# ONTAP 사이버 볼트를 통한 데이터 보호

## NetApp data management solutions

NetApp
January 27, 2026

# 목차

# ONTAP 사이버 볼트를 통한 데이터 보호

## ONTAP 사이버 볼트 개요

사이버 금고를 구축해야 하는 가장 큰 이유는 사이버 공격, 특히 랜섬웨어와 데이터 침해가 점점 더 만연해지고 정교해지고 있기 때문입니다. "피싱 증가로 인해" 그리고 자격 증명을 훔치는 방법은 점점 더 정교해지고 있으며, 랜섬웨어 공격을 시작하는 데 사용된 자격 증명은 인프라 시스템에 액세스하는 데 사용될 수 있습니다. 이런 경우에는 강화된 인프라 시스템조차도 공격의 위험에 노출됩니다. 손상된 시스템에 대한 유일한 방어 수단은 데이터를 사이버 금고에 보호하고 격리하는 것입니다.

NetApp의 ONTAP 기반 사이버 볼트는 조직에 가장 중요한 데이터 자산을 보호하기 위한 포괄적이고 유연한 솔루션을 제공합니다. ONTAP 강력한 강화 방법론을 통한 논리적 에어 갭을 활용하여 진화하는 사이버 위협에 탄력적으로 대응할 수 있는 안전하고 격리된 스토리지 환경을 구축할 수 있도록 지원합니다. ONTAP 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서도 데이터의 기밀성, 무결성, 가용성을 보장할 수 있습니다.

> 2024년 7월부터 이전에 PDF로 게시되었던 기술 보고서의 콘텐츠가 ONTAP 제품 문서에 통합되었습니다. 또한, 이 문서와 같은 새로운 기술 보고서(TR)에는 더 이상 TR 번호가 부여되지 않습니다.

### 사이버 볼트란 무엇인가요?

사이버 볼트는 주요 IT 인프라와 분리된 격리된 환경에 중요한 데이터를 저장하는 특정 데이터 보호 기술입니다.

메인 네트워크에 영향을 미치는 맬웨어, 랜섬웨어 또는 내부 위협과 같은 위협으로부터 면역이 있는 "에어갭", 변경 불가능 및 *삭제 불가능*한 데이터 저장소입니다. 사이버 볼트는 *변경 불가능*하고 *삭제 불가능*한 스냅샷을 통해 구현될 수 있습니다.

기존 방식을 사용하는 에어 갭 백업에는 공간을 만들고 1차 및 2차 미디어를 물리적으로 분리하는 작업이 포함됩니다. 미디어를 다른 곳으로 옮기거나 연결을 끊으면 악의적인 행위자가 데이터에 액세스할 수 없습니다. 이렇게 하면 데이터는 보호되지만 복구 시간이 더 느려질 수 있습니다.

### NetApp의 사이버 볼트 접근 방식

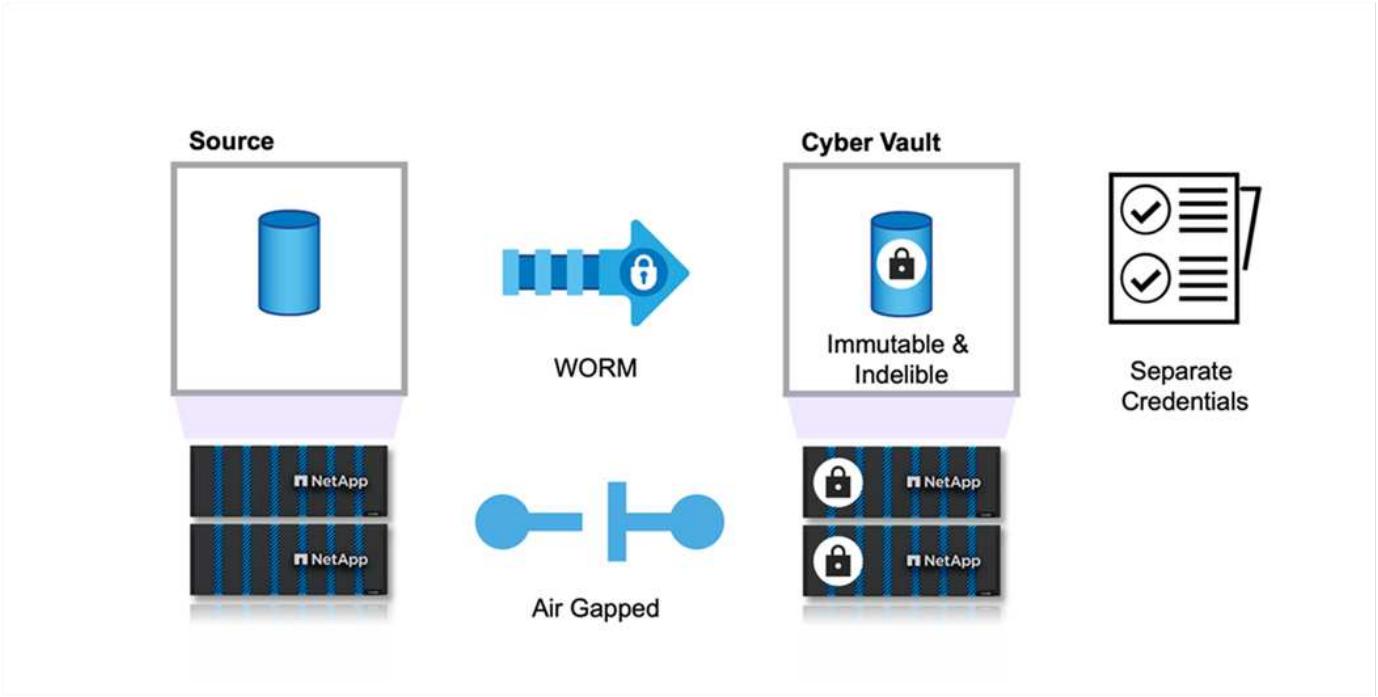
사이버 볼트를 위한 NetApp 참조 아키텍처의 주요 기능은 다음과 같습니다.

- 안전하고 격리된 저장 인프라(예: 에어갭 저장 시스템)
- 데이터 사본은 예외 없이 *변경 불가능*하고 *삭제 불가능*해야 합니다.
- 엄격한 접근 제어 및 다중 요소 인증
- 빠른 데이터 복구 기능

ONTAP 활용하여 NetApp 스토리지를 에어갭 사이버 볼트로 사용할 수 있습니다."WORM 보호 스냅샷 복사본에 대한 SnapLock Compliance" . Cyber Vault에서 모든 기본 SnapLock Compliance 작업을 수행할 수 있습니다. 사이버 볼트 볼륨을 구성하면 자동으로 보호되므로 스냅샷 복사본을 WORM에 수동으로 커밋할 필요가 없습니다. 논리적 공기 간격에 대한 자세한 내용은 여기에서 확인할 수 있습니다."블로그"

SnapLock Compliance 은행 및 금융 규정 SEC 70-a-4(f), FINRA 4511(c) 및 CFTC 1.31(c)-(d)를 준수하는 데

사용됩니다. 본 회사는 이러한 규정을 준수한다는 것을 Cohasset Associates에서 인증받았습니다(요청 시 감사 보고서 제공). 이 인증을 통해 SnapLock Compliance 사용하면 전 세계 최대 규모의 금융 기관에서 은행 기록의 보존 및 검색을 보장하기 위해 사용하는 강화된 데이터 공기 차단 메커니즘을 얻을 수 있습니다.




# 사이버 볼트 **ONTAP** 용어

## 이는 사이버 볼트 아키텍처에서 일반적으로 사용되는 용어입니다.

자율 랜섬웨어 보호**(ARP)** - 자율 랜섬웨어 보호(ARP) 기능은 NAS(NFS 및 SMB) 환경에서 작업 부하 분석을 사용하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 실시간으로 감지하고 경고합니다. 공격이 의심되면 ARP는 예약된 스냅샷 복사본의 기존 보호 외에도 새로운 스냅샷 복사본을 생성합니다. 자세한 내용은 다음을 참조하세요."자율 랜섬웨어 보호에 대한 ONTAP 문서"

에어갭**(**논리적**)** - ONTAP 활용하여 NetApp 스토리지를 논리적 에어갭 사이버 볼트로 구성할 수 있습니다."WORM 보호 스냅샷 복사본에 대한 SnapLock Compliance"

공기 갭**(**물리적**)** - 물리적 공기 갭 시스템에는 네트워크 연결이 없습니다. 테이프 백업을 사용하면 이미지를 다른 위치로 옮길 수 있습니다. SnapLock Compliance 논리적 공기 간격은 물리적 공기 간격 시스템만큼 견고합니다.

보스천 호스트 - 공격을 견딜 수 있도록 구성된 격리된 네트워크의 전용 컴퓨터입니다.

변경 불가능한 스냅샷 복사본 - 예외 없이 수정할 수 없는 스냅샷 복사본(지원 조직이나 저장 시스템을 저수준 포맷하는 기능 포함).

삭제할 수 없는 스냅샷 사본 - 예외 없이 삭제할 수 없는 스냅샷 사본(지원 조직이나 저장 시스템을 저수준 포맷하는 기능 포함).

변조 방지 스냅샷 복사본 - 변조 방지 스냅샷 복사본은 SnapLock Compliance 시계 기능을 사용하여 지정된 기간 동안 스냅샷 복사본을 잠급니다. 이러한 잠긴 스냅샷은 어떠한 사용자나 NetApp 지원팀에서도 삭제할 수 없습니다. 랜섬웨어 공격, 맬웨어, 해커, 사기성 관리자 또는 실수로 인한 삭제로 인해 볼륨이 손상된 경우 잠긴 스냅샷 복사본을 사용하여 데이터를 복구할 수 있습니다. 자세한 내용은 다음을 참조하세요."변조 방지 스냅샷 복사본에 대한 ONTAP 문서"

- SnapLock* - SnapLock 규제 및 거버넌스 목적으로 파일을 수정하지 않은 상태로 보관하기 위해 WORM 스토리지를 사용하는 조직을 위한 고성능 규정 준수 솔루션입니다. 자세한 내용은 다음을 참조하십시오. "SnapLock 에 대한 ONTAP 문서" .
- SnapMirror* - SnapMirror 데이터를 효율적으로 복제하도록 설계된 재해 복구 복제 기술입니다. SnapMirror 온프레미스 또는 클라우드의 보조 시스템에 미러(또는 데이터의 정확한 사본), 볼트(스냅샷 사본을 장기간 보존하는 데이터 사본) 또는 둘 다를 생성할 수 있습니다. 이러한 사본은 재해, 클라우드로의 데이터 유출, 사이버 보관소(보관소 정책을 사용하고 보관소를 잠그는 경우) 등 다양한 목적으로 사용될 수 있습니다. 자세한 내용은 다음을 참조하세요."SnapMirror 에 대한 ONTAP 문서"
- SnapVault* - ONTAP 9.3에서는 SnapVault 더 이상 사용되지 않으며 대신 Vault 또는 mirror-vault 정책을 사용하여 SnapMirror 구성하게 되었습니다. 이 용어는 여전히 사용되지만 더 이상 쓰이지 않습니다. 자세한 내용은 다음을 참조하십시오. "SnapVault 에 대한 ONTAP 문서" .

# ONTAP 사용한 사이버 볼트 크기 조정

사이버 볼트의 크기를 결정하려면 주어진 복구 시간 목표(RTO) 내에 얼마나 많은 데이터를 복원해야 하는지 이해해야 합니다. 적절한 크기의 사이버 보관소 솔루션을 올바르게 설계하는 데에는 여러 요소가 고려됩니다. 사이버 볼트의 크기를 결정할 때는 성능과 용량을 모두 고려해야 합니다.

