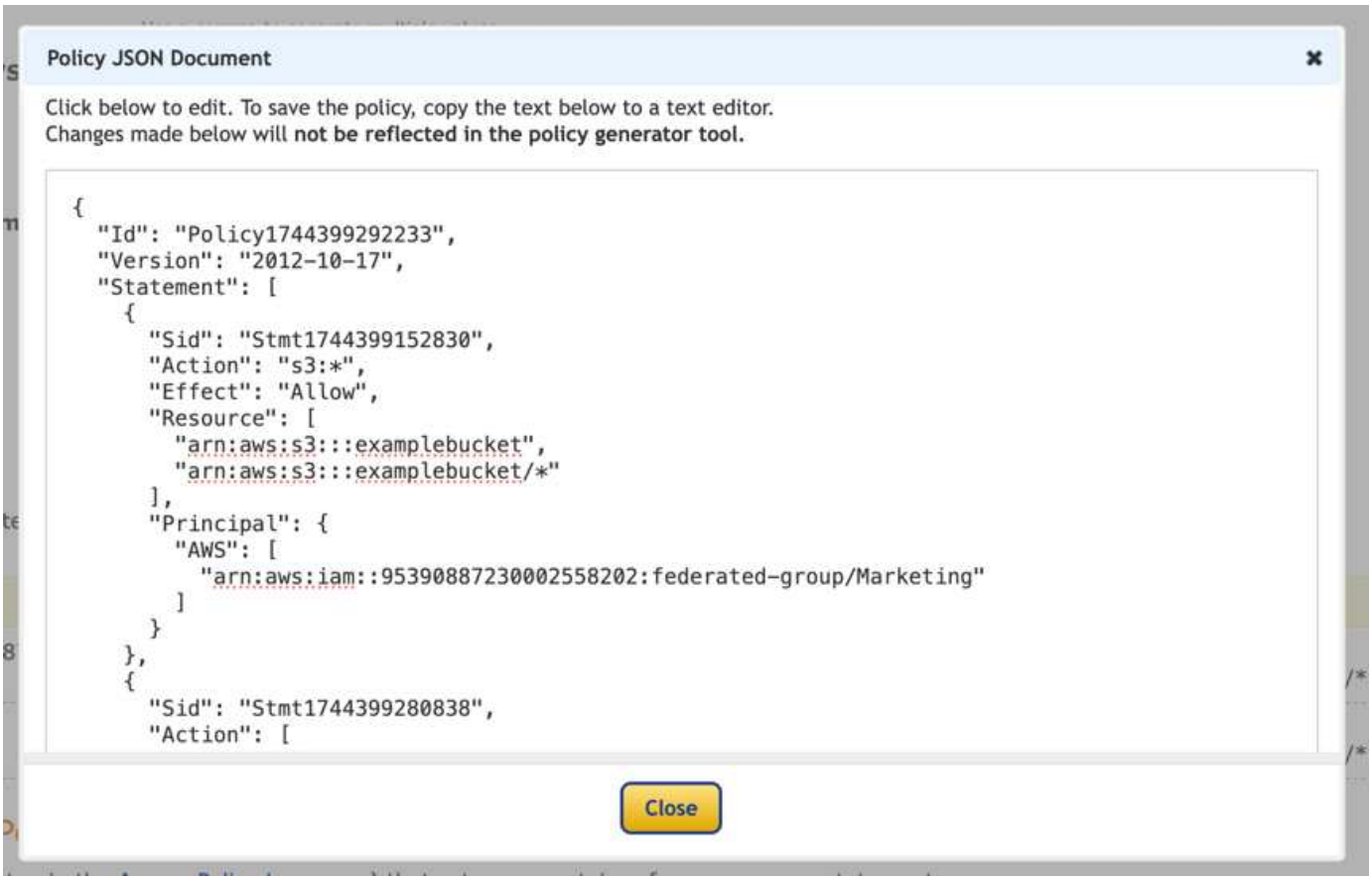


- Insira as informações do bucket - ARN:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*



- Clique no botão "Adicionar declaração"

- Clique no botão "gerar política" e uma janela pop-up aparecerá com a política gerada.



- Copie o texto json completo que deve ser assim:

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

este json pode ser usado como está, ou você pode remover as linhas ID e versão acima da linha "Statement" e você pode personalizar o Sid para cada permissão com um título mais significativo para cada permissão, ou estes podem ser removidos também.

Por exemplo:

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Políticas de grupo (IAM)

Acesso ao bucket do estilo do Home Directory

Essa política de grupo só permitirá que os usuários acessem objetos no intervalo chamado nome de usuário do usuário.

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

Negar criação de bucket de bloqueio de objetos

Esta política de grupo restringirá os usuários a criar um bucket com o bloqueio de objetos ativado no bucket.

Esta política não é aplicada na IU do StorageGRID, ela só é aplicada pela API S3.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Limite de retenção de bloqueio de objetos

Esta política de bucket restringirá a duração de retenção de bloqueio de objetos a 10 dias ou menos

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

Restrinja os usuários de excluir objetos por versionID

Esta política de grupo irá restringir os usuários de excluir objetos versionados por versionID

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Restrinja um grupo a um subdiretório único (prefixo) com acesso somente leitura

Essa diretiva permite que os membros do grupo tenham acesso somente leitura a um subdiretório (prefixo) dentro de um intervalo. O nome do intervalo é "estudo" e o subdiretório é "study01".

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3::: study"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

Políticas do bucket

Restrinja o bucket a um único usuário com acesso somente leitura

Essa política permite que um único usuário tenha acesso somente leitura a um bucket e explicitamente o acesso da denys a todos os outros usuários. Agrupar as declarações deny no topo da política é uma boa prática para uma avaliação mais rápida.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

restrinja um intervalo a alguns usuários com acesso somente leitura.

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

Restrinja as exclusões do usuário de objetos versionados em um bucket

Esta política de bucket irá restringir um usuário(identificado pelo UserId "56622399308951294926") de excluir objetos versionados por versionID

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

Ciclo de vida do bucket no StorageGRID

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos específicos são excluídos do sistema StorageGRID.

O que é uma configuração de ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras que são aplicadas aos objetos em buckets específicos do S3. Cada regra especifica quais objetos são afetados e quando esses objetos expirarão (em uma data específica ou após algum número de dias).

Cada objeto segue as configurações de retenção de um ciclo de vida do bucket do S3 ou de uma política de ILM. Quando um ciclo de vida do bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política ILM para objetos que correspondam ao filtro do ciclo de vida do bucket. Os objetos que não correspondem ao filtro do ciclo de vida do bucket usam as configurações de retenção da política ILM. Se

um objeto corresponder a um filtro do ciclo de vida do bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e está implícito que as versões do objeto serão mantidas para sempre.

Como resultado, um objeto pode ser removido da grade, mesmo que as instruções de colocação em uma regra ILM ainda se apliquem ao objeto. Ou um objeto pode ser retido na grade mesmo depois que quaisquer instruções de posicionamento do ILM para o objeto tenham expirado

O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:

- Expiração: Exclua um objeto quando uma data especificada é atingida ou quando um número especificado de dias é atingido, a partir de quando o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclua um objeto quando um número especificado de dias é atingido, a partir de quando o objeto se tornou inatual.
- Filtro (prefixo, Tag)
- Status *ID

O StorageGRID dá suporte ao uso das seguintes operações de bucket para gerenciar configurações do ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Estrutura de uma política de ciclo de vida

Como primeira etapa na criação de uma configuração de ciclo de vida, você cria um arquivo JSON que inclui uma ou mais regras. Por exemplo, este arquivo JSON inclui três regras, como segue:

1. A **Regra 1** aplica-se apenas a objetos que correspondem ao prefixo category1/ e que têm um valor key2 de tag2. O parâmetro Expiration especifica que os objetos que correspondem ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A **Regra 2** se aplica apenas a objetos que correspondem ao prefixo category2/. O parâmetro Expiration especifica que os objetos que correspondem ao filtro expirarão 100 dias após serem ingeridos.

   > As regras que especificam um número de dias são relativas a quando o objeto foi ingerido. Se a data atual exceder a data de ingestão mais o número de dias, alguns objetos podem ser removidos do intervalo assim que a configuração do ciclo de vida for aplicada.

3. A **Regra 3** se aplica somente a objetos que correspondem ao prefixo category3/. O parâmetro Expiration especifica que quaisquer versões desatualizadas de objetos correspondentes expirarão 50 dias após se tornarem desatualizadas.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplique a configuração do ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, você o aplica a um bucket emitindo uma solicitação PutBucketLifecycleConfiguration.

Essa solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket `testbucket` chamado .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação GetBucketLifecycleConfiguration. Por exemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Exemplo de políticas de ciclo de vida para buckets padrão (sem versão)

Excluir objetos após 90 dias

Caso de uso: Esta política é ideal para gerenciar dados relevantes apenas por um tempo limitado, como arquivos temporários, logs ou dados de processamento intermediário. Benefício: Reduz os custos de armazenamento e garante que o bucket esteja organizado.

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

Exemplo de políticas de ciclo de vida para buckets versionados

Excluir versões não atuais após 10 dias

Caso de uso: Esta política ajuda a gerenciar o armazenamento de objetos de versão desatualizada, que podem se acumular ao longo do tempo e consumir espaço significativo. Benefício: Otimize o uso do

armazenamento mantendo apenas a versão mais recente.

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

Mantenha 5 versões não atuais

Caso de uso: Útil quando você deseja manter um número limitado de versões anteriores para fins de recuperação ou auditoria. Benefício: Manter versões não atuais suficientes para garantir histórico e pontos de recuperação suficientes.

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

Remover marcadores de exclusão quando não houver outras versões

Caso de uso: Esta política ajuda a gerenciar os marcadores de exclusão restantes após a remoção de todas as versões não atuais, que podem se acumular ao longo do tempo. Benefício: Reduz a desordem desnecessária.

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

Exclua as versões atuais após 30 dias, exclua as versões não atuais após 60 dias e remova os marcadores de exclusão criados pela exclusão da versão atual quando não houver mais outras versões.

Caso de uso: Fornecer um ciclo de vida completo para versões atuais e não atuais, incluindo os marcadores de exclusão. Benefício: Reduzir os custos de armazenamento e garantir que o bucket esteja organizado, mantendo pontos de recuperação e histórico suficientes.

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      },
    },
    {
      "ID": "noncurrent version retention",
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

remova marcadores de exclusão que não tenham outras versões e existam há 5 dias, mantenha 4 versões não atuais e pelo menos 30 dias de histórico para objetos com o prefixo "accounts_" e mantenha 2 versões e pelo menos 10 dias de histórico para todas as outras versões de objetos.

Caso de uso: Forneça regras exclusivas para objetos específicos, juntamente com outros objetos, para gerenciar o ciclo de vida completo das versões atuais e não atuais, incluindo os marcadores de exclusão. Benefício: Reduza os custos de armazenamento e garanta que o bucket esteja organizado, mantendo pontos de recuperação e histórico suficientes para atender a uma variedade de requisitos do cliente.

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Status": "Enabled",
      "Expiration": {
        "Days": 5,
        "ExpiredObjectDeleteMarker": true
      },
    },
    {
      "ID": "accounts version retention",
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      },
      "Filter": {
          "Prefix":"account_"
      }
    },
    {
      "ID": "noncurrent version retention",
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

Conclusão

- Revise e atualize regularmente as políticas de ciclo de vida e alinhe-as com as metas de ILM e gerenciamento de dados.
- Teste as políticas em um ambiente ou bucket não produtivo antes de aplicá-las amplamente para garantir que funcionem conforme o esperado
- Use IDs descritivos para regras para torná-las mais intuitivas, pois a estrutura lógica pode ficar complexa
- Monitore o impacto dessas políticas de ciclo de vida do bucket no uso e no desempenho do armazenamento para fazer os ajustes necessários.

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

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.

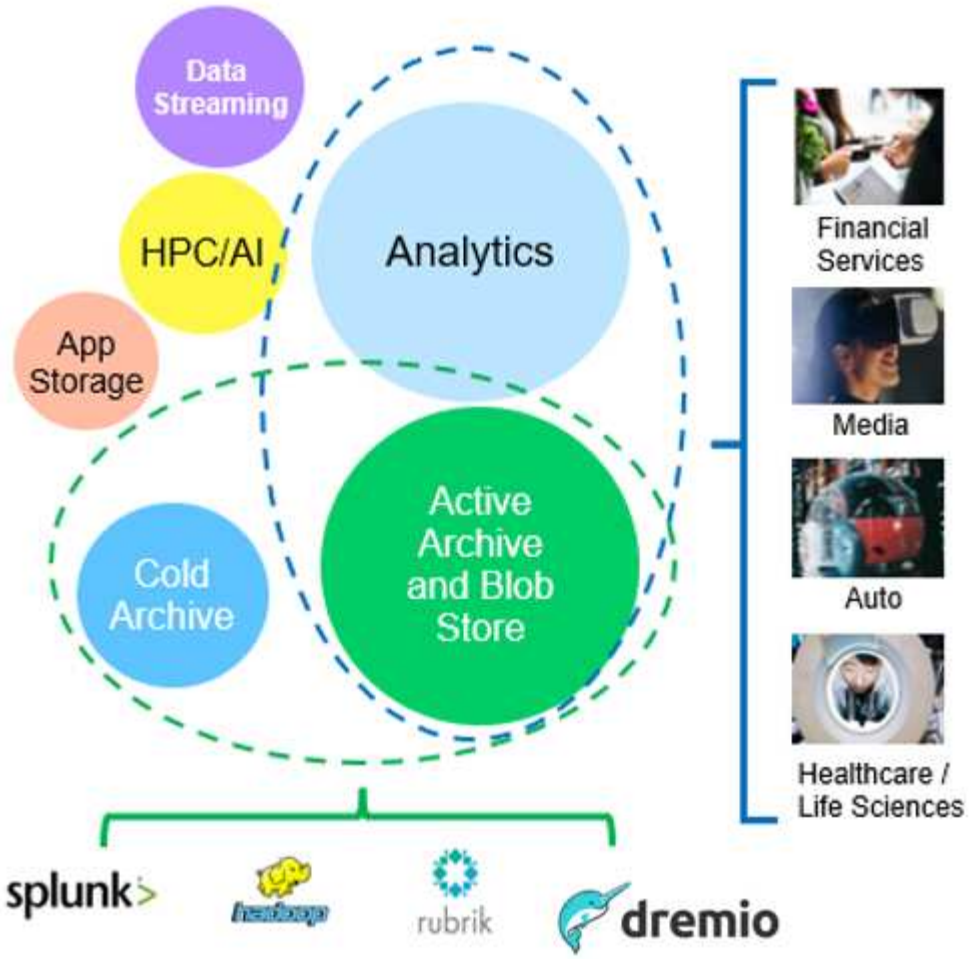
Backup de dados e recuperação de desastres: as empresas podem usar o StorageGRID S3 como uma solução confiável e econômica para fazer backup de dados críticos e recuperá-los em caso de desastre.

- 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

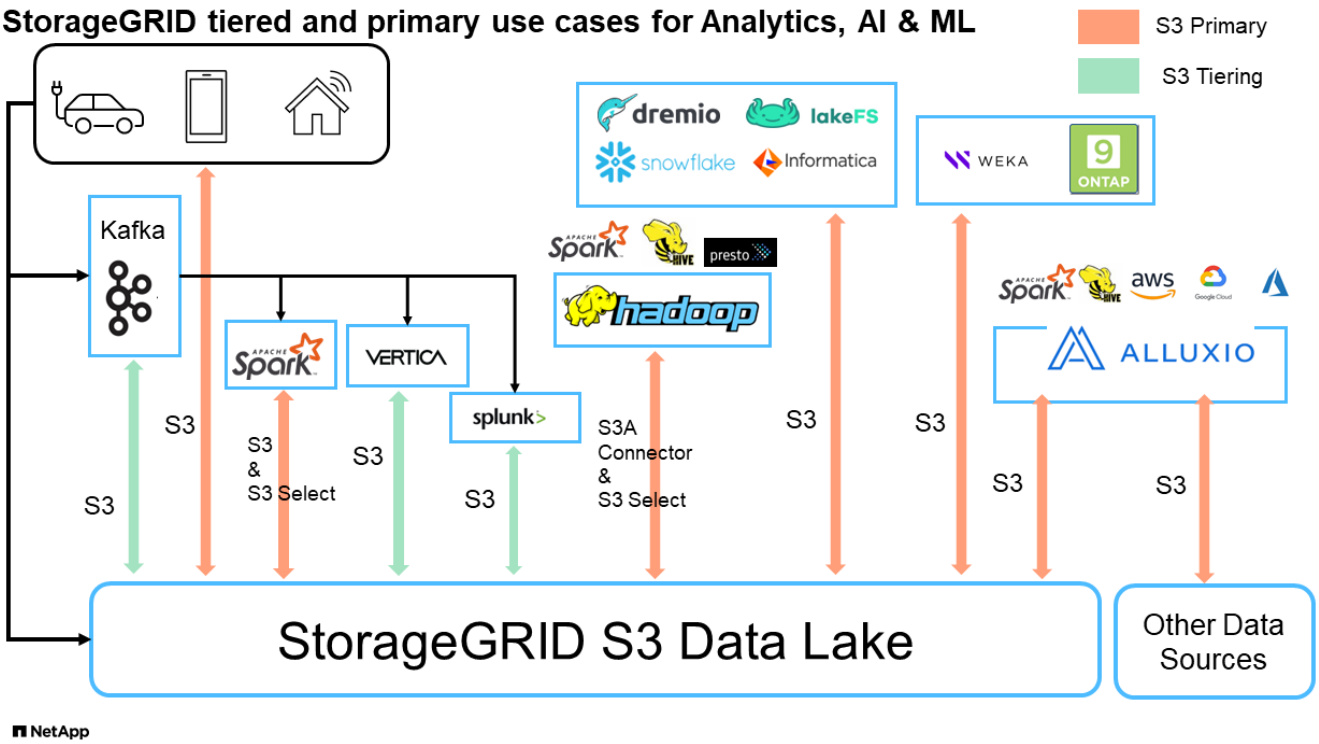


Entre as opções acima, o Big Data Analytics é um dos principais casos de uso e seu uso está em alta.

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 v25,2 (1 coordenador e 5 executores)
  - Trino v438 (1 coordenador e 5 trabalhadores)
  - Starburst v453 (1 coordenador 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	36	32	28
S3 pedidos de divisão	OBTER	1.117.184	2.074.610	3.939.690	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, 2500 - 3000 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	120	509
512	CABEÇA (objeto inexistente)	156.027	12.103	96	0
0	CABEÇA (objeto existente)	982.126	922.732	0	0
0	Total de solicitações	2.567.390	3.033.603	3.939,906	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)	22	28	22
TPCDS 99 consultas e total de minutos 2 (cache ativado)	16	28	21,5
S3 pedidos de divisão	Obter (cache desativado)	1.985.922	938.639
931.582	Obter (cache ativado)	611.347	30.158
3.281	Observação: Toda a gama GANHA	Alcance obter tamanho: 67% 1MB, 15% 100KB, 10% 500KB, 3500 - 4500 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	1465	0
0	CABEÇA (objeto inexistente)	1464	0
0	CABEÇA (objeto existente)	3.702	509
509	Total de solicitações (cache desativado)	1.992.553	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 200GB LUN para tabelas de nó Admin 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 .

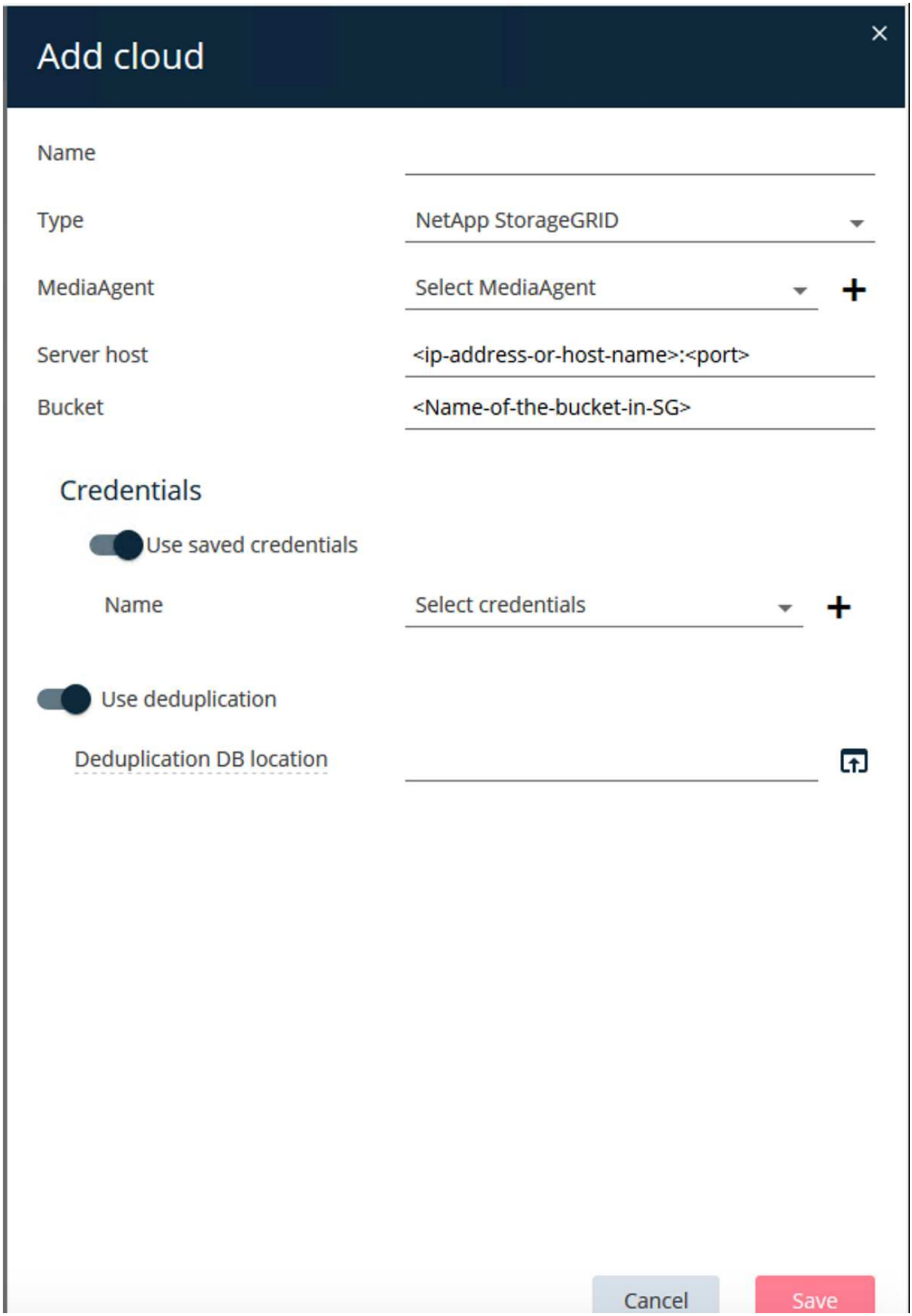
Execute um trabalho de proteção de dados

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.

