SnapMirror S3によるバケットの保護

ONTAP 9

NetApp
February 12, 2026

目次

SnapMirror S3によるバケットの保護

ONTAP SnapMirror S3について学ぶ

ONTAP 9.10.1以降では、SnapMirrorのミラーリングとバックアップの機能を使用してONTAP S3オブジェクト ストアのバケットを保護できます。標準のSnapMirrorとは異なり、SnapMirror S3を使うと、AWS S3などのNetApp以外のデスティネーションへのミラーリングとバックアップができます。

SnapMirror S3では、ONTAP S3バケットから次のデスティネーションへのアクティブなミラーとバックアップをサポートしています。

ターゲット	アクティブなミラーとテイクオーバーのサポート	バックアップとリストアのサポート
ONTAP S3 • 同じSVM内のバケット • 同じクラスタ内の別のSVM内のバケット • 別のクラスタ内のSVM内のバケット	はい	はい
StorageGRID	いいえ	はい
AWS S3	いいえ	はい
Cloud Volumes ONTAP for Azure	はい	はい
Cloud Volumes ONTAP for AWS	はい	はい
Cloud Volumes ONTAP for Google Cloud	はい	はい

ONTAP S3サーバ上の既存のバケットを保護することも、新しく作成したバケットですぐにデータ保護を有効にすることもできます。

SnapMirror S3の要件

- ONTAPのバージョン

  ソースとデスティネーションのクラスタでONTAP 9.10.1以降が実行されている必要があります。

  SnapMirror S3はMetroCluster構成ではサポートされていません。

- ライセンス

  "ONTAP One"ソフトウェア スイートで利用可能な次のライセンスは、ONTAPソース システムとデスティネーション システムで次の項目へのアクセスを提供するために必要です：

  - ONTAP S3プロトコルおよびストレージ
  - SnapMirror S3：NetAppの他のオブジェクト ストア（ONTAP S3、StorageGRID、Cloud Volumes

ONTAP）をターゲットにするため

- SnapMirror S3からAWS S3（"ONTAP One互換性バンドル"で利用可能）を含むサードパーティのオブジェクト ストアへ
- クラスタでONTAP 9.10.1を実行している場合は、"FabricPoolライセンス"が必要です。

- ONTAP S3
  - ソースとデスティネーションのSVMでONTAP S3サーバが実行されている必要があります。
  - TLSアクセス用のCA証明書はS3サーバをホストするシステムにインストールすることを推奨しますが、必須ではありません。
    - S3サーバの証明書への署名に使用されたCA証明書を、S3サーバをホストするクラスタの管理Storage VMにインストールする必要があります。
    - 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。
    - ソースまたはデスティネーションのStorage VMがHTTPSをリスンしていない場合、CA証明書をインストールする必要はありません。
- ピアリング（ONTAP S3ターゲットの場合）
  - クラスタ間LIFが設定されている必要があります（リモートのONTAPターゲットの場合）。ソース クラスタとデスティネーション クラスタのクラスタ間LIFは、ソースとデスティネーションのS3サーバのデータLIFに接続できます。
  - ソースとデスティネーションのクラスタがピアリングされている必要があります（リモートのONTAPターゲットの場合）。
  - ソースとデスティネーションのStorage VMがピアリングされている必要があります（すべてのONTAPターゲットで必須）。
- SnapMirrorポリシー
  - すべてのSnapMirror S3関係にS3固有のSnapMirrorポリシーが必要ですが、複数の関係に同じポリシーを使用することができます。
  - 独自のポリシーを作成することも、次の値を含むデフォルトの **Continuous** ポリシーを受け入れることもできます：
    - スロットル（スループット / 帯域幅の上限）：無制限。
    - 回復ポイント目標の時間：1時間（3600秒）。

> ⓘ 2つのS3バケットがSnapMirror関係にある場合、現バージョンのオブジェクトの有効期限を定めた（削除するための）ライフサイクル ポリシーが存在すると、パートナー バケットにも同様の処理がレプリケートされることに注意してください。これは、パートナー バケットが読み取り専用またはパッシブである場合も同様です。

