보안

ONTAP Technical Reports

NetApp
January 23, 2026

목차

보안

ONTAP 보안 기술 보고서

ONTAP는 보안을 솔루션의 일부로 통합하여 지속적으로 발전하고 있습니다. ONTAP의 최신 릴리즈에는 조직이 하이브리드 클라우드 전체에서 데이터를 보호하고, 랜섬웨어 공격을 방지하고, 업계 권장 사례를 준수하는 데 매우 중요한 새로운 보안 기능이 다수 포함되어 있습니다. 이러한 새로운 기능은 조직의 Zero Trust 모델 전환도 지원합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP 보안 및 데이터 암호화"설명합니다.

ONTAP 사이버 소산

"ONTAP 사이버 소산" NetApp의 ONTAP 기반 사이버 저장소는 가장 중요한 데이터 자산을 보호하는 포괄적이고 유연한 솔루션을 제공합니다. ONTAP은 강력한 강화 방법론을 통해 논리적 공기 흐름을 활용하여 진화하는 사이버 위협에 맞서 복원력을 갖춘 격리된 보안 스토리지 환경을 만들 수 있도록 지원합니다. ONTAP을 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서 데이터의 기밀성, 무결성, 가용성을 보장할 수 있습니다.

랜섬웨어

"TR-4572: 랜섬웨어용 NetApp 솔루션" 랜섬웨어의 진화 과정을 알아보고, 랜섬웨어용 NetApp 솔루션을 사용하여 공격을 식별하고, 확산을 방지하고, 최대한 빠르게 복구하는 방법을 살펴보십시오. 이 문서에 제공된 지침과 솔루션은 조직이 사이버 복원력 있는 솔루션을 보유하면서 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 설계되었습니다.

"TR-4526: NetApp SnapLock를 사용한 규정 준수 WORM 스토리지"
많은 기업에서는 규정 준수 요구 사항을 충족하거나 단순히 데이터 보호 전략에 다른 계층을 추가하기 위해 WORM(Write Once, Read Many) 데이터 스토리지를 사용하고 있습니다. ONTAP에서 WORM 솔루션인 SnapLock를 WORM 데이터 스토리지가 필요한 환경에 통합하는 방법에 대해 알아보십시오.

제로 트러스트

"NetApp와 제로 트러스트" 제로 트러스트는 네트워크 중심의 접근 방식으로 MCAP(마이크로 코어 및 경계)를 설계하여 데이터, 서비스, 애플리케이션 또는 자산을 세분화 게이트웨이라고 하는 제어 기능을 사용해 왔습니다. ONTAP는 제로 트러스트에 대한 데이터 중심 접근 방식을 취하며 스토리지 관리 시스템이 세분화 게이트웨이가 되어 고객 데이터의 액세스를 보호하고 모니터링합니다. 특히 FPolicy Zero Trust 엔진과 FPolicy 파트너 에코시스템은 정상 및 비정상적인 데이터 액세스 패턴을 세부적으로 이해하고 내부자 위협을 식별하기 위한 제어 센터가 됩니다.

다단계 인증

"TR-4647: ONTAP 모범 사례 및 구현 가이드의 다중 요소 인증"
System Manager, Active IQ Unified Manager 및 ONTAP SSH(Secure Shell) CLI 인증을 사용하여 관리 액세스에 대한 ONTAP의 다단계 인증 기능에 대해 알아보십시오.

"TR-4717: 공통 액세스 카드를 사용한 ONTAP SSH 인증"
ONTAP에서 CAC(Common Access Card)에 저장된 공개 키를 통해 ONTAP 스토리지 관리자를 인증하기 위해 ActivClient 소프트웨어와 함께 타사 SSH 클라이언트를 구성 및 테스트하는 방법을 알아봅니다.

멀티 테넌시

"TR-4160: ONTAP의 보안 멀티 테넌시"
설계 고려 사항 및 권장 사례를 비롯하여 ONTAP에서 스토리지 VM을 사용하여 보안 멀티 테넌시를 구현하는 방법에 대해 알아보십시오.

표준

"TR-4401: PCI-DSS 4.0 및 ONTAP"
PCI DSS 4.0 표준에 따라 시스템을 검증하고 NetApp ONTAP 시스템에 적용하는 제어 요구 사항을 충족하는 방법에 대해 알아보십시오.

속성 기반 액세스 제어

"ONTAP로 속성 기반 액세스 제어" RBAC(역할 기반 액세스 제어) 및 ABAC(속성 기반 액세스 제어)를 지원하도록 NFSv4.2 보안 레이블 및 확장 속성(xattrs)을 구성하는 방법에 대해 알아봅니다. 이 방법은 사용자, 리소스 및 환경 특성을 기준으로 사용 권한을 정의하는 권한 부여 전략입니다.

랜섬웨어에 대한 **NetApp** 솔루션

랜섬웨어 및 **NetApp**의 보호 포트폴리오

랜섬웨어는 2024년에 조직 중단을 초래하는 가장 중요한 위협 중 하나로 남아 있습니다. 에 따르면 "Sophos, 2024년 랜섬웨어 상태" 랜섬웨어 공격은 설문조사에 참여한 고객의 72%에 영향을 미친 것으로 나타났습니다. 랜섬웨어 공격은 그 영향과 수익을 극대화하기 위해 인공 지능과 같은 고급 기술을 사용하는 위협 공격자로 인해 더 정교하고 타겟이 되도록 진화하고 있습니다.

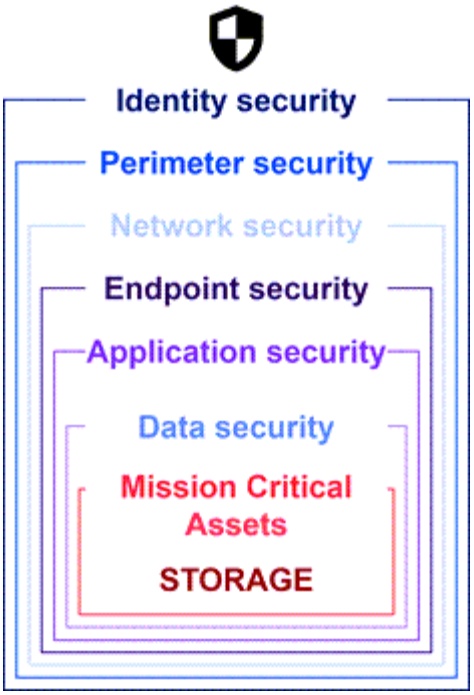
조직은 경계, 네트워크, ID, 애플리케이션, 데이터가 스토리지 수준에서 어디에 있는지, 그리고 이러한 계층을 안전하게 보호해야 합니다. 스토리지 계층에서 사이버 보호에 대한 데이터 중심의 접근 방식을 채택하는 것은 오늘날의 위협 환경에서 매우 중요합니다. 단일 솔루션으로 모든 공격을 차단할 수는 없지만, 파트너 관계 및 타사를 포함한 솔루션 포트폴리오를 사용하면 계층화된 방어 체계를 구축할 수 있습니다.

는 NetApp 제품 포트폴리오에 대해 자세히 살펴봅니다가시성, 감지, 해결을 위한 다양한 효과적인 툴을 제공하므로 랜섬웨어를 조기에 탐지하고 확산을 방지하고 필요한 경우 신속하게 복구하여 비용이 많이 드는 다운타임을 방지할 수 있습니다. 기존의 계층화된 방어 솔루션은 가시성과 감지를 위한 타사 및 파트너 솔루션처럼 널리 사용되고 있습니다. 효과적인 치료는 위협에 대한 대응의 중요한 부분입니다. 변경 불가능한 NetApp 스냅샷 기술 및 SnapLock 논리적 AIR GAP 솔루션을 활용하는 고유한 업계 접근법은 업계 차별화 요소이자 랜섬웨어 수정 기능에 대한 업계 모범 사례입니다.

2024년 7월부터 이전에 PDF로 게시되었던 NetApp Ransomware Protection_ 의 기술 보고서 _TR-4572: docs.netapp.com 에서 콘텐츠를 볼 수 있습니다.

데이터는 **1**차 타겟입니다

데이터를 직접 타겟으로 삼는 사이버 범죄자들이 점차 그 가치를 인식하게 되고 있습니다. 경계, 네트워크 및 애플리케이션 보안은 중요하지만 우회할 수 있습니다. 소스에서 데이터를 보호하는 데 중점을 둔 스토리지 계층은 중요한 최종 방어선을 제공합니다. 랜섬웨어 공격의 목표는 운영 데이터에 액세스하여 암호화하거나 액세스할 수 없도록 렌더링하는 것입니다. 이를 위해서는 공격자들이 경계에서 애플리케이션 보안에 이르기까지 오늘날 조직이 배포한 기존의 방어 체계를 이미 뚫어야만 합니다.



안타깝게도 많은 기업들은 데이터 레이어에서 보안 기능을 활용하지 못하고 있습니다. 이것이 바로 NetApp 랜섬웨어 차단 포트폴리오가 제공하는 이유입니다.

랜섬웨어의 실제 비용

몸값 지급 자체는 기업에 미치는 가장 큰 금전적 효과가 아닙니다. 지불액은 중요하지 않지만 랜섬웨어 사고로 인해 발생하는 다운타임 비용과 비교해 볼 수 있습니다.

몸값 지불은 랜섬웨어 이벤트를 처리할 때 복구 비용의 한 요소에 불과합니다. 지불된 모든 랜스를 제외하고, 2024개 조직은 랜섬웨어 공격으로부터 복구하는 평균 비용이 27만 3천 달러로, 2023년 보고된 1.820만 달러에서 거의 100만 달러 "2024 Sophos 랜섬웨어 상태" 증가했습니다. 전자 상거래, 주식 거래, 의료 등 IT 가용성에 크게 의존하는 조직의 경우 비용이 10배 이상 높을 수 있습니다.

보험 비용은 보험 회사를 대상으로 랜섬웨어 공격이 발생할 가능성이 매우 높기 때문에 지속적으로 증가하고 있습니다.

