Fsas Technologies

C140-0091-02Z3

ETERNUS AX series オールフラッシュアレイ，ETERNUS HX series ハイブリッドアレイ

S3 SnapMirror によるバケットの保護

ONTAP 9

目次

はじめに

本書は、https://storage-system.fujitsu.com/manual/ja/axhx/s3-snapmirror/index.html に基づいて作成されました。

第 2 版
2025 年 3 月

登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/
本書では、本文中の™、® などの記号は省略しています。

本書の読み方

対象読者

本書は、ETERNUS AX/HX の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

関連マニュアル

ETERNUS AX/HX に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

本書の表記について

本文中の記号

本文中では、以下の記号を使用しています。

注意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備考	本文を補足する内容や、参考情報を記述しています。

1. S3 SnapMirror の概要

ONTAP 9.10.1 以降では、SnapMirror ミラーリングおよびバックアップ機能を使用して、ONTAP S3 オブジェクトストア内のバケットを保護できます。標準の SnapMirror とは異なり、S3 SnapMirror は AWS S3 のような当社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を可能にします。

S3 SnapMirror は、ONTAP S3 バケットから以下のデスティネーションへのアクティブミラーとバックアップ層をサポートします。

ターゲット	アクティブミラーおよびテイクオーバーのサポート	バックアップおよびリストアのサポート
ONTAP S3 • 同一 SVM 内のバケット • 同一クラスタ上の異なる SVM 内のバケット • 異なるクラスタ上の SVM 内のバケット	サポート	サポート
StorageGRID	未サポート	サポート
AWS S3	未サポート	サポート
Cloud Volumes ONTAP for Azure	サポート	サポート
Cloud Volumes ONTAP for AWS	サポート	サポート
Cloud Volumes ONTAP for Google Cloud	サポート	サポート

ONTAP S3 サーバー上の既存のバケットを保護することも、データ保護を直接有効にした新しいバケットを作成することもできます。

1.1 S3 SnapMirror の要件

- ONTAP バージョン
  ONTAP 9.10.1 以降がソースクラスタおよびデスティネーションクラスタで実行されている必要があります。
- ライセンス
  ONTAP のソースシステムおよびデスティネーションシステムでは、以下のライセンスバンドルが必要です。
  - Core Bundle
    ONTAP S3 プロトコルおよびストレージ用のライセンスバンドルです。
  - Data Protection Bundle
    S3 SnapMirror で、他のオブジェクトストアターゲット（ONTAP S3、StorageGRID、および Cloud Volumes ONTAP）をターゲットにする場合に必要なライセンスバンドルです。
  - Data Protection Bundle and Hybrid Cloud Bundle
    S3 SnapMirror で、AWS S3 などのサードパーティのオブジェクトストアをターゲットにする場合に必要なライセンスバンドルです。
- ONTAP One
  S3 SnapMirror で、SnapMirror Cloud を使用した AWS S3 など、サードパーティのオブジェクトストアをターゲットにする場合に必要です。
- ONTAP S3
  - ソース SVM とデスティネーション SVM で ONTAP S3 サーバーを実行している必要があります。
  - 必須ではありませんが、TLS アクセス用の CA 証明書を S3 サーバー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。
    - S3 サーバーの証明書の署名に使用した CA 証明書は、S3 サーバー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 ベンダーによって署名された証明書を使用できます。
    - ソース Storage VM またはデスティネーション Storage VM が HTTPS で受信接続していない場合は、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 を構成する必要があります（リモート 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をピアリングします（リモート ONTAP ターゲットの場合）。
  - ソース Storage VM およびデスティネーション Storage VM をピアリングします（すべての ONTAP ターゲットの場合）。
- SnapMirror ポリシー
  - S3 固有の SnapMirror ポリシーは、すべての S3 SnapMirror 関係で設定が必要ですが、同じポリシーを複数の関係に使用することができます。
  - 独自のポリシーを作成するか、以下の値を含むデフォルトの Continuous ポリシーを設定してください。
    - スロットル（スループットおよび帯域幅の上限）：無制限
    - 目標復旧時点：1 時間（3600 秒）
- root ユーザーキー
  S3 SnapMirror 関係には、ストレージ VM の root ユーザーのアクセスキーが必要です。デフォルトでは、ONTAP からの割り当てはありません。S3 SnapMirror 関係を初めて作成するときは、キーがソースとデスティネーションの両方の Storage VM に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。キーを再生成する必要がある場合は、アクセスキーと秘密キーのペアを使用す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構成が新しいキーで更新されていることを必ず確認してください。