## 성능 크기 고려 사항

1. 소스 플랫폼 모델은 무엇입니까(FAS 대 AFF A-Series 대 AFF C-Series)?
2. 소스와 사이버 볼트 간의 대역폭과 지연 시간은 어떻게 됩니까?
3. 파일 크기는 얼마나 되고, 파일 수는 몇 개입니까?
4. 귀하의 회복 시간 목표는 무엇입니까?
5. RTO 내에 얼마나 많은 데이터를 복구해야 합니까?
6. 사이버 볼트는 몇 개의 SnapMirror 팬인 관계를 수집하게 될까요?
7. 동시에 단일 복구가 발생합니까, 아니면 여러 복구가 발생합니까?
8. 여러 번의 복구가 동일한 기본 복구에서 일어날까요?
9. 볼트에서 복구하는 동안 SnapMirror 볼트로 복제되나요?

### 크기 조정 예

다양한 사이버 볼트 구성의 예는 다음과 같습니다.


| Platform | AFF A1K | AFF C400 | AFF C250 | FAS70 |
|---|---|---|---|---|
| Estimated RTO (100TB) | 5 HR | 18 HR | 24 HR | 24> HR |
| Relative cost | High | Moderate | Low | Ultra Low |

## 용량 크기 고려 사항

ONTAP 사이버 볼트 대상 볼륨에 필요한 디스크 공간의 양은 다양한 요소에 따라 달라지는데, 그 중 가장 중요한 요소는 소스 볼륨의 데이터 변경 속도입니다. 대상 볼륨의 백업 일정과 스냅샷 일정은 모두 대상 볼륨의 디스크 사용량에 영향을 미치며, 소스 볼륨의 변경 속도는 일정하지 않을 가능성이 높습니다. 최종 사용자나 애플리케이션 동작의 향후 변경 사항을 수용하는 데 필요한 것보다 더 많은 저장 용량을 버퍼로 제공하는 것이 좋습니다.

ONTAP 에서 1개월 동안 보존할 관계의 크기를 조정하려면 기본 데이터 세트의 크기, 데이터 변경률(일일 변경률), 중복 제거 및 압축 절감(해당되는 경우)을 포함한 여러 요소를 기반으로 저장 요구 사항을 계산해야 합니다.

단계별 접근 방식은 다음과 같습니다.

첫 번째 단계는 사이버 볼트로 보호하고 있는 소스 볼륨의 크기를 아는 것입니다. 이는 사이버 보관소 목적지에 처음 복제되는 기본 데이터 양입니다. 다음으로, 데이터 세트에 대한 일일 변화율을 추정합니다. 이는 매일 변경되는 데이터의 비율입니다. 데이터의 동적성을 잘 이해하는 것이 중요합니다.

예를 들어:

- 1차 데이터 세트 크기 = 5TB
- 일일 변화율 = 5% (0.05)
- 중복 제거 및 압축 효율성 = 50% (0.50)

이제 계산을 살펴보겠습니다.

- 일일 데이터 변경률을 계산합니다.

```
Changed data per day = 5000 * 5% = 250GB
```

- 30일 동안 변경된 총 데이터를 계산합니다.

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- 필요한 총 저장 공간을 계산하세요.

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- 중복 제거 및 압축 절감을 적용합니다.

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

저장 요구 사항 요약

- 효율성이 없다면 30일 치의 사이버 보관소 데이터를 저장하려면 *12.5TB*가 필요할 것입니다.
- 50% 효율성으로 보면 중복 제거 및 압축 후 *6.25TB*의 저장 공간이 필요합니다.

스냅샷 복사본에는 메타데이터로 인해 추가적인 오버헤드가 발생할 수 있지만, 일반적으로 이는 사소합니다.

하루에 여러 번 백업을 수행하는 경우 매일 수행되는 스냅샷 복사본 수에 따라 계산을 조정하세요.

시간 경과에 따른 데이터 증가를 고려하여 미래에도 대응할 수 있는 크기 조정을 보장합니다.

# ONTAP 사용하여 사이버 볼트 만들기

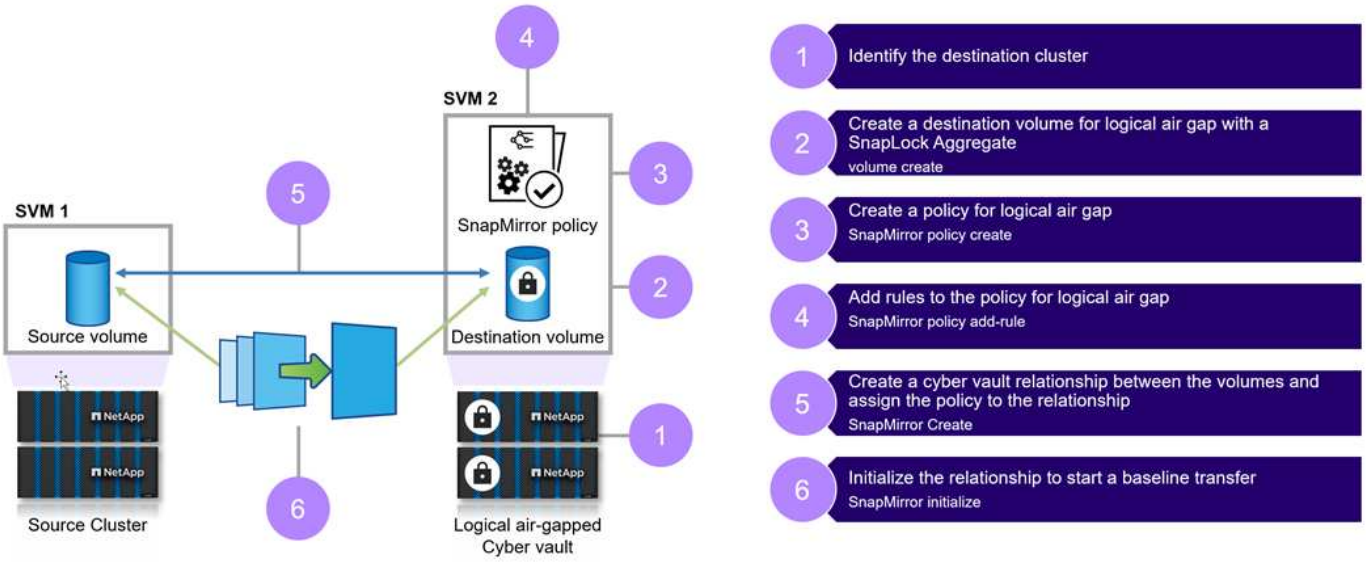
아래 단계는 ONTAP 사용하여 사이버 볼트를 만드는 데 도움이 됩니다.

시작하기 전에

- 소스 클러스터는 ONTAP 9 이상을 실행해야 합니다.
- 소스 및 대상 집계는 64비트여야 합니다.
- 소스 및 대상 볼륨은 피어링된 SVM이 있는 피어링된 클러스터에 생성되어야 합니다. 자세한 내용은 다음을 참조하세요. "클러스터 피어링" .
- 볼륨 자동 증가가 비활성화된 경우 대상 볼륨의 여유 공간은 소스 볼륨의 사용 공간보다 최소 5% 이상 많아야 합니다.

이 작업에 관하여

다음 그림은 SnapLock Compliance 볼트 관계를 초기화하는 절차를 보여줍니다.




단계

1. 에어갭 데이터를 수신할 사이버 볼트가 될 대상 어레이를 식별합니다.
2. 목적지 배열에서 사이버 볼트를 준비하려면"ONTAP One 라이선스 설치" ,"규정 준수 시계 초기화" , 그리고 9.10.1 이전의 ONTAP 릴리스를 사용하는 경우"SnapLock Compliance 집계 생성" .
3. 대상 배열에서 DP 유형의 SnapLock Compliance 대상 볼륨을 만듭니다.

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

4. 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. 볼륨을 사용하세요 `-snaplock-type` 규정 준수 유형을 지정하는 옵션입니다. ONTAP 9.10.1 이전의 ONTAP 릴리스에서는 SnapLock 모드에서 규정 준수가 집계에서 상속되었습니다. 버전 유연한 대상 볼륨은 지원되지 않습니다. 대상 볼륨의 언어 설정은 소스

볼륨의 언어 설정과 일치해야 합니다.

다음 명령은 2GB SnapLock Compliance 볼륨을 생성합니다. `dstvolB` ~에 `SVM2` 전체적으로 `node01_aggr` :

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

5. 대상 클러스터에서 에어갭을 생성하려면 다음에서 설명한 대로 기본 보존 기간을 설정하십시오."기본 보존 기간 설정" . 볼트 대상인 SnapLock 볼륨에는 기본 보존 기간이 할당됩니다. 이 기간의 값은 처음에 최소 0년, 최대 100년으로 설정됩니다( ONTAP 9.10.1부터). 이전 ONTAP 릴리스의 경우 SnapLock Compliance 볼륨의 값은 0~70입니다. 각 NetApp 스냅샷 복사본은 처음에 이 기본 보존 기간으로 커밋됩니다. 기본 보존 기간을 변경해야 합니다. 필요한 경우 보관 기간을 나중에 연장할 수 있지만, 절대로 단축할 수는 없습니다. 자세한 내용은 다음을 참조하세요. "보존 시간 설정 개요" .

   서비스 제공자는 보존 기간을 결정할 때 고객의 계약 종료일을 고려해야 합니다. 예를 들어, 사이버 볼트의 보관 기간이 30일이고 보관 기간이 만료되기 전에 고객의 계약이 종료되는 경우, 사이버 볼트에 있는 데이터는 보관 기간이 만료될 때까지 삭제할 수 없습니다.

6. "새로운 복제 관계 생성"3단계에서 만든 새로운 SnapLock 대상과 SnapLock 이 아닌 소스 사이입니다.

   이 예제에서는 XDPDefault 정책을 사용하여 대상 SnapLock 볼륨 dstvolB와 새로운 SnapMirror 관계를 생성하여 매시간 일정에 따라 매일 및 매주 레이블이 지정된 스냅샷 복사본을 보관합니다.

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

   "사용자 정의 복제 정책 만들기"또는"사용자 정의 일정" 사용 가능한 기본값이 적합하지 않은 경우.

7. 대상 SVM에서 5단계에서 만든 SnapVault 관계를 초기화합니다.

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

8. 다음 명령은 SVM1의 소스 볼륨 srcvolA와 SVM2의 대상 볼륨 dstvolB 간의 관계를 초기화합니다.

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

9. 관계가 초기화되고 유휴 상태가 되면 대상에서 스냅샷 표시 명령을 사용하여 복제된 스냅샷 복사본에 적용된 SnapLock 만료 시간을 확인합니다.

   이 예제에서는 SnapMirror 레이블과 SnapLock 만료 날짜가 있는 볼륨 dstvolB의 스냅샷 복사본을 나열합니다.

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

# 사이버 볼트 강화

ONTAP 사이버 볼트를 강화하기 위한 추가 권장 사항은 다음과 같습니다. 더 많은 권장 사항과 절차에 대해서는 아래의 ONTAP 강화 가이드를 참조하세요.

### 사이버 볼트 강화 권장 사항

- 사이버 볼트의 관리 평면을 분리합니다.
- 대상 클러스터에서 데이터 LIF를 활성화하지 마십시오. 이는 추가 공격 벡터이기 때문입니다.
- 대상 클러스터에서 서비스 정책을 사용하여 소스 클러스터에 대한 클러스터 간 LIF 액세스를 제한합니다.
- 서비스 정책 및 요새 호스트를 사용하여 제한된 액세스를 위해 대상 클러스터의 관리 LIF를 분할합니다.
- SnapMirror 트래픽에 필요한 포트만 허용하도록 소스 클러스터에서 사이버 볼트로의 모든 데이터 트래픽을 제한합니다.
- 가능한 경우 ONTAP 내에서 불필요한 관리 액세스 방법을 비활성화하여 공격 표면을 줄이십시오.
- 감사 로깅 및 원격 로그 저장 활성화
- 여러 관리자 검증을 활성화하고 일반 스토리지 관리자(예: CISO 직원) 외부의 관리자로부터 검증을 요구합니다.
- 역할 기반 액세스 제어 구현
- System Manager 및 ssh에 대한 관리 다중 요소 인증 요구
- 스크립트 및 REST API 호출에 토큰 기반 인증을 사용하세요.