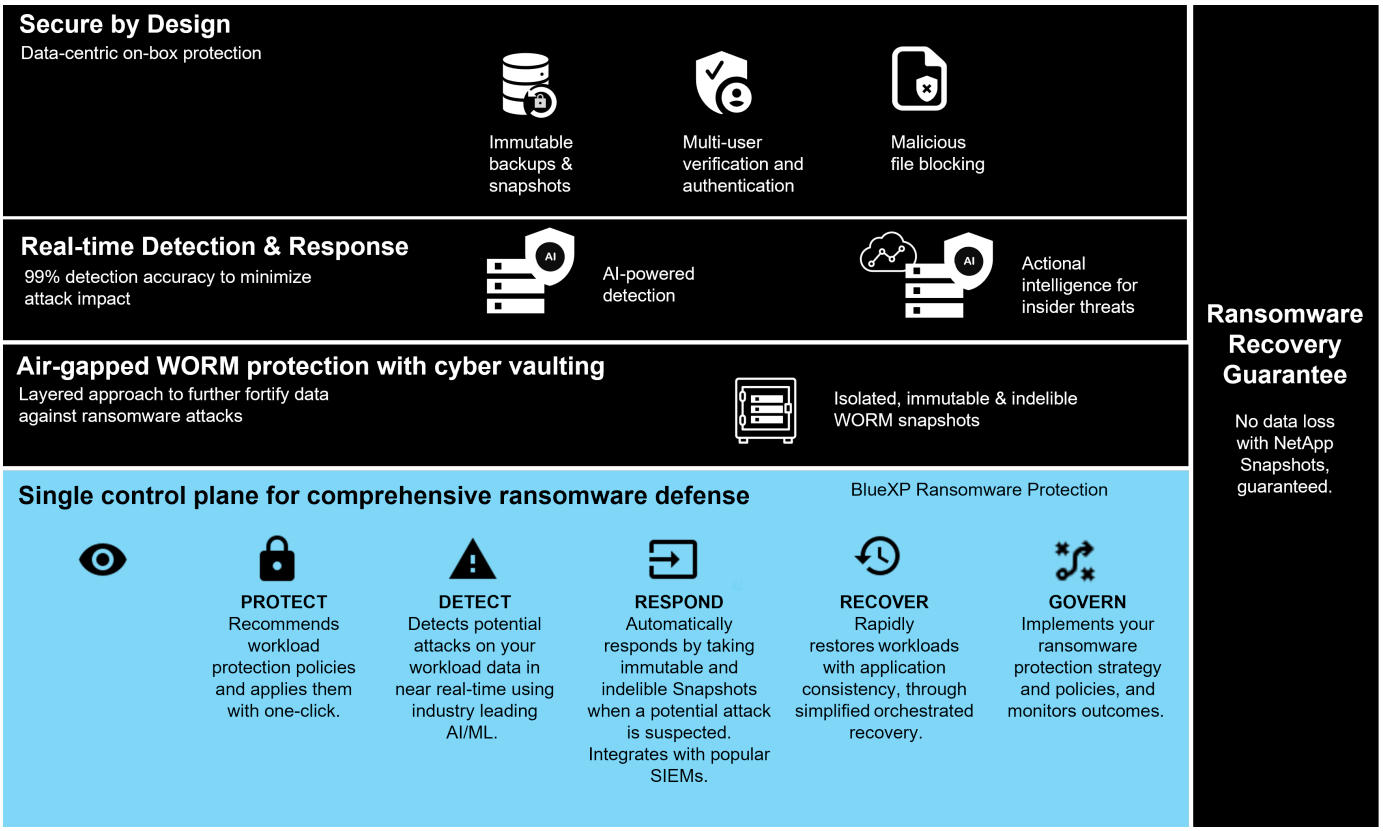
데이터 계층에서 랜섬웨어 방어

NetApp은 스토리지 계층에서 데이터가 상주하는 위치까지 조직 전체에서 광범위하고 심층적인 보안 태세를 이해합니다. 보안 스택은 복잡하며 기술 스택의 모든 수준에서 보안을 제공해야 합니다.

데이터 레이어에서 실시간 보호가 훨씬 더 중요하고 고유한 요구 사항이 있습니다. 효율성을 높이려면 이 계층의 솔루션이 다음과 같은 중요한 속성을 제공해야 합니다.

- * 보안 설계 * 를 통해 공격 성공 가능성을 최소화합니다
- * 실시간 감지 및 응답 * 을 통해 공격이 성공할 경우 미치는 영향을 최소화합니다
- * Air-gapped WORM 보호 * 로 중요한 데이터 백업을 격리합니다
- * 포괄적인 랜섬웨어 방어를 위한 단일 제어 플레인 *

NetApp은 이러한 모든 것을 제공할 수 있습니다.



NetApp의 랜섬웨어 방어 포트폴리오

NetApp는 "랜섬웨어 방지 기능 내장"중요한 데이터를 실시간으로 강력한 다면적인 방어 기능을 제공합니다. 고급 AI 기반 감지 알고리즘은 데이터 패턴을 지속적으로 모니터링하여 99% 정확성으로 잠재적 랜섬웨어 위협을 신속하게 식별합니다. 공격에 신속하게 대응함으로써 신속하게 데이터를 스냅샷하고 복사본을 보호하여 신속한 복구를 보장합니다.

데이터를 더욱 강화하기 위해 NetApp의 "사이버 보관" 기능은 논리적 공극으로 데이터를 격리합니다. 중요한 데이터를 보호함으로써 신속한 비즈니스 연속성을 보장합니다.

NetApp"NetApp 랜섬웨어 보호" 단일 제어 평면을 통해 엔드 투 엔드 워크로드 중심 랜섬웨어 방어를 지능적으로 조정하고 실행하여 운영 부담을 줄여 단 한 번의 클릭으로 위험에 처한 중요한 워크로드 데이터를 식별하고 보호하고, 잠재적 공격의 영향을 제한하기 위해 정확하고 자동으로 감지하고 대응하고, 며칠이 아닌 몇 분 내에 워크로드를 복구하여 귀중한 워크로드 데이터를 보호하고 비용이 많이 드는 중단을 최소화할 수 있습니다.

데이터에 대한 무단 액세스를 보호하기 위한 기본 내장 ONTAP 솔루션에는 "다중 관리자 인증(MAV)"볼륨 삭제, 추가 관리 사용자 생성 또는 스냅샷 삭제와 같은 작업을 적어도 두 번째 지정된 관리자로부터 승인을 받은 후에만 수행할 수 있는 강력한 기능이 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다. 스냅샷을 삭제하기 전에 지정된 관리자 승인자를 원하는 수만큼 구성할 수 있습니다.

NetApp ONTAP는 "다중 요소 인증(MFA)" System Manager와 SSH CLI 인증의 웹 기반 요구사항을 해결합니다.

NetApp의 랜섬웨어 방지 기능은 끊임없이 변화하는 위협 환경에서 안심할 수 있도록 제공합니다. 이 포괄적인 접근 방식은 현재의 랜섬웨어 변종을 방어할 뿐만 아니라 새로운 위협에 대응하여 데이터 인프라에 장기적인 보안을 제공합니다.

다른 보호 옵션에 대해 알아봅니다

- "Digital Advisor 랜섬웨어 방어"
- "Data Infrastructure Insights 스토리지 워크로드 보안"
- "FPolicy를 참조하십시오"
- "SnapLock 및 변조 방지 스냅샷"

랜섬웨어 복구 보장

NetApp은 랜섬웨어 공격이 발생할 경우 스냅샷 데이터의 복원을 보장합니다. 보장: 스냅샷 데이터 복원을 지원할 수 없는 경우 NetApp이 바로잡을 것입니다. 이 보장은 AFF A-Series, AFF C-Series, ASA 및 FAS 시스템을 새로 구매할 때 사용할 수 있습니다.

자세한 정보

- "복구 보장 서비스 설명"
- "랜섬웨어 복구 보장 블로그"..

관련 정보

- "NetApp 지원 사이트 리소스 페이지"
- "NetApp 제품 보안"

랜섬웨어 보호를 위해 **SnapLock** 및 변조 방지 스냅샷

NetApp의 Snap Arsenal에서 중요한 무기는 랜섬웨어 위협을 방어하는 데 매우 효과적인 것으로 입증된 SnapLock입니다. SnapLock는 무단 데이터 삭제를 방지함으로써 추가적인 보안 계층을 제공하여 악의적인 공격이 발생했을 때도 중요 데이터를 그대로 유지하고 액세스할 수 있도록 합니다.

SnapLock 규정 준수

SLC(SnapLock Compliance)는 데이터를 지워지지 않는 보호 기능을 제공합니다. SLC는 관리자가 스토리지를 다시 초기화하려고 시도해도 데이터가 삭제되는 것을 금지합니다. 다른 경쟁 제품과 달리 SnapLock Compliance는 해당 제품의 지원 팀을 통해 사회 공학 해킹에 취약하지 않습니다. SnapLock Compliance 볼륨으로 보호되는 데이터는 만료 날짜에 도달할 때까지 복구할 수 있습니다.

SnapLock를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "SnapLock 설명서"

변조 방지 스냅샷

변조 방지 스냅샷(TPS) 복사본은 악의적인 공격으로부터 데이터를 보호하는 편리하고 빠른 방법을 제공합니다. SnapLock Compliance와 달리 TPS는 일반적으로 사용자가 정해진 시간 동안 데이터를 보호하고 빠른 복구를 위해 로컬에 남겨둘 수 있거나 운영 시스템에서 데이터를 복제할 필요가 없는 운영 시스템에서 사용됩니다. TPS는 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 ONTAP 관리자가 기본 스냅샷을 삭제하지 못하도록 방지합니다. 스냅샷과 SnapLock Compliance 볼륨의 삭제 불가능한 특성이 같지는 않지만 볼륨이 SnapLock를 사용하도록 설정되어 있지 않더라도 스냅샷 삭제는 금지됩니다.

스냅샷을 무단 변경으로부터 보호하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"..

FPolicy 파일 차단

FPolicy는 원치 않는 파일이 엔터프라이즈급 스토리지 어플라이언스에 저장되지 않도록 차단합니다. 또한 FPolicy는 알려진 랜섬웨어 파일 확장자를 차단하는 방법을 제공합니다. 사용자는 여전히 홈 폴더에 대한 모든 액세스 권한을 가지고 있지만 FPolicy는 관리자가 차단으로 표시한 파일을 사용자가 저장할 수 없도록 합니다. 해당 파일이 MP3 파일 또는 알려진 랜섬웨어 파일 확장자인지 여부는 중요하지 않습니다.

FPolicy 기본 모드로 악성 파일 차단

NetApp FPolicy 기본 모드(파일 정책 이라는 이름의 진화)는 파일 확장 차단 프레임워크로, 원치 않는 파일 확장명이 사용자 환경에 유입되는 것을 차단할 수 있습니다. 10년 이상 ONTAP의 일부였으며 랜섬웨어로부터 보호하는 데 매우 유용합니다. 이 제로 트러스트 엔진은 액세스 제어 목록(ACL) 권한을 넘어서는 추가 보안 조치를 취하기 때문에 유용합니다.

ONTAP System Manager와 NetApp Console 에서는 3000개가 넘는 파일 확장자 목록을 참조할 수 있습니다.

> 일부 확장은 사용자의 환경에서 합법적일 수 있으며 이러한 확장을 차단하면 예기치 않은 문제가 발생할 수 있습니다. 기본 FPolicy를 구성하기 전에 환경에 적합한 목록을 생성하십시오.

FPolicy 기본 모드는 모든 ONTAP 라이센스에 포함되어 있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 3부 - 강력한 기본(무료) 툴인 ONTAP FPolicy"

FPolicy 외부 모드로 사용자 및 엔터티 행동 분석(UEBA)을 설정합니다

FPolicy 외부 모드는 파일 활동 알림 및 제어 프레임워크로, 파일 및 사용자 활동에 대한 가시성을 제공합니다. 이러한 알림은 외부 솔루션에서 AI 기반 분석을 수행하여 악의적인 행동을 감지하는 데 사용할 수 있습니다.

특정 작업이 수행되도록 허용하기 전에 FPolicy 서버의 승인을 기다리도록 FPolicy 외부 모드도 구성할 수 있습니다. 이와 같은 여러 정책을 클러스터에서 구성할 수 있으므로 유연성이 크게 향상됩니다.

> FPolicy 서버는 승인을 제공하도록 구성된 경우 FPolicy 요청에 응답해야 합니다. 그렇지 않으면 스토리지 시스템 성능이 저하될 수 있습니다.

FPolicy 외부 모드가 에 포함되어 "모든 ONTAP 라이센스"있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 4부 - FPolicy 외부 모드를 사용하는 UBA 및 ONTAP"

Data Infrastructure Insights 스토리지 워크로드 보안

SWS(스토리지 워크로드 보안)는 ONTAP 환경의 보안 태세, 복구 가능성 및 책임성을 크게 향상시키는 NetApp Data Infrastructure Insights 의 기능입니다. SWS는 사용자 중심 접근

방식을 취해 환경 내 모든 인증된 사용자의 모든 파일 활동을 추적합니다. 이 솔루션은 고급 분석을 사용하여 모든 사용자의 일반적이고 계절적인 접속 패턴을 파악합니다. 이러한 패턴은 랜섬웨어 서명이 없어도 의심스러운 동작을 빠르게 식별하는 데 사용됩니다.

SWS가 잠재적인 랜섬웨어나 데이터 삭제를 감지하면 다음과 같은 자동 조치를 취할 수 있습니다.

- 영향을 받는 볼륨의 스냅샷을 생성합니다.
- 악의적인 활동으로 의심되는 사용자 계정 및 IP 주소를 차단합니다.
- 관리자에게 알림을 보냅니다.

