SnapLock 기술을 사용한 아카이브 및 규정 준수

ONTAP 9

NetApp
May 09, 2024

목차

SnapLock 기술을 사용한 아카이브 및 규정 준수

SnapLock란

SnapLock는 WORM 스토리지를 사용하여 규정 및 거버넌스 목적으로 수정되지 않은 형태로 파일을 유지하는 조직을 위한 고성능 규정 준수 솔루션입니다.

SnapLock는 SEC 17a-4, HIPAA, FINRA, CFTC 및 GDPR과 같은 규정을 준수하기 위해 데이터의 삭제, 변경 또는 이름 변경을 방지합니다. SnapLock를 사용하면 파일을 저장한 후 지정된 보존 기간 또는 무기한으로 삭제할 수 없고 쓸 수 없는 상태로 커밋하는 특수한 용도의 볼륨을 생성할 수 있습니다. SnapLock에서는 CIFS 및 NFS와 같은 표준 개방형 파일 프로토콜을 통해 파일 레벨에서 이 보존을 수행할 수 있습니다. SnapLock에서 지원되는 개방형 파일 프로토콜은 NFS(버전 2, 3 및 4) 및 CIFS(SMB 1.0, 2.0 및 3.0)입니다.

SnapLock를 사용하면 파일 및 스냅샷 복사본을 WORM 스토리지에 커밋하고 WORM 보호 데이터에 대한 보존 기간을 설정할 수 있습니다. SnapLock WORM 스토리지는 NetApp 스냅샷 기술을 사용하고 SnapMirror 복제 및 SnapVault 백업을 데이터에 대한 백업 복구 보호를 제공하는 기본 기술로 활용할 수 있습니다. WORM 스토리지에 대한 자세한 내용: "NetApp SnapLock-TR-4526을 사용하여 WORM 스토리지를 준수합니다".

애플리케이션을 사용하여 NFS 또는 CIFS를 통해 WORM에 파일을 커밋하거나 SnapLock 자동 커밋 기능을 사용하여 파일을 WORM에 자동으로 커밋할 수 있습니다. _WORM 추가 가능 파일_을 사용하여 로그 정보와 같이 점증적으로 기록된 데이터를 보존할 수 있습니다. 자세한 내용은 을 참조하십시오 "볼륨 추가 모드를 사용하여 WORM 추가 가능 파일을 생성합니다".

SnapLock는 대부분의 규정 준수 요구사항을 충족하는 데이터 보호 방법을 지원합니다.

- SnapLock for SnapVault를 사용하여 2차 스토리지에서 WORM 상태로 스냅샷 복사본을 보호할 수 있습니다. 을 참조하십시오 "WORM에 스냅샷 복사본 커밋".
- SnapMirror를 사용하여 재해 복구를 위해 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 을 참조하십시오 "WORM 파일 미러링".

SnapLock는 NetApp ONTAP의 라이센스 기반 기능입니다. 단일 라이센스를 사용하면 SnapLock를 엄격한 규정 준수 모드로 사용하여 SEC Rule 17a-4 및 느슨한 엔터프라이즈 모드와 같은 외부 규정을 충족함으로써 디지털 자산 보호를 위해 내부적으로 규정된 규정을 준수할 수 있습니다. SnapLock 라이센스는 의 일부입니다 "ONTAP 1 을 참조하십시오" 소프트웨어 제품군:

SnapLock는 모든 AFF 및 FAS 시스템과 ONTAP Select에서 지원됩니다. SnapLock는 소프트웨어 전용 솔루션이 아니라 통합 하드웨어 및 소프트웨어 솔루션입니다. 이러한 차이는 SEC 17a-4와 같이 통합 하드웨어 및 소프트웨어 솔루션이 필요한 엄격한 WORM 규정에 중요합니다. 자세한 내용은 을 참조하십시오 "SEC Interpretation: 중개업체의 전자 저장 - 딜러 기록".

SnapLock로 할 수 있는 일

SnapLock를 구성한 후 다음 작업을 수행할 수 있습니다.

- "WORM에 파일을 커밋합니다"
- "2차 스토리지를 위해 WORM에 스냅샷 복사본 커밋"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "법적 증거 자료 보관 을 사용하여 소송 중에 WORM 파일을 보관하십시오"

- "권한 있는 삭제 기능을 사용하여 WORM 파일을 삭제합니다"
- "파일 보존 기간을 설정합니다"
- "SnapLock 볼륨을 이동합니다"
- "랜섬웨어 공격을 차단하려면 스냅샷 복사본을 잠그십시오"
- "감사 로그와 함께 SnapLock 사용을 검토합니다"
- "SnapLock API 사용"

SnapLock 규정 준수 및 엔터프라이즈 모드

SnapLock 규정 준수 및 엔터프라이즈 모드는 각 모드에서 WORM 파일을 보호하는 수준에 따라 크게 다릅니다.

SnapLock 모드	보호 수준	WORM 파일 보존 중 삭제
준수 모드	파일 레벨에서	삭제할 수 없습니다
엔터프라이즈 모드	디스크 레벨에서 복구	감사된 "권한 삭제" 절차를 사용하여 규정 준수 관리자가 삭제할 수 있습니다

보존 기간이 경과하면 더 이상 필요하지 않은 파일을 삭제할 책임이 있습니다. 파일이 규정 준수 모드이든 엔터프라이즈 모드이든 WORM에 커밋되면 보존 기간이 만료된 후에도 수정할 수 없습니다.

보존 기간 중 또는 이후에 WORM 파일을 이동할 수 없습니다. WORM 파일을 복사할 수 있지만 WORM 특성이 유지되지 않습니다.

다음 표에는 SnapLock 규정 준수 및 엔터프라이즈 모드에서 지원하는 기능의 차이가 나와 있습니다.

제공합니다	SnapLock 규정 준수	SnapLock 엔터프라이즈
권한 있는 삭제를 사용하여 파일을 활성화 및 삭제합니다	아니요	예
디스크를 다시 초기화합니다	아니요	예
보존 기간 동안 SnapLock 애그리게이트 및 볼륨을 제거합니다	아니요	예. SnapLock 감사 로그 볼륨을 제외하고 가능합니다
Aggregate 또는 볼륨의 이름을 바꿉니다	아니요	예
비NetApp 디스크를 사용합니다	아니요	예(와 함께 "FlexArray 가상화")
감사 로깅을 위해 SnapLock 볼륨을 사용합니다	예	예, ONTAP 9.5부터 시작합니다

SnapLock에서 지원 및 지원되지 않는 기능

다음 표에는 SnapLock 규정 준수 모드, SnapLock 엔터프라이즈 모드 또는 둘 다에서 지원되는 기능이 나와 있습니다.

피처	SnapLock 규정 준수 지원	SnapLock Enterprise에서 지원됩니다
일관성 그룹	아니요	아니요
암호화된 볼륨	예, ONTAP 9.2부터 시작합니다. 에 대해 자세히 알아보십시오 암호화 및 SnapLock.	예, ONTAP 9.2부터 시작합니다. 에 대해 자세히 알아보십시오 암호화 및 SnapLock.
SnapLock 애그리게이트에서 Fabric으로 구성	아니요	예, ONTAP 9.8부터 시작합니다. 에 대해 자세히 알아보십시오 FabricPool on SnapLock 엔터프라이즈 애그리게이트.
Flash Pool 애그리게이트로 전환 가능	예, ONTAP 9.1부터 사용 가능합니다.	예, ONTAP 9.1부터 사용 가능합니다.
플랙스클론	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.
FlexGroup 볼륨	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].
LUN을 클릭합니다	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.
MetroCluster 구성	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.
MAV(Multi-admin verification)	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.
산	아니요	아니요
단일 파일 SnapRestore	아니요	예
SnapMirror 비즈니스 연속성	아니요	아니요
SnapRestore	아니요	예
SMTape	아니요	아니요

SnapMirror Synchronous	아니요	아니요
SSD를 지원합니다	예, ONTAP 9.1부터 사용 가능합니다.	예, ONTAP 9.1부터 사용 가능합니다.
스토리지 효율성 기능	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.

