



# **WORM** 파일 관리

## ONTAP 9

NetApp  
February 12, 2026

# 목차

WORM 파일 관리 .....	1
ONTAP SnapLock 사용하여 WORM 파일 관리 .....	1
ONTAP SnapLock 사용하여 WORM에 파일 커밋 .....	1
WORM에 파일을 수동으로 커밋합니다 .....	1
파일을 WORM에 자동으로 커밋합니다 .....	2
WORM 추가 가능 파일을 생성합니다 .....	3
명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성합니다 .....	3
볼륨 추가 모드를 사용하여 WORM 추가 가능 파일을 생성합니다 .....	4
ONTAP 볼트 대상의 WORM에 스냅샷 커밋 .....	5
ONTAP SnapMirror 사용하여 재해 복구를 위한 WORM 파일 미러링 .....	8
ONTAP SnapLock Legal Hold를 사용하여 소송 중 WORM 파일 보관 .....	12
ONTAP SnapLock 사용하여 WORM 파일 삭제 .....	13
SnapLock 관리자 계정을 만듭니다 .....	13
권한 있는 삭제 기능을 활성화합니다 .....	13
엔터프라이즈 모드 WORM 파일을 삭제합니다 .....	14

# WORM 파일 관리

## ONTAP SnapLock 사용하여 WORM 파일 관리

WORM 파일은 다음과 같은 방법으로 관리할 수 있습니다.

- "WORM에 파일을 커밋합니다"
- "볼트 대상에서 WORM에 스냅샷을 커밋합니다"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "소송 중에 WORM 파일 보존"
- "WORM 파일을 삭제합니다"

## ONTAP SnapLock 사용하여 WORM에 파일 커밋

파일을 수동으로 커밋하거나 자동으로 커밋하여 WORM(Write Once, Read Many)에 커밋할 수 있습니다. WORM 추가 가능 파일을 생성할 수도 있습니다.

### WORM에 파일을 수동으로 커밋합니다

파일을 읽기 전용으로 만들어 WORM에 파일을 수동으로 커밋합니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경할 수 있습니다. 응용 프로그램이 파일에 대한 쓰기를 완료했는지 확인하여 파일이 너무 일찍 커밋되지 않았는지 또는 많은 볼륨 때문에 자동 커밋 스캐너에 대한 배율 조정 문제가 있는지 확인하려면 파일을 수동으로 커밋하도록 선택할 수 있습니다.

#### 시작하기 전에

- 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- 파일에 쓸 수 있어야 합니다.

#### 이 작업에 대해

볼륨 ComplianceClock 시간은 명령이나 프로그램이 실행될 때 파일의 ctime 필드에 기록됩니다. ComplianceClock 시간은 파일의 보존 시간에 도달한 시점을 결정합니다.

#### 단계

1. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod -w document.txt
```

Windows 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
attrib +r document.txt
```

## 파일을 **WORM**에 자동으로 커밋합니다

SnapLock 자동 커밋 기능을 사용하면 파일을 WORM에 자동으로 커밋할 수 있습니다. 자동 커밋 기능은 자동 커밋 기간 동안 파일이 변경되지 않은 경우 SnapLock 볼륨에서 파일을 WORM 상태로 커밋합니다. 자동 커밋 기능은 기본적으로 비활성화되어 있습니다.

### 시작하기 전에

- 자동 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨이 온라인 상태여야 합니다.
- SnapLock 볼륨은 읽기-쓰기 볼륨이어야 합니다.



SnapLock 자동 커밋 기능은 볼륨에 있는 모든 파일을 검사하여 자동 커밋 요구 사항을 충족하는 경우 파일을 커밋합니다. 파일이 자동 커밋될 준비가 된 시점과 SnapLock 자동 커밋 스캐너에서 실제로 커밋된 시점 사이에 시간 간격이 있을 수 있습니다. 그러나 파일이 자동 커밋될 수 있는 즉시 파일 시스템에 의해 수정 및 삭제로부터 보호됩니다.

### 이 작업에 대해

`autocommit period _` 는 파일이 자동 커밋되기 전에 변경되지 않은 상태로 유지해야 하는 시간을 지정합니다. 자동 커밋 기간이 경과하기 전에 파일을 변경하면 파일의 자동 커밋 기간이 다시 시작됩니다.

다음 표에는 자동 커밋 기간에 대해 가능한 값이 나와 있습니다.

값	단위	참고
없음	-	기본값입니다.
5-5256000	분	-
1-87600)을 참조하십시오	시간	-
1-3650	일	-
1-120으로 설정합니다	개월	-
1-10	년	-



최소값은 5분이고 최대값은 10년입니다.