S3 サーバーの設定については、以下のトピックを参照してください。

- Storage VM で S3 サーバーを有効にする
- S3 の構成手順について

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

- ミラーリングとバックアップの準備（System Manager の場合、手順 1~6）
- クラスタおよび SVM のピアリング（CLI）

1.2 サポートされる SnapMirror 関係

S3 SnapMirror は、ファンアウトおよびカスケード関係をサポートします。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」を参照してください。

S3 SnapMirror は、ファンイン配置（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間のデータ保護関係）をサポートしていません。S3 SnapMirror 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ミラーをサポートしますが、各ソースバケットは、セカンダリクラスタ上に独自のデスティネーションバケットを持つ必要があります。

1.3 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ときは、ユーザーとグループを作成してアクセスを制御することができます。詳細については、以下のトピックを参照してください。

- S3 ユーザーとグループの作成（System Manager）
- S3 ユーザーの作成（CLI）
- S3 グループの作成と変更（CLI）

2. リモートクラスタでのミラーリングとバックアップ保護

2.1 新しいバケットのミラー関係の作成（リモートクラスタ）

作成した新しい S3 バケットは、リモートクラスタ上の S3 SnapMirror デスティネーション上ですぐに保護することができます。

要件

- ONTAP のバージョン、ライセンス、および S3 サーバー設定の要件を満たしていること。
- ソースクラスタとデスティネーションクラスタの間にピアリング関係があり、ソース Storage VM とデスティネーション Storage VM の間にピアリング関係があること。
- CA 証明書は、ソース VM とデスティネーション VM の両方に必要です。自己署名 CA 証明書または外部 CA ベンダーによって署名された証明書を使用できます。

このタスクについて

ソースシステムとデスティネーションシステムの両方でタスクを実行する必要があります。

System Manager

1. この Storage VM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の Storage VM に存在することを確認し、キーが存在していない場合は再生成します。
   - 1-1 **[ストレージ]>[Storage VM]** の順にクリックし、Storage VM を選択します。
   - 1-2 **[設定]** タブで、**S3** タイルの をクリックします。
   - 1-3 **[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。
   - 1-4 アクセスキーが表示されていない場合は、**[root]** の横にある から **[キーを再生成]** をクリックします。
     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. ソースとデスティネーションの両方で Storage VM を編集してユーザーを追加し、グループにユーザーを追加します。
   [ストレージ]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、S3 の下の をクリックします。
   詳細は、「S3 ユーザーとグループの作成」を参照してください。

3 既存のポリシーがなく、デフォルトポリシーを使用しない場合は、ソースクラスタで S3 SnapMirror ポリシーを作成します。

3-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。

3-2 **[保護ポリシー]** の横にある →をクリックし、**[追加]** をクリックします。

- ポリシー名と説明を入力します。
- ポリシースコープとして、クラスタまたは SVM を選択します。
- S3 SnapMirror 関係に **[Continuous]** を選択します。
- **[Throttle]** と **[Recovery Point Objective]** の値を入力します。

4 SnapMirror 保護がついたバケットを作成します。

4-1 **[ストレージ]>[バケット]** の順にクリックし、**[追加]** をクリックします。権限の検証はオプションですが、実行することを推奨します。

4-2 バケット名を入力し、Storage VM を選択し、サイズを入力した後、**[その他のオプション]** をクリックします。

4-3 **[権限]** の下にある **[追加]** をクリックします。

- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

4-4 **[保護]** で、**[SnapMirror を有効にする（ONTAP またはクラウド）]** チェックボックスをオンにします。次に、以下の値を入力します。

- デスティネーション
  - **TARGET**
    ONTAP System
  - **CLUSTER**
    リモートクラスタを選択します。
  - **STORAGE VM**
    リモートクラスタ上の Storage 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**
    *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。

外部 CA ベンダーによって署名された証明書を使用する場合は、**[Use the same certificate on the destination]** チェックボックスをオンにします。

[Destination Settings] 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に独自の値を入力することもできます。

[保存] をクリックすると、新しいバケットがソース Storage VM に作成され、デスティネーション Storage VM に作成した新しいバケットにミラーリングされます。

CLI

1. この SVM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の SVM に存在することを確認し、キーが存在していない場合は再生成します。

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

   root ユーザーのアクセスキーが存在していることを確認します。存在しない場合は、以下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 とデスティネーション SVM の両方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 SVM とデスティネーション SVM の両方のデフォルト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,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal - -resource test-bucket, test-bucket /*
   ```

4. 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、ソース SVM で S3 SnapMirror 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]
   ```

   パラメーター：

   - `-type continuous`
     S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
   - `-rpo`
     目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
   - `-throttle`
     スループットおよび帯域幅の上限をキロバイト単位または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 ソースクラスタおよびデスティネーションクラスタの管理 SVM に CA サーバー証明書をインストールします。