FabricPool on SnapLock 엔터프라이즈 애그리게이트

FabricPool은 ONTAP 9.8부터 SnapLock 엔터프라이즈 애그리게이트에서 지원됩니다. 그러나 클라우드 관리자가 해당 데이터를 삭제할 수 있으므로 FabricPool 데이터를 퍼블릭 또는 프라이빗 클라우드로 계층화하면 SnapLock에서 더 이상 보호되지 않는다는 사실을 NetApp 어카운트 팀이 설명하는 제품 분산 요청을 개설해야 합니다.

> FabricPool에서 퍼블릭 또는 프라이빗 클라우드로 계층화하는 데이터는 클라우드 관리자가 삭제할 수 있으므로 SnapLock에서 더 이상 보호되지 않습니다.

FlexGroup 볼륨

SnapLock는 ONTAP 9.11.1부터 FlexGroup 볼륨을 지원하지만 다음 기능은 지원되지 않습니다.

- 법적 증거 자료 보관
- 이벤트 기반 보존
- SnapLock for SnapVault(ONTAP 9.12.1부터 지원됨)

또한 다음과 같은 행동을 인지해야 합니다.

- FlexGroup 볼륨의 VCC(Volume Compliance Clock)는 루트 구성 요소 VCC에 의해 결정됩니다. 모든 비루트 구성 요소들은 VCC를 루트 VCC와 긴밀히 동기화하게 됩니다.
- SnapLock 구성 속성은 FlexGroup 전체에 대해서만 설정됩니다. 개별 구성 요소마다 기본 보존 시간 및 자동 커밋 기간과 같은 서로 다른 구성 속성을 사용할 수 없습니다.

LUN 지원

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.

MetroCluster 지원

MetroCluster 구성에서 SnapLock 지원은 SnapLock 규정 준수 모드와 SnapLock 엔터프라이즈 모드 간에 다릅니다.

SnapLock 규정 준수

- ONTAP 9.3부터 SnapLock 규정 준수는 미러링되지 않은 MetroCluster 애그리게이트에서 지원됩니다.
- ONTAP 9.3부터 SnapLock 규정 준수는 미러링된 애그리게이트에서 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 지원됩니다.

- MetroCluster를 사용하여 SVM별 SnapLock 구성을 운영 사이트 및 2차 사이트에 복제할 수 있습니다.

SnapLock 엔터프라이즈

- ONTAP 9부터 SnapLock 엔터프라이즈 애그리게이트가 지원됩니다.
- ONTAP 9.3부터는 권한이 있는 삭제 기능이 있는 SnapLock 엔터프라이즈 애그리게이트가 지원됩니다.
- MetroCluster를 사용하여 SVM별 SnapLock 구성을 두 사이트 모두에 복제할 수 있습니다.

MetroCluster 구성 및 규정 준수 클럭

MetroCluster 구성에는 VCC(Volume Compliance Clock)와 SCC(System Compliance Clock)라는 두 가지 준수 클록 메커니즘이 사용됩니다. VCC 및 SCC는 모든 SnapLock 구성에 사용할 수 있습니다. 노드에 새 볼륨을 생성할 때 해당 노드에 있는 SCC의 현재 값으로 VCC가 초기화됩니다. 볼륨이 생성된 후에는 항상 VCC를 통해 볼륨 및 파일 보존 시간을 추적합니다.

볼륨이 다른 사이트에 복제되면 해당 VCC도 복제됩니다. 예를 들어, 사이트 A에서 사이트 B로 볼륨 전환이 발생하면 사이트 A의 SCC가 사이트 A가 오프라인이 되면 사이트 B에서 VCC가 계속 업데이트됩니다.

사이트 A가 다시 온라인 상태가 되고 볼륨 스위치백을 수행하면 볼륨의 VCC가 계속 업데이트되는 동안 사이트 A SCC 클록이 다시 시작됩니다. 스위치오버 및 스위치백 작업과 관계없이 VCC가 지속적으로 업데이트되기 때문에 파일 보존 시간은 SCC 클럭에 의존하지 않고 늘어나지 않습니다.

MAV(Multi-admin verification) 지원

ONTAP 9.13.1 부터는 클러스터 관리자가 일부 SnapLock 작업을 실행하기 전에 쿼럼을 승인해야 하는 클러스터에서 다중 관리 검증을 명시적으로 활성화할 수 있습니다. MAV가 활성화되면 기본 보존 시간, 최소 보존 시간, 최대 보존 시간, 볼륨 추가 모드, 자동 커밋 기간 및 권한 삭제 등의 SnapLock 볼륨 속성에 쿼럼이 승인되어야 합니다. 에 대해 자세히 알아보십시오 "5일".

스토리지 효율성

ONTAP 9.9.1부터 SnapLock은 데이터 컴팩션, 볼륨 간 중복제거, SnapLock 볼륨 및 애그리게이트를 위한 적응형 압축과 같은 스토리지 효율성 기능을 지원합니다. 스토리지 효율성에 대한 자세한 내용은 를 참조하십시오 "CLI를 통한 논리적 스토리지 관리 개요".

암호화

ONTAP는 스토리지 미디어의 용도 변경, 반환, 잘못된 위치 변경 또는 도난 시 유휴 데이터를 읽을 수 없도록 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공합니다.

- 법적 고지 사항: * NetApp은 자체 암호화 드라이브 또는 볼륨의 SnapLock 보호 WORM 파일이 인증 키가 손실되거나 실패한 인증 시도 횟수가 지정된 제한을 초과하여 드라이브가 영구적으로 잠기는 경우 이를 복구할 수 있다고 보장할 수 없습니다. 인증 실패에 대한 책임은 사용자에게 있습니다.

ONTAP 9.2부터는 SnapLock 애그리게이트에서 암호화된 볼륨이 지원됩니다.

7-Mode 전환

7-Mode 전환 도구의 CBT(Copy-Based Transition) 기능을 사용하여 SnapLock 볼륨을 7-Mode에서 ONTAP로 마이그레이션할 수 있습니다. 대상 볼륨의 SnapLock 모드인 Compliance 또는 Enterprise는 소스 볼륨의 SnapLock 모드와 일치해야 합니다. CFT(Copy-Free Transition)를 사용하여 SnapLock 볼륨을 마이그레이션할 수는 없습니다.

SnapLock를 구성합니다

SnapLock를 구성합니다

SnapLock를 사용하기 전에 과 같은 다양한 작업을 완료하여 SnapLock를 구성해야 합니다 "SnapLock 라이센스를 설치합니다" SnapLock 볼륨으로 애그리게이트를 호스팅하는 각 노드에 대해 를 초기화합니다 "규정 준수 시계", ONTAP 9.10.1 이전의 ONTAP 릴리즈를 실행하는 클러스터에 대한 SnapLock 애그리게이트를 생성합니다. "SnapLock 볼륨을 생성하고 마운트합니다"등.