### 단계

1. SnapLock 볼륨의 파일을 WORM에 자동 커밋:

```
* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-autos커밋  
-period_autosit_period_*
```

에 대한 자세한 내용은 `volume snaplock modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령은 파일이 5시간 동안 변경되지 않는 한 SVM VS1 볼륨 'vol1'에 있는 파일을 자동으로 커밋합니다.

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

## WORM 추가 가능 파일을 생성합니다

WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성하거나 SnapLock\_VOLUME append mode\_feature를 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다.

## 명령 또는 프로그램을 사용하여 **WORM** 추가 가능 파일을 생성합니다

NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의  $n \times 256KB + 1$  바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

현재 활성 256KB 청크를 초과하는 순서가 없는 쓰기는 활성 256KB 청크가 최신 오프셋으로 재설정되고 이전 오프셋에 대한 쓰기가 실패하고 'ROFS(읽기 전용 파일 시스템)' 오류가 발생합니다. 쓰기 오프셋은 클라이언트 애플리케이션에 따라 다릅니다. WORM 추가 파일 쓰기 의미를 준수하지 않는 클라이언트는 쓰기 콘텐츠가 잘못 종료될 수 있습니다. 따라서 클라이언트가 순서가 지정되지 않은 쓰기에 대한 오프셋 제한을 따르는지 확인하거나 파일 시스템을 동기식 모드로 마운트하여 동기식 쓰기를 보장하는 것이 좋습니다.

단계

1. 적합한 명령 또는 프로그램을 사용하여 원하는 보존 시간으로 길이가 0인 파일을 생성합니다.

UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 길이가 0인 파일에서 document.txt:

```
touch -a -t 202011210600 document.txt
```

2. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod 444 document.txt
```

3. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 다시 쓰기 가능으로 변경합니다.



파일에 데이터가 없기 때문에 이 단계는 규정 준수 위험으로 간주되지 않습니다.

UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 쓰기 가능하게 만듭니다.

```
chmod 777 document.txt
```

4. 적절한 명령 또는 프로그램을 사용하여 파일에 데이터 쓰기를 시작합니다.

UNIX 셸에서 다음 명령을 사용하여 데이터를 document.txt에 씁니다.

```
echo test data >> document.txt
```



파일에 데이터를 더 이상 추가할 필요가 없는 경우 파일 권한을 다시 읽기 전용으로 변경합니다.

## 볼륨 추가 모드를 사용하여 **WORM** 추가 가능 파일을 생성합니다

ONTAP 9.3부터는 SnapLock\_VOLUME APPEND MODE\_(VAM) 기능을 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

- WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨을 마운트 해제하고 스냅샷과 사용자가 생성한 파일을 비워야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의  $n \times 256KB + 1$  바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

볼륨에 대해 자동 커밋 기간을 지정하면 자동 커밋 기간보다 긴 기간 동안 수정되지 않은 WORM 추가 가능 파일이 WORM에 커밋됩니다.



VAM은 SnapLock 감사 로그 볼륨에서 지원되지 않습니다.

단계

1. VAM 활성화:

