ローカル クラスタでのミラーとバックアップによる保護
ONTAP 9

NetApp
February 12, 2026

目次

ローカル クラスタでのミラーとバックアップによる保護

ローカルクラスタ上の新しい **ONTAP S3** バケットのミラー関係を作成する

新しいS3バケットを作成すると、同じクラスター内のSnapMirror S3宛先にすぐに保護できます。データのミラーリングは、ソースと同じストレージVMまたは別のストレージVM内のバケットに行うことができます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。
- ソースとデスティネーションのStorage VM間にピア関係が確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
   b. *設定*タブで、S3 タイルの をクリックします。
   c. *Users*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. 存在しない場合は、*root*の横にあるをクリックし、*キーの再生成*をクリックします。既にキーが存在する場合は、再生成しないでください。
2. ストレージ VM を編集して、ソース ストレージ VM と宛先ストレージ VM の両方でユーザーを追加し、ユーザーをグループに追加します：ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. **Protection > Overview** をクリックし、**Local Policy Settings** をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. SnapMirror保護を適用してバケットを作成します。
   a. **Storage > Buckets** をクリックし、**Add** をクリックします。
   b. 名前を入力し、ストレージ VM を選択し、サイズを入力して、*その他のオプション*をクリックします。
   c. *権限*で、*追加*をクリックします。権限の確認は任意ですが、推奨されます。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - デフォルト `(bucketname, bucketname/*)` または必要な他の値を使用します

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。
   d. *保護*で、*SnapMirrorを有効にする（ONTAPまたはCloud）*にチェックを入れます。次に、以下の値を入力します：

- デスティネーション
  - **TARGET**：ONTAPシステム
  - **CLUSTER**：ローカル クラスターを選択します。
  - **STORAGE VM**：ローカルクラスタ上のストレージ VM を選択します。
  - **S3 SERVER CA CERTIFICATE**：ソース証明書の内容をコピーして貼り付けます。
- ソース
  - **S3 SERVER CA CERTIFICATE**：宛先証明書の内容をコピーして貼り付けます。

5. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
6. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
7. *保存*をクリックします。ソースストレージVMに新しいバケットが作成され、デスティネーションストレージVMに作成された新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. この SVM の最初のSnapMirror S3 関係である場合は、ソース SVM と宛先 SVM の両方にルート ユーザー キーが存在することを確認し、存在しない場合は再生成します：
   `vserver object-store-server user show`

   ルートユーザーのアクセスキーがあることを確認してください。ない場合は、以下を入力してください（
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   キーがすでにある場合は再生成しないでください。

2. ソースとデスティネーションの両方のSVMにバケットを作成します。

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

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーにアクセス ルールを追加します。

```
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. 既存のSnapMirror S3ポリシーがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous` – SnapMirror S3 関係の唯一のポリシータイプ（必須）。
   - `-rpo` – 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

   例

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

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source* S3 サーバーの証明書に署名した CA 証明書を管理 SVM にインストールします：
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. 管理 SVM に、宛先 S3 サーバーの証明書に署名した CA 証明書をインストールします：
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate` + 外部 CA ベンダーによって署名された証明書を使用している場合は、この証明書を管理 SVM にインストールするだけで済みます。

   ```
   `security certificate install`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-
   cli/security-certificate-install.html["ONTAPコマンド リファレンス
   "^]をご覧ください。
   ```

6. SnapMirror S3 関係を作成します：
`snapmirror create -source-path src_svm_name:/bucket/bucket_name`

`-destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

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

7. ミラーリングがアクティブであることを確認します：
`snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

ローカル クラスタ上の既存の **ONTAP S3** バケットのミラー関係を作成します

同じクラスタ内の既存のS3バケットの保護は、たとえば、ONTAP 9.10.1よりも前のリリースからS3の設定をアップグレードした場合など、いつでも開始できます。データは、ソースとは別のStorage VMまたは同じStorage VMのバケットにミラーリングできます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。
- ソースとデスティネーションのStorage VM間にピア関係が確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
   b. *設定*タブで、*S3*タイルの をクリックします。
   c. *ユーザー*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. ない場合は、*root*の横にあるをクリックし、*Regenerate Key*をクリックします。既にキーが存在する場合は再生成しないでください。
2. 既存のユーザーとグループがソースとターゲットの両方のストレージVMに存在し、適切なアクセス権を持っていることを確認します：*ストレージ > ストレージVM*を選択し、ストレージVMを選択して*設定*タブを開きます。最後に*S3*タイルを見つけて を選択し、*ユーザー*タブ、*グループ*タブの順に選択して、ユーザーとグループのアクセス設定を表示します。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. *保護 > 概要*をクリックし、*ローカルポリシー設定*をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. 既存のバケットのバケット アクセス ポリシーが引き続き要件を満たしていることを確認します。
   a. **Storage > Buckets** をクリックし、保護するバケットを選択します。
   b. *権限*タブで *編集*をクリックし、*権限*の下の*追加*をクリックします。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - デフォルト値 `*(bucketname, bucketname/*)*`または必要なその他の値を使用します。

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。
5. SnapMirror S3を使用して既存のバケットを保護します。
   a. ストレージ > バケット をクリックし、保護するバケットを選択します。

b. *Protect*をクリックし、次の値を入力します：

- デスティネーション
  - **TARGET**：ONTAPシステム
  - **CLUSTER**：ローカル クラスターを選択します。
  - **STORAGE VM**：同じまたは別のストレージ VM を選択します。
  - **S3 SERVER CA CERTIFICATE**：*source* 証明書の内容をコピーして貼り付けます。
- ソース
  - **S3 SERVER CA CERTIFICATE**：_宛先_証明書の内容をコピーして貼り付けます。

6. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
7. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
8. *保存*をクリックします。既存のバケットが、宛先ストレージVMの新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. この SVM の最初のSnapMirror S3 関係である場合は、ソース SVM と宛先 SVM の両方にルート ユーザー キーが存在することを確認し、存在しない場合は再生成します：
   `vserver object-store-server user show`

   ルートユーザーのアクセスキーがあることを確認してください。ない場合は、以下を入力してください（
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   キーがすでにある場合は再生成しないでください。

2. デスティネーションSVMにミラー ターゲットにするバケットを作成します。

   `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. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーのアクセス ルールが

正しいことを確認します。

`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]`

例