- ルート ユーザ キー Storage VMルート ユーザ アクセス キーはSnapMirror S3関係に必要です。ONTAPではデフォルトで割り当てられません。SnapMirror S3関係を初めて作成する際は、ソースとデスティネーションの両方のStorage VMにキーが存在することを確認し、存在しない場合は再生成する必要があります。再生成が必要な場合は、アクセス キーとシークレット キーのペアを使用しているすべてのクライアントとすべてのSnapMirrorオブジェクト ストア設定が新しいキーで更新されていることを確認する必要があります。

S3サーバの設定については、次のトピックを参照してください。

- "Storage VMでのS3サーバの有効化"

- "ONTAP S3の設定プロセスについて"

クラスタおよびStorage VMのピアリングについては、次のトピックを参照してください。

- "Prepare for mirroring and vaulting（System Manager、手順1～6）"
- "Cluster and SVM peering（CLI）"

サポートされるSnapMirror関係

SnapMirror S3はファンアウトとカスケード関係をサポートしています。概要については、"ファンアウト構成およびカスケード構成のデータ保護"をご覧ください。

SnapMirror S3では、ファンイン構成（複数のソース バケットと1つのデスティネーション バケットの間のデータ保護関係）はサポートされません。SnapMirror S3では、複数のクラスタから単一のセカンダリ クラスタへの複数のバケットのミラーはサポートされますが、各ソース バケットに対応する独自のデスティネーション バケットがセカンダリ クラスタに必要です。

SnapMirror S3はMetroCluster環境ではサポートされていません。

S3バケットへのアクセスの制御

新しいバケットを作成する際、ユーザとグループを作成してアクセスを制御できます。

SnapMirror S3 はソース バケットからデスティネーション バケットにオブジェクトを複製しますが、ソース オブジェクト ストアからデスティネーション オブジェクト ストアにユーザー、グループ、およびポリシーを複製しません。

フェイルオーバー イベント中にクライアントがデスティネーション バケットにアクセスできるように、ユーザー、グループ ポリシー、権限、および同様のコンポーネントをデスティネーション オブジェクト ストアで構成する必要があります。

移行元ユーザーと移行先ユーザーは、デスティネーション クラスタでユーザーが作成されるときに移行元キーが手動で提供される場合、同じアクセス キーとシークレット キーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

詳細については、次のトピックを参照してください。

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"

S3 オブジェクトロックとSnapMirror S3によるバージョン管理を使用する

オブジェクト ロックとバージョン管理が有効になっているONTAPバケットでSnapMirror S3を使用できますが、いくつかの考慮事項があります：

- Object Lockが有効になっているソースバケットをレプリケートするには、デスティネーションバケットでもObject Lockが有効になっている必要があります。さらに、ソースとデスティネーションの両方でバージョン管理が有効になっている必要があります。これにより、両方のバケットのデフォルトの保持ポリシーが異なる場合に、削除がデスティネーションバケットにミラーリングされる問題を回避できます。
- S3 SnapMirrorはオブジェクトの過去のバージョンをレプリケートしません。オブジェクトの現在のバージョンのみがレプリケートされます。

オブジェクトロックされたオブジェクトが宛先バケットにミラーリングされると、元の保持期間が維持されます。ロックされていないオブジェクトが複製された場合は、宛先バケットのデフォルトの保持期間が適用されます。例：

- バケットAのデフォルトの保持期間は30日間、バケットBのデフォルトの保持期間は60日間です。バケットAからバケットBに複製されたオブジェクトは、バケットBのデフォルトの保持期間よりも短いにもかかわらず、30日間の保持期間を維持します。
- バケットAにはデフォルトの保持期間がなく、バケットBにはデフォルトの保持期間が60日間あります。ロック解除されたオブジェクトがバケットAからバケットBに複製されると、60日間の保持期間が適用されます。バケットAでオブジェクトが手動でロックされた場合、バケットBに複製される際に元の保持期間が維持されます。
- バケットAのデフォルトの保持期間は30日間ですが、バケットBにはデフォルトの保持期間がありません。バケットAからバケットBに複製されたオブジェクトは、30日間の保持期間を維持します。