내부자 위협을 빠르게 차단하고 모든 파일 활동을 추적하기 위해 자동화된 조치를 취할 수 있기 때문에 SWS를 사용하면 랜섬웨어 이벤트에서 훨씬 더 쉽고 빠르게 복구할 수 있습니다. 사용자는 고급 감사 및 포렌식 도구가 내장되어 있어 공격의 영향을 받은 볼륨 및 파일, 공격이 발생한 사용자 계정 및 수행된 악의적인 작업을 즉시 확인할 수 있습니다. 자동 스냅샷은 손상을 완화하고 파일 복원을 가속화합니다.

ONTAP의 ARP(자율적 랜섬웨어 방어)의 경고도 SWS에서 볼 수 있으므로 ARP와 SWS를 모두 사용하여 랜섬웨어 공격으로부터 보호할 수 있는 단일 인터페이스를 제공합니다.

자세한 정보

- "NetApp Data Infrastructure Insights"

NetApp ONTAP 내장형 AI 기반 감지 및 응답 기능

랜섬웨어 위협이 점점 더 정교해짐에 따라 방어 메커니즘도 갖춰져야 합니다. NetApp의 ARP(자율 랜섬웨어 방어)는 ONTAP에 내장된 지능형 이상 징후 감지 기능을 갖춘 AI를 기반으로 합니다. 이를 통해 사이버 레질리언스에 또 다른 방어 계층을 추가합니다.

ARP 및 ARP/AI는 ONTAP 내장 관리 인터페이스인 System Manager를 통해 구성할 수 있으며 볼륨별로 활성화됩니다.

자율 랜섬웨어 보호(ARP)

9.10.1 이후 내장된 또 다른 네이티브 ONTAP 솔루션인 ARP(자율 랜섬웨어 방어)는 NAS 스토리지 볼륨 워크로드 파일 활동 및 데이터 엔트로피를 연구하여 잠재적 랜섬웨어를 자동으로 감지합니다. ARP는 관리자에게 전례 없는 온박스(on-box) 잠재적인 랜섬웨어 감지를 위한 실시간 감지, 인사이트 및 데이터 복구 지점을 제공합니다.

ARP를 지원하는 ONTAP 9.15.1 및 이전 버전의 경우 ARP는 일반적인 작업 부하 데이터 활동을 학습하기 위해 학습 모드에서 시작됩니다. 대부분의 환경에서 이 작업에는 7일이 걸릴 수 있습니다. 학습 모드가 완료되면 ARP가 자동으로

활성 모드로 전환되어 랜섬웨어가 될 수 있는 비정상적인 워크로드 활동을 찾기 시작합니다.

비정상적인 활동이 감지되면 자동 스냅샷이 즉시 생성되므로 감염된 데이터를 최소화하면서 공격 시간과 최대한 가까운 복원 지점을 제공합니다. 이와 동시에 관리자가 비정상적인 파일 활동을 확인할 수 있도록 자동 경고(구성 가능)가 생성되므로 해당 활동이 실제로 악의적인지 확인하고 적절한 조치를 취할 수 있습니다.

작업이 예상 작업량인 경우 관리자는 이를 가양성 작업으로 쉽게 표시할 수 있습니다. ARP는 이 변경 사항을 정상적인 워크로드 활동으로 인식하여 앞으로 발생할 수 있는 공격 대상으로 더 이상 플래그를 지정하지 않습니다.

ARP를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "자율 랜섬웨어 보호"

자율 랜섬웨어 방어**/AI(ARP/AI)**

ONTAP 9.15.1에서 기술 미리보기로 소개된 ARP/AI는 NAS 스토리지 시스템을 온박스 실시간 감지를 한 차원 높여줍니다. 새로운 AI 기반 감지 기술은 100만 개 이상의 파일과 알려진 다양한 랜섬웨어 공격에 대해 훈련됩니다. ARP에서 사용되는 신호 외에 ARP/AI는 헤더 암호화도 감지합니다. AI 출력 및 추가 신호를 통해 ARP/AI는 99% 이상의 검출 정확도를 제공할 수 있습니다. 이는 ARP/AI가 AAA 등급에서 가장 높은 등급을 받은 독립 테스트 연구소인 SE Labs에 의해 검증되었습니다.

모델을 지속적으로 클라우드에서 훈련하기 때문에 ARP/AI는 학습 모드가 필요하지 않습니다. 이 기능은 켜지는 순간 활성화됩니다. 또한 지속적인 훈련은 새로운 랜섬웨어 공격이 발생했을 때 ARP/AI가 항상 검증된다는 것을 의미합니다. ARP/AI에는 모든 고객에게 새로운 매개 변수를 제공하여 랜섬웨어 탐지를 최신 상태로 유지하는 자동 업데이트 기능도 제공됩니다. ARP의 다른 모든 탐지, 인사이트 및 데이터 복구 지점 기능은 ARP/AI에 대해 유지됩니다.

ARP/AI를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "블로그:NetApp의 AI 기반 실시간 랜섬웨어 감지 솔루션은 AAA 등급을 획득했습니다"

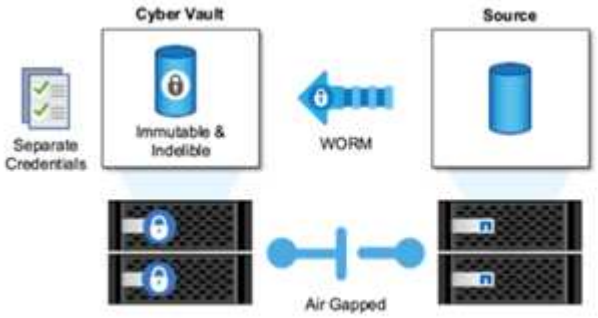
ONTAP의 사이버 보관을 이용한 에어갭 **WORM** 보호

NetApp의 사이버 소산 접근 방식은 논리적으로 에어갭 사이버 틈새를 위해 특별 제작된 참조 아키텍처입니다. 이 접근 방식은 보안 강화 및 SnapLock 같은 규정 준수 기술을 활용하여 변경 불가능하며 지워지지 않는 스냅샷을 허용합니다.

SnapLock Compliance과 논리적 격차가 있는 사이버 소산

공격자가 백업 사본을 폐기하고 경우에 따라 암호화하는 경향이 증가하고 있습니다. 따라서 사이버 보안 업계의 많은 기업들이 전반적인 사이버 복원력 전략의 일환으로 에어 갭 백업을 사용하도록 권장합니다.

문제는 기존 공기 격차(테이프 및 오프라인 미디어)가 복원 시간을 크게 증가시켜 가동 중지 시간과 전반적인 관련 비용을 증가시킬 수 있다는 것입니다. 에어 갭 솔루션에 대한 보다 현대적인 접근 방식도 문제가 될 수 있습니다. 예를 들어, 새 백업 복사본을 받기 위해 백업 볼트가 일시적으로 열렸다가 기본 데이터에 대한 네트워크 연결을 끊고 다시 한 번 "공기 차단"하는 경우 공격자는 임시 열기의 이점을 활용할 수 있습니다. 연결이 온라인 상태일 때 공격자는 데이터를 손상시키거나 파괴할 수 있습니다. 이러한 유형의 구성은 일반적으로 원치 않는 복잡성을 가중시킵니다. 논리적 공기 격차는 백업을 온라인 상태로 유지하면서 동일한 보안 보호 원칙을 가지고 있기 때문에 전통적인 또는 현대적인 공기 격차의 훌륭한 대안이 됩니다. NetApp를 사용하면 논리적 공기 가핑을 사용하여 테이프 또는 디스크 공기 게핑의 복잡성을 해결할 수 있으며, 이 작업은 변경 불가능한 스냅샷과 NetApp SnapLock Compliance로 달성할 수 있습니다.



NetApp은 10년 이상 SnapLock 기능을 발표하여 HIPAA(Health Insurance Portability and Accountability Act), 사베인즈 옥슬리(Sarbanes-Oxley) 및 기타 규정 데이터 규정 준수 요구 사항을 해결했습니다. 또한 기본 스냅샷을 SnapLock 볼륨에 저장하여 복사본을 WORM에 커밋하여 삭제를 방지할 수 있습니다. SnapLock 라이센스 버전은 SnapLock Compliance 및 SnapLock Enterprise의 두 가지입니다. 랜섬웨어 보호를 위해 NetApp은 ONTAP 관리자 또는 NetApp 지원팀에서도 스냅샷이 잠겨 있고 삭제할 수 없는 특정 보존 기간을 설정할 수 있으므로 SnapLock Compliance를 권장합니다.

자세한 정보

- "블로그: ONTAP 사이버 소산 개요"

변조 방지 스냅샷

SnapLock Compliance를 논리적 AIR Gap으로 활용하면 공격자가 백업 복사본을 삭제하지 못하도록 완벽하게 보호할 수 있지만, SnapVault를 사용하여 스냅샷을 2차 SnapLock 지원 볼륨으로 이동해야 합니다. 결과적으로 많은 고객이 네트워크를 통한 보조 스토리지에 이 구성을 구현합니다. 따라서 기본 스토리지에서 기본 볼륨 스냅샷을 복원하는 것보다 복원 시간이 더 길 수 있습니다.

ONTAP 9.12.1부터 무단 변경 방지 스냅샷은 기본 스토리지 및 기본 볼륨의 스냅샷에 대해 SnapLock Compliance 수준에 가까운 보호 기능을 제공합니다. SnapVault를 사용하여 스냅샷을 보조 SnapLocked 볼륨에 볼트할 필요가 없습니다. 변조 방지 스냅샷은 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 전체 ONTAP 관리자가 기본 스냅샷을 삭제하지 못하도록 방지합니다. 따라서 복원 시간이 빨라지고 무단 변경 방지 및 보호된 스냅샷으로 FlexClone 볼륨을 백업할 수 있습니다. 기존의 SnapLock Compliance 저장 스냅샷으로는 할 수 없는 작업입니다.

SnapLock Compliance 스냅샷과 무단 변경 방지 스냅샷의 주요 차이점은 만료 날짜에 도달하지 않은 SnapLock Compliance 볼륨에 저장된 스냅샷이 있을 경우 SnapLock Compliance에서는 ONTAP 어레이를 초기화하고 초기화할 수 없다는 것입니다. 스냅샷을 무단 변경으로부터 보호하려면 SnapLock Compliance 라이센스가 필요합니다.

자세한 정보

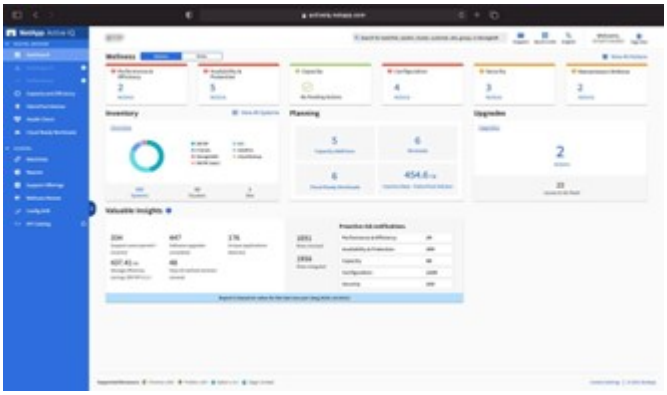
- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"

Digital Advisor 랜섬웨어 방어

Active IQ 기반 Digital Advisor는 실행 가능한 인텔리전스를 통해 최적의 데이터 관리를 지원하여 NetApp 스토리지의 사전 예방적 관리 및 최적화를 간소화합니다. 다양한 설치 기반에서 수집된 원격 측정 데이터를 활용하여 고급 AI 및 ML 기술을 통해 스토리지 환경의 위험을 줄이고 성능 및 효율성을 개선할 수 있는 기회를 발견합니다.