5-1 ソースクラスタで、*デスティネーション*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 *src_admin_svm* -cert-name *dest_server_certificate*

5-2 デスティネーションクラスタで、*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。

詳細は、`security certificate install` のマニュアルページを参照してください。

6 ソース SVM で、S3 SnapMirror 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、デフォルトポリシーを使用することもできます。
例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/testbucket
-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
```

2.2 既存バケットのミラー関係の作成（リモートクラスタ）

既存の S3 バケットの保護はいつでも開始できます。たとえば、ONTAP 9.10.1 より前のリリースから S3 構成をアップグレードした場合などです。

要件

- ONTAP のバージョン、ライセンス、および S3 サーバー設定の要件を満たしていること。
- ソースクラスタとデスティネーションクラスタの間にピアリング関係があり、ソース Storage VM とデスティネーション Storage VM の間にピアリング関係があること。
- CA 証明書は、ソース VM とデスティネーション VM の両方に必要です。自己署名 CA 証明書または外部 CA ベンダーによって署名された証明書を使用できます。

このタスクについて

ソースクラスタとデスティネーションクラスタの両方でタスクを実行する必要があります。

System Manager

1 この Storage VM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の Storage VM に存在することを確認し、キーが存在していない場合は再生成します。

1-1 **[ストレージ]>[Storage VM]** の順にクリックし、Storage VM を選択します。

1-2 **[設定]** タブで、**S3** タイルの をクリックします。

1-3 **[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。

1-4 アクセスキーが表示されていない場合は、**[root]** の横にある から **[キーを再生成]** をクリックします。
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 ソースとデスティネーションの両方の Storage VM で、ユーザーとグループのアクセス権が正しいことを確認します。
[ストレージ]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、**S3** の下の をクリックします。
詳細は、「S3 ユーザーとグループの作成」を参照してください。

3 既存のポリシーがなく、デフォルトポリシーを使用しない場合は、ソースクラスタで S3 SnapMirror ポリシーを作成します。

3-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。

3-2 **[保護ポリシー]** の横にある をクリックし、**[追加]** をクリックします。

3-3 ポリシー名と説明を入力します。

3-4 ポリシースコープとして、クラスタまたは SVM を選択します。

3-5 S3 SnapMirror 関係に **[Continuous]** を選択します。

3-6 **[Throttle]** と **[Recovery Point Objective]** の値を入力します。

4 設定後も、既存のバケットのバケットアクセスポリシーが要件を満たしていることを確認します。

4-1 **[ストレージ]>[バケット]** の順にクリックし、保護するバケットを選択します。

4-2 **[権限]** タブで、 **[編集]** をクリックし、**[権限]** 配下の **[追加]** をクリックします。

- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

5 S3 SnapMirror 保護を使用して既存のバケットを保護します。

5-1 **[ストレージ]>[バケット]** の順にクリックし、保護するバケットを選択します。

5-2 **[保護]** をクリックし、以下の値を入力します。

- デスティネーション
  - **TARGET**
    ONTAP System
  - **CLUSTER**
    リモートクラスタを選択します。
  - **STORAGE VM**
    リモートクラスタ上の Storage 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**
    *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。

外部 CA ベンダーによって署名された証明書を使用する場合は、**[Use the same certificate on the destination]** チェックボックスをオンにします。

[Destination Settings] 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に独自の値を入力することもできます。

[保存] をクリックすると、既存のバケットがデスティネーション Storage VM の新しいバケットにミラーリングされます。

CLI

1 この SVM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の SVM に存在することを確認し、キーが存在していない場合は再生成します。

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

root ユーザーのアクセスキーが存在していることを確認します。存在しない場合は、以下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 ミラーリングのターゲットとなるバケットをデスティネーション SVM に作成します。

```
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 デフォルトバケットポリシーのアクセスルールが、ソース SVM とデスティネーション SVM の両方で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 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、ソース SVM で S3 SnapMirror 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]`

パラメーター：

- `-type continuous`
  S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
- `-rpo`
  目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
- `-throttle`
  スループットおよび帯域幅の上限をキロバイト単位または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 ソースクラスタおよびデスティネーションクラスタの管理 SVM に CA 証明書をインストールします。

5-1 ソースクラスタで、*デスティネーション*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 *src_admin_svm* -cert-name *dest_server_certificate*