リモート クラスタでのミラーとバックアップによる保護

リモート クラスタ上の新しい**ONTAP S3**バケットのミラー関係を作成します

新しい S3 バケットを作成すると、リモート クラスター上の SnapMirror S3 デスティネーションにすぐに保護できます。

タスク概要

このタスクはソースとデスティネーションの両方のシステムで実行する必要があります。

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クラスタ間にピア関係が、ソースとデスティネーションのStorage VM間にピア関係がそれぞれ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. 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. ソースとデスティネーションの両方のStorage VMで、Storage VMを編集してユーザを追加し、グループにユーザを追加します。

   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. ソースクラスタで、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. *ストレージ > バケット*をクリックし、*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。
   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。
      - **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

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
  - ターゲット：**ONTAP**システム
  - **CLUSTER**：リモート クラスターを選択します。
  - **STORAGE VM**：リモートクラスタ上のストレージ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** サーバー **CA** 証明書： デスティネーション 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SVM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。

   ```
   vserver object-store-server user show
   ```

   rootユーザのアクセス キーがあることを確認します。キーがない場合は次のように入力します。

   ```
   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]
   ```

   例

   ```
   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. ソースSVMで、既存のものがなくデフォルトのポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成します：
   `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：

   - type `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. ソースとデスティネーションのクラスタの管理SVMに、CAサーバ証明書をインストールします。

   a. ソース クラスタで、デスティネーション S3サーバ証明書に署名したCA証明書をインストールします：
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. デスティネーション クラスタに、ソース S3 サーバー証明書に署名した CA 証明書をインストールします：
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

外部CAベンダーが署名した証明書を使用する場合は、ソースとデスティネーションの管理SVMに同じ証明書をインストールします。

`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. ソース SVM で、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"

リモート 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

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。

タスク概要

このタスクはソースとデスティネーションの両方のクラスタで実行する必要があります。

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クラスタ間にピア関係が、ソースとデスティネーションのStorage VM間にピア関係がそれぞれ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。

手順

ミラー関係は、System ManagerまたはONTAP CLIを使用して作成できます。

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. *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、*キーの再生成*をクリックします。すでにキーが存在する場合は、キーを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. ソースクラスタで、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*を選択し、*Local Policy Settings*をクリックします。
   b. *保護ポリシー*の横にある を選択し、*追加*をクリックします。
   c. ポリシーの名前と説明を入力します。
   d. ポリシーの対象として、クラスタとSVMのいずれかを選択します。
   e. SnapMirror S3 関係には 継続 を選択します。
   f. *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**：ユーザーグループの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保護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**：リモート クラスターを選択します。
  - **STORAGE VM**：リモートクラスタ上のストレージ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に対する最初のSnapMirror S3関係の場合、ソースSVMとデスティネーション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てください：
   `vserver object-store-server user show` + ルートユーザーのアクセスキーが存在することを確認してください。存在しない場合は、以下を入力してください：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + キーが既に存在す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

```
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. ソースSVMで、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

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

5. ソースとデスティネーションのクラスタの管理SVMに、CA証明書をインストールします。

   a. ソース クラスタで、デスティネーション S3サーバ証明書に署名したCA証明書をインストールします：
   security certificate install -type server-ca -vserver *src_admin_svm* -cert-name *dest_server_certificate*

   b. デスティネーション クラスタに、ソース S3サーバ証明書に署名したCA証明書をインストールします：
   security certificate install -type server-ca -vserver *dest_admin_svm* -cert-name *src_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、ソースおよびデスティネーションの管理SVMに同じ証明書をインストールします。

   `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. ソース SVM で、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:/bucket/test-
   bucket -destination-path 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"

リモート 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。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。

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。

SnapMirror S3 はソース バケットからデスティネーション バケットにオブジェクトを複製しますが、ソース オブジェクト ストアからデスティネーション オブジェクト ストアにユーザー、グループ、およびポリシーを複製しません。

フェイルオーバー イベント中にクライアントがデスティネーション バケットにアクセスできるように、ユーザー、グループ ポリシー、権限、および同様のコンポーネントをデスティネーション オブジェクト ストアで構成する必要があります。

移行元ユーザーと移行先ユーザーは、デスティネーション クラスタでユーザーが作成されるときに移行元キーが手動で提供される場合、同じアクセス キーとシークレット キーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

