



Guias de recursos do produto

How to enable StorageGRID in your environment

NetApp

December 11, 2024

This PDF was generated from <https://docs.netapp.com/pt-br/storagegrid-enable/product-feature-guides/create-cloud-storage-pool-aws-google-cloud.html> on December 11, 2024. Always check docs.netapp.com for the latest.

Índice

- Guias de recursos do produto 1
 - Crie o Cloud Storage Pool para AWS ou Google Cloud 1
 - Criar Cloud Storage Pool para Azure Blob Storage 1
 - Use um Cloud Storage Pool para backup 2
 - Configurar o serviço de integração de pesquisa StorageGRID 3
 - Clone de nó 19
 - Como utilizar o remapeamento de portas 22
 - Procedimento de realocação do local da grade e mudança de rede em todo o local 33
 - Migração de storage baseado em objetos do ONTAP S3 para o StorageGRID 38

Guias de recursos do produto

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.

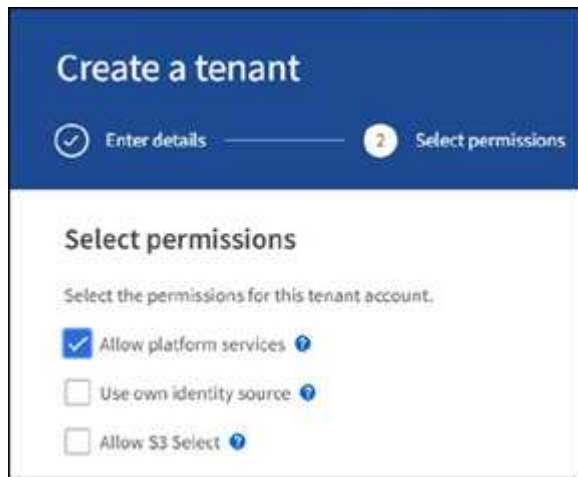
Os serviços de plataforma são configurados pelo locatário do S3 por meio da IU do Tenant Manager. Para obter mais informações, "[Considerações sobre o uso de serviços de plataforma](#)" consulte .

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 local](#) seção .



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:nnnnn: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:nnnnn: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

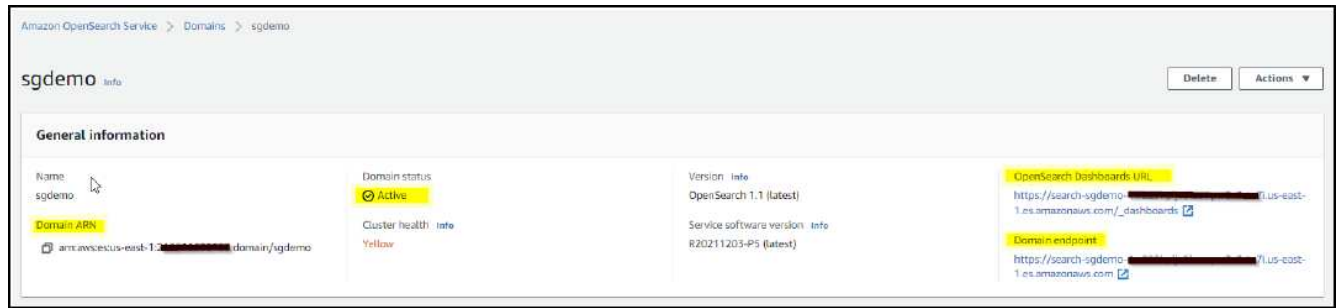
JSON

Import policy

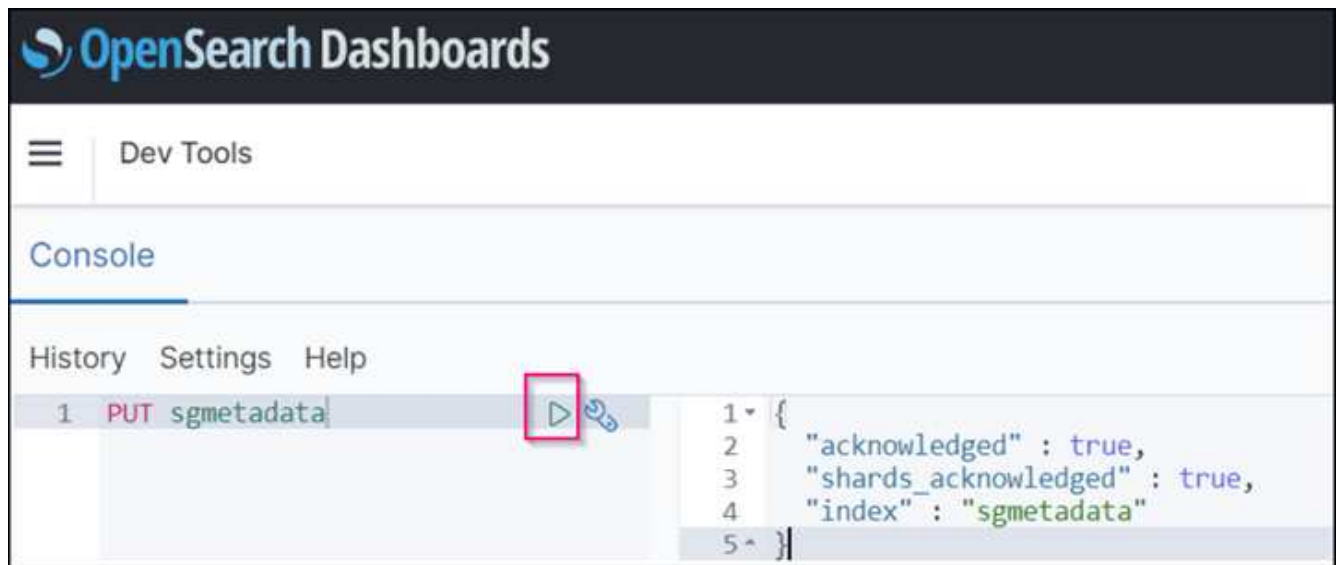
Access policy

```
3-   "Statement": [  
4-     {  
5-       "Effect": "Allow",  
6-       "Principal": {  
7-         "AWS": "arn:aws:iam::222222222222:user/ashwin"  
8-       },  
9-       "Action": "es:*",  
10-      "Resource": "arn:aws:es:us-east-1:222222222222:domain/sgdemo/*"  
11-    },  
12-    {  
13-      "Effect": "Allow",  
14-      "Principal": {  
15-        "AWS": "*"   
16-      },  
17-      "Action": [  
18-        "es:ESHttpPost"  
19-      ],  
20-      "Condition": {  
21-        "IpAddress": {  
22-          "aws:SourceIp": [  
23-            "216.239.59.0/24"  
24-          ]  
25-        }  
26-      },  
27-      "Resource": "arn:aws:es:us-east-1:222222222222:domain/sgdemo/*"  
28-    }  
  ]  
}
```

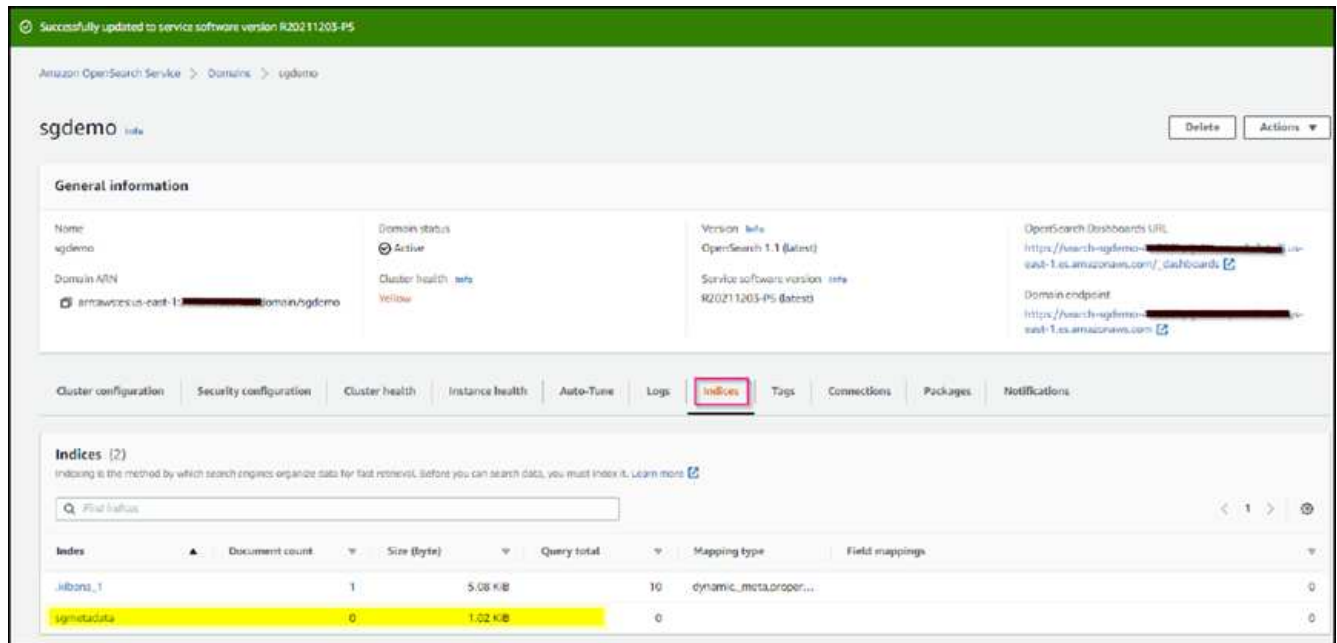

2. Aguarde de 15 a 20 minutos para que o domínio fique ativo.



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`.

Create endpoint

1 Enter details ————— 2 Select authentication type Optional ————— 3 Verify server Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name [?](#)

URI [?](#)

URN [?](#)

Cancel

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.

Create endpoint

Enter details
 2 Select authentication type Optional
 Verify server Optional

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Access Key ▼

Access key ID ?

AKIA[REDACTED]UWO

Secret access key ?

..... 👁

[Previous](#) [Continue](#)

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.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

1 endpoint [Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	aws-opensearch		Search	https://search-sgdemo-1-2021-11-01-1234567890.us-east-1.es.amazonaws.com/	arn:aws:es:us-east-1:2021-11-01:sgdemo/domain/sgdemo/sgmetadata/_doc

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.

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.



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.



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.

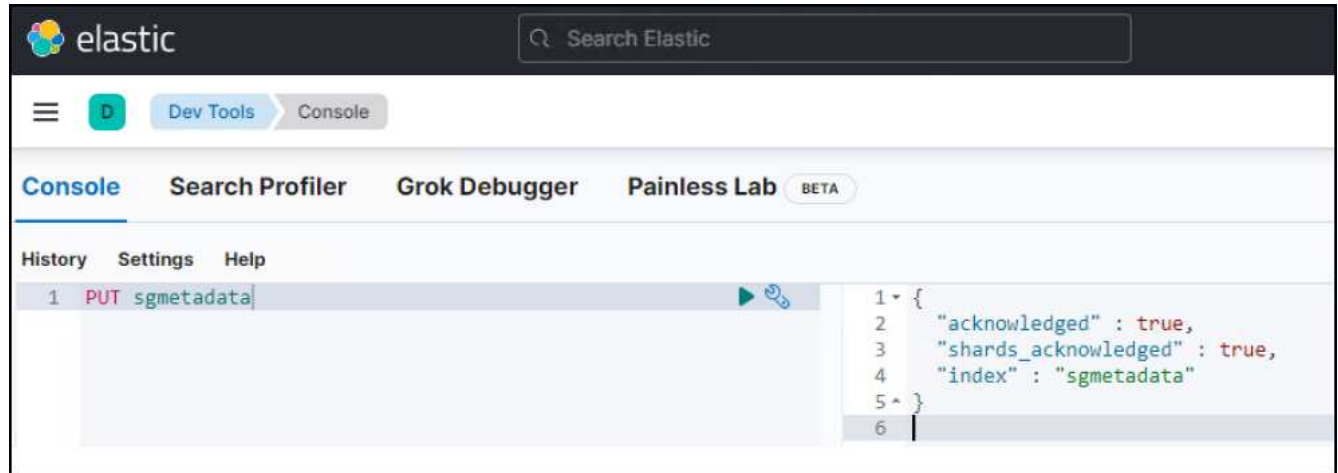
1. In a new terminal session, run:

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

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`

Create endpoint

1 Enter details — 2 Select authentication type Optional — 3 Verify server Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name [?](#)

URI [?](#)

URN [?](#)

Cancel [Continue](#)

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.

Authentication type [?](#)

Select the method used to authenticate connections to the endpoint.

Basic HTTP [v](#)

Username [?](#)

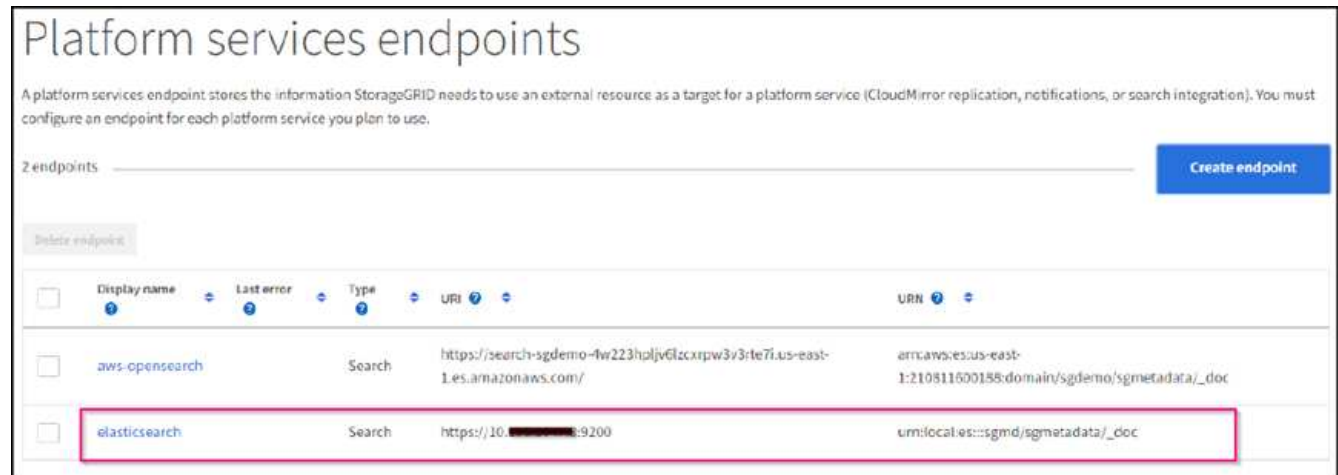
Password [?](#)

 [v](#)

Previous [Continue](#)

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.