참고해주세요"ONTAP 강화 가이드" ,"다중 관리자 검증 개요" 그리고"ONTAP 다중 인증 가이드" 이러한 강화 단계를 수행하는 방법에 대해 알아보세요.

# 사이버 볼트 상호 운용성

ONTAP 하드웨어와 소프트웨어를 사용하여 사이버 볼트 구성을 생성할 수 있습니다.

## ONTAP 하드웨어 권장 사항

모든 ONTAP 통합 물리적 어레이는 사이버 볼트 구현에 사용될 수 있습니다.

- FAS 하이브리드 스토리지는 가장 비용 효율적인 솔루션을 제공합니다.
- AFF C 시리즈는 가장 효율적인 전력 소비와 밀도를 제공합니다.
- AFF A-Series는 최고의 RTO를 제공하는 가장 성능이 뛰어난 플랫폼입니다. 최근 발표된 최신 AFF A-시리즈를 통해 이 플랫폼은 성능 저하 없이 최고의 스토리지 효율성을 제공할 것입니다.

## ONTAP 소프트웨어 권장 사항

ONTAP 9.14.1부터 SnapMirror 관계의 SnapMirror 정책에서 특정 SnapMirror 레이블에 대한 보존 기간을 지정할 수 있으므로 소스 볼륨에서 대상 볼륨으로 복제된 스냅샷 복사본이 규칙에 지정된 보존 기간 동안 보존됩니다. 보존 기간이 지정되지 않으면 대상 볼륨의 기본 보존 기간이 사용됩니다.

ONTAP 9.13.1부터 SnapLock 볼트 관계의 대상 SnapLock 볼륨에서 잠긴 스냅샷 복사본을 즉시 복원할 수 있습니다. 이를 위해 FlexClone 생성합니다. 자세히 알아보세요 "SnapLock 유형으로 FlexClone 볼륨 생성" .

## MetroCluster 구성

MetroCluster 구성의 경우 다음 사항을 알고 있어야 합니다.

- SnapVault 관계는 동기화 소스 SVM 간에만 생성할 수 있으며, 동기화 소스 SVM과 동기화 대상 SVM 간에는 생성할 수 없습니다.
- 동기화 소스 SVM의 볼륨에서 데이터 제공 SVM으로 SnapVault 관계를 생성할 수 있습니다.
- 데이터 제공 SVM의 볼륨에서 동기화 소스 SVM의 DP 볼륨으로 SnapVault 관계를 생성할 수 있습니다.

# 사이버 볼트 자주 묻는 질문

이 FAQ는 NetApp 고객과 파트너를 대상으로 합니다. 이 문서에서는 NetApp의 ONTAP 기반 사이버 볼트 참조 아키텍처에 대해 자주 묻는 질문에 답변합니다.

## NetApp 사이버 볼트란 무엇인가요?

사이버 볼트는 주요 IT 인프라와 분리된 격리된 환경에 데이터를 저장하는 특정 데이터 보호 기술입니다.

사이버 볼트는 악성 소프트웨어, 랜섬웨어 또는 내부 위협과 같이 기본 데이터에 영향을 미치는 위협으로부터 면역이 있는 "공기 차단" 방식의 변경 불가능하고 삭제 불가능한 데이터 저장소입니다. 변경 불가능한 NetApp ONTAP 스냅샷 복사본을 사용하여 사이버 볼트를 구축하고 NetApp SnapLock Compliance 사용하여 삭제할 수 없게 만들 수 있습니다. SnapLock Compliance 보호가 적용되는 동안에는 ONTAP 관리자나 NetApp 지원팀에서도 데이터를 수정하거나 삭제할 수 없습니다.

기존 방식을 이용한 에어 갭 백업에는 공간을 만들고 1차 매체와 2차 매체를 물리적으로 분리하는 작업이 포함됩니다. 사이버 볼트를 활용한 에어갭핑에는 표준 데이터 액세스 네트워크 외부의 별도의 데이터 복제 네트워크를 사용하여 스냅샷 사본을 영구적인 대상에 복제하는 작업이 포함됩니다.

공기 단절 네트워크를 넘어서는 추가 조치에는 필요하지 않을 때 사이버 보관소의 모든 데이터 접근 및 복제 프로토콜을 비활성화하는 것이 포함됩니다. 이를 통해 대상 사이트에서의 데이터 접근이나 데이터 유출이 방지됩니다. SnapLock Compliance 사용하면 물리적 분리가 필요하지 않습니다. SnapLock Compliance 보관된 특정 시점의 읽기 전용 스냅샷 사본을 보호하여 삭제로부터 안전하고 변경할 수 없는 빠른 데이터 복구를 가능하게 합니다.

## NetApp의 사이버 볼트 접근 방식

SnapLock 기반의 NetApp 사이버 볼트는 조직에 가장 중요한 데이터 자산을 보호하기 위한 포괄적이고 유연한 솔루션을 제공합니다. NetApp ONTAP 의 강화 기술을 활용하여 진화하는 사이버 위협에 면역이 있는 안전하고, 공기 차단되고, 격리된 사이버 볼트를 만들 수 있도록 지원합니다. NetApp 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서도 데이터의 기밀성, 무결성, 가용성을 보장할 수 있습니다.

사이버 볼트를 위한 NetApp 참조 아키텍처의 주요 기능은 다음과 같습니다.

- 안전하고 격리된 저장 인프라(예: 에어갭 저장 시스템)
- 데이터의 백업 사본은 변경 불가능하고 삭제 불가능합니다.
- 엄격하고 별도의 접근 제어, 다중 관리자 검증 및 다중 요소 인증
- 빠른 데이터 복구 기능

## 사이버 볼트 자주 묻는 질문

사이버볼트는 **NetApp** 의 제품인가요**?**

아니요, "사이버 금고"는 업계 전반에서 쓰이는 용어입니다. NetApp 고객이 자체 사이버 볼트를 쉽게 구축하고 수십 가지 ONTAP 보안 기능을 활용하여 사이버 위협으로부터 데이터를 보호할 수 있도록 참조 아키텍처를 만들었습니다. 자세한 내용은 다음에서 확인할 수 있습니다."ONTAP 문서 사이트" .

**NetApp** 의 사이버 볼트는 **LockVault**나 **SnapVault** 의 또 다른 이름일까요**?**

LockVault는 현재 ONTAP 버전에서는 사용할 수 없는 Data ONTAP 7모드의 기능입니다.

SnapVault 현재 SnapMirror의 볼트 정책으로 구현된 기능을 나타내는 기존 용어입니다. 이 정책을 사용하면 대상 볼륨이 소스 볼륨과 다른 수량의 스냅샷 복사본을 보관할 수 있습니다.

사이버 볼트는 SnapMirror 와 볼트 정책, SnapLock Compliance 함께 사용하여 변경 및 삭제가 불가능한 데이터 사본을 생성합니다.

사이버 볼트**, FAS ,** 용량 플래시 또는 성능 플래시에 어떤 **NetApp** 하드웨어를 사용할 수 있나요**?**

사이버 볼트를 위한 이 참조 아키텍처는 전체 ONTAP 하드웨어 포트폴리오에 적용됩니다. 고객은 AFF A-시리즈, AFF C-시리즈 또는 FAS 플랫폼을 볼트로 사용할 수 있습니다. 플래시 기반 플랫폼은 가장 빠른 복구 시간을 제공하는 반면, 디스크 기반 플랫폼은 가장 비용 효율적인 솔루션을 제공합니다. 복구되는 데이터 양과 여러 복구가 병렬로 진행되는 경우 디스크 기반 시스템(FAS)을 사용하면 완료하는 데 며칠에서 몇 주가 걸릴 수 있습니다. 비즈니스 요구 사항을 충족하는 사이버 볼트 솔루션의 적절한 규모를 결정하려면 NetApp 또는 파트너 담당자에게 문의하세요.

**Cloud Volumes ONTAP** 사이버 볼트 소스로 사용할 수 있나요**?**

네, 하지만 CVO를 소스로 사용하려면 SnapLock Compliance ONTAP 사이버 볼트의 요구 사항이므로 데이터를 온프레미스 사이버 볼트 대상에 복제해야 합니다. 하이퍼스케일러 기반 CVO 인스턴스의 데이터 복제에는 유출 요금이 발생할 수 있습니다.

**Cloud Volumes ONTAP** 사이버 볼트 목적지로 사용할 수 있나요**?**

Cyber Vault 아키텍처는 ONTAP의 SnapLock Compliance의 삭제 불가능성에 의존하며 온프레미스 구현을 위해 설계되었습니다. 클라우드 기반 Cyber Vault 아키텍처는 향후 출판을 위해 조사 중입니다.

**ONTAP Select** 사이버 볼트 소스로 사용할 수 있나요**?**

네, ONTAP Select 온프레미스 하드웨어 기반 사이버 볼트 대상에 대한 소스로 사용될 수 있습니다.

**ONTAP Select** 사이버 볼트 목적지로 사용할 수 있나요**?**

아니요, ONTAP Select SnapLock Compliance 사용할 수 있는 기능이 없으므로 사이버 볼트 대상으로 사용해서는 안 됩니다.

**NetApp** 의 사이버 볼트는 **SnapMirror** 만 사용하는 건가요**?**

아니요. NetApp 사이버 볼트 아키텍처는 다양한 ONTAP 기능을 활용하여 안전하고, 격리되고, 공기 간격이 좁고 강화된 데이터 사본을 만듭니다. 추가적으로 사용할 수 있는 기술에 대한 자세한 내용은 다음 질문을 참조하세요.

사이버 볼트에 사용되는 다른 기술이나 구성이 있나요**?**

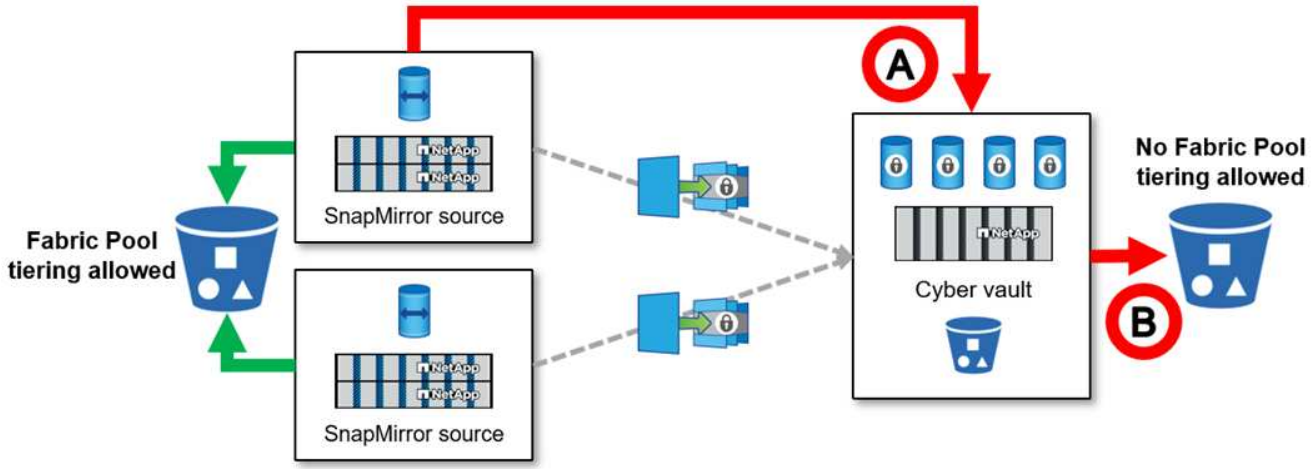
NetApp 사이버 볼트의 기반은 SnapMirror 와 SnapLock Compliance 변조 방지 스냅샷 복사본, 다중 요소 인증(MFA), 다중 관리자 확인, 역할 기반 액세스 제어, 원격 및 로컬 감사 로깅과 같은 추가 ONTAP 기능을 사용하면 데이터의 보안과 안전성이 향상됩니다.