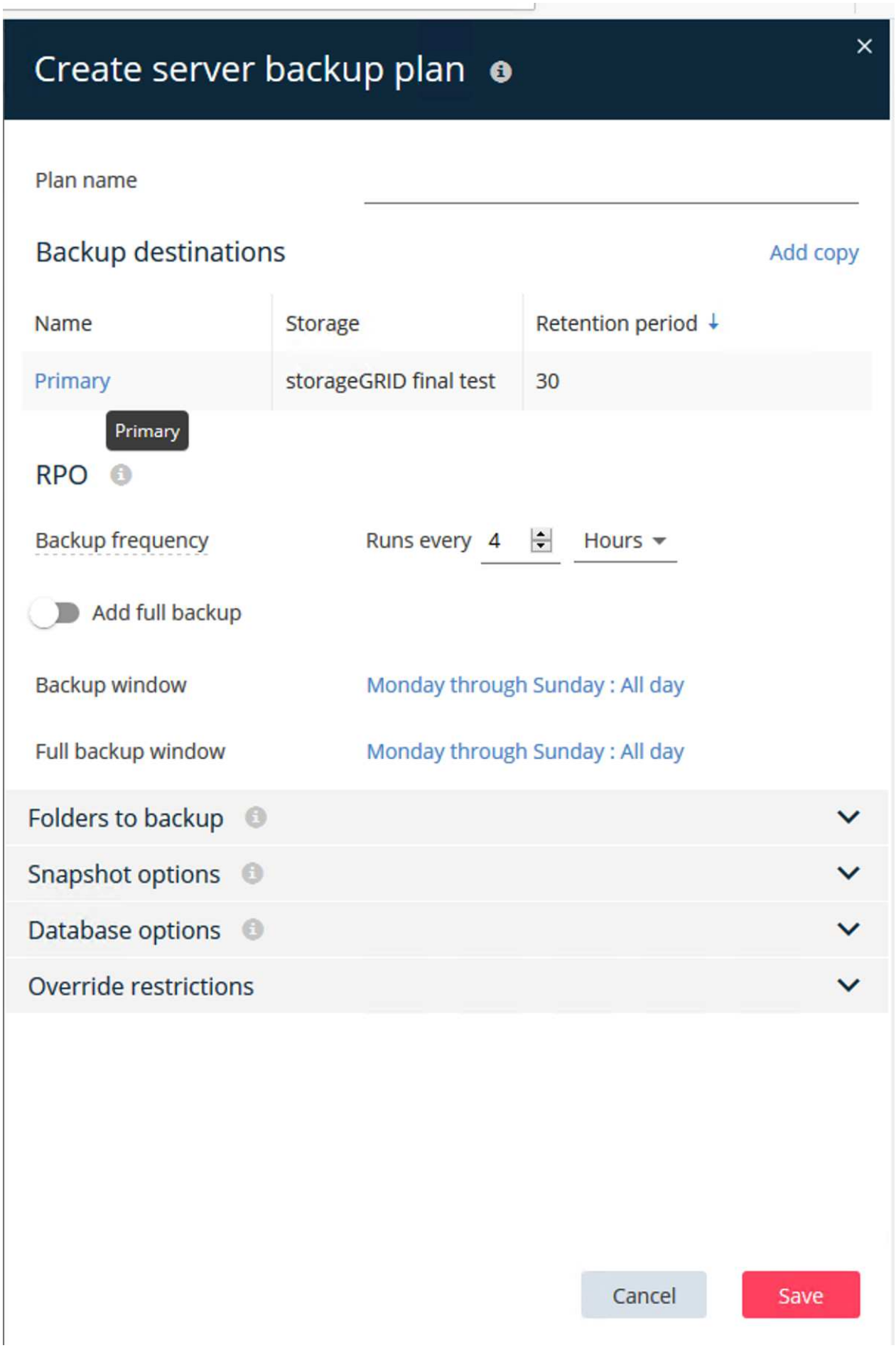
   Siga as etapas na documentação do StorageGRID no "como configurar um ponto de extremidade do balanceador de carga (porta)". Certifique-se de que tem uma porta HTTPS com um certificado auto-assinado e o endereço IP ou o nome de domínio do endpoint StorageGRID.

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.

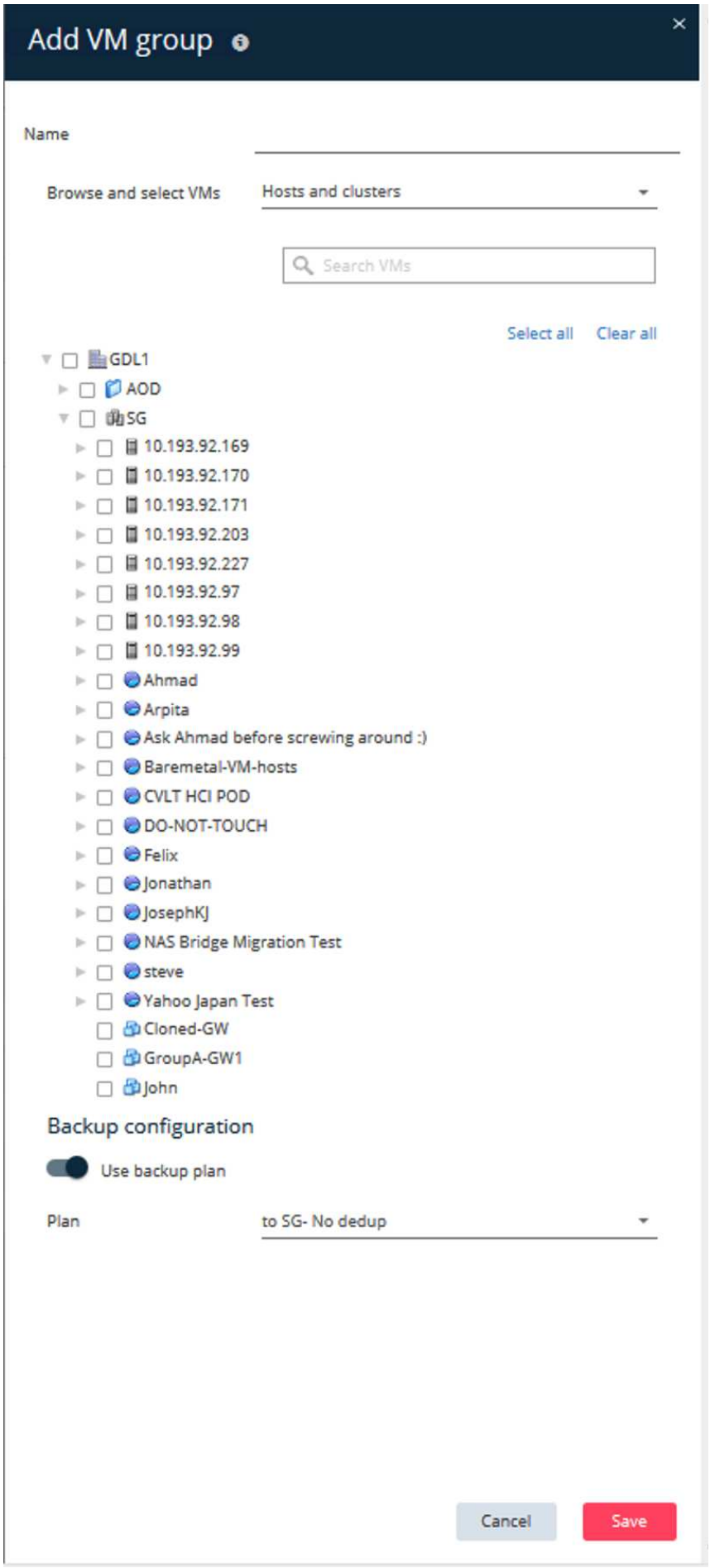

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to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

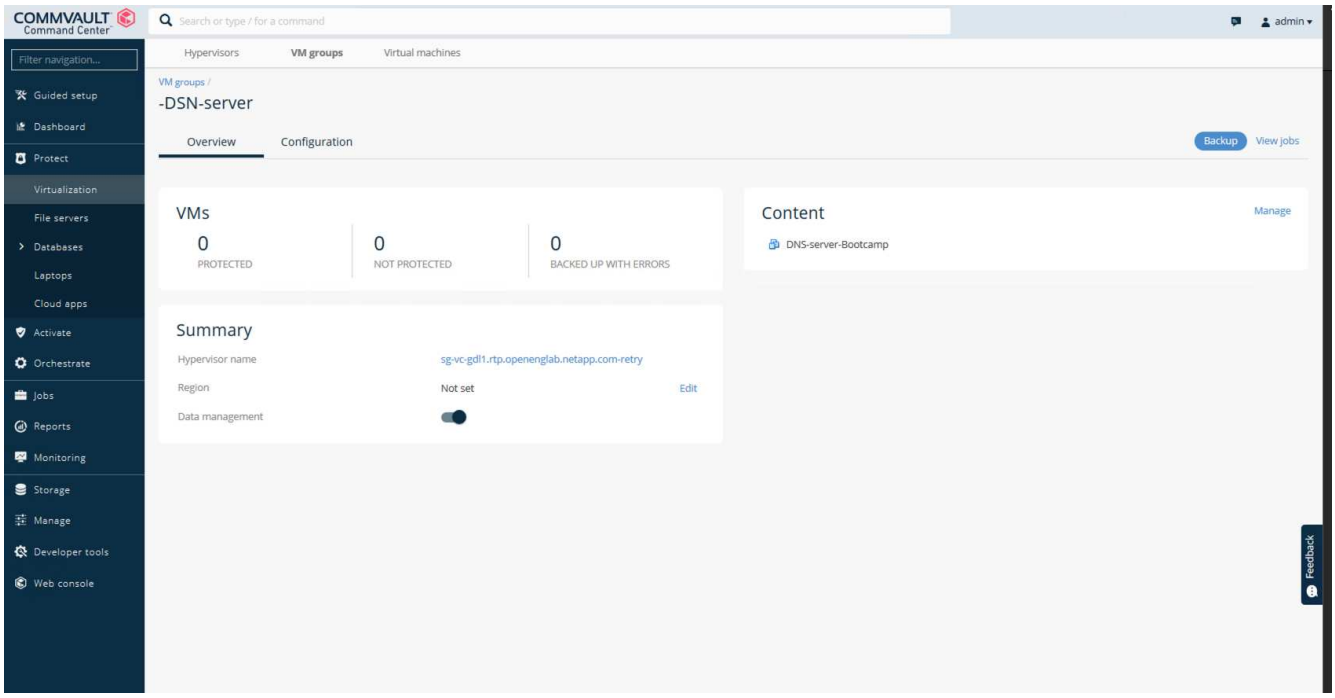
Etapa 3: Inicie um trabalho de backup para proteger suas cargas de trabalho

Passos

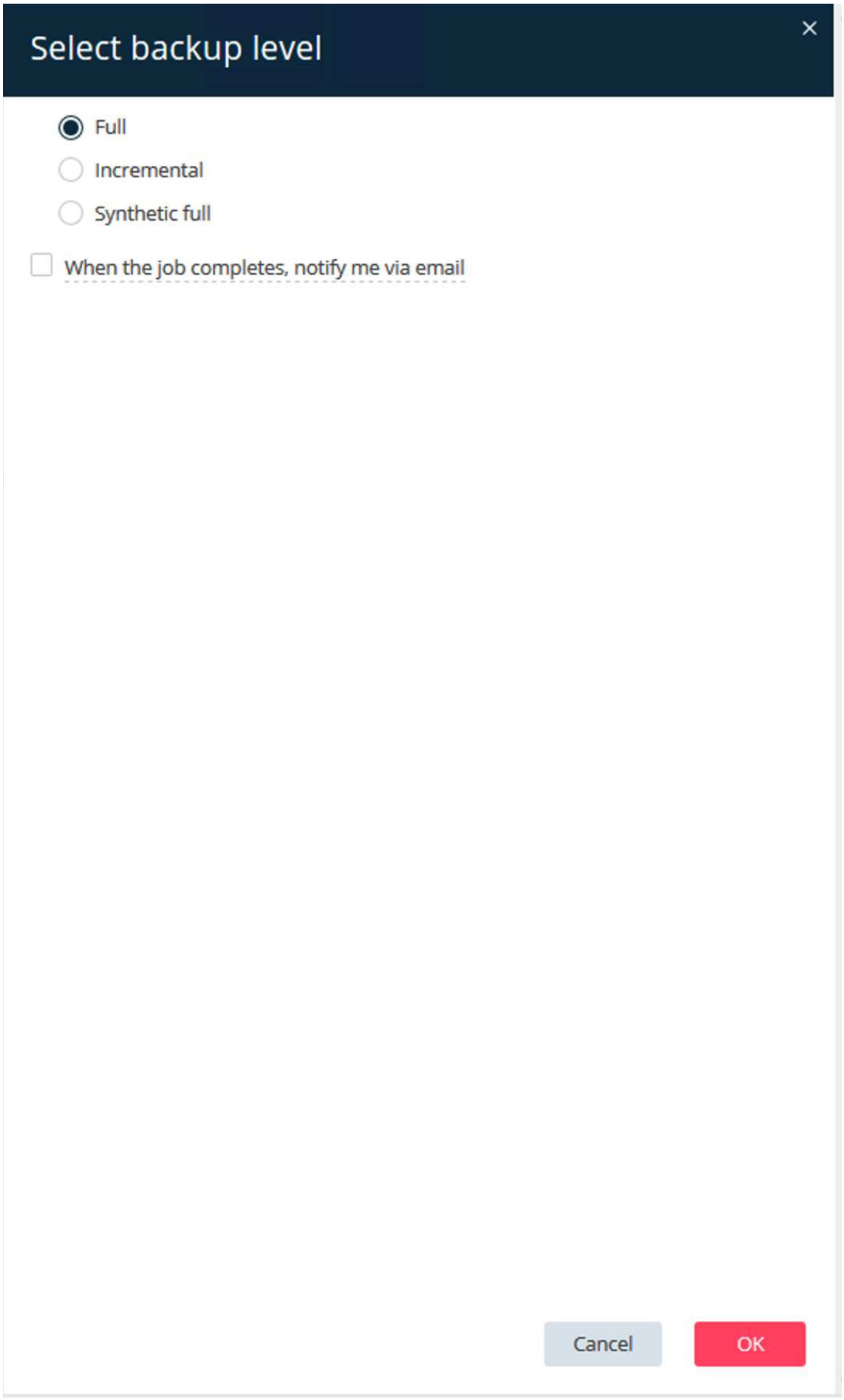
1. No CommVault Command Center, navegue para proteger > virtualização.
2. Adicione um hypervisor do VMware vCenter Server.
3. Clique no hypervisor que você acabou de adicionar.
4. Clique em Adicionar grupo VM para responder à caixa de diálogo Adicionar grupo VM para que você possa ver o ambiente do vCenter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

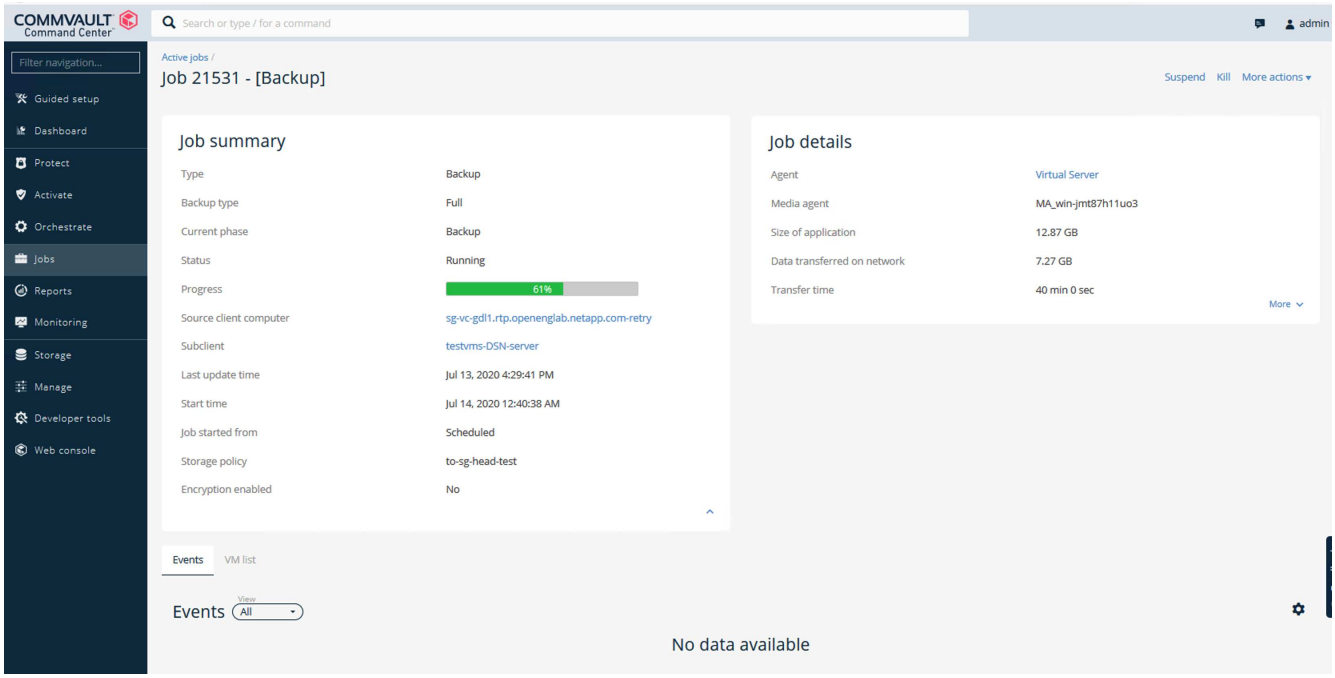
5. Selecione um datastore, uma VM ou uma coleção de VMs e insira um nome para ele.
6. Selecione o plano de cópia de segurança que criou na tarefa anterior.
7. Clique em Salvar para ver o grupo de VM que você criou.
8. No canto superior direito da janela do grupo VM, selecione Backup:



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.

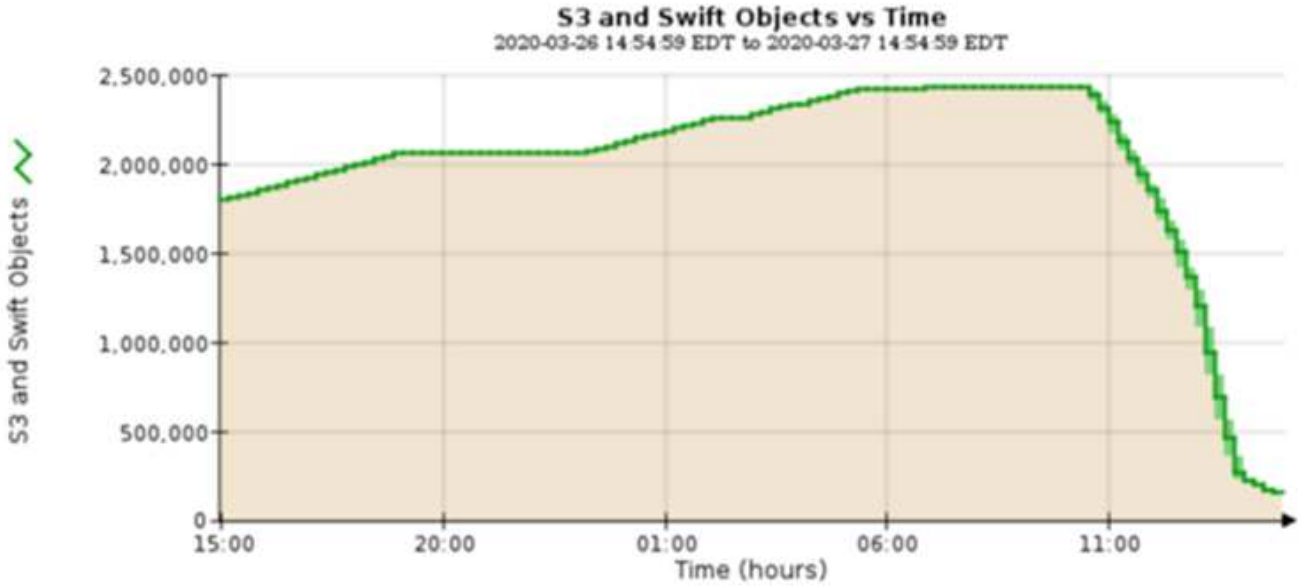
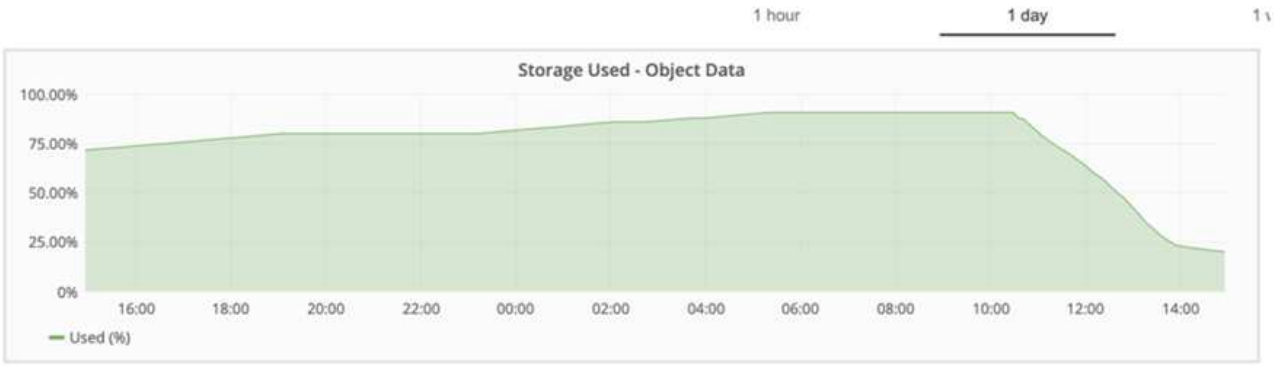


Figura 2: Liberando 80TB TB de storage em menos de 3 horas.



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.