이 "NetApp 디지털 자문" 방법은 도움이 될 뿐만 "보안 취약점을 제거합니다" 아니라 랜섬웨어로부터 보호하는 것과 관련된 통찰력과 지침도 제공합니다. 전용 웰니스 카드는 필요한 조치와 해결된 위험을 보여줍니다. 따라서 시스템이

이러한 모범 사례 권장 사항을 충족하는지 확인할 수 있습니다.



랜섬웨어 방어 웰빙 페이지에서 추적된 위험 및 작업은 다음과 같습니다.

- 볼륨 스냅샷 수가 적기 때문에 잠재적인 랜섬웨어 방어가 줄어듭니다.
- NAS 프로토콜용으로 구성된 모든 SVM(스토리지 가상 머신)에 FPolicy가 사용되지 않는다.

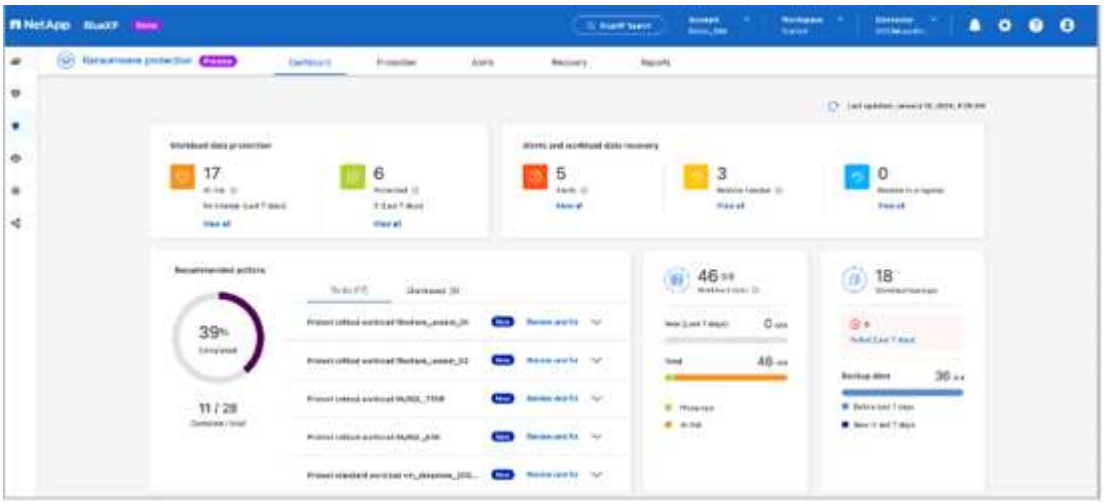
랜섬웨어 방어의 실제 적용 사례를 보려면 을 참조하십시오."디지털 자문업체"

NetApp 랜섬웨어 보호로 포괄적인 복원력 제공

랜섬웨어는 확산을 막고 비용이 많이 드는 가동 중지 시간을 피하기 위해 가능한 한 일찍 감지하는 것이 중요합니다. 그러나 효과적인 랜섬웨어 탐지 전략에는 단일 계층 이상의 보호가 포함되어야 합니다. NetApp의 랜섬웨어 보호는 NetApp Console 사용하여 데이터 서비스로 확장되는 실시간 온박스 기능과 사이버 보관을 위한 격리된 계층형 솔루션을 포함하는 포괄적인 접근 방식을 취합니다.

NetApp 랜섬웨어 보호

NetApp Console 포괄적이고 워크로드 중심의 랜섬웨어 방어를 지능적으로 조율하는 단일 제어 평면입니다. NetApp 랜섬웨어 보호는 ARP, FPolicy, 변조 방지 스냅샷과 같은 ONTAP 의 강력한 사이버 복원력 기능과 NetApp Backup and Recovery 와 같은 NetApp 데이터 서비스를 통합합니다. 또한 단일 UI를 통해 종단 간 방어를 제공하기 위해 자동화된 워크플로를 통해 권장 사항과 지침을 추가합니다. 공격이 발생한 경우 비즈니스를 운영하는 애플리케이션이 보호되고 최대한 빨리 복구될 수 있도록 워크로드 수준에서 작동합니다.



고객 이점:

- 랜섬웨어 대비 지원을 통해 운영 오버헤드를 줄이고 효율성을 높일 수 있습니다
- AI/ML을 통한 이상 징후 탐지는 정확성을 높이고 위험을 억제하기 위한 더 빠른 응답을 제공합니다
- 안내된 애플리케이션 정합성이 보장된 복원을 통해 몇 분 내에 워크로드를 더 쉽게 복구할 수 있습니다

"NetApp 랜섬웨어 보호"NIST 기능을 더 쉽게 구현할 수 있습니다.

- NetApp 스토리지의 데이터를 자동으로 검색 * 하고 우선 순위를 정할 수 있습니다 *.
- * 상위 워크로드 데이터 백업, 변경 불가, 보안 구성, 악성 파일 차단 및 다양한 보안 도메인에 대한 원 클릭 보호 *.
- * 차세대 AI 기반 이상 징후 감지 * 를 사용하여 * 랜섬웨어를 최대한 빠르게 * 감지합니다 *
- 응답 및 워크플로우 자동화, 최고의 * SIEM 및 XDR 솔루션 * 과의 통합
- 간소화된 * 오케스트레이션 * 을 통해 데이터를 빠르게 복원하여 애플리케이션 가동 시간을 단축합니다.
- 랜섬웨어 보호 * 전략 * 및 * 정책 * 을 구현하고 * 결과를 모니터링 * 하십시오.

NetApp와 제로 트러스트

NetApp와 제로 트러스트

제로 트러스트는 일반적으로 마이크로 코어 및 주변 장치(MCAP)를 설계하여 데이터, 서비스, 애플리케이션 또는 자산을 세그먼트 게이트웨이라고 하는 제어 기능으로 보호하는 네트워크 중심 접근 방식이었습니다. NetApp ONTAP는 제로 트러스트에 대한 데이터 중심 접근 방식을 취하고 있습니다. 제로 트러스트는 스토리지 관리 시스템이 세분화 게이트웨이가 되어 고객 데이터의 액세스 보호 및 모니터링을 수행합니다. 특히 FPolicy Zero Trust 엔진과 FPolicy 파트너 에코시스템은 정상 및 비정상적인 데이터 액세스 패턴을 세부적으로 이해하고 내부자 위협을 식별하기 위한 제어 센터가 됩니다.

2024년 7월부터 NetApp과 제로 트러스트: 데이터 중심의 제로 트러스트 모델 활성화 _ 의 내용이 docs.netapp.com 에서 제공됩니다. 이 모델은 이전에 PDF로 게시되었습니다.

데이터는 조직의 가장 중요한 자산입니다. 2022년 기준 내부자 위협은 데이터 침해의 18%가 원인입니다. "Verizon 데이터 침해 조사 보고서" 조직은 NetApp ONTAP 데이터 관리 소프트웨어를 사용하여 데이터에 관한 업계 최고 수준의 제로 트러스트 제어를 구현하여 경계를 강화할 수 있습니다.

Zero Trust란 무엇입니까??

제로 트러스트 모델은 Forrester Research의 John Kindervag에 의해 처음 개발되었습니다. 네트워크 보안은 외부에서 들어오는 것이 아니라 내부 외부로부터의 네트워크 보안을 지향합니다. 인사이드아웃 제로 트러스트 방식에서는 마이크로코어 및 경계(MCAP)를 식별합니다. MCAP는 포괄적인 제어 집합으로 보호할 데이터, 서비스, 애플리케이션 및 자산의 내부 정의입니다. 안전한 외주개념은 더 이상 유효하지 않습니다. 신뢰할 수 있고 경계를 통해 성공적으로 인증할 수 있는 엔터티는 조직이 공격에 취약해질 수 있습니다. 내부자는 정의상 이미 보안 경계의 내부에 있습니다. 직원, 계약업체 및 파트너는 내부자이며 조직의 인프라 내에서 역할을 수행하기 위해서는 적절한 제어하에 작업을 수행할 수 있어야 합니다.

제로 트러스트는 2019년 9월 DoD에 약속을 제공하는 기술로 언급되었습니다. "FY19-23 DoD 디지털 현대화 전략" 제로 트러스트를 데이터 침해를 막기 위해 아키텍처 전체에 보안을 통합하는 사이버 보안 전략인 "로 정의합니다. 이

데이터 중심 보안 모델은 신뢰할 수 있거나 신뢰할 수 없는 네트워크, 장치, 사용자 또는 프로세스의 개념을 없애고, 최소 권한 액세스라는 개념 하에서 인증 및 권한 부여 정책을 가능하게 하는 다중 속성 기반 신뢰 수준으로 전환합니다. 제로 트러스트를 구현하려면 기존 인프라를 사용하여 보안을 구현하는 방법을 보다 간단하고 효율적인 방식으로 설계하고 방해받지 않는 운영을 가능하게 해야 합니다."

2020년 8월 NIST 발표 "SPECIAL Pub 800-207 제로 트러스트 아키텍처" (ZTA), ZTA는 네트워크 위치가 더 이상 리소스의 보안 태세의 주요 구성 요소로 간주되지 않기 때문에 네트워크 세그먼트가 아닌 리소스 보호에 중점을 둡니다. 리소스는 데이터와 컴퓨팅입니다. ZTA 전략은 엔터프라이즈 네트워크 설계자를 위한 것입니다. ZTA는 원래 Forrester 개념에서 몇 가지 새로운 용어를 소개합니다. PDP(Policy Decision Point)와 PEP(Policy Enforcement Point)라는 보호 메커니즘은 Forrester 세그멘테이션 게이트웨이와 유사합니다. ZTA는 네 가지 배포 모델을 도입합니다.

- 장치 에이전트 또는 게이트웨이 기반 배포
- 독립 기반 구축(Forrester MCAP와 다소 유사함)
- 리소스 포털 기반 배포
- 장치 응용 프로그램 샌드박싱

이 설명서의 목적상 당사는 NIST ZTA 대신 Forrester Research의 개념과 용어를 사용합니다.

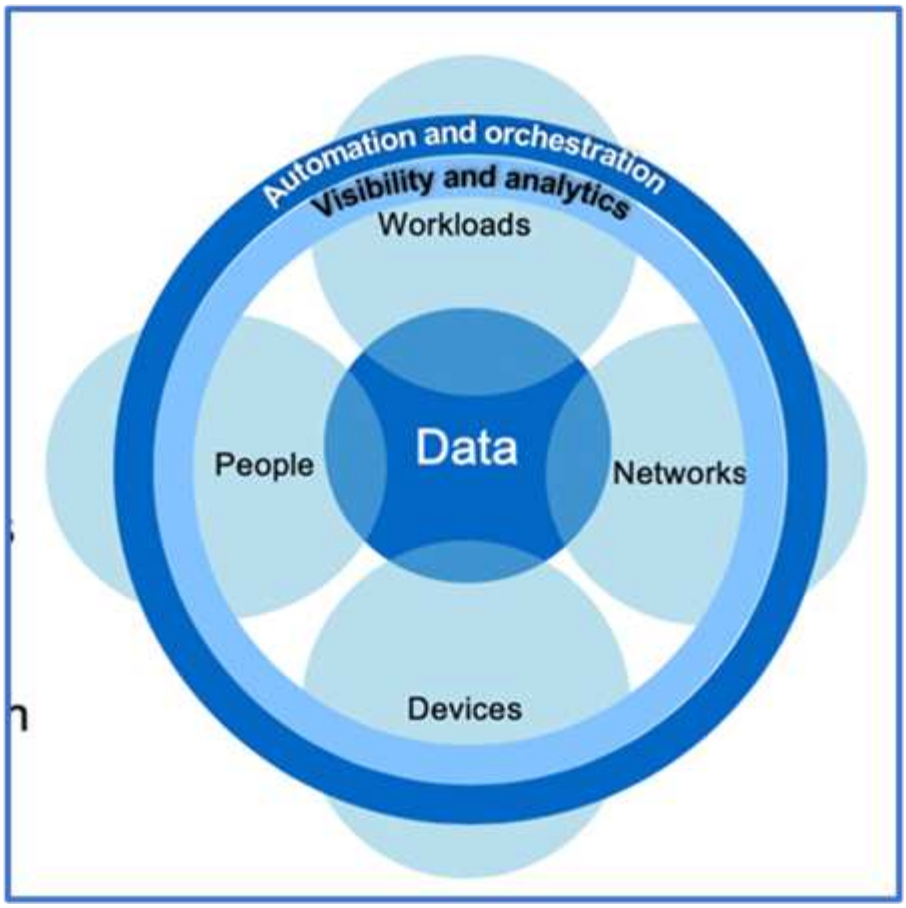
보안 리소스

취약성 및 사고 보고, NetApp 보안 응답 및 고객 기밀성에 대한 자세한 내용은 를 참조하십시오 "NetApp 보안 포털".