**ONTAP** 스냅샷 복사본이 사이버 볼트에 사용하기에 더 나은 이유는 무엇입니까**?**

ONTAP 스냅샷 사본은 기본적으로 변경 불가능하며 SnapLock Compliance 통해 삭제할 수 없게 만들 수 있습니다. NetApp 지원조차도 SnapLock 스냅샷 복사본을 삭제할 수 없습니다. 더 나은 질문은 NetApp 사이버 볼트가 업계의 다른 사이버 볼트보다 왜 더 나은가 하는 것입니다. 첫째, ONTAP 은 지구상에서 가장 안전한 스토리지로, 하드웨어와 소프트웨어 계층 모두에서 비밀 및 최고 비밀 데이터를 저장할 수 있는 CSfC 검증을 획득했습니다. 더 많은 정보"CSfC는 여기에서 찾을 수 있습니다" . 또한 ONTAP 스토리지 계층에서 에어 갭을 생성할 수 있으며, 사이버 볼트 시스템이 복제를 제어하여 사이버 볼트 네트워크 내에 에어 갭을 생성할 수 있습니다.

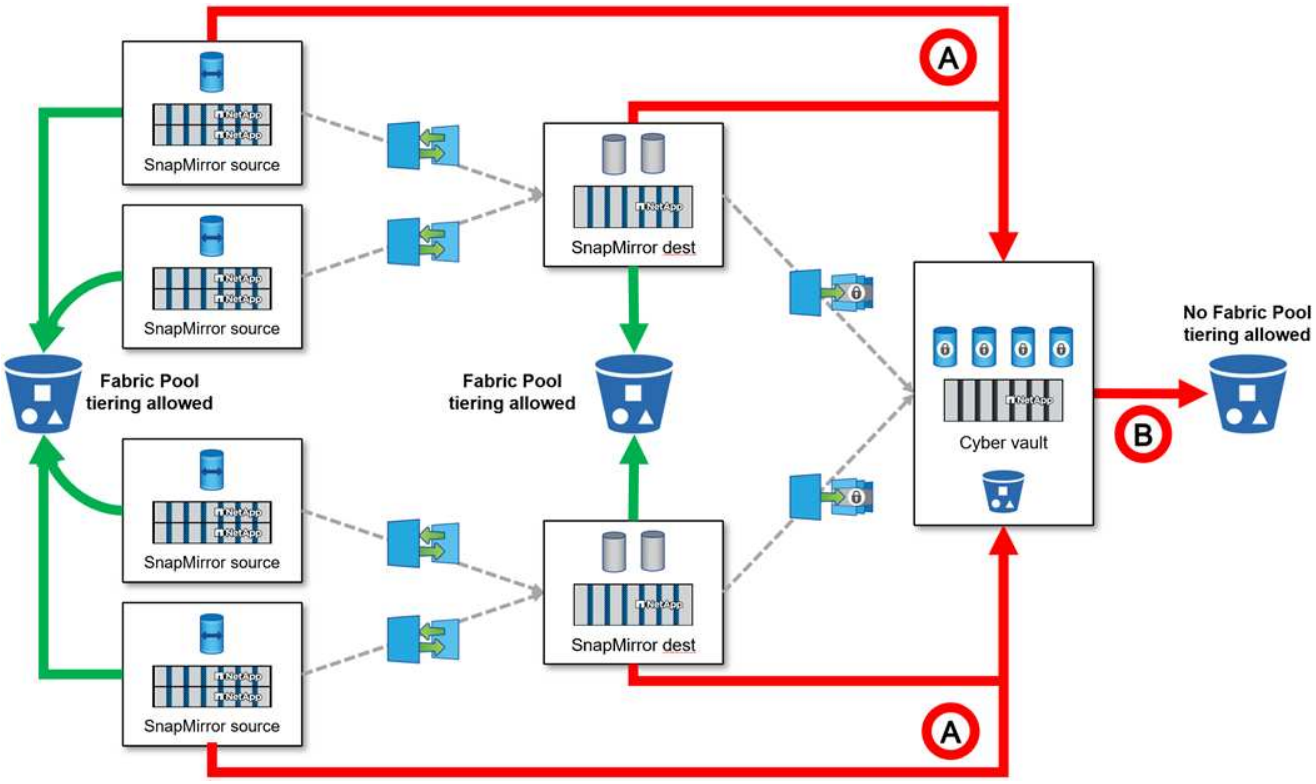
사이버 볼트의 볼륨이 **ONTAP Fabric Pool**을 사용할 수 있나요**?**

아니요, 사이버 볼트 볼륨(SnapLock Compliance SnapMirror 대상)은 정책에 관계없이 Fabric Pool을 사용하여 계층화할 수 없습니다.




Fabric 풀을 사이버 볼트와 함께 사용할 수 없는 시나리오는 여러 가지가 있습니다.

1. Fabric Pool 콜드 티어는 사이버 볼트 클러스터를 사용할 수 없습니다. 이는 S3 프로토콜을 활성화하면 사이버 볼트 참조 아키텍처의 보안 특성이 무효화되기 때문입니다. 또한, Fabric 풀에 사용되는 S3 버킷은 보호될 수 없습니다.
2. 사이버 볼트의 SnapLock Compliance 볼륨은 데이터가 볼륨에 잠겨 있으므로 S3 버킷에 계층화할 수 없습니다.



**ONTAP S3 Worm**을 사이버 볼트에서 사용할 수 있나요**?**

아니요, S3는 참조 아키텍처의 보안 특성을 무효화하는 데이터 액세스 프로토콜입니다.

**NetApp** 사이버 볼트는 다른 **ONTAP** 특성이나 프로필에서 실행됩니까**?**

아니요, 참조 아키텍처입니다. 고객은 다음을 사용할 수 있습니다."참조 아키텍처" 사이버 금고를 구축하거나 사용할 수 있습니다."PowerShell 스크립트를 생성, 강화 및 검증합니다." 사이버 금고.

사이버 금고에서 **NFS, SMB, S3**와 같은 데이터 프로토콜을 켤 수 있나요**?**

기본적으로 사이버 볼트의 데이터 프로토콜은 보안을 위해 비활성화되어야 합니다. 그러나 사이버 볼트에서 데이터 프로토콜을 활성화하여 복구를 위해 또는 필요할 때 데이터에 액세스할 수 있습니다. 이 작업은 일시적으로 수행해야 하며 복구가 완료된 후에는 비활성화해야 합니다.

기존 **SnapVault** 환경을 사이버 볼트로 전환할 수 있나요**?** 아니면 모든 것을 다시 시드해야 하나요**?**

네. SnapMirror 대상(볼트 정책 포함)인 시스템을 가져와 데이터 프로토콜을 비활성화하고 시스템을 강화할 수 있습니다."ONTAP 강화 가이드" 안전한 장소에 격리하고 참조 아키텍처의 다른 절차에 따라 대상을 다시 시드하지 않고도 사이버 볼트로 만들 수 있습니다.

추가 질문이 있으신가요**?** 질문이 있으시면 ng-cyber-vault@netapp.com으로 이메일을 보내주세요! 귀하의 질문에 답변하고 FAQ에 질문을 추가해 드리겠습니다.

# 사이버 볼트 리소스

## 이 사이버 보관소 정보에 설명된 내용에 대해 자세히 알아보려면 다음 추가 정보 및 보안 개념을 참조하세요.

- "NetApp 사이버 볼트: 다층 데이터 보호 솔루션 개요"
- "NetApp, 업계 최초 AI 기반 온박스 랜섬웨어 탐지 솔루션으로 AAA 등급 획득"
- "세계에서 가장 안전한 스토리지로 사이버 복원력을 강화하세요"
- "ONTAP 보안 강화 가이드"
- "NetApp 제로 트러스트"
- "NetApp 사이버 복원력"
- "NetApp 데이터 보호"
- "CLI를 사용한 클러스터 및 SVM 피어링 개요"
- "SnapVault 보관"
- "구성, 분석, Cron 스크립트"

# PowerShell을 사용하여 ONTAP 사이버 볼트 생성, 강화 및 검증

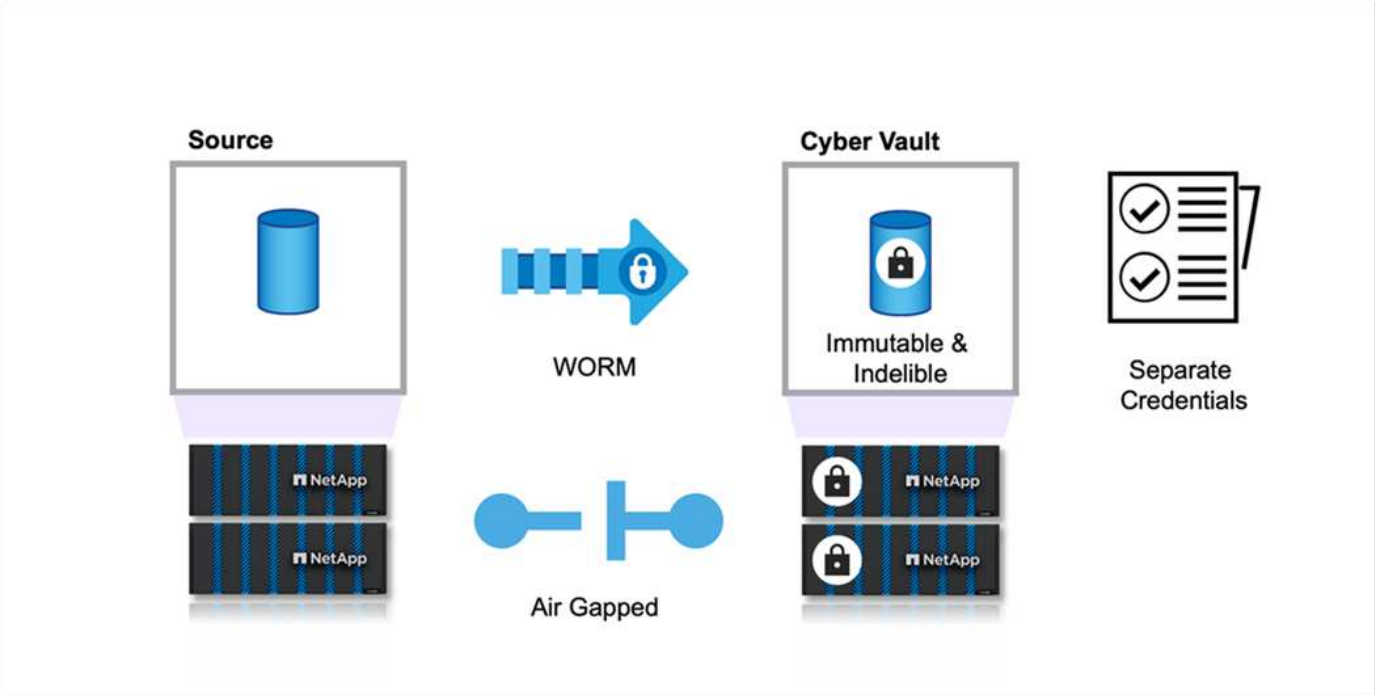
## PowerShell을 사용한 ONTAP 사이버 볼트 개요

오늘날의 디지털 환경에서 조직의 중요 데이터 자산을 보호하는 것은 단순히 모범 사례가 아니라 비즈니스의 필수 사항입니다. 사이버 위협은 전례 없는 속도로 진화하고 있으며, 기존의 데이터 보호 조치로는 더 이상 민감한 정보를 안전하게 보호하기에 충분하지 않습니다. 여기서 사이버 볼트가 등장합니다. NetApp의 최첨단 ONTAP 기반 솔루션은 고급 에어갭 기술과 강력한 데이터 보호 조치를 결합하여 사이버 위협에 대한 뚫을 수 없는 장벽을 구축합니다. 사이버 볼트는 보안 강화 기술을 통해 가장 귀중한 데이터를 격리하여 공격 표면을 최소화하고 가장 중요한 데이터를 기밀로 유지하고 손상되지 않은 상태로 필요할 때 쉽게 사용할 수 있도록 합니다.