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

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

関連情報

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"
- "SnapMirrorフェイルオーバーの開始"
- "snapmirror show"

リモート 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。

リストア処理はリモート 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. *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、*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。
     - デスティネーション S3 サーバー 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 S3 サーバー CA 証明書の内容。
4. *Destination*の下に、*source* S3サーバーCA証明書の内容をコピーして貼り付けます。
5. 復元の進行状況を監視するには、*保護 > 関係*をクリックします。

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. 復元用の新しいデスティネーション バケットを作成します。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"を参照してください。
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

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_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。

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。

クラウド ターゲットでのバックアップによる保護

ONTAP SnapMirror S3クラウドターゲット関係の要件

ソースとターゲットの環境が、SnapMirror S3によるクラウド ターゲットへのバックアップ保護の要件を満たしていることを確認します。

データ バケットにアクセスするには、オブジェクト ストア プロバイダの有効なアカウント クレデンシャルが必要です。

クラスタをクラウド オブジェクト ストアに接続するためには、クラスタ間LIFとIPspaceがクラスタに設定されている必要があります。ローカル ストレージからクラウド オブジェクト ストアにデータをシームレスに転送するためには、各ノードにクラスタ間LIFを作成します。

StorageGRIDをターゲットにする場合は、次の情報を確認しておく必要があります。

- サーバ名：完全修飾ドメイン名（FQDN）またはIPアドレスで表されます。
- バケット名：バケットがすでに存在している必要があります。
- アクセス キー
- シークレット キー

さらに、StorageGRIDサーバ証明書の署名に使用するCA証明書を、 `security certificate install`コマンドを使用してONTAP S3クラスタの管理ストレージVMにインストールする必要があります。詳細については、StorageGRIDを使用する場合は"CA証明書のインストール"を参照してください。

AWS S3をターゲットにする場合は、次の情報を確認しておく必要があります。

- サーバ名：完全修飾ドメイン名（FQDN）またはIPアドレスで表されます。
- バケット名：バケットがすでに存在している必要があります。
- アクセス キー
- シークレット キー

ONTAPクラスタの管理Storage VM用のDNSサーバが、FQDN（使用している場合）をIPアドレスに解決できる必要があります。

関連情報

- "security certificate install"

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

新しい S3 バケットを作成すると、SnapMirror S3 ターゲット バケットにすぐにバックアップできます。このターゲット バケットは、オブジェクト ストア プロバイダー（StorageGRID システムまたは Amazon S3 デプロイメント）上にあります。

開始する前に

- オブジェクト ストア プロバイダの有効なアカウント クレデンシャルと設定情報が必要です。
- ソース システムにクラスタ間ネットワーク インターフェイスとIPspaceが設定されている必要があります。
- • ソース ストレージ VM の DNS 構成は、ターゲットの FQDN を解決できる必要があります。

System Manager

1. Storage VMを編集してユーザを追加し、グループにユーザを追加します。
   a. 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。

2. ソース システムにクラウド オブジェクト ストアを追加します。
   a. *保護 > 概要*をクリックし、*クラウドオブジェクトストア*を選択します。
   b. *追加*をクリックし、*Amazon S3*または*StorageGRID*を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセス キー
      - シークレット キー
      - コンテナ（バケット）の名前
3. 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：
   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** および **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
```

- リソース：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。

d. *保護*で、*SnapMirrorを有効化（ONTAPまたはクラウド）*をチェックし、*クラウドストレージ*を選択してから、*クラウドオブジェクトストア*を選択します。

*保存*をクリックすると、ソースストレージVMに新しいバケットが作成され、クラウドオブジェクトストアにバックアップされます。

CLI

1. このSVMで最初のSnapMirror S3関係を作成する場合は、ソースSVMとデスティネーションSVMの両方にルートユーザ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` + ルートユーザのアクセスキーが存在することを確認します。存在しない場合は、次のように入力します：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + キーがすでに存在する場合は、再生成しないでください。
2. ソース 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. 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]`

   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：* `type continuous` – SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo` – リカバリ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. ターゲットが StorageGRID システムの場合は、ソース クラスタの管理 SVM に StorageGRID CA サーバ証明書をインストールします。
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

```
`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宛先オブジェクトストアを定義します：
`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`

