FlexPod 및 보안

FlexPod

NetApp

October 30, 2025

목차

FlexPod 및 보안

FlexPod, 랜섬웨어에 대한 솔루션

TR-4802: FlexPod, 랜섬웨어에 대한 솔루션

NetApp의 Arvind Ramakrishnan

파트너 후원:

랜섬웨어를 이해하려면 먼저 암호화에 대한 몇 가지 핵심 사항을 이해해야 합니다. 암호화 그래픽 방법을 사용하면 공유 비밀 키(대칭 키 암호화) 또는 키 쌍(비대칭 키 암호화)으로 데이터를 암호화할 수 있습니다. 이러한 키 중 하나는 널리 사용되는 공개 키이고 다른 하나는 비공개 개인 키입니다.

랜섬웨어는 암호화 바이러스 를 기반으로 하는 맬웨어의 한 유형으로, 암호화를 사용하여 악성 소프트웨어를 작성합니다. 이 맬웨어는 대칭 키 암호화와 비대칭 키 암호화를 모두 사용하여 피해자의 데이터를 잠그고 피해자의 데이터를 해독할 키를 제공하는 대가로 금전을 요구합니다.

랜섬웨어의 작동 방식

다음 단계에서는 랜섬웨어가 암호화를 사용하여 피해자의 암호 해독 또는 복구 범위 없이 피해자의 데이터를 암호화하는 방법을 설명합니다.

1. 공격자는 비대칭 키 암호화에서와 같이 키 쌍을 생성합니다. 생성된 공개 키는 맬웨어 내에 배치되고 맬웨어는 해제됩니다.
2. 맬웨어가 피해자의 컴퓨터 또는 시스템에 침입한 후 pseudorandom 숫자 생성기(PRNG) 또는 기타 실행 가능한 임의의 숫자 생성 알고리즘을 사용하여 임의의 대칭 키를 생성합니다.
3. 맬웨어는 이 대칭 키를 사용하여 피해자의 데이터를 암호화합니다. 결과적으로 맬웨어에 포함된 공격자의 공개 키를 사용하여 대칭 키를 암호화합니다. 이 단계의 출력은 암호화된 대칭 키의 비대칭 암호문과 피해자 데이터의 대칭 암호문입니다.
4. 맬웨어는 피해자의 데이터와 데이터를 암호화하는 데 사용된 대칭 키를 제로(삭제)하여 복구 범위를 남기지 않습니다.
5. 피해자는 이제 대칭 키의 비대칭 암호문과 데이터를 암호화하는 데 사용된 대칭 키를 얻기 위해 지불해야 하는 랜섬 값을 표시합니다.
6. 피해자는 몸값을 지불하고 비대칭 암호문을 공격자와 공유합니다. 공격자는 개인 키로 암호문을 해독하여 대칭 키를 만듭니다.
7. 공격자는 이 대칭 키를 피해자와 공유합니다. 이 키를 사용하여 모든 데이터를 해독하고 공격에서 복구할 수 있습니다.

당면 과제

개인 및 조직은 랜섬웨어의 공격을 받을 때 다음과 같은 문제에 직면해 있습니다.

- 가장 중요한 과제는 조직 또는 개인의 생산성을 즉각적으로 저하시키는 것입니다. 모든 중요 파일을 다시 확보하고 시스템을 안전하게 보호해야 하므로 정상 상태로 복원하는 데 시간이 걸립니다.
- 고객 또는 고객에 속하는 중요한 기밀 정보가 포함된 데이터 유출로 인해 조직이 분명히 피하고 싶어 하는 위기 상황이 발생할 수 있습니다.
- 데이터가 잘못 유출되거나 완전히 삭제될 가능성이 매우 높습니다. 이로 인해 조직과 개인에게 재앙이 될 수 있는 무리턴 지점이 될 수 있습니다.
- 랜섬을 지불한 후에는 공격자가 데이터를 복원할 키를 제공할 것이라는 보장이 없습니다.
- 공격자는 대가를 지불하더라도 중요한 데이터의 브로드캐스트를 삼가한다는 보장은 없습니다.
- 대규모 엔터프라이즈에서 랜섬웨어 공격으로 이어받은 허점을 식별하는 일은 지루한 작업이며, 모든 시스템을 보호하는 데는 많은 노력이 필요합니다.

