Proteção de espelho e backup no cluster local

ONTAP 9

NetApp
January 17, 2025

Índice

Proteção de espelho e backup no cluster local 1
Criar uma relação de espelho para um novo bucket (cluster local) 1
Criar uma relação de espelhamento para um bucket existente (cluster local) 5
Takeover e fornecimento de dados do bucket do destino (cluster local) 9
Restaurar um bucket da VM de armazenamento de destino (cluster local) 10

Proteção de espelho e backup no cluster local

Criar uma relação de espelho para um novo bucket (cluster local)

Ao criar novos buckets do S3, você pode protegê-los imediatamente para um destino do SnapMirror S3 no mesmo cluster. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Configurações**, clique no bloco S3.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma.
2. Edite a VM de armazenamento para adicionar usuários e adicionar usuários a grupos, tanto nas VMs de armazenamento de origem quanto de destino: 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.
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 depois 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,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.
   d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**. Em seguida, introduza os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster local.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de origem.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de destino.

5. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
6. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
7. Clique em **Salvar**. Um novo bucket é criado na VM de storage de origem e é espelhado em um novo bucket que é criado a VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie buckets nas SVMs de origem e de destino:

   ```
   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 às políticas de bucket padrão nas SVMs de origem e de destino:

   ```
   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`*`]`

```
src_cluster::> 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:

   - `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

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

5. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`src_server_certificate`*
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`dest_server_certificate`* Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

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

6. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]``

   Você pode usar uma política criada ou aceitar o padrão.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

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

Criar uma relação de espelhamento para um bucket existente (cluster local)

Você pode começar a proteger buckets S3 existentes no mesmo cluster a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma
2. Verifique se os usuários e grupos existentes estão presentes e têm o acesso correto nas VMs de armazenamento de origem e destino: Selecione **armazenamento > VMs de armazenamento** e, em seguida, selecione a VM de armazenamento e, em seguida, a guia **Configurações**. Por fim, localize o bloco **S3**, selecione e selecione a guia **usuários** e, em seguida, a guia **grupos** para exibir as configurações de acesso de usuário e grupo.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
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 **Configuração 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. Verifique se a política de acesso ao bucket do bucket existente continua atendendo às suas necessidades:
   a. Clique em **armazenamento > baldes** e, em seguida, 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. Proteja um balde existente com o SnapMirror S3:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.

b. Clique em **Protect** e insira os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione a mesma ou outra VM de armazenamento.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *destination*.

6. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
7. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
8. Clique em **Salvar**. O bucket existente é espelhado em um novo bucket na VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie um bucket no SVM de destino para ser o destino espelhado:

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. Verifique se as regras de acesso às políticas de bucket padrão estão corretas nas SVMs de origem e de destino:

`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:

   - `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. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *src_server_certificate*`
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *dest_server_certificate*` Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

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

6. Criar uma relação do SnapMirror S3:
   `snapmirror create -source-path *src_svm_name*:/bucket/*bucket_name* -destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

Você pode usar uma política criada ou aceitar o padrão.

Exemplo

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

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

Takeover e fornecimento de dados do bucket do destino (cluster local)

Se os dados em um bucket de origem ficarem indisponíveis, você poderá interromper a relação do SnapMirror para tornar o bucket de destino gravável e começar a fornecer dados.

Sobre esta tarefa

Quando uma operação de aquisição é executada, o bucket de origem é convertido em somente leitura e o bucket de destino original é convertido em leitura-gravação, revertendo assim a relação do SnapMirror S3.

Quando o bucket de origem desativado estiver disponível novamente, o SnapMirror S3 ressincroniza automaticamente o conteúdo dos dois buckets. Não é necessário ressincronizar explicitamente a relação, como é necessário para implantações padrão de volume SnapMirror.

Se o intervalo de destino estiver em um cluster remoto, a operação de aquisição deve ser iniciada a partir do cluster remoto.

System Manager

Faça failover do bucket indisponível e comece a fornecer dados:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em , selecione **failover** e, em seguida, clique em **failover**.

CLI

1. Inicie uma operação de failover para o bucket de destino:
`snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verifique o status da operação de failover:
`snapmirror show -fields status`

Exemplo

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Restaurar um bucket da VM de armazenamento de destino (cluster local)

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

Sobre esta tarefa

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

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.

A operação de restauração deve ser iniciada a partir do cluster local.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e, em seguida, selecione o intervalo.
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.
4. Copie e cole o conteúdo do certificado de CA do servidor S3 de destino.
   - 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.
5. Em **destino**, copie e cole o conteúdo do certificado de CA do servidor S3 de origem.
6. Clique em **proteção** > relacionamentos para monitorar o progresso da restauração.

Restaure os baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets bloqueados e restaurá-los conforme necessário.

Você pode restaurar um bucket bloqueado por objeto para um bucket novo ou existente. Você pode selecionar um bucket bloqueado por objeto como destino nos seguintes cenários:

- **Restaurar para um novo bucket**: Quando o bloqueio de objetos está ativado, um bucket pode ser restaurado criando um bucket que também tem o bloqueio de objetos ativado. Ao restaurar um bucket bloqueado, o modo de bloqueio de objetos e o período de retenção do bucket original são replicados. Também pode definir um período de retenção de bloqueio diferente para o novo balde. Este período de retenção é aplicado a objetos não bloqueados de outras fontes.
- **Restaurar para um bucket existente**: Um bucket bloqueado por objeto pode ser restaurado para um bucket existente, desde que o controle de versão e um modo de bloqueio de objeto semelhante estejam ativados no bucket existente. O período de retenção do balde original é mantido.
- **Restaurar bucket não bloqueado**: Mesmo que o bloqueio de objetos não esteja habilitado em um bucket, você pode restaurá-lo para um bucket que tenha o bloqueio de objetos ativado e esteja no cluster de origem. Quando você restaura o bucket, todos os objetos não bloqueados ficam bloqueados e o modo de retenção e a posse do bucket de destino se aplicam a eles.

CLI

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

Exemplo

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Informações sobre direitos autorais

Informações sobre marcas comerciais