



자율 랜섬웨어 보호

ONTAP 9

NetApp
August 31, 2024

목차

자율 랜섬웨어 보호	1
자율 랜섬웨어 보호 개요	1
자율 랜섬웨어 보호 사용 사례 및 고려사항	3
자율주행 랜섬웨어 보호 활성화	7
새로운 볼륨에서 자율 랜섬웨어 보호를 기본적으로 활성화하십시오	9
Autonomous 랜섬웨어 Protection을 일시 중지하여 워크로드 이벤트를 분석에서 제외합니다	11
자율적 랜섬웨어 방어 공격 감지 매개 변수를 관리합니다	12
비정상적인 활동에 응답합니다	17
랜섬웨어 공격 후 데이터 복원	20
자동 스냅샷 복사본에 대한 옵션을 수정합니다	23

자율 랜섬웨어 보호

자율 랜섬웨어 보호 개요

ONTAP 9.10.1부터 ARP(Autonomous 랜섬웨어 보호) 기능은 NAS(NFS 및 SMB) 환경에서 워크로드 분석을 사용하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하여 경고합니다.

공격이 의심되면 ARP는 예약된 Snapshot 복제본으로부터 기존 보호 기능 외에 새 Snapshot 복제본도 생성합니다.

라이선스 및 지원

ARP에는 라이선스가 필요합니다. ARP는 에서 사용할 수 있습니다 ["ONTAP One 라이선스"](#). ONTAP One 라이선스가 없는 경우 ONTAP 버전에 따라 다른 ARP를 사용할 수 있습니다.

ONTAP 릴리스	라이선스
ONTAP 9.11.1 이상	안티 랜섬웨어
ONTAP 9.10.1	Mt_EK_MGMT(멀티 테넌트 키 관리)

- ONTAP 9.11.1 이상으로 업그레이드하고 ARP가 이미 시스템에 구성되어 있는 경우, 새로운 Anti-랜섬웨어 라이선스를 구입할 필요가 없습니다. 새 ARP 구성의 경우 새 라이선스가 필요합니다.
- ONTAP 9.11.1 이상에서 ONTAP 9.10.1로 되돌려지는 경우, 안티랜섬웨어 라이선스로 ARP를 활성화한 경우 경고 메시지가 표시되고 ARP를 다시 구성해야 할 수 있습니다. ["ARP를 되돌리는 방법에 대해 알아보십시오"](#).

System Manager 또는 ONTAP CLI를 사용하여 볼륨별로 ARP를 구성할 수 있습니다.

ONTAP 랜섬웨어 보호 전략

효과적인 랜섬웨어 탐지 전략에는 단일 이상의 보호 계층이 포함되어야 합니다.

예를 들어, 차량의 안전 기능을 들 수 있습니다. 안전 벨트와 같은 단일 기능에 의존하여 사고 시 사용자를 완전히 보호하지 않습니다. 에어백, 안티 브레이크 및 전방 충돌 경고는 모두 추가적인 안전 기능으로 훨씬 더 나은 결과를 제공합니다. 랜섬웨어 보호는 동일한 방법으로 확인해야 합니다.

ONTAP에는 FPolicy, Snapshot 복사본, SnapLock, Active IQ 디지털 자문과 같은 기능이 포함되어 랜섬웨어로부터 보호하지만, 다음 정보는 머신 러닝 기능이 있는 ARP 기본 기능에 초점을 맞춥니다.

ONTAP의 다른 안티 랜섬웨어 기능에 대한 자세한 내용은 를 참조하십시오 ["Ransomware 및 NetApp의 보호 포트폴리오"](#).

ARP가 감지하는 것

ARP는 공격자가 몸값을 지불하기 전까지 데이터를 보유하는 서비스 거부 공격으로부터 보호하도록 설계되었습니다. ARP는 다음을 기반으로 실시간 랜섬웨어 탐지를 제공합니다.

- 들어오는 데이터를 암호화된 데이터 또는 일반 텍스트로 식별합니다.
- 탐지 분석
 - 엔트로피: 파일의 데이터 임의 정도 평가
 - 파일 확장명 형식: 일반 확장명 형식에 맞지 않는 확장자입니다
 - 파일 **IOPS**: 데이터 암호화(ONTAP 9.11.1부터 시작)로 인해 비정상적인 볼륨 활동이 급증함

ARP는 적은 수의 파일만 암호화한 후 대부분의 랜섬웨어 공격의 확산을 감지하고 자동으로 조치를 취하여 데이터를 보호하고 의심스러운 공격이 발생하고 있음을 사용자에게 알릴 수 있습니다.



랜섬웨어 탐지 또는 방지 시스템이 랜섬웨어 공격에서 안전을 완벽하게 보장할 수는 없습니다. 공격이 탐지되지 않을 수도 있지만, 안티바이러스 소프트웨어가 침입에 대한 감지에 실패한 경우 ARP는 중요한 추가 방어 계층으로 작용합니다.

학습 및 활성화 모드

ARP에는 두 가지 모드가 있습니다.

- * 학습 * (또는 "드라이 런" 모드)
- * 활성화 * (또는 "활성화" 모드)

ARP를 활성화하면 `_learning mode_`에서 실행됩니다. 학습 모드에서 ONTAP 시스템은 엔트로피, 파일 확장자 유형 및 파일 IOPS와 같은 분석 영역을 기반으로 경고 프로필을 개발합니다. 학습 모드에서 충분한 시간 동안 ARP를 실행하여 워크로드 특성을 평가한 후 활성화 모드로 전환하고 데이터 보호를 시작할 수 있습니다. ARP가 활성화 모드로 전환되면 ONTAP는 위협이 감지될 경우 데이터를 보호하기 위해 ARP 스냅샷 복사본을 생성합니다.

30일 동안 ARP를 학습 모드로 두는 것이 좋습니다. ONTAP 9.13.1 부터 ARP는 최적의 학습 기간을 자동으로 결정하고 30일 이전에 발생할 수 있는 스위치를 자동화합니다.

활성 모드에서 파일 확장자가 비정상적으로 플래그되는 경우 경고를 평가해야 합니다. 경고를 통해 데이터를 보호하거나 경고를 거짓 긍정으로 표시할 수 있습니다. 경고를 `false positive`로 표시하면 경고 프로필이 업데이트됩니다. 예를 들어, 새 파일 확장자에 의해 경고가 트리거되고 이 경고를 `false positive`로 표시하면 다음에 파일 확장명이 관찰될 때 알림이 수신되지 않습니다. 명령을 입력합니다 `security anti-ransomware volume workload-behavior show` 볼륨에서 감지된 파일 확장자를 표시합니다. (학습 모드 초기에 이 명령을 실행하고 파일 유형을 정확하게 표시한다면 ONTAP에서 다른 메트릭을 계속 수집하므로 해당 데이터를 액티브 모드로 이동하기 위한 기반으로 사용해서는 안 됩니다.)

ONTAP 9.11.1부터 ARP에 대한 검출 파라미터를 사용자 정의할 수 있다. 자세한 내용은 을 참조하십시오 [ARP 공격 탐지 매개변수를 관리합니다.](#)

위협 평가 및 **ARP** 스냅샷 사본

활성 모드에서 ARP는 학습된 분석에 대해 측정된 수신 데이터를 기반으로 위협 가능성을 평가합니다. ARP가 위협을 탐지할 때 측정이 할당됩니다.

