Proteja buckets com o SnapMirror S3

ONTAP 9

NetApp
January 17, 2025

Índice

Proteja buckets com o SnapMirror S3

Visão geral do SnapMirror S3

A partir do ONTAP 9.10,1, você pode proteger buckets em armazenamentos de objetos do ONTAP S3 usando a funcionalidade de espelhamento e backup do SnapMirror. Ao contrário do SnapMirror padrão, o SnapMirror S3 permite o espelhamento e os backups para destinos que não sejam NetApp, como o AWS S3.

O SnapMirror S3 é compatível com espelhos ativos e categorias de backup dos buckets do ONTAP S3 nos seguintes destinos:

Alvo	É compatível com espelhos ativos e takeover?	É compatível com backup e restauração?
ONTAP S3 • Buckets no mesmo SVM • Buckets em diferentes SVMs no mesmo cluster • Buckets em SVMs em diferentes clusters	Sim	Sim
StorageGRID	Não	Sim
AWS S3	Não	Sim
Cloud Volumes ONTAP para Azure	Sim	Sim
Cloud Volumes ONTAP para AWS	Sim	Sim
Cloud Volumes ONTAP para Google Cloud	Sim	Sim

Você pode proteger buckets existentes nos servidores do ONTAP S3 ou criar novos buckets com a proteção de dados ativada imediatamente.

Requisitos do SnapMirror S3

- Versão de ONTAP

  O ONTAP 9.10,1 ou posterior deve estar em execução nos clusters de origem e destino.

- Licenciamento

  As seguintes licenças estão disponíveis no "ONTAP One"pacote de software são necessárias em sistemas de origem e destino ONTAP para fornecer acesso a:

  - Protocolo e storage ONTAP S3
  - SnapMirror S3 para segmentar outros destinos de armazenamento de objetos NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP)
  - SnapMirror S3 para segmentar armazenamentos de objetos de terceiros, incluindo AWS S3 (disponível no "Pacote de compatibilidade ONTAP One")

- ONTAP S3
  - Os servidores ONTAP S3 devem estar executando SVMs de origem e destino.
  - Recomenda-se, mas não é necessário, que os certificados de CA para acesso TLS sejam instalados em sistemas que hospedem servidores S3.
    - Os certificados de CA usados para assinar os certificados dos servidores S3 devem ser instalados na VM de armazenamento de administrador dos clusters que hospedam os servidores S3.
    - Você pode usar um certificado de CA autoassinado ou um certificado assinado por um fornecedor de CA externo.
    - Se as VMs de armazenamento de origem ou destino não estiverem escutando em HTTPS, não será necessário instalar certificados de CA.
- Peering (para alvos ONTAP S3)
  - Os LIFs entre clusters devem ser configurados (para destinos ONTAP remotos) e os LIFs entre clusters do cluster de origem e destino podem se conetar às LIFs de dados do servidor S3 de origem e destino.
  - Os clusters de origem e destino são direcionados (para destinos ONTAP remotos).
  - As VMs de armazenamento de origem e destino são direcionadas (para todos os destinos do ONTAP).
- Política de SnapMirror
  - Uma política SnapMirror específica para S3 é necessária para todos os relacionamentos do SnapMirror S3, mas você pode usar a mesma política para vários relacionamentos.
  - Você pode criar sua própria política ou aceitar a política padrão **contínua**, que inclui os seguintes valores:
    - Acelerador (limite superior em taxa de transferência/largura de banda) - ilimitado.
    - Tempo para objetivo do ponto de recuperação: 1 hora (3600 segundos).

> Você deve estar ciente de que quando dois buckets do S3 estiverem em um relacionamento do SnapMirror, se houver políticas de ciclo de vida configuradas para que a versão atual de um objeto expire (seja excluída), a mesma ação será replicada para o bucket do parceiro. Isso é verdade mesmo que o intervalo do parceiro seja somente leitura ou passivo.

- Chaves de usuário raiz armazenamento VM chaves de acesso de usuário raiz são necessárias para relacionamentos do SnapMirror S3; o ONTAP não as atribui por padrão. Na primeira vez que você criar uma relação do SnapMirror S3, você deve verificar se as chaves existem nas VMs de armazenamento de origem e destino e regenerá-las se não o fizerem. Se você precisar regenerá-los, você deve garantir que todos os clientes e todas as configurações de armazenamento de objetos do SnapMirror usando o par de chaves secretas e de acesso sejam atualizados com as novas chaves.