ONTAP로 제로 트러스트에 대한 데이터 중심 접근 방식 설계

제로 트러스트 네트워크는 데이터 중심 접근 방식으로 정의되며, 보안 제어는 데이터와 최대한 가까운 위치에 있어야 합니다. ONTAP의 기능을 NetApp FPolicy 파트너 에코시스템과 결합하여 데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공할 수 있습니다.

ONTAP는 NetApp의 보안이 풍부한 데이터 관리 소프트웨어이며, FPolicy 제로 트러스트 엔진은 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다.



제로 트러스트 데이터 중심 **MCAP** 설계

데이터 중심의 제로 트러스트 MCAP를 설계하려면 다음 단계를 따르십시오.

1. 모든 조직 데이터의 위치를 식별합니다.
2. 데이터를 분류합니다.
3. 더 이상 필요하지 않은 데이터는 안전하게 폐기합니다.
4. 데이터 분류에 액세스해야 하는 역할을 이해합니다.
5. 최소 권한 원칙을 적용하여 액세스 제어를 적용합니다.
6. 관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오.
7. 유휴 데이터와 사용 중인 데이터에 암호화 사용
8. 모든 액세스를 모니터링하고 기록합니다.
9. 의심스러운 액세스 또는 행동을 경고합니다.

모든 조직 데이터의 위치를 식별합니다

ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석에 대한 자세한 내용은 모든 액세스 모니터링 및 로그에서 설명합니다. 데이터가 어디에 있고 누가 데이터에 액세스할 수 있는지 모르는 경우 사용자 행동 분석을 통해 경험적 관찰을 통해 분류 및 정책을 수립할 수 있습니다.

데이터를 분류합니다

Zero Trust 모델의 용어로, 데이터 분류에는 유해 데이터를 식별하는 것이 포함됩니다. 유해 데이터는 조직 외부에 노출될 의도가 없는 민감한 데이터입니다. 유해 데이터가 공개되면 규정 준수에 문제가 생기고 조직의 평판이 손상될 수 있습니다. 규정 준수 측면에서 독성 데이터에는 카드 소지자 데이터가 포함됩니다. "PCI-DSS(Payment Card Industry Data Security Standard)" , EU의 개인 데이터 "일반 데이터 보호 규정(GDPR)" 또는 의료 데이터 "HIPAA(Health Insurance Portability and Accountability Act)" . NetApp 사용할 수 있습니다 "NetApp Data Classification" (이전 명칭: Cloud Data Sense)는 데이터를 자동으로 스캔, 분석, 분류하는 AI 기반 툴킷입니다.

더 이상 필요하지 않은 데이터는 안전하게 폐기합니다

조직의 데이터를 분류한 후 일부 데이터가 더 이상 필요하지 않거나 조직의 기능과 관련이 없다는 것을 알게 될 수 있습니다. 불필요한 데이터의 보유는 책임이며, 그러한 데이터는 삭제되어야 한다. 데이터를 암호화하여 삭제하는 고급 메커니즘은 저장된 데이터 암호화의 보안 삭제 설명을 참조하십시오.

데이터 분류에 액세스해야 하는 역할을 이해하고 액세스 제어를 적용하기 위해 최소 권한 원칙을 적용합니다

중요한 데이터에 대한 액세스를 매핑하고 최소 권한 원칙을 적용하면 조직 내 사용자가 작업을 수행하는 데 필요한 데이터만 액세스할 수 있습니다. 이 프로세스에는 역할 기반 액세스 제어가 포함되는데, 이 제어는 ("RBAC"데이터 액세스 및 관리 액세스에 적용됩니다.

ONTAP를 사용하면 스토리지 가상 머신(SVM)을 ONTAP 클러스터 내의 테넌트가 조직 데이터 액세스를 분할하는 데 사용할 수 있습니다. RBAC는 데이터 액세스뿐만 아니라 SVM에 대한 관리 액세스에도 적용할 수 있습니다. RBAC는 클러스터 관리 레벨에서 적용할 수도 있습니다.

RBAC와 더불어 MAV(ONTAP)를 사용하면 한 명 이상의 관리자가 또는 같은 명령을 승인하도록 할 수 있습니다 "다중 관리자 인증" `volume delete` `volume snapshot delete`. MAV가 활성화되면 MAV를 수정하거나 사용하지 않도록 하려면 MAV 관리자의 승인이 필요합니다.

스냅샷을 보호하는 또 다른 방법은 ONTAP를 "스냅샷 잠금"사용하는 것입니다. 스냅샷 잠금은 볼륨 스냅샷 정책에 대한 보존 기간에 수동 또는 자동으로 스냅샷을 지울 수 없는 SnapLock 기능입니다. 스냅샷 잠금은 무단 변경 방지 스냅샷 잠금이라고도 합니다. 스냅샷 잠금의 목적은 악의적인 관리자 또는 신뢰할 수 없는 관리자가 운영 및 보조 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 하는 것입니다. 랜섬웨어에 의해 손상된 볼륨을 복원하기 위해 기본 시스템에서 잠긴 스냅샷의 신속한 복구를 수행할 수 있습니다.

관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오

클러스터 관리 RBAC 외에도 "다단계 인증(MFA)" ONTAP 웹 관리 액세스 및 SSH(Secure Shell) 명령줄 액세스용으로 구축할 수 있습니다. 관리 액세스를 위한 MFA는 미국 공공 부문 조직 또는 PCI-DSS를 준수해야 하는 조직의 요구 사항입니다. MFA를 사용하면 공격자가 사용자 이름과 암호만 사용하여 계정을 손상시킬 수 없습니다. MFA를 인증하려면 두 개 이상의 독립적인 요소가 필요합니다. 2단계 인증의 예로는 개인 키와 같이 사용자가 소유한 것과 암호 등 사용자가 알고 있는 것을 들 수 있습니다. ONTAP System Manager 또는 ActiveIQ Unified Manager에 대한 관리 웹 액세스는 SAML(Security Assertion Markup Language) 2.0을 통해 활성화됩니다. SSH 명령줄 액세스는 공개 키 및 암호와 함께 연결된 2단계 인증을 사용합니다.

ONTAP의 ID 및 액세스 관리 기능을 사용하여 API를 통해 사용자 및 시스템 액세스를 제어할 수 있습니다.

- 사용자:
  - 인증 및 권한 부여 SMB 및 NFS용 NAS 프로토콜 기능을 사용합니다.
  - * 감사 * 액세스 및 이벤트의 syslog. 인증 및 권한 부여 정책을 테스트하기 위한 CIFS 프로토콜에 대한 자세한 감사 로깅 파일 수준에서 세부적인 NAS 액세스에 대한 FPolicy 감사
- 장치:

- * 인증. * API 액세스를 위한 인증서 기반 인증.
- * 승인. * 기본 또는 맞춤형 역할 기반 액세스 제어(RBAC)
- * 감사 * 수행한 모든 작업의 syslog.

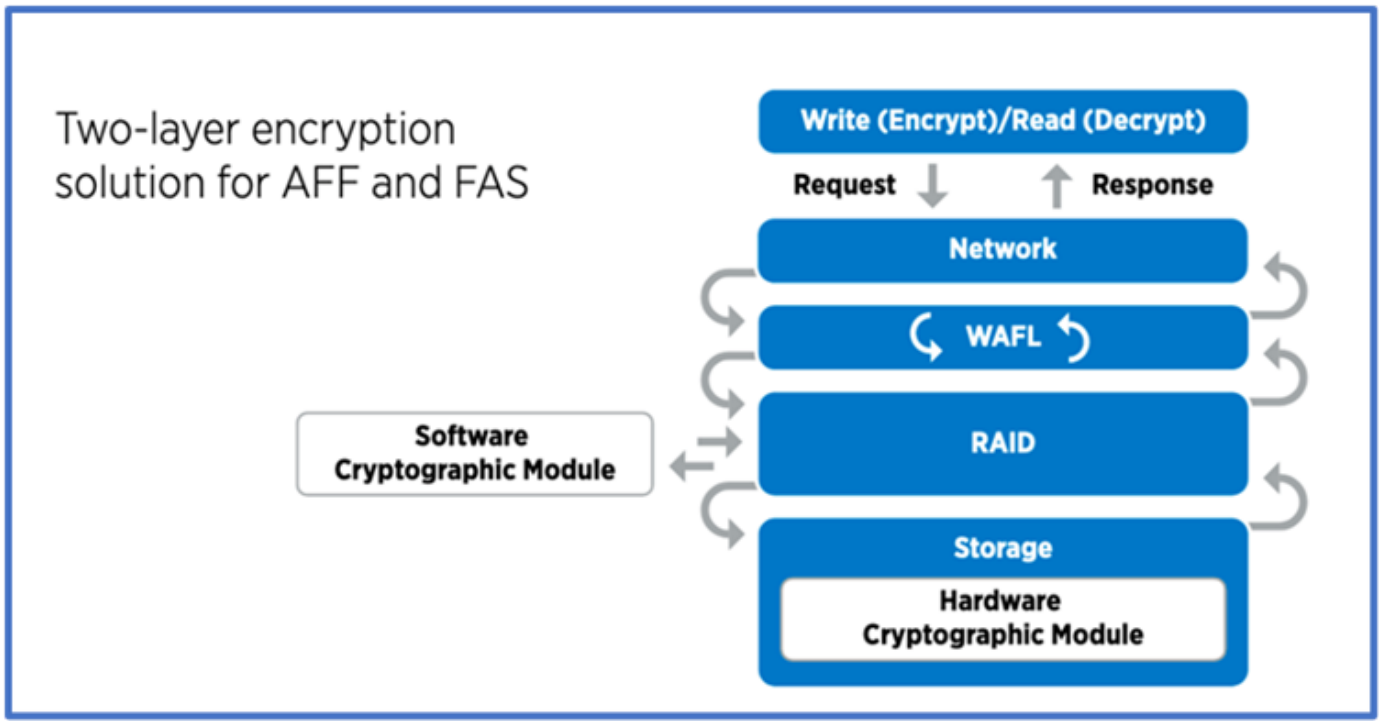
유휴 데이터와 사용 중인 데이터에 암호화 사용

유휴 데이터의 암호화

조직에서 드라이브의 용도를 변경하거나 결함 있는 드라이브를 반환하거나 판매 또는 거래하여 대용량 드라이브로 업그레이드하는 경우, 스토리지 시스템의 위험과 인프라 격차를 줄이기 위한 새로운 요구사항이 있습니다. 스토리지 엔지니어는 데이터의 관리자이자 운영자로서 라이프사이클 전반에서 데이터를 안전하게 관리하고 유지해야 합니다. "NetApp 스토리지 암호화(NSE) 및 AMP, #44, NetApp 볼륨 암호화(NVE) 및 AMP, #44, NetApp 애그리게이트 암호화" 독성 여부와 관계없이 일상 작업에 영향을 주지 않고 유휴 데이터를 항상 암호화할 수 있도록 지원합니다. "NSE를 선택합니다" 는 FIPS 140-2 레벨 2 검증된 자체 암호화 드라이브를 사용하는 ONTAP 하드웨어 "사용되지 않는 데이터" 솔루션입니다. "NVE와 NAE" 는 를 사용하는 ONTAP 소프트웨어 "사용되지 않는 데이터" "FIPS 140-2 Level 1 검증 NetApp 암호화 모듈"솔루션입니다. NVE와 NAE에서는 하드 드라이브 또는 Solid State Drive를 유휴 데이터 암호화에 사용할 수 있습니다. 또한 NSE 드라이브를 사용하여 암호화 이중화와 추가 보안을 제공하는 네이티브 계층화된 암호화 솔루션을 제공할 수 있습니다. 한 계층이 침해되더라도 두 번째 계층은 여전히 데이터를 보호합니다. 이러한 기능을 통해 ONTAP은 에 대한 유리한 위치를 점할 수 "양자 지원 암호화"있습니다.