5-2 デスティネーションクラスタで、*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。

詳細は、`security certificate install` のマニュアルページを参照してください。

6 ソース SVM で、S3 SnapMirror 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、デフォルトポリシーを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
```

2.3 デスティネーションバケットからのテイクオーバーとデータ提供（リモートクラスタ）

ソースバケット内のデータが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。

このタスクについて

テイクオーバー操作が実行されると、ソースバケットは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は読み取り / 書き込みに変換されるため、S3 SnapMirror 関係が逆転します。

無効にしたソースバケットが再び使用可能になると、S3 SnapMirror は 2 つのバケットの内容を自動的に再同期します。ボリューム SnapMirror 導入の場合のように、関係を明示的に再同期する必要はありません。

テイクオーバー操作は、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を実行し、データの提供を開始します。

1 **[保護]>[関係]** をクリックし、**[S3 SnapMirror]** を選択します。

2 ⋮ をクリックし、**[Failover]** を選択して、**[Failover]** 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操作を開始します。

```
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
```

2.4 デスティネーション Storage VM（リモートクラスタ）からバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、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入力します。

このタスクについて

デスティネーションバケットを既存のバケットまたは新しいバケットにリストアできます。リストア操作のターゲットバケットは、デスティネーションバケットの論理使用領域よりも大きい必要があります。

既存のバケットを使用する場合は、リストア操作を開始するときにバケットを空にする必要があります。リストアは時間内にバケットを「ロールバック」しない代わりに、空のバケットに以前の内容を入力します。

リストア操作は、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、**[S3 SnapMirror]** を選択します。
2. ⋮ をクリックし、**[Restore]** を選択します。
3. **[ソース]** で、**[既存バケット]**（デフォルト）または **[新規バケット]** を選択します。
   - **[既存バケット]**（デフォルト）にリストアするには、以下の操作を行います。
     (1) 既存バケットを検索するクラスタとストレージ VM を選択します。
     (2) 既存バケットを選択します。
     (3) デスティネーション S3 サーバーの CA 証明書の内容をコピーして貼り付けます。
   - **[新規バケット]** にリストアするには、以下の値を入力します。
     - 新しいバケットをホストするクラスタおよび Storage VM。
     - 新しいバケットの名前、容量、およびパフォーマンスのサービスレベル。
       詳細は、「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 サーバーの CA 証明書の内容。
4. **[デスティネーション]** で、ソース S3 サーバーの CA 証明書の内容をコピーして貼り付けます。
5. **[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。

CLI

1. 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ます。詳細は、「4.2 新しいバケットのバックアップ関係の作成（クラウドターゲット）」(P.24) 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操作を開始します。

   ```
   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
   ```

3. ローカルクラスタでのミラーリングとバックアップ保護

3.1 新しいバケットのミラー関係の作成（ローカルクラスタ）

作成した新しい S3 バケットは、同一クラスタ上の S3 SnapMirror デスティネーション上ですぐに保護することができます。別の Storage VM またはソースと同じ Storage VM のバケットにデータをミラーリングできます。

要件

- ONTAP のバージョン、ライセンス、および S3 サーバー設定の要件を満たしていること。
- ソース Storage VM とデスティネーション Storage VM の間に、ピアリング関係が存在していること。
- CA 証明書は、ソース VM とデスティネーション VM の両方に必要です。自己署名 CA 証明書または外部 CA ベンダーによって署名された証明書を使用できます。

System Manager

1. この Storage VM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の Storage VM に存在することを確認し、キーが存在していない場合は再生成します。
   - 1-1 **[ストレージ]>[Storage VM]** の順にクリックし、Storage VM を選択します。
   - 1-2 **[設定]** タブで、S3 タイルの をクリックします。
   - 1-3 **[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。
   - 1-4 アクセスキーが表示されていない場合は、**[root]** の横にある から **[キーを再生成]** をクリックします。
     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. ソースとデスティネーションの両方で Storage VM を編集してユーザーを追加し、グループにユーザーを追加します。
   [ストレージ]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、S3 の下の をクリックします。
   詳細は、「S3 ユーザーとグループの作成」を参照してください。
3. 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror ポリシーを作成します。
   - 3-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。
   - 3-2 **[保護ポリシー]** の横にある をクリックし、**[追加]** をクリックします。
     - ポリシー名と説明を入力します。
     - ポリシースコープとして、クラスタまたは SVM を選択します。
     - S3 SnapMirror 関係に **[Continuous]** を選択します。
     - **[Throttle]** と **[Recovery Point Objective]** の値を入力します。
4. SnapMirror 保護がついたバケットを作成します。

4-1 **[ストレージ]>[バケット]** の順にクリックし、**[追加]** をクリックします。

4-2 バケット名を入力し、Storage VM を選択し、サイズを入力した後、**[その他のオプション]** をクリックします。

4-3 [権限] の下にある **[追加]** をクリックします。権限の検証はオプションですが、実行することを推奨します。

- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

4-4 **[保護]** で、**[SnapMirror を有効にする（ONTAP またはクラウド）]** チェックボックスをオンにします。次に、以下の値を入力します。

- デスティネーション
  - **TARGET**
    ONTAP System
  - **CLUSTER**
    リモートクラスタを選択します。
  - **STORAGE VM**
    リモートクラスタ上の Storage 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**
    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。

外部 CA ベンダーによって署名された証明書を使用する場合は、**[Use the same certificate on the destination]** チェックボックスをオンにします。

[Destination Settings] 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に独自の値を入力することもできます。

[保存] をクリックすると、新しいバケットがソース Storage VM に作成され、デスティネーション Storage VM に作成した新しいバケットにミラーリングされます。

CLI

1 この SVM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の SVM に存在することを確認し、キーが存在していない場合は再生成します。

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

root ユーザーのアクセスキーが存在していることを確認します。存在しない場合は、以下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 とデスティネーション SVM の両方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 SVM とデスティネーション SVM の両方のデフォルト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 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror 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]
```