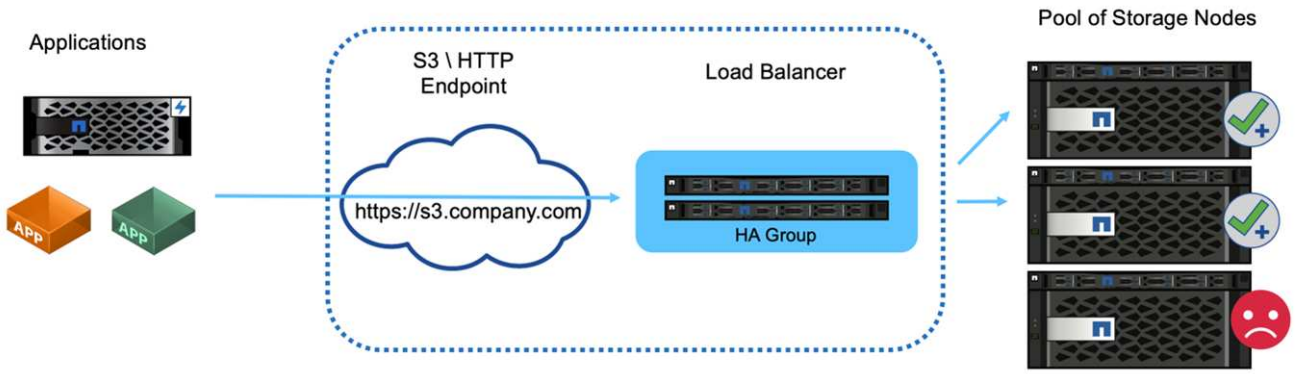
Storage de objetos é sinônimo do termo storage de nuvem e, como seria de esperar, aplicações que utilizam o storage de nuvem abordam esse storage por meio de um URL. Por trás desse URL simples, o StorageGRID pode dimensionar a capacidade, a performance e a durabilidade em um único local ou em locais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

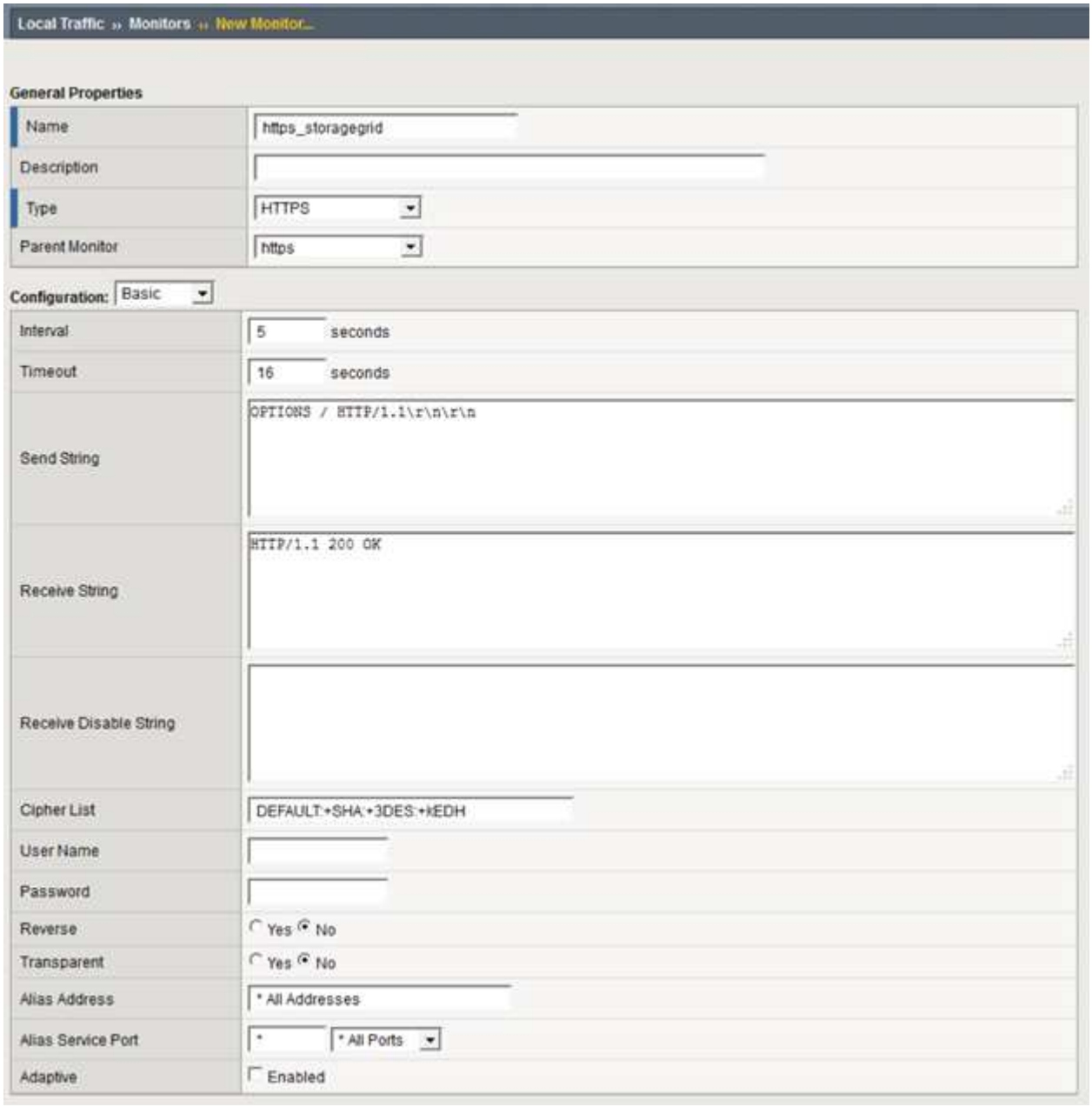
Para configurar o monitor de verificação de integridade do gerenciador de tráfego local F5 BIG-IP, siga estas etapas:

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`.



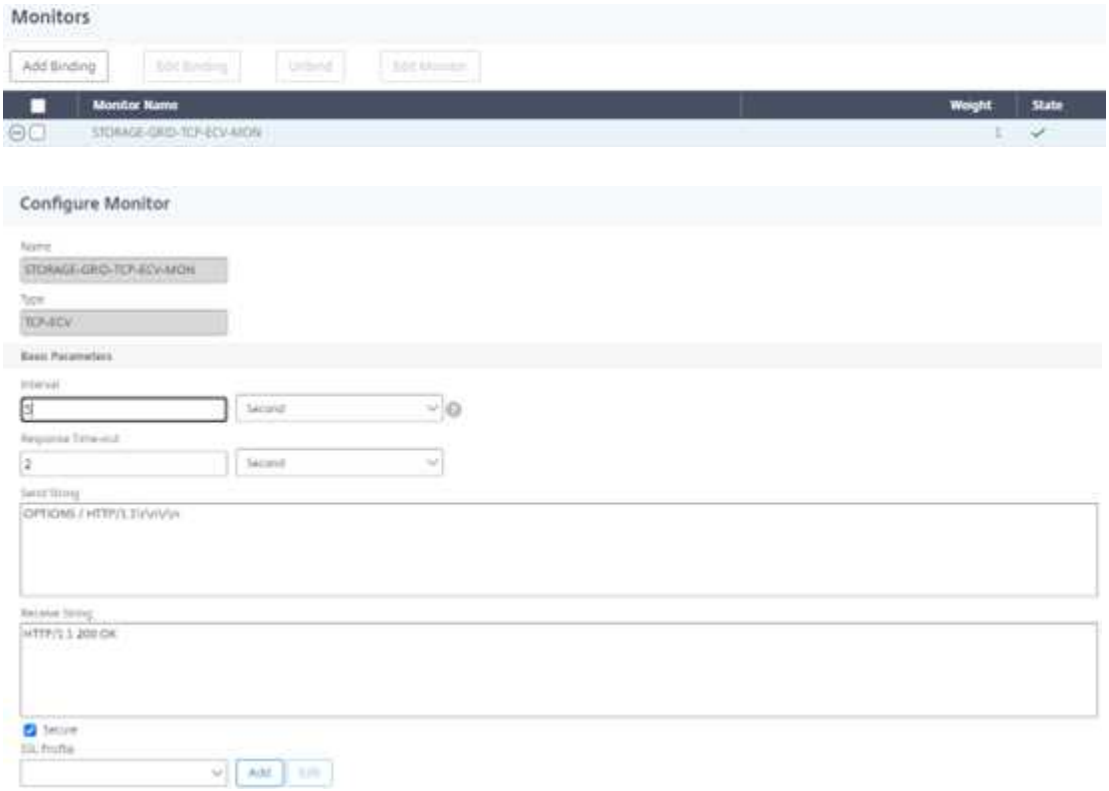
2. Em criar pool, crie um pool para cada porta necessária.
   a. Atribua o monitor de integridade que você criou na etapa anterior.
   b. Selecione um método de balanceamento de carga.
   c. Selecione a porta de serviço: 18082 (S3).
   d. Adicionar nós.

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.

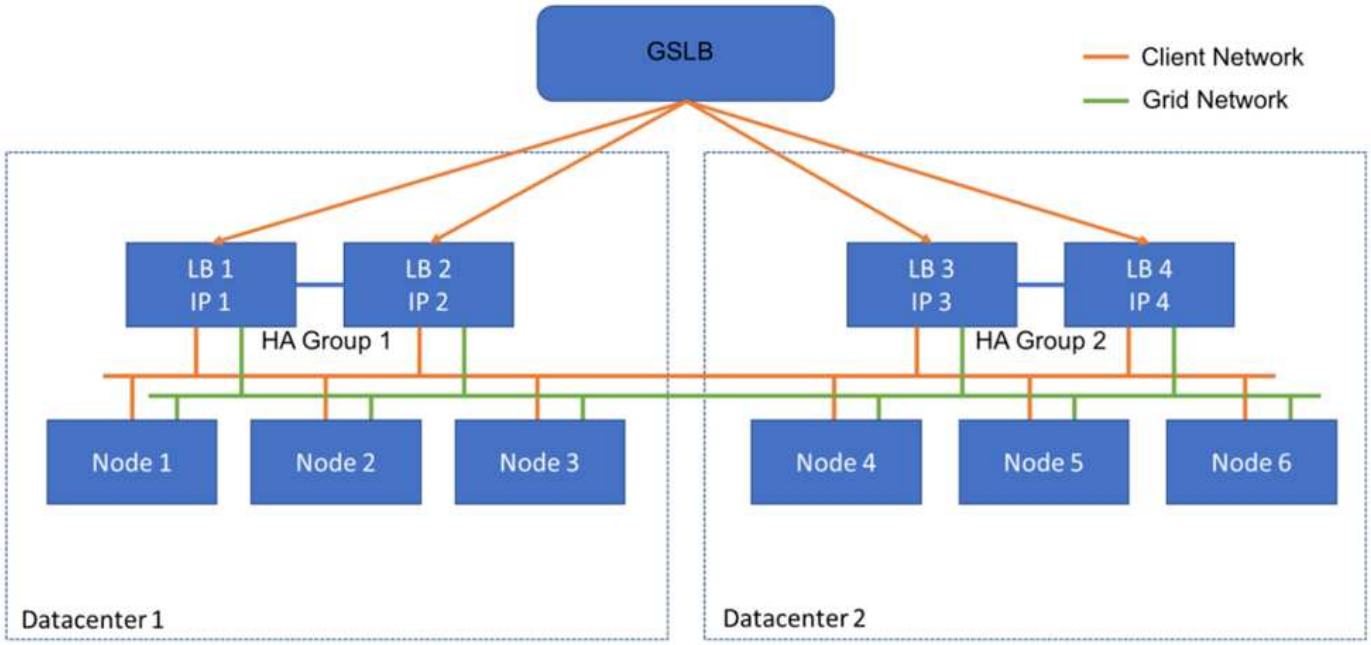
Depois que o balanceador de carga estiver configurado, você deverá validar a conexão usando ferramentas como OpenSSL e AWS CLI. Outros aplicativos, como o navegador S3, podem ignorar a configuração incorreta do SSL.

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/
- 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
LDAP	Lightweight Directory Access Protocol

Termo ou acrônimo	Definição
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. O StorageGRID suporta os seguintes conjuntos de codificação para TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 Suporte para TLS v1,2 e 1,3. 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. 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. 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. 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: • Mensagens de auditoria do sistema • Mensagens de auditoria de armazenamento de objetos • Mensagens de auditoria do protocolo HTTP • 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. A autenticação do usuário de quem enviou a unidade de dados do protocolo é fornecida pelo protocolo de autenticação HMAC-SHA ou HMAC-MD5. 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/
- 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.

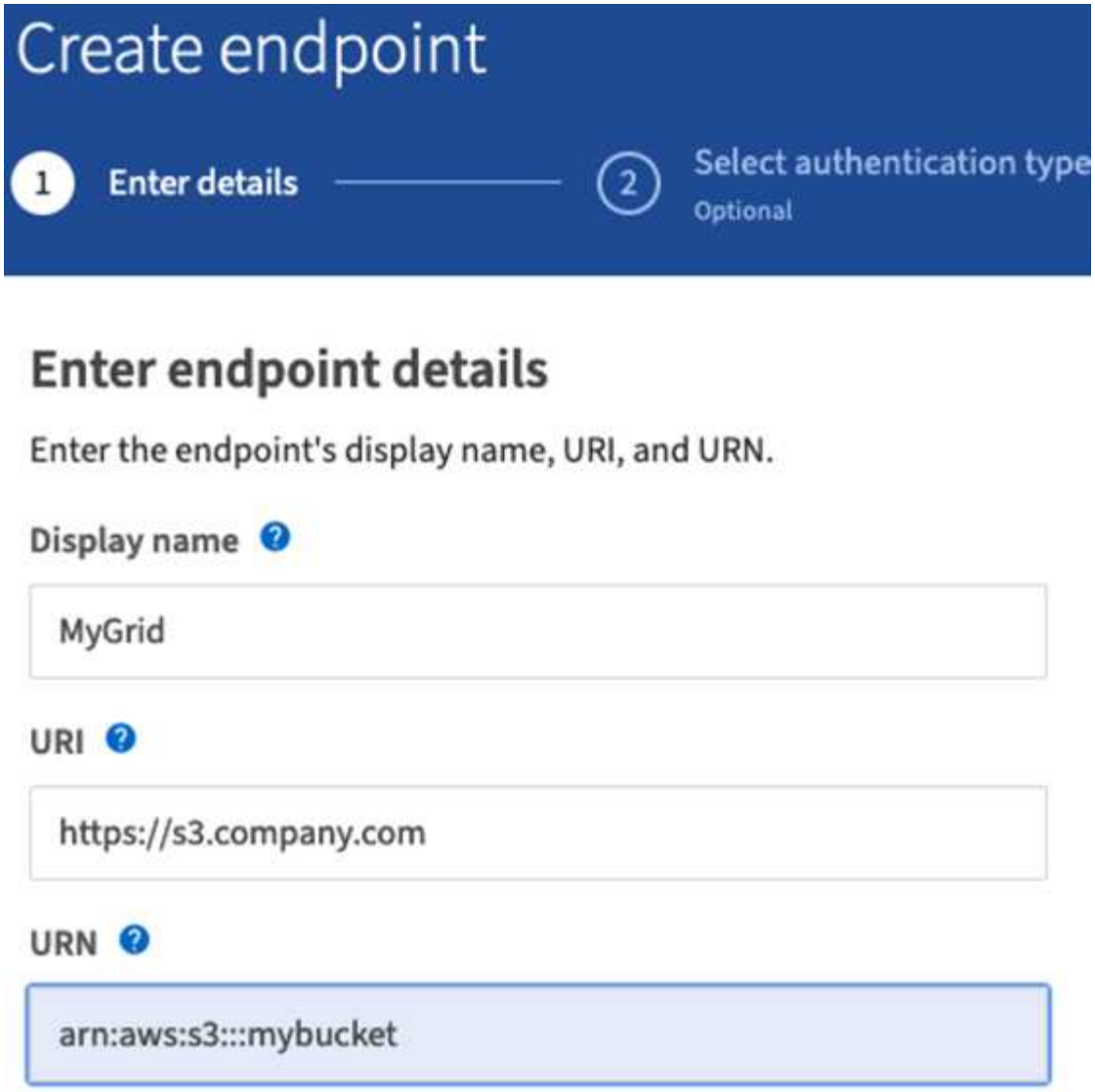
O StorageGRID CloudMirror é um componente do StorageGRID que pode ser configurado para replicar os objetos de um bucket para um destino definido à medida que são ingeridos no bucket de origem e não replica exclusões. Como o CloudMirror é um componente integrado do StorageGRID, ele não pode ser desativado 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

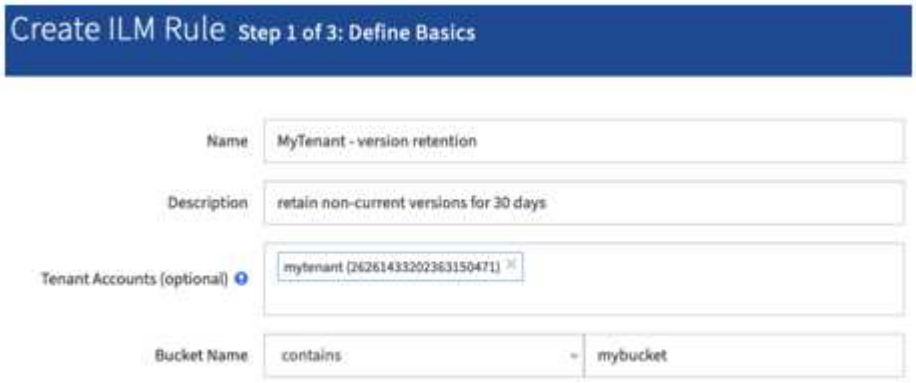
1. Para configurar o CloudMirror, crie um endpoint de serviços de plataforma para o destino S3.