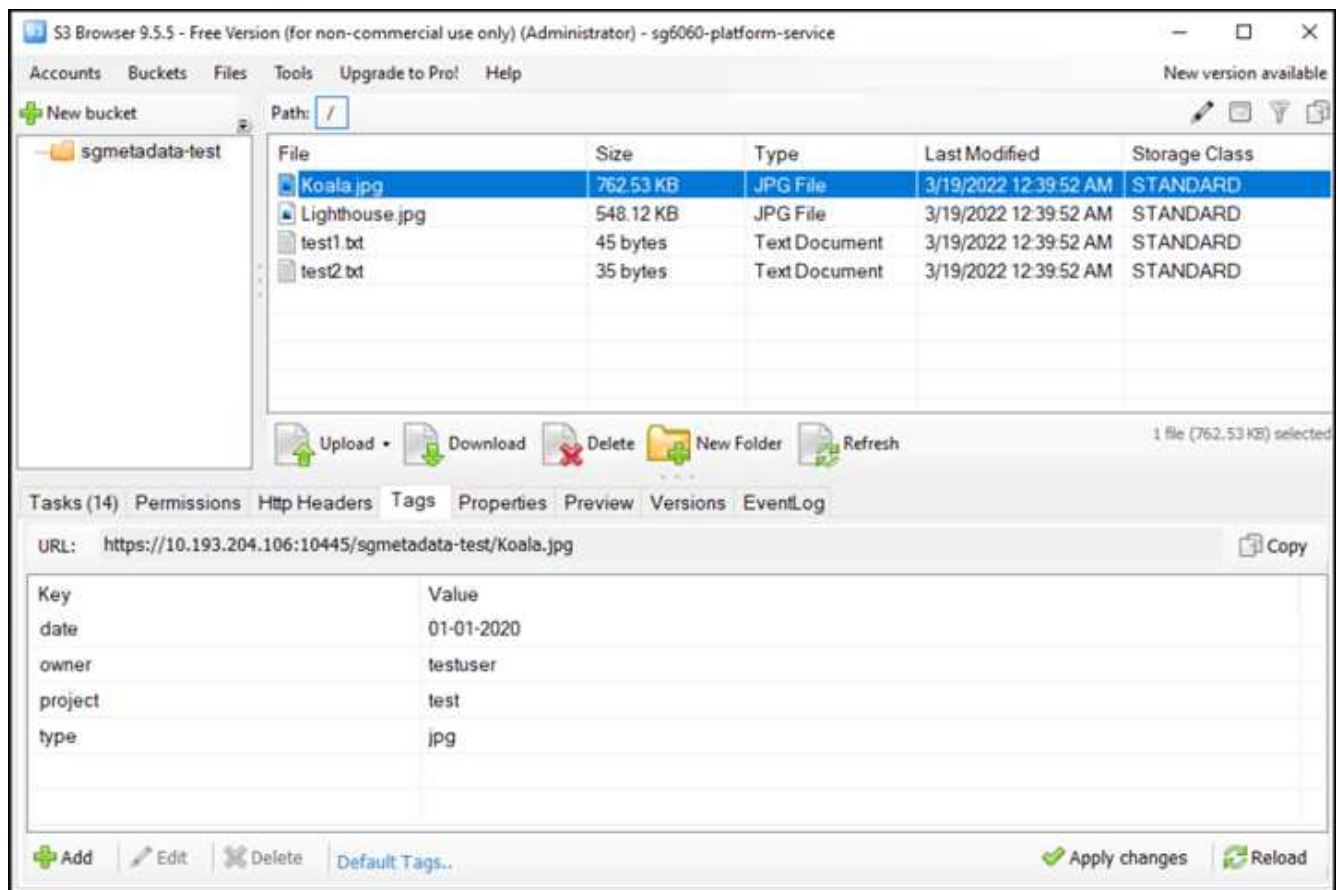
Neste exemplo, não usamos nenhum prefixo, o que significa que os metadados de cada objeto neste intervalo são enviados para o endpoint Elasticsearch definido anteriormente.

```

<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 conectar 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": { }
  }
}

```

```

1 GET sgmetadata/_search
2 {
3   "query": {
4     "match_all": { }
5   }
6 }

```

```

1 {
2   "took": 1,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": {
12      "value": 4,
13      "relation": "eq"
14    },
15    "max_score": 1.0,
16    "hits": [
17      {
18        "_index": "sgmetadata",
19        "_id": "sgmetadata-test_test1.txt",
20        "_score": 1.0,
21        "_source": {
22          "bucket": "sgmetadata-test",
23          "key": "test1.txt",
24          "accountId": "18656646746705016489",
25          "size": 45,
26          "md5": "36b194a8ac536f09a7061f024b97211e",
27          "region": "us-east-1",
28          "metadata": {
29            "s3b-last-modified": "20170429T010249Z",
30            "sha256": "6bf95e898615852c94fa701580d9a0399487f4cbe4429e1a1d7d7f427ab10f51"
31          },
32          "tags": {
33            "owner": "testuser",
34            "project": "test"
35          }
36        }
37      },
38      {
39        "_index": "sgmetadata",
40        "_id": "sgmetadata-test_Koala.jpg",
41        "_score": 1.0,
42        "_source": {
43          "bucket": "sgmetadata-test",
44          "key": "Koala.jpg",
45          "accountId": "18656646746705016489",
46          "size": 780831,
47          "md5": "2b04df3ecc1d94sfddff082d139c6f15",
48          "region": "us-east-1",
49          "metadata": {
50            "s3b-last-modified": "20190102T070949Z",
51            "sha256": "84adda0e4c52c469ace6e0c674a9144cd43eb2628c401c8b56b41242e2be4af1"
52          },
53          "tags": {
54            "date": "01-01-2020",
55            "owner": "testuser",
56            "project": "test",
57            "type": "jpg"
58          }
59        }
60      }
61    ]
62  }
63 }

```

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" }
      }
    }
  }
}

```

+

The screenshot shows the Elastic Search console interface. The top navigation bar includes 'elastic', 'Search Elastic', and various tool tabs like 'Dev Tools', 'Console', 'Search Profiler', 'Grok Debugger', and 'Painless Lab'. The main area is split into two panes. The left pane shows the search query being executed, which is highlighted with a red box:

```

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

```

The right pane displays the search results in JSON format. The response includes metadata such as 'took', 'timed_out', 'shards', and 'hits'. The 'hits' array contains two documents, each with a '_source' field containing detailed metadata and a 'tags' field with a 'type' of 'jpg'.

```

{
  "took": 1,
  "timed_out": false,
  "shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 2,
    "value": 2,
    "relation": "eq"
  },
  "max_score": 0.18232156,
  "hits": [
    {
      "_index": "sgmetadata",
      "_id": "sgmetadata-test_koala.jpg",
      "_score": 0.18232156,
      "_source": {
        "bucket": "sgmetadata-test",
        "key": "Koala.jpg",
        "accountId": "18656646746705016489",
        "size": 788831,
        "md5": "2b84df3ecc1d94af0dff882d139c6f15",
        "region": "us-east-1",
        "metadata": {
          "s3b-last-modified": "20190102T070049Z",
          "sha256": "84a4da0e4c52c409ace6a0c674a9144cd43eb2628c001c0b56b4124e2be4af1"
        },
        "tags": [
          {
            "date": "01-01-2020",
            "owner": "testuser",
            "project": "test",
            "type": "jpg"
          }
        ]
      }
    },
    {
      "_index": "sgmetadata",
      "_id": "sgmetadata-test_lighthouse.jpg",
      "_score": 0.18232156,
      "_source": {
        "bucket": "sgmetadata-test",
        "key": "Lighthouse.jpg",
        "accountId": "18656646746705016489",
        "size": 561270,
        "md5": "8969288f4245120e7c3870287cce0ff3",
        "region": "us-east-1",
        "metadata": {
          "s3b-last-modified": "20090714T053221Z",
          "sha256": "ffb6372ca435196075b8d8d29c98e9ccbe905d400ba057c0544fa001fa4d0e73"
        },
        "tags": [
          {
            "date": "02-02-2022",
            "owner": "testuser",
            "project": "test",
            "type": "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 de 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, conectando-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.

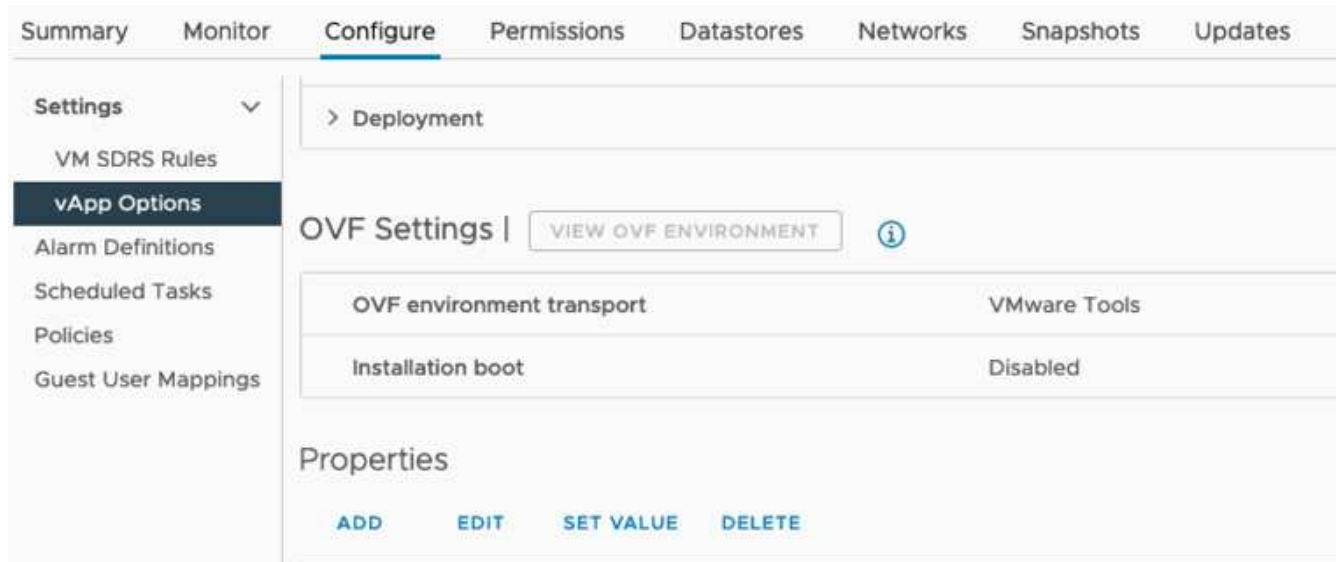
Implante o nó de gateway de substituição

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.

Edit property | Inbound port remapping specificati... X

General | **Type**

Static property

Type: String

User configurable:

Length: 0 - 65535

Default value: _____

Dynamic property

Macro: IP address

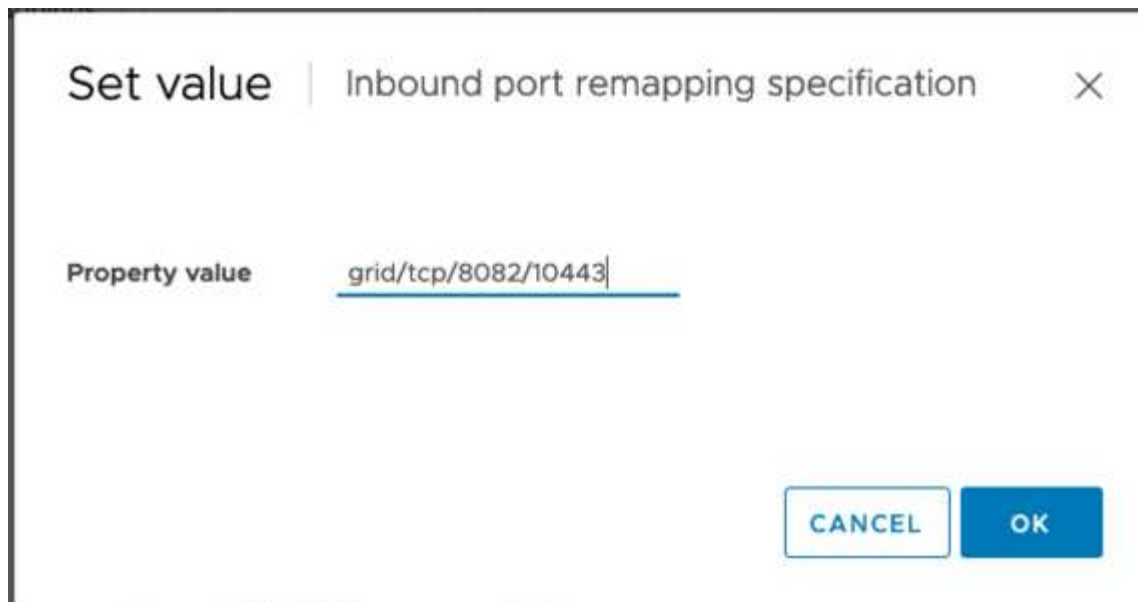
Network: MGMT_564

CANCEL SAVE

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.

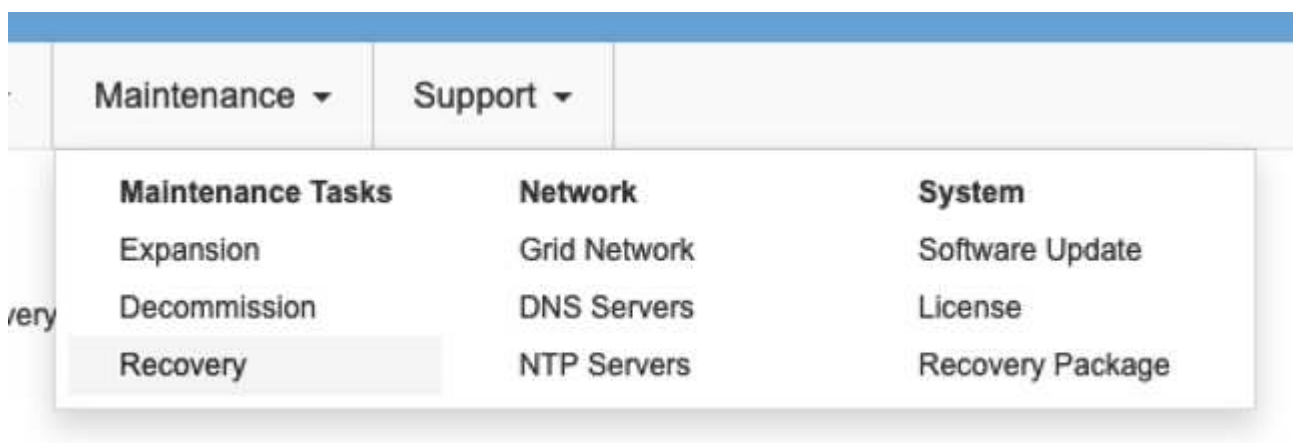


- Se você estiver usando várias redes, use uma vírgula (,) para separar as cadeias de rede, por exemplo, Grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

Recupere o nó de gateway

Para recuperar o Gateway Node, siga estas etapas:

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



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

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
No results found.			