パラメーター：

- `-type continuous`
  S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
- `-rpo`
  目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
- `-throttle`
  スループットおよび帯域幅の上限をキロバイト単位または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 サーバー証明書をインストールします。

5-1 *ソース* 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
```

5-2 *デスティネーション* 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 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。

詳細は、`security certificate install` のマニュアルページを参照してください。

6 S3 SnapMirror 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、デフォルトポリシーを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:/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
```

3.2 既存バケットのミラー関係の作成（ローカルクラスタ）

同一クラスタ上にある既存の S3 バケットの保護は、いつでも開始できます。たとえば、ONTAP 9.10.1 より前のリリースから S3 構成をアップグレードした場合などです。別の Storage VM またはソースと同じ Storage VM のバケットにデータをミラーリングできます。

要件

- ONTAP のバージョン、ライセンス、および S3 サーバー設定の要件を満たしていること。
- ソース Storage VM とデスティネーション Storage VM の間に、ピアリング関係が存在していること。
- CA 証明書は、ソース VM とデスティネーション VM の両方に必要です。自己署名 CA 証明書または外部 CA ベンダーによって署名された証明書を使用できます。

System Manager

1 この Storage VM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の Storage VM に存在することを確認し、キーが存在していない場合は再生成します。

1-1 **[ストレージ]>[Storage VM]** の順にクリックし、Storage VM を選択します。

1-2 **[設定]** タブで、**S3** タイルの をクリックします。

1-3 **[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。

1-4 アクセスキーが表示されていない場合は、**[root]** の横にある から **[キーを再生成]** をクリックします。
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 ソースとデスティネーションの両方の Storage VM で、ユーザーとグループのアクセス権が正しいことを確認します。
[ストレージ]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、S3 の下の をクリックします。

詳細は、「S3 ユーザーとグループの作成」を参照してください。

3 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror ポリシーを作成します。

3-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。

3-2 **[保護ポリシー]** の横にある →をクリックし、**[追加]** をクリックします。

- ポリシー名と説明を入力します。
- ポリシースコープとして、クラスタまたは SVM を選択します。
- S3 SnapMirror 関係に **[Continuous]** を選択します。
- **[Throttle]** と **[Recovery Point Objective]** の値を入力します。

4 設定後も、既存のバケットのバケットアクセスポリシーが要件を満たしていることを確認します。

4-1 **[ストレージ]>[バケット]** の順にクリックし、保護するバケットを選択します。

4-2 **[権限]** タブで、 **[編集]** をクリックし、**[権限]** 配下の **[追加]** をクリックします。

- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

5 S3 SnapMirror を使用して、既存のバケットを保護します。

5-1 **[ストレージ]>[バケット]** の順にクリックし、保護するバケットを選択します。

5-2 **[保護]** をクリックし、以下の値を入力します。

- デスティネーション
  - **TARGET**
    ONTAP System
  - **CLUSTER**
    ローカルクラスタを選択します。
  - **STORAGE VM**
    同一の Storage VM または別の Storage 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**
    *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。

外部 CA ベンダーによって署名された証明書を使用する場合は、**[Use the same certificate on the destination]** チェックボックスをオンにします。

[Destination Settings] 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に独自の値を入力することもできます。

[保存] をクリックすると、既存のバケットがデスティネーション Storage VM の新しいバケットにミラーリングされます。

CLI

1. この SVM の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の SVM に存在することを確認し、キーが存在していない場合は再生成します。

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

   root ユーザーのアクセスキーが存在していることを確認します。存在しない場合は、以下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. ミラーリングのターゲットとなるバケットをデスティネーション SVM に作成します。