- 낮음: 볼륨에서 비정상 상태를 가장 빨리 감지합니다(예: 볼륨에서 새 파일 확장자가 관찰됨).
- 보통: 파일 확장자가 표시되지 않은 동일한 여러 개의 파일이 관찰됩니다.
 - ONTAP 9.10.1에서 Moderate로 에스컬레이션하기 위한 임계값은 100개 이상의 파일입니다. ONTAP 9.11.1부터 파일 수량은 수정할 수 있으며 기본값은 20입니다.

위협이 낮은 상황에서 ONTAP는 비정상성을 감지하고 볼륨의 스냅샷 복사본을 생성하여 최상의 복구 지점을 생성합니다. ONTAP는 ARP 스냅샷 복사본의 이름을 로 접두어 붙입니다 Anti-ransomware-backup 예를 들어 쉽게 식별할 수 있도록 합니다 Anti_ransomware_backup.2022-12-20_1248.

ONTAP에서 분석 보고서를 실행하고 비정상 상태가 랜섬웨어 프로필과 일치하는지 확인하는 위협이 보통 수준으로 증가합니다. 하위 수준에 남아 있는 위협은 System Manager의 이벤트 섹션에 기록되고 표시됩니다. 공격 가능성이 보통이면 ONTAP에서 위협을 평가하라는 EMS 알림을 생성합니다. ONTAP는 낮은 위협에 대한 경고를 보내지 않지만 ONTAP 9.14.1부터 시작할 수 있습니다 [알림 설정을 수정합니다](#). 자세한 내용은 [을 참조하십시오 비정상적인 활동에 응답합니다](#).

System Manager의 이벤트 섹션 또는 에서 수준에 관계없이 위협에 대한 정보를 볼 수 있습니다 security anti-ransomware volume show 명령.

ARP 스냅샷 복사본은 최소 2일 동안 보존됩니다. ONTAP 9.11.1부터 보존 설정을 수정할 수 있습니다. 자세한 내용은 [을 참조하십시오 스냅샷 복사본에 대한 옵션을 수정합니다](#).

랜섬웨어 공격 후 ONTAP에서 데이터를 복구하는 방법

공격이 의심되면 해당 시점에 시스템에서 볼륨 Snapshot 복사본을 생성한 후 해당 복사본을 잠급니다. 나중에 공격이 확인되면 ARP 스냅샷 복사본을 사용하여 볼륨을 복원할 수 있습니다.

잠긴 스냅샷 복사본은 일반적인 방법으로 삭제할 수 없습니다. 그러나 나중에 이 공격을 가양성 공격으로 표시하기로 결정하면 잠긴 복사본이 삭제됩니다.

영향을 받는 파일과 공격 시간을 알 수 있으므로 전체 볼륨을 스냅샷 복사본 중 하나로 되돌리는 것이 아니라 다양한 Snapshot 복사본에서 영향을 받는 파일을 선택적으로 복구할 수 있습니다.

ARP는 검증된 ONTAP 데이터 보호 및 재해 복구 기술을 기반으로 구축되며, 랜섬웨어 공격에 대응합니다. 데이터 복구에 대한 자세한 내용은 다음 항목을 참조하십시오.

- ["Snapshot 복사본에서 복구\(System Manager\)"](#)
- ["스냅샷 복사본에서 파일 복원\(CLI\)"](#)
- ["스마트 랜섬웨어 복구"](#)

자율 랜섬웨어 보호 사용 사례 및 고려사항

ARP(Autonomous Ransomware Protection)는 ONTAP 9.10.1부터 NAS 워크로드에 사용할 수 있습니다. ARP를 배포하기 전에 권장되는 용도 및 지원되는 구성뿐만 아니라 성능에 미치는 영향을 알고 있어야 합니다.

지원 구성 및 지원되지 않는 구성

ARP를 사용하도록 결정할 때 볼륨의 워크로드가 ARP에 적합하고 필요한 시스템 구성을 충족하는지 확인하는 것이 중요합니다.

적합한 워크로드

ARP는 다음과 같은 경우에 적합합니다.

- 데이터베이스를 NFS 스토리지에 저장합니다

- Windows 또는 Linux 홈 디렉토리

사용자가 학습 기간 동안 발견되지 않은 확장자를 가진 파일을 만들 수 있기 때문에 이 작업 부하에서 오탐이 발생할 가능성이 높습니다.

- 이미지 및 비디오

예: 의료 기록 및 전자 설계 자동화(EDA) 데이터

부적합한 워크로드

ARP는 다음에 적합하지 않습니다.

- 파일 생성 또는 삭제 빈도가 높은 워크로드(몇 초 안에 수십만 개의 파일(예: 테스트/개발 워크로드))
- ARP의 위협 감지는 파일 생성, 이름 변경 또는 삭제 작업에서 비정상적인 급증을 인식하는 능력에 따라 달라집니다. 애플리케이션 자체가 파일 활동의 소스인 경우 랜섬웨어 활동과 효과적으로 구별될 수는 없습니다.
- 애플리케이션 또는 호스트가 데이터를 암호화하는 워크로드
ARP는 수신 데이터를 암호화 또는 암호화되지 않은 상태로 구별하는 것에 의존합니다. 애플리케이션 자체에서 데이터를 암호화하면 기능의 효율성이 감소합니다. 그러나 이 기능은 파일 작업(삭제, 덮어쓰기, 생성 또는 새 파일 확장명으로 생성 또는 이름 바꾸기)과 파일 유형에 따라 계속 작동할 수 있습니다.

지원되는 구성

ARP는 ONTAP 9.10.1부터 온-프레미스 ONTAP 시스템의 NFS 및 SMB 볼륨에 대해 사용할 수 있습니다.

다른 구성 및 볼륨 유형에 대한 지원은 다음 ONTAP 버전에서 제공됩니다.

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
비동기식 SnapMirror로 보호되는 볼륨	✓	✓	✓	✓		
비동기식 SnapMirror(SVM 재해 복구)로 SVM 보호	✓	✓	✓	✓		
SVM 데이터 이동성 (vserver migrate)	✓	✓	✓	✓		
FlexGroup 볼륨	✓	✓	✓			
다중 관리 검증	✓	✓	✓			

SnapMirror 및 ARP 상호 운용성

ONTAP 9.12.1부터 비동기식 SnapMirror 대상 볼륨에서 ARP가 지원됩니다. ARP는 ** SnapMirror Synchronous에서 지원되지 않습니다.

SnapMirror 소스 볼륨이 ARP가 활성화된 경우 SnapMirror 대상 볼륨은 자동으로 ARP 구성 상태(학습, 활성화 등), ARP 교육 데이터 및 소스 볼륨의 ARP 생성 스냅샷을 가져옵니다. 명시적 활성화가 필요하지 않습니다.

대상 볼륨이 읽기 전용(RO) 스냅샷 복사본으로 구성되어 있지만, 해당 데이터에 대한 ARP 처리는 수행되지 않습니다. 그러나 SnapMirror 대상 볼륨이 읽기-쓰기(RW)로 변환되면 ARP는 RW로 변환된 대상 볼륨에서 자동으로 활성화됩니다. 대상 볼륨에는 소스 볼륨에 이미 기록된 내용 외에 추가 학습 절차가 필요하지 않습니다.

ONTAP 9.10.1 및 9.11.1에서 SnapMirror는 ARP 구성 상태, 훈련 데이터 및 Snapshot 복사본을 소스에서 타겟 볼륨으로 전송하지 않습니다. 따라서 SnapMirror 대상 볼륨이 RW로 변환될 때 대상 볼륨의 ARP는 변환 후 학습 모드에서 명시적으로 활성화되어야 합니다.