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 registros 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`

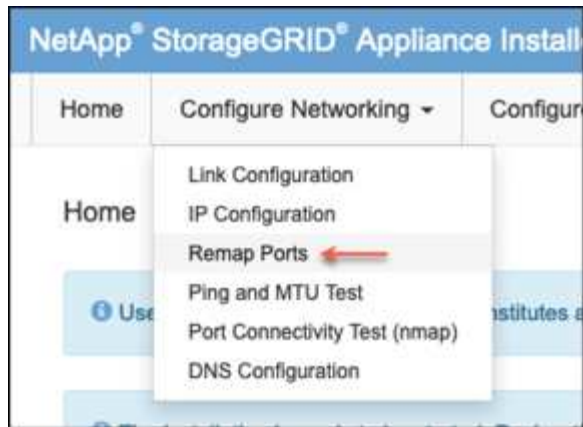
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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.
```

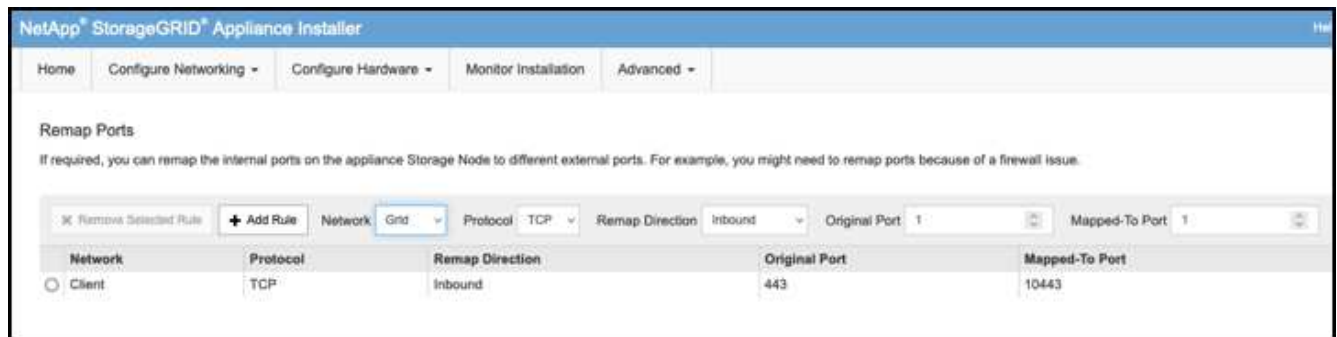
2. Após algum tempo, o aparelho reiniciará e você poderá acessar o nó PGE UI.
3. Navegue até Configurar rede



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 registros 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

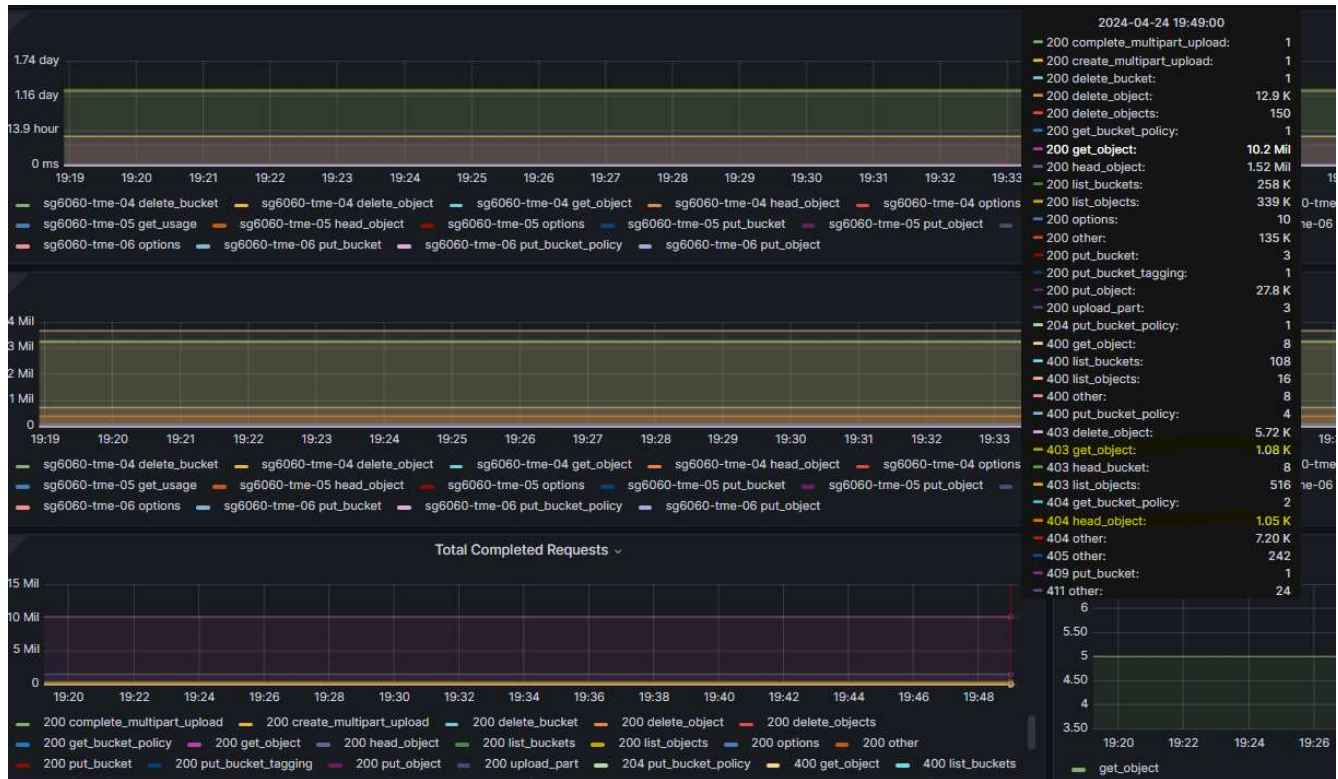
Este guia descreve a preparação e o procedimento para a realocação do local do StorageGRID em uma grade de vários locais. Você deve ter uma compreensão completa deste procedimento e Planejar com antecedência para garantir um processo suave e minimizar a interrupção para os clientes.

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

```

10.45.74.14 - PuTTY
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

Generating new grid networking description file... PASSED.
Running provisioning... PASSED.
Updating network configuration on LONDON-S1... PASSED.
Updating network configuration on LONDON-S2... PASSED.
Updating network configuration on LONDON-S3... PASSED.
Updating network configuration on LONDON-ADM1... PASSED.
Finished staging network changes. You must manually restart these nodes for the changes to take effect:

LONDON-ADM1 (has IP 10.45.74.14 until restart)
LONDON-S1 (has IP 10.45.74.16 until restart)
LONDON-S2 (has IP 10.45.74.17 until restart)
LONDON-S3 (has IP 10.45.74.18 until restart)

Importing bundles... PASSED.
*****
*                               *
*             IMPORTANT         *
*                               *
* A new recovery package has been generated as a result of the *
* configuration change. Select Maintenance > Recovery Package *
* in the Grid Manager to download it.                          *
*****

Network Update Complete. Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]>

```

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

