랜섬웨어 공격을 방어하십시오

ASA r2

NetApp
February 11, 2026

목차

랜섬웨어 공격을 방어하십시오

ASA r2 스토리지 시스템에 대한 랜섬웨어 공격으로부터 보호하기 위해 변조 방지 스냅샷을 생성합니다.

랜섬웨어 공격에 대한 보호를 강화하기 위해 스냅샷을 원격 클러스터에 복제하고 대상 스냅샷을 잠가 변조 방지를 보장합니다. 잠긴 스냅샷은 실수로 또는 악의적으로 삭제할 수 없습니다. 스토리지 유닛이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수 있습니다.

SnapLock Compliance 클록을 초기화한다

무단 변경 방지 스냅샷을 생성하려면 로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화해야 합니다.

단계

1. 클러스터 > 개요 * 를 선택합니다.
2. 노드 * 섹션에서 * SnapLock Compliance 시계 초기화 * 를 선택합니다.
3. Initialize * 를 선택합니다.
4. 규정 준수 클록이 초기화되었는지 확인
   a. 클러스터 > 개요 * 를 선택합니다.
   b. Nodes * 섹션에서 를 선택한 다음 * SnapLock Compliance Clock * 을 선택합니다.

다음 단계

로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화한 후에는 을(를) 시작할 "잠긴 스냅샷이 있는 복제 관계를 생성합니다"수 있습니다.

ASA r2 스토리지 시스템에서 AI를 사용하여 자율적인 랜섬웨어 보호 기능을 활성화하세요.

ONTAP 9.17.1부터 인공지능(AI)을 활용한 자율형 랜섬웨어 보호(ARP/AI)를 사용하여 ASA r2 시스템의 데이터를 보호할 수 있습니다. ARP/AI는 잠재적인 랜섬웨어 위협을 신속하게 감지하고, 데이터를 보호하기 위해 ARP 스냅샷을 자동으로 생성하며, 의심스러운 활동을 감지하면 시스템 관리자에 경고 메시지를 표시합니다.

ARP는 머신러닝 모델을 활용한 랜섬웨어 분석 기능을 통해 사이버 복원력을 향상시킵니다. 이 모델은 SAN 환경에서 98%의 정확도로 끊임없이 진화하는 랜섬웨어를 탐지합니다. ARP의 머신러닝 모델은 모의 랜섬웨어 공격 전후의 대규모 파일 데이터셋을 기반으로 사전 학습됩니다. 이러한 리소스 집약적인 학습은 ONTAP 외부에서 수행되며, 학습된 모델은 ONTAP에 포함되어 제공됩니다. 이 모델은 접근하거나 수정할 수 없습니다. ARP/AI는 활성화 즉시 작동하며, "학습 기간"가 필요하지 않습니다.

> 어떤 랜섬웨어 탐지 또는 예방 시스템도 랜섬웨어 공격으로부터 완벽한 안전을 보장할 수는 없습니다. 공격이 탐지되지 않을 수도 있지만, ARP/AI는 안티바이러스 소프트웨어가 침입을 탐지하지 못할 경우 중요한 추가 방어 계층 역할을 합니다.

이 작업에 대해

- ARP/AI 지원이 포함되어 있습니다. "ONTAP One 라이센스" .
- ARP/AI는 SnapMirror 액티브 동기화, SnapMirror 동기식 또는 SnapLock으로 보호되는 스토리지 유닛에서 지원되지 않습니다.
- ONTAP 9.18.1부터는 ONTAP 9.18.1로 업그레이드하거나 새로운 ONTAP 9.18.1 ASA r2 클러스터를 초기화한 후 12시간이 지나면 새로 생성되는 모든 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다.
- ARP/AI를 활성화한 후에는 다음을 수행해야 합니다. "보안 파일에 대한 자동 업데이트를 활성화하세요" 자동으로 새로운 보안 업데이트를 받습니다.

클러스터의 모든 스토리지 유닛에서 **ARP/AI** 활성화

ONTAP 9.17.1을 실행 중인 경우 클러스터에 생성된 모든 스토리지 유닛에 대해 기본적으로 ARP/AI를 활성화할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 랜섬웨어 방지 옆에서 ⋮를 선택한 다음 *기존의 모든 스토리지 유닛에서 활성화*를 선택합니다.
3. *활성화*를 선택하세요.

스토리지 **VM**의 모든 스토리지 장치에서 **ARP/AI**를 활성화합니다.