사이버 볼트는 방화벽, 네트워킹, 스토리지 등 여러 계층의 보호로 구성된 안전한 저장 시설입니다. 이러한 구성 요소는 중요한 비즈니스 운영에 필요한 중요한 복구 데이터를 보호합니다. 사이버 보관소의 구성 요소는 보관소 정책에 따라 필수 생산 데이터와 정기적으로 동기화되지만, 그 외에는 접근할 수 없습니다. 이러한 격리되고 연결되지 않은 설정 덕분에 사이버 공격으로 인해 프로덕션 환경이 손상되더라도 사이버 보관소에서 안정적이고 최종적인 복구를 쉽게 수행할 수 있습니다.

NetApp 사용하면 네트워크 구성, LIF 비활성화, 방화벽 규칙 업데이트, 시스템을 외부 네트워크 및 인터넷에서 격리하여 사이버 볼트에 대한 에어갭을 쉽게 생성할 수 있습니다. 이러한 강력한 접근 방식은 시스템을 외부 네트워크 및 인터넷에서 효과적으로 분리하여 원격 사이버 공격과 무단 액세스 시도로부터 탁월한 보호 기능을 제공하고, 시스템을 네트워크 기반 위협과 침입으로부터 면역 상태로 만듭니다.

이를 SnapLock Compliance 보호 기능과 결합하면 ONTAP 관리자나 NetApp 지원팀조차도 데이터를 수정하거나 삭제할 수 없습니다. SnapLock 은 SEC 및 FINRA 규정에 따라 정기적으로 감사를 받으며, 이를 통해 데이터 복원력이 은행업계의 엄격한 WORM 및 데이터 보존 규정을 충족하는지 확인합니다. NetApp NSA CSfC에서 최고 기밀 데이터를 저장하는 데 적합하다고 검증받은 유일한 엔터프라이즈 스토리지입니다.



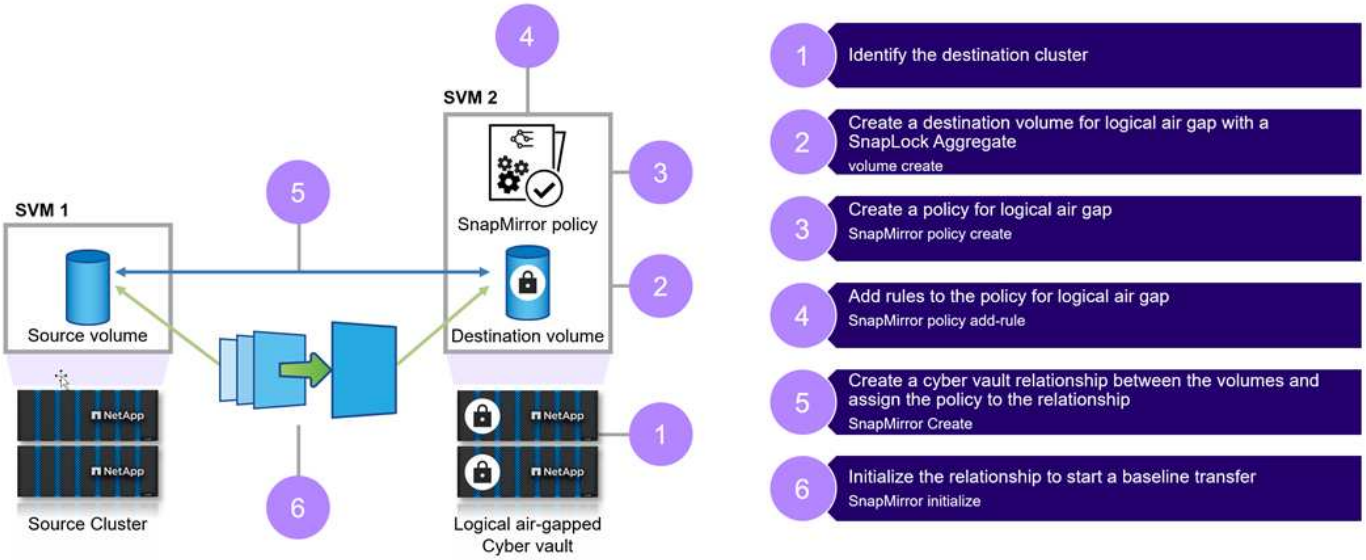

이 문서에서는 온프레미스 ONTAP 스토리지용 NetApp 사이버 볼트를 자동으로 구성하여 변경 불가능한 스냅샷을 통해 증가하는 사이버 공격으로부터 보호 계층을 추가하여 신속하게 복구하는 방법 ONTAP 설명합니다. 이 아키텍처의

일부로 전체 구성은 ONTAP 모범 사례에 따라 적용됩니다. 마지막 섹션에는 공격이 발생한 경우 복구를 수행하는 방법에 대한 지침이 있습니다.

동일한 솔루션은 FSx ONTAP 사용하여 AWS에서 지정된 사이버 볼트를 생성하는 데 적용할 수 있습니다.

**ONTAP** 사이버 볼트를 만드는 고급 단계

- 피어링 관계 만들기
  - ONTAP 스토리지를 사용하는 생산 사이트는 지정된 사이버 볼트 ONTAP 스토리지와 피어링됩니다.
- SnapLock Compliance 볼륨 생성
- SnapMirror 관계 및 레이블 설정 규칙을 설정합니다.
  - SnapMirror 관계 및 적절한 일정이 구성됩니다.
- SnapMirror (볼트) 전송을 시작하기 전에 보존 기간을 설정하세요.
  - 복사된 데이터에는 보존 잠금이 적용되어, 내부자 침입이나 데이터 오류로 인한 데이터 유출을 방지합니다. 이를 사용하면 보존 기간이 만료되기 전에 데이터를 삭제할 수 없습니다.
  - 조직은 요구 사항에 따라 이 데이터를 몇 주/몇 달 동안 보관할 수 있습니다.
- 레이블을 기반으로 SnapMirror 관계를 초기화합니다.
  - 초기 시딩 및 증분적 영구 전송은 SnapMirror 일정에 따라 발생합니다.
  - SnapLock 규정 준수로 데이터가 보호되며(변경 불가능하고 삭제 불가능) 데이터를 복구할 수 있습니다.
- 엄격한 데이터 전송 제어를 구현합니다
  - 사이버 보관소는 생산 현장의 데이터로 일정 기간 동안 잠금 해제되며 보관소의 데이터와 동기화됩니다. 전송이 완료되면 연결이 끊어지고 닫히고 다시 잠깁니다.
- 빠른 회복
  - 생산 현장에서 기본이 영향을 받는 경우 사이버 보관소의 데이터는 원래 생산 현장이나 선택한 다른 환경으로 안전하게 복구됩니다.



솔루션 구성 요소

소스 및 대상 클러스터에서 NetApp ONTAP 9.15.1을 실행합니다.

ONTAP One: NetApp ONTAP의 올인원 라이선스.

ONTAP One 라이선스에서 사용되는 기능:

- SnapLock Compliance
- SnapMirror
- 다중 관리자 검증
- ONTAP 에서 노출된 모든 강화 기능
- 사이버 볼트에 대한 별도의 RBAC 자격 증명

> 모든 ONTAP 통합 물리적 어레이는 사이버 볼트에 사용할 수 있지만, AFF C 시리즈 용량 기반 플래시 시스템과 FAS 하이브리드 플래시 시스템은 이 목적에 가장 비용 효율적인 이상적인 플랫폼입니다. 를 참조해주세요"ONTAP 사이버 볼트 크기 조정" 사이즈 가이드를 참조하세요.

## PowerShell을 사용한 ONTAP 사이버 볼트 생성

기존 방식을 사용하는 에어 갭 백업에는 공간을 만들고 1차 및 2차 미디어를 물리적으로 분리하는 작업이 포함됩니다. 미디어를 다른 곳으로 옮기거나 연결을 끊으면 악의적인 행위자가 데이터에 액세스할 수 없습니다. 이렇게 하면 데이터는 보호되지만 복구 시간이 더 느려질 수 있습니다. SnapLock Compliance 사용하면 물리적 분리가 필요하지 않습니다. SnapLock Compliance 보관된 스냅샷 시점의 읽기 전용 사본을 보호하여 데이터에 빠르게 액세스할 수 있고 삭제나 지울 수 없으며 수정이나 변경이 불가능한 안전한 데이터를 제공합니다.

필수 조건

이 문서의 다음 섹션에 있는 단계를 시작하기 전에 다음 전제 조건이 충족되었는지 확인하세요.

- 소스 클러스터는 ONTAP 9 이상을 실행해야 합니다.
- 소스 및 대상 집계는 64비트여야 합니다.
- 소스 클러스터와 대상 클러스터는 피어링되어야 합니다.
- 소스 및 대상 SVM은 피어링되어야 합니다.
- 클러스터 피어링 암호화가 활성화되어 있는지 확인하세요.

ONTAP 사이버 보관소로의 데이터 전송을 설정하려면 여러 단계가 필요합니다. 기본 볼륨에서 적절한 일정을 사용하여 어떤 복사본을 언제 만들지 지정하는 스냅샷 정책을 구성하고 SnapVault 에서 어떤 복사본을 전송해야 하는지 지정하는 레이블을 지정합니다. 보조적인 스냅샷 복사본의 레이블을 지정하고 사이버 볼트에 보관해야 하는 복사본의 수를 지정하는 SnapMirror 정책을 2차적으로 만들어야 합니다. 이러한 정책을 구성한 후 SnapVault 관계를 만들고 전송 일정을 설정합니다.

> 이 문서에서는 기본 저장소와 지정된 ONTAP 사이버 보관소가 이미 설정 및 구성되어 있다고 가정합니다.

사이버 볼트 클러스터는 소스 데이터와 같은 데이터 센터에 있을 수도 있고 다른 데이터 센터에 있을 수도 있습니다.

**ONTAP** 사이버 볼트를 만드는 단계

1. ONTAP CLI 또는 시스템 관리자를 사용하여 규정 준수 시계를 초기화합니다.
2. SnapLock 규정 준수를 활성화하여 데이터 보호 볼륨을 만듭니다.
3. SnapMirror create 명령을 사용하여 SnapVault 데이터 보호 관계를 만듭니다.
4. 대상 볼륨에 대한 기본 SnapLock Compliance 보존 기간을 설정합니다.

기본 보존 기간은 "최소한으로 설정"되어 있습니다. 볼트 대상인 SnapLock 볼륨에는 기본 보존 기간이 할당됩니다. 이 기간의 값은 처음에 최소 0년, 최대 100년으로 설정됩니다( ONTAP 9.10.1부터). 이전 ONTAP 릴리스의 경우 SnapLock Compliance 볼륨의 값은 0~70입니다. 각 NetApp 스냅샷 복사본은 처음에 이 기본 보존 기간으로 커밋됩니다. 필요한 경우 보관 기간을 나중에 연장할 수 있지만, 절대로 단축할 수는 없습니다. 자세한 내용은 다음을 참조하세요. "보존 시간 설정 개요" .