```

Network Update Complete. Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]> a
Restart aborted. You must manually restart this node as soon as possible
Press Enter to return to the previous menu.

```

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 dispositivo](#) seção .
5. Encerre todos os nós e/ou dispositivos no local, rotule/remova as unidades de disco, se necessário, despenda, 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>:8443>o . 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 'shutdown -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>:8443>o . Confirme se o armazenamento está em ótimo estado e conectividade 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 conectividade, 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

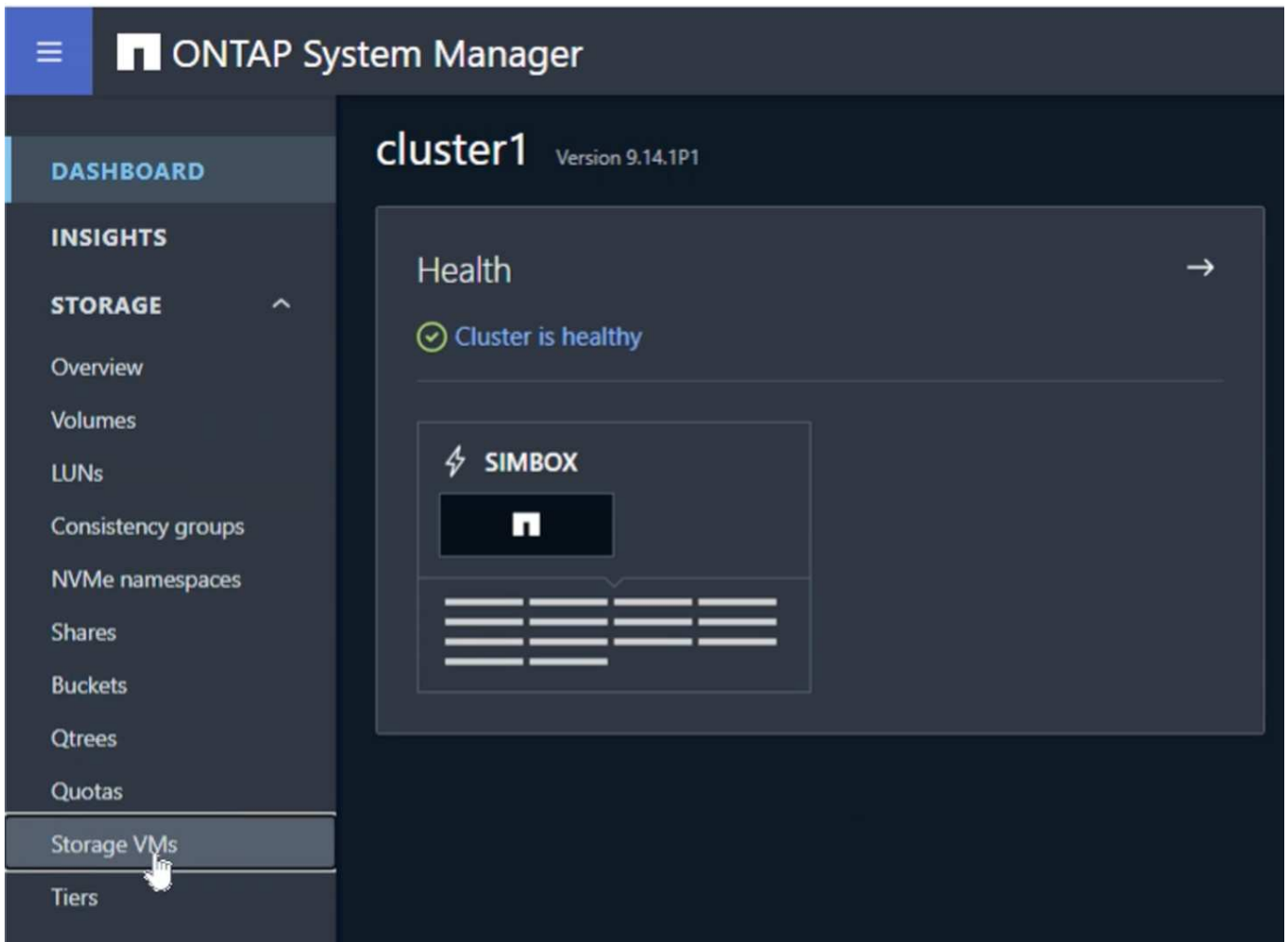
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

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.

Add storage VM



STORAGE VM NAME

svm_demo

Access protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Enable S3

S3 SERVER NAME

s3portal.demo.netapp.com

Enable TLS

PORT

443

CERTIFICATE

Use system-generated certificate

Use external-CA signed certificate

Use HTTP (non-secure)

PORT

8080

DEFAULT LANGUAGE

c.utf_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

onPrem-01

IP ADDRESS

192.168.0.200

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

Default

Storage VM administration

Enable maximum capacity limit

The maximum capacity that all volumes in this storage VM can allocate. [Learn More](#)

Manage administrator account

Save

Cancel

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


Added storage VM ✕

STORAGE VM
svm_demo


S3 SERVER NAME
s3portal.demo.netapp.com

User details

USER NAME
sm_s3_user

 The secret key won't be displayed again. Save this key for future use.

ACCESS KEY

34EH21411SMW1YOV3NQY

SECRET KEY
[Show secret key](#)



Download Close

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


Services

NIS

Not configured

Name service switch



Services lookup order 

HOSTS
Files, then DNS

GROUP
Files



NAME MAP
Files

NETGROUP
Files

DNS

Not configured

Defina o nome DNS e o IP.

Add DNS domain ✕

DNS domains

demo.netapp.com

+ Add

Name servers

192.168.0.253

+ Add

Cancel

Cancel **Save**

Crie o SVM S3 User

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

Protocols

NFS

Not configured



SMB/CIFS

Not configured



NVMe

Not configured



S3

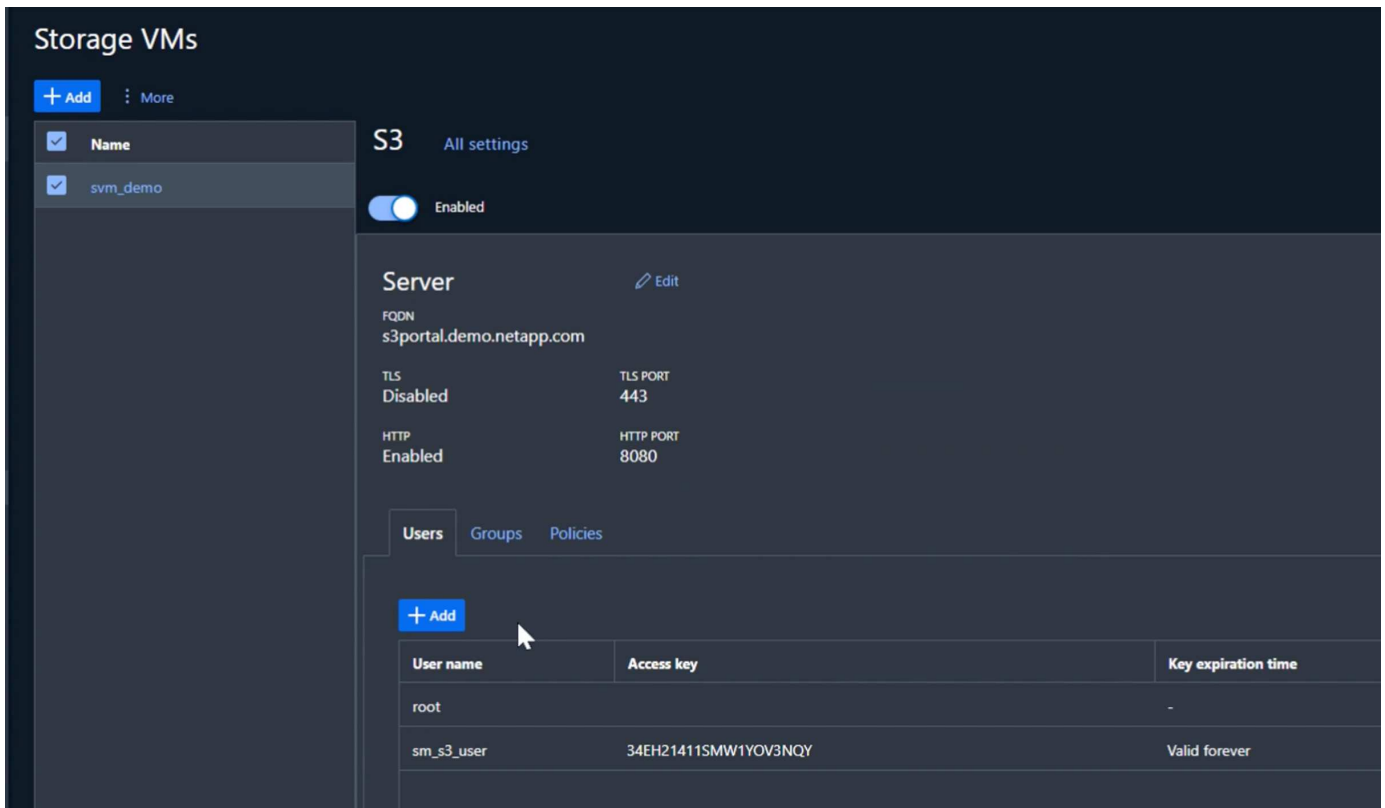
STATUS
✓ Enabled

TLS
Disabled

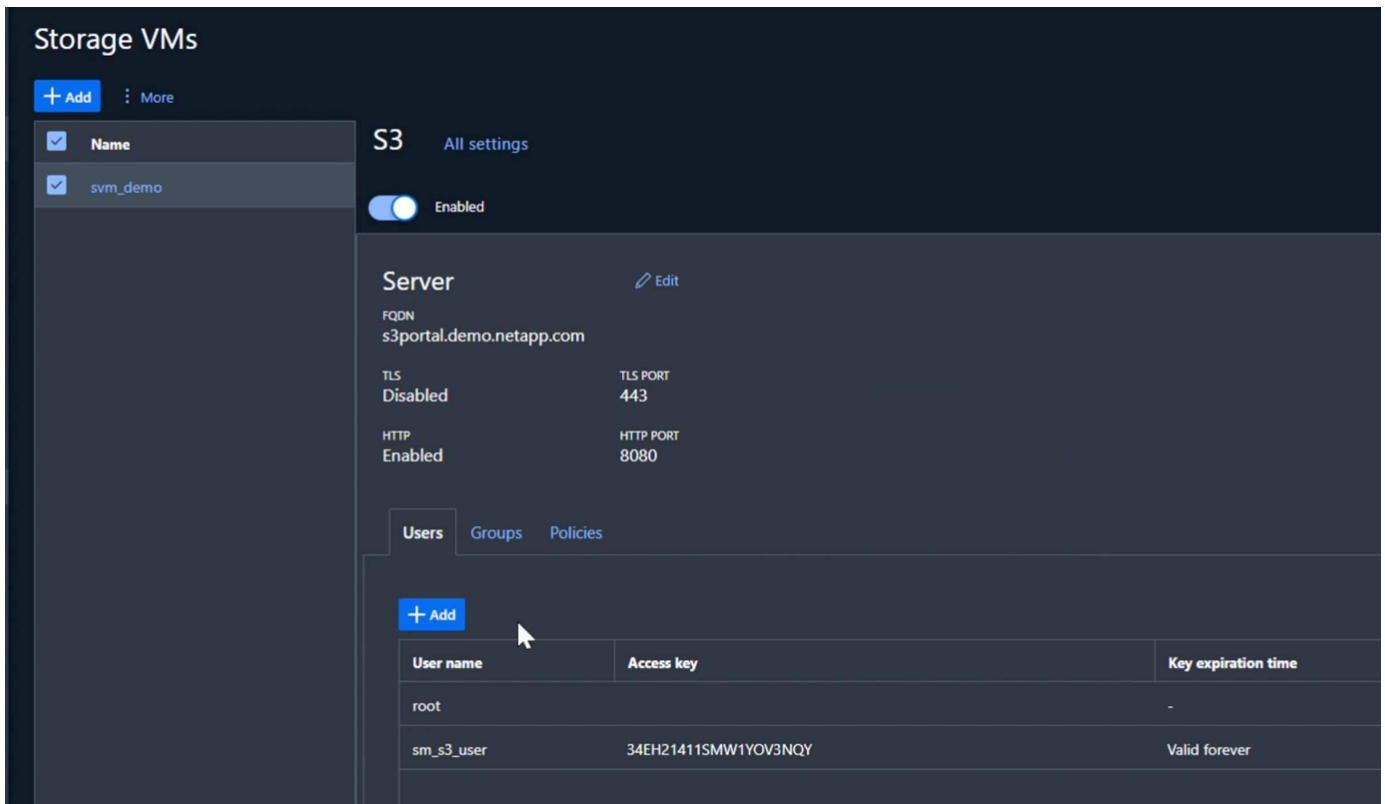
HTTP
Enabled



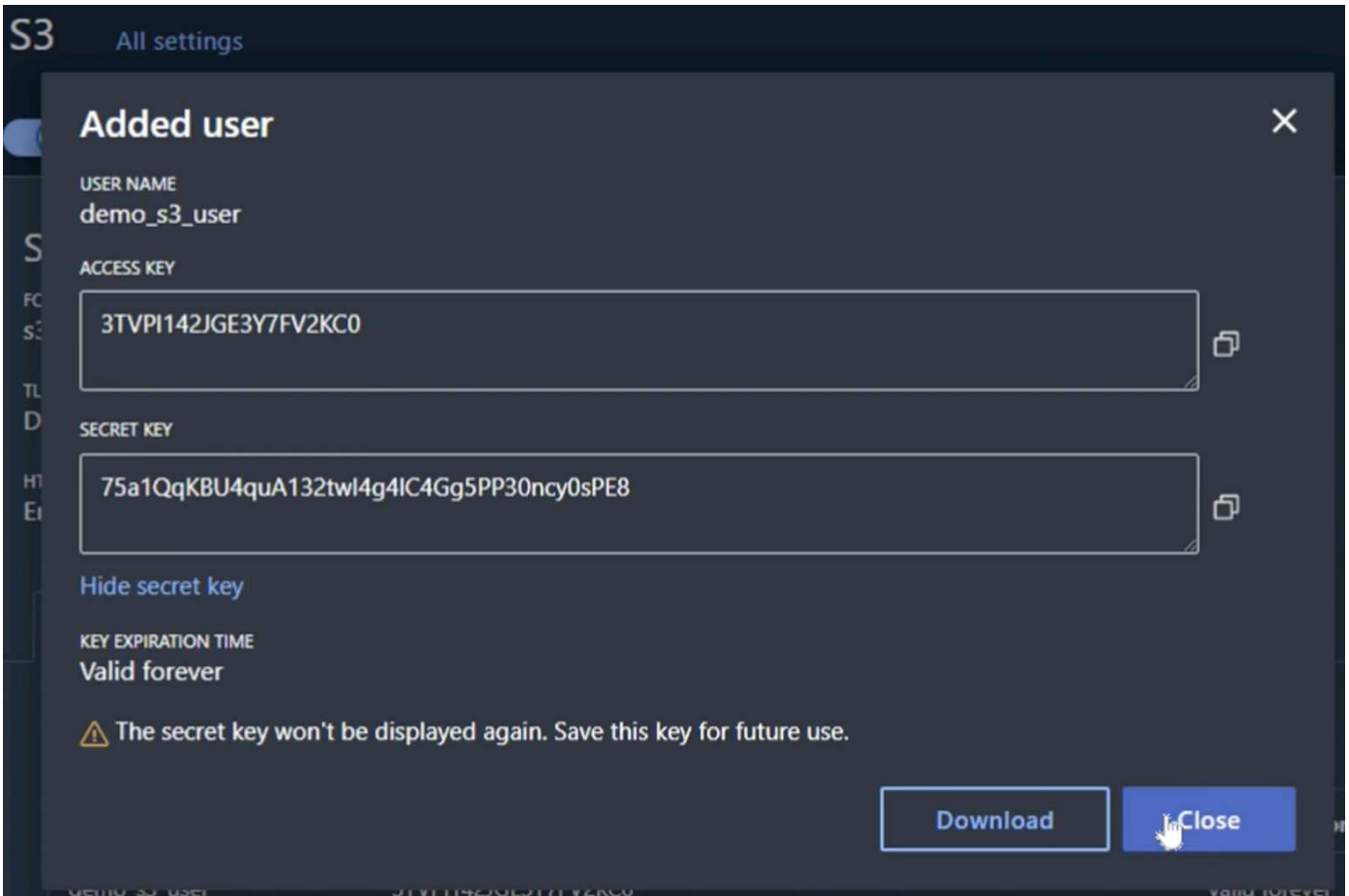
Adicionar um novo utilizador.



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.

Add group ✕

NAME

demo_s3_group

USERS

demo_s3_user ✕

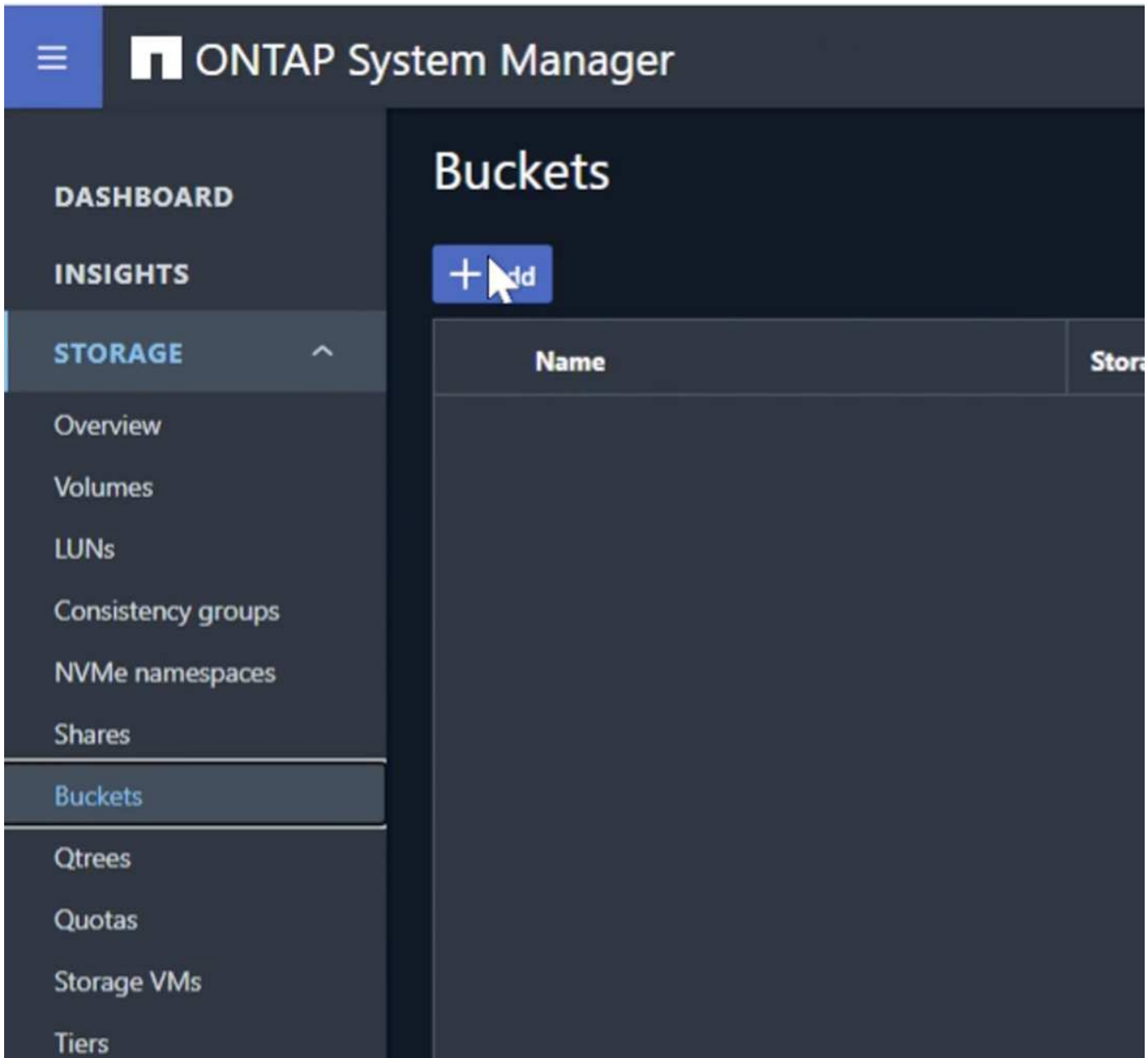
POLICIES

FullAccess ✕

Cancel Save

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".

Add bucket ✕

NAME

CAPACITY

100 GiB

Enable ListBucket access for all users on the storage VM "svm_demo".
Enabling this will allow users to access the bucket.

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

Add bucket



NAME

bucket

FOLDER (OPTIONAL)

Browse

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

100



GiB



Use for tiering

If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

Enable versioning

Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Extreme



Not sure? [Get help selecting type](#)

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).

Add bucket ✕

NAME

ontap-dummy

CAPACITY

100 ▲▼ GiB ▼

Enable ListBucket access for all users on the storage VM "svm_demo".
Enabling this will allow users to access the bucket.

More options Cancel Save

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

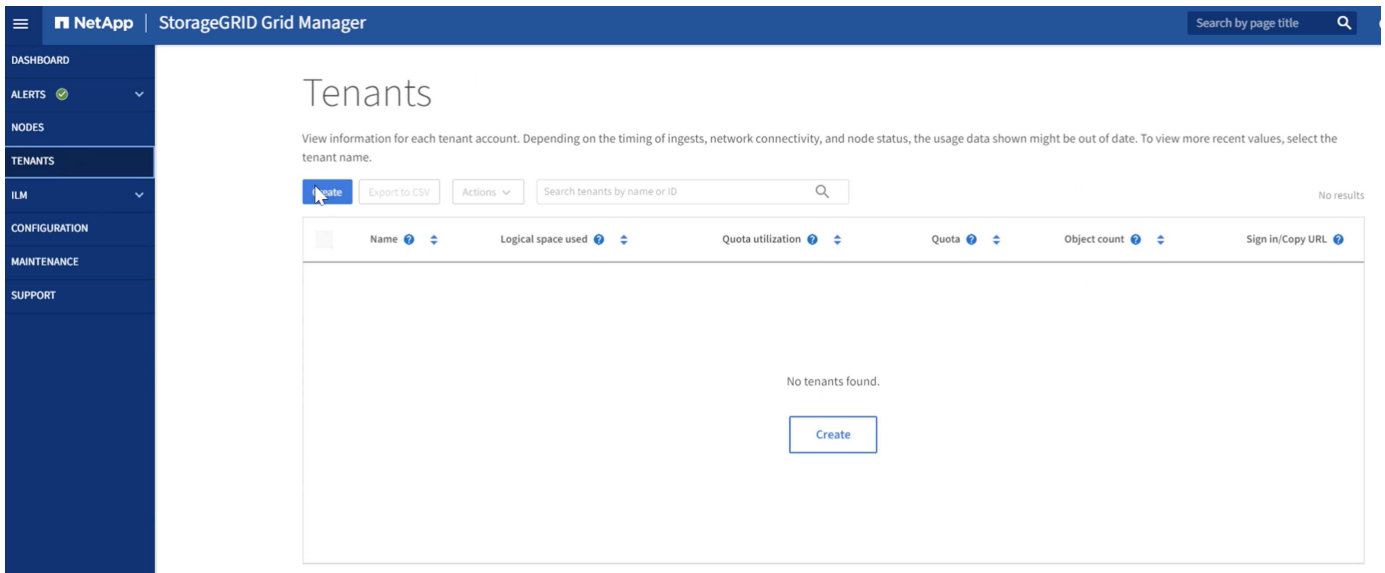
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

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.

Tenants

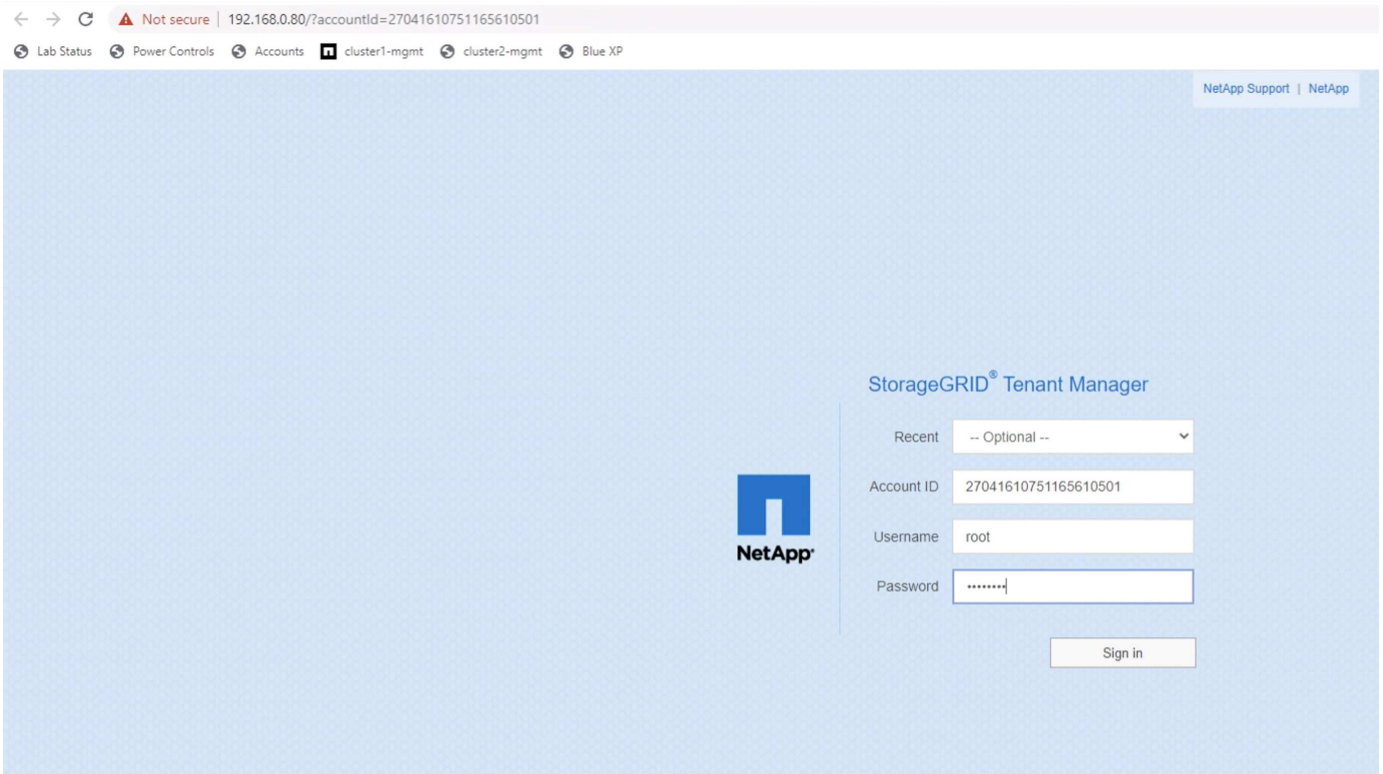
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Creating one result

<input type="checkbox"/>	Name ? ↕	Logical space used ? ↕	Quota utilization ? ↕	Quota ? ↕	Object count ? ↕	Sign in/Copy URL ?
<input type="checkbox"/>	tenant_demo	0 bytes	—	—	0	→ 📄

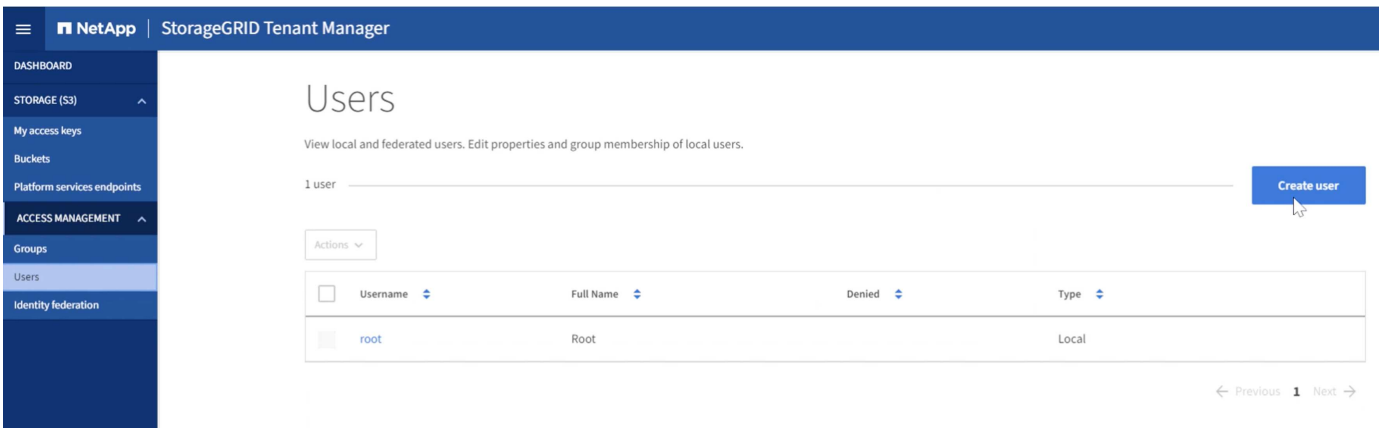
← Previous 1 Next →

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.



Enter user credentials

Create a new local user and configure user access.

Full name 

Must contain at least 1 and no more than 128 characters

Username 

Password

Must contain at least 8 and no more than 32 characters

Confirm password

Deny access

Do you want to prevent this user from signing in regardless of assigned group permissions?



Yes



No

[Cancel](#)

[Continue](#)

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.

Not secure | https://192.168.0.80/ui/#/users/ebc132e2-cfc3-42c0-a445-3b4465cb523c

Power Controls Accounts cluster1-mgmt cluster2-mgmt Blue XP

NetApp | StorageGRID Tenant Manager

Users > Demo S3 User

Overview

Full name: **Demo S3 User**

Username: **demo_s3_user**

User type: **Local**

Denied access: **Yes**

Access mode: **No Groups**

Group membership: **None**

[Password](#)
[Access](#)
[Access keys](#)
[Groups](#)

Change password

Change this user's password.

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

NetApp | StorageGRID Tenant Manager

DASHBOARD

STORAGE (S3)

My access keys

Buckets

Platform services endpoints

ACCESS MANAGEMENT

Groups

Users

Identity federation

Users

View local and federated users. Edit properties and group membership of local users.

2 users

Actions

<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	demo_s3_user	Demo S3 User	✓	Local

← Previous 1 Next →

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.

Create access key



1 Choose expiration time ————— 2 Download access key

Download access key

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

 You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

7CT7L1X5MIO5091E86TR



Secret access key

RIJnC5N5FX9RSWgFdj6SQ7wMrFRZYu5bQLdNQT0c



 Download .csv

Finish

Crie o grupo de segurança

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

Create group ✕

1 Choose a group type — 2 Manage permissions — 3 Set S3 group policy — 4 Add users Optional

Choose a group type ?

Create a new local group or import a group from the external identity source.

Local group **Federated group**

Create local groups to assign permissions to any local users you defined in StorageGRID.

Display name

Must contain at least 1 and no more than 32 characters

Unique name ?

[Cancel](#) [Continue](#)

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



Choose a group type

2

Manage permissions

3

Set S3 group policy

4

Add users
Optional

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions

Select the permissions you want to assign to this group.

Root access

Allows users to access all administration features. Root access permission supersedes all other permissions.

Manage all buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage endpoints

Allows users to configure endpoints for platform services.

Manage your own S3 credentials

Allows users to create and delete their own S3 access keys.

[Previous](#)

[Continue](#)

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/*"]
    }
  ]
}