ONTAP 9.17.1을 실행 중인 경우 스토리지 가상 머신(VM)에 생성된 모든 스토리지 유닛에 대해 기본적으로 ARP/AI를 활성화할 수 있습니다. 즉, 스토리지 VM에 새로 생성되는 모든 스토리지 유닛에는 ARP/AI가 자동으로 활성화됩니다. 또한 스토리지 VM에 있는 기존 스토리지 유닛에도 ARP/AI를 적용할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. 시스템 관리자에서 *클러스터 > 스토리지 VM*을 선택합니다.
2. ARP/AI를 활성화할 스토리지 VM을 선택합니다.
3. 보안 섹션에서 랜섬웨어 방지 옆을 선택하세요. ⋮ ; 그런 다음 *랜섬웨어 방지 설정 편집*을 선택합니다.
4. *랜섬웨어 방지 기능 활성화*를 선택하세요.

   이렇게 하면 기본적으로 선택된 스토리지 VM에서 생성되는 모든 향후 스토리지 유닛에서 ARP/AI가 활성화됩니다.

5. 선택한 스토리지 VM의 기존 스토리지 장치에 ARP를 적용하려면 *이 스토리지 VM의 모든 해당 기존 스토리지 장치에 이 변경 사항 적용*을 선택합니다.
6. 저장 * 을 선택합니다.

결과

스토리지 VM에서 생성하는 모든 새 스토리지 유닛은 기본적으로 랜섬웨어 공격으로부터 보호되며, 의심스러운 활동은 System Manager에서 보고됩니다.

스토리지 VM의 특정 스토리지 장치에 대해 ARP/AI를 활성화합니다.

ONTAP 9.17.1을 실행 중이고 스토리지 VM의 모든 스토리지 유닛에서 ARP/AI를 활성화하지 않으려면 활성화할 특정 유닛을 선택할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. ARP/AI를 활성화할 저장 장치를 선택하세요.
3. 선택하다 ⋮ ; 그런 다음 *랜섬웨어 방지 기능 사용*을 선택합니다.
4. *활성화*를 선택하세요.

결과

선택한 저장 장치는 랜섬웨어 공격으로부터 보호되며, 의심스러운 활동은 시스템 관리자에 보고됩니다.

ASA r2 스토리지 시스템에서 기본 자율형 랜섬웨어 보호 기능을 비활성화하십시오.

새로운 ONTAP 9.18.1 ASA r2 클러스터를 초기화하거나 클러스터를 ONTAP 9.18.1로 업그레이드하면 12시간의 유예 기간 후 모든 새 스토리지 장치에서 ARP/AI가 기본적으로 자동으로 활성화됩니다. 유예 기간 동안 ARP/AI를 비활성화하지 않으면 유예 기간이 종료될 때 새 스토리지 장치에 대해 클러스터 전체에서 활성화됩니다.

ONTAP 9.17.1에서 생성된 스토리지 장치는 ARP/AI용 "수동으로 활성화됨"이어야 합니다.

단계

최초 12시간의 유예 기간 동안 또는 그 이후에 기본 활성화를 비활성화할 수 있습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. ARP 비활성화:
   - 12시간 유예 기간 동안 비활성화하려면:
     i. **Anti-ransomware** 항목에서 *Don't enable*을 선택한 다음 *Disable*을 선택하십시오.
   - 12시간 유예 기간 후 비활성화하려면:
     i. 랜섬웨어 방지 항목에서 를 선택한 다음 *새 저장 장치에 대해 활성화*를 선택 해제합니다.
     ii. *저장*을 선택합니다

CLI

1. 기본 활성화 상태를 확인합니다.

```
security anti-ransomware auto-enable show
```

2. 기존 볼륨 및 새 볼륨에 대한 기본 활성화를 비활성화합니다.

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

ASA r2 스토리지 시스템에서 ARP/AI 스냅샷 보존 기간 수정

인공지능(ARP/AI)을 활용한 자율 랜섬웨어 보호 기능이 ASA r2 시스템 스토리지 유닛 하나 이상에서 비정상적인 활동을 감지하면 자동으로 ARP 스냅샷을 생성하여 스토리지 유닛의 데이터를 보호합니다. 스토리지 용량 및 비즈니스 데이터 요구 사항에 따라 기본 ARP 스냅샷 보존 기간을 늘리거나 줄일 수 있습니다. 예를 들어, 비즈니스 크리티컬 애플리케이션의 보존 기간을 늘려 필요한 경우 데이터 복구를 위한 보존 기간을 늘리거나, 비핵심 애플리케이션의 보존 기간을 줄여 스토리지 공간을 절약할 수 있습니다.

ARP 스냅샷의 기본 보존 기간은 비정상적인 활동에 대한 대응 조치에 따라 달라집니다.

만약 당신이 이 작업을 수행한다면...	**ARP** 스냅샷은 기본적으로 다음 항목에 대해 보관됩니다.
거짓 양성으로 표시	12시간
잠재적인 랜섬웨어 공격으로 표시	7일
즉각적인 조치를 취하지 마십시오	10일

기본 보존 기간은 ONTAP 명령줄 인터페이스(CLI)를 사용하여 수정할 수 있습니다 . "ONTAP 자동 스냅샷에 대한 옵션 수정" 기본 보존 기간을 변경하는 단계는 다음과 같습니다.

