



ローカルクラスタでのミラーとバックアップの 保護 ONTAP 9

NetApp
December 20, 2024

目次

ローカルクラスタでのミラーとバックアップの保護	1
新しいバケット（ローカルクラスタ）のミラー関係を作成する	1
既存のバケット（ローカルクラスタ）のミラー関係を作成する	5
デスティネーションバケット（ローカルクラスタ）からテイクオーバーしてデータを提供	9
デスティネーションStorage VM（ローカルクラスタ）からバケットをリストアする	10

ローカルクラスタでのミラーとバックアップの保護

新しいバケット（ローカルクラスタ）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きに、同じクラスタ上のSnapMirror S3デスティネーションでバケットをただちに保護することができます。データは、ソースと同じStorage VMまたは別の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が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
 - a. Storage > Storage VM* をクリックし、Storage VM を選択します。
 - b. [設定]タブで、[S3]タイトル内をクリックし  ます。
 - c. [Users] タブで、root ユーザのアクセスキーがあることを確認します
 - d. 表示されていない場合は、* root の横にあるをクリックし 、Regenerate Key *をクリックします。すでに存在するキーを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ます。[ストレージ]>[Storage VM]*をクリックし、Storage VMをクリックして[設定]*をクリックし、[S3]の下をクリックし  ます。

詳細については、を参照してください ["S3ユーザとグループの追加"](#)。

3. SnapMirror S3ポリシーを作成します（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）。
 - 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. の横にあるをクリックし 、[追加]*をクリックします。
 - ポリシーの名前と説明を入力します。
 - ポリシースコープ（クラスタまたはSVM）を選択します
 - SnapMirror S3関係の場合は*[Continuous]*を選択します。
 - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
 - a. [* 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。
 - b. 名前を入力し、Storage VM を選択してサイズを入力し、* その他のオプション * をクリックします。
 - c. [Permissions] で、[Add] をクリックします。権限の検証はオプションですが、推奨されます。
 - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
 - アクション-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-デフォルト値または必要なその他の値を使用します。(bucketname, bucketname/*)

これらのフィールドの詳細については、を参照してください ["バケットへのユーザアクセスの管理"](#)。

- d. [Protection] で、[Enable SnapMirror (ONTAP or Cloud)] をオンにします。次に、次の値を入

力します。

- デスティネーション
 - *ターゲット* : ONTAP システム
 - *cluster* : ローカルクラスタを選択します。
 - *Storage VM* : ローカルクラスタのStorage VMを選択します。
 - *S3 サーバ CA 証明書* : 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 サーバ 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. チェック *外部 CA ベンダーが署名し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します。
 6. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
 7. [保存 (Save)] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage 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でONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"[バケットを作成する](#)"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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
```

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

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

すでに存在するキーを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. SnapMirror S3ポリシーを作成します（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）。

```
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—目標復旧時点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. *destination_S3*サーバ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`。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

詳細については、のマニュアルページを参照して `security certificate install` 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
```




既存のバケット（ローカルクラスタ）のミラー関係を作成する

S3設定をONTAP 9.10.1より前のリリースからアップグレードした場合など、同じクラスタ上の既存のS3バケットの保護はいつでも開始できます。データは、ソースと同じStorage VMまたは別の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が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
 - a. Storage > Storage VM* をクリックし、Storage VM を選択します。
 - b. [設定]タブで、* S3 *タイトル内をクリックします 。
 - c. [Users] タブで、root ユーザのアクセスキーがあることを確認します。
 - d. 表示されていない場合は、* root の横にあるをクリックし 、Regenerate Key *をクリックします。キーがすでに存在する場合は再生成しない
2. ソースとデスティネーションの両方のStorage VMに既存のユーザとグループが存在し、正しいアクセス権があることを確認します。[ストレージ]>[Storage VM]*を選択し、Storage VMを選択して、[設定]タブを選択します。最後に、S3 タイトルを探し 、を選択して Users タブを選択し、Groups * タブを選択して、ユーザ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、を参照してください "[S3ユーザとグループの追加](#)"。

3. SnapMirror S3ポリシーを作成します（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）。
 - a. [* 保護]、[概要 *]の順にクリックし、[ローカルポリシーの設定 *] をクリックします。
 - b. の横にあるをクリックし 、[追加]*をクリックします。
 - ポリシーの名前と説明を入力します。
 - ポリシースコープ（クラスタまたはSVM）を選択します
 - SnapMirror S3関係の場合は*[Continuous]*を選択します。
 - スロットル値および * 目標復旧時点 * 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ニーズ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]の順にクリックし、保護するバケットを選択します。
 - b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
 - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
 - アクション-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-デフォルト値または必要なその他の値を使用します (*bucketname*, *bucketname/**)。

これらのフィールドの詳細については、を参照してください "[バケットへのユーザアクセスの管理](#)"。

5. SnapMirror S3で既存のバケットを保護します。
 - a. [* Storage * > * Buckets] をクリックして、保護するバケットを選択します。

b. [*Protect] をクリックして、次の値を入力します。

- デスティネーション

- * ターゲット * : ONTAP システム
- * cluster * : ローカルクラスタを選択します。
- * Storage VM * : 同じ Storage VM または別の Storage VM を選択します。
- * S3 サーバ CA 証明書 * : `_source_certificate` の内容をコピーして貼り付けます。

- ソース

- * S3 サーバ CA 証明書 * : `_destination_certificate` の内容をコピーして貼り付けます。

6. チェック * 外部 CA ベンダーが署名し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します。
7. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存 (Save)] をクリックします。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。

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でONTAP 9.14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"[バケットを作成する](#)"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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
```

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

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

すでに存在するキーを再生成しないでください。

2. ミラーターゲットとして使用するデスティネーションSVMに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へのアクセスルール

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. SnapMirror S3ポリシーを作成します（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）。

```
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`—目標復旧時点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. `destination_S3`サーバ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`。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

詳細については、のマニュアルページを参照して `security certificate install` 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
```

デスティネーションバケット（ローカルクラスタ）からテイクオーバーしてデータを提供

ソースバケット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。

タスクの内容

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るため、SnapMirror S3関係が反転されます。

無効にしたソースバケットが再び使用可能になると、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環境のように、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は、リモートクラスタからテイクオーバー処理を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、[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. フェイルオーバー処理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
```

デスティネーションStorage VM（ローカルクラスタ）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オブジェクトをリストアすることでデータを再取り込みできます。

タスクの内容


デスティネーションバケットは、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。リストア処理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使用済み論理スペースよりも大きくする必要があります。

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. [* 保護]、[関係]の順にクリックし、バケットを選択します。
2. をクリックし 、[* リストア]*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。
 - 既存の Bucket *（デフォルト）にリストアするには、次の操作を実行します。
 - クラスタとStorage VMを選択して既存のバケットを検索します。
 - 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。
 - 新しいバケットへのリストアを実行するには、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、[を参照してください "ストレージサービスレベル"](#)。
 - デスティネーションS3サーバCA証明書の内容。
5. 「* Destination *」の下にあるソース S3 サーバ CA 証明書の内容をコピーして貼り付けます。
6. [* 保護*] > [関係] の順にクリックして、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復元

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。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、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レプリケートされます。新しいバケットに対して別の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、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：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、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

CLI

1. オブジェクトを新しいバケットにリストアする場合は、新しいバケットを作成します。詳細については、[を参照してください "新しいバケット（クラウドターゲット）のバックアップ関係を作成"](#)。
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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。