   ```
   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. デフォルトバケットポリシーのアクセスルールが、ソース SVM とデスティネーション SVM の両方で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,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal - -resource test-bucket, test-bucket /*
   ```

4. 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror 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]
   ```

   パラメーター：

   - `-type continuous`
     S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
   - `-rpo`
     目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
   - `-throttle`
     スループットおよび帯域幅の上限をキロバイト単位または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 サーバー証明書をインストールします。

5-1 *ソース* 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
```

5-2 *デスティネーション* 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 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。

詳細は、`security certificate install` のマニュアルページを参照してください。

6 S3 SnapMirror 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、デフォルトポリシーを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
```

3.3 デスティネーションバケットからのテイクオーバーとデータ提供（ローカルクラスタ）

ソースバケット内のデータが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。

このタスクについて

テイクオーバー操作が実行されると、ソースバケットは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は読み取り / 書き込みに変換されるため、S3 SnapMirror 関係が逆転します。

無効にしたソースバケットが再び使用可能になると、S3 SnapMirror は 2 つのバケットの内容を自動的に再同期します。通常のボリューム SnapMirror 導入の場合のように、リレーションシップ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上にある場合、テイクオーバー操作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を実行し、データの提供を開始します。

1. **[保護]>[関係]** をクリックし、**[S3 SnapMirror]** を選択します。
2. ⋮ をクリックし、**[Failover]** を選択して、**[Failover]** 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操作を開始します。

   ```
   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
   ```

3.4 デスティネーションからバケットをリストアする（ローカルクラスタ）

ソースバケットのデータが失われたり破損したりした場合は、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入力します。

このタスクについて

デスティネーションバケットを既存のバケットまたは新しいバケットにリストアできます。リストア操作のターゲットバケットは、デスティネーションバケットの論理使用領域よりも大きい必要があります。

既存のバケットを使用する場合は、リストア操作を開始するときにバケットを空にする必要があります。リストアは時間内にバケットを「ロールバック」しない代わりに、空のバケットに以前の内容を入力します。

リストア操作は、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、バケットを選択します。
2. ⋮ をクリックし、**[Restore]** を選択します。
3. **[ソース]** で、**[既存バケット]**（デフォルト）または **[新規バケット]** を選択します。
   - **[既存バケット]**（デフォルト）にリストアするには、以下の操作を行います。
     (1) 既存バケットを検索するクラスタとストレージ VM を選択します。
     (2) 既存バケットを選択します。

4. デスティネーション S3 サーバーの CA 証明書の内容をコピーして貼り付けます。

   ■ **[新規バケット]** にリストアするには、以下の値を入力します。

   - 新しいバケットをホストするクラスタおよび Storage VM。
   - 新しいバケットの名前、容量、およびパフォーマンスのサービスレベル。
     詳細は、「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 サーバーの CA 証明書の内容。

5. **[デスティネーション]** で、ソース S3 サーバーの 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。

CLI

1. 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ます。詳細は、「3.1 新しいバケットのミラー関係の作成（ローカルクラスタ）」(P.15) 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操作を開始します。

   `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
```

4. クラウドターゲットによるバックアップ保護

4.1 クラウドターゲット関係の要件

ソース環境とターゲット環境が、クラウドターゲットに関する S3 SnapMirror 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認証情報が必要です。

クラスタがクラウドオブジェクトストアに接続できるようにするには、クラスタ上でクラスタ間ネットワークインターフェイスと IPspace を構成する必要があります。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には、各ノードにクラスタネットワークインターフェイスを作成して入力する必要があります。

StorageGRID ターゲットの場合は、以下の情報が必要です。

- 完全修飾ドメイン名（FQDN）または IP アドレスで表現されるサーバー名
- すでに存在しているバケットの名前
- アクセスキー
- 秘密鍵

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

AWS S3 ターゲットの場合、以下の情報が必要です。

- 完全修飾ドメイン名（FQDN）または IP アドレスで表現されるサーバー名
- すでに存在しているバケットの名前
- アクセスキー
- 秘密鍵

FQDN を 使用している場合 、ONTAP クラスタの管理ストレージ VM の DNS サーバーは、FQDN を IP アドレスに名前解決できる必要があります。

4.2 新しいバケットのバックアップ関係の作成（クラウドターゲット）

新しい S3 バケットを作成したら、すぐに StorageGRID システムまたは Amazon S3 デプロイメントのオブジェクトストアプロバイダにある S3 SnapMirror ターゲットバケットにバックアップできます。

要件

- オブジェクトストアプロバイダの有効なアカウント資格情報と構成情報があること。
- クラスタ間ネットワークインターフェイスと IPspace がソースシステムに構成されていること。
- ソース Storage 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]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、**S3** の下の をクリックします。
詳細は、「S3 ユーザーとグループの作成」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。