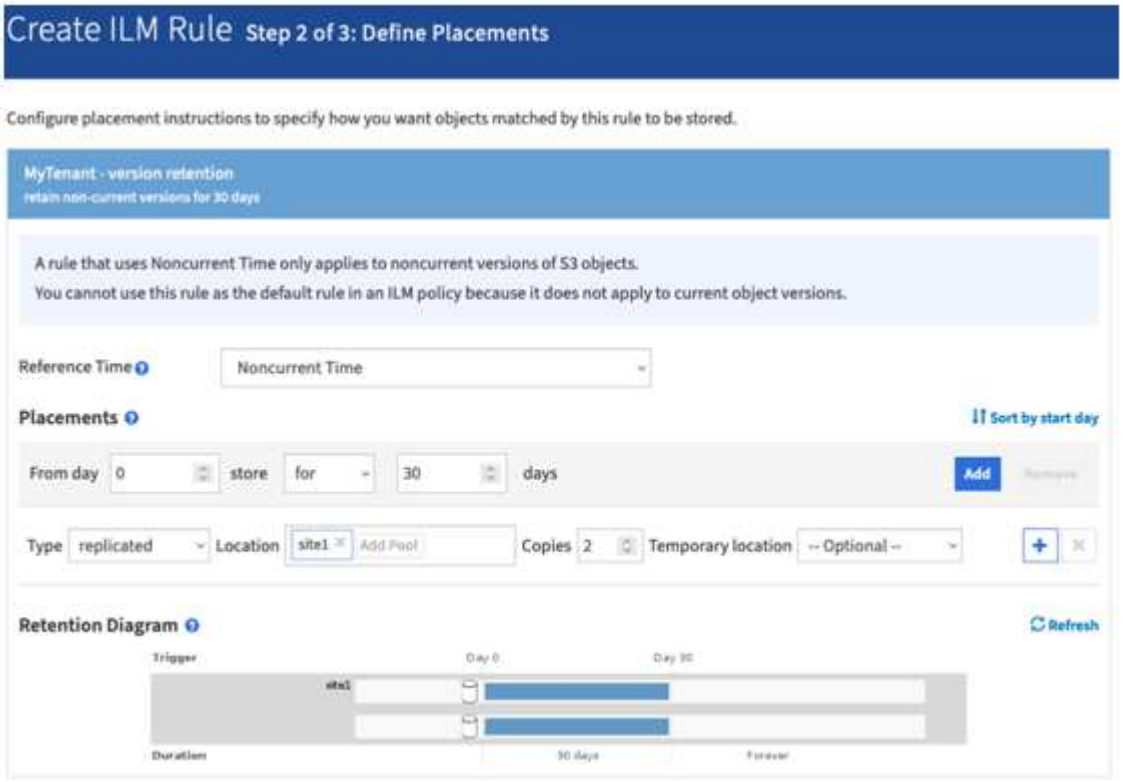


2. No intervalo de origem, configure a replicação para usar o ponto de extremidade configurado.

```
<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.

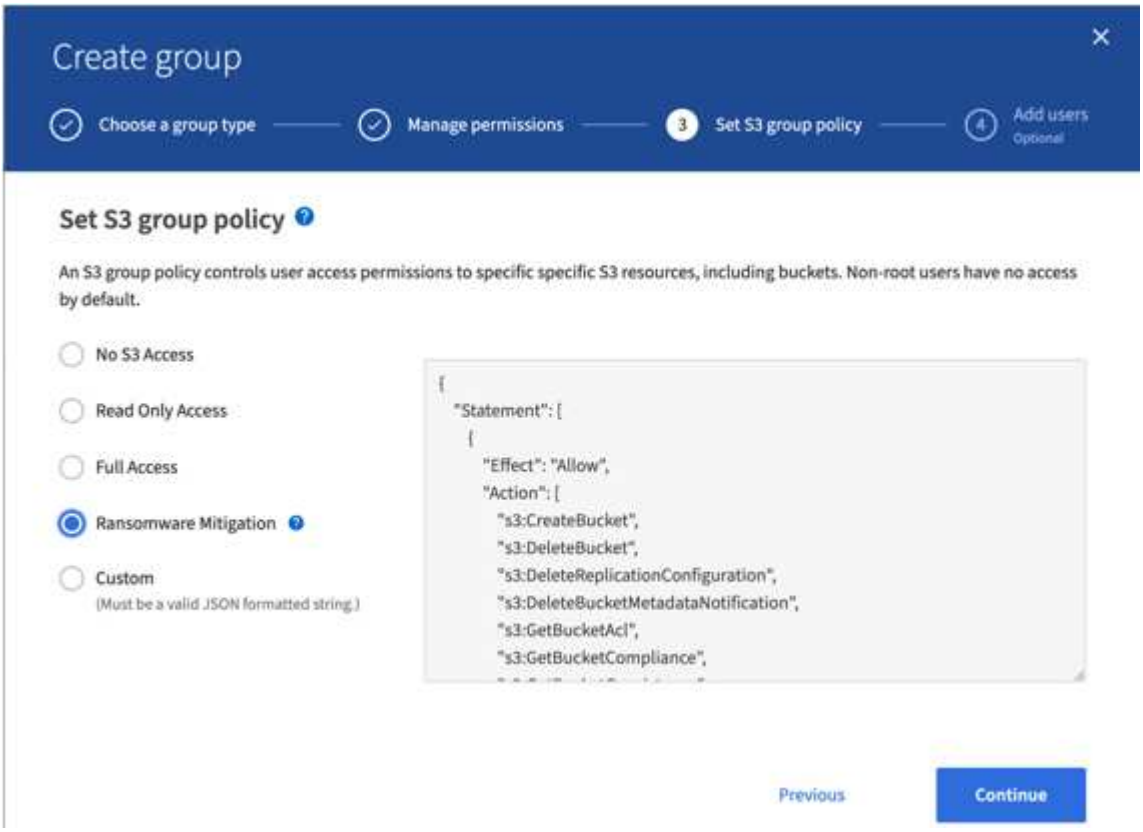
Defesa contra ransomware usando o controle de versão com a política protetora do IAM

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

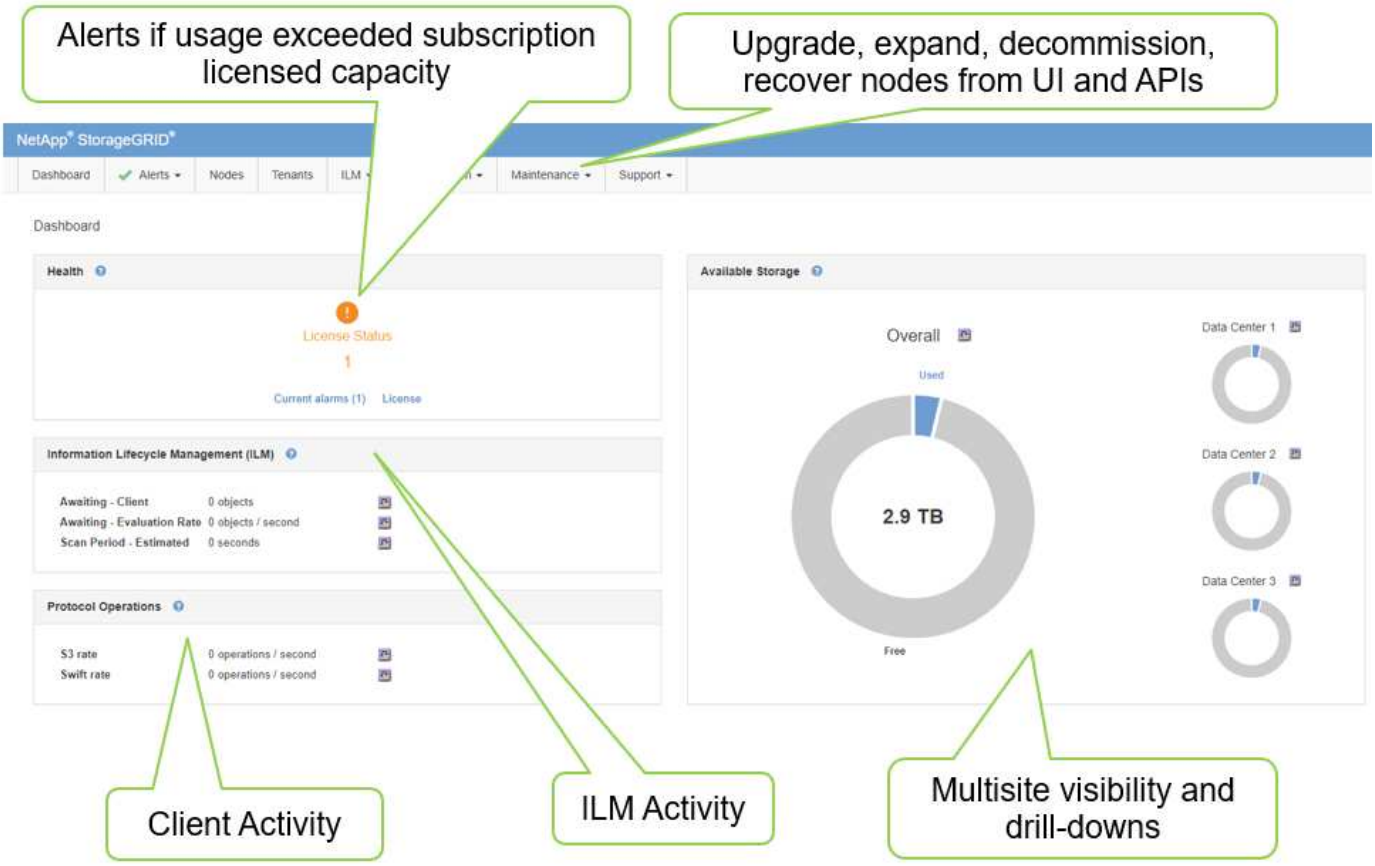
Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- 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/
- 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.

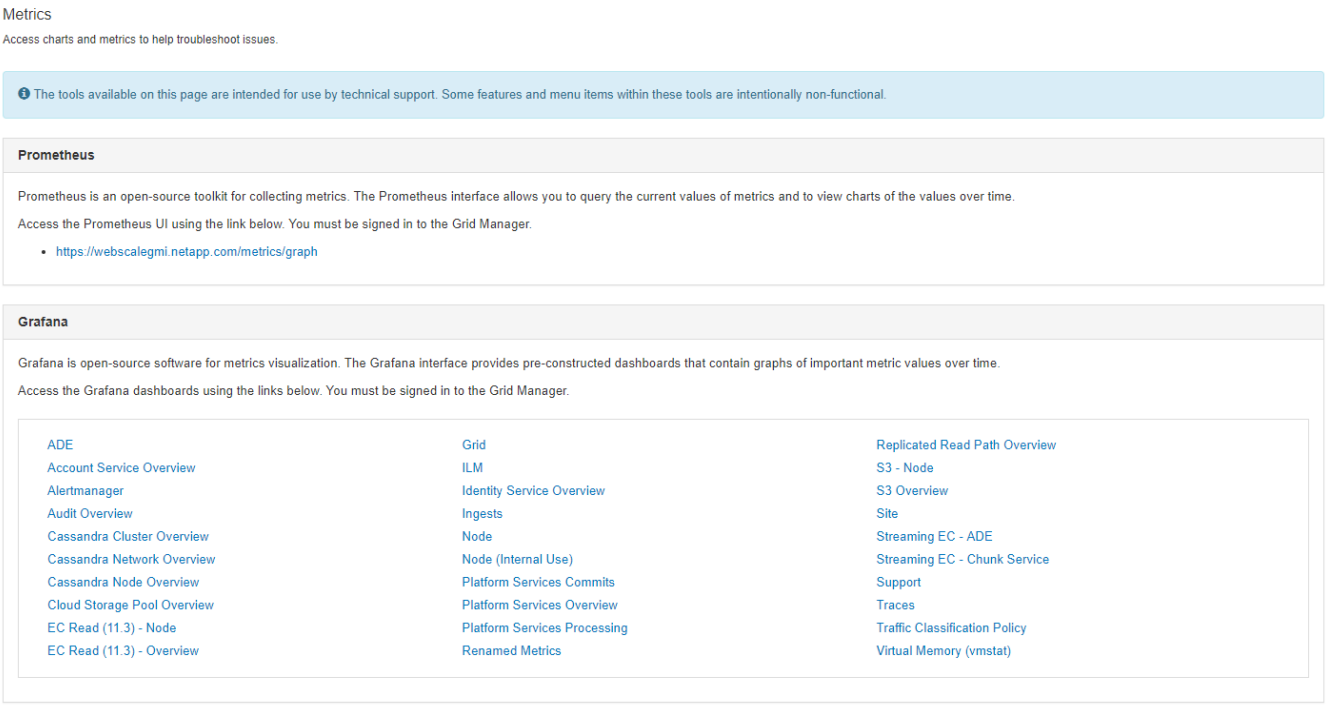
Para obter mais informações sobre alertas, consulte o "documentação do produto" disponível on-line e em formato PDF.

Monitoramento avançado em StorageGRID

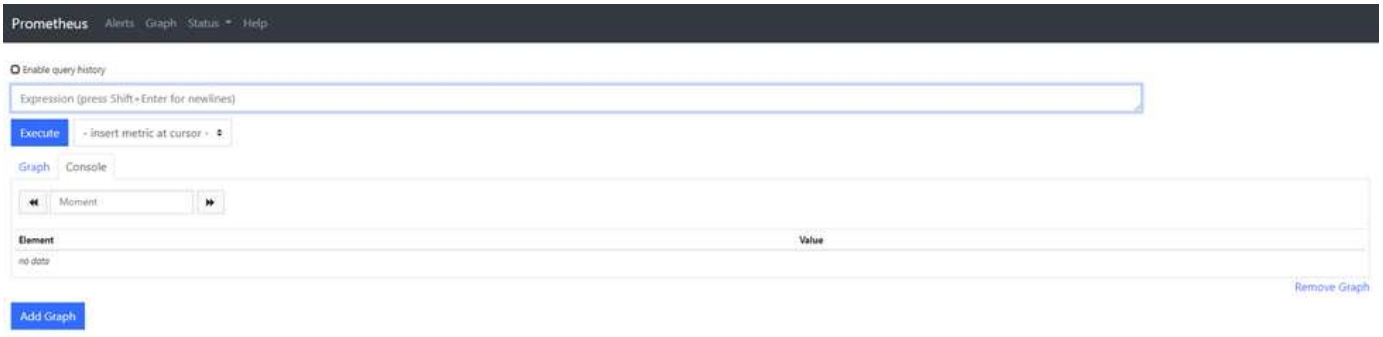
Saiba como acessar e exportar métricas para ajudar a solucionar problemas.

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.



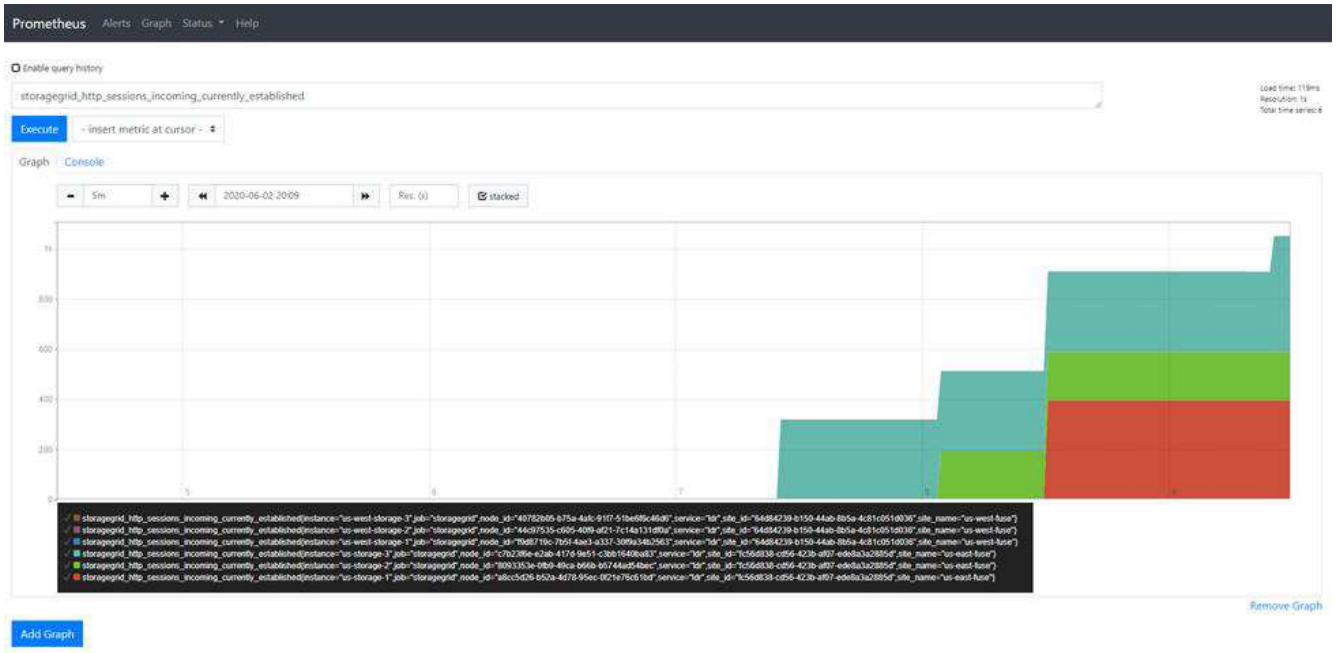
Com essa visualização, você pode acessar a interface Prometheus. A partir daí, você pode pesquisar as

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.

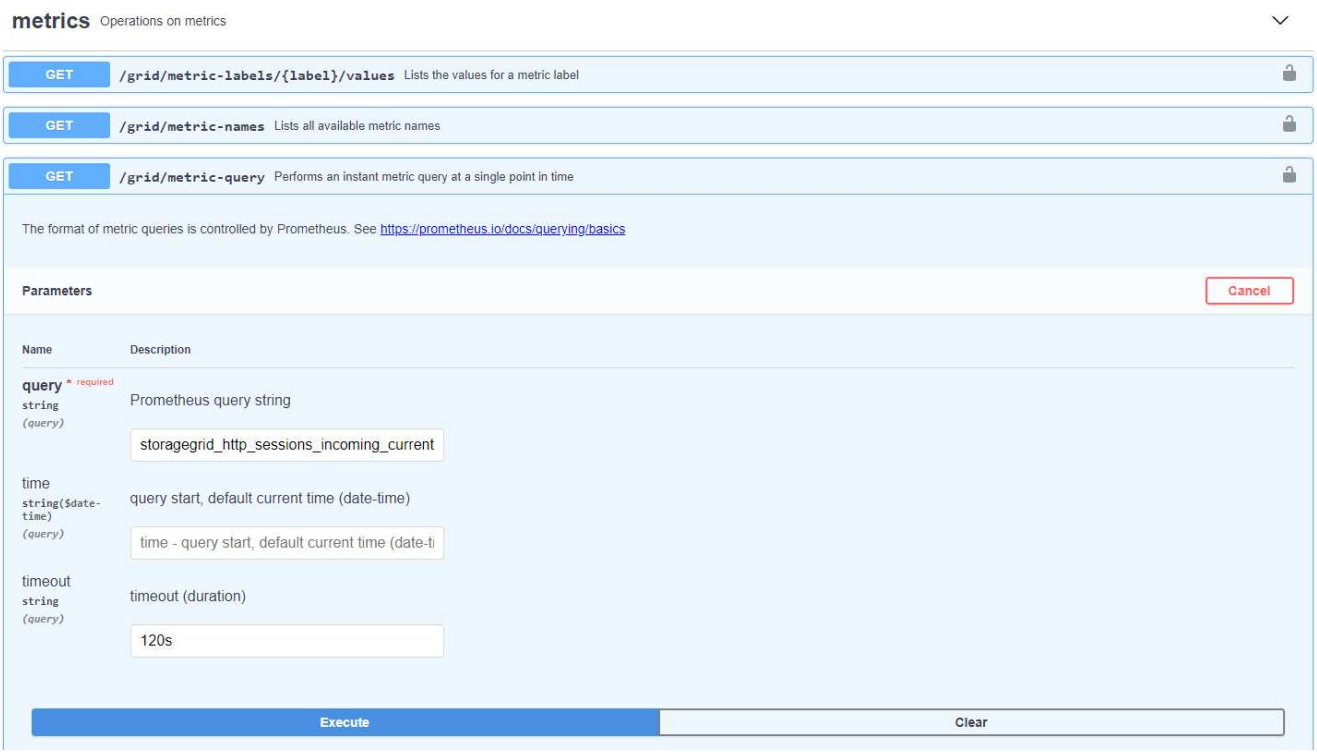
Não é recomendado fazer uma interface direta com nossa instância Prometheus porque isso requer a abertura de portas adicionais. Acessar métricas por meio de nossa API é o método recomendado e seguro.

Exportar métricas por meio da API

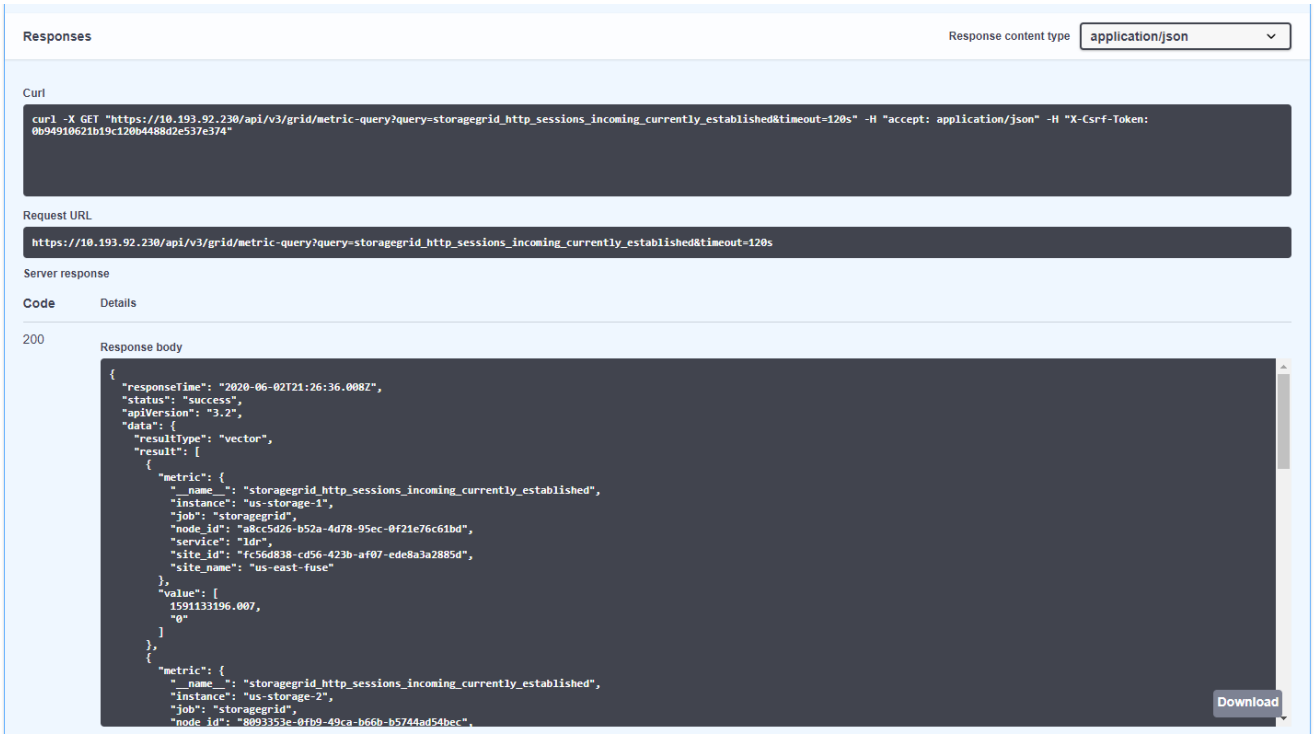
Você também pode acessar os mesmos dados por meio da API de gerenciamento do StorageGRID.

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

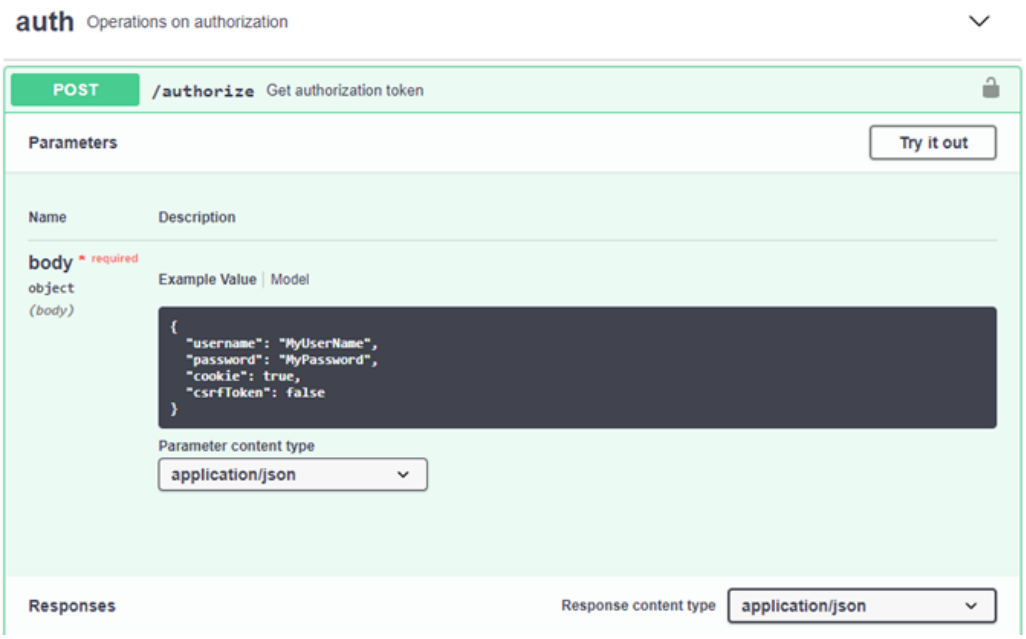
Acesse métricas usando curl no StorageGRID

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

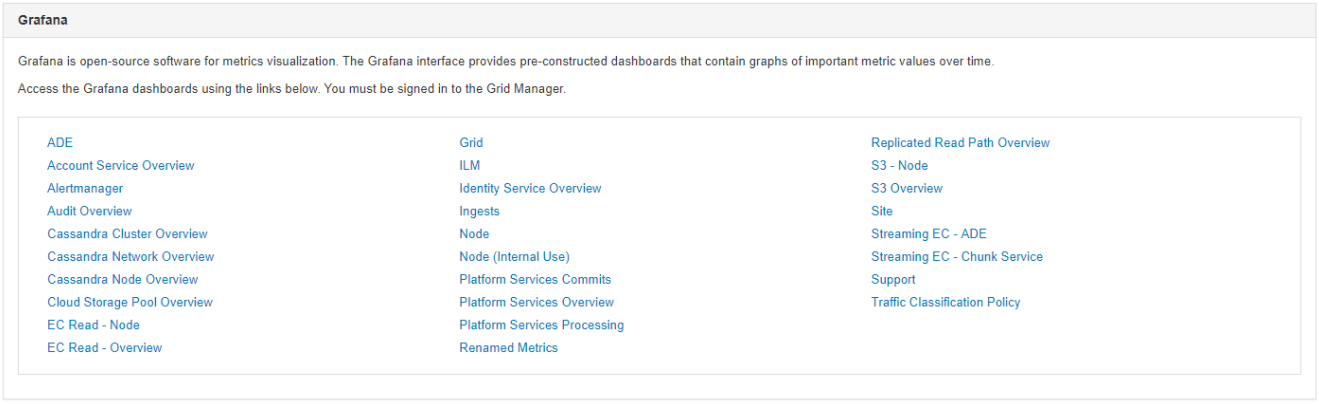
Saiba como usar a interface Grafana para visualizar e monitorar seus dados do StorageGRID.

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.

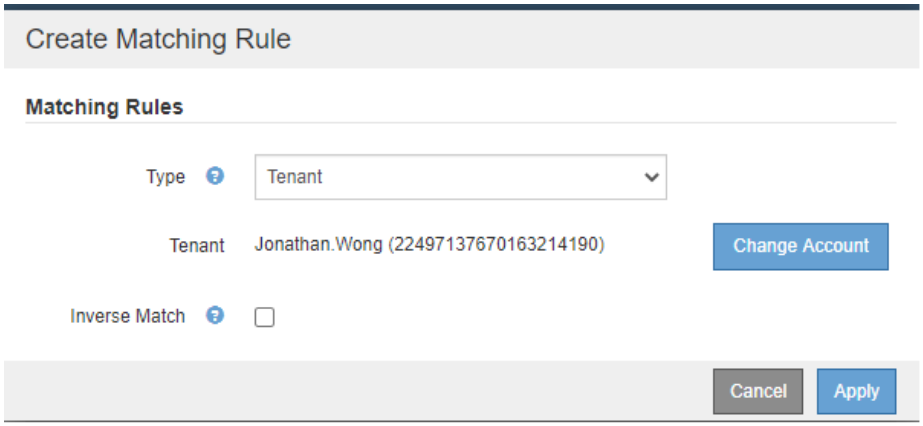
As políticas de classificação de tráfego fornecem um método para monitorar e/ou limitar o tráfego com base em um locatário específico, buckets, sub-redes IP ou pontos de extremidade do balanceador de carga. A conetividade de rede e a largura de banda são métricas especialmente importantes para o StorageGRID.

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

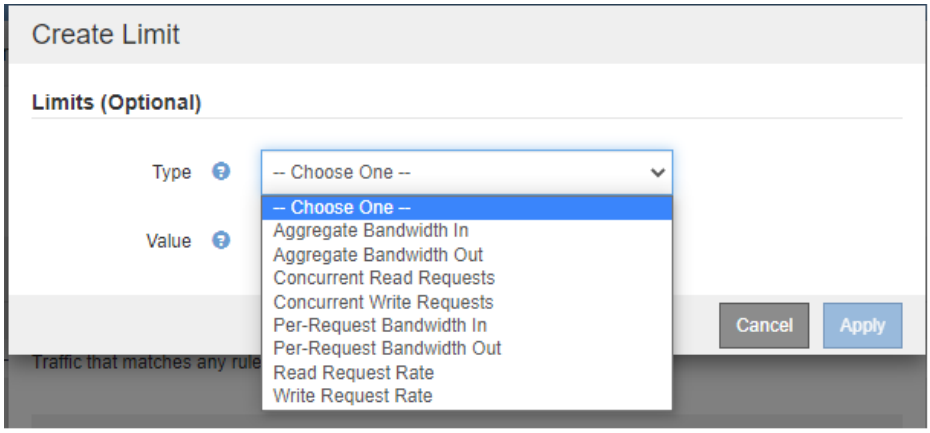
Passos

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.

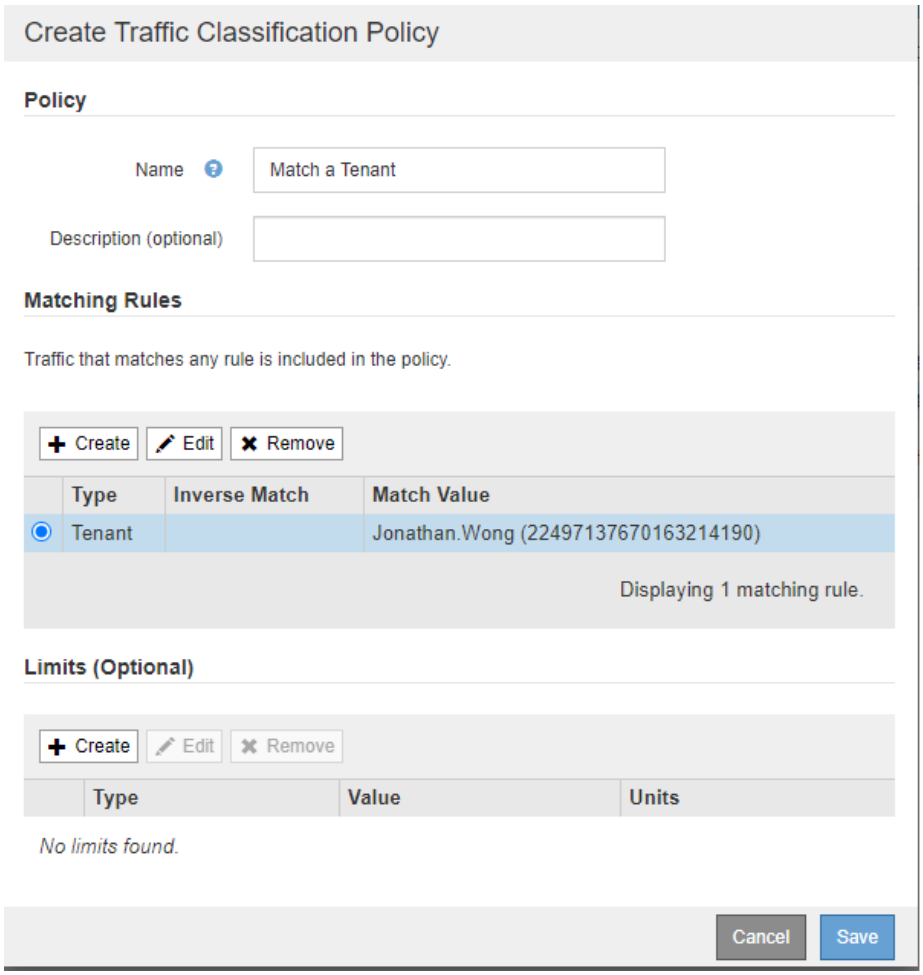
4. Crie uma regra correspondente.



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/
- 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

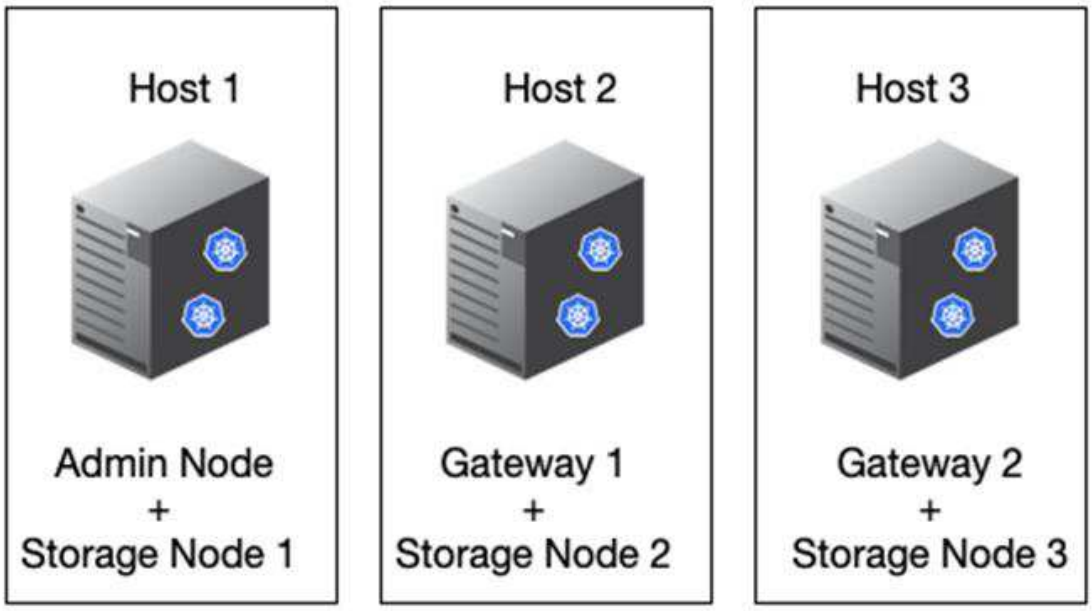
Contêiner do gateway

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 `/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

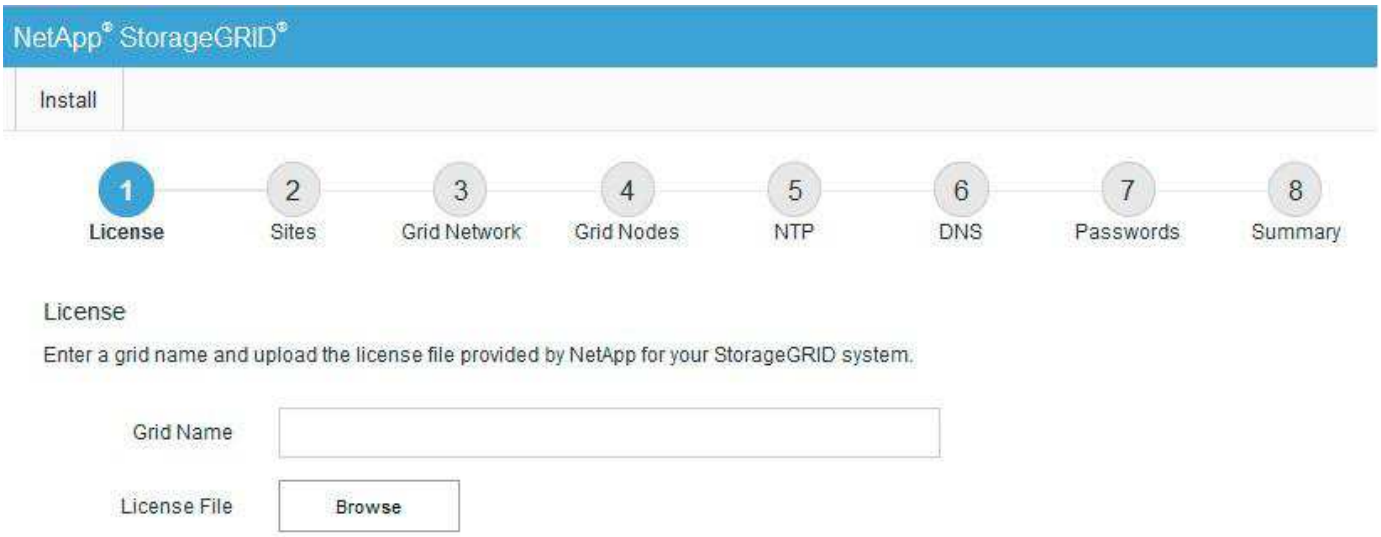
1. Acesse o Grid Manager no seguinte endereço:

   ```
   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.