위에 나열된 내용은 수동 단계를 포함합니다. 보안 전문가들은 오류가 발생할 가능성이 큰 수동 관리를 피하기 위해 프로세스를 자동화할 것을 권장합니다. 아래는 SnapLock 준수 및 시계 초기화의 전제 조건과 구성을 완전히 자동화하는 코드 조각입니다.

다음은 ONTAP 규정 준수 시계를 초기화하는 PowerShell 코드 예입니다.

```
function initializeSnapLockComplianceClock {
    try {
        $nodes = Get-NcNode

        $isInitialized = $false
        logMessage -message "Cheking if snaplock compliance clock is
initialized"
        foreach($node in $nodes) {
            $check = Get-NcSnaplockComplianceClock -Node $node.Node
            if ($check.SnaplockComplianceClockSpecified -eq "True") {
                $isInitialized = $true
            }
        }

        if ($isInitialized) {
            logMessage -message "SnapLock Compliance clock already
initialized" -type "SUCCESS"
        } else {
            logMessage -message "Initializing SnapLock compliance clock"
            foreach($node in $nodes) {
                Set-NcSnaplockComplianceClock -Node $node.Node
            }
            logMessage -message "Successfully initialized SnapLock
Compliance clock" -type "SUCCESS"
        }
    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

다음은 ONTAP 사이버 볼트를 구성하는 PowerShell 코드 예입니다.

```
function configureCyberVault {
    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if the volume already exists and is of type
snaplock compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
```

```
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                # Create SnapLock Compliance volume
                logMessage -message "Creating SnapLock Compliance volume:
$($DESTINATION_VOLUME_NAMES[$i])"
                New-NcVol -Name $DESTINATION_VOLUME_NAMES[$i] -Aggregate
$DESTINATION_AGGREGATE_NAMES[$i] -SnaplockType Compliance -Type DP -Size
$DESTINATION_VOLUME_SIZES[$i] -ErrorAction Stop | Select-Object -Property
Name, State, TotalSize, Aggregate, Vserver
                logMessage -message "Volume $($DESTINATION_VOLUME_NAMES[
$i]) created successfully" -type "SUCCESS"
            }

            # Set SnapLock volume attributes
            logMessage -message "Setting SnapLock volume attributes for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
            Set-NcSnaplockVolAttr -Volume $DESTINATION_VOLUME_NAMES[$i]
-MinimumRetentionPeriod $SNAPLOCK_MIN_RETENTION -MaximumRetentionPeriod
$SNAPLOCK_MAX_RETENTION -ErrorAction Stop | Select-Object -Property Type,
MinimumRetentionPeriod, MaximumRetentionPeriod
            logMessage -message "SnapLock volume attributes set
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"

            # checking snapmirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and ($_.Status
-eq "snapmirrored" -or $_.Status -eq "uninitialized") }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship already
exists for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            } else {
                # Create SnapMirror relationship
                logMessage -message "Creating SnapMirror relationship for
```

```
volume: $($DESTINATION_VOLUME_NAMES[$i])"
                New-NcSnapmirror -SourceCluster $SOURCE_ONTAP_CLUSTER_NAME
-SourceVserver $SOURCE_VSERVER -SourceVolume $SOURCE_VOLUME_NAMES[$i]
-DestinationCluster $DESTINATION_ONTAP_CLUSTER_NAME -DestinationVserver
$DESTINATION_VSERVER -DestinationVolume $DESTINATION_VOLUME_NAMES[$i]
-Policy $SNAPMIRROR_PROTECTION_POLICY -Schedule $SNAPMIRROR_SCHEDULE
-ErrorAction Stop | Select-Object -Property SourceCluster, SourceLocation,
DestinationCluster, DestinationLocation, Status, Policy, Schedule
                logMessage -message "SnapMirror relationship created
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            }

        } catch {
            handleError -errorMessage $_.Exception.Message
        }
    }
}
```

1. 위의 단계를 모두 완료하면 SnapLock Compliance 와 SnapVault 사용한 에어갭 사이버 볼트가 준비됩니다.

스냅샷 데이터를 사이버 볼트로 전송하기 전에 SnapVault 관계를 초기화해야 합니다. 하지만 그 전에 금고의 보안을 강화하는 것이 필요합니다.

## PowerShell을 사용한 ONTAP 사이버 볼트 강화

ONTAP 사이버 볼트는 기존 솔루션에 비해 사이버 공격에 대한 회복력이 더 뛰어납니다. 보안을 강화하기 위한 아키텍처를 설계할 때 공격 표면적을 줄이는 방안을 고려하는 것이 중요합니다. 이는 강화된 암호 정책 구현, RBAC 활성화, 기본 사용자 계정 잠금, 방화벽 구성, 볼트 시스템 변경 사항에 대한 승인 흐름 활용 등 다양한 방법을 통해 달성할 수 있습니다. 더욱이 특정 IP 주소에서 네트워크 접근 프로토콜을 제한하면 잠재적인 취약점을 제한하는 데 도움이 될 수 있습니다.

ONTAP ONTAP 스토리지를 강화할 수 있는 일련의 제어 기능을 제공합니다. 사용하세요"ONTAP 에 대한 지침 및 구성 설정" 조직이 정보 시스템의 기밀성, 무결성, 가용성에 대한 규정된 보안 목표를 충족하도록 돕습니다.

강화 모범 사례

수동 단계

1. 사전 정의되고 사용자 정의된 관리 역할로 지정된 사용자를 만듭니다.
2. 네트워크 트래픽을 분리하기 위해 새로운 IP 공간을 만듭니다.
3. 새로운 IPspace에 있는 새로운 SVM을 만듭니다.
4. 방화벽 라우팅 정책이 올바르게 구성되었는지 확인하고 모든 규칙을 정기적으로 감사하고 필요에 따라 업데이트하세요.

**ONTAP CLI** 또는 자동화 스크립트를 통해

1. 다중 요소 인증(MFA)에 더해 다중 관리자 인증(MAV)으로 관리를 보호하여 데이터 스토리지 VM에 대한 관리 액세스 보안을 강화하십시오.
2. 클러스터 간 "전송 중" 표준 데이터에 대한 암호화를 활성화합니다.
3. 강력한 암호화로 SSH를 보호하고 안전한 비밀번호를 적용하세요.
4. 글로벌 FIPS를 활성화합니다.
5. Telnet 및 원격 셸(RSH)을 비활성화해야 합니다.
6. 기본 관리자 계정을 잠급니다.
7. 데이터 LIF를 비활성화하고 원격 액세스 포인트를 보호합니다.
8. 사용하지 않거나 불필요한 프로토콜과 서비스를 비활성화하고 제거합니다.
9. 네트워크 트래픽을 암호화합니다.
10. 슈퍼유저와 관리자 역할을 설정할 때 최소 권한의 원칙을 사용하세요.
11. 허용된 IP 옵션을 사용하여 특정 IP 주소의 HTTPS 및 SSH를 제한합니다.
12. 전송 일정에 따라 복제를 중지하고 다시 시작합니다.

1~4번 항목은 격리된 네트워크 지정, IP 공간 분리 등 수동 개입이 필요하며 사전에 수행되어야 합니다. 강화를 구성하는 방법에 대한 자세한 정보는 다음에서 찾을 수 있습니다."ONTAP 보안 강화 가이드" . 나머지는 쉽게 자동화하여 배포와 모니터링을 쉽게 할 수 있습니다. 이러한 조직적인 접근 방식의 목적은 볼트 컨트롤러를 미래에도 사용할 수 있도록 강화 단계를 자동화하는 메커니즘을 제공하는 것입니다. 사이버 보관소의 에어갭이 열려 있는 기간은 가능한 한 짧아야 합니다. SnapVault 증분적 영구 기술을 활용하여 마지막 업데이트 이후의 변경 사항만 사이버 볼트로 옮기므로 사이버 볼트가 열려 있어야 하는 시간을 최소화합니다. 워크플로를 더욱 최적화하기 위해 사이버 볼트 개방은 복제 일정과 조정되어 가장 작은 연결 창을 보장합니다.

다음은 ONTAP 컨트롤러를 강화하기 위한 PowerShell 코드 예입니다.

```
function removeSvmDataProtocols {
    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            # Remove NFS
            logMessage -message "Removing NFS protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcNfsService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "NFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
```

```
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            # Remove SMB/CIFS
            logMessage -message "Removing SMB/CIFS protocol on vServer :
$DESTINATION_VSERVER"
            $domainAdministratorUsername = Read-Host -Prompt "Enter Domain
administrator username"
            $domainAdministratorPassword = Read-Host -Prompt "Enter Domain
administrator password" -AsSecureString
            $plainPassword = [Runtime.InteropServices.Marshal
]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($
domainAdministratorPassword))
            Remove-NcCifsServer -VserverContext $DESTINATION_VSERVER
-AdminUsername $domainAdministratorUsername -AdminPassword $plainPassword
-Confirm:$false -ErrorAction Stop
            logMessage -message "SMB/CIFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            # Remove iSCSI
            logMessage -message "Removing iSCSI protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcIscsiService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "iSCSI protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
```

```
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            # Remove FCP
            logMessage -message "Removing FC protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcFcpService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "FC protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function disableSvmDataLifs {
    try {
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Disabling all data lifs on vServer :
$DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $disableLif = Set-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName -AdministrativeStatus down -ErrorAction Stop
            $disableLif | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address
        }
        logMessage -message "Disabled all data lifs on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

```
function configureMultiAdminApproval {
    try {

        # check if multi admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            logMessage -message "Setting Multi-admin verification rules"
            # Define the commands to be restricted
            $rules = @(
                "cluster peer delete",
                "vserver peer delete",
                "volume snapshot policy modify",
                "volume snapshot rename",
                "vserver audit modify",
                "vserver audit delete",
                "vserver audit disable"
            )
            foreach($rule in $rules) {
                Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
rule create -operation `"$rule`""
            }

            logMessage -message "Creating multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
approval-group create -name $MULTI_ADMIN_APPROVAL_GROUP_NAME -approvers
$MULTI_ADMIN_APPROVAL_USERS -email `"$MULTI_ADMIN_APPROVAL_EMAIL`""
            logMessage -message "Created multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification group
```

```
$MULTI_ADMIN_APPROVAL_GROUP_NAME"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -approval-groups $MULTI_ADMIN_APPROVAL_GROUP_NAME -required
-approvers 1 -enabled true"
            logMessage -message "Enabled multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function additionalSecurityHardening {
    try {
        $command = "set -privilege advanced -confirmations off;security
protocol modify -application telnet -enabled false;"
        logMessage -message "Disabling Telnet"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Disabled Telnet" -type "SUCCESS"

        #$command = "set -privilege advanced -confirmations off;security
config modify -interface SSL -is-fips-enabled true;"
        #logMessage -message "Enabling Global FIPS"
        ##Invoke-SSHCommand -SessionId $sshSession.SessionId -Command
$command -ErrorAction Stop
```

```
        #logMessage -message "Enabled Global FIPS" -type "SUCCESS"

        $command = "set -privilege advanced -confirmations off;network
interface service-policy modify-service -vserver cluster2 -policy default-
management -service management-https -allowed-addresses $ALLOWED_IPS;"
        logMessage -message "Restricting IP addresses $ALLOWED_IPS for
Cluster management HTTPS"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Successfully restricted IP addresses
$ALLOWED_IPS for Cluster management HTTPS" -type "SUCCESS"

        #logMessage -message "Checking if audit logs volume audit_logs
exists"
        #$volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Name
audit_logs -ErrorAction Stop

        #if($volume) {
        #    logMessage -message "Volume audit_logs already exists!
Skipping creation"
        #} else {
        #    # Create audit logs volume
        #    logMessage -message "Creating audit logs volume : audit_logs"
        #    New-NcVol -Name audit_logs -Aggregate
$DESTINATION_AGGREGATE_NAME -Size 5g -ErrorAction Stop | Select-Object
-Property Name, State, TotalSize, Aggregate, Vserver
        #    logMessage -message "Volume audit_logs created successfully"
-type "SUCCESS"
        #}

        ## Mount audit logs volume to path /vol/audit_logs
        #logMessage -message "Creating junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER"
        #Mount-NcVol -VserverContext $DESTINATION_VSERVER -Name audit_logs
-JunctionPath /audit_logs | Select-Object -Property Name, -JunctionPath
        #logMessage -message "Created junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER" -type "SUCCESS"

        #logMessage -message "Enabling audit logging for vServer
$DESTINATION_VSERVER at path /vol/audit_logs"
        #$command = "set -privilege advanced -confirmations off;vserver
audit create -vserver $DESTINATION_VSERVER -destination /audit_logs
-format xml;"
        #Invoke-SSHCommand -SessionI  $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Successfully enabled audit logging for
```

```
vServer $DESTINATION_VSERVER at path /vol/audit_logs"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

## PowerShell을 사용한 ONTAP 사이버 볼트 검증

강력한 사이버 볼트는 공격자가 높은 권한으로 환경에 액세스할 수 있는 자격 증명을 가지고 있는 경우에도 정교한 공격을 견뎌낼 수 있어야 합니다.

규칙이 적용되면 공격자가 어떻게든 침투할 수 있었다고 가정하고 볼트 측에서 스냅샷을 삭제하려는 시도는 실패하게 됩니다. 모든 강화 설정에도 필요한 제한을 두고 시스템을 보호함으로써 동일한 것이 적용됩니다.

일정에 따라 구성을 검증하는 PowerShell 코드 예제입니다.