2-1 **[Protection]>[Overview]** をクリックし、**[Cloud Object Stores]** を選択します。

2-2 **[追加]** をクリックし、**Amazon S3** または **StorageGRID** を選択します。

2-3 以下の値を入力します。
- クラウドオブジェクトストア名
- URL スタイル（パスまたは仮想ホスト形式）
- Storage VM（S3 が有効のもの）
- オブジェクトストアサーバー名（FQDN）
- オブジェクトストア証明書
- アクセスキー
- 秘密キー
- コンテナ（バケット）名

3 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror ポリシーを作成します。

3-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。

3-2 **[保護ポリシー]** の横にある →をクリックし、**[追加]** をクリックします。
- ポリシー名と説明を入力します。
- ポリシースコープとして、クラスタまたは SVM を選択します。
- S3 SnapMirror 関係に **[Continuous]** を選択します。
- **[Throttle]** と **[Recovery Point Objective]** の値を入力します。

4 SnapMirror 保護がついたバケットを作成します。

4-1 **[ストレージ]>[バケット]** の順にクリックし、**[追加]** をクリックします。

4-2 バケット名を入力し、Storage 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。

4-3 **[権限]** の下にある **[追加]** をクリックします。権限の検証はオプションですが、実行することを推奨します。
- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

4-4 **[保護]** で、**[SnapMirror（ONTAP またはクラウド）を有効にする]** チェックボックスをオンにします。**[クラウドストレージ]>[クラウドオブジェクトストア]** の順に選択します。

[保存] をクリックすると、ソース Storage 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 の最初の S3 SnapMirror 関係を作成する場合は、root ユーザーキーがソースとデスティネーションの両方の SVM に存在することを確認し、キーが存在していない場合は再生成します。

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

root ユーザーのアクセスキーが存在していることを確認します。存在しない場合は、以下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 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror 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]
```

パラメーター：

- `-type continuous`
  S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
- `-rpo`
  目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
- `-throttle`
  スループットおよび帯域幅の上限をキロバイト単位または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、StorageGRID の CA サーバー証明書をソースクラスタの管理 SVM に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
```

詳細は、`security certificate install` のマニュアルページを参照してください。

6 S3 SnapMirror デスティネーション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
```

パラメーター：

- `-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です。
- `-usage`
  このワークフローでは、`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`
  ターゲットサーバーの FQDN または IP アドレスです。
- `-is-ssl-enabled`
  SSL の有効化はオプションですが、推奨されています。

詳細は、`snapmirror object-store config create` のマニュアルページ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 S3 SnapMirror 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
```

パラメーター：

- `-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` です。
  作成したポリシーを使用することも、デフォルトポリシーを使用することもできます。
  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
```

4.3 既存バケット のバックアップ関係の作成（クラウドターゲット）

既存 S3 バケットのバックアップはいつでも開始できます。たとえば、ONTAP 9.10.1 より前のリリースから S3 構成をアップグレードした場合などです。

要件

- オブジェクトストアプロバイダの有効なアカウント資格情報と構成情報があること。
- クラスタ間ネットワークインターフェイスと IPspace がソースシステムに構成されていること。
- ソースストレージ VM の DNS 設定は、ターゲットの FQDN を名前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]>[Storage VM] をクリックし、Storage VM を選択して **[設定]** をクリックしてから、S3 の下の をクリックします。
   詳細は、「S3 ユーザーとグループの作成」を参照してください。
2. 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror ポリシーを作成します。
   - 2-1 **[保護]>[概要]** をクリックし、**[ローカルポリシーの設定]** をクリックします。
   - 2-2 **[保護ポリシー]** の横にある →をクリックし、**[追加]** をクリックします。
   - 2-3 ポリシー名と説明を入力します。
   - 2-4 ポリシースコープとして、クラスタまたは SVM を選択します。
   - 2-5 S3 SnapMirror 関係に **[Continuous]** を選択します。
   - 2-6 **[Throttle]** と **[Recovery Point Objective]** の値を入力します。
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。
   - 3-1 **[Protection]>[Overview]** 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。
   - 3-2 **[Add]** をクリックし、StorageGRID ウェブスケールに **[Amazon S3]** または **[Others]** を選択します。
   - 3-3 以下の値を入力します。
     - クラウドオブジェクトストア名
     - URL スタイル（パスまたは仮想ホスト形式）
     - Storage VM（S3 が有効のもの）
     - オブジェクトストアサーバー名（FQDN）
     - オブジェクトストア証明書
     - アクセスキー
     - 秘密キー
     - コンテナ（バケット）名
4. 設定後も、既存のバケットのバケットアクセスポリシーが要件を満たしていることを確認します。
   - 4-1 **[ストレージ]>[バケット]** の順にクリックし、保護するバケットを選択します。

4-2 **[権限]** タブで、 **[編集]** をクリックし、**[権限]** 配下の **[追加]** をクリックします。

- **Principal** および **Effect**
  ユーザーグループ設定に応じた値を選択するか、デフォルトを設定します。
- **アクション**
  以下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/**）またはその他の必要な値を使用します。
  各フィールドについての詳細は、「バケットへのユーザーアクセスの管理」を参照してください。

5 S3 SnapMirror を使用して、バケットをバックアップします。

5-1 **[ストレージ]**>**[バケット]** の順にクリックし、保護するバケットを選択します。

5-2 **[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、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 既存のポリシーがなく、デフォルトのポリシーを使用しない場合は、S3 SnapMirror 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]
```