Para obter informações sobre a configuração do servidor S3, consulte os seguintes tópicos:

- "Ative um servidor S3 em uma VM de armazenamento"
- "Sobre o processo de configuração do ONTAP S3"

Para obter informações sobre peering de VM de cluster e armazenamento, consulte o seguinte tópico:

- "Prepare-se para espelhamento e cofre (System Manager, passos 1-6)"
- "Peering de cluster e SVM (CLI)"

Relacionamentos SnapMirror compatíveis

O SnapMirror S3 é compatível com relações em fan-out e cascata. Para obter uma visão geral,"Implantações de proteção de dados em cascata e fan-out"consulte .

O SnapMirror S3 não é compatível com implantações fan-in (relacionamentos de proteção de dados entre vários buckets de origem e um único bucket de destino). O SnapMirror S3 é compatível com vários espelhos de bucket de vários clusters para um único cluster secundário, mas cada bucket do origem deve ter seu próprio bucket do destino no cluster secundário.

Controle o acesso aos buckets do S3

Ao criar novos buckets, você pode controlar o acesso criando usuários e grupos. Para obter mais informações, consulte os seguintes tópicos:

- "Adicionar S3 usuários e grupos (System Manager)"
- "Criar um usuário S3 (CLI)"
- "Criar ou modificar S3 grupos (CLI)"

Proteção de espelho e backup em um cluster remoto

Criar uma relação de espelhamento para um novo bucket (cluster remoto)

Ao criar novos buckets do S3, você pode protegê-los imediatamente em um destino do SnapMirror S3 em um cluster remoto.

Sobre esta tarefa

Você precisará executar tarefas em sistemas de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e 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. Edite a VM de storage para adicionar usuários e adicionar usuários a grupos, nas VMs de armazenamento de origem e 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. No cluster de origem, 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**. Verificar permissões é opcional, mas recomendado.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**.
      - **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 remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **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*.

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]`

   Exemplo

   ```
   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. No SVM de origem, 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:

   - Tipo `continuous` - o único tipo de política para relacionamentos 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 CA nas SVMs administrativas dos clusters de origem e destino:

   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3:
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

      Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado na SVM do administrador de origem e destino.

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

6. Na fonte SVM, crie 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`

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

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

Sobre esta tarefa

Você precisa executar tarefas nos clusters de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e 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.

Passos

Você pode criar uma relação de espelhamento usando o Gerenciador do sistema ou a CLI do ONTAP.

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. Selecione **Storage > Storage VMs** e, em seguida, 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. No cluster de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Selecione **proteção > Visão geral** e clique em **Configurações de política local**.
   b. Selecione ao lado de **políticas de proteção** e clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, cluster ou SVM.
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende 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 proteção 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 remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **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 esta for a primeira relação do SnapMirror S3 para este SVM, verifique se existem chaves de usuário raiz para SVMs de origem e de destino e regenere-as se não o fizerem:
   `vserver object-store-server user show` 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 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 das 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

```
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. No SVM de origem, 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 CA nas SVMs administrativas dos clusters de origem e destino:
   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`
   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3: `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado no SVM do administrador de origem e destino.

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

6. Na fonte SVM, crie 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:/bucket/test-
bucket -destination-path vs1:/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 remoto)

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 de volume SnapMirror.

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

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

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

Se os dados em um bucket de origem forem perdidos ou corrompidos, você poderá

preencher novamente os 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 do que o espaço lógico usado do intervalo 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.

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

System Manager

Restaure os dados de cópia de segurança:

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 do servidor *destination* S3.
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.

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. Crie o novo intervalo de destino para restauração. 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

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

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
```

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
```

Modificar uma política de espelho

Você pode querer modificar uma política de espelhamento do S3; por exemplo, se quiser ajustar os valores de RPO e acelerador.

System Manager

Se você quiser ajustar esses valores, você pode editar uma política de proteção existente.

1. Clique em **proteção > relacionamentos** e, em seguida, selecione a política de proteção para o relacionamento que deseja modificar.
2. Clique ⋮ ao lado do nome da política e, em seguida, clique em **Editar**.

CLI

Modificar uma política do SnapMirror S3:
`snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer] [-throttle throttle_type] [-comment text]`

Parâmetros:

- `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos.
- `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Informações sobre direitos autorais

Informações sobre marcas comerciais