준수 시계를 초기화합니다

SnapLock는 _ volume Compliance Clock _ 을(를) 사용하여 WORM 파일의 보존 기간을 변경할 수 있는 변조를 방지합니다. 먼저 SnapLock 애그리게이트를 호스팅하는 각 노드에서 _SYSTEM ComplianceClock_을 초기화해야 합니다.

ONTAP 9.14.1부터는 SnapLock 볼륨이 없거나 스냅샷 복사본 잠금이 설정된 볼륨이 없을 때 시스템 규정 준수 클록을 초기화하거나 다시 초기화할 수 있습니다. 시스템 관리자는 재초기화 기능을 사용하여 시스템 규정 준수 클록이 잘못 초기화되었을 수 있는 경우에 시스템 규정 준수 클록을 재설정하거나 시스템의 클럭 편차를 수정할 수 있습니다. ONTAP 9.13.1 이하 릴리즈에서는 노드에서 규정 준수 클록을 초기화한 후 다시 초기화할 수 없습니다.

시작하기 전에

규정 준수 클록을 다시 초기화하려면 다음을 수행합니다.

- 클러스터의 모든 노드가 정상 상태여야 합니다.
- 모든 볼륨이 온라인 상태여야 합니다.
- 복구 큐를 표시할 볼륨이 없습니다.
- SnapLock 볼륨이 없을 수 있습니다.
- 스냅샷 복사본 잠금이 설정된 볼륨을 사용할 수 없습니다.

규정 준수 시계 초기화를 위한 일반 요구 사항:

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다".

이 작업에 대해

시스템 Compliance Clock의 시간은 _ VOLUME Compliance Clock _ 에 의해 상속되며, 이 시간 중 후자는 볼륨에 있는 WORM 파일의 보존 기간을 제어합니다. 볼륨 준수 시계는 새 SnapLock 볼륨을 생성할 때 자동으로 초기화됩니다.

> 시스템 규정 준수 클럭의 초기 설정은 현재 하드웨어 시스템 클록을 기반으로 합니다. 따라서 각 노드에서 시스템 규정 준수 클록을 초기화하기 전에 시스템 시간과 시간대가 올바른지 확인해야 합니다. 노드에서 시스템 규정 준수 클록을 초기화하고 나면 SnapLock 볼륨 또는 잠금이 설정된 볼륨이 존재할 때 이를 다시 초기화할 수 없습니다.

단계

ONTAP CLI를 사용하여 규정 준수 클록을 초기화하거나 ONTAP 9.12.1부터 System Manager를 사용하여 규정 준수 클록을 초기화할 수 있습니다.

시스템 관리자

1. 클러스터 > 개요 * 로 이동합니다.
2. 노드 * 섹션에서 * SnapLock 준수 클럭 초기화 * 를 클릭합니다.
3. 규정 준수 시계 * 열을 표시하고 규정 준수 시계가 초기화되었는지 확인하려면 * 클러스터 > 개요 > 노드 * 섹션에서 * 표시/숨기기 * 를 클릭하고 * SnapLock 규정 준수 시계 * 를 선택합니다.

CLI를 참조하십시오

1. 시스템 규정 준수 클록을 초기화합니다.

   ' * SnapLock compliance-clock initialize-node_node_name_ * '

   다음 명령을 실행하면 시스템 Compliance Clock On이 초기화됩니다 `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. 메시지가 표시되면 시스템 클록이 올바른지, 규정 준수 클록을 초기화할지 확인합니다.

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. SnapLock 애그리게이트를 호스팅하는 각 노드에 대해 이 절차를 반복합니다.

NTP 구성 시스템에 대해 규정 준수 클럭 재동기화를 설정합니다

NTP 서버가 구성되어 있을 때 SnapLock 준수 클럭 시간 동기화 기능을 활성화할 수 있습니다.

필요한 것

- 이 기능은 고급 권한 수준에서만 사용할 수 있습니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다".
- 이 기능은 Cloud Volumes ONTAP, ONTAP Select 및 VIM 플랫폼에서만 사용할 수 있습니다.

이 작업에 대해

SnapLock 보안 클럭 데몬이 임계값을 초과하는 편중을 감지하면 ONTAP는 시스템 시간을 사용하여 시스템 및 볼륨 규정 준수 클럭을 모두 재설정합니다. 24시간이 기울기 임계값으로 설정됩니다. 즉, 편중이 하루 이상 지난 경우에만 시스템 규정 준수 클록이 시스템 클록과 동기화됩니다.

SnapLock 보안 클록 데몬은 편중을 감지하고 규정 준수 클럭을 시스템 시간으로 변경합니다. 시스템 시간이 NTP 시간과 동기화되는 경우에만 규정 준수 클록이 시스템 시간과 동기화되기 때문에 규정 준수 클록이 시스템 시간과 동기화되도록 시스템 시간을 수정하려는 시도가 실패합니다.

단계

1. NTP 서버가 구성된 경우 SnapLock 규정 준수 클럭 시간 동기화 기능을 활성화합니다.

   `* SnapLock 컴플라이언스-클록 NTP * '

   다음 명령을 실행하면 시스템 규정 준수 클럭 시간 동기화 기능이 설정됩니다.

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. 메시지가 표시되면 구성된 NTP 서버가 신뢰할 수 있고 통신 채널이 보안 상태인지 확인합니다.
3. 기능이 활성화되어 있는지 확인합니다.

   ``SnapLock compliance-clock NTP 쇼 *'

   다음 명령은 시스템 규정 준수 클럭 시간 동기화 기능이 설정되어 있는지 확인합니다.

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

SnapLock Aggregate를 생성합니다

볼륨 '-snaplock-type' 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전 릴리스의 경우 별도의 SnapLock 애그리게이트를 만들어야 합니다. 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.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- SnapLock입니다 "라이센스를 설치해야 합니다" 노드에서. 이 라이센스는 에 포함되어 있습니다 "ONTAP 1 을 참조하십시오".
- "노드의 규정 준수 클록을 초기화해야 합니다".
- 디스크를 "루트", "루트", "다토1" 및 "다토2"로 분할한 경우 스페어 디스크를 사용할 수 있는지 확인해야 합니다.

업그레이드 고려 사항

ONTAP 9.10.1로 업그레이드할 때 기존 SnapLock 및 비 SnapLock 애그리게이트는 SnapLock 볼륨과 비 SnapLock 볼륨 모두를 지원하도록 업그레이드되지만 기존 SnapLock 볼륨 특성은 자동으로 업데이트되지 않습니다. 예를 들어, 데이터 컴팩션, 볼륨 간 중복제거, 볼륨 간 백그라운드 중복제거 필드는 변경되지 않습니다. 기존 애그리게이트에 생성된 새로운 SnapLock 볼륨의 기본값이 비 SnapLock 볼륨과 같고, 새 볼륨 및 애그리게이트의 기본 값은 플랫폼에 따라 다릅니다.

되돌리기 고려 사항

9.10.1 이전의 ONTAP 버전으로 복구해야 하는 경우 모든 SnapLock 규정 준수, SnapLock 엔터프라이즈 및 SnapLock 볼륨을 고유한 SnapLock 애그리게이트로 이동해야 합니다.

이 작업에 대해

- FlexArray LUN에 대한 규정 준수 애그리게이트는 생성할 수 없지만 FlexArray LUN에서는 SnapLock 규정 준수 애그리게이트가 지원됩니다.
- SyncMirror 옵션을 사용하여 준수 애그리게이트를 생성할 수 없습니다.
- MetroCluster 구성에서 미러링된 Compliance Aggregate는 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 생성할 수 있습니다.

> MetroCluster 구성에서는 SnapLock Enterprise가 미러링된 Aggregate 및 미러링되지 않은 Aggregate에서 지원됩니다. SnapLock 규정 준수는 미러링되지 않은 애그리게이트에서만 지원됩니다.