ARP 및 가상 머신

ARP는 가상 머신(VM)에서 지원됩니다. ARP 감지는 VM 내부 및 외부의 변경에 대해 다르게 동작합니다. ARP는 VM 내부에 높은 엔트로피 파일이 있는 워크로드에 권장되지 않습니다.

VM 외부의 변경 사항

ARP는 새 확장자가 암호화된 볼륨에 들어갔거나 파일 확장자가 변경되는 경우 VM 외부의 NFS 볼륨에서 파일 확장자 변경을 감지할 수 있습니다. 감지 가능한 파일 확장자 변경 사항은 다음과 같습니다.

- .vmx입니다
- .vmxf입니다
- vmdk입니다
- - 평면.vmdk
- NVRAM을 입력합니다
- vmem입니다
- .vmsd입니다
- .vmsn입니다
- .vswp 를 참조하십시오
- .VMSS를 참조하십시오
- 로그
- -\#.log

VM 내부의 변경 사항

랜섬웨어 공격이 VM을 대상으로 하고 VM 외부의 변경 없이 VM 내부의 파일이 변경되는 경우 ARP는 VM의 기본 엔트로피가 낮을 경우(예: .txt, .docx 또는 .mp4 파일) 위협을 감지합니다. ARP는 이 시나리오에서 보호 스냅샷을 생성하지만 VM 외부의 파일 확장자가 변조되지 않았기 때문에 위협 경고를 생성하지 않습니다.

기본적으로 파일이 높은 엔트로피(예: .gzip 또는 암호로 보호된 파일)인 경우 ARP의 검색 기능이 제한됩니다. ARP는 이 경우에도 사전 예방적 스냅샷을 가져올 수 있지만, 파일 확장자가 외부에서 변경되지 않은 경우에는 알림이 발생하지 않습니다.

지원되지 않는 구성입니다

ARP는 다음 시스템 구성에서 지원되지 않습니다.

- ONTAP S3 환경
- 알아보십시오

ARP는 다음 볼륨 구성을 지원하지 않습니다.

- FlexGroup 볼륨(ONTAP 9.10.1 ~ 9.12.1의 경우. ONTAP 9.13.1부터 FlexGroup 볼륨이 지원됨)
- FlexCache 볼륨(ARP는 오리진 FlexVol 볼륨에서 지원되지만 캐시 볼륨에서는 지원되지 않음)
- 오프라인 볼륨
- SAN 전용 볼륨
- SnapLock 볼륨
- SnapMirror Synchronous
- 비동기 SnapMirror(ONTAP 9.10.1 및 9.11.1에서만 지원되지 않습니다. 비동기 SnapMirror는 ONTAP 9.12.1부터 지원됩니다. 자세한 내용은 을 참조하십시오 [\[snapmirror\]](#)참조)
- 제한된 볼륨
- 스토리지 VM의 루트 볼륨입니다
- 중지된 스토리지 VM의 볼륨입니다

ARP 성능 및 주파수 고려 사항

ARP는 처리량 및 피크 IOPS로 측정된 시스템 성능에 최소한의 영향을 줄 수 있습니다. ARP 기능의 영향은 특정 볼륨 작업 부하에 따라 달라집니다. 일반적인 워크로드의 경우 다음과 같은 구성 제한이 권장됩니다.

워크로드 특성	노드당 권장 볼륨 제한입니다	노드당 볼륨 제한을 초과할 경우 성능 저하: [*]
읽기 집약적 또는 데이터를 압축할 수 있습니다.	150	최대 IOPS의 4%
쓰기 집약적이고 데이터를 압축할 수 없습니다.	60	최대 IOPS의 10%

통과: [*] 권장 한도를 초과하여 추가된 볼륨의 수에 관계없이 시스템 성능이 이 비율을 초과하여 저하되지 않습니다.

ARP 분석은 우선 순위가 지정된 순서대로 실행되므로 보호된 볼륨의 수가 증가할수록 각 볼륨에서 분석 실행 빈도가 줄어듭니다.

ARP로 보호되는 볼륨을 사용한 다중 관리자 검증

ONTAP 9.13.1 부터는 ARP를 통한 추가 보안을 위해 MAV(Multi-admin verification)를 활성화할 수 있습니다. MAV를 사용하면 최소한 두 명 이상의 인증된 관리자가 ARP를 끄거나 ARP를 일시 중지하거나 의심스러운 공격을 보호된 볼륨에서 위양성(false positive)으로 표시해야 합니다. 자세한 내용을 알아보십시오 ["ARP 보호 볼륨에 대해 MAV를 활성화합니다"](#).

MAV 그룹에 대한 관리자를 정의하고 에 대한 MAV 규칙을 만들어야 합니다 `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, 및 `security anti-ransomware volume attack clear-suspect` 보호할 ARP 명령. MAV 그룹의 각 관리자는 각각의 새 규칙 요청 및 을 승인해야 합니다 ["MAV 규칙을 다시 추가합니다"](#) MAV 설정 내.

ONTAP 9.14.1부터 ARP는 ARP 스냅샷 생성 및 새 파일 확장자 관찰에 대한 경고를 제공합니다. 이러한 이벤트에 대한 알림은 기본적으로 해제되어 있습니다. 경고는 볼륨 또는 SVM 레벨에서 설정할 수 있습니다. 을 사용하여 SVM 레벨에서 MAV 규칙을 생성할 수 있습니다 security anti-ransomware vserver event-log modify 를 볼륨 레벨에서 사용할 수 있습니다 security anti-ransomware volume event-log modify.

다음 단계

- ["자율주행 랜섬웨어 보호 활성화"](#)
- ["ARP로 보호되는 볼륨에 대해 MAV를 활성화합니다"](#)

자율주행 랜섬웨어 보호 활성화

ONTAP 9.10.1.1부터 ARP(Autonomous 랜섬웨어Protection)는 새 볼륨이나 기존 볼륨에서 활성화할 수 있습니다. 먼저 학습 모드에서 ARP를 활성화하는데, 이 모드에서 시스템은 정상적인 동작을 특성화하기 위해 워크로드를 분석합니다. 기존 볼륨에서 ARP를 활성화하거나, 새 볼륨을 생성하고 ARP를 처음부터 활성화할 수 있습니다.

이 작업에 대해

ARP는 항상 먼저 학습(또는 건식 실행) 모드에서 활성화해야 합니다. 활성 모드에서 시작하면 과도한 거짓 양성 보고서가 발생할 수 있습니다.

최소 30일 동안 ARP를 학습 모드로 실행하는 것이 좋습니다. ONTAP 9.13.1 부터 ARP는 최적의 학습 기간을 자동으로 결정하고 30일 이전에 발생할 수 있는 스위치를 자동화합니다. 자세한 내용은 을 참조하십시오 ["학습 및 활성 모드"](#).



기존 볼륨에서 학습 및 활성 모드는 볼륨의 기존 데이터가 아닌 새로 기록된 데이터에만 적용됩니다. ARP에 대해 볼륨이 활성화된 후 새 데이터를 기반으로 이전 일반 데이터 트래픽의 특성이 가정되기 때문에 기존 데이터는 스캔되고 분석되지 않습니다.