NVE는 기밀 파일이 기밀이 아닌 볼륨에 작성될 때 데이터 유출로부터 독성 데이터를 암호화 방식으로 제거하는 기능을 "안전한 제거" 제공합니다.

ONTAP에 내장된 키 관리자인 를 "온보드 키 관리자(OKM)"사용하거나 "승인됨" , NSE 및 NVE와 함께 타사 "외부 키 관리자" 를 사용하여 키 자료를 안전하게 저장할 수 있습니다.



위의 그림에서 볼 수 있듯이 하드웨어 및 소프트웨어 기반 암호화를 결합할 수 있습니다. 이 기능으로 인해 는 "기밀 프로그램을 위한 NSA의 상용 솔루션에 대한 ONTAP 검증" 최고 비밀 데이터를 저장할 수 있게 되었습니다.

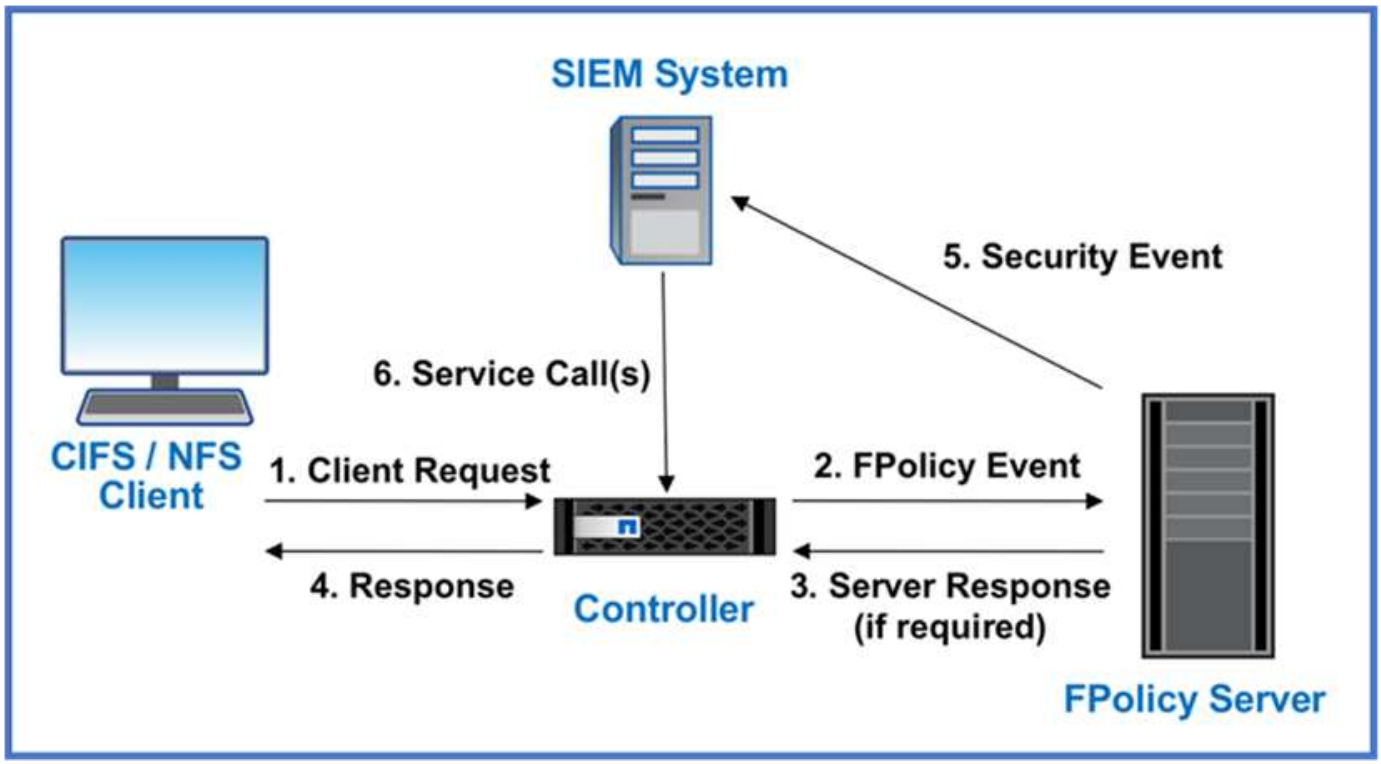
전송 중인 데이터 암호화

ONTAP의 전송 중인 데이터 암호화는 사용자 데이터 액세스 및 제어 플레인 액세스를 보호합니다. 사용자 데이터 액세스는 Microsoft CIFS 공유 액세스의 경우 SMB 3.0 암호화 또는 NFS Kerberos 5의 경우 krb5P로 암호화될 수 있습니다. CIFS, NFS 및 iSCSI에 대해 사용자 데이터 액세스를 암호화할 수도 "IPsec을 선택합니다" 있습니다. 컨트롤 플레인 액세스는 TLS(Transport Layer Security)로 암호화됩니다. ONTAP는 제어 플레인 액세스를 위한 규정 준수 모드를 제공하여 "FIPS 를 참조하십시오"FIPS 승인 알고리즘을 활성화하고 FIPS가 승인되지 않은 알고리즘을 비활성화합니다. 데이터 복제는 로 암호화됩니다. "클러스터 피어 암호화" ONTAP SnapVault 및 SnapMirror 기술에 대한 암호화를 제공합니다.

모든 액세스를 모니터링하고 기록합니다

RBAC 정책을 적용한 후에는 활성 모니터링, 감사 및 알림을 배포해야 합니다. NetApp ONTAP의 FPolicy 제로 트러스트 엔진을 과 결합하여 "NetApp FPolicy 파트너 에코시스템"데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공합니다. NetApp ONTAP는 보안이 풍부한 데이터 관리 소프트웨어이며 "FPolicy를 참조하십시오" , 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다. ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석을 사용하여 정상적인 패턴에서 벗어난 의심스럽거나 잘못된 데이터 액세스를 경고하고 필요한 경우 액세스를 거부하기 위한 조치를 취할 수 있습니다.

FPolicy 파트너는 사용자 행동 분석을 넘어 머신 러닝(ML) 및 인공 지능(AI)으로 이동하여 이벤트 충실도를 높이고 오탐률을 줄이고 있습니다. 모든 이벤트는 syslog 서버 또는 ML 및 AI를 활용할 수 있는 SIEM(Security Information and Event Management) 시스템에 로깅해야 합니다.



NetApp의 "DII 스토리지 워크로드 보안" 클라우드와 온프레미스 ONTAP 스토리지 시스템 모두에서 FPolicy 인터페이스와 사용자 행동 분석을 활용하여 악의적인 사용자 행동에 대한 실시간 알림을 제공합니다. 스토리지 워크로드 보안은 고급 머신 러닝과 이상 감지를 통해 악의적이거나 손상된 사용자가 조직 데이터를 오용하는 것을 방지합니다. 스토리지 워크로드 보안은 랜섬웨어 공격이나 기타 악의적인 행위를 식별하고 스냅샷을 호출하고 악의적인 사용자를 격리할 수 있습니다. 스토리지 워크로드 보안에는 사용자 및 엔터티 활동을 매우 자세히 볼 수 있는 포렌식 기능도

있습니다. 스토리지 워크로드 보안은 NetApp Data Infrastructure Insights 의 일부입니다.

ONTAP에는 스토리지 워크로드 보안뿐만 아니라 (ARP)라고 하는 온보드 랜섬웨어 감지 기능이 "자율 랜섬웨어 보호" 있습니다. ARP는 머신 러닝을 사용하여 비정상적인 파일 활동이 랜섬웨어 공격이 진행 중임을 나타내고 스냅샷을 호출하고 관리자에게 경고를 보냅니다. 스토리지 워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 외부 NetApp 보안 자동화 및 오케스트레이션 제어

자동화를 통해 최소한의 인적 지원만으로 프로세스 또는 절차를 수행할 수 있습니다. 조직은 자동화를 통해 제로 트러스트 구축을 수동 절차를 훨씬 넘어 확장할 수 있으므로 자동화되는 악의적인 활동을 방지할 수 있습니다.

Ansible은 오픈 소스 소프트웨어 프로비저닝, 구성 관리 및 애플리케이션 배포 툴입니다. 많은 유닉스와 유사한 시스템에서 실행되며, 유닉스와 유사한 시스템과 Microsoft Windows를 모두 구성할 수 있습니다. 시스템 구성을 설명하는 고유한 선언적 언어가 포함되어 있습니다. Ansible은 Michael DeHaan이 작성했으며 2015년에 Red Hat에 인수되었습니다. Ansible은 에이전트가 없습니다. SSH 또는 Windows 원격 관리를 통해 일시적으로 원격으로 연결하여 원격 PowerShell 실행 허용 을 수행할 수 있습니다. NetApp은 그 이상을 개발했으며 "ONTAP 소프트웨어용 Ansible 모듈 150개"Ansible 자동화 프레임워크와 추가적인 통합을 가능하게 했습니다. NetApp용 Ansible 모듈은 원하는 상태를 정의하고 타겟 NetApp 환경에 전달하는 방법에 관한 일련의 지침을 제공합니다. 이들 모듈은 라이센스 설정, 애그리게이트 및 스토리지 가상 머신 생성, 볼륨 생성, 스냅샷 복원 등의 작업을 지원할 목적으로 개발되었습니다. Ansible 역할은 NetApp DoD UC(Unified Capabilities "GitHub에 게시되었습니다") 배포 가이드에 따라 다릅니다.

사용자는 사용 가능한 모듈 라이브러리를 통해 쉽게 Ansible 플레이북을 개발하고 고유한 애플리케이션 및 비즈니스 요구사항에 맞게 맞춤화하여 일상적인 작업을 자동화할 수 있습니다. 플레이북을 작성한 후 특정 작업을 수행하도록 실행하면 시간이 절약되고 생산성이 향상됩니다. NetApp은 직접 사용하거나 필요에 맞게 맞춤화할 수 있는 샘플 플레이북을 마련하여 공유했습니다.

Data Infrastructure Insights 는 전체 인프라에 대한 가시성을 제공하는 인프라 모니터링 도구입니다. Data Infrastructure Insights 사용하면 퍼블릭 클라우드 인스턴스와 프라이빗 데이터 센터를 포함한 모든 리소스를 모니터링하고, 문제를 해결하고, 최적화할 수 있습니다. Data Infrastructure Insights 해결에 걸리는 평균 시간을 90%까지 단축하고 클라우드 문제의 80%가 최종 사용자에게 영향을 미치지 않도록 예방할 수 있습니다. 또한 실행 가능한 인텔리전스로 데이터를 보호함으로써 클라우드 인프라 비용을 평균 33% 절감하고 내부 위협에 대한 노출도 줄일 수 있습니다. Data Infrastructure Insights 의 스토리지 워크로드 보안 기능을 사용하면 AI와 ML을 활용한 사용자 행동 분석을 통해 내부 위협으로 인해 비정상적인 사용자 행동이 발생할 때 경고를 받을 수 있습니다. ONTAP 의 경우, 스토리지 워크로드 보안은 Zero Trust FPolicy 엔진을 활용합니다.

