WORM 파일 관리

ONTAP 9

NetApp
April 24, 2024

목차

WORM 파일 관리

WORM 파일 관리

WORM 파일은 다음과 같은 방법으로 관리할 수 있습니다.

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

WORM에 파일을 커밋합니다

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.

필요한 것

- 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 WORM에 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.

필요한 것

- 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_ *'

   전체 옵션 목록은 명령에 대한 man 페이지를 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.

필요한 것

WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.

이 작업에 대해

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

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.

필요한 것

- WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨은 마운트 해제되고 스냅샷 복사본과 사용자 생성 파일이 비어 있어야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의 n×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 *

   전체 옵션 목록은 명령에 대한 man 페이지를 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.

볼트 대상에서 WORM에 스냅샷 복사본을 커밋합니다

SnapLock for SnapVault를 사용하여 2차 스토리지에서 WORM 상태로 스냅샷 복사본을 보호할 수 있습니다. 볼트 대상에서 모든 기본 SnapLock 작업을 수행합니다. 타겟 볼륨이 읽기 전용으로 자동 마운트되므로 Snapshot 복사본을 WORM에 명시적으로 커밋할 필요가 없습니다. 따라서 SnapMirror 정책을 사용하여 타겟 볼륨에 예약된 Snapshot 복사본을 생성하는 것은 지원되지 않습니다.

시작하기 전에

- 소스 클러스터는 ONTAP 8.2.2 이상을 실행해야 합니다.
- 소스 및 타겟 애그리게이트는 64비트여야 합니다.
- 소스 볼륨은 SnapLock 볼륨일 수 없습니다.
- 피어링된 SVM이 있는 클러스터에서 소스 및 타겟 볼륨을 생성해야 합니다.

  자세한 내용은 을 참조하십시오 "클러스터 피어링".

- 볼륨 자동 확장 기능을 사용하지 않는 경우 대상 볼륨의 여유 공간은 소스 볼륨의 사용된 공간보다 최소 5% 이상 커야 합니다.

이 작업에 대해

소스 볼륨에서 NetApp 또는 타사 스토리지를 사용할 수 있습니다. 타사 스토리지의 경우 FlexArray 가상화를 사용해야 합니다.

> WORM 상태로 커밋된 스냅샷 복사본의 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 스냅샷 복사본이 SnapLock 볼트 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 그러나 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 무단 스냅샷 복사본이 지원됩니다.

ONTAP 9.14.1부터 SnapMirror 관계의 SnapMirror 정책에 특정 SnapMirror 레이블에 대한 보존 기간을 지정하여 소스에서 타겟 볼륨까지 복제된 스냅샷 복사본이 규칙에 지정된 보존 기간 동안 유지되도록 할 수 있습니다. 보존 기간을 지정하지 않으면 대상 볼륨의 기본 보존 기간이 사용됩니다.

ONTAP 9.13.1부터 에 FlexClone을 생성하여 SnapLock 소산 관계의 대상 SnapLock 볼륨에서 잠긴 스냅샷 복사본을 즉시 복원할 수 있습니다 `snaplock-type` 볼륨 클론 생성 작업을 실행할 때 옵션을 "비 SnapLock"으로 설정하고 Snapshot 복사본을 "상위 스냅샷"으로 지정합니다. 에 대해 자세히 알아보십시오 "SnapLock 형식으로 FlexClone 볼륨 생성".

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

1. 대상 클러스터를 식별합니다.
2. 대상 클러스터에서 "SnapLock 라이센스를 설치합니다", "준수 시계를 초기화합니다"9.10.1 이전 버전의 ONTAP 릴리스를 사용하는 경우 "SnapLock 애그리게이트를 생성합니다".
3. 대상 클러스터에서 소스 볼륨보다 크거나 같은 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 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을 사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다. volume-snaplock-type 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.

   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. 에 설명된 대로 대상 클러스터에서 기본 보존 기간을 설정합니다 기본 보존 기간을 설정합니다.

   > 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 스냅샷 복사본은 처음에 이 기본 보존 기간을 사용하여 커밋됩니다. 필요한 경우 보존 기간을 나중에 연장할 수 있습니다. 자세한 내용은 을 참조하십시오 보존 시간 개요를 설정합니다.

5. 새 복제 관계를 생성합니다 비 SnapLock 소스와 3단계에서 생성한 새 SnapLock 대상 간

   이 예에서는 일별 및 주별 이라는 레이블이 지정된 스냅샷 복사본을 시간별 스케줄로 저장할 수 있는 "XDPDefault" 정책을 사용하여 대상 SnapLock 볼륨 DstvolB와 새로운 SnapMirror 관계를 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

6. 대상 SVM에서 5단계에서 생성한 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
   ```

7. 관계가 초기화되고 유휴 상태가 된 후 대상에서 'napshot show' 명령을 사용하여 복제된 스냅샷 복사본에 적용된 SnapLock 만료 시간을 확인합니다.

   이 예에서는 SnapMirror 레이블과 SnapLock 만료 날짜가 있는 볼륨 DstvolB의 스냅샷 복사본을 보여 줍니다.

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

관련 정보

"클러스터 및 SVM 피어링"

"SnapVault를 사용한 볼륨 백업"

재해 복구를 위해 **WORM** 파일을 미러링합니다

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 을 참조하십시오 "클러스터 및 SVM 피어링".

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 을 참조하십시오 "데이터 보호".
- 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 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 보존 기간이 있는 경우 실제 볼륨 만료 기간이 마스킹되고 "무제한"으로 표시되지만 실제 볼륨 만료 기간 동안 스냅숏이 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.

에서 CLI를 사용하여 일관되지 않은 데이터를 캡처하기 위해 생성된 대상 볼륨의 잠긴 스냅샷 복사본을 소스에 복사할 수 있습니다 `snapmirror update -s snapshot` 명령. 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 클릭합니다 ⋮ 를 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 라이센스를 설치합니다", "준수 시계를 초기화합니다"9.10.1 이전 버전의 ONTAP 릴리스를 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 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을 사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다. volume-snaplock-type 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전 버전의 ONTAP 릴리스에서는 SnapLock 모드(준수 또는 엔터프라이즈)가 aggregate에서 상속됩니다. 버전에 상관없이 유연한 타겟 볼륨이 지원되지 않습니다. 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 정책 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|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 스냅샷 복사본을 만든 다음 해당 복사본과 이 복사본이 대상 볼륨에 참조하는 모든 데이터 블록을 전송합니다. 소스 볼륨의 다른 스냅샷 복사본도 타겟 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"

법적 증거 자료 보관 을 사용하여 소송 중에 **WORM** 파일을 보관하십시오

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

필요한 것

- 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-citigation-name_citigation_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-cigation-name_citigation_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 /
```

WORM 파일 삭제 개요

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.

필요한 것

- 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
   ```

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.

필요한 것

- 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. 'volume file retention show' 명령을 사용하여 삭제할 WORM 파일의 보존 시간을 확인할 수 있습니다. 자세한 내용은 명령에 대한 man 페이지를 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
   ```