시작하기 전에

- NFS나 SMB(또는 둘 다)에 대해 SVM(스토리지 VM)을 활성화해야 합니다.
- 를 클릭합니다 [올바른 라이선스입니다](#) ONTAP 버전용으로 설치해야 합니다.
- 클라이언트가 구성된 NAS 워크로드가 있어야 합니다.
- ARP를 설정하려는 볼륨은 보호되어야 하며 활성 상태여야 합니다 ["접합 경로"](#).
- 볼륨이 100% 미만이어야 합니다.
- ARP 활동의 알림을 포함하는 e-메일 알림을 보내도록 EMS 시스템을 구성하는 것이 좋습니다. 자세한 내용은 을 참조하십시오 ["이메일 알림을 보내도록 EMS 이벤트를 구성합니다"](#).
- ONTAP 9.13.1 부터는 ARP(Autonomous 랜섬웨어 보호) 구성에 2명 이상의 인증된 사용자 관리자가 필요할 수 있도록 MAV(Multi-admin verification)를 활성화하는 것이 좋습니다. 자세한 내용은 을 참조하십시오 ["다중 관리 검증을 활성화합니다"](#).

ARP를 활성화합니다

시스템 관리자 또는 ONTAP CLI를 사용하여 ARP를 사용하도록 설정할 수 있습니다.

시스템 관리자

단계

1. 스토리지 > 볼륨 * 을 선택한 다음 보호할 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 * Anti 랜섬웨어 * 상자의 학습 모드에서 사용 안 함으로 전환합니다.
3. 학습 기간이 끝나면 ARP를 활성 모드로 전환합니다.



ONTAP 9.13.1 부터는 ARP가 최적의 학습 기간을 자동으로 결정하고 스위치를 자동화합니다. 가능합니다 "[연결된 스토리지 VM에서 이 설정을 해제합니다](#)" 학습 모드를 활성 모드로 제어하려면 수동으로 전환합니다.

- a. 스토리지 > 볼륨 * 을 선택한 다음 활성 모드에 사용할 준비가 된 볼륨을 선택합니다.
 - b. 볼륨 * 개요의 * 보안 * 탭에서 * 랜섬웨어 방지 상자에서 * 활성 모드로 전환 * 을 선택합니다.
4. Anti-랜섬웨어 * 상자에서 볼륨의 ARP 상태를 확인할 수 있습니다.

모든 볼륨에 대한 ARP 상태를 표시하려면 * Volumes * 창에서 * 표시/숨기기 * 를 선택한 다음 * Anti-랜섬웨어 * 상태가 선택되었는지 확인합니다.

CLI를 참조하십시오

기존 볼륨과 새 볼륨에서 ARP를 활성화하는 경우 CLI를 사용하여 ARP를 활성화하는 프로세스가 다릅니다.

기존 볼륨에서 **ARP**를 활성화합니다

1. 학습 모드에서 랜섬웨어 보호를 활성화하려면 기존 볼륨을 수정하십시오.

```
'Security Anti-랜섬웨어 volume dry-run-volume_vol_name_-vserver_svm_name_'
```

ONTAP 9.13.1 이상을 실행 중인 경우 활성 상태로 자동 변경되도록 적응 학습이 활성화됩니다. 이 동작이 자동으로 활성화되지 않도록 하려면 모든 관련 볼륨에서 SVM 레벨에서 설정을 변경합니다.

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. 학습 기간이 끝나면 보호된 볼륨을 수정하여 아직 자동으로 실행되지 않은 경우 활성 모드로 전환합니다.

```
'Security Anti-랜섬웨어 volume enable-volume_vol_name_-vserver_svm_name_'
```

볼륨 수정 명령을 사용하여 활성 모드로 전환할 수도 있습니다.

```
'volume modify -volume_vol_name_-vserver_svm_name_-anti-랜섬웨어-state active
```

3. 볼륨의 ARP 상태를 확인합니다.

```
'보안 Anti 랜섬웨어 볼륨 쇼'
```

새 볼륨에서 **ARP**를 활성화합니다

1. 데이터를 프로비저닝하기 전에 랜섬웨어 방지 보호를 활성화한 상태로 새 볼륨을 생성하십시오.

```
'volume create-volume_vol_name_-vserver_svm_name_-aggregate_aggr_name_-size_nn_-anti-랜섬웨어-state dry-run-junction-path/path_name'
```

ONTAP 9.13.1 이상을 실행 중인 경우 활성 상태로 자동 변경되도록 적응 학습이 활성화됩니다. 이 동작이 자동으로 활성화되지 않도록 하려면 모든 관련 볼륨에서 SVM 레벨에서 설정을 변경합니다.

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. 학습 기간이 끝나면 보호된 볼륨을 수정하여 아직 자동으로 실행되지 않은 경우 활성 모드로 전환합니다.

```
'Security Anti-랜섬웨어 volume enable-volume_vol_name_-vserver_svm_name_'
```

볼륨 수정 명령을 사용하여 활성 모드로 전환할 수도 있습니다.

```
'volume modify -volume_vol_name_-vserver_svm_name_-anti-랜섬웨어-state active
```

3. 볼륨의 ARP 상태를 확인합니다.

```
'보안 안티 랜섬웨어 볼륨 쇼'
```

새로운 볼륨에서 자율 랜섬웨어 보호를 기본적으로 활성화하십시오

ONTAP 9.10.1부터 학습 모드에서 새로운 볼륨이 기본적으로 자동 랜섬웨어 보호(ARP)에 사용되도록 스토리지 VM(SVM)을 구성할 수 있습니다.

이 작업에 대해

기본적으로 새 볼륨은 ARP가 비활성화 모드로 생성됩니다. System Manager 및 CLI에서 이 설정을 수정할 수 있습니다. 기본적으로 활성화된 볼륨은 학습(또는 드라이 런) 모드에서 ARP로 설정됩니다.

ARP는 설정을 변경한 후 SVM에서 생성된 볼륨에서만 활성화됩니다. ARP는 기존 볼륨에서 활성화되지 않습니다. 자세한 내용을 알아보십시오 ["기존 볼륨에서 ARP를 활성화합니다"](#).

ONTAP 9.13.1 부터는 적응형 학습이 ARP 분석에 추가되었으며 학습 모드에서 활성 모드로 자동 전환됩니다. 자세한 내용은 을 참조하십시오 ["학습 및 활성 모드"](#).

시작하기 전에

- 를 클릭합니다 [올바른 라이선스입니다](#) ONTAP 버전용으로 설치해야 합니다.
- 볼륨이 100% 미만이어야 합니다.
- 접합 경로가 활성 상태여야 합니다.
- ONTAP 9.13.1 부터는 MAV(Multi-admin verification)를 활성화하여 두 명 이상의 인증된 사용자 관리자가 랜섬웨어 방지 작업에 필요할 수 있도록 하는 것이 좋습니다. ["자세한 정보"](#).

ARP를 학습에서 활성 모드로 전환합니다

ONTAP 9.13.1부터 ARP 분석에 적응형 학습이 추가되었습니다. 학습 모드에서 활성 모드로 자동 전환됩니다. 학습 모드에서 활성 모드로 자동 전환하기 위한 ARP의 자동 결정은 다음 옵션의 구성 설정을 기반으로 합니다.

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```


학습 후 30일 후에는 이러한 조건 중 하나 이상이 충족되지 않더라도 볼륨이 자동으로 활성 모드로 전환됩니다. 즉, 자동 전환이 활성화된 경우 볼륨은 최대 30일 후에 활성 모드로 전환됩니다. 최대 30일 값은 고정되어 있으며 수정할 수 없습니다.