```
* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-is-volume-append-mode
-enabled true|false *
```

에 대한 자세한 내용은 `volume snaplock modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령을 실행하면 SVM의 볼륨 'vol1'에서 VAM이 활성화됩니다.

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. 적합한 명령 또는 프로그램을 사용하여 쓰기 권한이 있는 파일을 만듭니다.

파일은 기본적으로 WORM-appendable입니다.

## ONTAP 볼트 대상의 WORM에 스냅샷 커밋

SnapVault용 SnapLock를 사용하여 보조 스토리지에서 WORM으로 스냅샷을 보호할 수 있습니다. 볼트 대상에서 모든 기본 SnapLock 작업을 수행합니다. 대상 볼륨은 읽기 전용으로 자동 마운트되므로 WORM에 스냅샷을 명시적으로 커밋할 필요가 없습니다.

시작하기 전에

- System Manager를 사용하여 관계를 구성하려면 소스 클러스터와 대상 클러스터 모두에서 ONTAP 9.15.1 이상이 실행 중이어야 합니다.
- 대상 클러스터에서:
  - ["SnapLock 라이선스를 설치합니다"](#).
  - ["준수 시계를 초기화합니다"](#).
  - 9.10.1 이전의 ONTAP 릴리즈와 함께 CLI를 사용하는 경우, ["SnapLock 애그리게이트를 생성합니다"](#).
- 보호 정책은 "볼트" 유형이어야 합니다.
- 소스 및 타겟 애그리게이트는 64비트여야 합니다.
- 소스 볼륨은 SnapLock 볼륨일 수 없습니다.
- ONTAP CLI를 사용하는 경우 소스 볼륨과 타겟 볼륨을 에서 생성해야 합니다 ["피어링된 클러스터"](#) 및 ["SVM"](#).

이 작업에 대해

소스 볼륨은 NetApp 또는 비 NetApp 스토리지를 사용할 수 있습니다.



WORM 상태로 커밋된 스냅샷의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.



LUN은 SnapLock 볼륨에서 지원되지 않습니다. LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 하지만 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을 사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다. '-snaplock-type' 볼륨 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 SnapLock 모드, 규정 준수 또는 엔터프라이즈가 aggregate에서 상속됩니다. 버전에 상관없이 유연한 타겟 볼륨이 지원되지 않습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

볼트 대상인 SnapLock 볼륨에 기본 보존 기간이 할당되어 있습니다. 이 기간의 값은 처음에 SnapLock 엔터프라이즈 볼륨의 경우 0년, SnapLock 규정 준수 볼륨의 경우 최대 30년으로 설정됩니다. 각 NetApp 스냅샷은 처음에는 이 기본 보존 기간을 사용하여 커밋됩니다. 필요한 경우 보존 기간을 나중에 연장할 수 있습니다. 자세한 내용은 ["보존 시간 개요를 설정합니다"](#) 참조하십시오.