```

Create group

Choose a group type — Manage permissions — **3 Set S3 group policy** — 4 Add users (Optional)

Set S3 group policy ?

An S3 group policy controls user access permissions to specific S3 resources, including buckets. Non-root users have no access by default.

- No S3 Access
- Read Only Access
- Full Access
- Custom (Must be a valid JSON formatted string.)

```

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

```

Previous **Continue**

Finalmente, adicione o usuário ao grupo e termine.

Create group

Choose a group type — Manage permissions — Set S3 group policy — 4 Add users Optional

Add users

(This step is optional. If required, you can save this group and add users later.)

Select local users to add to the group **Demo S3 Group**.

<input checked="" type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾
<input checked="" type="checkbox"/>	demo_s3_user	Demo S3 User	<input checked="" type="checkbox"/>

[Previous](#) **Create group**

Crie dois baldes

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

NetApp | StorageGRID Tenant Manager

Buckets

Create buckets and manage bucket settings.

0 buckets [Create bucket](#)

Actions ▾ [Experimental S3 Console](#)

Name ▾	Region ▾	Object Count ▾	Space Used ▾	Date Created ▾
No buckets found				

[Create bucket](#)

Defina o nome e a região do intervalo.

Create bucket

×

1 Enter details ————— 2 Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

[Cancel](#) [Continue](#)

Neste primeiro bucket, ative o controle de versão.

Create bucket

×

✓ Enter details ————— 2 Manage object settings
Optional

Manage object settings Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

Enable object versioning

[Previous](#) [Create bucket](#)

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

Create bucket ×

1 Enter details 2 Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

Cancel

Continue

Não ative o controle de versão neste segundo bucket.

Create bucket ×

✓ Enter details 2 Manage object settings
Optional

Manage object settings Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

Enable object versioning

Previous

Create 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 conectar ao seu sistema ONTAP.

Add New Account online help

 **Add New Account**
Enter new account details and click Add new account

Display name:

Assign any name to your account.

Account type:

Choose the storage you want to work with. Default is Amazon S3 Storage.

REST Endpoint:

Specify S3-compatible API endpoint. It can be found in storage documentation. Example: rest.server.com:8080

Access Key ID:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Secret Access Key:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

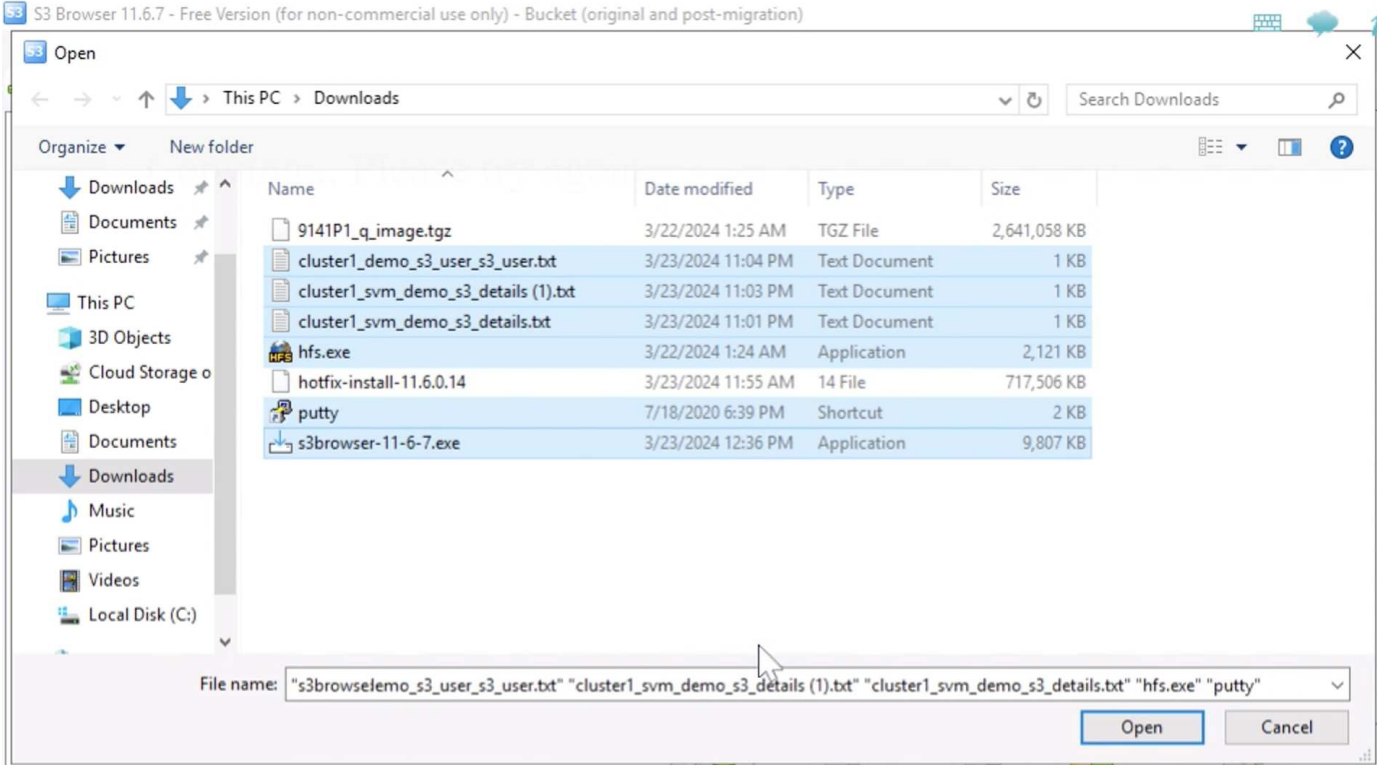
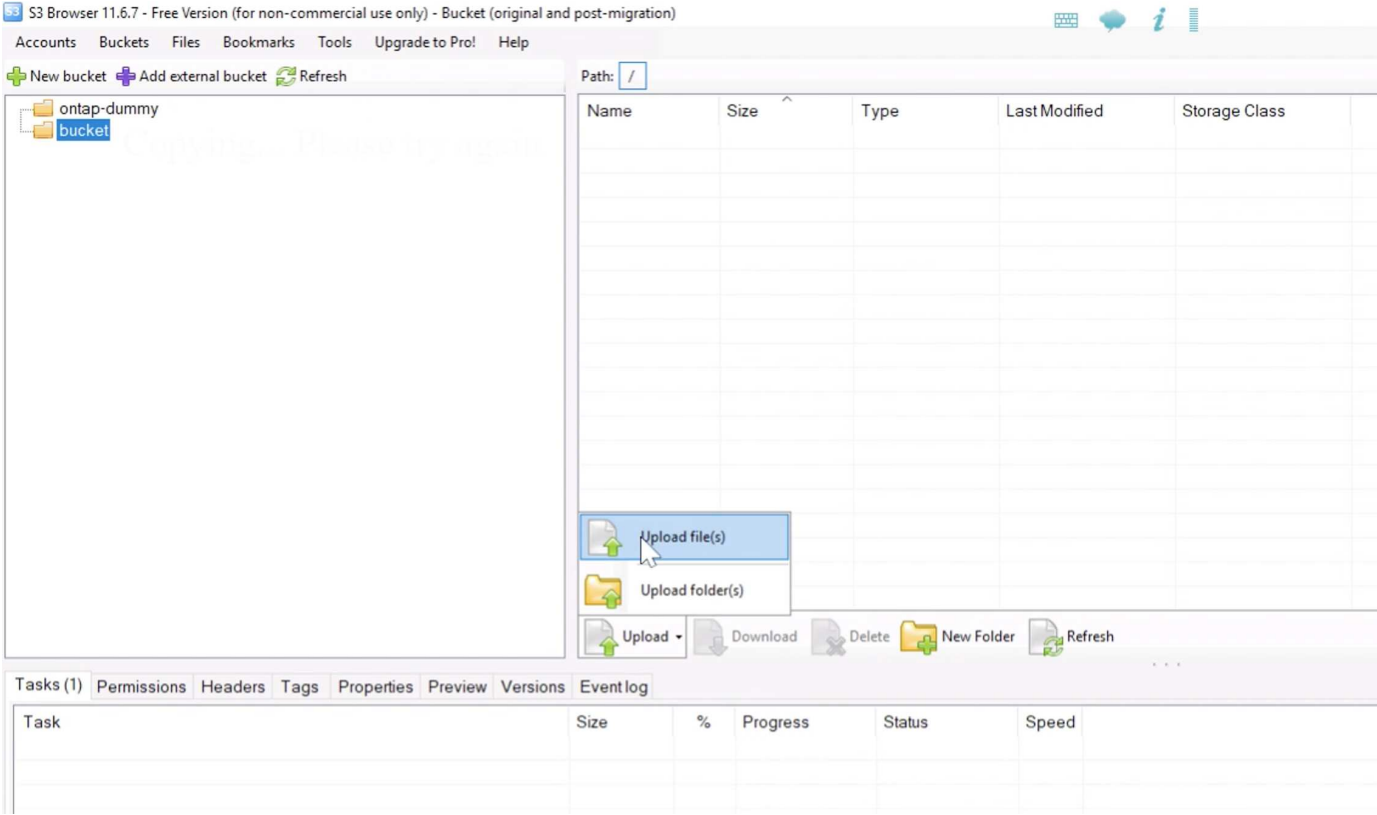
Encrypt Access Keys with a password:

