



원격 클러스터의 미러링 및 백업 보호

ONTAP 9

NetApp
February 12, 2026

목차

원격 클러스터의 미러링 및 백업 보호	1
원격 클러스터에서 새로운 ONTAP S3 버킷에 대한 미러 관계를 생성합니다	1
원격 클러스터에서 기존 ONTAP S3 버킷에 대한 미러 관계를 생성합니다	5
원격 클러스터의 대상 ONTAP S3 버킷에서 테이크오버합니다	9
원격 클러스터의 타겟 SVM에서 ONTAP S3 버킷을 복원합니다	10

원격 클러스터의 미러링 및 백업 보호

원격 클러스터에서 새로운 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

새로운 S3 버킷을 생성하면 원격 클러스터의 SnapMirror S3 대상으로 즉시 보호할 수 있습니다.

이 작업에 대해

소스 시스템과 대상 시스템 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이선스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
 - a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
 - b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 [편집 아이콘].
 - c. 사용자 * 탭에서 루트 사용자에게 대한 액세스 키가 있는지 확인합니다.
 - d. 없으면 * root * 옆에 있는 을 클릭한 [메뉴 옵션 아이콘] 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 스토리지 VM을 편집하여 사용자를 추가하고 소스 및 대상 스토리지 VM 모두에서 사용자를 그룹에 추가하려면 다음을 수행합니다.

스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM, * 설정 * 을 차례로 클릭한 다음 [편집 아이콘] S3를 클릭합니다.

을 참조하십시오 "[S3 사용자 및 그룹 추가](#)" 를 참조하십시오.

3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
 - a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
 - b. [화살표 아이콘]보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
 - 정책 이름과 설명을 입력합니다.
 - 정책 범위, 클러스터 또는 SVM을 선택합니다
 - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
 - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.

4. SnapMirror 보호를 통해 버킷 생성:

- a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
- b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
- c. 사용 권한 * 에서 * 추가 * 를 클릭합니다.
 - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
 - * 조치 * - 다음 값이 표시되는지 확인합니다.

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

- * 리소스 * - 기본값(*bucketname*, *bucketname/* *) 또는 필요한 기타 값을 사용합니다.

을 참조하십시오 "[버킷에 대한 사용자 액세스를 관리합니다](#)" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) 활성화 * 를 선택합니다. 그런 다음 다음 다음 값을 입력합니다.

▪ 목적지

- * 대상: ONTAP 시스템 *
- * 클러스터 *: 원격 클러스터를 선택합니다.
- * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
- * S3 서버 CA 인증서 *: `_source_certificate`의 내용을 복사하여 붙여 넣습니다.

▪ 출처

- * S3 서버 CA 인증서: * `destination_certificate`의 내용을 복사하여 붙여 넣습니다.

5. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.

6. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.

7. 저장 * 을 클릭합니다. 소스 스토리지 VM에 새 버킷이 생성되면 대상 스토리지 VM을 생성한 새 버킷에 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 ["버킷을 만듭니다"](#).

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성

`'vserver object-store-server user show'`를 선택합니다

루트 사용자에게 대한 액세스 키가 있는지 확인합니다. 없는 경우 다음을 입력합니다.

`'vserver object-store-server user reenote-keys-vserver svm_name-user_root_'`

키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 소스 및 타겟 SVM 모두에 버킷 생성:

`'vserver object-store-server bucket create-vserver svm_name-bucket bucket_name[-size_integer_[KB|MB|GB|TB|PB]][-comment_text_][additional_options]'`

3. 소스 및 타겟 SVM의 기본 버킷 정책에 액세스 규칙을 추가합니다.

`'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_][-index_integer_]
```

예

```
src_cluster::> vsserver 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. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다.

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

매개 변수:

- 유형 continuous - SnapMirror S3 관계에 대한 유일한 정책 유형입니다(필수).
- -rpo - 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
- -throttle - 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

예

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

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 서버 인증서 설치:

- 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 CA 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vsserver_src_admin_svm-cert-name_dest_server_certificate_*'
- 대상 클러스터에서 *source_s3* 서버 인증서에 서명한 CA 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vsserver_dest_admin_svm-cert-name_src_server_certificate_*'

외부 CA 공급업체에서 서명한 인증서를 사용하는 경우, 소스 및 대상 관리 SVM에 동일한 인증서를 설치합니다.

에 대한 자세한 내용은 `security certificate install` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

```
'스냅미러 create-source-path_src_svm_name_:/bucket/bucket_name-destination  
-path_dest_peer_svm_name_:/bucket/bucket_name,...} [-policy policy_name]'입니다
```

생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

예

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

7. 미러링이 활성화 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- ["SnapMirror 생성"](#)
- ["스냅미러 정책 생성"](#)
- ["스냅미러 쇼"](#)

원격 클러스터에서 기존 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷을 보호할 수 있습니다.