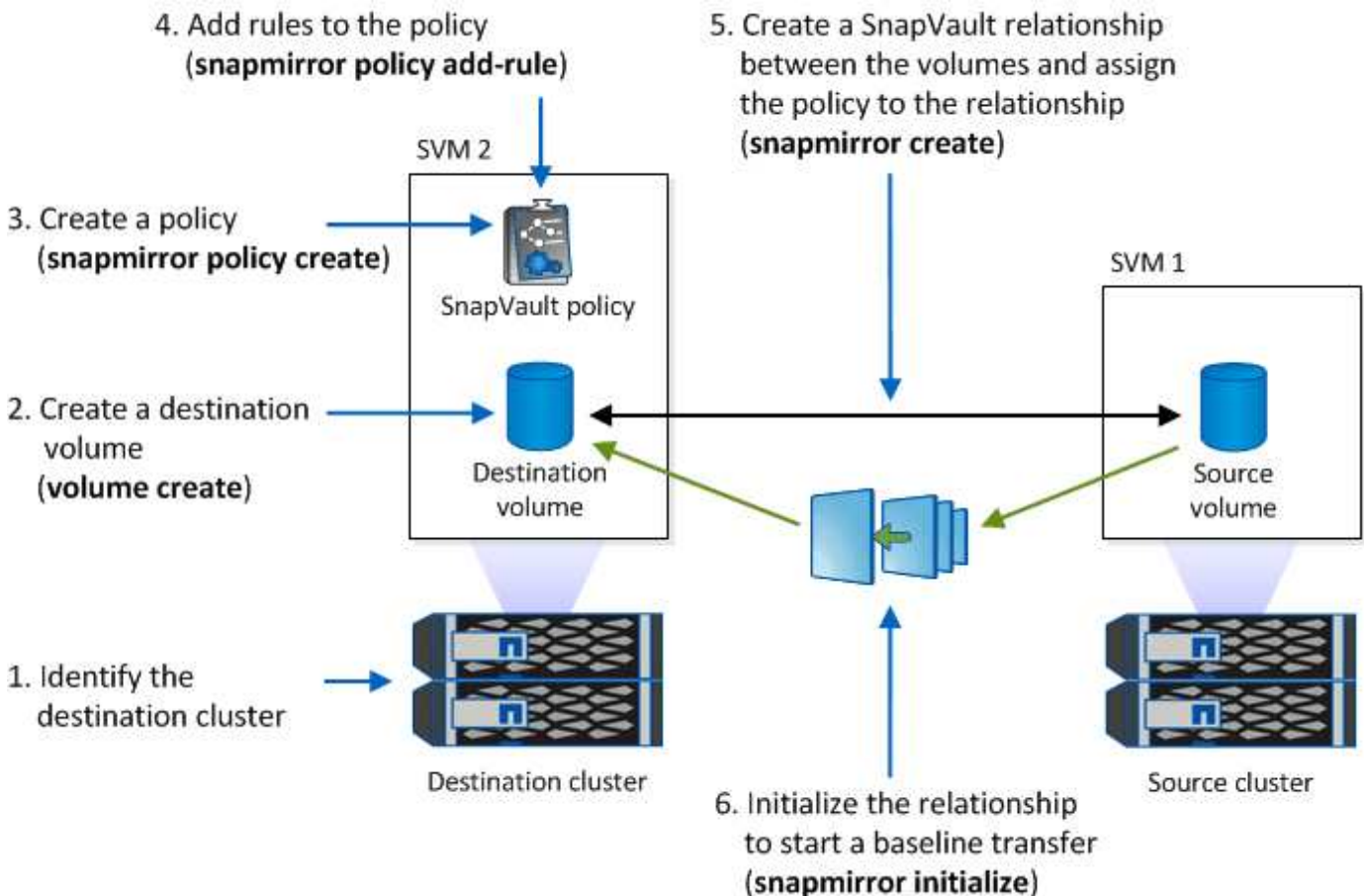
ONTAP 9.14.1부터 SnapMirror 관계의 SnapMirror 정책에서 특정 SnapMirror 레이블에 대한 보존 기간을 지정하여 소스에서 대상 볼륨으로의 복제된 스냅샷이 규칙에 지정된 보존 기간 동안 보존되도록 할 수 있습니다. 보존 기간을 지정하지 않으면 대상 볼륨의 기본 보존 기간이 사용됩니다.

ONTAP 9.13.1부터 옵션을 로 설정한 non-snaplock 상태로 FlexClone을 생성하고 볼륨 클론 생성 작업을 실행할 때 스냅샷을 "상위-스냅샷"으로 지정하여 SnapLock 소산 관계의 대상 SnapLock 볼륨에서 잠긴 스냅샷을 즉시 복원할 수 있습니다 snaplock-type. 에 대해 자세히 ["SnapLock 형식으로 FlexClone 볼륨 생성"](#) 알아보십시오.

MetroCluster 구성의 경우 다음 사항에 유의해야 합니다.

- 동기식 소스 SVM과 동기식-타겟 SVM 간에는 동기식-소스 SVM 사이만이 아니라 SnapVault 관계를 생성할 수 있습니다.
- 동기화 소스 SVM의 볼륨에서 데이터 지원 SVM으로 SnapVault 관계를 생성할 수 있습니다.
- 데이터 지원 SVM의 볼륨에서 동기화 소스 SVM의 DP 볼륨으로 SnapVault 관계를 생성할 수 있습니다.

다음 그림에서는 SnapLock 볼트 관계를 초기화하는 절차를 보여 줍니다.



단계

ONTAP CLI를 사용하여 SnapLock 볼트 관계를 만들거나, ONTAP 9.15.1부터 시스템 관리자를 사용하여 SnapLock 볼트 관계를 만들 수 있습니다.

## 시스템 관리자

1. 볼륨이 아직 없는 경우 소스 클러스터에서 \* 스토리지 > 볼륨 \* 으로 이동한 후 \* 추가 \* 를 선택합니다.
2. Add Volume \* (볼륨 추가 \*) 창에서 \* More Options \* (추가 옵션 \*)를 선택합니다.
3. 볼륨 이름, 크기, 익스포트 정책 및 공유 이름을 입력합니다.
4. 변경 사항을 저장합니다.
5. 대상 클러스터에서 \* 보호 > 관계 \* 로 이동합니다.
6. 소스 \* 열 위에서 \* 보호 \* 를 선택하고 메뉴에서 \* 볼륨 \* 을 선택합니다.
7. protect volumes \* 창에서 보호 정책으로 \* Vault \* 를 선택합니다.
8. 소스 \* 섹션에서 보호할 클러스터, 스토리지 VM 및 볼륨을 선택합니다.
9. 대상 \* 섹션의 \* 구성 세부 정보 \* 에서 \* 대상 스냅샷 잠금 \* 을 선택한 다음 잠금 방법으로 \* SnapLock for SnapVault \* 를 선택합니다. \* 선택한 정책 유형이 유형이 아닌 경우, SnapLock 라이선스가 설치되지 않았거나 규정 준수 클럭이 초기화되지 않은 경우 \* 잠금 방법 \* 이 표시되지 vault 않습니다.
10. 아직 활성화되지 않은 경우 \* SnapLock 준수 클럭 초기화 \* 를 선택합니다.
11. 변경 사항을 저장합니다.

## CLI를 참조하십시오

1. 대상 클러스터에서 소스 볼륨보다 크거나 같은 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate  
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP  
-size <size>
```

