Proteção de backup com destinos em nuvem

ONTAP 9

NetApp
January 17, 2025

Índice

Proteção de backup com destinos em nuvem

Requisitos para relacionamentos de destino na nuvem

Certifique-se de que seus ambientes de origem e destino atendam aos requisitos de proteção de backup do SnapMirror S3 para destinos na nuvem.

Você deve ter credenciais de conta válidas com o provedor de armazenamento de objetos para acessar o intervalo de dados.

LIFs entre clusters e um espaço IPspace devem ser configurados no cluster antes que o cluster possa se conetar a um armazenamento de objetos em nuvem. Você deve criar LIFs entre clusters em cada nó para transferir dados de forma otimizada do storage local para o armazenamento de objetos em nuvem.

Para alvos StorageGRID, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

Além disso, o certificado da CA usado para assinar o certificado do servidor StorageGRID precisa ser instalado na VM de armazenamento de administrador do cluster do ONTAP S3 usando o `security certificate install command`. Para obter mais informações, consulte "Instalando um certificado CA" se você usa o StorageGRID.

Para os destinos do AWS S3, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

O servidor DNS para a VM de armazenamento de administrador do cluster ONTAP deve ser capaz de resolver FQDNs (se usado) para endereços IP.

Criar um relacionamento de backup para um novo bucket (destino na nuvem)

Ao criar novos buckets do S3, você pode fazer backup deles imediatamente em um bucket de destino do SnapMirror S3 em um provedor de armazenamento de objetos, que pode ser um sistema StorageGRID ou uma implantação do Amazon S3.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.

- • A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Edite a VM de armazenamento para adicionar usuários e para adicionar usuários a grupos:
   a. Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em **S3**.

      Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Stores**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **StorageGRID**.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
        bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
        ```

      - **Recursos** - Use os padrões `_(bucketname, bucketname/*)` ou outros valores que você

precisa.

Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.

d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**, selecione **armazenamento em nuvem** e, em seguida, selecione **armazenamento de objetos em nuvem**.

Quando você clica em **Salvar**, um novo bucket é criado na VM de armazenamento de origem e é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Se esta for a primeira relação do SnapMirror S3 para este SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e regenere-as se não o fizerem:
`vserver object-store-server user show` Confirme que há uma chave de acesso para o usuário raiz. Se não houver, digite:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` Não regenere a chave se já existir.
2. Crie um bucket no SVM de origem:
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. Adicione regras de acesso à política de bucket padrão:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

Exemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Se o destino for um sistema StorageGRID, instale o certificado do servidor da CA StorageGRID no SVM admin do cluster de origem:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

   Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   Exemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Criar um relacionamento de backup para um bucket existente (destino na nuvem)

Você pode começar a fazer backup de buckets S3 existentes a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.
- A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Verifique se os usuários e grupos estão definidos corretamente: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em abaixo de S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, o cluster ou o SVM
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Insira os valores de objetivo **Throttle** e **ponto de recuperação**.
3. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Store**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **outros** para o StorageGRID Webscale.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende às suas necessidades:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Recursos** - Use os padrões *`(bucketname, bucketname/*)`* ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Faça backup do balde usando o SnapMirror S3:

a. Clique em **Storage** > **Buckets** e selecione o bucket que deseja fazer backup.

b. Clique em **Protect**, selecione **Cloud Storage** em **Target** e, em seguida, selecione **Cloud Object Store**.

Quando você clica em **Salvar**, o bucket existente é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Verifique se as regras de acesso na política de bucket padrão estão corretas:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. Se o destino for um sistema StorageGRID, instale o certificado da CA StorageGRID no SVM de administrador do cluster de origem:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Consulte a `security certificate install` página de manual para obter detalhes.

4. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password`

target_secret_key

Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path *svm_name*:/bucket/*bucket_name* -destination -path *object_store_name*:/objstore -policy *policy_name*`

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
   -destination-path sgws-store:/objstore -policy test-policy
   ```

6. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Restaurar um bucket do destino na nuvem

Quando os dados em um bucket de origem são perdidos ou corrompidos, você pode preencher novamente seus dados restaurando de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O bucket de destino para a operação de restauração deve ser maior que o espaço lógico usado do bucket de destino.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
     - Copie e cole o conteúdo do certificado da CA do servidor *destination* S3.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA de servidor S3 de destino.
4. Em **destino**, copie e cole o conteúdo do certificado da CA do servidor *source* S3.
5. Clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

Procedimento CLI

1. Crie o novo intervalo de destino para restauração. Para obter mais informações, "Criar um relacionamento de backup para um bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   Exemplo

   O exemplo a seguir restaura um bucket de destino para um bucket existente.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

Informações sobre direitos autorais

Informações sobre marcas comerciais