이 작업에 대해

소스 및 대상 클러스터 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이선스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 미러 관계를 생성할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
 - a. 스토리지 > 스토리지 VM * 을 선택한 다음 스토리지 VM을 선택합니다.
 - b. 설정 * 탭에서 * S3 * 타일을 클릭합니다  .
 - c. 사용자 * 탭에서 루트 사용자에게 대한 액세스 키가 있는지 확인합니다.
 - d. 없으면 * root * 옆에 있는 을  클릭한 다음 * 키 재생성 * 을 클릭합니다 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 기존 사용자 및 그룹이 존재하고 소스 및 대상 스토리지 VM 모두에서 올바른 액세스 권한이 있는지 확인합니다. * 스토리지 > 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다. 마지막으로 * S3 * 타일을 찾아 를 선택하고  * 사용자 * 탭을 선택한 다음 * 그룹 * 탭을 선택하여 사용자 및 그룹 액세스 설정을 확인합니다.

을 참조하십시오 "[S3 사용자 및 그룹 추가](#)" 를 참조하십시오.

3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
 - a. 보호 > 개요 * 를 선택한 다음 * 로컬 정책 설정 * 을 클릭합니다.
 - b. 보호 정책 * 옆에 있는 을  선택한 다음 * 추가 * 를 클릭합니다.
 - c. 정책 이름과 설명을 입력합니다.
 - d. 클러스터 또는 SVM에서 정책 범위를 선택합니다.
 - e. SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
 - f. 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
 - a. 스토리지 > 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
 - b. 사용 권한 * 탭에서  * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
 - * Principal and Effect *: 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
 - * 조치 *: 다음 값이 표시되는지 확인하십시오.

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

- * 리소스 *: 기본값(*bucketname, bucketname/* *) 또는 필요한 기타 값을 사용합니다.

을 참조하십시오 "[버킷에 대한 사용자 액세스를 관리합니다](#)" 이 필드에 대한 자세한 내용은 를 참조하십시오.

5. SnapMirror S3 보호로 기존 버킷 보호:
 - a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
 - b. 보호 * 를 클릭하고 다음 값을 입력합니다.

- 목적지
 - * 대상 *: ONTAP 시스템
 - * 클러스터 *: 원격 클러스터를 선택합니다.
 - * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
 - * S3 서버 CA 인증서 *: `_source_certificate`의 내용을 복사하여 붙여 넣습니다.
- 출처
 - * S3 서버 CA 인증서 *: `_destination_certificate`의 내용을 복사하여 붙여 넣습니다.

6. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
7. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
8. 저장 * 을 클릭합니다. 기존 버킷은 대상 스토리지 VM의 새 버킷으로 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 ["버킷을 만듭니다"](#).

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우, 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우


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

 루트 사용자 키를 다시 생성하십시오. + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 이 없으면 다음을 입력합니다


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

 + 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 대상 SVM에서 미래 타겟으로 사용할 버킷을 생성합니다.

```
'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. 기본 버킷 정책의 액세스 규칙이 소스 및 타겟 SVM에서 모두 올바른지 확인합니다.

```
'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_]_[-index_integer_]'
```

예

```
src_cluster::> vsserver 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. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다.

'스냅샷 정책 생성 - vsserver svm_name - policy policy_name - type continuous [-RPO_integer_] [-throttle_throttle_type_] [-comment_text_] [additional_options]'

매개 변수:

- continuous – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
- '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
- '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

예

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

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 인증서 설치:

- 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 CA 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vsserver_src_admin_svm-cert-name_dest_server_certificate_*'
- 대상 클러스터에서 *SOURCE_S3* 서버 인증서에 서명한 CA 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vsserver_dest_admin_svm-cert-name_src_server_certificate_*' + 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 소스 및 대상 SVM 관리자에 동일한 인증서를 설치합니다.

에 대한 자세한 내용은 `security certificate install` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

'스냅미러 create-source-path_src_svm_name_:/bucket/bucket_name-destination-path dest_peer_svm_name:/bucket/bucket_name,...} [-policy policy_name]'

생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

예

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

7. 미러링이 활성화 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- ["SnapMirror 생성"](#)
- ["스냅미러 정책 생성"](#)
- ["스냅미러 쇼"](#)

원격 클러스터의 대상 **ONTAP S3** 버킷에서 테이크오버합니다

소스 버킷의 데이터를 사용할 수 없는 경우 SnapMirror 관계를 중단하여 대상 버킷에 대한 쓰기 가능 및 데이터 제공을 시작할 수 있습니다.