다음 명령을 실행하면 이름이 2GB SnapLock Compliance 볼륨이 생성됩니다 dstvolB 인치 SVM2  
애그리게이트 node01\_aggr:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. 대상 클러스터에서 "기본 보존 기간을 설정합니다".
3. "새 복제 관계를 생성합니다" 비 SnapLock 소스와 사용자가 생성한 새 SnapLock 대상 간

이 예에서는 매일 및 매주 레이블이 지정된 스냅샷을 시간별 일정에 따라 볼팅하는 정책을 사용하여  
XDPDefault 대상 SnapLock 볼륨과의 새로운 SnapMirror 관계를 dstvolB 생성합니다.

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



"사용자 지정 복제 정책을 생성합니다" 또는 a "사용자 지정 일정" 사용 가능한 기본값이  
적합하지 않은 경우

4. 대상 SVM에서 생성된 SnapVault 관계를 초기화합니다.

```
snapmirror initialize -destination-path <destination_path>
```

다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 관계가 초기화되고 유효 상태가 되면 대상에서 명령을 사용하여 `snapshot show` 복제된 스냅샷에 적용되는 SnapLock 만료 시간을 확인합니다.

이 예에서는 SnapMirror 레이블과 SnapLock 만료 날짜가 있는 볼륨의 스냅샷을 `dstvolB` 나열합니다.

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

#### 관련 정보

- ["클러스터 및 SVM 피어링"](#)
- ["SnapVault를 사용한 볼륨 백업"](#)
- ["SnapMirror 초기화"](#)

## ONTAP SnapMirror 사용하여 재해 복구를 위한 WORM 파일 미러링

SnapMirror를 사용하여 재해 복구 및 기타 목적으로 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 소스 볼륨과 타겟 볼륨을 모두 SnapLock에 대해 구성해야 하며 두 볼륨 모두 동일한 SnapLock 모드, Compliance 또는 Enterprise를 사용해야 합니다. 볼륨과 파일의 모든 주요 SnapLock 속성이 복제됩니다.

#### 필수 구성 요소

피어링된 SVM이 있는 클러스터에서 소스 및 타겟 볼륨을 생성해야 합니다. 자세한 내용은 ["클러스터 및 SVM 피어링"](#) 참조하십시오.

#### 이 작업에 대해

- ONTAP 9.5부터 DP(데이터 보호) 유형 관계가 아닌 XDP(확장된 데이터 보호) 유형의 SnapMirror 관계로 WORM 파일을 복제할 수 있습니다. XDP 모드는 ONTAP 버전에 독립적이며 동일한 블록에 저장된 파일을 구분할 수 있으므로 복제된 Compliance 모드 볼륨을 재동기화하는 것이 훨씬 쉬워집니다. 기존 DP 유형 관계를 XDP 유형 관계로 변환하는 방법에 대한 자세한 내용은 ["데이터 보호"](#) 참조하십시오.
- SnapLock에서 데이터 손실을 결정하면 DP 유형의 SnapMirror 관계에 대한 재동기화 작업이 Compliance-Mode 볼륨에 대해 실패합니다. 재동기화 작업이 실패하면 "volume clone create" 명령을 사용하여 대상 볼륨의 클론을 생성할 수 있습니다. 그런 다음 소스 볼륨을 클론과 다시 동기화할 수 있습니다.

- SnapLock 볼륨의 SnapMirror 관계는 다음을 지원합니다. `MirrorAllSnapshots async-mirror` 유형의 정책입니다. SnapLock 볼륨의 보존 기간은 볼륨이 보유하고 있는 모든 WORM 파일 중 최대 보존 기간에 따라 결정됩니다. 대상이 소스의 DR 복사본이므로 대상 SnapLock 볼륨의 보존 기간은 소스와 동일합니다.
- SnapLock 호환 볼륨 간의 XDP 유형의 SnapMirror 관계는 중단 후 대상의 데이터가 소스(중단 후)에서 분기된 경우에도 중단 후 재동기화를 지원합니다.

재동기화에서 일반 스냅샷을 넘어 소스 간에 데이터 발산이 감지되면 대상에서 새 스냅샷이 잘려 이러한 발산을 캡처합니다. 새 스냅샷과 공통 스냅샷은 모두 다음과 같이 보존 시간으로 잠깁니다.

- 대상의 볼륨 만료 시간입니다
- 볼륨 만료 시간이 지난 시간이거나 설정되지 않은 경우 스냅샷이 30일 동안 잠깁니다
- 대상에 법적 보류가 있는 경우 실제 볼륨 만료 기간이 마스킹되고 "무제한"으로 표시됩니다. 그러나 실제 볼륨 만료 기간 동안 스냅샷은 잠깁니다.