제로 트러스트 및 하이브리드 클라우드 구축

NetApp 은 하이브리드 클라우드의 데이터 권위자입니다. NetApp Amazon Web Services(AWS), Microsoft Azure, Google Cloud 및 기타 주요 클라우드 공급업체와 협력하여 온프레미스 데이터 관리 시스템을 하이브리드 클라우드로 확장하기 위한 다양한 옵션을 제공합니다. NetApp 하이브리드 클라우드 솔루션은 온프레미스 ONTAP 시스템 및 ONTAP Select 소프트웨어 정의 스토리지에서 사용할 수 있는 것과 동일한 Zero Trust 보안 제어를 지원합니다.

AWS(FSxN), Google Cloud(GCNV), Microsoft Azure용 Azure NetApp Files 등 엔터프라이즈급 클라우드 기반 파일 서비스를 사용하면 일반적인 CAPEX 제약 없이 퍼블릭 클라우드에서 용량을 쉽게 확장할 수 있습니다. 분석 및 DevOps와 같은 데이터 집약적 워크로드에 적합한 이러한 클라우드 데이터 서비스는 NetApp 의 탄력적인 온디맨드

스토리지 서비스와 ONTAP 데이터 관리를 완벽하게 관리되는 제품으로 결합합니다.

ONTAP NetApp SnapMirror 데이터 복제 소프트웨어를 통해 온프레미스 ONTAP 시스템과 AWS, Google Cloud 또는 Azure 스토리지 환경 간에 데이터를 이동할 수 있도록 합니다.

속성 기반 액세스 제어

ONTAP로 속성 기반 액세스 제어

9.12.1부터 ONTAP를 NFSv4.2 보안 레이블 및 확장 속성(xattrs)으로 구성하여 특성 및 ABAC(속성 기반 액세스 제어)를 포함하는 RBAC(역할 기반 액세스 제어)를 지원할 수 있습니다.

ABAC는 사용자 속성, 리소스 속성 및 환경 조건을 기반으로 사용 권한을 정의하는 권한 부여 전략입니다. ONTAP와 NFS v4.2 보안 레이블 및 xattrs의 통합은 NIST 특별 간행물 800-162에 명시된 ABAC 솔루션에 대한 NIST 표준을 준수합니다.

NFS v4.2 보안 레이블 및 xattrs를 사용하여 파일에 사용자 정의 속성 및 레이블을 할당할 수 있습니다. ONTAP는 ABAC 지향 ID 및 액세스 관리 소프트웨어와 통합하여 이러한 속성 및 레이블을 기반으로 세분화된 파일 및 폴더 액세스 제어 정책을 적용할 수 있습니다.

관련 정보

- "ABAC에 대한 ONTAP의 접근 방식"
- "NFS in NetApp ONTAP: 모범 사례 및 구축 가이드"

ONTAP의 ABAC(속성 기반 액세스 제어)에 대한 접근 방식입니다

ONTAP는 NFS v4.2 보안 레이블 및 NFS를 사용한 확장 특성(xattrs)을 비롯하여 파일 수준 ABAC(속성 기반 액세스 제어)를 달성하는 데 사용할 수 있는 몇 가지 접근 방식을 제공합니다.

NFS v4.2 보안 레이블

ONTAP 9.9.1부터 NFS라는 이름의 NFS v4.2 기능이 지원됩니다.

NFS v4.2 보안 레이블은 SELinux 레이블 및 MAC(필수 액세스 제어)를 사용하여 세분화된 파일 및 폴더 액세스를 관리하는 방법입니다. 이러한 MAC 레이블은 파일과 폴더와 함께 저장되며 UNIX 권한 및 NFS v4.x ACL과 함께 작동합니다.

NFS v4.2 보안 레이블을 지원한다는 것은 ONTAP가 이제 NFS 클라이언트의 SELinux 레이블 설정을 인식하고 이해한다는 것을 의미합니다. NFS v4.2 보안 레이블은 RFC-7204에 설명되어 있습니다.

NFS v4.2 보안 레이블의 사용 사례는 다음과 같습니다.

- 가상 머신(VM) 이미지의 MAC 레이블 지정
- 공공 부문의 데이터 보안 분류(비밀, 최고 비밀 및 기타 분류)
- 보안 규정 준수
- 디스크 없는 Linux

NFS v4.2 보안 레이블을 사용하도록 설정합니다

다음 명령을 사용하여 NFS v4.2 보안 레이블을 설정하거나 해제할 수 있습니다(고급 권한 필요).

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

에 대한 자세한 내용은 `vserver nfs modify` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS v4.2 보안 레이블에 대한 적용 모드입니다

ONTAP 9.9.1부터 ONTAP는 다음 적용 모드를 지원합니다.

- 제한된 서버 모드: ONTAP는 라벨을 적용할 수 없지만 라벨을 저장 및 전송할 수 있습니다.

  MAC 레이블을 변경하는 기능은 클라이언트에 달려 있습니다.

- * 게스트 모드 *: 클라이언트가 NFS-Aware(v4.1 이하)로 표시되지 않으면 MAC 레이블이 전송되지 않습니다.

  ONTAP는 현재 전체 모드를 지원하지 않습니다(MAC 레이블 저장 및 적용).

NFS v4.2 보안 레이블 예

다음 예제 구성은 Red Hat Enterprise Linux 릴리스 9.3(Plow)을 사용하는 개념을 보여 줍니다.

John R. Smith의 자격 증명을 기반으로 생성된 사용자는 `jrsmith` 다음과 같은 계정 Privileges를 가지고 있습니다.

- 사용자 이름 = `jrsmith`
- Privileges= `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

다음 MLS Privileges 표에 설명된 대로 권한이 있는 사용자인 관리자 계정과 사용자라는 두 가지 역할이 있습니다. `jrsmith`

사용자	역할	유형	레벨
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

이 예제 환경에서는 사용자가 `jrsmith` 에 있는 `s3` 수준의 파일에 액세스할 수 `s0` 있습니다. 관리자가 사용자 관련 데이터에 액세스하지 못하도록 하기 위해 아래에 설명된 대로 기존 보안 분류를 개선할 수 있습니다.

- S0 = 권한 관리자 사용자 데이터
- S0 = 분류되지 않은 데이터
- S1 = 대외비
- S2 = 비밀 데이터

- S3 = 상위 암호 데이터

MCS를 사용하는 **NFS v4.2** 보안 레이블 예

MLS(다중 수준 보안) 외에도 MCS(다중 범주 보안)라는 또 다른 기능을 사용하여 프로젝트와 같은 범주를 정의할 수 있습니다.

NFS 보안 레이블	값
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

확장 속성**(xattrs)**

ONTAP 9.12.1부터 ONTAP는 xattrs.xattrs를 지원하므로 ACL(액세스 제어 목록) 또는 사용자 정의 속성과 같이 시스템에서 제공하는 것 이상의 파일 및 디렉토리와 메타데이터를 연결할 수 있습니다.

xattrs를 구현하려면 Linux에서 및 `getfattr` 명령줄 유틸리티를 사용할 수 `setfattr` 있습니다. 이러한 도구는 파일과 디렉토리에 대한 추가 메타데이터를 관리하는 강력한 방법을 제공합니다. 부적절하게 사용하면 예기치 않은 동작 또는 보안 문제가 발생할 수 있으므로 주의하여 사용해야 합니다. 자세한 사용 지침은 항상 `setfattr` 및 `getfattr` man 페이지 또는 기타 신뢰할 수 있는 문서를 참조하십시오.

ONTAP 파일 시스템에서 xattrs가 활성화된 경우 사용자는 파일에 대한 임의의 속성을 설정, 수정 및 검색할 수 있습니다. 이러한 특성은 액세스 제어 정보와 같은 표준 파일 속성 집합으로 캡처되지 않은 파일에 대한 추가 정보를 저장하는 데 사용할 수 있습니다.

ONTAP에서 xattrs를 사용하기 위한 몇 가지 요구 사항과 제한 사항이 있습니다.

- Red Hat Enterprise Linux 8.4 이상
- Ubuntu 22.04 이상
- 각 파일에는 최대 128개의 xattrs를 포함할 수 있습니다
- Xattr 키는 255바이트로 제한됩니다
- 결합된 키 또는 값 크기는 xattr 당 1,729바이트입니다
- 디렉터리 및 파일에는 xattrs가 있을 수 있습니다
- xattrs를 설정 및 검색하려면 `w` 사용자 및 그룹에 대해 쓰기 모드 비트를 활성화해야 합니다

Xattrs는 사용자 네임스페이스 내에서 활용되며 ONTAP 자체에는 고유한 의미를 부여하지 않습니다. 대신 실제 애플리케이션은 파일 시스템과 상호 작용하는 클라이언트측 애플리케이션에 의해 결정되고 관리됩니다.

Xattr 사용 사례 예:

- 파일 생성을 담당하는 응용 프로그램의 이름을 기록합니다
- 파일을 가져온 이메일 메시지에 대한 참조 유지 관리
- 파일 객체 구성을 위한 범주화 프레임워크 설정
- 원본 다운로드 소스의 URL로 파일 레이블 지정

xattrs 관리 명령입니다

- `setfattr` 파일 또는 디렉토리의 확장 속성을 설정합니다.

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  명령 예:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` 특정 확장 특성의 값을 검색하거나 파일 또는 디렉토리의 모든 확장 특성을 나열합니다.

  특정 속성:
  ```
  getfattr -n <attribute_name> <file or directory name>
  ```

  모든 속성:
  ```
  getfattr <file or directory name>
  ```

  명령 예:

  ```
  getfattr -n user.comment example.txt
  ```

Xattr 키 값 쌍의 예

다음 표에서는 두 개의 xattr 키 값 쌍의 예를 보여 줍니다.

문자 수	값
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

xattrs에 대한 ACE의 사용자 권한

ACE(액세스 제어 항목)는 파일 또는 디렉터리와 같은 특정 리소스에 대해 개별 사용자 또는 사용자 그룹에 부여된 액세스 권한이나 권한을 정의하는 ACL 내의 구성 요소입니다. 각 ACE는 허용 또는 거부된 액세스 유형을 지정하며 특정 보안 주체(사용자 또는 그룹 ID)와 연결됩니다.

xattrs에 ACE(액세스 제어 항목)가 필요합니다

- xattr 검색: 사용자가 파일이나 디렉터리의 확장 속성을 읽는 데 필요한 권한입니다. "R"은 읽기 권한이 필요하다는 것을 나타냅니다.
- xattrs 설정: 확장 속성을 수정하거나 설정하는 데 필요한 권한. "a,""w" 및 "T"는 추가, 쓰기 및 xattrs와 관련된 특정 사용 권한 등 다양한 사용 권한의 예를 나타냅니다.
- 파일: 사용자는 확장 속성을 설정하려면 추가, 쓰기 및 xattrs와 관련된 특수 권한이 필요합니다.

- 디렉토리: 확장 속성을 설정하려면 특정 권한 "T"가 필요합니다.

파일 형식	**xattr**를 검색합니다	**xattrs**를 설정합니다
파일	R	a, w, T, 키
디렉토리	R	T

ABAC ID 및 액세스 제어 소프트웨어와의 통합

ABAC의 기능을 최대한 활용하기 위해 ONTAP는 ABAC 중심의 ID 및 액세스 관리 소프트웨어와 통합할 수 있습니다.

ABAC 시스템에서는 PEP(Policy Enforcement Point)와 PDP(Policy Decision Point)가 중요한 역할을 합니다. PEP는 액세스 제어 정책을 적용하는 역할을 담당하며 PDP는 정책에 따라 액세스 허용 또는 거부 여부를 결정합니다.