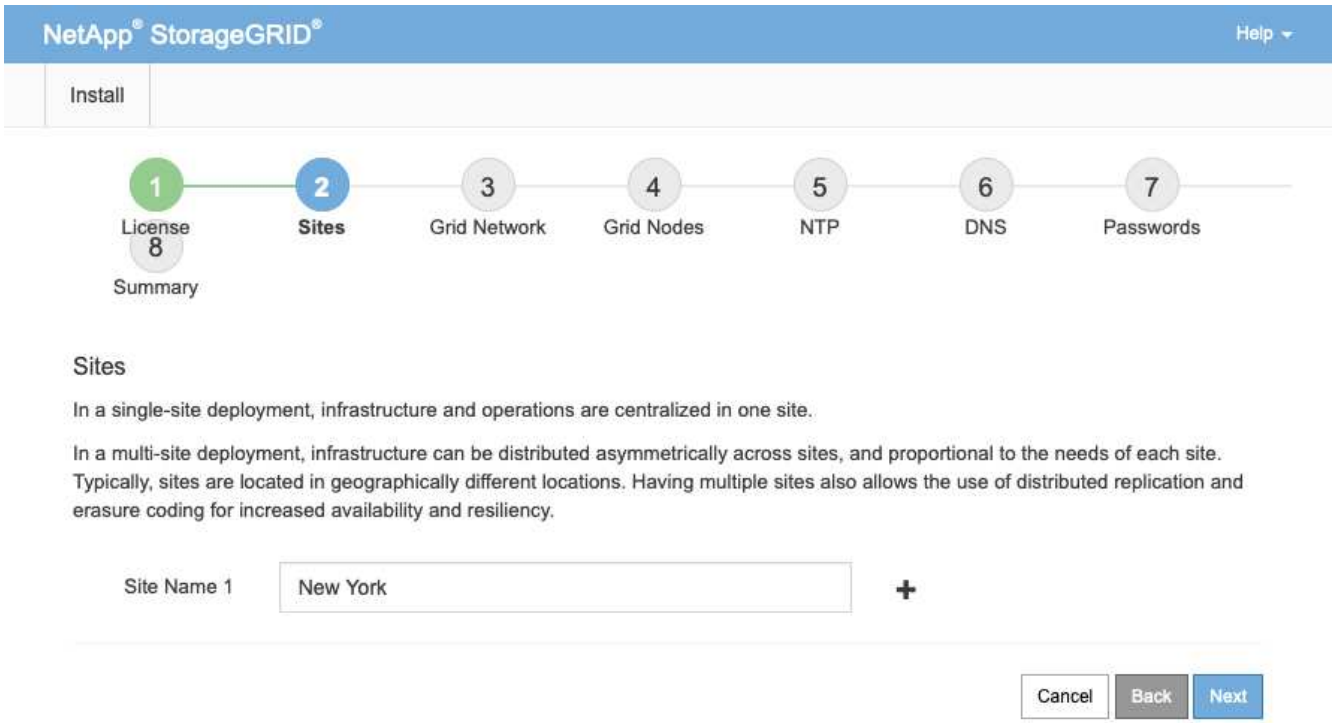
Você deve especificar o nome do seu sistema StorageGRID e fazer o upload do arquivo de licença fornecido pelo NetApp.

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

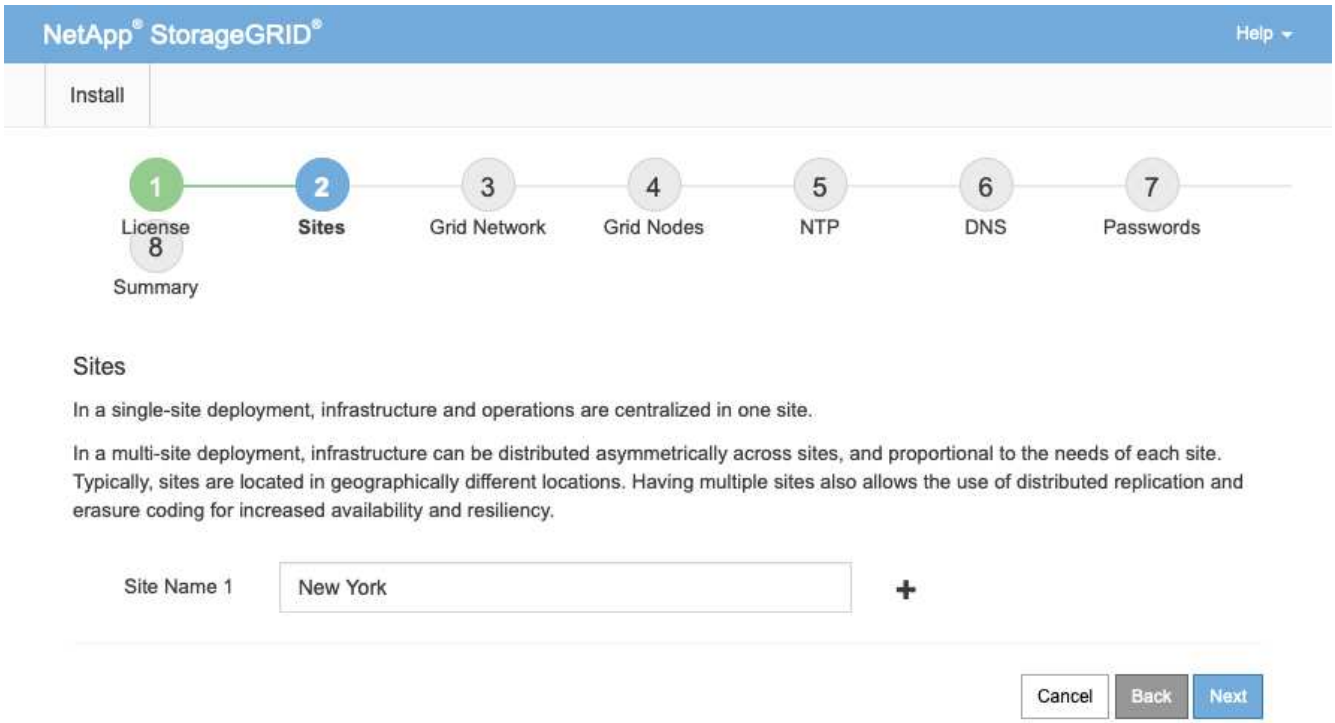
Saiba como adicionar sites ao StorageGRID para aumentar a confiabilidade e a capacidade de armazenamento.

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.

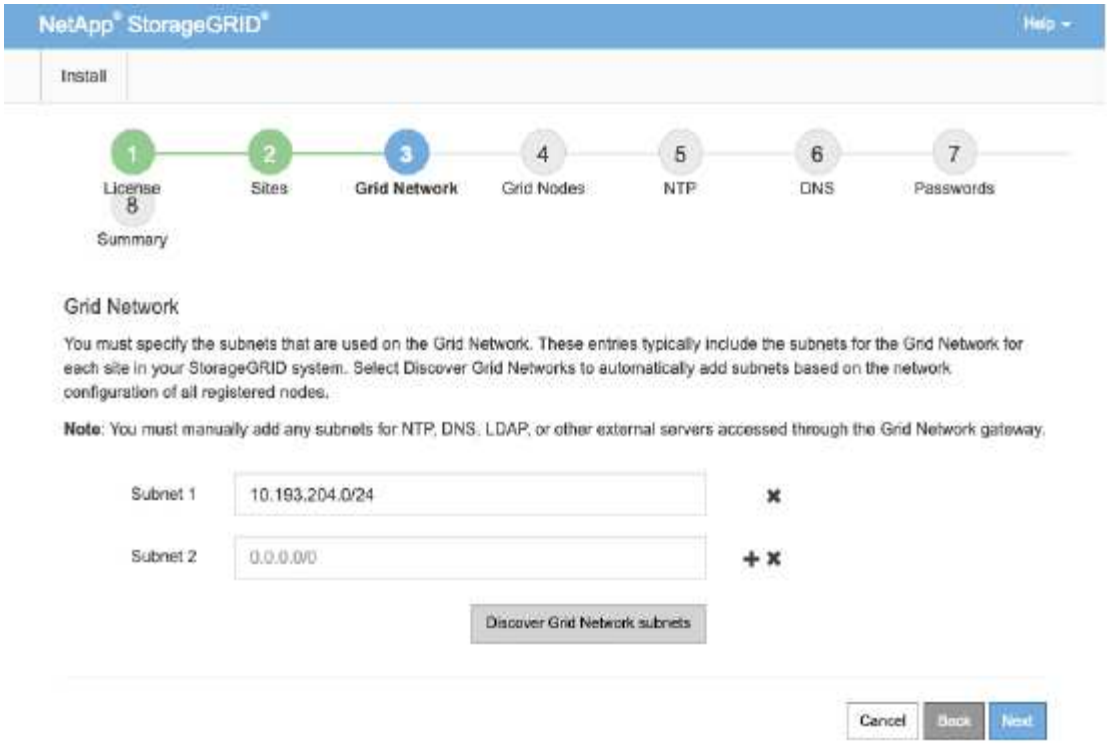
As entradas de sub-rede incluem as sub-redes para a rede de grade para cada site em seu sistema StorageGRID, além de quaisquer sub-redes que devem ser acessíveis através da rede de grade (por exemplo, as sub-redes que hospedam seus servidores NTP).

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.

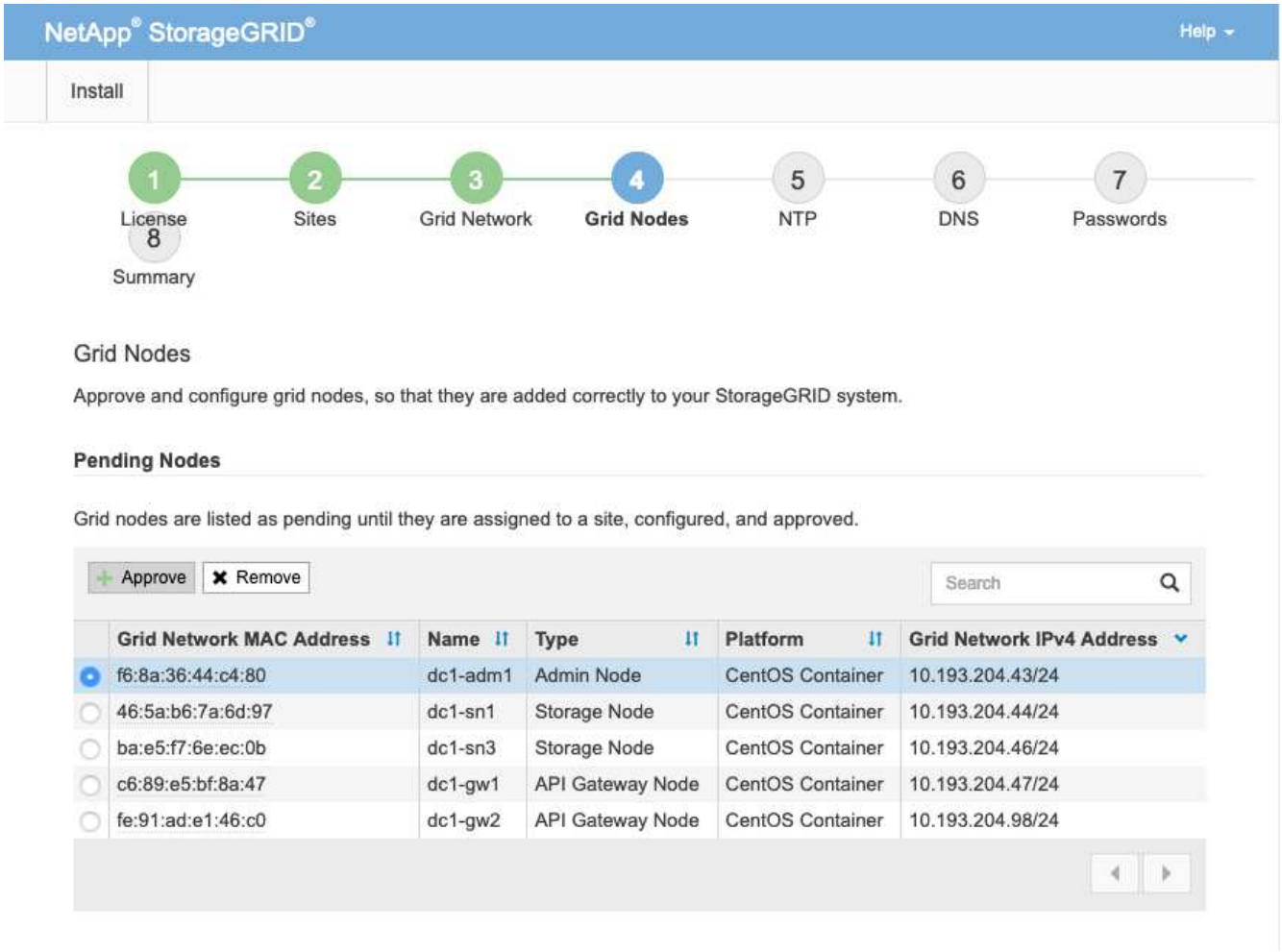
Para aprovar nós de grade pendentes, execute as seguintes etapas:

Passos

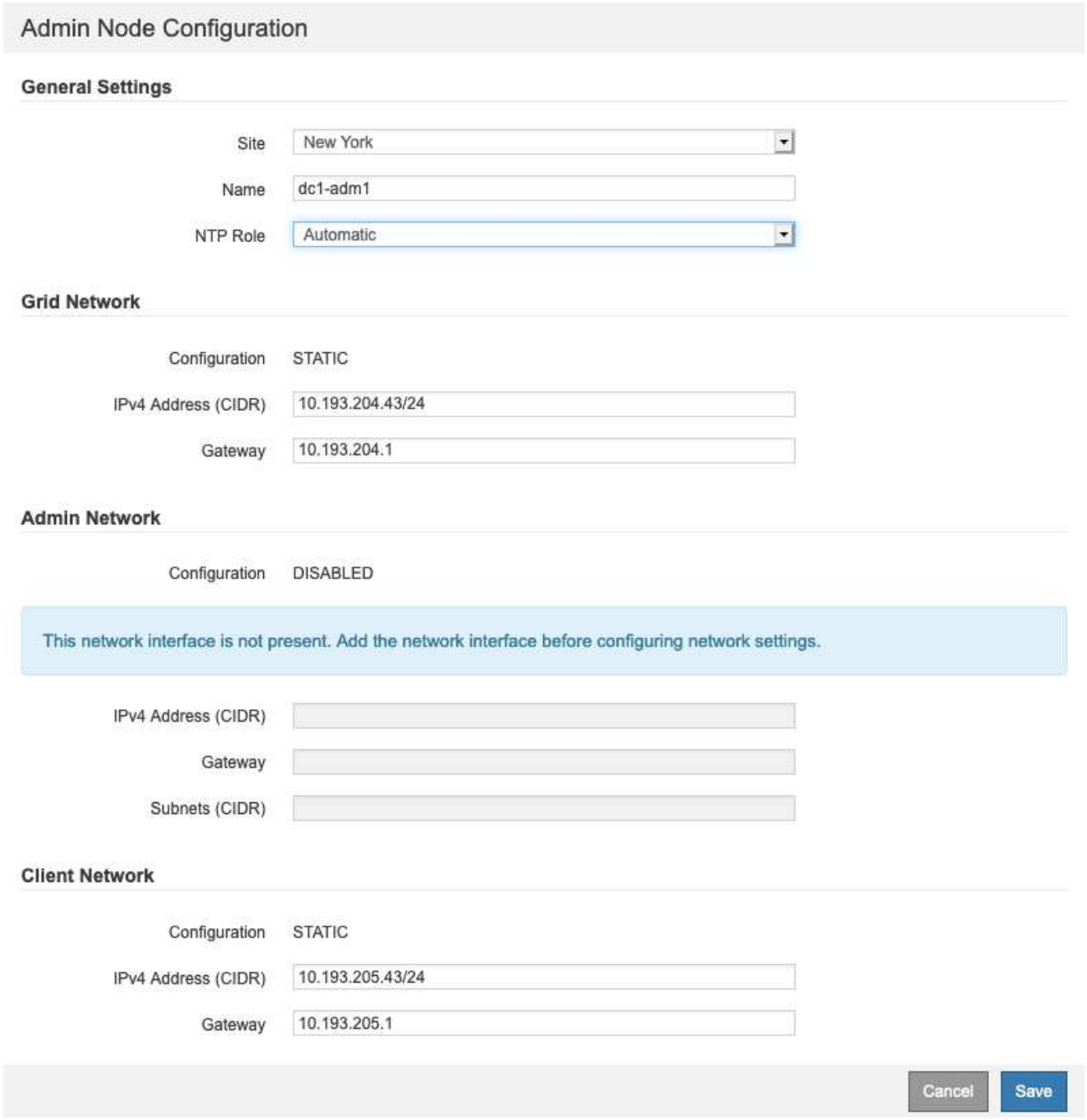
1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

   > 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:

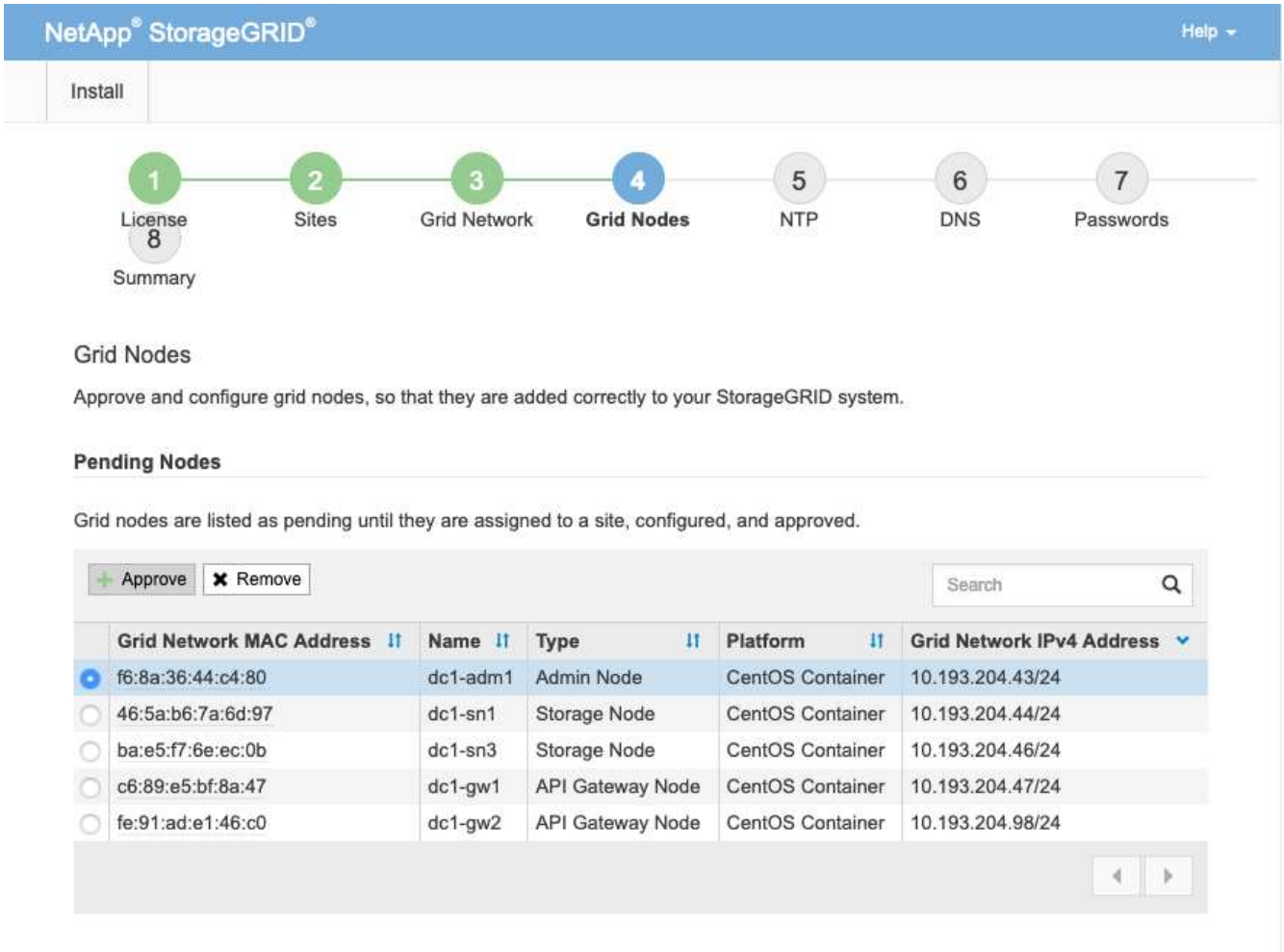
a. Reinicie o aparelho: No Instalador de aparelhos, selecione **Avançado › Reboot**. A reinicialização pode levar vários minutos.
b. Selecione **Configurar rede › Link Configuration** e ative as redes apropriadas.
c. Selecione **Configurar rede › Configuração IP** e configure as redes ativadas.
d. Volte 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.