기본값을 포함한 ARP 구성 옵션에 대한 자세한 내용은 [클릭](#) 참조하십시오 "ONTAP 명령 참조입니다".

단계

시스템 관리자 또는 ONTAP CLI를 사용하여 기본적으로 ARP를 활성화할 수 있습니다.

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 선택한 다음 ARP로 보호할 볼륨이 포함된 스토리지 VM을 선택합니다.
2. 설정 * 탭으로 이동합니다. 보안 * 에서 안티 랜섬웨어 타일을 찾은 다음 을 선택합니다 
3. NAS 볼륨에 대해 ARP를 활성화하려면 확인란을 선택합니다. 스토리지 VM의 모든 유효한 NAS 볼륨에서 ARP를 활성화하려면 추가 확인란을 선택합니다.



ONTAP 9.13.1 로 업그레이드한 경우 * 충분한 학습 * 설정이 자동으로 활성화되면 * 학습 모드에서 활성 모드로 자동 전환됩니다. 이를 통해 ARP는 최적의 학습 기간을 결정하고 스위치를 활성 모드로 자동 전환할 수 있습니다. 활성 모드로 수동으로 전환하려면 설정을 끕니다.

CLI를 참조하십시오

1. 새 볼륨에서 ARP를 기본적으로 사용하도록 기존 SVM을 수정합니다. 'vserver modify -vserver_svm_name_-anti-랜섬웨어-default-volume-state dry-run'

CLI에서 새 볼륨에 대해 기본적으로 ARP가 설정된 새 SVM을 생성할 수도 있습니다. 'vserver create-vserver svm_name-anti-랜섬웨어-default-volume-state dry-run[other parameters as needed]'

ONTAP 9.13.1 이상으로 업그레이드한 경우, 적응형 학습이 활성화되어 활성 상태로 자동 변경됩니다. 이 동작을 자동으로 사용하지 않으려면 다음 명령을 사용합니다.

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

Autonomous 랜섬웨어 Protection을 일시 중지하여 워크로드 이벤트를 분석에서 제외합니다

비정상적인 워크로드 이벤트가 발생할 것으로 예상되는 경우 언제든지 ARP(Autonomous 랜섬웨어 보호) 분석을 일시 중지 및 재개할 수 있습니다.

ONTAP 9.13.1 부터는 다중 관리 확인(MAV)을 활성화하여 두 명 이상의 인증된 사용자 관리자가 ARP를 일시 중지해야 합니다. ["자세한 정보"](#).

이 작업에 대해

ARP 일시 중지 중에는 이벤트가 기록되지 않으며 새 쓰기에 대한 작업도 기록되지 않습니다. 그러나 백그라운드에서 이전 로그에 대한 분석 작업은 계속됩니다.



ARP 비활성화 기능을 사용하여 분석을 일시 중지하지 마십시오. 이렇게 하면 볼륨에서 ARP가 비활성화되고 학습된 워크로드 동작에 대한 기존 정보가 모두 손실됩니다. 이 경우 학습 기간을 다시 시작해야 합니다.

단계

시스템 관리자 또는 ONTAP CLI를 사용하여 ARP를 일시 중지할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택한 다음 ARP를 일시 중지할 볼륨을 선택합니다.
2. 볼륨 개요의 보안 탭에서 * 안티 랜섬웨어 * 상자에서 * 안티 랜섬웨어 * 일시 중지 * 를 선택합니다.



ONTAP 9.13.1 부터, ARP 설정을 보호하기 위해 MAV를 사용하는 경우, 일시 중지 작업은 하나 이상의 추가 관리자의 승인을 얻으라는 메시지를 표시합니다. "모든 관리자로부터 승인을 받아야 합니다" MAV 승인 그룹과 연관되거나 작업이 실패합니다.

CLI를 참조하십시오

1. 볼륨에서 ARP 일시 중지:

```
'Security Anti-랜섬웨어 volume pause-vserver_svm_name_-volume_vol_name_'
```

2. 처리를 재개하려면 를 사용합니다 `resume` 명령:

```
'Security Anti-랜섬웨어 volume resume - vserver_svm_name_-volume_vol_name_'
```

3. * ARP 설정을 보호하기 위해 MAV(ONTAP 9.13.1로 시작하는 ARP에서 사용 가능)를 사용하는 경우 * 일시 중지 작업은 하나 이상의 추가 관리자의 승인을 얻도록 요청합니다. MAV 승인 그룹과 연결된 모든 관리자로부터 승인을 받아야 합니다. 그렇지 않으면 작업이 실패합니다.

MAV를 사용 중이고 예상 일시 중지 작업에 추가 승인이 필요한 경우 각 MAV 그룹 승인자는 다음을 수행합니다.

- a. 요청 표시:

```
security multi-admin-verify request show
```

- b. 요청 승인:

```
security multi-admin-verify request approve -index[number returned from show request]
```

마지막 그룹 승인자에 대한 응답은 볼륨이 수정되었고 ARP 상태가 일시 중지되었음을 나타냅니다.

MAV를 사용하고 있고 MAV 그룹 승인자인 경우 일시 중지 작업 요청을 거부할 수 있습니다.

```
security multi-admin-verify request veto -index[number returned from show request]
```

자율적 랜섬웨어 방어 공격 감지 매개 변수를 관리합니다

ONTAP 9.11.1부터는 특정 자율 랜섬웨어 차단 지원 볼륨에서 랜섬웨어 감지 매개 변수를 수정하고 알려진 서지(surge)를 일반 파일 활동으로 보고할 수 있습니다. 감지 매개 변수를 조정하면 특정 볼륨 작업량에 따라 보고의 정확도를 높일 수 있습니다.

공격 탐지 작동 방식

ARP(Autonomous Ransomware Protection)가 학습 모드에 있을 때 볼륨 행동에 대한 기준 값을 개발합니다. 엔트로피, 파일 확장자 및 ONTAP 9.11.1부터 IOPS가 지원됩니다. 이러한 기준선은 랜섬웨어 위협을 평가하는 데 사용됩니다. 이러한 조건에 대한 자세한 내용은 [을 참조하십시오 ARP가 감지하는 것](#).

ONTAP 9.10.1에서 ARP는 다음 조건을 모두 감지하면 경고를 발생시킵니다.

- 이전에 볼륨에서 관찰되지 않은 파일 확장명을 가진 20개 이상의 파일
- 높은 엔트로피 데이터

ONTAP 9.11.1부터 ARP는 `_ONLY_ONLY_ONE` 조건이 충족되면 위협 경고를 발생시킵니다. 예를 들어, 이전에 볼륨에서 관찰되지 않은 파일 확장자를 가진 20개 이상의 파일이 24시간 내에 관찰되는 경우 ARP는 이를 관찰된 엔트로피의 위협_무관_으로 분류합니다. (24시간 및 20개의 파일 값은 기본값이며 수정할 수 있습니다.)

ONTAP 9.14.1부터 ARP가 새 파일 확장자를 관찰하고 ARP가 스냅샷을 생성할 때 경고를 구성할 수 있습니다. 자세한 내용은 [을 참조하십시오 \[modify-alerts\]](#)

특정 볼륨 및 워크로드에는 서로 다른 감지 매개 변수가 필요합니다. 예를 들어, ARP 지원 볼륨은 다양한 유형의 파일 확장자를 호스팅할 수 있습니다. 이 경우 이전에 보지 못한 파일 확장자의 임계값 수를 기본값인 20보다 큰 수로 수정하거나 이전에 보지 못한 파일 확장자를 기준으로 경고를 비활성화할 수 있습니다. ONTAP 9.11.1부터 공격 감지 매개 변수를 수정하여 특정 워크로드에 더 잘 맞출 수 있습니다.