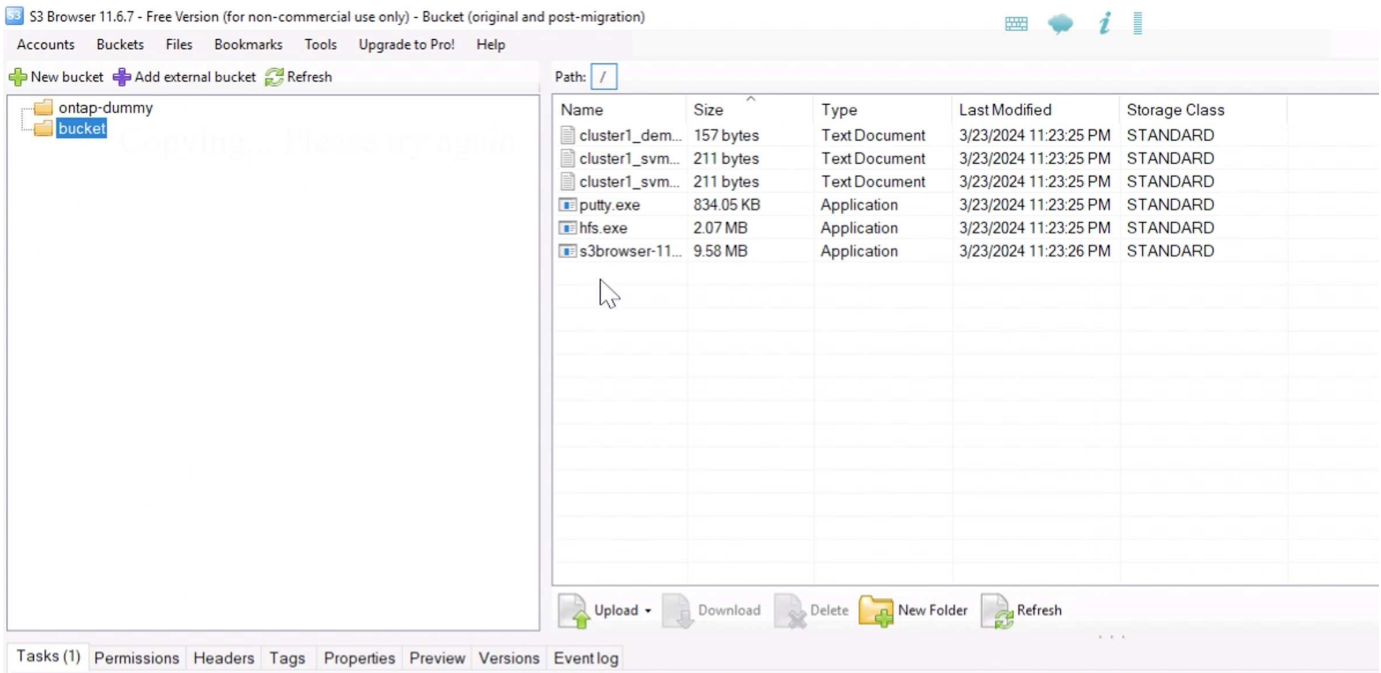
Turn this option on if you want to protect your Access Keys with a master password.

Use secure transfer (SSL/TLS)
If checked, all communications with the storage will go through encrypted SSL/TLS channel

[advanced settings..](#)

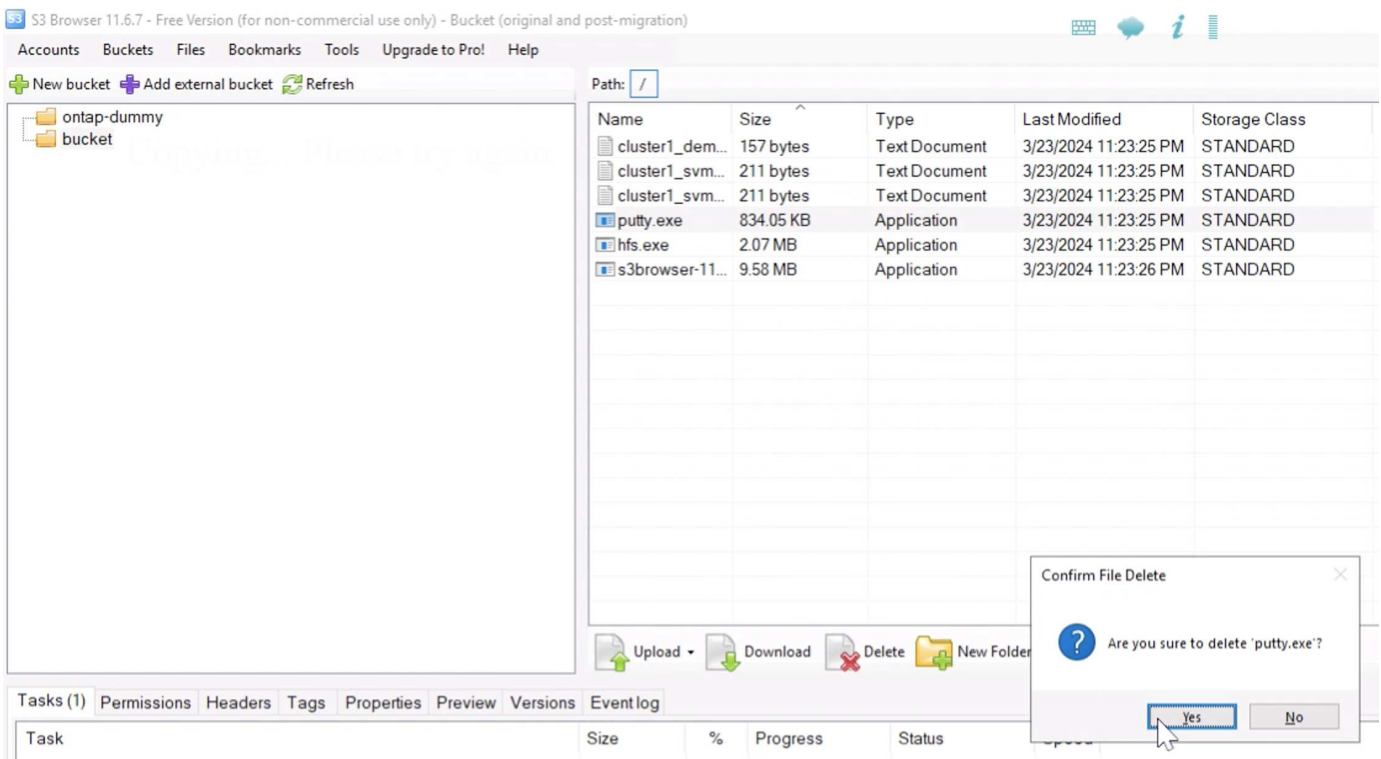
Agora permite carregar alguns arquivos para o bucket habilitado para versionamento.



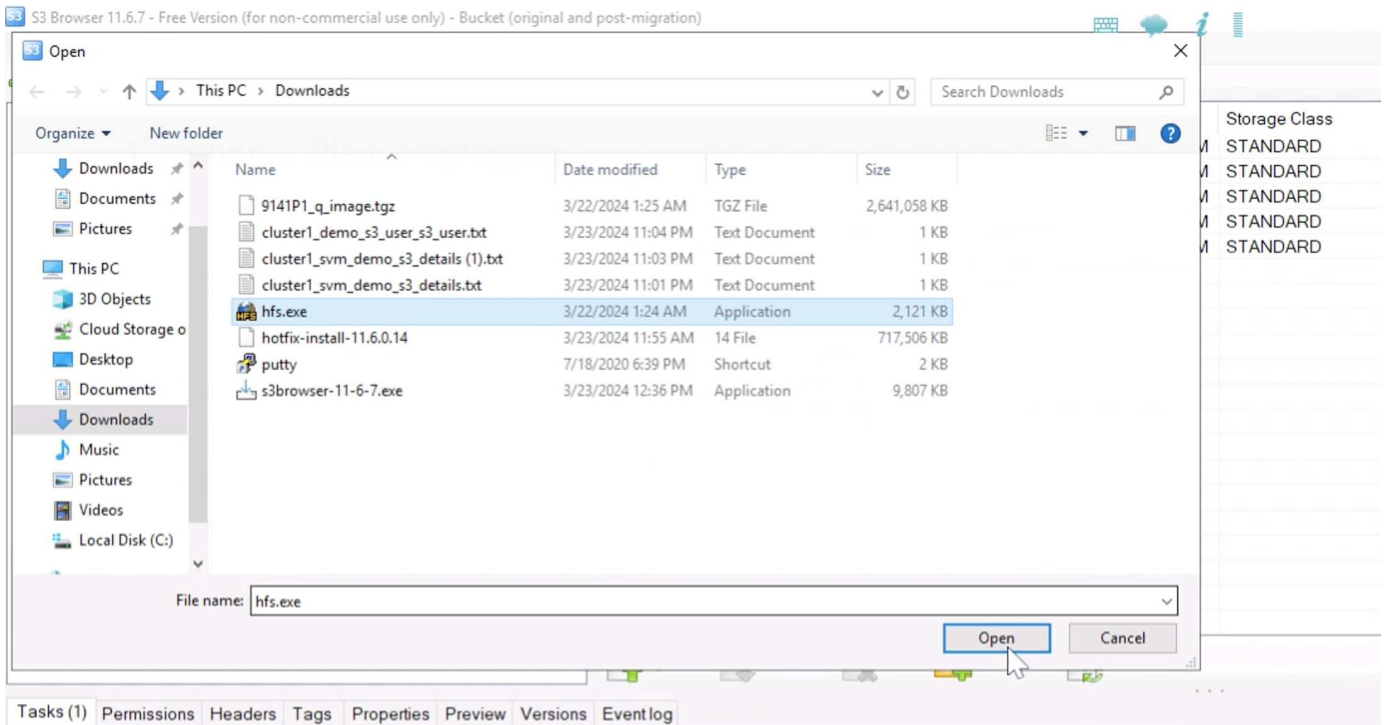


Agora vamos criar algumas versões de objetos no bucket.

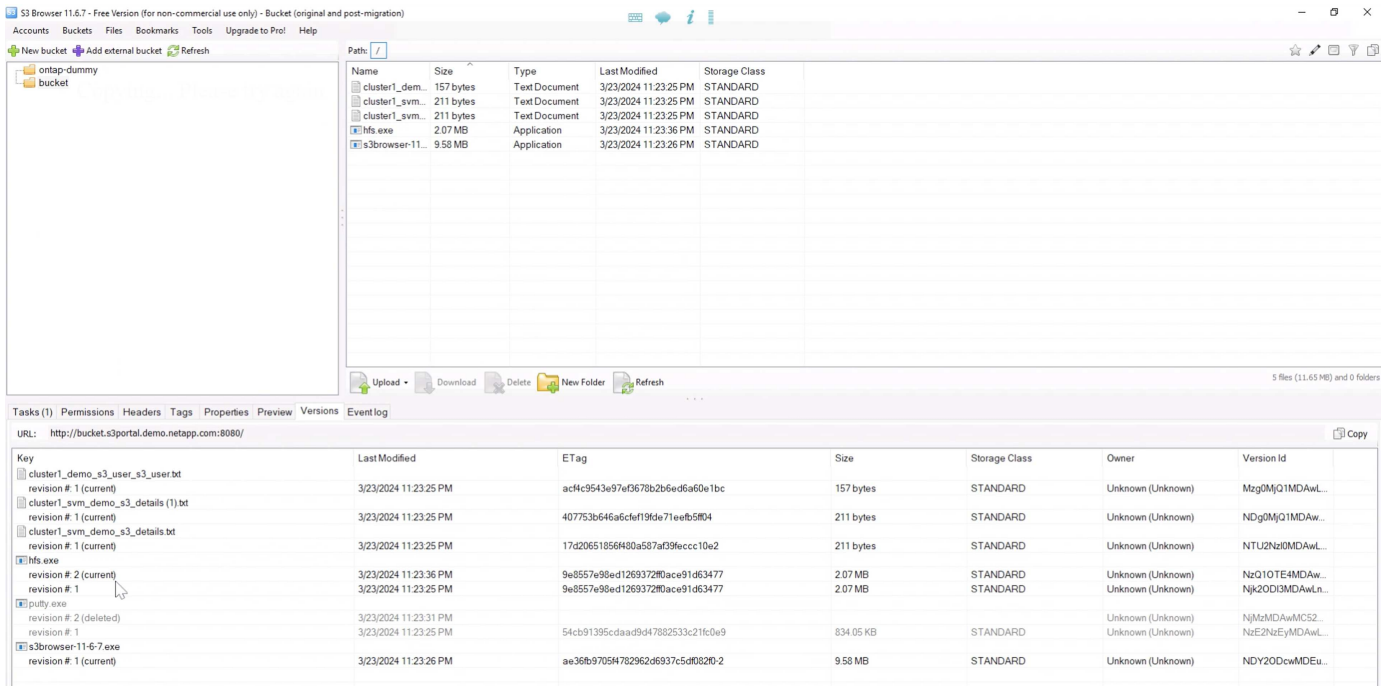
Eliminar um ficheiro.