```
function analyze {

    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if volume is of type SnapLock Compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
-type "SUCCESS"
            } else {
                handleError -errorMessage "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) does not exist in vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to create and configure the cyber vault SnapLock Compliance
volume"
            }

            # checking SnapMirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
```

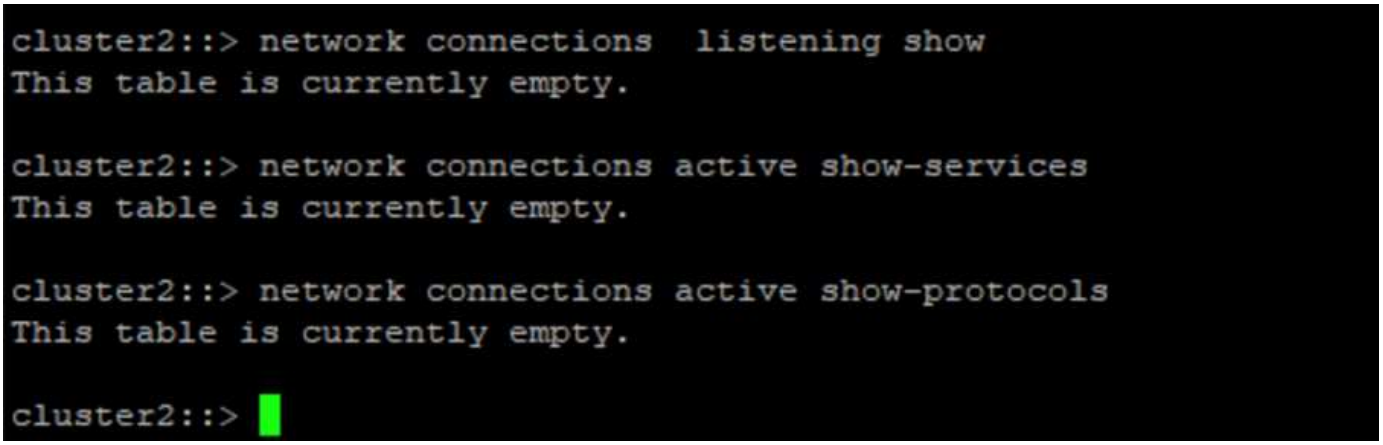
```
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and $_.Status
-eq "snapmirrored" }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship successfully
configured and in healthy state" -type "SUCCESS"
            } else {
                handleError -errorMessage "SnapMirror relationship does
not exist between the source volume $($SOURCE_VOLUME_NAMES[$i]) and
destination SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])
(or) SnapMirror status uninitialized/unhealthy. Recommendation: Run the
script with SCRIPT_MODE `"configure`" to create and configure the cyber
vault SnapLock Compliance volume and configure the SnapMirror
relationship"
            }
        }
        catch {
            handleError -errorMessage $_.Exception.Message
        }
    }

    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            handleError -errorMessage "NFS service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable NFS on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
```

```
            handleError -errorMessage "CIFS/SMB server running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable CIFS/SMB on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            handleError -errorMessage "iSCSI service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable iSCSI on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            handleError -errorMessage "FCP service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable FCP on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking if all data lifs are disabled on vServer
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Checking if all data lifs are disabled for
vServer : $DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
```

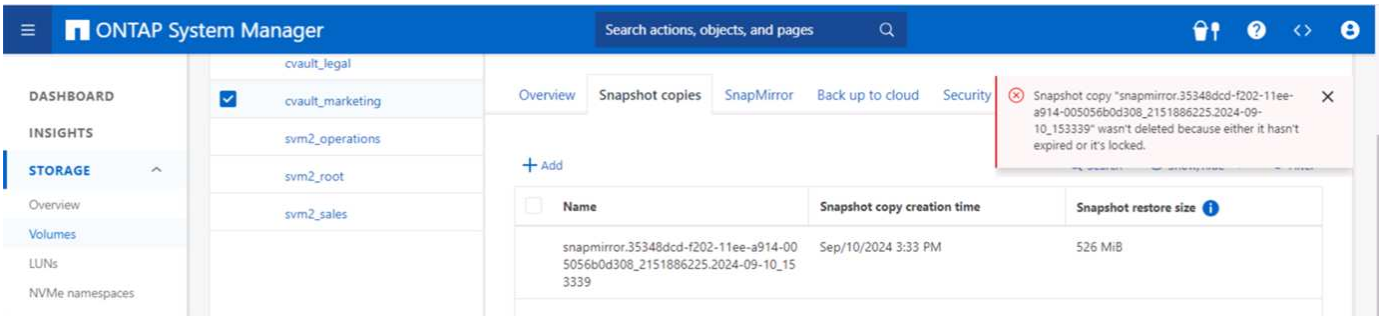
```
            $checkLif = Get-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName | Where-Object { $_.OpStatus -eq "down" }
            if($checkLif) {
                logMessage -message "Data lif $($lif.InterfaceName)
disabled for vServer $DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                handleError -errorMessage "Data lif $($lif.InterfaceName)
is enabled. Recommendation: Run the script with SCRIPT_MODE `"configure`"
to disable Data lifs for vServer $DESTINATION_VSERVER"
            }
        }
        logMessage -message "All data lifs are disabled for vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

        # check if multi-admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Multi-admin verification is not
configured or not enabled. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to enable and configure Multi-admin verification"
        }

        # check if telnet is disabled
        logMessage -message "Checking if telnet is disabled"
        $telnetConfig = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; security protocol show -application
telnet"
        if ($telnetConfig.Value -match "enabled" -and $telnetConfig.Value
-match "false") {
            logMessage -message "Telnet is disabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Telnet is enabled. Recommendation:
Run the script with SCRIPT_MODE `"configure`" to disable telnet"
        }

        # check if network https is restricted to allowed IP addresses
```

```
        logMessage -message "Checking if HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS"
        $networkServicePolicy = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; network interface service-policy show"
        if ($networkServicePolicy.Value -match "management-https:
$($ALLOWED_IPS)") {
            logMessage -message "HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS" -type "SUCCESS"
        } else {
            handleError -errorMessage "HTTPS is not restricted to allowed
IP addresses $ALLOWED_IPS. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to restrict allowed IP addresses for HTTPS management"
        }
    }
    catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

이 스크린샷은 볼트 컨트롤러에 연결이 없다는 것을 보여줍니다.




이 스크린샷은 스냅샷을 조작할 수 있는 기능이 없음을 보여줍니다.



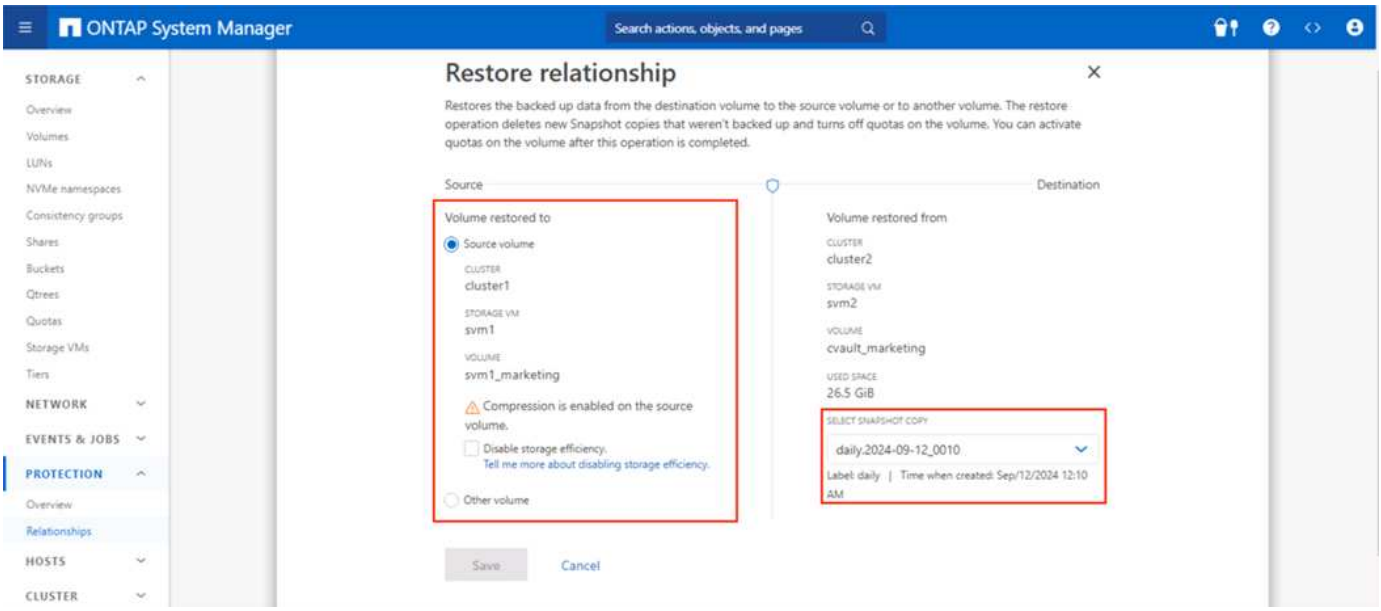

공기 간격 기능을 검증하고 확인하려면 아래 단계를 따르세요.

- 네트워크 격리 기능과 데이터가 전송되지 않을 때 연결을 중지하는 기능을 테스트합니다.
- 허용된 IP 주소 외의 다른 엔터티에서 관리 인터페이스에 액세스할 수 없는지 확인합니다.
- 다중 관리자 검증을 통해 추가적인 승인 계층을 제공합니다.
- CLI 및 REST API를 통해 액세스하는 기능을 검증합니다.
- 소스에서 볼트로 전송 작업을 트리거하고 볼트에 저장된 복사본이 수정될 수 없도록 보장합니다.
- 볼트로 전송된 변경 불가능한 스냅샷 복사본을 삭제해보세요.
- 시스템 시계를 조작하여 보존 기간을 변경해 보세요.