공격 탐지 매개 변수를 수정합니다

ARP 가능 볼륨의 예상 동작에 따라 공격 감지 매개 변수를 수정할 수 있습니다.

단계

1. 기존 공격 탐지 매개 변수 보기:

```
security anti-ransomware volume attack-detection-parameters show -vserver  
svm_name -volume volume_name
```

```

security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume voll

Vserver Name : vs1
Volume Name : voll
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24

```

2. 표시된 모든 필드는 부울 또는 정수 값으로 수정할 수 있습니다. 필드를 수정하려면 을 사용합니다 security anti-ransomware volume attack-detection-parameters modify 명령.

매개 변수의 전체 목록은 을 참조하십시오 ["ONTAP 명령 참조입니다"](#).

알려진 서지를 보고합니다

ARP는 활성 모드에서도 감지 매개변수에 대한 기준 값을 계속 수정합니다. 볼륨 활동(일회성 서지 또는 새로운 정상성의 특징인 서지)의 급증을 알면 안전한 것으로 보고해야 합니다. 수동으로 이러한 서지를 안전한 것으로 보고하면 ARP의 위협 평가의 정확도를 높이는 데 도움이 됩니다.

일회성 급증을 보고합니다

1. 알려진 상황에서 일회성 서지가 발생하고 향후 상황에서 ARP가 비슷한 서지를 보고하려면 워크로드 동작에서 서지를 지웁니다.

```

security anti-ransomware volume workload-behavior clear-surge -vserver
svm_name -volume volume_name

```

기준선 서지 수정

1. 보고된 서지가 정상적인 응용 프로그램 동작으로 간주되어야 하는 경우 서지를 보고하여 기준 서지 값을 수정합니다.

```

security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver svm_name -volume volume_name

```

ARP 경고를 구성합니다

ONTAP 9.14.1부터 ARP를 사용하면 두 ARP 이벤트에 대한 경고를 지정할 수 있습니다.

- 볼륨에서 새 파일 확장명을 관찰합니다
- ARP 스냅샷 생성

이러한 두 이벤트에 대한 경고는 개별 볼륨 또는 전체 SVM에 설정할 수 있습니다. SVM에 대해 경고를 활성화하면 알림을 사용하도록 설정한 후 생성된 볼륨에서만 경고 설정이 상속됩니다. 기본적으로 알림은 모든 볼륨에 대해 활성화되지 않습니다.

이벤트 경고는 다중 관리자 확인을 통해 제어할 수 있습니다. 자세한 내용은 [을 참조하십시오](#) [ARP로 보호되는 볼륨을 사용한 다중 관리자 검증](#).

시스템 관리자

볼륨에 대한 알림을 설정합니다

1. 볼륨**으로 이동합니다. 설정을 수정할 개별 볼륨을 선택합니다.
2. 보안 탭을 선택한 다음 이벤트 보안 설정** 을 선택합니다.
3. 새 파일 확장명이 감지됨 및 랜섬웨어 스냅샷 생성됨 에 대한 알림을 받으려면 심각도 제목 아래의 드롭다운 메뉴를 선택합니다. 설정을 이벤트 생성 안 함에서 알림으로 수정합니다.
4. 저장을 선택합니다.

SVM에 대한 알림 설정

1. 스토리지 VM**으로 이동한 다음 설정을 활성화할 SVM을 선택합니다.
2. 보안 제목 아래에서 안티 랜섬웨어 카드를 찾습니다. 그런 다음 랜섬웨어 이벤트 심각도 편집 을 선택합니다
⋮ .
3. 새 파일 확장명이 감지됨 및 랜섬웨어 스냅샷 생성됨 에 대한 알림을 받으려면 심각도 제목 아래의 드롭다운 메뉴를 선택합니다. 설정을 이벤트 생성 안 함에서 알림으로 수정합니다.
4. 저장을 선택합니다.

CLI를 참조하십시오

볼륨에 대한 알림을 설정합니다

- 새 파일 확장자에 대한 알림을 설정하려면 다음을 수행합니다.

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- ARP 스냅샷 생성을 위한 경고를 설정하려면:

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- 를 사용하여 설정을 확인합니다 anti-ransomware volume event-log show 명령.

SVM에 대한 알림 설정

- 새 파일 확장자에 대한 알림을 설정하려면 다음을 수행합니다.

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- ARP 스냅샷 생성을 위한 경고를 설정하려면:

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- 를 사용하여 설정을 확인합니다 security anti-ransomware vserver event-log show 명령.

추가 정보

- "자율적 랜섬웨어 방어 공격 및 자율적 랜섬웨어 방어 스냅샷을 이해합니다"

비정상적인 활동에 응답합니다

ARP(Autonomous 랜섬웨어 Protection)가 보호 볼륨에서 비정상적인 활동을 감지하면 경고를 표시합니다. 알림을 평가하여 활동이 허용 가능한지(가양성) 또는 공격이 악의적으로 보이는지 여부를 결정해야 합니다.

이 작업에 대해

ARP는 높은 데이터 엔트로피, 데이터 암호화와 비정상적인 볼륨 활동 및 비정상적인 파일 확장자의 조합을 감지할 때 의심되는 파일 목록을 표시합니다.

경고가 발생하면 다음 두 가지 방법 중 하나로 파일 작업을 지정하여 응답합니다.

- 거짓 긍정

식별된 파일 유형이 작업 부하에 필요합니다. 이 파일 유형은 무시해도 됩니다.

- 잠재적 랜섬웨어 공격

식별된 파일 유형이 작업 부하에서 예기치 않은 유형이므로 잠재적 공격으로 간주해야 합니다.

두 경우 모두 알림 업데이트 및 삭제 후 정상적인 모니터링이 재개됩니다. ARP는 후속 파일 활동을 모니터링하기 위해 사용자의 선택을 사용하여 위협 평가 프로파일에 평가를 기록합니다.

공격이 의심되는 경우에는 알림을 지우기 전에 공격이 공격인지 여부를 확인하고, 공격에 대한 대응 및 보호된 데이터를 복원해야 합니다. ["랜섬웨어 공격에서 복구하는 방법에 대해 자세히 알아보십시오"](#).



전체 볼륨을 복원하는 경우 지울 알림이 없습니다.

시작하기 전에

ARP가 활성 모드에서 실행되고 있어야 합니다.

단계


System Manager 또는 ONTAP CLI를 사용하여 비정상적인 작업에 응답할 수 있습니다.

시스템 관리자

1. "비정상적인 활동" 알림을 수신하면 링크를 따라가십시오. 또는 * Volumes * 개요의 * Security * 탭으로 이동합니다.

경고는 * Events * 메뉴의 * Overview * 창에 표시됩니다.
2. "Detected abnormal volume activity(비정상적인 볼륨 활동이 감지됨)" 메시지가 표시되면 의심되는 파일을 봅니다.

보안 * 탭에서 * 의심되는 파일 형식 보기 * 를 선택합니다.
3. 의심되는 파일 유형* 대화 상자에서 각 파일 유형을 조사하여 "거짓 긍정" 또는 "잠재적인 랜섬웨어 공격"으로 표시합니다.