단계

1. SnapLock 애그리게이트 생성:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

명령의 man 페이지에는 전체 옵션 목록이 포함되어 있습니다.

다음 명령을 실행하면 node1에 3개의 디스크가 있는 "aggr1"이라는 SnapLock "Compliance" Aggregate가 생성됩니다.

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

SnapLock 볼륨을 생성하고 마운트합니다

WORM 상태로 커밋하려는 파일 또는 스냅샷 복사본에 대한 SnapLock 볼륨을 생성해야 합니다. ONTAP 9.10.1.1부터 애그리게이트 유형에 관계없이 생성한 모든 볼륨은 기본적으로 비 SnapLock 볼륨으로 생성됩니다. '-snaplock-type' 옵션을 사용하여 준수 또는 엔터프라이즈 를 SnapLock 유형으로 지정하여 SnapLock 볼륨을 명시적으로 생성해야 합니다. 기본적으로 SnapLock 유형은 비 SnapLock으로 설정됩니다.

시작하기 전에

- SnapLock 애그리게이트는 온라인 상태여야 합니다.
- 당신은 해야 한다 "SnapLock 라이센스가 설치되어 있는지 확인합니다". 노드에 SnapLock 라이센스가 설치되어 있지 않으면 을 수행해야 합니다 "설치합니다" 있습니다. 이 라이센스는 에 포함되어 있습니다 "ONTAP 1 을 참조하십시오". ONTAP One 이전에는 SnapLock 라이센스가 보안 및 규정 준수 번들에 포함되어 있었습니다. 보안 및 규정 준수 번들은 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 있습니다 "ONTAP One으로 업그레이드하십시오".
- "노드의 규정 준수 클록을 초기화해야 합니다".

이 작업에 대해

적절한 SnapLock 권한을 사용하여 언제든지 엔터프라이즈 볼륨을 삭제하거나 이름을 바꿀 수 있습니다. 보존 기간이 경과하기 전에는 Compliance 볼륨을 폐기할 수 없습니다. Compliance 볼륨의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다. 클론 볼륨은 상위 볼륨과 동일한 SnapLock 유형이 됩니다.

> 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 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행합니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SnapLock 볼륨을 생성할 수 있습니다.

단계

1. Storage > Volumes * 로 이동한 다음 * Add * 를 클릭합니다.
2. 볼륨 추가 * 창에서 * 추가 옵션 * 을 클릭합니다.
3. 볼륨의 이름과 크기를 포함하여 새 볼륨 정보를 입력합니다.
4. SnapLock 사용 * 을 선택하고 SnapLock 유형(준수 또는 엔터프라이즈)을 선택합니다.
5. 자동 커밋 파일 * 섹션에서 * 수정 * 을 선택하고 파일이 자동으로 커밋되기 전에 변경되지 않은 상태로 유지되는 시간을 입력합니다. 최소값은 5분이고 최대값은 10년입니다.
6. Data Retention * 섹션에서 최소 및 최대 보존 기간을 선택합니다.
7. 기본 보존 기간을 선택합니다.
8. 저장 * 을 클릭합니다.
9. 볼륨 * 페이지에서 새 볼륨을 선택하여 SnapLock 설정을 확인합니다.

CLI를 참조하십시오

1. SnapLock 볼륨 생성:

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

전체 옵션 목록은 명령에 대한 man 페이지를 참조하십시오. SnapLock 볼륨에는 '-nvfail', '-atime-update', '-is-AutoBalance-eligible', '-space-mgmt-try-first', ' vmalign' 옵션이 없습니다.

다음 명령을 실행하면 vs1에 vol1이라는 SnapLock "Compliance" 볼륨이 생성됩니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

SnapLock 볼륨을 마운트합니다

NAS 클라이언트 액세스를 위해 SVM 네임스페이스의 접합 경로에 SnapLock 볼륨을 마운트할 수 있습니다.

필요한 것

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

- SnapLock 볼륨은 SVM의 루트 아래에서만 마운트할 수 있습니다.
- SnapLock 볼륨 아래에 일반 볼륨을 마운트할 수 없습니다.

단계

1. SnapLock 볼륨 마운트:

   '* 볼륨 마운트 - vserver_SVM_name_-volume_volume_name_-junction-path_path_*'

   전체 옵션 목록은 명령에 대한 man 페이지를 참조하십시오.

   다음 명령을 실행하면 이름이 vol1인 SnapLock 볼륨이 VS1 네임스페이스에서 junction path/sales에 마운트됩니다.

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

보존 시간을 설정합니다

파일의 보존 시간을 명시적으로 설정하거나 볼륨에 대한 기본 보존 기간을 사용하여 보존 시간을 파생시킬 수 있습니다. 보존 시간을 명시적으로 설정하지 않으면 SnapLock에서는 기본 보존 기간을 사용하여 보존 시간을 계산합니다. 이벤트 후에 파일 보존을 설정할 수도 있습니다.

보존 기간 및 보존 시간에 대해 설명합니다

WORM 파일의 _retention period_는 파일이 WORM 상태로 커밋된 후 보존되어야 하는 시간을 지정합니다. WORM 파일의 _retention time_은 파일을 더 이상 보존할 필요가 없는 시간입니다. 예를 들어, 2020년 11월 10일 오전 6시부터 WORM 상태로 커밋된 파일의 보존 기간은 20년이며, 보존 기간은 2010년 11월 10일 오전 6시입니다

> ONTAP 9.10.1부터 최대 10월 26일, 3058까지의 보존 기간 및 최대 100년의 보존 기간을 설정할 수 있습니다. 보존 날짜를 확장하면 이전 정책이 자동으로 변환됩니다. ONTAP 9.9.1 및 이전 릴리즈에서는 기본 보존 기간을 무한으로 설정하지 않으면 지원되는 최대 보존 시간은 1월 19 2071(GMT)입니다.

중요한 복제 고려 사항

1월 19일 2071(GMT) 이후의 보존 날짜를 사용하여 SnapLock 소스 볼륨과 SnapMirror 관계를 설정할 때 타겟 클러스터에서 ONTAP 9.10.1 이상이 실행 중이어야 하며, 그렇지 않으면 SnapMirror 전송이 실패합니다.

중요한 되돌리기 고려 사항

보존 기간이 "January 19, 2071 8:44:07 AM"보다 늦은 파일이 있는 경우 ONTAP는 클러스터가 ONTAP 9.10.1에서 이전 ONTAP 버전으로 복구되지 않도록 합니다.

보존 기간 이해

SnapLock 규정 준수 또는 엔터프라이즈 볼륨의 보존 기간은 4가지입니다.

- 최소 보존 기간(min), 기본값 0
- 최대 보존 기간(최대)(기본값: 30년

- ONTAP 9.10.1부터 준수 모드 및 엔터프라이즈 모드 모두에 대해 기본 보존 기간(기본값: "in")입니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 기본 보존 기간이 모드에 따라 다릅니다.
  - 준수 모드의 경우 기본값은 'Max'입니다.
  - 엔터프라이즈 모드의 경우 기본값은 'in'입니다.
- 지정되지 않은 보존 기간.

  ONTAP 9.8부터 볼륨에 있는 파일의 보존 기간을 '지정 안 됨'으로 설정하여 절대 보존 시간을 설정할 때까지 파일을 보존할 수 있습니다. 새 절대 보존 시간이 이전에 설정한 절대 시간보다 이후인 경우 절대 보존 시간을 지정하지 않은 보존으로 설정하고 다시 절대 보존으로 설정할 수 있습니다.