## ONTAP 사이버 볼트 데이터 복구

운영 데이터 센터에서 데이터가 파괴된 경우, 사이버 보관소에 있는 데이터를 선택한 환경으로 안전하게 복구할 수 있습니다. 물리적으로 공기가 차단된 솔루션과 달리 공기가 차단된 ONTAP 사이버 볼트는 SnapLock Compliance 및 SnapMirror 와 같은 기본 ONTAP 기능을 사용하여 구축되었습니다. 그 결과, 빠르고 쉽게 실행할 수 있는 복구 프로세스가 탄생했습니다.

랜섬웨어 공격을 받아 사이버 보관소에서 복구해야 하는 경우, 사이버 보관소에 저장된 스냅샷 사본을 사용하여 암호화된 데이터를 복원하므로 복구 프로세스가 간단하고 쉽습니다.




필요한 경우 데이터를 빠르게 검증하고, 분리하고, 분석하여 복구할 수 있도록 데이터를 온라인으로 다시 가져오는 더 빠른 방법을 제공해야 하는 경우입니다. FlexClone 에서 스냅 잠금 유형 옵션을 스냅 잠금이 아닌 유형으로 설정하면 이를 쉽게 달성할 수 있습니다.

ONTAP 9.13.1부터 SnapLock 볼트 관계의 대상 SnapLock 볼륨에 잠긴 스냅샷 복사본을 복원하려면 snaplock-type 옵션을 "non-snaplock"으로 설정하여 FlexClone 생성하면 됩니다. 볼륨 복제본 생성 작업을 실행할 때 스냅샷 복사본을 "부모 스냅샷"으로 지정합니다. SnapLock 유형으로 FlexClone 볼륨을 생성하는 방법에 대한 자세한 정보"여기."

사이버 보관소에서 복구 절차를 연습하면 사이버 보관소에 연결하고 데이터를 검색하기 위한 적절한 단계가 확립됩니다. 사이버 공격 발생 시 복구를 위해서는 절차를 계획하고 테스트하는 것이 필수적입니다.

## 추가 고려 사항

### ONTAP 기반 사이버 볼트를 설계하고 배포할 때는 추가로 고려해야 할 사항이 있습니다.

용량 크기 고려 사항

ONTAP 사이버 볼트 대상 볼륨에 필요한 디스크 공간의 양은 다양한 요소에 따라 달라지는데, 그 중 가장 중요한 요소는 소스 볼륨의 데이터 변경 속도입니다. 대상 볼륨의 백업 일정과 스냅샷 일정은 모두 대상 볼륨의 디스크 사용량에 영향을 미치며, 소스 볼륨의 변경 속도는 일정하지 않을 가능성이 높습니다. 최종 사용자나 애플리케이션 동작의 향후 변경 사항을 수용하는 데 필요한 것보다 더 많은 저장 용량을 버퍼로 제공하는 것이 좋습니다.

ONTAP 에서 1개월 동안 보존할 관계의 크기를 조정하려면 기본 데이터 세트의 크기, 데이터 변경률(일일 변경률), 중복 제거 및 압축 절감(해당되는 경우)을 포함한 여러 요소를 기반으로 저장 요구 사항을 계산해야 합니다.

단계별 접근 방식은 다음과 같습니다.

첫 번째 단계는 사이버 볼트로 보호하고 있는 소스 볼륨의 크기를 아는 것입니다. 이는 사이버 보관소 목적지에 처음 복제되는 기본 데이터 양입니다. 다음으로, 데이터 세트에 대한 일일 변화율을 추정합니다. 이는 매일 변경되는 데이터의 비율입니다. 데이터의 동적성을 잘 이해하는 것이 중요합니다.

예를 들어:

- 1차 데이터 세트 크기 = 5TB
- 일일 변화율 = 5% (0.05)
- 중복 제거 및 압축 효율성 = 50% (0.50)

이제 계산을 살펴보겠습니다.

- 일일 데이터 변경률을 계산합니다.

  ```
  Changed data per day = 5000 * 5% = 250GB
  ```

- 30일 동안 변경된 총 데이터를 계산합니다.

  ```
  Total changed data in 30 days = 250 GB * 30 = 7.5TB
  ```

- 필요한 총 저장 공간을 계산하세요.

  ```
  TOTAL = 5TB + 7.5TB = 12.5TB
  ```

- 중복 제거 및 압축 절감을 적용합니다.

  ```
  EFFECTIVE = 12.5TB * 50% = 6.25TB
  ```

저장 요구 사항 요약

- 효율성이 없다면 30일 치의 사이버 보관소 데이터를 저장하려면 *12.5TB*가 필요할 것입니다.
- 50% 효율성으로 보면 중복 제거 및 압축 후 *6.25TB*의 저장 공간이 필요합니다.

스냅샷 복사본에는 메타데이터로 인해 추가적인 오버헤드가 발생할 수 있지만, 일반적으로 이는 사소합니다.

하루에 여러 번 백업을 수행하는 경우 매일 수행되는 스냅샷 복사본 수에 따라 계산을 조정하세요.

시간 경과에 따른 데이터 증가를 고려하여 미래에도 대응할 수 있는 크기 조정을 보장합니다.

기본/소스에 대한 성능 영향

데이터 전송은 풀 작업이기 때문에 기본 저장소 성능에 미치는 영향은 작업 부하, 데이터 볼륨 및 백업 빈도에 따라 달라질 수 있습니다. 그러나 데이터 전송은 데이터 보호 및 백업 작업을 사이버 볼트 저장 시스템으로 오프로드하도록 설계되었기 때문에 기본 시스템에 미치는 전반적인 성능 영향은 일반적으로 적당하고 관리 가능합니다. 초기 관계 설정 및 첫 번째 전체 백업 중에 상당한 양의 데이터가 기본 시스템에서 사이버 볼트 시스템( SnapLock Compliance 볼륨 )으로 전송됩니다. 이로 인해 기본 시스템의 네트워크 트래픽과 I/O 부하가 증가할 수 있습니다. 최초의 전체 백업이 완료되면 ONTAP 마지막 백업 이후 변경된 블록만 추적하고 전송하면 됩니다. 이로 인해 초기 복제에 비해 I/O 부하가 훨씬 작아집니다. 증분 업데이트는 효율적이며 기본 저장소 성능에 미치는 영향이 최소화됩니다. 볼트 프로세스는 백그라운드에서 실행되므로 기본 시스템의 프로덕션 작업 부하를 방해할 가능성이 줄어듭니다.

- 스토리지 시스템에 추가적인 부하를 처리할 수 있는 충분한 리소스(CPU, 메모리, IOP)가 있는지 확인하면 성능에 미치는 영향을 완화할 수 있습니다.

## 구성, 분석, **Cron** 스크립트

NetApp 다음을 생성했습니다."다운로드 가능한 단일 스크립트" 사이버 볼트 관계를 구성, 검증, 일정을 예약하는 데 사용됩니다.

이 스크립트의 기능

- 클러스터 피어링
- SVM 피어링
- DP 볼륨 생성
- SnapMirror 관계 및 초기화
- 사이버 볼트에 사용되는 ONTAP 시스템 강화
- 이전 일정에 따라 관계를 중단하고 재개합니다.
- 보안 설정을 주기적으로 검증하고 이상 사항을 보여주는 보고서를 생성합니다.

이 스크립트를 사용하는 방법

"스크립트를 다운로드하세요"스크립트를 사용하려면 아래 단계를 따르세요.

- 관리자 권한으로 Windows PowerShell을 실행합니다.
- 스크립트가 포함된 디렉토리로 이동합니다.

- 스크립트를 사용하여 실행하세요 `.\` 필수 매개변수와 함께 구문

> 모든 정보를 입력했는지 확인하세요. 첫 번째 실행(구성 모드)에서는 프로덕션 시스템과 새로운 사이버 보관소 시스템 모두에 대한 자격 증명을 요청합니다. 그런 다음 시스템 간에 SVM 피어링(존재하지 않는 경우), 볼륨 및 SnapMirror 생성하고 초기화합니다.

> Cron 모드는 데이터 전송의 정지 및 재개를 예약하는 데 사용할 수 있습니다.

작동 모드

자동화 스크립트는 실행을 위한 3가지 모드를 제공합니다. `configure` , `analyze` 그리고 `cron` .

```
if($SCRIPT_MODE -eq "configure") {
        configure
    } elseif ($SCRIPT_MODE -eq "analyze") {
        analyze
    } elseif ($SCRIPT_MODE -eq "cron") {
        runCron
    }
```

- 구성 - 유효성 검사를 수행하고 시스템을 에어갭으로 구성합니다.
- 분석 - 모니터링 그룹에 이상 및 의심스러운 활동에 대한 정보를 전송하여 구성이 변경되지 않도록 보장하는 자동화된 모니터링 및 보고 기능입니다.
- Cron - 연결이 끊긴 인프라를 활성화하기 위해 Cron 모드는 LIF를 자동으로 비활성화하고 전송 관계를 중지합니다.

선택한 볼륨의 데이터를 전송하는 데는 시스템 성능과 데이터 양에 따라 시간이 걸립니다.

```
./script.ps1 -SOURCE_ONTAP_CLUSTER_MGMT_IP "172.21.166.157"
-SOURCE_ONTAP_CLUSTER_NAME "NTAP915_Src" -SOURCE_VSERVER "svm_NFS"
-SOURCE_VOLUME_NAME "Src_RP_Vol01" -DESTINATION_ONTAP_CLUSTER_MGMT_IP
"172.21.166.159" -DESTINATION_ONTAP_CLUSTER_NAME "NTAP915_Destn"
-DESTINATION_VSERVER "svm_nim_nfs" -DESTINATION_AGGREGATE_NAME
"NTAP915_Destn_01_VM_DISK_1" -DESTINATION_VOLUME_NAME "Dst_RP_Vol01_Vault"
-DESTINATION_VOLUME_SIZE "5g" -SNAPLOCK_MIN_RETENTION "15minutes"
-SNAPLOCK_MAX_RETENTION "30minutes" -SNAPMIRROR_PROTECTION_POLICY
"XDPDefault" -SNAPMIRROR_SCHEDULE "5min" -DESTINATION_CLUSTER_USERNAME
"admin" -DESTINATION_CLUSTER_PASSWORD "PASSWORD123"
```

## ONTAP 사이버 볼트 PowerShell 솔루션 결론

ONTAP 이 제공하는 강력한 강화 방법론을 갖춘 에어 갭을 활용함으로써 NetApp 진화하는 사이버 위협에 탄력적으로 대응할 수 있는 안전하고 격리된 스토리지 환경을 구축할 수 있도록 지원합니다. 이 모든 작업은 기존 스토리지 인프라의 민첩성과 효율성을 유지하면서 수행됩니다.

## 이러한 보안 액세스를 통해 회사는 기존 인력, 프로세스 및 기술 프레임워크를 최소한으로 변경하면서 엄격한 안전 및 가동 시간 목표를 달성할 수 있습니다.

ONTAP 사이버 볼트는 ONTAP 의 기본 기능을 사용하여 데이터의 변경 불가능하고 지울 수 없는 복사본을 만들어 추가적인 보호를 제공하는 간편한 방법입니다. 전반적인 보안 태세에 NetApp의 ONTAP 기반 사이버 볼트를 추가하면 다음과 같은 이점이 있습니다.

- 운영 및 백업 네트워크와 분리되어 연결이 끊어진 환경을 만들고 해당 환경에 대한 사용자 액세스를 제한합니다.

## 저작권 정보



## 상표 정보