パラメータ：* `-object-store-name` – ローカル ONTAP システム上のオブジェクトストアターゲットの名前。* `-usage` – このワークフローには `data`を使用します。* `-provider-type` – `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server` – ターゲットサーバの FQDN または IP アドレス。* `-is-ssl-enabled` – SSL の有効化はオプションですが、推奨されます。+ `snapmirror object-store config create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

例

```
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. SnapMirror S3 関係を作成します：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path` - 前の手順で作成したオブジェクト ストア名と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトを受け入れることもできます。

例

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

8. 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"

既存の**ONTAP S3**バケットのクラウドバックアップ関係を作成する

既存のS3バケットのバックアップは、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。

開始する前に

- オブジェクト ストア プロバイダの有効なアカウント クレデンシャルと設定情報が必要です。
- ソース システムにクラスタ間ネットワーク インターフェイスとIPspaceが設定されている必要があります。
- ソースStorage VMのDNS設定でターゲットのFQDNを解決できる必要があります。

System Manager

1. ユーザーとグループが正しく定義されていることを確認します：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。

2. 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。
   c. ポリシーの名前と説明を入力します。
   d. ポリシーの対象として、クラスタまたはSVMを選択します。
   e. SnapMirror S3 関係には 継続 を選択します。
   f. *スロットル*と*リカバリポイント目標値*を入力します。
3. ソース システムにクラウド オブジェクト ストアを追加します。
   a. *保護 > 概要*をクリックし、*クラウドオブジェクトストア*を選択します。
   b. 追加*をクリックし、**StorageGRID Webscale** の ***Amazon S3** または その他 を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセス キー
      - シークレット キー
      - コンテナ（バケット）の名前
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. 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. *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を使用してバケットをバックアップします。
   a. ストレージ > バケット をクリックし、バックアップするバケットを選択します。
   b. *保護*をクリックし、*ターゲット*の下の*クラウドストレージ*を選択して、*クラウドオブジェクトストア*を選択します。

*保存*をクリックすると、既存のバケットがクラウドオブジェクトストアにバックアップされます。

CLI

1. 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 /*
   ```

2. 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：* `type continuous` – SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo` – リカバリ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
   ```

3. ターゲットが StorageGRID システムの場合は、ソース クラスタの管理 SVM に StorageGRID CA 証明書をインストールします。
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   ```
   `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。
   ```

4. SnapMirror S3宛先オブジェクトストアを定義します：
`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`

パラメータ：* `-object-store-name` – ローカルONTAPシステム上のオブジェクトストアターゲットの名前。* `-usage` – このワークフローには `data`を使用します。* `-provider-type` – `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server` – ターゲットサーバのFQDNまたはIPアドレス。* `-is-ssl-enabled` – SSLの有効化はオプションですが、推奨されます。+ `snapmirror object-store config create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

例

```
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. SnapMirror S3 関係を作成します：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path` - 前の手順で作成したオブジェクト ストア名と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトを受け入れることもできます。

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

6. 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"

クラウドターゲットから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。

System Manager

バックアップ データをリストアします。

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、*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。
     - デスティネーション S3 サーバー 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。
4. *Destination*の下に、*source* S3サーバーCA証明書の内容をコピーして貼り付けます。
5. 復元の進行状況を監視するには、*保護 > 関係*をクリックします。

CLIの手順

1. 復元用の新しいデスティネーション バケットを作成します。詳細については、"バケット（クラウド ターゲット）のバックアップ関係を作成する"を参照してください。
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 object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   例

   次の例では、デスティネーション バケットを既存のバケットにリストアします。
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   `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。

ONTAP SnapMirror S3ポリシーを変更する

RPO とスロットル値を調整する場合は、S3 SnapMirrorポリシーを変更することがあります。

System Manager

1. *保護 > 関係*をクリックし、変更する関係の保護ポリシーを選択します。
2. ポリシー名の横にある ⋮ をクリックし、*編集*をクリックします。

CLI

SnapMirror S3ポリシーを変更します：

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

パラメータ：

- `-rpo`：回復ポイント目標の時間を秒単位で指定します。
- `-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。

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

関連情報

- "snapmirror policy modify"

著作権に関する情報

商標に関する情報