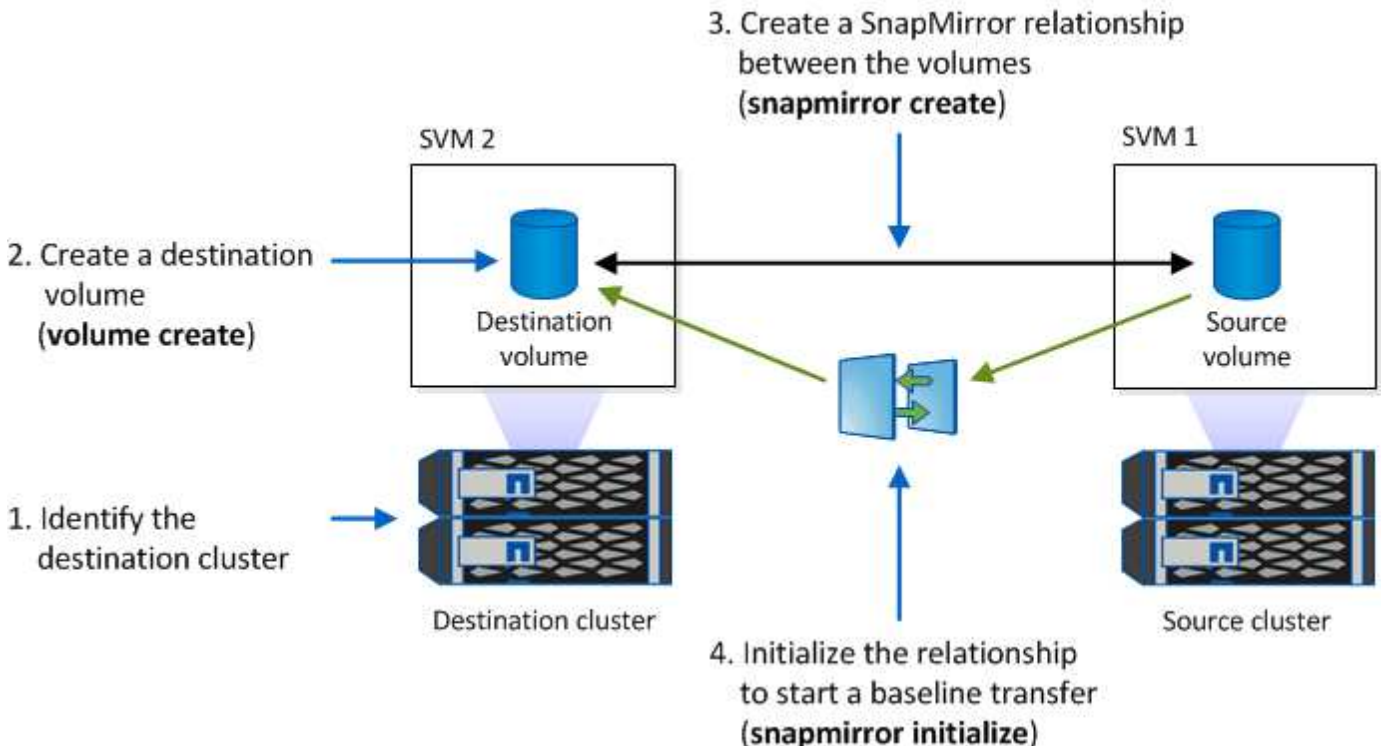
대상 볼륨의 만료 기간이 소스보다 이후인 경우 대상 만료 기간이 유지되고 재동기화 후 소스 볼륨의 만료 기간에 의해 덮어쓰이지 않습니다.

대상과 소스가 다른 법적 구속이 있는 대상에는 재동기화가 허용되지 않습니다. 재동기화를 시도하기 전에 소스와 대상에서 동일한 법적 증거 자료 보관 또는 모든 법적 고지를 해제해야 합니다.

다양한 데이터를 캡처하기 위해 생성된 대상 볼륨의 잠긴 스냅샷은 CLI를 사용하여 소스에 복사할 수 있습니다 `snapmirror update -s snapshot`. 복제된 스냅샷은 소스에서 계속 잠깁니다.

- SVM 데이터 보호 관계는 지원되지 않습니다.
- 로드 공유 데이터 보호 관계는 지원되지 않습니다.


다음 그림에서는 SnapMirror 관계를 초기화하는 절차를 보여 줍니다.



## 시스템 관리자

ONTAP 9.12.1부터 System Manager를 사용하여 WORM 파일의 SnapMirror 복제를 설정할 수 있습니다.