이 값을 선택한 경우...	이 조치를 취하십시오...
거짓 양성	업데이트 * 및 * 의심되는 파일 유형 지우기 * 를 선택하여 결정을 기록하고 정상적인 ARP 모니터링을 재개합니다.  ONTAP 9.13.1 부터, ARP 설정을 보호하기 위해 MAV를 사용하는 경우, 의심스러운 작업이 하나 이상의 추가 관리자의 승인을 얻으라는 메시지를 표시합니다. "모든 관리자로부터 승인을 받아야 합니다" MAV 승인 그룹과 연관되거나 작업이 실패합니다.
잠재적인 랜섬웨어 공격	공격에 대응하고 보호된 데이터를 복원합니다. 그런 다음 * 업데이트 * 및 * 의심되는 파일 유형 지우기 * 를 선택하여 결정을 기록하고 정상적인 ARP 모니터링을 재개합니다. 전체 볼륨을 복원한 경우 삭제할 의심스러운 파일 유형이 없습니다.

CLI를 참조하십시오

1. 랜섬웨어 공격이 의심되는 경우 다음 사항을 통지하여 공격의 시간 및 심각도를 확인하십시오.

'Security Anti-랜섬웨어 volume show -vserver_svm_name_-volume_vol_name_'

샘플 출력:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

EMS 메시지를 확인할 수도 있습니다.

이벤트 로그 show-message-name callhome.arw.activity.seen`

2. 공격 보고서를 생성하고 출력 위치를 기록합니다.

'Security Anti-랜섬웨어 volume attack generate-report-volume_vol_name_-dest-path_file_location_ /

샘플 출력:

"Report" report_file_vs0_vol1_14-09-2021_01-21-08" 경로 "vs0:vol1/" 에서 사용할 수 있습니다

3. 관리 클라이언트 시스템에서 보고서를 봅니다. 예를 들면 다음과 같습니다.

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08  
  
19 "9/14/2021 01:03:23" test_dir_1/test_file_1.jpg.lckd  
20 "9/14/2021 01:03:46" test_dir_2/test_file_2.jpg.lckd  
21 "9/14/2021 01:03:46" test_dir_3/test_file_3.png.lckd`
```

4. 파일 확장명 평가에 따라 다음 작업 중 하나를 수행합니다.

◦ 거짓 양성

다음 명령을 입력하여 결정 사항을 기록하고, 허용되는 확장자 목록에 새 확장을 추가한 후, 정상적인 안티 랜섬웨어 모니터링을 재개합니다.

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive true
```

다음 매개 변수 중 하나를 사용하여 의심되는 목록에 있는 파일의 '[seq-no_integer]' 시퀀스 번호를 식별합니다. `[extension_text,... [start-time_date_time_-end-time_date_time_]` MM/DD/YYYY HH:MM:SS 형식으로 지을 파일 범위의 시작 및 종료 시간.

◦ 잠재적인 랜섬웨어 공격

공격에 대한 대응 및 "ARP 생성 백업 스냅샷으로부터 데이터를 복구합니다". 데이터가 복구된 후 다음 명령을 입력하여 결정을 기록하고 정상적인 ARP 모니터링을 재개합니다.

```
'안티 랜섬웨어 볼륨 공격 clear-suspect-vserver_svm_name_-volume_vol_name_[extension  
identifier]-false-positive false'
```

다음 매개 변수 중 하나를 사용하여 확장자가 무엇인지 확인하십시오. "[seq-no_integer]" 의심되는 목록에 있는 파일의 시퀀스 번호 [extension_text,... [start-time_date_time_-end-time_date_time_]` MM/DD/YYYY HH:MM:SS 형식으로 지을 파일 범위의 시작 및 종료 시간.

전체 볼륨을 복원한 경우 삭제할 의심스러운 파일 유형이 없습니다. ARP 생성 백업 스냅샷이 제거되고 공격 보고서가 지워집니다.

5. MAV를 사용하고 있고 예상되는 경우 clear-suspect 작업에 추가 승인이 필요합니다. 각 MAV 그룹 승인자는 다음을 수행해야 합니다.

a. 요청 표시:

```
security multi-admin-verify request show
```

b. 정상적인 랜섬웨어 방지 모니터링 재개 요청을 승인합니다.

```
security multi-admin-verify request approve -index[number returned from show request]
```

마지막 그룹 승인자에 대한 응답은 볼륨이 수정되었고 가양성이 기록되었음을 나타냅니다.

6. MAV를 사용하고 있고 MAV 그룹 승인자인 경우 의심스러운 요청을 거부할 수도 있습니다.

```
security multi-admin-verify request veto -index[number returned from show request]
```

추가 정보

- ["KB: 자율 랜섬웨어 보호 공격과 자율 랜섬웨어 보호 스냅샷 이해"](#).

랜섬웨어 공격 후 데이터 복원

ARP(자율적 랜섬웨어 방어)는 이러한 스냅샷 복사본을 생성합니다

Anti_ransomware_backup 잠재적 랜섬웨어 위협을 감지한 경우 이러한 ARP 스냅샷 복사본 중 하나 또는 볼륨의 다른 스냅샷 복사본을 사용하여 데이터를 복원할 수 있습니다.

이 작업에 대해

볼륨에 SnapMirror 관계가 있는 경우 스냅샷 복사본에서 복원한 직후 볼륨의 모든 미러 복사본을 수동으로 복제합니다. 그렇지 않으면 미러 복사본을 사용할 수 없게 되므로 복사본을 삭제하고 다시 생성해야 합니다.

가 아닌 다른 스냅샷에서 복원합니다 Anti_ransomware_backup 스냅샷 시스템 공격이 식별되면 먼저 ARP 스냅샷을 해제해야 합니다.

시스템 공격이 보고되지 않은 경우 먼저 에서 복구해야 합니다 Anti_ransomware_backup 그런 다음, 선택한 스냅샷 복사본에서 볼륨의 후속 복원을 완료합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 데이터를 복원할 수 있습니다.

시스템 관리자

시스템 공격 후 복원

1. ARP 스냅샷에서 복원하려면 2단계로 건너뛩니다. 이전 스냅샷 복사본에서 복원하려면 먼저 ARP 스냅샷의 잠금을 해제해야 합니다.
 - a. 스토리지 > 볼륨 * 을 선택합니다.
 - b. 보안 * 을 선택한 다음 * 의심되는 파일 형식 보기 * 를 선택합니다
 - c. 파일을 "거짓 양성"으로 표시합니다.
 - d. Update * 및 * Clear Suspect File Types * 를 선택합니다

2. 볼륨에 Snapshot 복사본을 표시합니다.

스토리지 > 볼륨 * 을 선택한 다음 볼륨 및 * Snapshot 복사본 * 을 선택합니다.

3. 복원할 스냅샷 복사본 옆의 를 선택하고 * 복원 * 을 선택합니다 . .

시스템 공격이 확인되지 않은 경우 복원합니다

1. 볼륨에 Snapshot 복사본을 표시합니다.

스토리지 > 볼륨 * 을 선택한 다음 볼륨 및 * Snapshot 복사본 * 을 선택합니다.

2. 스냅샷을 선택합니다 : Anti_ransomware_backup .
3. Restore * 를 선택합니다.
4. Snapshot Copies * 메뉴로 돌아가서 사용할 Snapshot 복사본을 선택합니다. Restore * 를 선택합니다.