  ONTAP 9.12.1부터 보존 기간이 설정된 WORM 파일 `unspecified` SnapLock 볼륨에 대해 구성된 최소 보존 기간으로 보존 기간을 설정해야 합니다. 에서 파일 보존 기간을 변경하는 경우 `unspecified` 지정된 새 보존 시간은 파일에 이미 설정된 최소 보존 시간보다 커야 합니다.

따라서 Compliance-mode 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 30년 동안 파일이 유지됩니다. 마찬가지로 엔터프라이즈 모드 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 파일이 0년 동안 또는 전혀 보존되지 않습니다.

기본 보존 기간을 설정합니다

'volume SnapLock modify' 명령을 사용하여 SnapLock 볼륨의 파일에 대한 기본 보존 기간을 설정할 수 있습니다.

필요한 것

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

다음 표에는 기본 보존 기간 옵션에 사용할 수 있는 값이 나와 있습니다.

> 기본 보존 기간은 최소 보존 기간보다 크거나 같고 최대 보존 기간보다 작거나 같아야 합니다(<=).

값	단위	참고
0-65535	초	
0-24	시간	
0-365일	일	
0-12로 설정합니다	개월	
0-100입니다	년	ONTAP 9.10.1부터. 이전 ONTAP 릴리스의 경우 값은 0-70입니다.
최대	-	최대 보존 기간을 사용합니다.
최소	-	최소 보존 기간을 사용합니다.

값	단위	참고
무한대	-	파일을 영구적으로 보존합니다.
지정되지 않음	-	절대 보존 기간이 설정될 때까지 파일을 보존합니다.

최대 및 최소 보존 기간의 값과 범위는 해당되지 않는 최대 및 최소 보존 기간을 제외하고 동일합니다. 이 작업에 대한 자세한 내용은 을 참조하십시오 "보존 시간 개요를 설정합니다".

'volume SnapLock show' 명령을 사용하여 볼륨에 대한 보존 기간 설정을 볼 수 있습니다. 자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

> 파일이 WORM 상태로 커밋된 후에는 보존 기간을 늘릴 수 있지만 줄일 수는 없습니다.

단계

1. SnapLock 볼륨에 있는 파일의 기본 보존 기간을 설정합니다.

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-default-retention -period_default_retention_period_-minimum-retention-period_min_retention_period_-maximum-retention -period_max_retention_period_ *'

   전체 옵션 목록은 명령에 대한 man 페이지를 참조하십시오.

   > 다음 예에서는 최소 및 최대 보존 기간이 이전에 수정되지 않은 것으로 가정합니다.

   다음 명령을 실행하면 Compliance 또는 Enterprise 볼륨의 기본 보존 기간이 20일로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 70년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   -retention-period 70years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period max -maximum-retention-period 10years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10일로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 무한으로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

파일의 보존 시간을 명시적으로 설정합니다

파일의 마지막 액세스 시간을 수정하여 파일의 보존 시간을 명시적으로 설정할 수 있습니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 마지막 액세스 시간을 수정할 수 있습니다.

이 작업에 대해

파일이 WORM에 커밋된 후에는 보존 시간을 늘릴 수 있지만 줄일 수는 없습니다. 보존 시간은 파일의 atime 필드에 저장됩니다.

> 파일의 보존 시간을 명시적으로 '무한'으로 설정할 수는 없습니다. 이 값은 기본 보존 기간을 사용하여 보존 시간을 계산하는 경우에만 사용할 수 있습니다.

단계

1. 적절한 명령 또는 프로그램을 사용하여 보존 시간을 설정할 파일의 마지막 액세스 시간을 수정합니다.

   UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 "document.txt" 파일에서 다음을 수행합니다.

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

   > 적합한 명령 또는 프로그램을 사용하여 Windows의 마지막 액세스 시간을 수정할 수 있습니다.

이벤트 후 파일 보존 기간을 설정합니다

ONTAP 9.3부터 EBR(SnapLock_Event Based Retention)_Feature를 사용하여 이벤트 발생 후 파일이 유지되는 기간을 정의할 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

이벤트 보존 정책 _ 은(는) 이벤트가 발생한 후 파일의 보존 기간을 정의합니다. 정책은 단일 파일 또는 디렉토리의 모든 파일에 적용할 수 있습니다.

- 파일이 WORM 파일이 아닌 경우 정책에 정의된 보존 기간 동안 WORM 상태로 커밋됩니다.
- 파일이 WORM 파일 또는 WORM 추가 가능 파일인 경우 보존 기간은 정책에 정의된 보존 기간만큼 연장됩니다.

Compliance-mode 또는 Enterprise-mode 볼륨을 사용할 수 있습니다.

EBR 정책은 법적 증거 자료 보관 아래의 파일에 적용할 수 없습니다.

고급 사용에 대한 자세한 내용은 을 참조하십시오 "NetApp SnapLock를 사용하여 WORM 스토리지 규정 준수".

* _ EBR을 사용하여 이미 존재하는 WORM 파일의 보존 기간을 연장합니다. _ *
EBR은 기존 WORM 파일의 보존 기간을 연장하려는 경우에 편리합니다. 예를 들어, 직원이 원천징수를 변경한 후 3년 동안 직원 W-4 기록을 수정되지 않은 형태로 유지하는 것이 회사의 정책일 수 있습니다. 다른 회사 정책에서는 직원이 종료된 후 5년 동안 W-4 기록을 보관해야 할 수 있습니다. 이 경우 5년의 보존 기간을 사용하여 EBR 정책을 생성할 수 있습니다. 직원이 종료된 후("이벤트") 직원의 W-4 기록에 EBR 정책을 적용하여 보존 기간이 연장될 수 있습니다. 이는 일반적으로 보존 기간을 수동으로 연장하는 것보다 쉽습니다. 특히 많은 수의 파일이 관련된 경우 더욱 그렇습니다.

단계

1. EBR 정책 생성:

   ``SnapLock 이벤트 보존 정책 생성 - vserver_SVM_name_-name_policy_name_-retention-period_retention_period_ *’

   다음 명령은 VS1, 보존 기간 10년을 포함한 EBR 정책 'EMPLOYEE_EXIT’를 생성한다.

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. EBR 정책 적용:

   '* SnapLock 이벤트-보존 적용 - vserver_SVM_name_-name_policy_name_-volume_volume_name_-path_path_name_*'

   다음 명령을 실행하면 VS1 디렉토리에 있는 모든 파일에 VS1 의 EBR 정책 'EMPLOYEE_EXIT’가 적용됩니다.

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

감사 로그를 생성합니다

ONTAP 9.9.1 이하 버전을 사용하는 경우, 권한 있는 삭제 또는 SnapLock 볼륨 이동을 수행하기 전에 먼저 SnapLock 애그리게이트를 생성한 다음 SnapLock 보호 감사 로그를 생성해야 합니다. 감사 로그는 SnapLock 관리자 계정의 생성 및 삭제, 로그 볼륨 수정, 권한 있는 삭제 활성화 여부, 권한 있는 삭제 작업 및 SnapLock 볼륨 이동 작업을 기록합니다.

ONTAP 9.10.1부터는 SnapLock 애그리게이트를 생성할 수 없습니다. 에는 -snaplock-type 옵션을 사용해야 합니다 "SnapLock 볼륨을 명시적으로 생성합니다" SnapLock 형식으로 Compliance 또는 Enterprise를 지정합니다.

시작하기 전에

ONTAP 9.9.1 이하 버전을 사용하는 경우 SnapLock 애그리게이트를 생성하려면 클러스터 관리자여야 합니다.