이 작업에 대해

테이크오버 작업이 수행되면 소스 버킷이 읽기 전용으로 전환되고 원래 타겟 버킷은 읽기-쓰기로 변환되어 SnapMirror S3 관계를 반대로 전환합니다.

비활성화된 소스 버킷을 다시 사용할 수 있게 되면 SnapMirror S3는 두 버킷의 콘텐츠를 자동으로 다시 동기화합니다. 볼륨 SnapMirror 구축에 필요한 것처럼 관계를 명시적으로 재동기화할 필요는 없습니다.

테이크오버 작업은 원격 클러스터에서 시작되어야 합니다.

SnapMirror S3는 소스 버킷에서 타겟 버킷으로 오브젝트를 복제하지만 소스 오브젝트 저장소의 사용자, 그룹 및 정책을 타겟 오브젝트 저장소로 복제하지 않습니다.

페일오버 이벤트 중에 클라이언트가 대상 버킷에 액세스할 수 있도록 대상 오브젝트 저장소에서 사용자, 그룹 정책, 권한 및 유사한 구성 요소를 구성해야 합니다.

대상 클러스터에서 사용자가 생성될 때 소스 키를 수동으로 제공하는 경우 소스 및 대상 사용자가 동일한 액세스 및 암호 키를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

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

시스템 관리자

사용할 수 없는 버킷에서 페일오버 및 데이터 서비스 시작:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을  클릭하고 * 페일오버 * 를 선택한 다음 * 페일오버 * 를 클릭합니다.

CLI를 참조하십시오

1. '스냅미러 페일오버 시작-목적지-PATH_svm_name_:/bucket/bucket_name' 대상 버킷에 대한 페일오버 작업을 시작합니다
2. 페일오버 작업의 상태 '스냅샷 표시 - 필드 상태'를 확인합니다

예

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

관련 정보

- ["S3 사용자 및 그룹 추가\(System Manager\)"](#)
- ["S3 사용자 생성\(CLI\)"](#)
- ["S3 그룹 생성 또는 수정\(CLI\)"](#)
- ["스냅미러 페일오버 시작"](#)
- ["스냅미러 쇼"](#)

원격 클러스터의 타겟 SVM에서 ONTAP S3 버킷을 복원합니다

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 오브젝트를 복원하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용된 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 콘텐츠로 채웁니다.

복구 작업은 원격 클러스터에서 시작해야 합니다.

시스템 관리자

백업된 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을  클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
 - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
 - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
 - 기존 버킷을 선택합니다.
 - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
 - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
 - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
 - 새로운 버킷의 이름, 용량 및 성능 서비스 수준.
을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
 - destination_s3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

잠긴 버킷을 복원합니다

ONTAP 9.14.1부터 잠긴 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

오브젝트 잠금 버킷은 새 버킷이나 기존 버킷으로 복원할 수 있습니다. 다음과 같은 시나리오에서 오브젝트 잠금 버킷을 대상으로 선택할 수 있습니다.

- * 새 버킷으로 복원 * : 오브젝트 잠금이 활성화된 경우, 버킷을 생성하여 오브젝트 잠금이 활성화된 버킷을 복원할 수 있습니다. 잠긴 버킷을 복원하면 원래 버킷의 오브젝트 잠금 모드와 보존 기간이 복제됩니다. 새 버킷에 대해 다른 잠금 보존 기간을 정의할 수도 있습니다. 이 보존 기간은 다른 소스의 잠기지 않은 개체에 적용됩니다.
- * 기존 버킷으로 복원 * : 기존 버킷에서 버전 관리 및 유사한 오브젝트 잠금 모드가 활성화되어 있는 한 오브젝트 잠금 버킷을 기존 버킷으로 복원할 수 있습니다. 원래 버킷의 보존 기간이 유지됩니다.
- * 비잠금 버킷 복원 * : 버킷에서 오브젝트 잠금이 활성화되지 않은 경우에도 오브젝트 잠금이 활성화되어 있고 소스 클러스터에 있는 버킷으로 복원할 수 있습니다. 버킷을 복원하면 잠기지 않은 모든 객체가 잠기며 대상 버킷의 보존 모드 및 기간을 적용할 수 있습니다.

CLI를 참조하십시오

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 "[새 ONTAP S3 버킷에 대한 클라우드 백업 관계를 생성한다](#)"참조하십시오.
2. 대상 버킷에 대한 복원 작업을 시작합니다. '스냅미러 복구 - 소스 - path_svm_name_:/bucket/bucket_name - destination-path_svm_name_:/bucket/bucket_name'

예

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

에 대한 자세한 내용은 `snapmirror restore` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.