CLI를 참조하십시오

시스템 공격 후 복원

1. ARP 스냅샷 복사본에서 복원하려면 2단계로 건너뛩니다. 이전 스냅샷 사본에서 데이터를 복원하려면 ARP 스냅샷의 잠금을 해제해야 합니다.



를 사용 중인 경우 이전 Snapshot 복사본에서 복원하기에 앞서 Anti-랜섬웨어 SnapLock만 릴리즈하면 됩니다 volume snap restore 아래에 설명된 대로 명령을 실행합니다. Flex Clone, Single File Snap Restore 또는 기타 방법을 사용하여 데이터를 복구하는 경우에는 이 작업이 필요하지 않습니다.

공격을 "거짓 양성" 및 "용의자 명시"로 표시:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

다음 매개 변수 중 하나를 사용하여 확장을 식별합니다.

[-seq-no integer] 의심되는 목록에 있는 파일의 시퀀스 번호입니다.

[-extension text, ...] 파일 확장자

[-start-time date_time -end-time date_time] 지을 파일 범위의 시작 및 종료 시간(예: "MM/DD/YYYY HH:MM:SS" 형식)

2. 볼륨의 스냅샷 복사본을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 "vol1"의 스냅샷 복사본을 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

3. 스냅샷 복사본에서 볼륨 콘텐츠를 복원합니다.

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

시스템 공격이 확인되지 않은 경우 복원합니다

1. 볼륨의 스냅샷 복사본을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 "vol1"의 스냅샷 복사본을 보여 줍니다.


```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. 스냅샷 복사본에서 볼륨 콘텐츠를 복원합니다.

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

3. 원하는 스냅샷 복사본을 사용하여 볼륨을 복원하려면 1단계와 2단계를 반복합니다.

추가 정보

- ["KB: ONTAP에서 랜섬웨어 방지 및 복구 기능을 사용할 수 있습니다"](#)

자동 스냅샷 복사본에 대한 옵션을 수정합니다

ONTAP 9.11.1부터 CLI를 사용하여 의심되는 랜섬웨어 공격에 대응하여 자동으로 생성되는 ARP(자율적 랜섬웨어 차단) 스냅샷 복사본의 보존 설정을 제어할 수 있습니다.

시작하기 전에

노드 SVM에서는 ARP 스냅샷 옵션만 수정할 수 있습니다.

단계


1. 현재 ARP 스냅샷 복사 설정을 모두 표시하려면 'vserver options -vserver_svm_name_arw *'를 입력합니다



를 클릭합니다 vserver options 명령은 숨겨진 명령입니다. man 페이지를 보려면 를 입력합니다 man vserver options ONTAP CLI에서

2. 선택한 현재 ARP 스냅샷 복사 설정을 표시하려면 'vserver options-vserver_svm_name_-option-name_arw_setting_name_'을 입력합니다
3. ARP 스냅샷 복사 설정을 수정하려면 'vserver options-vserver_svm_name_-option-name_arw_setting_name_-option-value_arw_setting_value_'를 입력합니다

다음 설정을 수정할 수 있습니다.

ARW 설정	설명
arw.snap.max.count	<p>특정 시간에 볼륨에 존재할 수 있는 ARP Snapshot 복사본의 최대 수를 지정합니다. ARP Snapshot 복사본의 총 수가 지정된 한도 내에 있도록 이전 복사본이 삭제됩니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 3과 8 사이의 정수를 사용할 수 있습니다. 기본값은 6입니다.</p>
arw.snap.create.interval.hours	<p>ARP 스냅샷 사본 사이의 간격을 시간 단위로 지정합니다. 새로운 ARP 스냅샷 복사본은 데이터 엔트로피 기반 공격이 의심되고 가장 최근에 생성된 ARP 스냅샷 복사본이 지정된 간격보다 오래된 경우에 생성됩니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 1에서 48 사이의 정수를 사용할 수 있습니다. 기본값은 4입니다.</p>
arw.snap.normal.retain.interval.hours	<p>ARP 스냅샷 복제본이 유지되는 기간을 시간 단위로 지정합니다. ARP 스냅샷 복사본이 보존 임계값에 도달하면 삭제되기 전에 생성된 다른 ARP 스냅샷 복사본이 생성됩니다. 보존 임계값보다 오래된 ARP 스냅샷 복사본은 둘 이상 존재할 수 없습니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 4에서 96 사이의 정수를 사용할 수 있습니다. 기본값은 48입니다.</p>
arw.snap.max.retain.interval.days	<p>ARP 스냅샷 복사본을 유지할 수 있는 최대 지속 시간을 일 수 _ 단위로 지정합니다. 이 기간보다 오래된 ARP 스냅샷 복사본은 볼륨에 보고된 공격이 없으면 삭제됩니다.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>보통 위협이 감지되면 ARP 스냅샷 복사본의 최대 보존 간격은 무시됩니다. 위협에 대한 응답으로 생성된 ARP 스냅샷 복사본은 위협에 응답할 때까지 유지됩니다. 위협을 false positive로 표시 볼륨에서 ARP 스냅샷 복사본을 삭제합니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 1에서 365 사이의 정수를 사용할 수 있습니다. 기본값은 5입니다.</p> </div>
arw.snap.create.interval.hours.post.max.count	<p>볼륨에 이미 최대 ARP 스냅샷 복사본 수가 포함되어 있을 때 ARP 스냅샷 사본 사이의 간격(시간)을 지정합니다. 최대 수에 도달하면 새 복사본을 위한 공간을 만들기 위해 ARP 스냅샷 복사본이 삭제됩니다. 이 옵션을 사용하여 이전 복사본을 보존하도록 새 ARP 스냅샷 복사본 생성 속도를 줄일 수 있습니다. 볼륨에 이미 최대 ARP 스냅샷 복사본 수가 포함되어 있는 경우 이 옵션에 지정된 간격은 다음 ARP 스냅샷 복사본 생성에 대신 사용됩니다 arw.snap.create.interval.hours.</p> <p>를 클릭합니다 -option-value 매개 변수에는 4에서 48 사이의 정수를 사용할 수 있습니다. 기본값은 8입니다.</p>

ARW 설정	설명
arw.surge.snap.interval.days	<p>입출력 급증에 대한 응답으로 생성된 ARP 스냅샷 복사본의 간격을 일 수 _ 단위로 지정합니다. ONTAP는 IO 트래픽의 급증이 있고 마지막으로 생성된 ARP 스냅샷 복사본이 지정된 간격보다 오래된 경우 ARP 스냅샷 서지 복제본을 생성합니다. 또한 이 옵션은 ARP 서지 스냅샷 복사본의 보존 기간을 _ 일 _ 로 지정합니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 1에서 365 사이의 정수를 사용할 수 있습니다. 기본값은 5입니다.</p>
arw.snap.new.extns.interval.hours	<p>이 옵션은 새 파일 확장자가 감지될 때 생성된 ARP 스냅샷 사본 사이의 간격 _ 시간 _ 을(를) 지정합니다. 새 ARP 스냅샷 복사본은 언제 생성됩니다</p> <p>새 파일 확장자가 관찰되었습니다. 새 파일 확장자를 관찰할 때 생성된 이전 스냅샷이 지정된 간격보다 오래되었습니다. 새 파일 확장자를 자주 생성하는 작업 부하에서 이 간격은 ARP 스냅샷 복사본의 빈도를 제어하는 데 도움이 됩니다. 이 옵션은 에 독립적입니다 arw.snap.create.interval.hours, 데이터 엔트로피 기반 ARP 스냅샷 복사본의 간격을 지정합니다.</p> <p>를 클릭합니다 -option-value 매개 변수에는 24에서 8760 사이의 정수를 사용할 수 있습니다. 기본값은 48입니다.</p>

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.