이 작업에 대해

로그 파일 보존 기간이 경과할 때까지 감사 로그를 삭제할 수 없습니다. 보존 기간이 경과한 후에도 감사 로그를 수정할 수 없습니다. 이는 SnapLock 규정 준수 모드와 엔터프라이즈 모드 모두에서 마찬가지입니다.

> ONTAP 9.4 이하 버전에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨을 사용할 수 없습니다. SnapLock 준수 볼륨을 사용해야 합니다. ONTAP 9.5 이상에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨 또는 SnapLock 규정 준수 볼륨을 사용할 수 있습니다. 모든 경우에 감사 로그 볼륨은 교차점 경로 '/snaplock_audit_log'에 마운트되어야 합니다. 다른 볼륨은 이 접합 경로를 사용할 수 없습니다.

SnapLock Audit 로그는 감사 로그 볼륨의 루트 아래의 '/sSnapLock_log' 디렉토리에서 privdel_log'(권한 삭제 작업) 및 'system_log'(기타 모든 것)라는 하위 디렉토리에 있습니다. 감사 로그 파일 이름에는 첫 번째 기록 작업의 타임스탬프가 포함되어 있어 작업이 실행된 대략적인 시간만큼 레코드를 쉽게 검색할 수 있습니다.

- 'SnapLock log file show' 명령을 사용하여 감사 로그 볼륨에서 로그 파일을 볼 수 있습니다.
- 'SnapLock log file archive' 명령을 사용하여 현재 로그 파일을 보관하고 새 로그 파일을 만들 수 있습니다. 이 명령은 별도의 파일에 감사 로그 정보를 기록해야 하는 경우에 유용합니다.

자세한 내용은 명령에 대한 man 페이지를 참조하십시오.

> 데이터 보호 볼륨은 SnapLock 감사 로그 볼륨으로 사용할 수 없습니다.

단계

1. SnapLock Aggregate를 생성합니다.

   SnapLock Aggregate를 생성합니다

2. 감사 로깅을 위해 구성하려는 SVM에서 SnapLock 볼륨을 생성합니다.

   SnapLock 볼륨을 생성합니다

3. 감사 로깅을 위해 SVM 구성:

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

> 감사 로그 파일의 최소 기본 보존 기간은 6개월입니다. 영향을 받는 파일의 보존 기간이 감사 로그의 보존 기간보다 긴 경우 로그의 보존 기간이 파일의 보존 기간을 상속합니다. 따라서 권한이 있는 삭제를 사용하여 삭제된 파일의 보존 기간이 10개월이고 감사 로그의 보존 기간이 8개월인 경우 로그 보존 기간은 10개월로 연장됩니다. 보존 시간 및 기본 보존 기간에 대한 자세한 내용은 을 참조하십시오 "보존 시간을 설정합니다".

다음 명령어는 SnapLock volume logVol을 이용하여 Audit logging을 위한 'VM1'을 설정한다. 감사 로그의 최대 크기는 20GB이며 8개월 동안 유지됩니다.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. 감사 로깅을 위해 구성한 SVM에서 SnapLock 볼륨을 연결 경로 '/sSnapLock_audit_log'에 마운트합니다.

   SnapLock 볼륨을 마운트합니다

SnapLock 설정을 확인합니다

'volume file fingerprint start' 및 'volume file fingerprint dump' 명령을 사용하여 파일 유형(Regular, WORM 또는 WORM appendable), 볼륨 만료 날짜 등 파일 및 볼륨에 대한 주요 정보를 볼 수 있습니다.

단계

1. 파일 지문 생성:

   '* 볼륨 파일 지문 시작 - vserver_SVM_name_-file_file_path_*'

```
svm1::> volume file fingerprint start -vserver svm1 -file
/vol/sle/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show
-session-id 16842791" to view the fingerprint session status.
```

   이 명령어는 'volume file fingerprint dump' 명령어에 대한 입력으로 사용할 수 있는 세션 ID를 생성한다.

> 세션 ID와 함께 볼륨 파일 fingerprint show 명령을 사용하여 지문 작업의 진행률을 모니터링할 수 있습니다. 지문 표시를 시도하기 전에 작업이 완료되었는지 확인하십시오.

2. 파일의 지문을 표시합니다.

   '* 볼륨 파일 지문 덤프 - session-id_session_ID_ * '

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
```

```
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
```

```
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

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 **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.