ASA r2 스토리지 시스템에서 AI 알림을 통해 자율적인 랜섬웨어 보호에 대응

인공지능(ARP/AI)을 활용한 자율 랜섬웨어 보호 기능이 ASA r2 시스템 스토리지 유닛 하나 이상에서 비정상적인 활동을 감지하면 시스템 관리자 대시보드에 경고가 생성됩니다. 경고를 확인하고 활동을 확인한 후, 필요한 경우 데이터에 대한 잠재적 위협을 차단하기 위한 조치를 취해야 합니다.

ARP/AI 경고 메시지가 표시되면 조치를 취하기 전에 적절한 애플리케이션 무결성 검사기를 사용하여 스토리지 유닛의 데이터 무결성을 확인해야 합니다. 스토리지 유닛의 데이터 무결성을 확인하면 해당 활동이 허용 가능한 수준인지 아니면 잠재적인 랜섬웨어 공격인지 판단하는 데 도움이 됩니다.

비정상적인 활동이 발생하면...	그러면 이렇게 하세요...
허용 가능	해당 활동을 거짓 양성으로 표시합니다.
잠재적인 랜섬웨어 공격	해당 활동을 랜섬웨어 공격의 가능성이 있는 활동으로 표시합니다.
불확정	즉각적인 조치를 취하지 마십시오. 최대 7일 동안 저장 장치를 모니터링하십시오. 저장 장치가 계속 정상적으로 작동하면 해당 활동을 오탐(false positive)으로 표시하십시오. 저장 장치에서 비정상적인 활동이 계속 나타나면 해당 활동을 잠재적인 랜섬웨어 공격으로 표시하십시오.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.

   ARP가 하나 이상의 저장 장치에서 비정상적인 활동을 감지하면 경고 아래에 메시지가 나타납니다.

2. 경고 메시지를 선택하세요.
3. 이벤트 개요*에서 비정상적인 활동이 있는 저장 장치 수를 나타내는 *경고 메시지를 선택합니다.
4. *비정상적인 활동이 있는 보관 장치*에서 보관 장치를 선택하세요.
5. *보안*을 선택하세요.

   저장 장치에 비정상적인 활동이 있는 경우 랜섬웨어 방지 아래에 메시지가 표시됩니다.

6. *작업 선택*을 선택하세요.
7. *거짓 양성으로 표시*를 선택하거나 *잠재적 랜섬웨어 공격으로 표시*를 선택합니다.

다음 단계

스토리지 유닛 활동의 급증(일회성 급증이든 새로운 정상 상태의 특징인 급증이든)을 알고 있다면 안전하다고 보고해야 합니다. 이러한 급증을 수동으로 안전하다고 보고하면 ARP의 위협 평가 정확도를 높이는 데 도움이 됩니다. "알려진 ARP/AI 급증 보고" 방법을 알아보십시오.

ASA r2 스토리지 시스템에서 AI를 사용하여 자율 랜섬웨어 보호를 일시 중지하거나 재개하세요.

ONTAP 9.17.1부터 인공지능(ARP/AI)을 활용한 자율형 랜섬웨어 보호 기능을 사용하여 ASA r2 시스템의 데이터를 보호할 수 있습니다. 비정상적인 워크로드 이벤트를 계획하는 경우, 랜섬웨어 공격의 오탐지를 방지하기 위해 ARP/AI 분석을 일시적으로 중단할 수 있습니다. 워크로드 이벤트가 완료되면 ARP/AI 분석을 재개할 수 있습니다.

ARP/AI 일시 중지

비정상적인 작업 부하 이벤트를 시작하기 전에 랜섬웨어 공격에 대한 오탐지 방지를 위해 ARP/AI 분석을 일시적으로 중단해야 할 수도 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. ARP/AI를 일시 중지할 저장 장치를 선택하세요.
3. *랜섬웨어 방지 일시 중지*를 선택하세요.

결과

선택한 저장 장치에 대한 ARP/AI 분석이 일시 중지되고, ARP/AI를 재개할 때까지 시스템 관리자에 의심스러운 활동이 보고되지 않습니다.

ARP/AI 재개

비정상적인 작업 부하 중에 ARP/AI를 일시 중지한 경우, 작업이 완료된 후 다시 시작하여 랜섬웨어 공격으로부터 데이터를 보호해야 합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. ARP/AI를 재개할 저장 장치를 선택하세요.
3. *랜섬웨어 방지 재개*를 선택하세요.

결과

잠재적인 랜섬웨어 공격에 대한 분석이 재개되고, 의심스러운 활동이 시스템 관리자에게 보고됩니다.