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



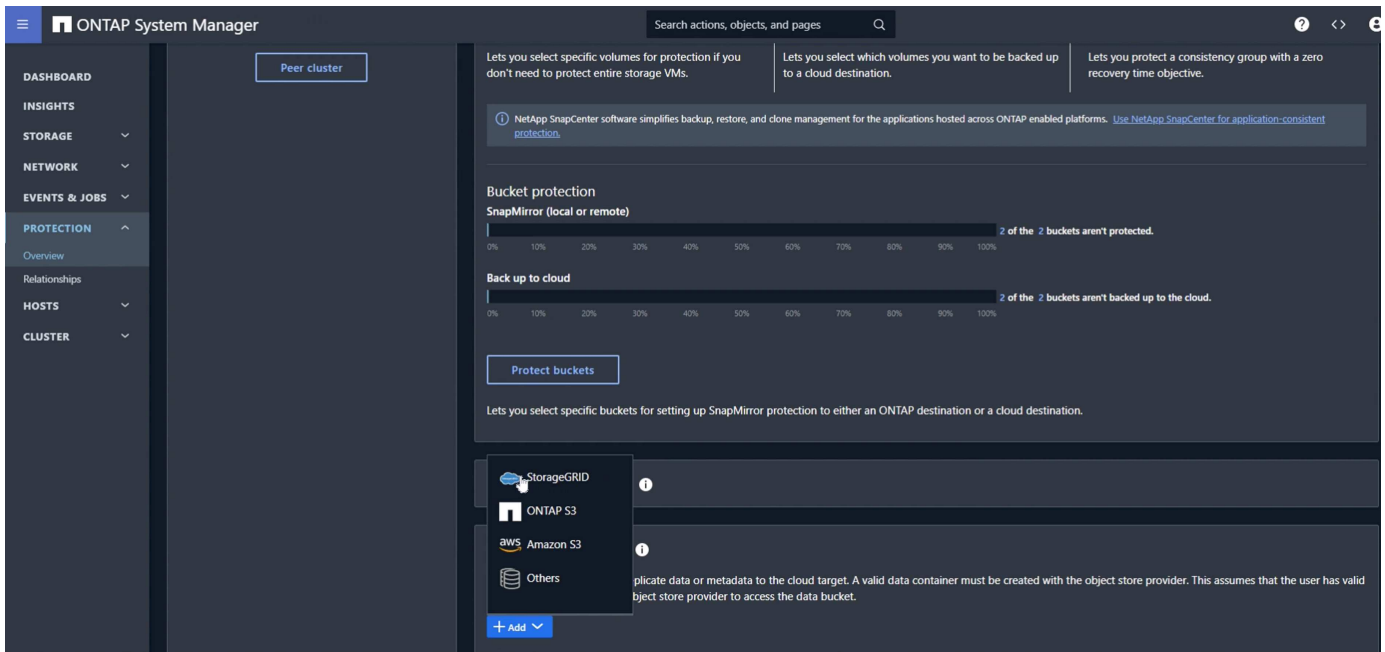
Em S3Browser podemos ver as versões dos objetos que acabamos de criar.



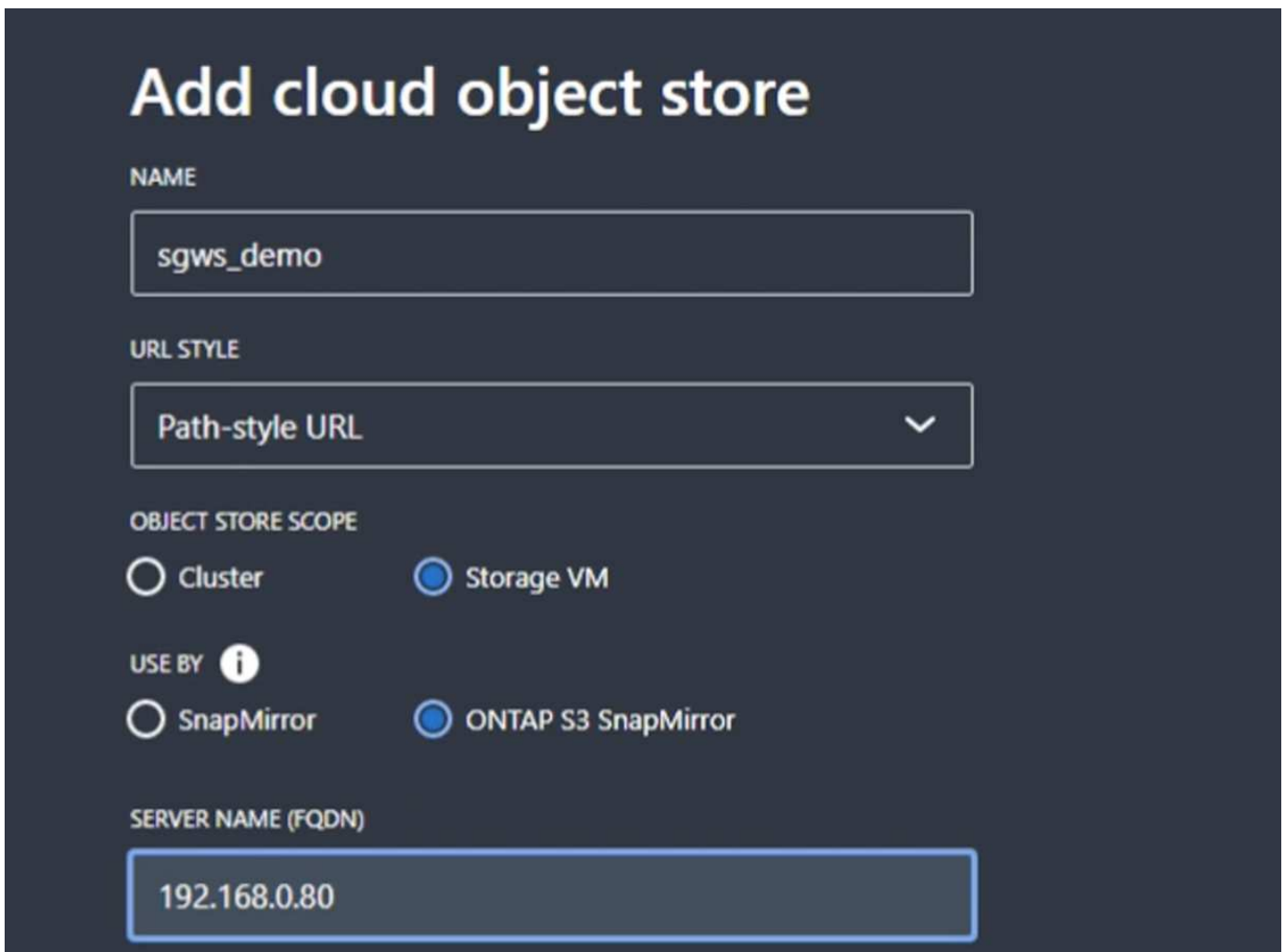
Estabeleça a relação de replicação

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-style). 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.

ACCESS KEY
7CT7L1X5MIO5091E86TR

SECRET KEY
.....

CONTAINER NAME ⓘ
bucket

Network for cloud object store

Considerations

NODE	IP ADDRESS	SUBNET MASK	BROADCAST DOMAIN	GATEWAY
onPrem-01	192.168.0.113	24	Default	192.168.0.1

Use HTTP proxy

Save Cancel

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).

ONTAP System Manager

Back up to cloud
2 of the 2 buckets aren't backed up to the cloud.

Protect buckets

Lets you select specific buckets for setting up SnapMirror protection to either an ONTAP destination or a cloud destination.

Local policy settings ⓘ

Protection policies

Applicable when this cluster is the destination

- Asynchronous
At 5 minutes past the hour, every hour
- AutomatedFailOver
No schedules
- CloudBackupDefault
No schedules
- Continuous
No schedules

Snapshot policies

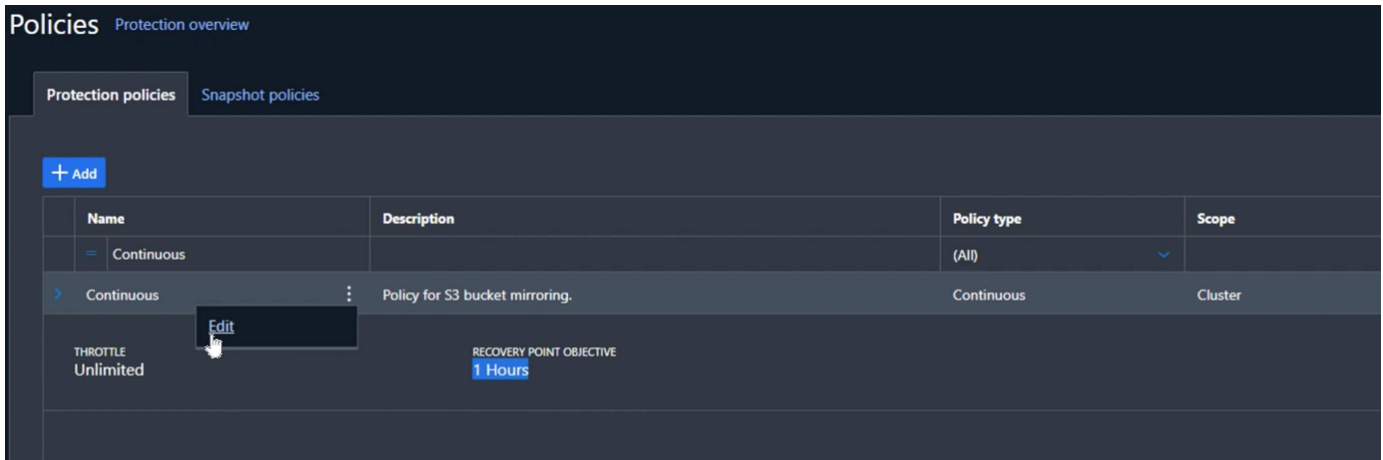
Applicable when this cluster is the source or wh...

- default
3 Schedules
- default-1weekly
3 Schedules
- none
No schedules

Schedules

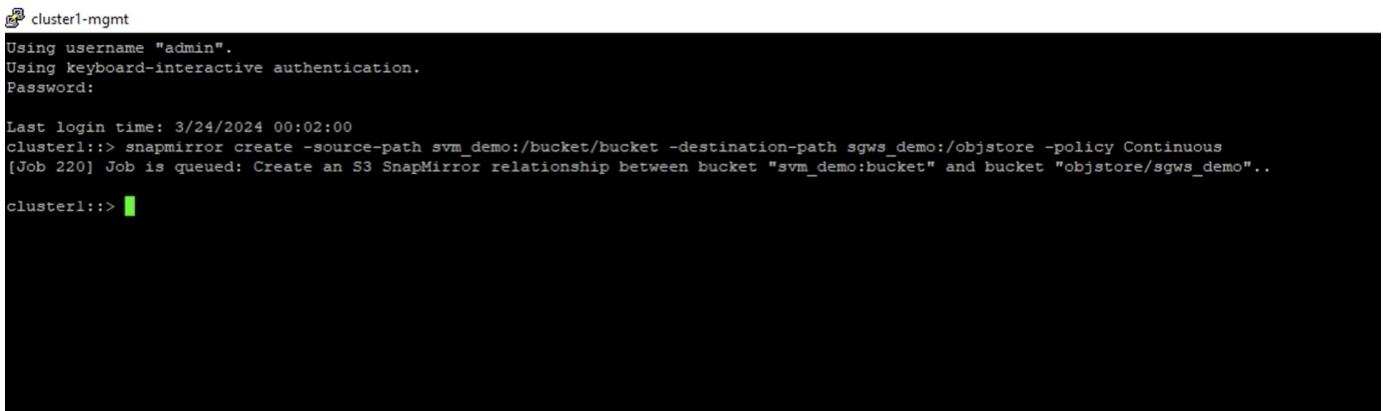
- 5min
At 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, and 55 minutes past the hour, every hour
- 6-hourly
At 12:15 AM, 06:15 AM, 12:15 PM and 06:15 PM, every day
- 8hour
At 02:15 AM, 10:15 AM and 06:15 PM, every day
- 10min
- 12-hourly

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

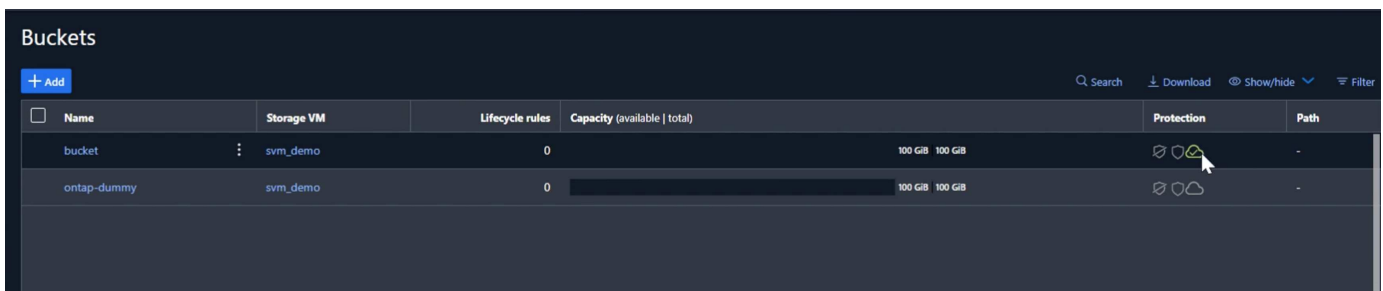


Agora podemos configurar o SnapMirror para replicar o bucket.