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 **WORM**에 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
   ```

SnapLock 볼륨을 이동합니다

ONTAP 9.8부터 SnapLock 볼륨을 엔터프라이즈부터 규정 준수까지 동일한 유형의 대상 Aggregate로 이동할 수 있습니다. SnapLock 볼륨을 이동하려면 SnapLock 보안 역할이 할당되어야 합니다.

SnapLock 보안 관리자 계정을 만듭니다

SnapLock 볼륨 이동을 수행하려면 SnapLock 보안 관리자 권한이 있어야 합니다. 이 권한은 ONTAP 9.8에 도입된 _SnapLock_역할을 통해 부여됩니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 이 SnapLock 보안 역할을 가진 SnapLock 보안 사용자를 만들도록 요청할 수 있습니다.

필요한 것

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

이 작업에 대해

SnapLock 역할은 데이터 SVM과 연결된 vsadmin-SnapLock 역할과는 달리 관리 SVM과 연결됩니다.

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 미리 정의된 "SnapLock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 admin SVM 'cluster1'에 액세스할 수 있습니다.

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

SnapLock 볼륨을 이동합니다

'volume move' 명령을 사용하여 SnapLock 볼륨을 대상 애그리게이트로 이동할 수 있습니다.

필요한 것

- SnapLock 볼륨 이동을 수행하기 전에 SnapLock으로 보호되는 감사 로그를 생성해야 합니다.

  "감사 로그를 생성합니다".

- ONTAP 9.10.1 이전 버전의 ONTAP를 사용하는 경우 대상 애그리게이트는 이동할 SnapLock 볼륨과 동일한 SnapLock 유형이어야 합니다. Compliance to Compliance 또는 Enterprise to Enterprise입니다. ONTAP 9.10.1부터는 이러한 제한이 없어지기 때문에 aggregate에 Compliance 및 Enterprise SnapLock 볼륨과 비 SnapLock 볼륨이 모두 포함될 수 있습니다.
- SnapLock 보안 역할을 가진 사용자여야 합니다.

단계

1. 보안 연결을 사용하여 ONTAP 클러스터 관리 LIF에 로그인합니다.

   ' * ssh SnapLock_user@cluster_mgmt_ip *'

2. SnapLock 볼륨 이동:

   '* volume move start -vserver_SVM_name_-volume_snaplock_volume_name_-destination -aggregate_destination_name_*'

3. 볼륨 이동 작업의 상태를 확인합니다.

   '* 볼륨 이동 표시 -volume_snaplock_volume_name_-vserver_SVM_name_-필드 볼륨, 단계, SVM*

랜섬웨어 공격을 차단하려면 스냅샷 복사본을 잠그십시오

ONTAP 9.12.1부터 비 SnapLock 볼륨에 Snapshot 복사본을 잠가 랜섬웨어 공격으로부터 보호할 수 있습니다. 스냅샷 복사본을 잠그면 실수로 또는 악의적으로 삭제할 수 없습니다.

SnapLock 컴플라이언스 클록 기능을 사용하면 만료 시간에 도달할 때까지 스냅샷 복사본을 삭제할 수 없도록 지정된 기간 동안 스냅샷 복사본을 잠글 수 있습니다. Snapshot 복사본을 잠그면 무단 변경 방지 기능이 되어 랜섬웨어 위협으로부터 보호됩니다. 잠겨 있는 Snapshot 복사본을 사용하여 랜섬웨어 공격으로 볼륨이 손상된 경우 데이터를 복구할 수 있습니다.

ONTAP 9.14.1부터 스냅샷 복사본 잠금은 SnapLock 소산 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 장기 보존 스냅샷 복사본을 지원합니다. 스냅샷 복사본 잠금은 에 연결된 SnapMirror 정책 규칙을 사용하여 보존 기간을 설정하여 사용할 수 있습니다 기존 정책 레이블. 이 규칙은 볼륨에 설정된 기본 보존 기간을 재정의합니다. SnapMirror 레이블과 연결된 보존 기간이 없으면 볼륨의 기본 보존 기간이 사용됩니다.

스냅샷 복사본의 요구 사항 및 고려 사항을 무단 변경 방지

- ONTAP CLI를 사용하는 경우 클러스터의 모든 노드에서 ONTAP 9.12.1 이상을 실행해야 합니다. System Manager를 사용하는 경우 모든 노드에서 ONTAP 9.13.1 이상을 실행해야 합니다.
- "SnapLock 라이센스가 클러스터에 설치되어 있어야 합니다". 이 라이센스는 에 포함되어 있습니다 "ONTAP 1 을 참조하십시오".
- "클러스터의 규정 준수 클록을 초기화해야 합니다".
- 볼륨에서 스냅샷 잠금이 활성화된 경우 클러스터를 ONTAP 9.12.1 이후 버전의 ONTAP로 업그레이드할 수 있습니다. 그러나 잠긴 스냅샷 복사본의 만료 날짜가 모두 만료되어 삭제되고 스냅샷 복사본 잠금이 비활성화되기 전에는 이전 버전의 ONTAP로 되돌릴 수 없습니다.
- 스냅샷이 잠기면 볼륨 만료 시간이 스냅샷 복사본의 만료 시간으로 설정됩니다. 둘 이상의 스냅샷 복사본이 잠겨 있는 경우 볼륨 만료 시간은 모든 스냅샷 복사본 중에서 가장 큰 만료 시간을 반영합니다.
- 잠긴 스냅샷 복사본의 보존 기간이 스냅샷 복사본 보존 기간보다 우선적으로 적용됩니다. 즉, 잠긴 스냅샷 복사본의 보존 기간이 만료되지 않은 경우 유지 수 제한이 적용되지 않습니다.
- SnapMirror 관계에서 미러 소산 정책 규칙에 보존 기간을 설정할 수 있으며, 타겟 볼륨에 스냅샷 복사본 잠금이 활성화된 경우 타겟에 복제된 스냅샷 복사본에 보존 기간이 적용됩니다. 보존 기간이 keep 카운트보다 우선합니다. 예를 들어, 만료일이 경과하지 않은 Snapshot 복사본은 keep 카운트가 초과되더라도 보존됩니다.
- 비 SnapLock 볼륨의 스냅샷 복사본 이름을 바꿀 수 있습니다. SnapMirror 관계의 운영 볼륨에 대한 스냅샷 이름 바꾸기 작업은 정책이 MirrorAllSnapshots인 경우에만 보조 볼륨에 반영됩니다. 다른 정책 유형의 경우 업데이트 중에는 이름이 변경된 스냅샷 복사본이 전파되지 않습니다.
- ONTAP CLI를 사용하는 경우 로 잠긴 스냅샷 복사본을 복원할 수 있습니다 `volume snapshot restore` 잠긴 스냅샷 복사본이 최신 상태인 경우에만 명령 복원 중인 스냅샷 복사본 이외의 만료되지 않은 스냅샷 복사본이 있는 경우 스냅샷 복사본 복원 작업이 실패합니다.

무단 스냅샷 복사본으로 지원되는 기능

- FlexGroup 볼륨

  스냅샷 복사본 잠금은 FlexGroup 볼륨에서 지원됩니다. 스냅샷 잠금은 루트 구성 요소 스냅샷 복사본에만 적용됩니다. FlexGroup 볼륨은 루트 구성 요소 만료 시간이 경과한 경우에만 삭제할 수 있습니다.

- FlexVol에서 FlexGroup로의 변환

  잠긴 스냅샷 복사본이 있는 FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 수 있습니다. 스냅샷 복사본은 변환 후에도

잠겨 있습니다.

- 볼륨 클론 및 파일 클론

  잠긴 스냅샷 복사본에서 볼륨 클론 및 파일 클론을 생성할 수 있습니다.

지원되지 않는 기능입니다

다음 기능은 현재 무단 스냅샷 복사본에서는 지원되지 않습니다.

- Cloud Volumes ONTAP
- 정합성 보장 그룹
- FabricPool
- FlexCache 볼륨
- SMTape
- SnapMirror 비즈니스 연속성(SM-BC)
- 를 사용하는 SnapMirror 정책 규칙입니다 `-schedule` 매개 변수
- SnapMirror Synchronous
- SVM 데이터 이동성(소스 클러스터에서 타겟 클러스터로 SVM을 마이그레이션 또는 재배치하는 데 사용)

볼륨을 생성할 때 스냅샷 복사본 잠금을 설정합니다

ONTAP 9.12.1부터 새 볼륨을 만들거나 를 사용하여 기존 볼륨을 수정할 때 스냅샷 복사본 잠금을 활성화할 수 있습니다 `-snapshot-locking-enabled` 의 옵션 `volume create` 및 `volume modify` CLI에서의 명령. ONTAP 9.13.1 부터 시스템 관리자를 사용하여 스냅샷 복사본 잠금을 활성화할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동하고 * Add * 를 선택합니다.
2. Add Volume * (볼륨 추가 *) 창에서 * More Options * (추가 옵션 *)를 선택합니다.
3. 볼륨 이름, 크기, 엑스포트 정책 및 공유 이름을 입력합니다.
4. 스냅샷 잠금 사용 * 을 선택합니다. SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.
5. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
6. 변경 사항을 저장합니다.
7. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
8. SnapLock 스냅샷 복사본 잠금 * 이 * 사용 * 으로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 새 볼륨을 생성하고 스냅샷 복사본 잠금을 활성화하려면 다음 명령을 입력합니다.

   `volume create -vserver vserver_name -volume volume_name -snapshot-locking -enabled true`

   다음 명령을 실행하면 vol1이라는 새 볼륨에서 스냅샷 복사본 잠금이 설정됩니다.

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

기존 볼륨에서 스냅샷 복사본 잠금 을 활성화합니다

ONTAP 9.12.1부터 ONTAP CLI를 사용하여 기존 볼륨에서 스냅샷 복사본 잠금을 활성화할 수 있습니다. ONTAP 9.13.1 부터 시스템 관리자를 사용하여 기존 볼륨에서 스냅샷 복사본 잠금을 활성화할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 선택합니다 ⋮ 편집 > 볼륨 * 을 선택합니다.
3. 볼륨 편집 * 창에서 스냅샷 복사본(로컬) 설정 섹션을 찾아 * 스냅샷 잠금 활성화 * 를 선택합니다.

   SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.

4. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
5. 변경 사항을 저장합니다.
6. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
7. SnapLock 스냅샷 복사본 잠금 * 이 * 사용 * 으로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 스냅샷 복사본 잠금을 사용하도록 기존 볼륨을 수정하려면 다음 명령을 입력합니다.

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

잠긴 스냅샷 복사본 정책을 생성하고 보존을 적용합니다

ONTAP 9.12.1부터 스냅샷 복사본 보존 기간을 적용하기 위한 스냅샷 복사본 정책을 생성하고 이 정책을 볼륨에 적용하여 지정된 기간 동안 스냅샷 복사본을 잠글 수 있습니다. 보존 기간을 수동으로 설정하여 스냅샷 복사본을 잠글 수도 있습니다. ONTAP 9.13.1 부터는 시스템 관리자를 사용하여 스냅샷 복사본 잠금 정책을 생성하고 볼륨에 적용할 수 있습니다.

스냅샷 복사본 잠금 정책을 생성합니다

시스템 관리자

1. 스토리지 > 스토리지 VM * 으로 이동하여 스토리지 VM을 선택합니다.
2. 설정 * 을 선택합니다.
3. Snapshot Policies * 를 찾아 선택합니다 →.
4. 스냅샷 정책 추가 * 창에서 정책 이름을 입력합니다.
5. 를 선택합니다 + Add .
6. 일정 이름, 유지할 최대 스냅샷 복사본, SnapLock 보존 기간을 비롯한 스냅샷 복사본 일정 세부 정보를 제공합니다.
7. SnapLock 보존 기간 * 열에 스냅샷 복사본을 보존할 시간, 일, 월 또는 년의 수를 입력합니다. 예를 들어, 보존 기간이 5일인 스냅샷 복사본 정책은 스냅샷 복사본이 생성된 후 5일 동안 잠기고, 이 기간 동안에는 삭제할 수 없습니다. 다음과 같은 보존 기간 범위가 지원됩니다.
   - 연도: 0-100
   - 월: 0-1200
   - 일 수: 0 - 36500
   - 시간: 0-24
8. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 스냅샷 복사본 정책을 생성하려면 다음 명령을 입력합니다.

   `volume snapshot policy create -policy policy_name -enabled true -schedule1` *`schedule1_name`* `-count1` *`maximum_Snapshot_copies -retention-period1 _retention_period`*

   다음 명령을 실행하면 스냅샷 복사본 잠금 정책이 생성됩니다.

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   스냅샷 복사본은 활성 보존 상태에 있는 경우 교체되지 않습니다. 즉, 아직 만료되지 않은 잠긴 스냅샷 복사본이 있는 경우 보존 횟수가 적용되지 않습니다.

볼륨에 잠금 정책을 적용합니다

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 선택합니다 ⋮ 편집 > 볼륨 * 을 선택합니다.
3. Edit Volume * (볼륨 편집 *) 창에서 * Schedule Snapshot copies * (스냅샷 복사본 예약 *)를 선택합니다.
4. 목록에서 잠금 스냅샷 복사본 정책을 선택합니다.
5. 스냅샷 복사본 잠금이 아직 활성화되지 않은 경우 * 스냅샷 잠금 활성화 * 를 선택합니다.
6. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 기존 볼륨에 스냅샷 복사본 잠금 정책을 적용하려면 다음 명령을 입력합니다.

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

수동 스냅샷 복사본 생성 중에 보존 기간을 적용합니다

스냅샷 복사본을 수동으로 생성할 때 스냅샷 복사본 보존 기간을 적용할 수 있습니다. 볼륨에 스냅샷 복사본 잠금이 설정되어 있어야 합니다. 그렇지 않으면 보존 기간 설정이 무시됩니다.

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 복사본 * 탭을 선택합니다.
3. 를 선택합니다 + Add .
4. 스냅샷 복사본 이름 및 SnapLock 만료 시간을 입력합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
5. 변경 사항을 저장합니다.
6. 볼륨 > 스냅샷 복사본 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되어 있는지 확인합니다.

CLI를 참조하십시오

1. 스냅샷 복사본을 수동으로 생성하고 잠금 보존 기간을 적용하려면 다음 명령을 입력합니다.

   ```
   volume snapshot create -volume volume_name -snapshot snapshot_copy_name
   -snaplock-expiry-time expiration_date_time
   ```

   다음 명령을 실행하면 새 스냅샷 복사본이 생성되고 보존 기간이 설정됩니다.

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

기존 스냅샷 복사본에 보존 기간을 적용합니다

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 복사본 * 탭을 선택합니다.
3. 스냅샷 복사본을 선택하고 를 선택합니다 ⋮을 클릭하고 * Modify SnapLock Expiration Time * 을 선택합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
4. 변경 사항을 저장합니다.
5. 볼륨 > 스냅샷 복사본 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되어 있는지 확인합니다.

CLI를 참조하십시오

1. 기존 스냅샷 복사본에 보존 기간을 수동으로 적용하려면 다음 명령을 입력합니다.

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   다음 예에서는 기존 스냅샷 복사본에 보존 기간을 적용합니다.

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

기존 정책을 수정하여 장기 보존을 적용합니다

ONTAP 9.14.1부터 스냅샷 복사본의 장기 보존을 설정하는 규칙을 추가하여 기존 SnapMirror 정책을 수정할 수 있습니다. 이 규칙은 SnapLock 소산 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 기본 볼륨 보존 기간을 재정의하는 데 사용됩니다.

1. 기존 SnapMirror 정책에 규칙 추가:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of Snapshot copies> -retention
   -period [<integer> days|months|years]
   ```