### 단계

1. Storage > Volumes \* 로 이동합니다.
2. 표시/숨기기 \* 를 클릭하고 \* SnapLock 유형 \* 을 선택하여 \* 볼륨 \* 창에 열을 표시합니다.
3. SnapLock 볼륨을 찾습니다.
4. 을  클릭하고 \* 보호 \* 를 선택합니다.
5. 대상 클러스터와 대상 스토리지 VM을 선택합니다.
6. 추가 옵션 \* 을 클릭합니다.
7. 기존 정책 표시 \* 를 선택하고 \* DPDefault(레거시) \* 를 선택합니다.
8. Destination Configuration details \* 섹션에서 \* Override transfer schedule \* 을 선택하고 \* hourly \* 를 선택합니다.
9. 저장 \* 을 클릭합니다.
10. 소스 볼륨 이름 왼쪽의 화살표를 클릭하여 볼륨 세부 정보를 확장하고 페이지 오른쪽의 원격 SnapMirror 보호 세부 정보를 검토합니다.
11. 원격 클러스터에서 \* 보호 관계 \* 로 이동합니다.
12. 관계를 찾고 대상 볼륨 이름을 클릭하여 관계 세부 정보를 봅니다.
13. 대상 볼륨 SnapLock 유형 및 기타 SnapLock 정보를 확인합니다.

### CLI를 참조하십시오

1. 대상 클러스터를 식별합니다.
2. 대상 클러스터에서 "SnapLock 라이선스를 설치합니다", "준수 시계를 초기화합니다" 및 9.10.1 이전의 ONTAP 릴리즈를 사용하는 경우, "SnapLock 애그리게이트를 생성합니다"
3. 대상 클러스터에서 소스 볼륨과 크기가 같거나 더 큰 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

\* 볼륨 생성 - vserver\_SVM\_name\_-volume\_volume\_name\_-aggregate\_aggregate\_name\_-snaplock-type compliance|enterprise-type dp-size\_size\_ \*



ONTAP 9.10.1부터 SnapLock 볼륨과 SnapLock 아닌 볼륨이 동일한 집계에 존재할 수 있습니다. 따라서 ONTAP 9.10.1을 사용하는 경우 별도의 SnapLock 집계를 만들 필요가 없습니다. 볼륨 -snaplock-type 옵션을 사용하여 규정 준수 또는 엔터프라이즈 SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리스에서는 SnapLock 모드(규정 준수 또는 엔터프라이즈)가 집계에서 상속되었습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

다음 명령을 실행하면 node01\_aggr 집계 'sVM2'에 dstvolB라는 이름의 2GB SnapLock 'Compliance' 볼륨이 생성됩니다.

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. 대상 SVM에서 SnapMirror 정책을 생성합니다.

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

다음 명령을 실행하면 SVM 전체의 정책 'VM1-mirror'가 생성됩니다.

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. 대상 SVM에서 SnapMirror 일정을 생성합니다.

\* 작업 일정 cron create-name\_schedule\_name\_-DayOfWeek\_day\_of\_week\_-hour\_hour\_-minute\_minute\_\*

다음 명령을 실행하면 "weekendcron"이라는 SnapMirror 스케줄이 생성됩니다.

```
SVM2::> job schedule cron create -name weekendcron -dayofweek  
"Saturday, Sunday" -hour 3 -minute 0
```

6. 대상 SVM에서 SnapMirror 관계 생성:

```
snapmirror create -source-path source_path -destination-path  
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 SnapMirror 관계가 생성되고 정책 'VM1-mirror'와 스케줄 'weekendcron'이 할당됩니다.

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule  
weekendcron
```



XDP 유형은 ONTAP 9.5 이상에서 사용할 수 있습니다. ONTAP 9.4 이전 버전에서 DP 유형을 사용해야 합니다.

7. 대상 SVM에서 SnapMirror 관계를 초기화합니다.

```
snapmirror initialize -destination-path destination_path
```

초기화 프로세스는 대상 볼륨에 대해 \_baseline 전송\_을 수행합니다. SnapMirror는 소스 볼륨의 스냅샷을 만든 다음 복사본과 이 복사본이 타겟 볼륨에 참조하는 모든 데이터 블록을 전송합니다. 또한 소스 볼륨의 다른 모든 스냅샷을 대상 볼륨으로 전송합니다.

다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

## 관련 정보

- ["클러스터 및 SVM 피어링"](#)
- ["볼륨 재해 복구 준비"](#)
- ["데이터 보호"](#)
- ["SnapMirror 생성"](#)
- ["SnapMirror 초기화"](#)
- ["스냅미러 정책 생성"](#)

# ONTAP SnapLock Legal Hold를 사용하여 소송 중 WORM 파일 보관

ONTAP 9.3부터는 *Legal Hold* 기능을 사용하여 소송 기간 동안 준수 모드 WORM 파일을 보존할 수 있습니다.