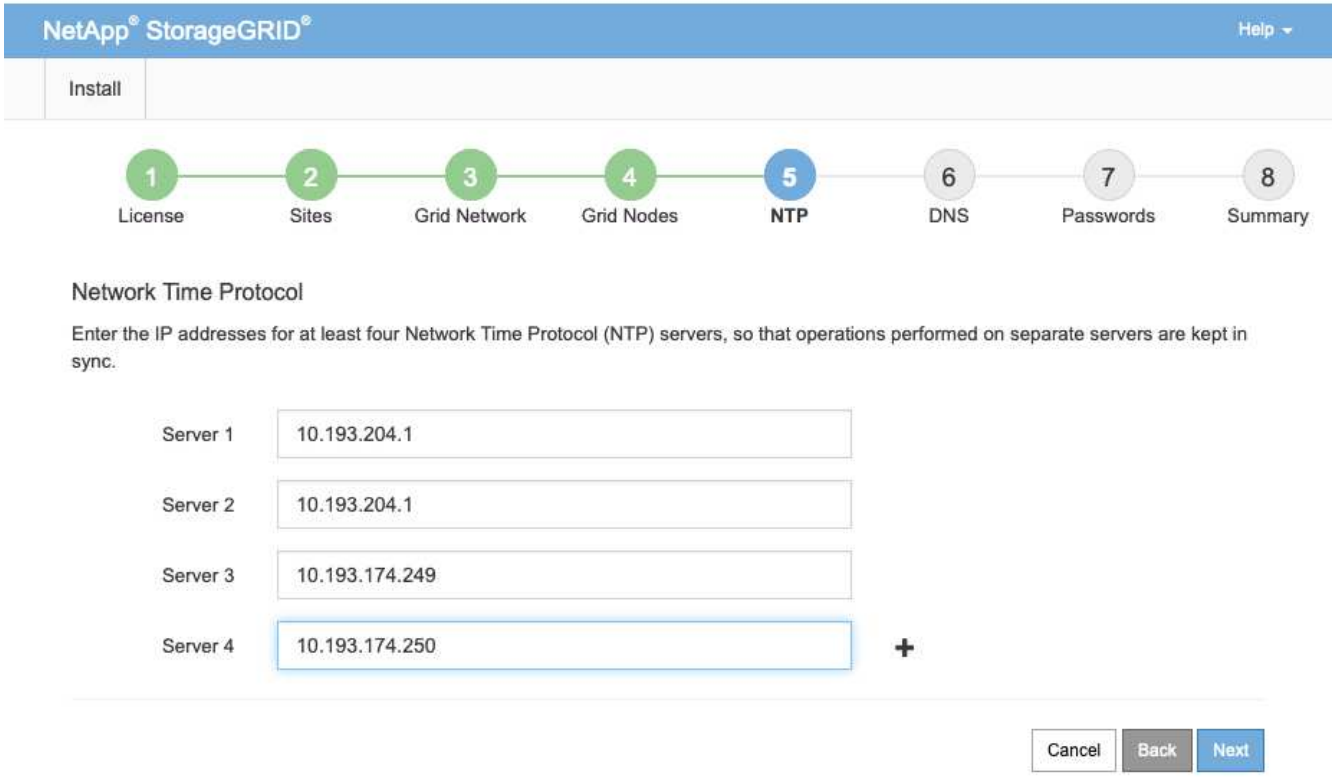
Os servidores NTP externos são usados pelos nós aos quais você atribuiu anteriormente as funções NTP principais.

> 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.

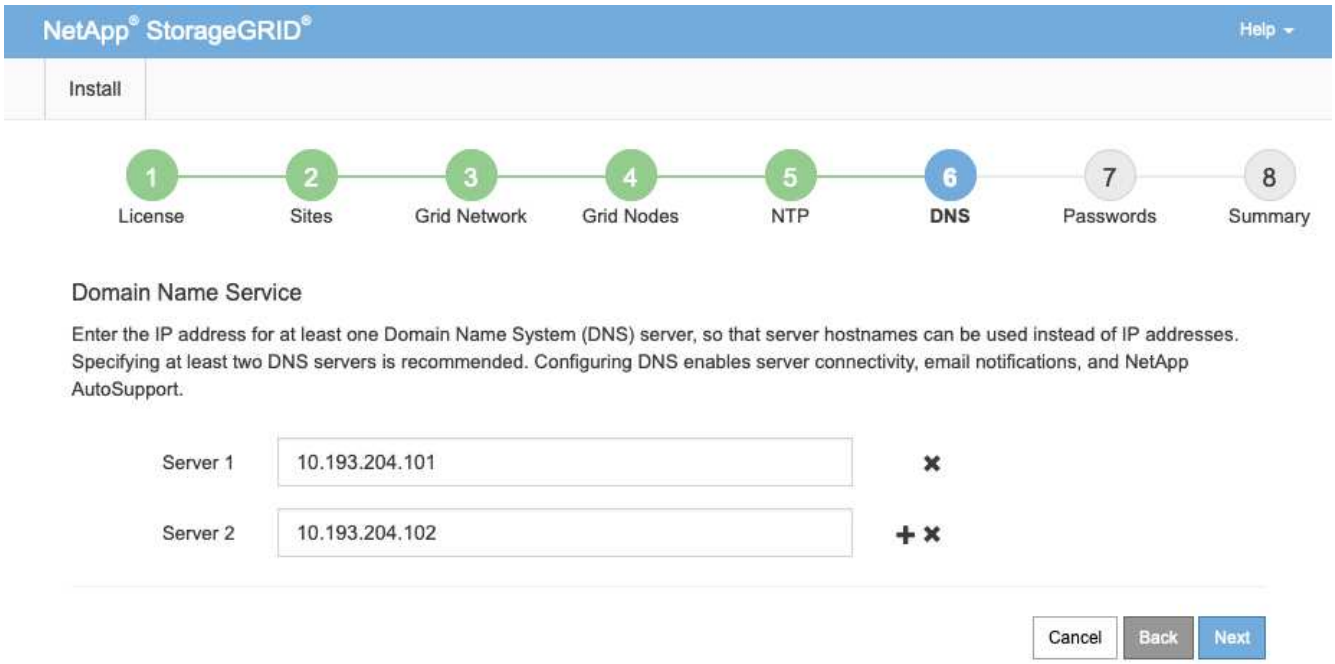
Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificado (FQDN) em vez de endereços IP para notificações de e-mail e mensagens NetApp AutoSupport. A NetApp recomenda especificar pelo menos dois servidores DNS.

> 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.

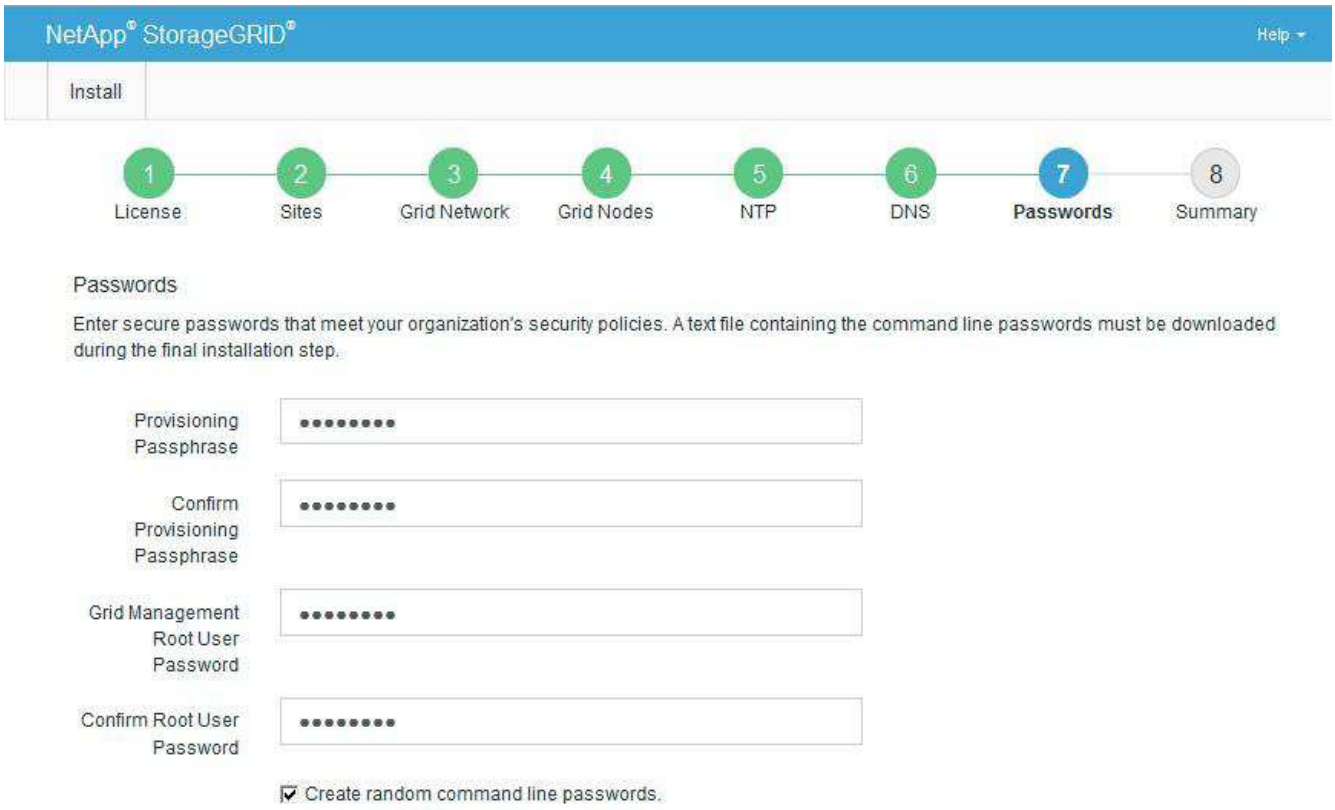
Especifique as senhas do sistema para o StorageGRID

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.

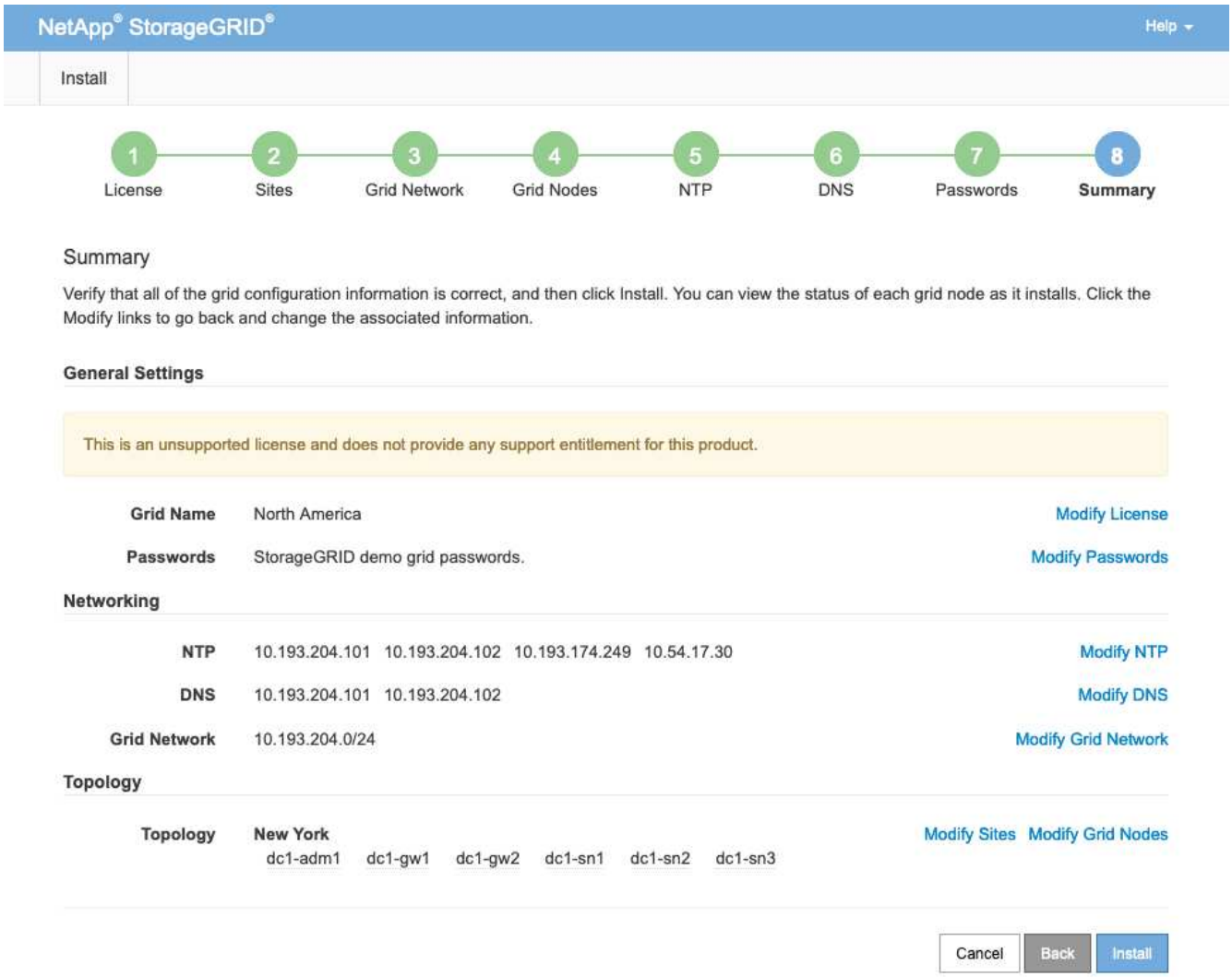
Revise a configuração e conclua a instalação do StorageGRID

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.

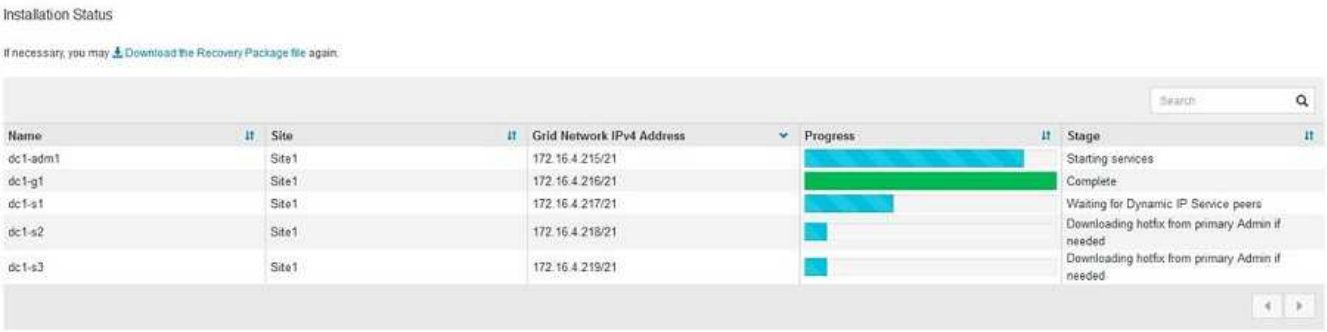
   Quando a instalação progride até o ponto em que a topologia da grade é definida, você será solicitado a baixar o arquivo do Pacote de recuperação (`.zip`) e confirmar que você pode acessar o conteúdo desse arquivo. Você deve baixar o arquivo do pacote de recuperação para que você possa recuperar o sistema 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

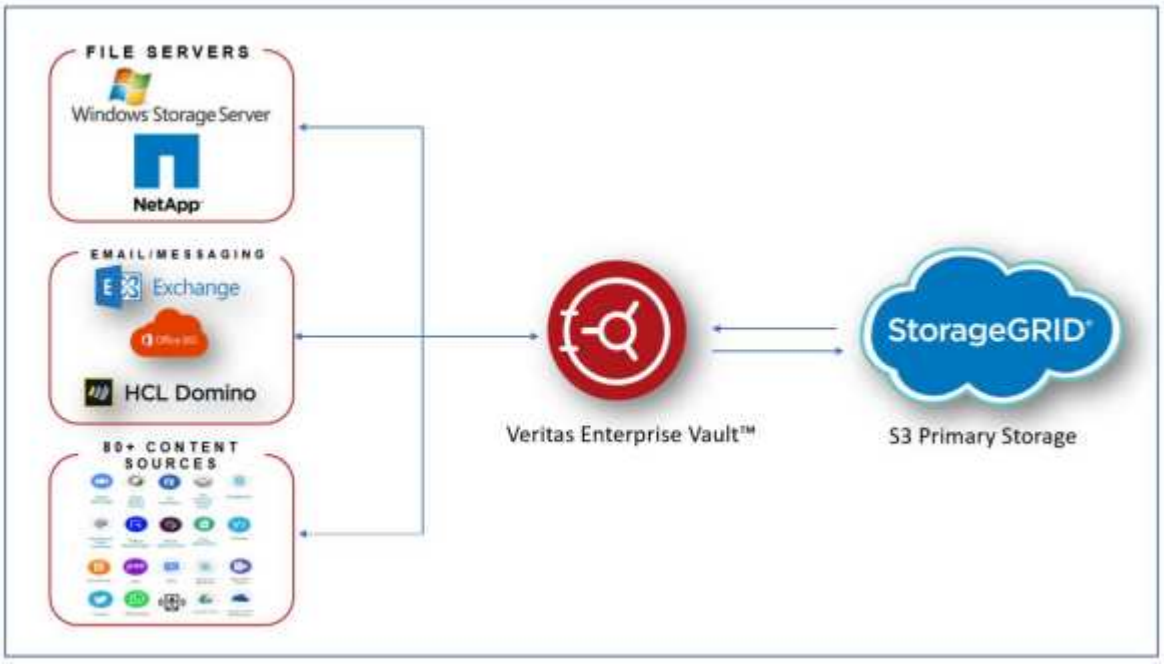
Introdução à configuração do StorageGRID para failover de site

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/

- 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.