실용적인 환경에서 조직은 NFS 보안 레이블과 xattrs를 혼합하여 사용할 수 있습니다. 이러한 메타데이터는 분류, 보안, 애플리케이션, 콘텐츠 등 다양한 메타데이터를 나타내는 데 사용되며, 이는 모두 ABAC 결정에 중요한 역할을 합니다. 예를 들어 xattrs는 PDP가 의사 결정 프로세스에 사용하는 리소스 속성을 저장하는 데 사용될 수 있습니다. 파일의 분류 수준(예: "분류되지 않음", "기밀", "비밀" 또는 "최고 비밀")을 나타내도록 속성을 정의할 수 있습니다. 그런 다음 PDP는 이 속성을 활용하여 사용자가 분류 수준이 허용 수준 이하인 파일만 액세스하도록 제한하는 정책을 적용할 수 있습니다.

> 이 컨텐츠는 고객의 ID, 인증 및 액세스 서비스에 최소한 파일 시스템에 대한 액세스를 위한 중개인 역할을 하는 PEP와 PDP가 포함되어 있다고 가정합니다.

ABAC에 대한 프로세스 흐름의 예

1. 사용자가 PEP에 대한 시스템 액세스에 대한 자격 증명(예: PKI, OAuth, SAML)을 제공하고 PDP에서 결과를 가져옵니다.

   PEP의 역할은 사용자의 액세스 요청을 가로채서 PDP로 전달하는 것입니다.

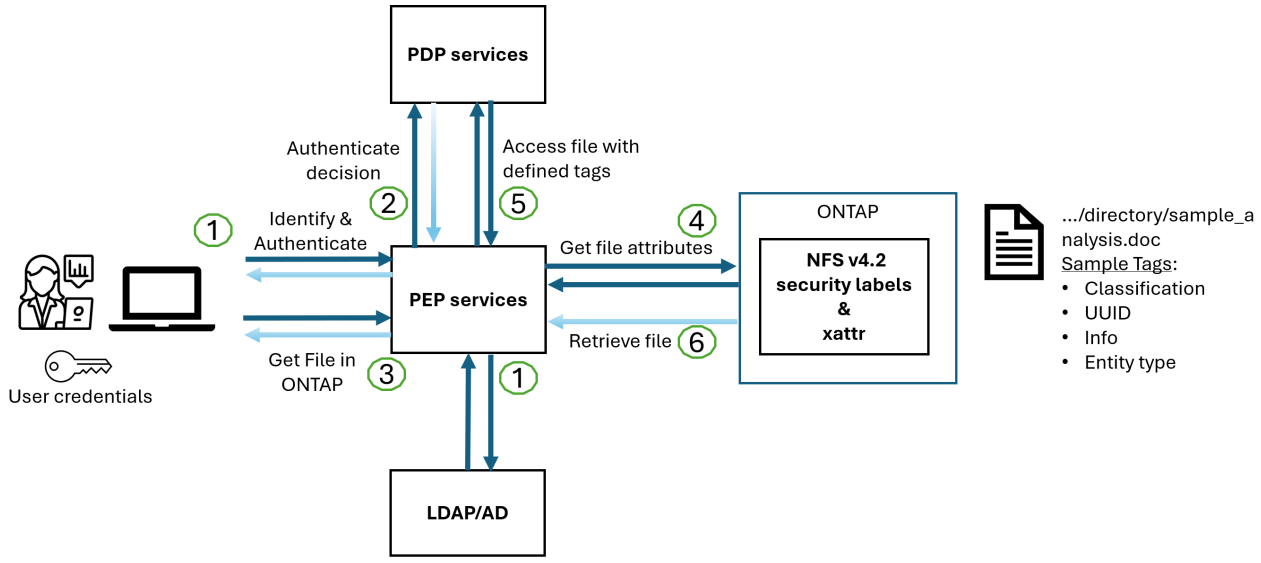
2. 그런 다음 PDP는 설정된 ABAC 정책에 대해 이 요청을 평가합니다.

   이러한 정책에서는 사용자, 해당 리소스 및 주변 환경과 관련된 다양한 특성을 고려합니다. 이러한 정책에 따라 PDP는 액세스 권한을 허용하거나 거부하도록 결정한 다음 이 결정을 다시 PEP에 전달합니다.

   PDP는 PEP에 적용할 정책을 제공합니다. 그런 다음 PEP는 PDP의 결정에 따라 사용자의 액세스 요청을 허용하거나 거부하여 이 결정을 적용합니다.

3. 요청이 성공하면 사용자는 ONTAP에 저장된 파일(예: AFF, AFF-C)을 요청합니다.
4. 요청이 성공하면 PEP는 문서에서 미세 입자 액세스 제어 태그를 가져옵니다.
5. PEP는 해당 사용자의 인증서를 기반으로 사용자에 대한 정책을 요청합니다.
6. PEP는 사용자가 파일에 액세스할 수 있고 사용자가 파일을 검색할 수 있는 경우 정책 및 태그에 따라 결정합니다.

> 실제 액세스는 토큰을 사용하여 수행할 수 있습니다.



ONTAP 클론 복제 및 **SnapMirror**

ONTAP의 클론 생성 및 SnapMirror 기술은 파일 데이터의 모든 측면을 보존하고 파일과 함께 전송할 수 있도록 효율적이고 안정적인 데이터 복제 및 복제 기능을 제공하도록 설계되었습니다. xattrs는 보안 레이블, 액세스 제어 정보, 사용자 정의 데이터 등 파일과 관련된 추가 메타데이터를 저장하는 데 있어 중요한 역할을 합니다.

ONTAP의 FlexClone 기술을 사용하여 볼륨을 클론 복제하면 볼륨의 쓰기 가능한 정확한 복제본이 생성됩니다. 이 복제 프로세스는 즉각적이고 공간 효율적이며 모든 파일 데이터와 메타데이터가 포함되어 xattrs가 완전히 복제되도록 합니다. 마찬가지로, SnapMirror는 데이터가 완벽한 충실도로 보조 시스템에 미러링되도록 보장합니다. 여기에는 이 메타데이터에 의존하는 응용 프로그램이 올바르게 작동하는 데 중요한 xattrs가 포함됩니다.

NetApp ONTAP는 클론 복제 및 복제 작업에 xattrs를 포함함으로써 모든 특성을 갖춘 전체 데이터 세트를 운영 및 2차 스토리지 시스템에서 일관되게 사용할 수 있도록 보장합니다. 일관된 데이터 보호, 빠른 복구, 규정 준수 및 규정 준수 표준을 준수해야 하는 조직에는 이러한 포괄적인 데이터 관리 접근 방식이 필수적입니다. 또한 온프레미스와 클라우드에서 다양한 환경에서 데이터 관리를 간소화하여 이러한 프로세스 중에 데이터가 완전하고 변경되지 않았다는 확신을 사용자에게 제공합니다.

NFS v4.2 보안 레이블에는 에 정의된 문제점이 NFS v4.2 보안 레이블있습니다.

라벨에 대한 변경 감사

xattrs 또는 NFS 보안 레이블의 변경 사항을 감사하는 것은 파일 시스템 관리 및 보안의 중요한 부분입니다. 표준 파일 시스템 감사 툴을 사용하면 xattrs 및 보안 레이블 수정을 비롯하여 파일 시스템에 대한 모든 변경 사항을 모니터링하고 기록할 수 있습니다.

Linux 환경에서 `auditd` 데몬은 일반적으로 파일 시스템 이벤트에 대한 감사를 설정하는 데 사용됩니다. 관리자는, `lsetxattr` 등의 xattr 변경과 관련된 특정 시스템 호출을 감시하고 `fsetxattr`, 특성을 설정하고 `removexattr`, `lremovexattr` `fremovexattr` 속성을 제거하는 규칙을 구성할 수 `setxattr` 있습니다.

ONTAP FPolicy는 파일 작업을 실시간으로 모니터링하고 제어하기 위한 강력한 프레임워크를 제공하여 이러한 기능을 확장합니다. 다양한 xattr 이벤트를 지원하도록 FPolicy를 구성하여 파일 작업을 세부적으로 제어하고 포괄적인 데이터 관리 정책을 적용할 수 있습니다.

특히 NFS v3 및 NFS v4 환경에서 xattrs를 사용하는 사용자의 경우 특정 파일 작업 및 필터 조합만 모니터링에

지원됩니다. NFS v3 및 NFS v4 파일 액세스 이벤트의 FPolicy 모니터링을 위해 지원되는 파일 작업 및 필터 조합 목록은 아래에 자세히 설명되어 있습니다.

지원되는 파일 작업	지원되는 필터
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

SetAttr 작업에 대한 **auditd** 로그 스니펫의 예:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

"ONTAP FPolicy를 사용해 보십시오"xattrs로 작업하는 사용자를 위해 파일 시스템의 무결성과 보안을 유지하는 데 필수적인 가시성과 제어 계층을 제공합니다. FPolicy의 고급 모니터링 기능을 활용하면 xattrs에 대한 모든 변경 사항을 추적하고 감사하며 보안 및 규정 준수 표준에 부합하도록 할 수 있습니다. 파일 시스템 관리에 대한 이러한 사전 예방적 접근 방식 때문에 데이터 거버넌스 및 보호 전략을 개선하려는 모든 조직에 ONTAP FPolicy를 사용하도록 적극 권장합니다.

데이터에 대한 액세스를 제어하는 예

John R. Smith의 PKI 인증서에 저장된 데이터에 대한 다음 예제 항목은 NetApp의 접근 방식을 파일에 적용하고 세분화된 액세스 제어를 제공하는 방법을 보여 줍니다.

> ⓘ 이러한 예는 설명을 위한 것이며 NFS v4.2 보안 레이블 및 xattrs와 관련된 메타데이터를 결정하는 것은 고객의 책임입니다. 업데이트 및 레이블 보존에 대한 자세한 내용은 간단한 사용을 위해 생략됩니다.

- PKI 인증서 값 예 *

키	값
entitySecurityMark를 클릭합니다	T:s01 = 분류되지 않음

키	값

정보	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

사양	"DoD"
UUID입니다	b4111349-7875-4115-AD30-0928565f2e15

관리자 조직	{
	"value": "DoD"
	}

키	값

브리핑	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

시민 상태	{
	"value": "US"
	}

여유값	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

국가/지역 제휴	[
	{
	"value": "USA"
	}
	]

키	값

디지털 식별자입니다	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

파종	<pre>{
	  "value": "DoD"
	}</pre>

DutyOrganization(이중 조직	<pre>{
	  "value": "DoD"
	}</pre>

entityType 을 선택합니다	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControls를 참조하십시오	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

이러한 PKI 권한은 데이터 유형 및 특성을 포함한 John R. Smith의 액세스 세부 정보를 보여 줍니다.

IC-TDF 메타데이터가 파일과 별도로 저장되는 시나리오에서 NetApp는 세분화된 액세스 제어 계층을 추가로 지원합니다. 여기에는 디렉토리 레벨 및 각 파일과 관련된 액세스 제어 정보가 모두 저장됩니다. 예를 들어, 파일에 연결된 다음 태그를 고려해 보십시오.

- NFS v4.2 보안 레이블: 보안 결정을 내리는 데 사용됩니다
- xattrs: 파일 및 조직 프로그램 요구 사항과 관련된 보충 정보를 제공합니다

다음 키-값 쌍은 xattrs로 저장될 수 있는 메타데이터의 예이며 파일의 생성자 및 관련 보안 분류에 대한 자세한 정보를 제공합니다. 이 메타데이터는 클라이언트 응용 프로그램에서 정보에 기반한 액세스 결정을 내리고 조직의 표준 및 요구 사항에 따라 파일을 구성하는 데 활용될 수 있습니다.

- xattr 키-값 쌍의 예 *

키	값
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

키	값

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

키	값
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

관련 정보

- "NFS in NetApp ONTAP: 모범 사례 및 구축 가이드"
- "ONTAP 명령 참조입니다"
- 설명 요청(RFC)
  - "RFC 7204: 레이블이 지정된 NFS에 대한 요구 사항"
  - "RFC 2203: RPCSEC_GSS 프로토콜 사양"
  - "RFC 3530: NFS(Network File System) 버전 4 프로토콜"