   다음 예에서는 "LockVault"라는 기존 정책에 6개월의 보존 기간을 적용하는 규칙을 만듭니다.

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

SnapLock API

Zephyr API를 사용하여 스크립트 또는 워크플로우 자동화의 SnapLock 기능과 통합할 수

있습니다. API는 HTTP, HTTPS 및 Windows DCE/RPC를 통한 XML 메시징을 사용합니다. 자세한 내용은 을 참조하십시오 "ONTAP 자동화 문서".

file-fingerprint-abort 를 참조하십시오

파일 지문 작업을 중단합니다.

파일 지문 덤프

파일 지문 정보를 표시합니다.

파일 지문 인식-GET-ITER

파일 지문 작업의 상태를 표시합니다.

파일 지문 시작

파일 지문을 생성합니다.

SnapLock-archive-vserver-log를 참조하십시오

활성 감사 로그 파일을 보관합니다.

SnapLock-create-vserver-log

SVM에 대한 감사 로그 구성을 생성합니다.

SnapLock-delete-vserver-log를 참조하십시오

SVM에 대한 감사 로그 구성을 삭제합니다.

snaplock-file-privileged-delete를 선택합니다

권한이 있는 삭제 작업을 실행합니다.

SnapLock-get-file-retention을 참조하십시오

파일의 보존 기간을 가져옵니다.

SnapLock - 노드 규정 준수 - 클록

노드 ComplianceClock 날짜 및 시간을 가져옵니다.

SnapLock-get-vserver-active-log-files-ITER로 이동합니다

활성 로그 파일의 상태를 표시합니다.

SnapLock-get-vserver-log-ITER

감사 로그 구성을 표시합니다.

SnapLock-modify-vserver-log에 기록됩니다

SVM에 대한 감사 로그 구성을 수정합니다.

SnapLock-set-file-retention을 참조하십시오

파일의 보존 시간을 설정합니다.

SnapLock-set-node-compliance-clock으로 설정됩니다

노드 ComplianceClock 날짜 및 시간을 설정합니다.

snaplock - 볼륨 설정 - 권한 있는 - 삭제

SnapLock 엔터프라이즈 볼륨에서 권한 있는 삭제 옵션을 설정합니다.

볼륨-GET-SnapLock-attrs

SnapLock 볼륨의 특성을 가져옵니다.

볼륨 세트 - SnapLock - attrs

SnapLock 볼륨의 속성을 설정합니다.