```
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. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo _integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous` – SnapMirror S3 関係の唯一のポリシータイプ（必須）。
   - `-rpo` – 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

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

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source* S3 サーバーの証明書に署名した CA 証明書を管理 SVM にインストールします：`security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. 管理 SVM に、宛先 S3 サーバーの証明書に署名した CA 証明書をインストールします：`security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate` + 外部 CA ベンダーによって署名された証明書を使用している場合は、この証明書を管理 SVM にインストールするだけで済みます。

`security certificate install`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"^]をご覧ください。

6. SnapMirror S3 関係を作成します：
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

   例

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

7. ミラーリングがアクティブであることを確認します：
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

ローカルクラスタ上のデスティネーションONTAP S3バケットから引き継ぎます

ソース バケットのデータを使用できなくなった場合は、SnapMirror関係を解除してデスティネーション バケットを書き込み可能にし、データの提供を開始できます。

タスク概要

テイクオーバー処理が実行されると、ソース バケットが読み取り専用に変換され、元のデスティネーション バケットが読み取り / 書き込みに変換されて、SnapMirror S3関係が反転します。

無効になったソース バケットが再び使用できるようになると、SnapMirror S3は2つのバケットの内容を自動的に再同期します。標準のVolume SnapMirrorの構成と違って、関係を明示的に再同期する必要はありません。

デスティネーション バケットがリモート クラスタにある場合、テイクオーバー処理はリモート クラスタから開始する必要があります。

System Manager

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. *保護 > 関係*をクリックし、*SnapMirror S3*を選択します。
2. ⋮をクリックし、*フェイルオーバー*を選択して、*フェイルオーバー*をクリックします。

CLI

1. デスティネーション バケットのフェイルオーバー処理を開始します。
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー操作のステータスを確認します：
   `snapmirror show -fields status`

例

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

関連情報

- "SnapMirrorフェイルオーバーの開始"
- "snapmirror show"

ローカル クラスタのデスティネーションSVMからONTAP S3バケットをリストアする

ソース バケットのデータがなくなったり破損したりした場合、デスティネーション バケットからオブジェクトをリストアしてデータを再度取り込むことができます。

タスク概要

デスティネーション バケットは既存のバケットにも新しいバケットにもリストアできます。リストア処理のターゲット バケットには、デスティネーション バケットの使用済み論理スペースよりも多くのスペースが必要です。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はローカル クラスタから開始する必要があります。

System Manager

バックアップ データをリストアします。

1. *Protection > Relationships*をクリックし、バケットを選択します。
2. ⋮をクリックし、*復元*を選択します。
3. ソース*で、*既存のバケット（デフォルト）または*新しいバケット*を選択します。
   - 既存のバケット（デフォルト）に復元するには、次の操作を実行します：
     - 既存のバケットを検索するクラスタとStorage VMを選択します。
     - 既存のバケットを選択します。
4. デスティネーションのS3サーバCA証明書の内容をコピーして貼り付けます。
   - *新しいバケット*に復元するには、次の値を入力します：
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンス サービス レベル。詳細については、"ストレージ サービス レベル"を参照してください。
     - デスティネーションのS3サーバCA証明書の内容。
5. *Destination*で、ソースS3サーバーCA証明書の内容をコピーして貼り付けます。
6. 保護 > 関係をクリックして、リストアの進行状況を監視します。

ロックされたバケットのリストア

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックされたバケットをデスティネーションとして選択できます。

- 新しいバケットへの復元：オブジェクトロックが有効になっている場合、オブジェクトロックが有効になっているバケットを作成することで、バケットを復元できます。ロックされたバケットを復元すると、元のバケットのオブジェクトロックモードと保持期間が複製されます。新しいバケットに異なるロック保持期間を定義することもできます。この保持期間は、他のソースのロックされていないオブジェクトに適用されます。
- 既存のバケットへの復元：オブジェクトロックされたバケットは、既存のバケットでバージョニングと同様のオブジェクトロックモードが有効になっている限り、既存のバケットに復元できます。元のバケットの保持期間は維持されます。
- ロックされていないバケットの復元：バケットでオブジェクトロックが有効になっていない場合でも、ソース クラスタ上のオブジェクトロックが有効になっているバケットに復元できます。バケットを復元すると、ロックされていないすべてのオブジェクトがロックされ、デスティネーション バケットの保持モードと保有期間が適用されます。

CLI

1. オブジェクトを新しいバケットに復元する場合は、新しいバケットを作成してください。詳細については、"新しいONTAP S3バケットのクラウドバックアップ関係を作成する"をご覧ください。
2. デスティネーション バケットのリストア処理を開始します。
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name`

例

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

`snapmirror restore`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-restore.html["ONTAPコマンド リファレンス"^]を参照してください。

著作権に関する情報

商標に関する情報