パラメーター：

- `-type continuous`
  S3 SnapMirror 関係の唯一のポリシータイプです（必須）。
- `-rpo`
  目標復旧時点（RPO）の時間を秒単位で指定します（オプション）。
- `-throttle`
  スループットおよび帯域幅の上限をキロバイト単位または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、StorageGRID CA 証明書をソースクラスタの管理 SVM に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
```

詳細は、security certificate install のマニュアルページを参照してください。

4 S3 SnapMirror のデスティネーション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
```

パラメーター：

- -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です。
- -usage
  このワークフローでは、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
  ターゲットサーバーの FQDN または IP アドレスです。
- -is-ssl-enabled
  SSL の有効化はオプションですが、推奨されています。

詳細は、snapmirror object-store config create のマニュアルページ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 S3 SnapMirror 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
```

パラメーター：

- -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 を指定します。
  作成したポリシーを使用することも、デフォルトポリシーを使用することもできます。
  例

```
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
```

4.4 クラウドターゲットからバケットを復元する

ソースバケットのデータが失われたり破損したりした場合は、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入力します。

このタスクについて

デスティネーションバケットを既存のバケットまたは新しいバケットにリストアできます。リストア操作のターゲットバケットは、デスティネーションバケットの論理使用領域よりも大きい必要があります。

既存のバケットを使用する場合は、リストア操作を開始するときにバケットを空にする必要があります。リストアは時間内にバケットを「ロールバック」しない代わりに、空のバケットに以前の内容を入力します。

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、**[S3 SnapMirror]** を選択します。
2. ⋮ をクリックし、**[Restore]** を選択します。
3. **[ソース]** で、**[既存バケット]**（デフォルト）または **[新規バケット]** を選択します。
   - **[既存バケット]**（デフォルト）にリストアするには、以下の操作を行います。
     (1) 既存バケットを検索するクラスタとストレージ VM を選択します。
     (2) 既存バケットを選択します。
     (3) *デスティネーション*S3 サーバーの CA 証明書の内容をコピーして貼り付けます。
   - **[新規バケット]** にリストアするには、以下の値を入力します。
     - 新しいバケットをホストするクラスタおよび Storage VM。
     - 新しいバケットの名前、容量、およびパフォーマンスのサービスレベル。
       詳細は、「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 サーバーの CA 証明書の内容。
4. **[デスティネーション]** で、*ソース* S3 サーバーの CA 証明書の内容をコピーして貼り付けます。
5. **[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。

CLI

1. 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ます。詳細は、「4.2 新しいバケットのバックアップ関係の作成（クラウドターゲット）」(P.24) 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操作を開始します。

   ```
   snapmirror restore -source-path object_store_name:/objstore -destination
   -path svm_name:/bucket/bucket_name
   ```

   例
   以下の例では、デスティネーションバケットを既存のバケットに復元します。

   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

5. ミラーポリシーの変更

RPO 値やスロットル値を調整する場合などは、S3 ミラーポリシーを変更する必要があります。

System Manager

これらの値を調整する場合は、既存の保護ポリシーを編集できます。

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 ⋮ から、**[編集]** を選択してクリックします。

CLI

1. S3 SnapMirror 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]
   ```

   パラメーター：

   - `-rpo`
     目標復旧時点（RPO）の時間を秒単位で指定します。
   - `-throttle`
     スループットおよび帯域幅の上限をキロバイト単位または秒単位で指定します。

   例

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

ETERNUS AX series オールフラッシュアレイ , ETERNUS HX series ハイブリッドアレイ
S3 SnapMirror によるバケットの保護

C140-0091-02Z3

発行年月　2025 年 3 月
発行責任　エフサステクノロジーズ株式会社

Fsas Technologies