## 시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.  
["SnapLock 관리자 계정을 만듭니다"](#)
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

## 이 작업에 대해

법적 증거 자료 보관 아래에 있는 파일은 무기한 보존 기간이 있는 WORM 파일처럼 작동합니다. 법적 증거 자료 보관 기간이 끝나는 시기를 지정하는 것은 귀하의 책임입니다.

법적 증거 자료 보관 아래에 넣을 수 있는 파일 수는 볼륨에서 사용 가능한 공간에 따라 다릅니다.

## 단계

### 1. 법적 증거 자료 보관 시작:

```
snaplock legal-hold begin -litigation-name <litigation_name> -volume  
<volume_name> -path <path_name>
```

다음 명령은 'vol1'의 모든 파일에 대해 법적 대기를 시작합니다.

```
cluster1::>snaplock legal-hold begin -litigation-name litigation1  
-volume vol1 -path /
```

### 2. 법적 증거 자료 보관 종료:

```
snaplock legal-hold end -litigation-name <litigation_name> -volume  
<volume_name> -path <path_name>
```

다음 명령은 'vol1'의 모든 파일에 대해 법적 보류를 종료합니다.

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume  
vol1 -path /
```

#### 관련 정보

- ["SnapLock 법적 증거 자료 보관 이 시작됩니다"](#)
- ["SnapLock 법적 증거 자료 보관 종료"](#)

## ONTAP SnapLock 사용하여 WORM 파일 삭제

권한 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다. 이 기능을 사용하려면 먼저 SnapLock 관리자 계정을 만든 다음 계정을 사용하여 기능을 활성화해야 합니다.

### SnapLock 관리자 계정을 만듭니다

권한 있는 삭제를 수행하려면 SnapLock 관리자 권한이 있어야 합니다. 이러한 권한은 vsadmin-SnapLock 역할에 정의되어 있습니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 SnapLock 관리자 역할을 가진 SVM 관리자 계정을 만들도록 요청할 수 있습니다.

#### 시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

#### 단계

1. SnapLock 관리자 역할을 사용하여 SVM 관리자 계정을 생성합니다.

```
* 보안 로그인 create-vserver_SVM_name_-user-or-group-name_user_or_group_name_-  
application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_*
```

다음 명령을 실행하면 사전 정의된 "vsadmin-snaplock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 'VM1'에 액세스할 수 있습니다.

```
cluster1::> security login create -vserver SVM1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role vsadmin-  
snaplock
```

에 대한 자세한 내용은 security login create ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

### 권한 있는 삭제 기능을 활성화합니다

삭제하려는 WORM 파일이 포함된 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 명시적으로 활성화해야 합니다.

이 작업에 대해

'-privileged-delete' 옵션의 값은 권한 있는 삭제 활성화 여부를 결정합니다. 가능한 값은 '사용', '사용 안 함', '영구 사용 안 함'입니다.



영구 불활성 상태가 단자다. 상태를 "영구 비활성화"로 설정한 후에는 볼륨에 대한 권한 있는 삭제를 활성화할 수 없습니다.

#### 단계

1. SnapLock 엔터프라이즈 볼륨에 대한 권한 있는 삭제 활성화:

```
* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-privileged-delete disabled|enabled|permanently-disabled *
```

다음 명령을 실행하면 'VM1'의 엔터프라이즈 볼륨 'dataVol'에 대한 권한 있는 삭제 기능이 활성화됩니다.

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged -delete enabled
```

## 엔터프라이즈 모드 **WORM** 파일을 삭제합니다

권한이 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다.

#### 시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.
- SnapLock 감사 로그를 생성하고 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 활성화해야 합니다.

#### 이 작업에 대해

만료된 WORM 파일을 삭제하려면 권한이 있는 삭제 작업을 사용할 수 없습니다. 명령을 사용하여 `volume file retention show` 삭제하려는 WORM 파일의 보존 시간을 볼 수 있습니다. 에 대한 자세한 내용은 `volume file retention show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### 단계

1. 엔터프라이즈 볼륨에서 WORM 파일 삭제:

```
* 볼륨 파일 권한이 있는-삭제-vserver_SVM_name_-file_file_path_*
```

다음 명령을 실행하면 SVM 'sVM1'에서 파일 '/vol/dataVol/F1'이 삭제됩니다.

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

## 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.