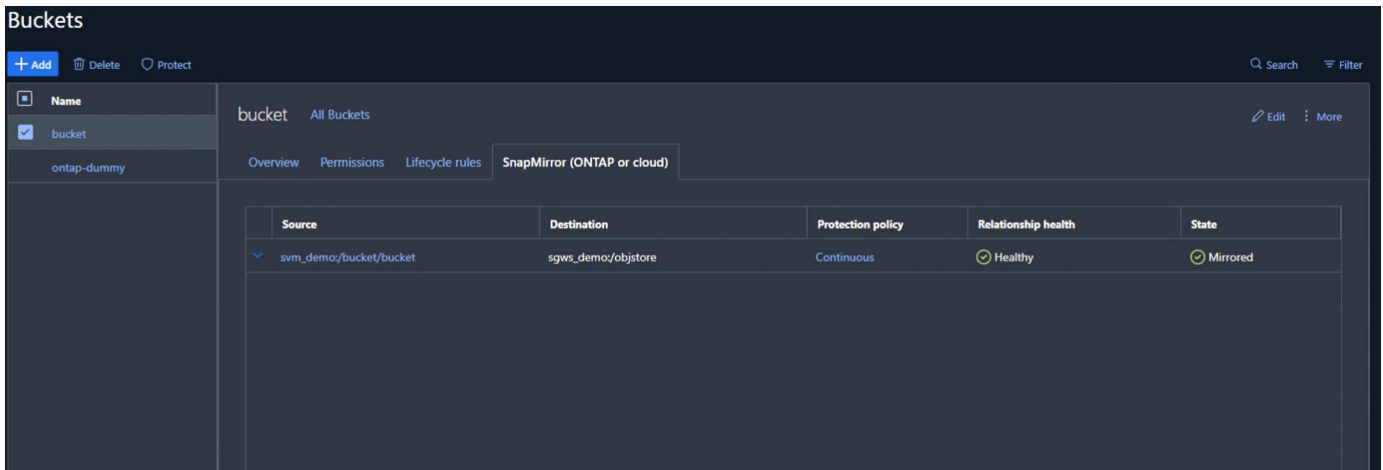
```
SnapMirror create -source-path sv_demo: /Bucket/bucket -destination-path sgws_demo: /Objstore -policy contínuo
```



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

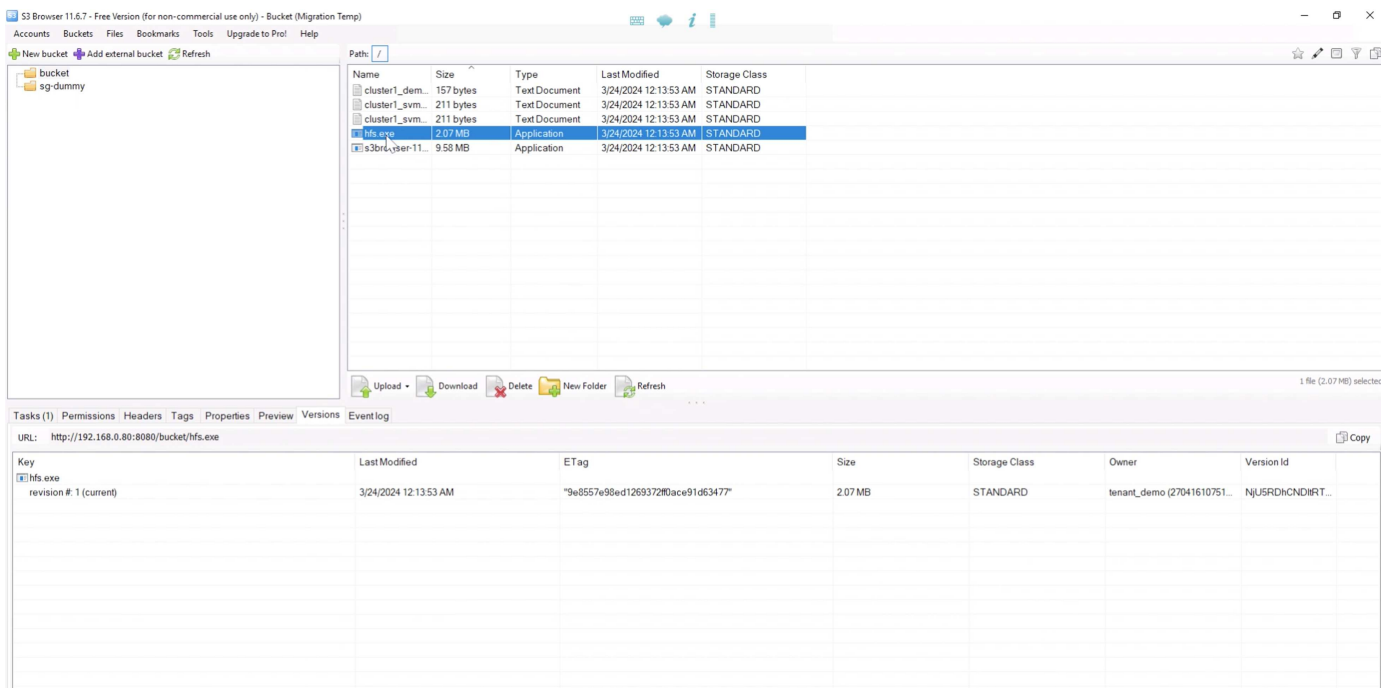


Se selecionarmos o bucket e irmos para a guia "SnapMirror (ONTAP ou nuvem)", veremos o status do SnapMirror Repationship.

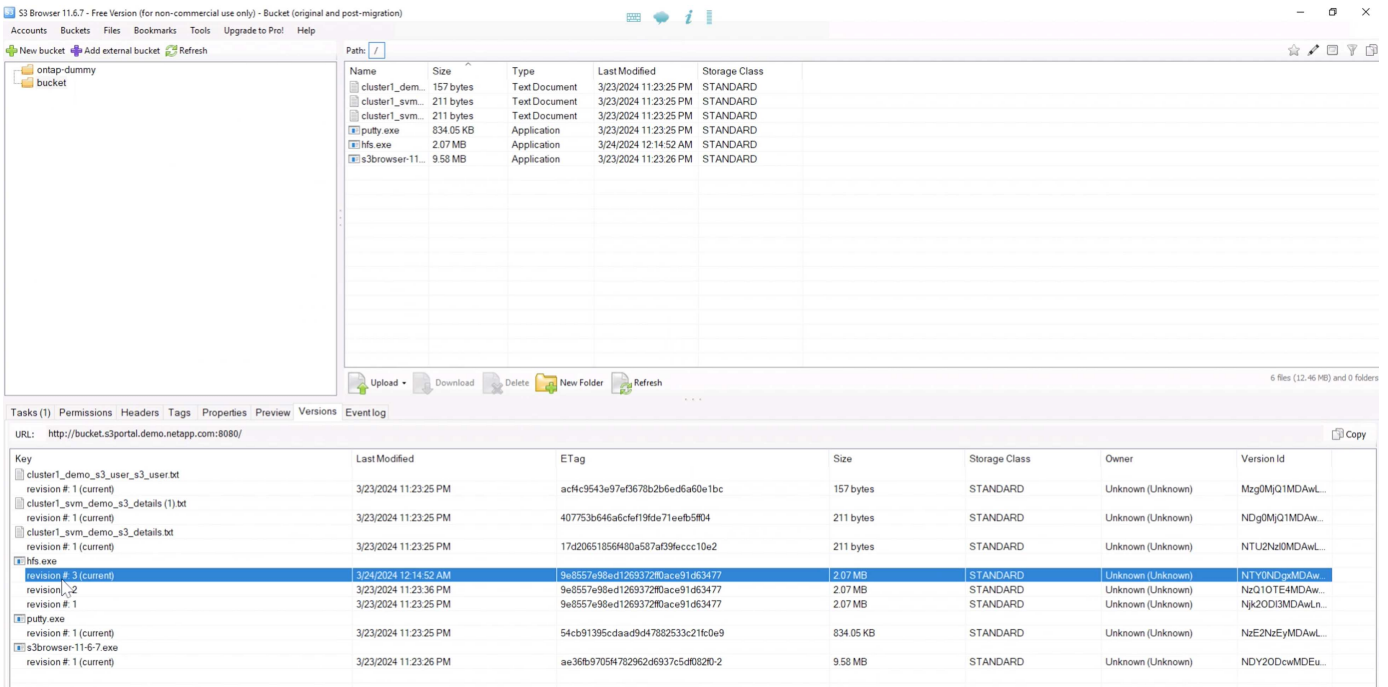


Os detalhes da replicação

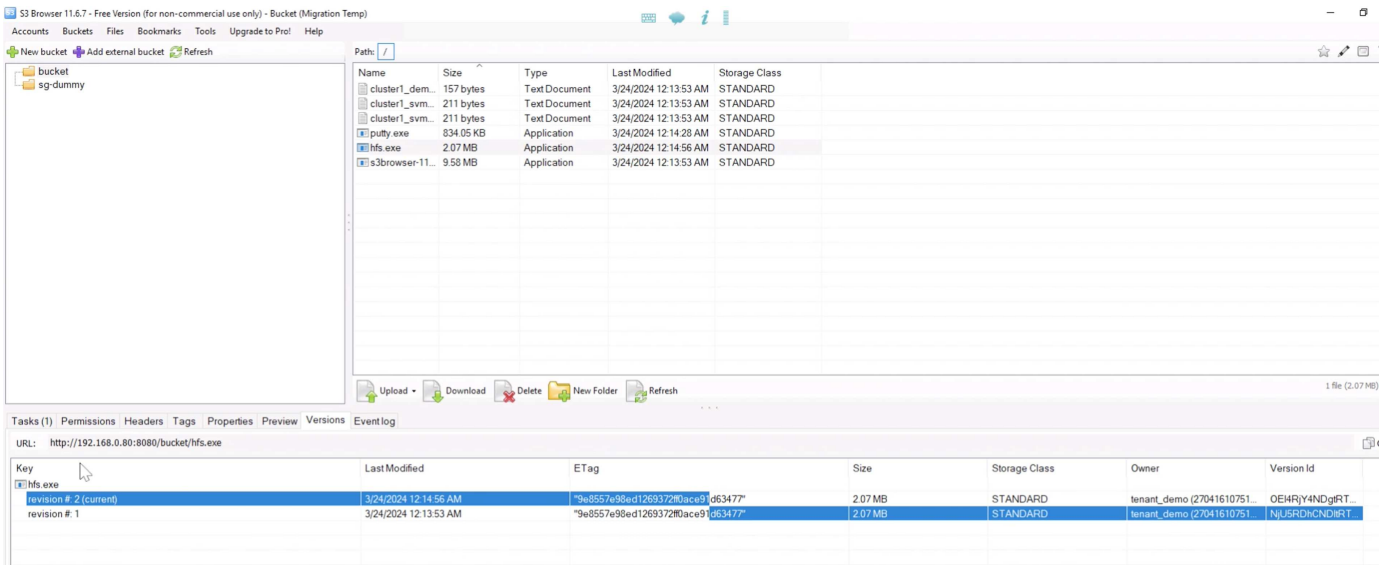
Agora temos um bucket replicando com sucesso do ONTAP para o StorageGRID. Mas o que está realmente replicando? Nossa origem e destino são ambos buckets versionados. As versões anteriores também replicam para o destino? Se olharmos para o nosso bucket do StorageGRID com S3Browser, veremos que as versões 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

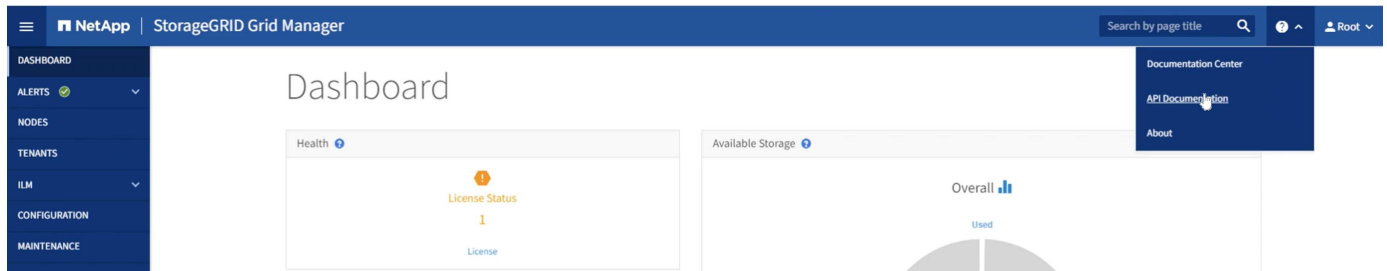
Habilitação de nível empresarial S3 com a migração otimizada de storage baseado em objetos do ONTAP S3 para o StorageGRID

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

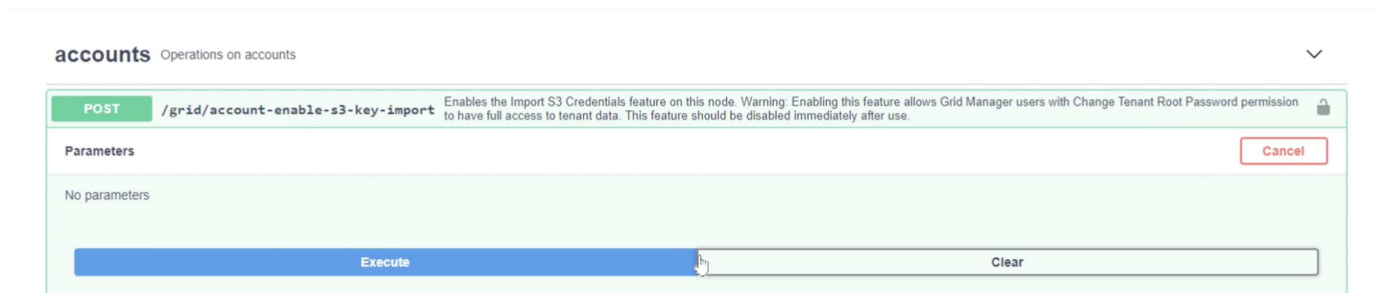
Migrar S3 chaves

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.

POST /grid/accounts/{id}/users/{user_id}/s3-access-keys Imports S3 credentials for a given user in a tenant account

Parameters

Name	Description
id * required string (path)	ID of Storage Tenant Account <input type="text" value="27041610751165610501"/>
user_id * required string (path)	ID of user in tenant account. <input type="text" value="ebc132e2-cfc3-42c0-a445-3b4465cb523c"/>
body * required (body)	Edit Value Model <pre>{ "accessKey": "3TVPI142JGE3Y7FV2KC0", "secretAccessKey": "75a1QqKBU4quA132twI4g41C4Gg5PP30ncy0sPE8" }</pre>

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"

POST /grid/account-disable-s3-key-import Disables the Import S3 Credentials feature on this node.

Parameters Cancel


No parameters

Execute

Responses Response content type application/json

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

Overview

Full name: ?	Demo S3 User 
Username: ?	demo_s3_user
User type: ?	Local
Denied access: ?	Yes
Access mode: ?	Read-only
Group membership: ?	Demo S3 Group

Password

Access

Access keys

Groups

Manage access keys

Add or delete access keys for this user.

Create key

Actions 

<input type="checkbox"/>	Access key ID 	Expiration time 
<input type="checkbox"/>	*****86TR	None
<input type="checkbox"/>	*****2KC0	None

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.

Edit group ✕

NAME

USERS

POLICIES

Cancel **Save**

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

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1 +

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

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.