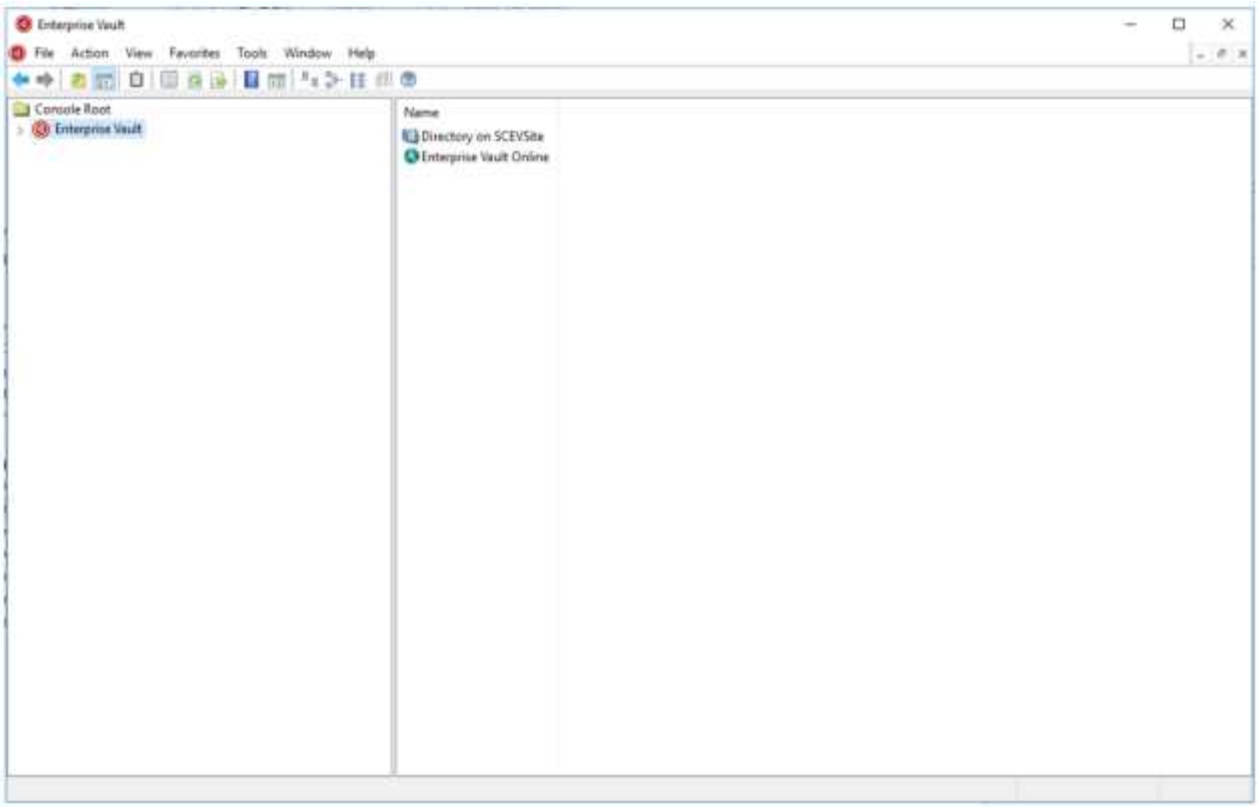
- Foram criados grupos de armazenamento de cofre e uma loja de cofre. Para obter mais informações, consulte o veritas Enterprise Vault Administration Guide.
- Um locatário, chave de acesso, chave secreta e bucket do StorageGRID foram criados.
- Foi criado um ponto de extremidade do balanceador de carga 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

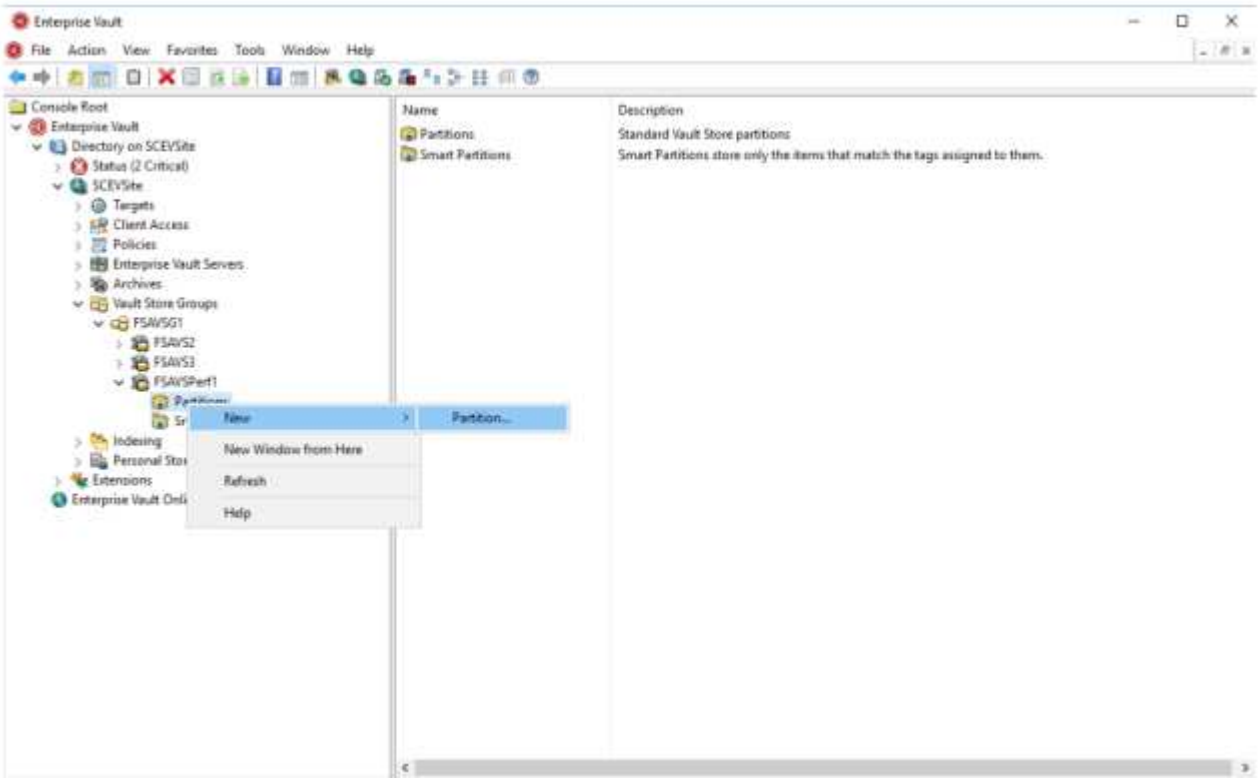
Para configurar o StorageGRID com o veritas Enterprise Vault, execute as seguintes etapas:

Passos

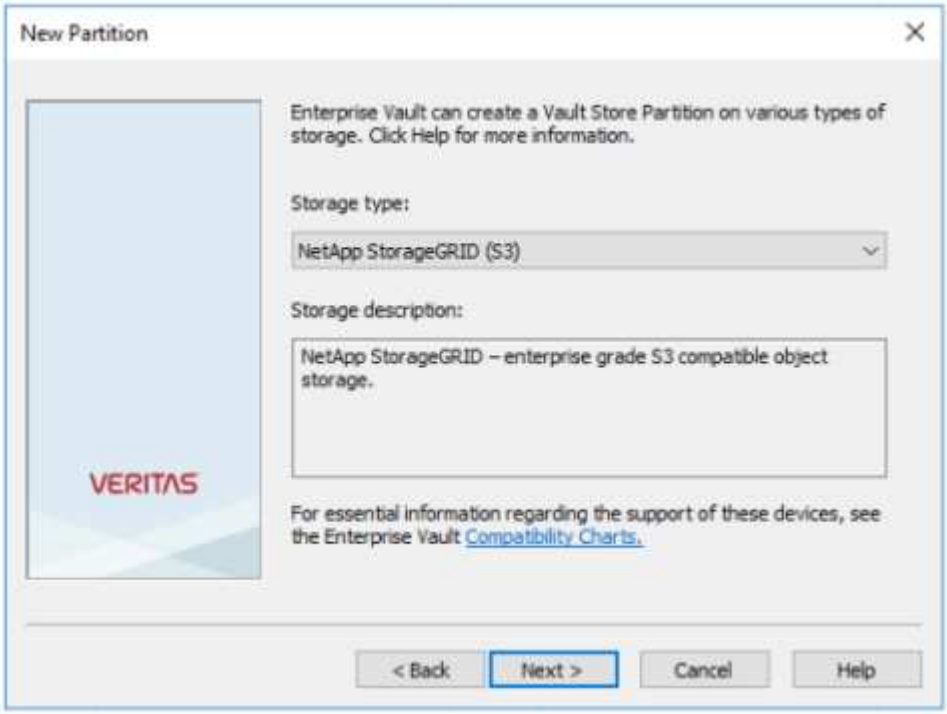
1. Inicie o console Enterprise Vault Administration.



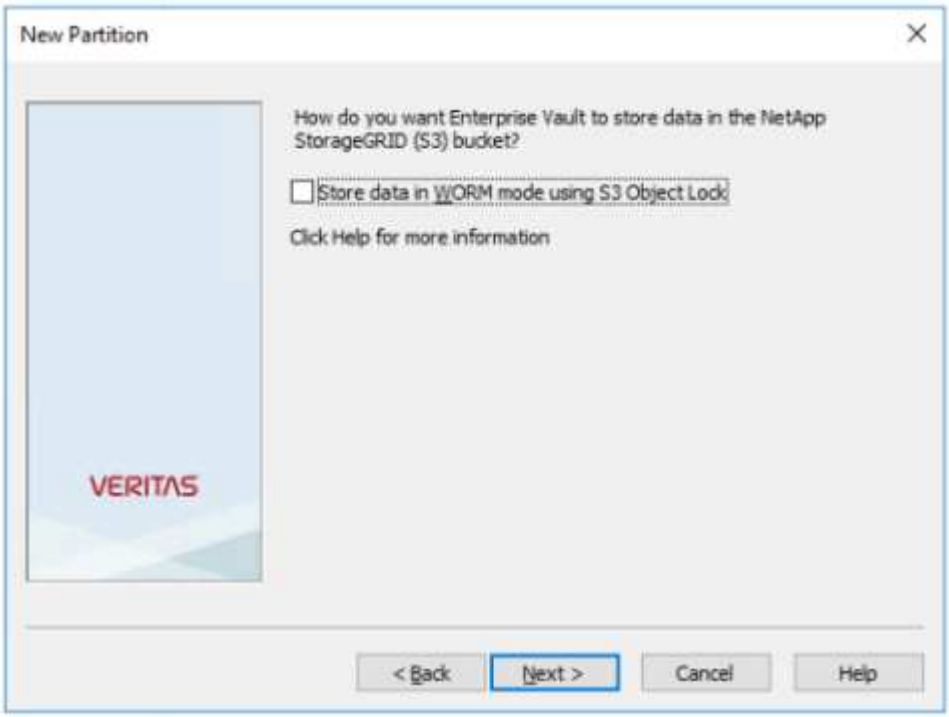
2. Crie uma nova partição de armazenamento do Vault no armazenamento apropriado do Vault. Expanda a pasta grupos do Vault Store e, em seguida, o armazenamento apropriado do Vault. Clique com o botão direito em partição e selecione **Nova › partição**.



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

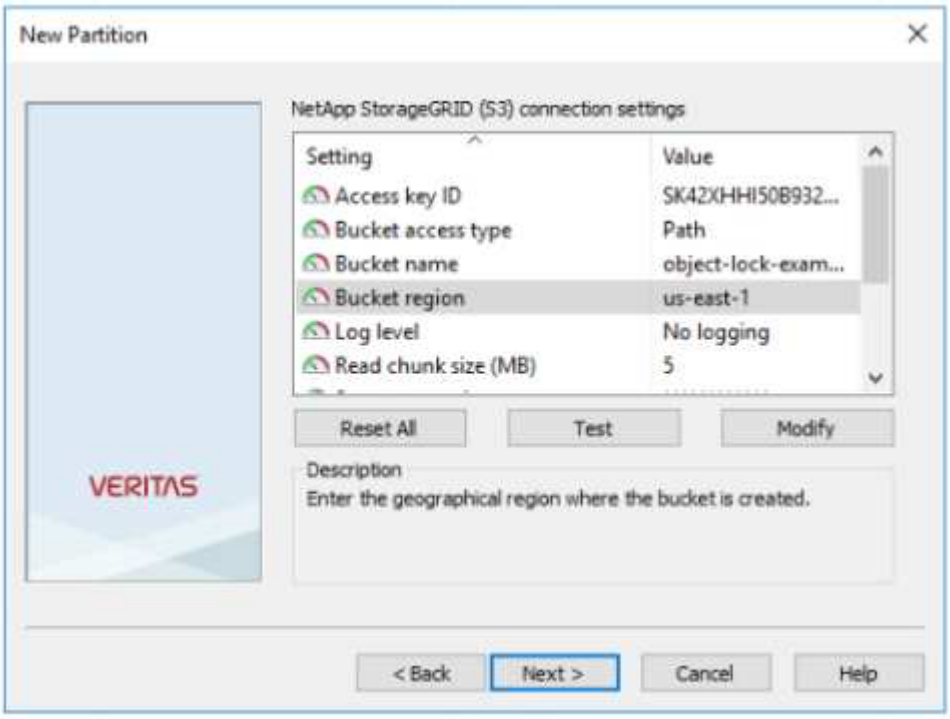


4. Deixe a opção armazenar dados no modo WORM usando S3 Object Lock desmarcada. Clique em seguinte.

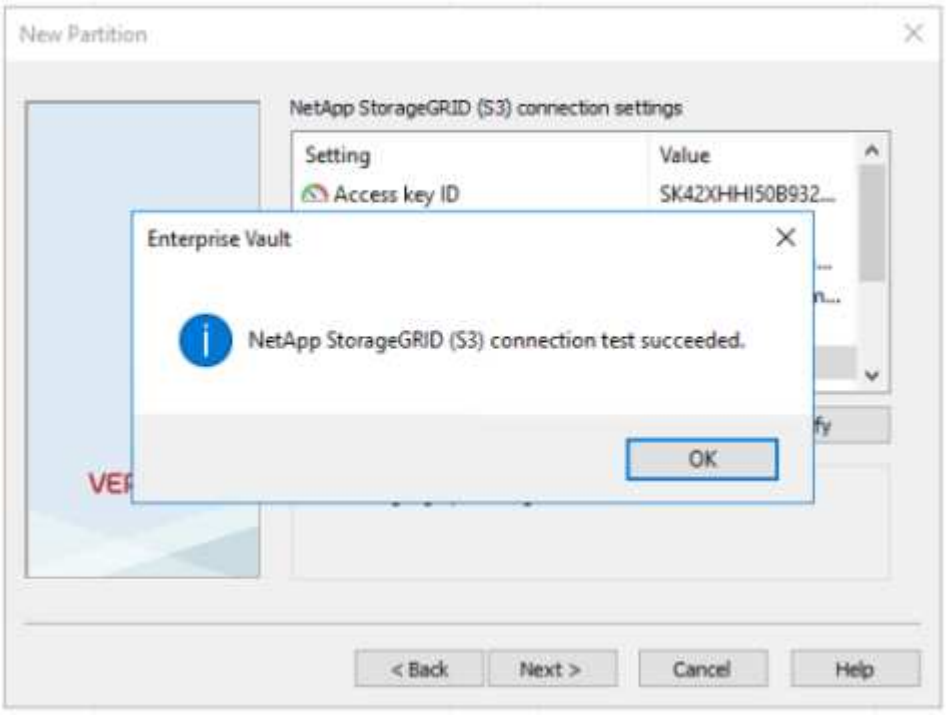


5. Na página de configurações de conexão, forneça as seguintes informações:
   - ID da chave de acesso
   - Chave de acesso secreto
   - Nome do host de serviço: Certifique-se de incluir a porta de endpoint do balanceador de carga (LBE) configurada no StorageGRID (como <a href="https://<hostname>:<LBE_port&gt"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

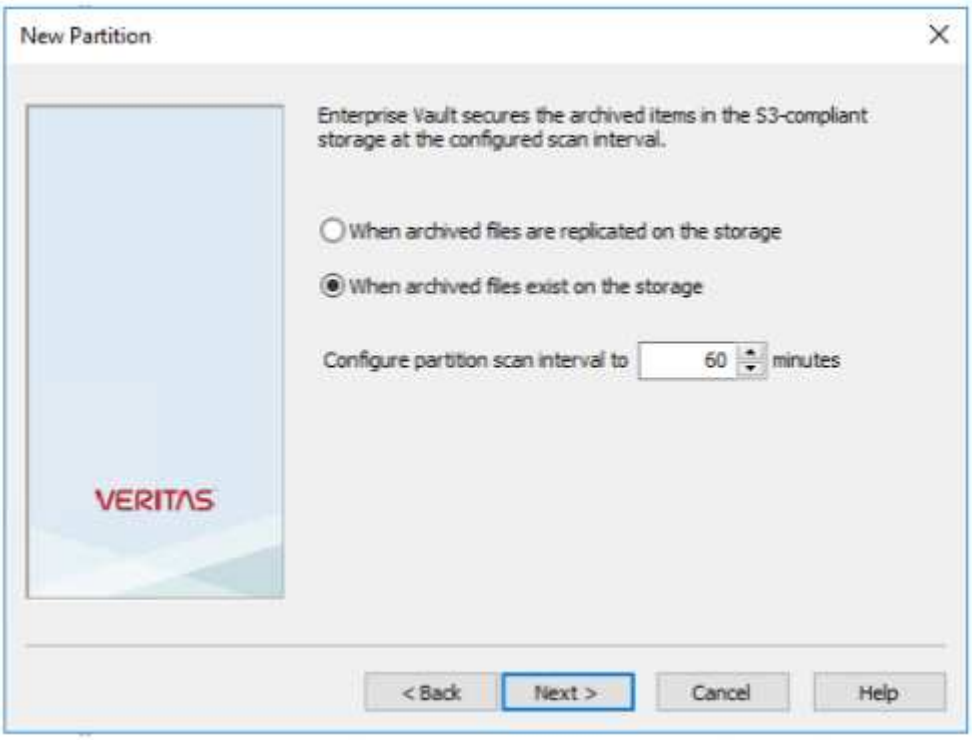
- Nome do bucket: Nome do bucket de destino pré-criado. o veritas Enterprise Vault não cria o bucket.
- Região do balde: `us-east-1` É o valor predefinido.



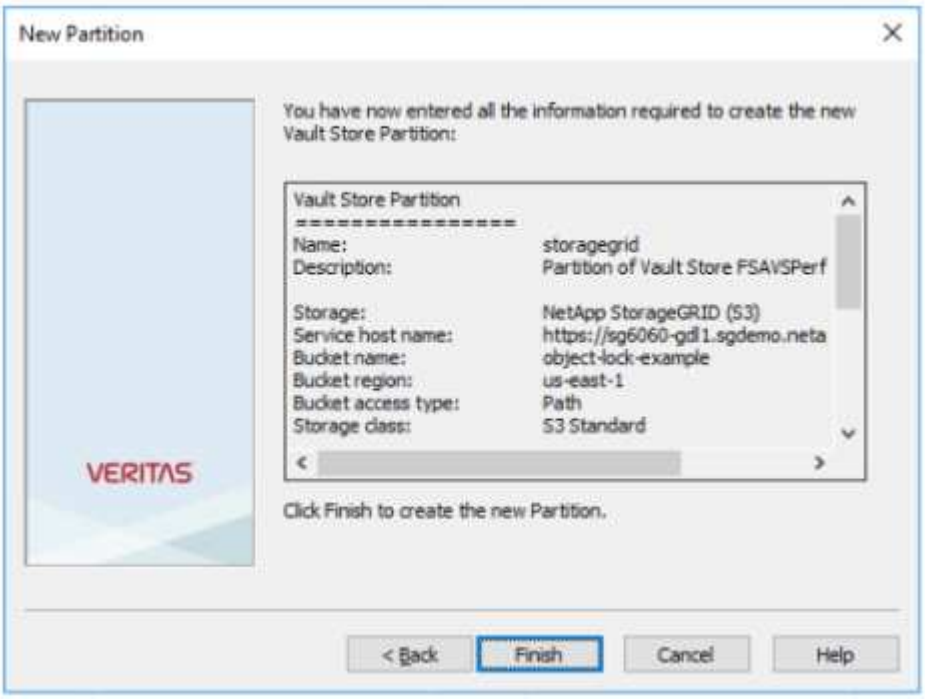
6. Para verificar a conexão com o bucket do StorageGRID, clique em testar. Verifique se o teste de conexão foi bem-sucedido. Clique em OK e em Avançar.



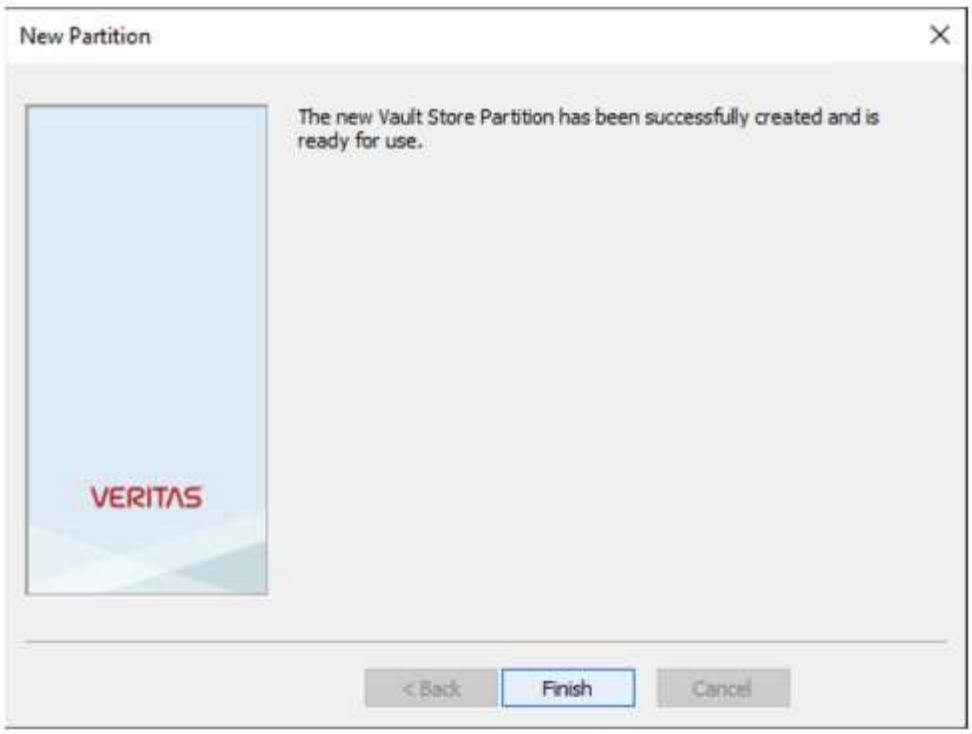
7. O StorageGRID não suporta o parâmetro de replicação S3. Para proteger seus objetos, o StorageGRID usa regras de gerenciamento do ciclo de vida das informações (ILM) para especificar esquemas de proteção de dados - várias cópias ou codificação de apagamento. Selecione a opção quando existirem ficheiros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

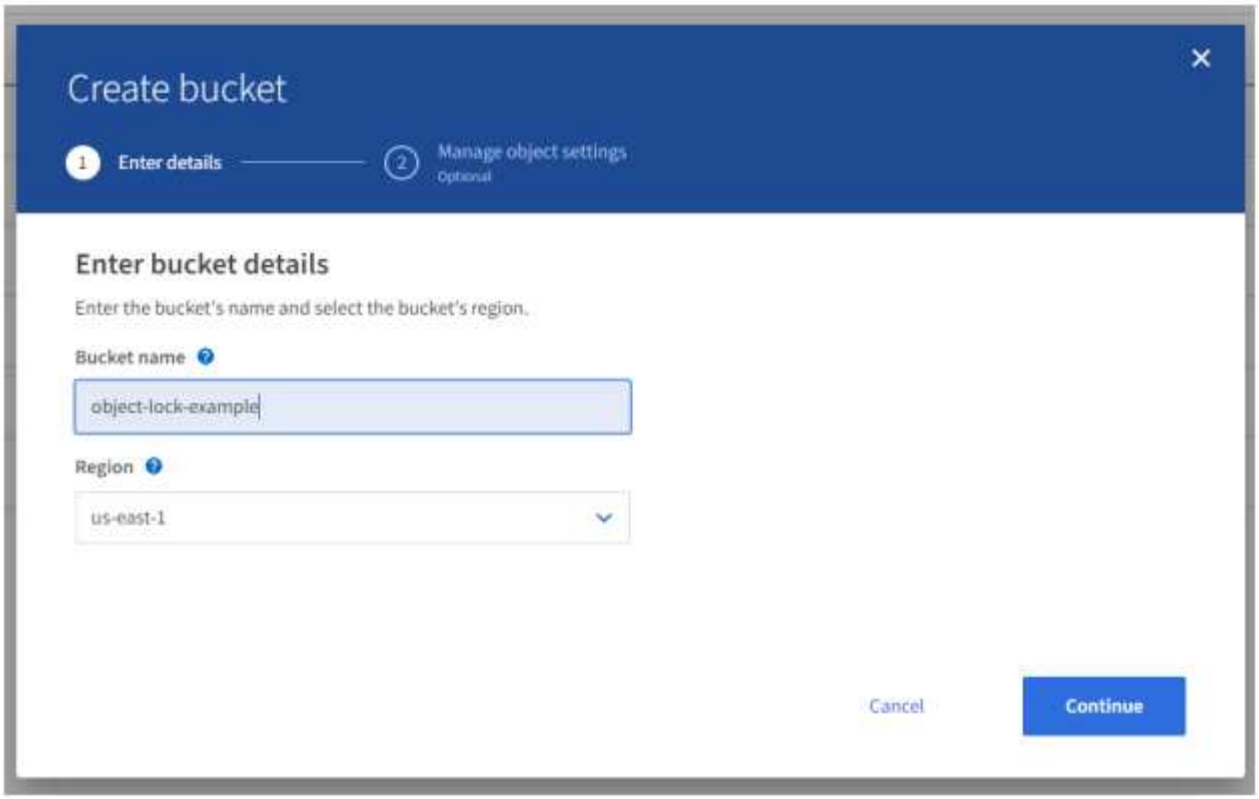
Para storage WORM, o StorageGRID usa o bloqueio de objetos S3 para reter objetos para conformidade. Isso requer o StorageGRID 11,6 ou superior, onde a retenção padrão do bucket do bloqueio de objetos S3 foi introduzida. O Enterprise Vault também requer a versão 14.2.2 ou superior.

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

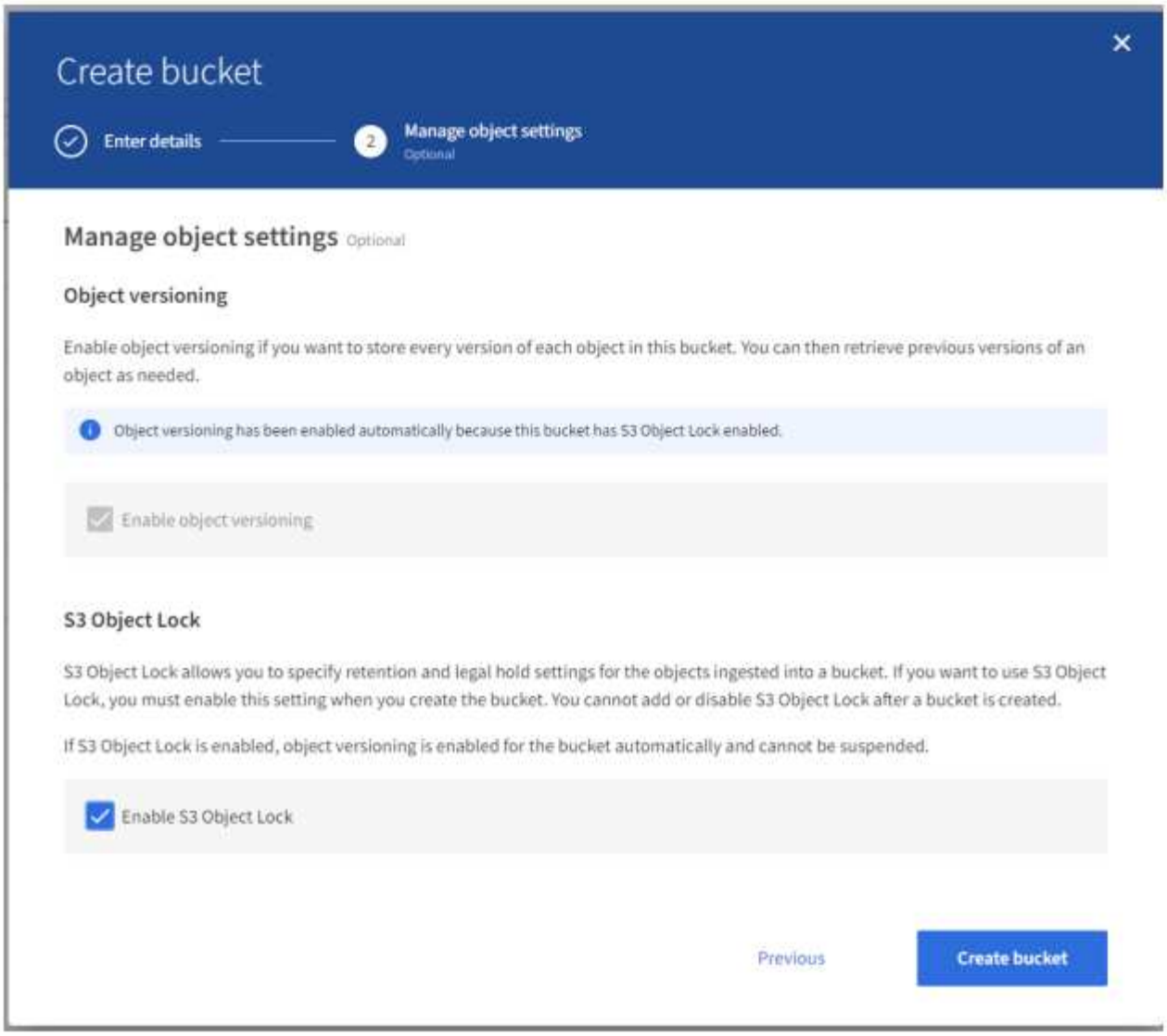
Para configurar a retenção padrão do bucket do bloqueio de objetos do StorageGRID S3, execute as seguintes etapas:

Passos

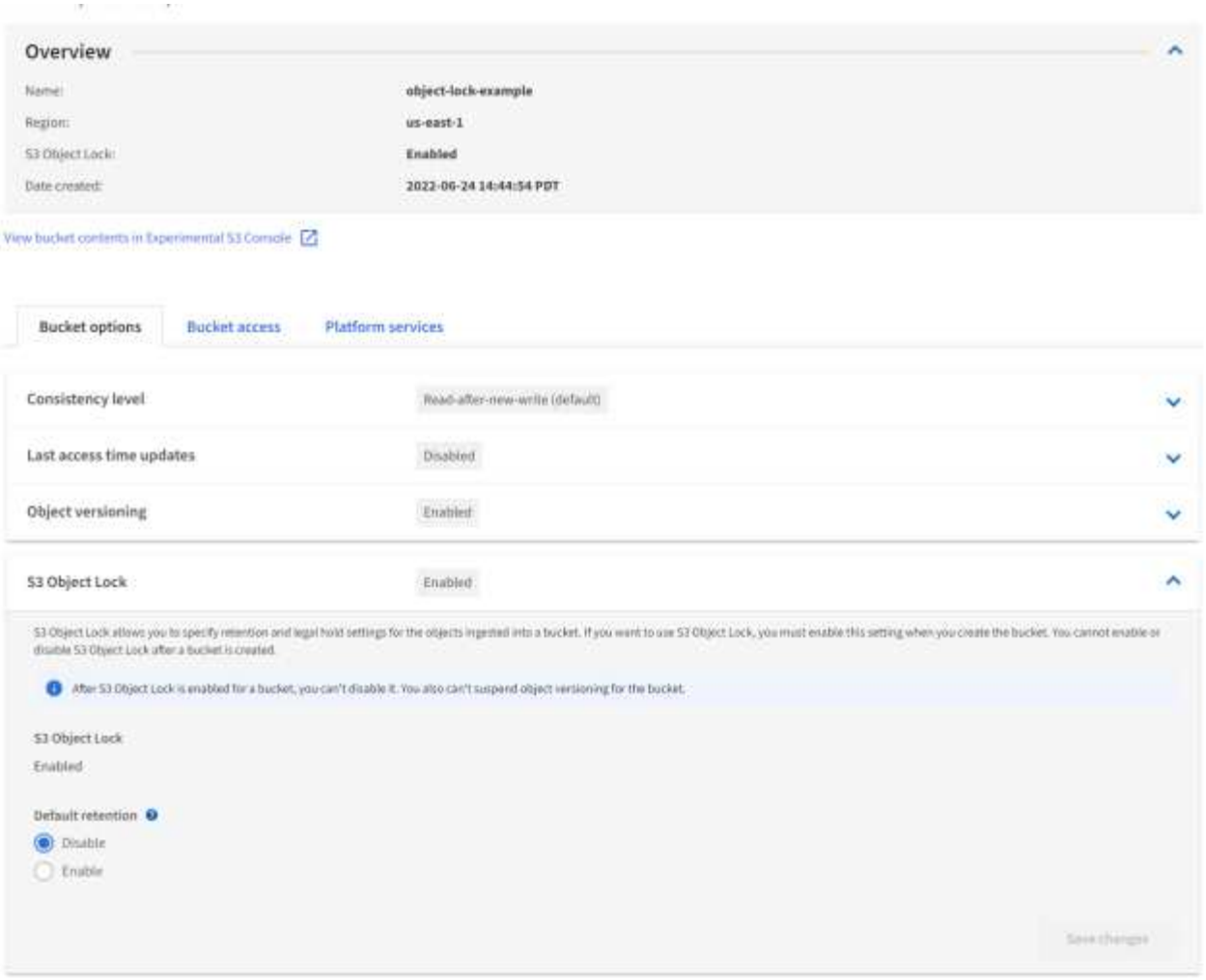
1. No Gerenciador do Locatário do StorageGRID, crie um bucket e clique em continuar



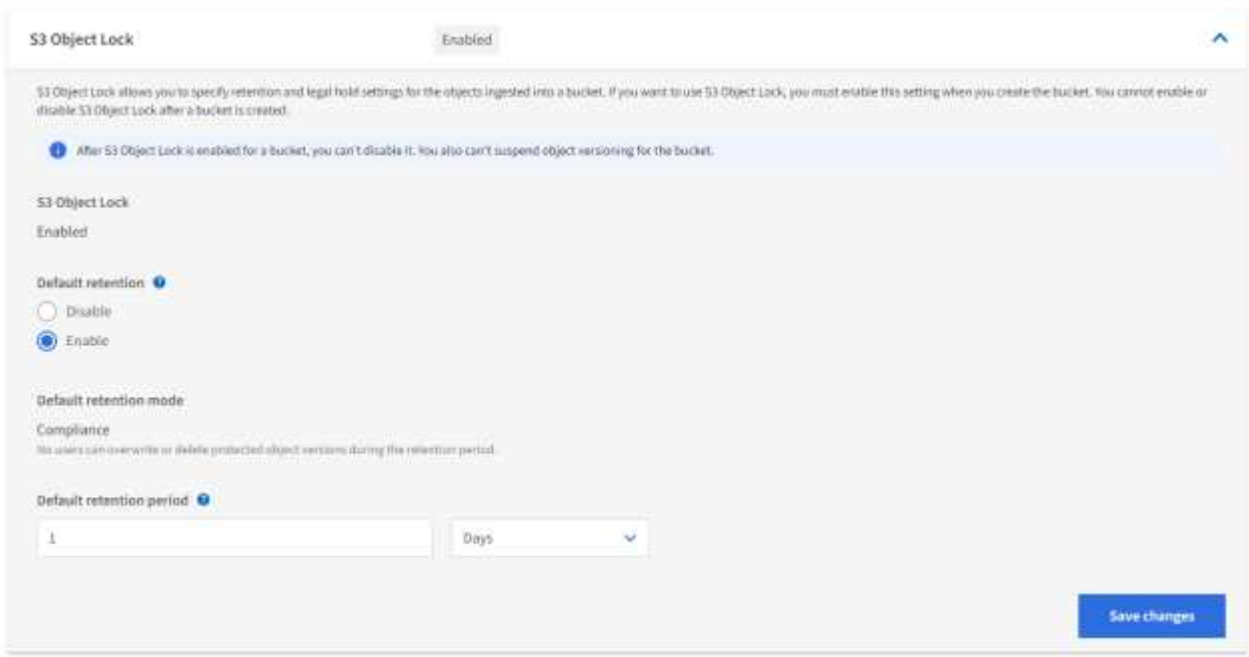
2. Selecione a opção Ativar bloqueio de objetos S3D e clique em criar balde.



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.



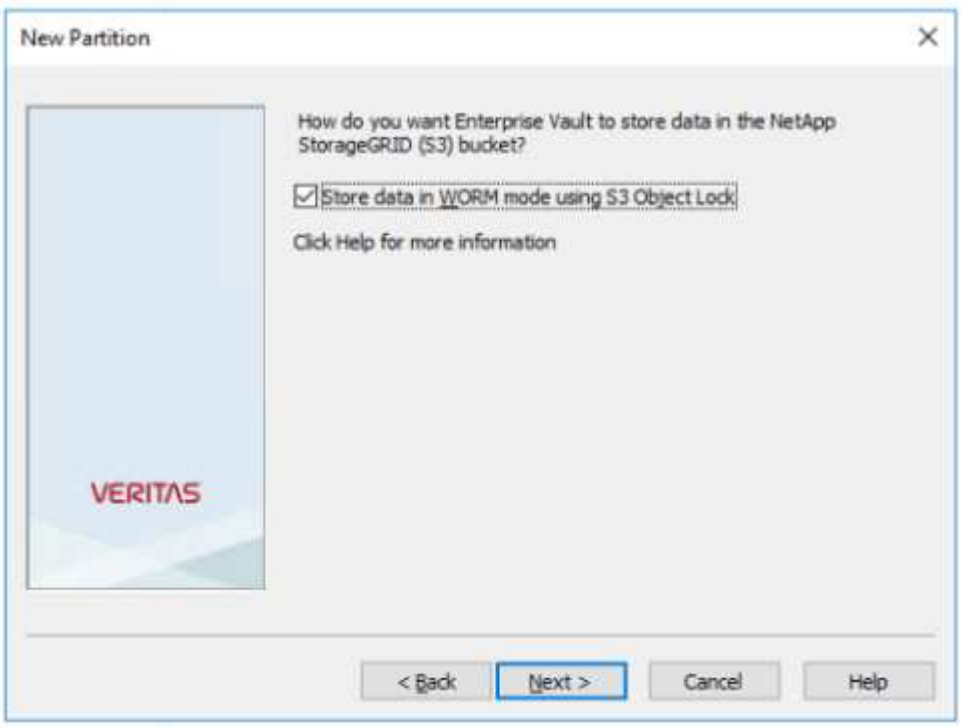
O bucket agora está pronto para ser usado pelo Enterprise Vault para armazenar dados WORM.

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

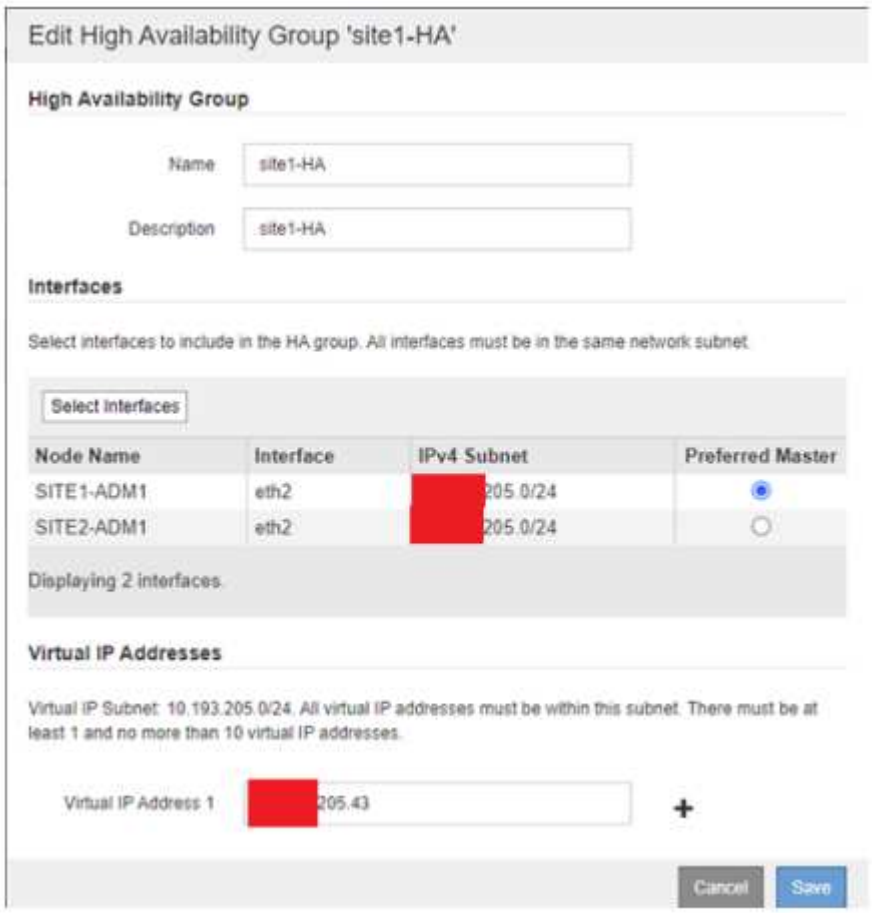
Para configurar o failover do site do StorageGRID, execute as seguintes etapas:

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.

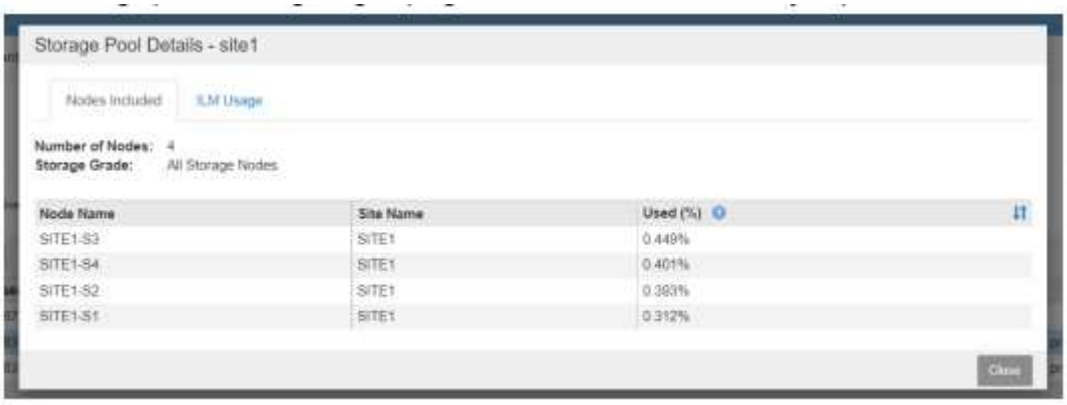


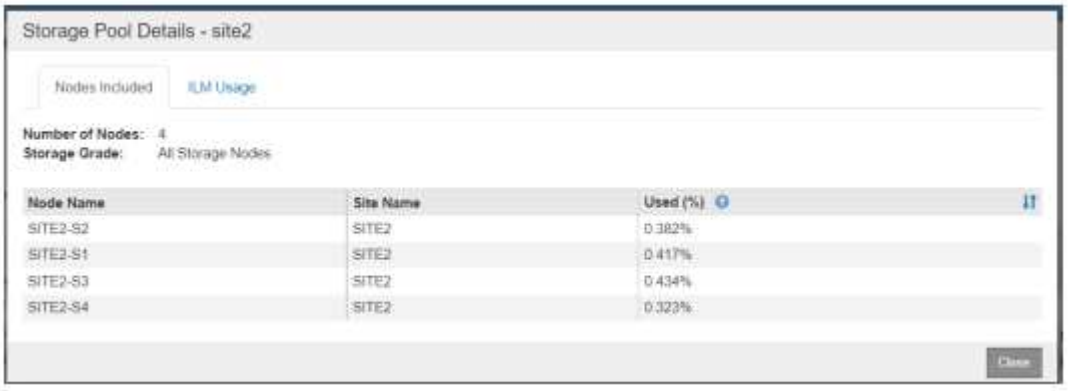
3. Esse endereço IP virtual (VIP) deve ser associado ao nome de host S3 usado durante a configuração de partição do veritas Enterprise Vault. O endereço VIP resolve o tráfego para O site1 e, durante A falha DO site1, o endereço VIP redireciona o tráfego para O site2 de forma transparente.
4. Certifique-se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

Passos para aceder ao software de avaliação StorageGRID

Esta instrução destina-se a vendas, parceiros e clientes potenciais da NetApp envolvidos com a NetApp.

Registre-se para uma conta

1. Registe-se para obter uma conta no "Site de suporte da NetApp" utilizando o e-mail da sua empresa.
   a. Certifique-se de que não iniciou sessão com a conta recém-criada.
   b. Se você já tiver uma conta, certifique-se de que não está conetado e prossiga com a próxima etapa.
2. Crie um caso de suporte não técnico para elevar os níveis de acesso ao "prospect". Para fazer isso, clique no ""Relatar um problema"link " no rodapé do site.
3. Selecione "problema de registo" como a categoria de feedback.
4. Na seção de comentários, escreva: "Meu endereço de e-mail da conta é *Your-Email-Address*. Gostaria de obter acesso a potenciais clientes para transferir o software de avaliação StorageGRID."
   a. Mencione o nome da pessoa interna do NetApp que sugeriu o pedido de acesso ao cliente potencial.

Baixar StorageGRID

1. Depois que seu caso de suporte for revisado e aprovado, o suporte da NetApp notificará você por e-mail de que sua conta recebeu acesso a clientes potenciais.
2. Faça download do "Software de avaliação StorageGRID".

O arquivo de licença Eval está localizado dentro do arquivo zip. Ele é o StorageGRID-Webscale-<version> NLF000000.txt uma vez descompactado.

Baixar o software é um processo que envolve medidas de conformidade comercial para aderir aos requisitos legais. Para garantir a conformidade, os usuários precisam criar uma conta e abrir um caso de suporte antes de obter acesso. Esse processo nos ajuda a manter o controle e a documentação adequados, ao mesmo tempo em que fornece aos clientes potenciais o software pronto para a produção de que precisam.

Nós fornecemos a versão "pronta para produção" do StorageGRID, que não é uma versão de código aberto ou alternativa. É importante notar que **o suporte não é fornecido** a menos que o cliente potencial atualize para uma licença de produção.

Por favor, entre em Contato com StorageGRID.NetApp.com para qualquer problema com os passos acima.

Blogs do NetApp StorageGRID

Você pode encontrar alguns ótimos blogs do NetApp StorageGRID aqui:

- Fev. 16 2024: "Apresentamos o StorageGRID 11,8: Segurança, simplicidade e experiência do usuário aprimorados"
- Fev. 16 2024: "Apresentamos o StorageGRID 11,8"
- Fev. 2 2024: "Anunciando o resumo da solução StorageGRID e lakeFS"
- Dez 12 2023: "Análise de big data no StorageGRID: Dremio tem um desempenho 23 vezes mais rápido do que o Apache Hive"
- Nov 7 2023: "Geleira Spectra Logic On-Prem com StorageGRID"
- Out 17 2023: "A partir do Hadoop: Modernizando a análise de dados com Dremio e StorageGRID"
- Set 1 2023: "Utilizando o Cloud Insights para monitorar e coletar logs usando o Fluent Bit"
- Ago 30 2023: "Ponto de montagem para o Amazon S3 File System agora é GA"
- Maio de 16 2023: "Apresentamos o StorageGRID 11,7 e o novo dispositivo de storage de objetos all-flash SGF6112"
- Maio de 16 2023: "Novidades da família de storage de objetos StorageGRID"
- Mar 30 2023: "Ponto de montagem para a versão alfa do Amazon S3 com StorageGRID"
- Mar 30 2023: "Use o BlueXP para proteger EPIC EHR com uma política de backup compatível com 3:2:1"
- Mar 14 2023: "Como fazer backup de bancos de dados EHR da Epic Systems com um comando em uma arquitetura compatível com 3:2:1"
- Fev. 14 2023: "O que o chocolate, esqui, relógios e mainframes têm em comum?"
- Janeiro de 18 2023: "Bloqueio de objetos do StorageGRID S3 validado para o veritas NetBackup"
- Janeiro de 16 2023: "A StorageGRID renova a certificação de conformidade NF203 e ISO/IEC 25051"
- Dez 6 2022: "A StorageGRID alcança a certificação de conformidade da KPMG"
- Nov 23 2022: "Inteligência artificial explicável com MLOps alimentados por NetApp e Modzy"
- Nov 7 2022: "Suporte ao StorageGRID e ao ONTAP S3: Diferenças, semelhanças e integração"
- Out 5 2022: "O NetApp Cloud Insights adiciona painéis de galeria do StorageGRID"
- Out 5 2022: "Descongele seus dados no StorageGRID para floco de neve"
- Set 26 2022: "NetApp StorageGRID para provedores de serviços"
- Set 19 2022: "Suporte à proteção contra DataLock e ransomware para StorageGRID"
- Set 1 2022: "Pegue essas métricas e Graph It"
- Ago 23 2022: "Construa seu data Lake no StorageGRID"
- Ago 17 2022: "Tudo começa com o Object Locking… criando um ecossistema de armazenamento S3 para aplicativos de backup críticos"
- Ago 16 2022: "Integração do StorageGRID com o stack de código aberto ELK para aprimorar a experiência do cliente"
- Ago 5 2022: "A NetApp StorageGRID obtém a certificação de segurança Common Criteria"
- Julho de 26 2022: "Confira a lista crescente de soluções de parceiros validadas para a StorageGRID"
- Junho de 9 2022: "Use o conetor Cloudera Hadoop S3A com StorageGRID"

- Maio de 26 2022: "StorageGRID: Armazenamento e gerenciamento de dados de replicação e backup no local"
- Maio de 24 2022: "Modernize seus workloads de análise com o NetApp e a Alluxio"
- Maio de 10 2022: "Lab on Demand é a sua melhor ferramenta de vendas para StorageGRID"

Documentação do NetApp StorageGRID

Você pode encontrar a documentação completa para cada versão do NetApp StorageGRID aqui:

- "Dispositivos StorageGRID"
- "StorageGRID 11,9"
- "StorageGRID 11,8"
- "StorageGRID 11,7"
- "StorageGRID 11,6"
- "StorageGRID 11,5"
- "StorageGRID 11,4"
- "StorageGRID 11,3"
- "StorageGRID 11,2"

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511

Informações sobre direitos autorais

Informações sobre marcas comerciais