누가 위험에 처합니까?

개인 및 대규모 조직을 포함하여 모든 사람이 랜섬웨어의 공격을 받을 수 있습니다. 잘 정의된 보안 수단과 관행을 구현하지 않는 조직은 이러한 공격에 훨씬 더 취약합니다. 대규모 조직에 가해지는 공격의 결과는 개인이 견딜 수 있는 것보다 몇 배 더 클 수 있습니다.

랜섬웨어는 모든 맬웨어 공격의 약 28%를 차지합니다. 다시 말해, 4개 맬웨어 사고 중 2개 이상이 랜섬웨어 공격입니다. 랜섬웨어는 인터넷을 통해 자동으로 무차별적으로 확산될 수 있으며, 보안 문제가 발생할 경우 피해자의 시스템에 진입하여 연결된 다른 시스템으로 계속 확산될 수 있습니다. 공격자들은 많은 파일 공유를 수행하거나, 많은 중요한 데이터를 보유하고 있거나, 공격에 대한 부적절한 보호를 유지하는 사람 또는 조직을 표적으로 삼는 경향이 있습니다.

공격자들은 다음과 같은 잠재적 표적에 집중하는 경향이 있습니다.

- 대학 및 학생 커뮤니티
- 정부 기관 및 기관
- 있습니다
- 은행

이것은 전체 대상 목록이 아닙니다. 이러한 범주 중 하나를 벗어나는 경우 공격으로부터 자신을 보호할 수 없습니다.

랜섬웨어는 시스템에 어떻게 들어가거나 확산됩니까?

랜섬웨어가 시스템에 들어오거나 다른 시스템으로 확산되는 방법에는 여러 가지가 있습니다. 오늘날의 세계에서 거의 모든 시스템은 인터넷, LAN, WAN 등을 통해 서로 연결되어 있습니다. 이러한 시스템 간에 생성 및 교환되는 데이터의 양은 증가만 되고 있습니다.

랜섬웨어가 확산되는 가장 일반적인 방법 중 일부에는 매일 데이터를 공유 또는 액세스하기 위해 사용하는 방법이 포함됩니다.

- 이메일
- P2P 네트워크
- 파일 다운로드
- 소셜 네트워킹
- 모바일 장치
- 안전하지 않은 공용 네트워크에 연결

- 웹 URL 액세스

데이터 손실의 결과

데이터 손실의 결과 또는 효과는 조직이 예상하는 것보다 훨씬 더 클 수 있습니다. 이러한 영향은 다운타임 기간 또는 조직이 데이터에 액세스할 수 없는 기간에 따라 달라질 수 있습니다. 공격이 지속되는 기간이 길수록 조직의 매출, 브랜드, 평판에 미치는 영향이 커집니다. 또한 조직은 법적 문제와 급격한 생산성 저하에 직면할 수 있습니다.

이러한 문제는 시간이 지나면서 계속 지속되기 때문에 공격이 어떻게 반응하는지에 따라 조직 문화가 확대되고 결국 조직 문화가 변하게 될 수 있습니다. 오늘날의 세계에서 정보가 빠른 속도로 퍼지고 조직에 대한 부정적인 뉴스가 퍼지면 회사의 명성에 영구적인 손상을 줄 수 있습니다. 조직은 데이터 손실에 대해 막대한 처벌을 받을 수 있으며, 이로 인해 결과적으로 비즈니스가 종료될 수 있습니다.

재무적 영향

최근 에 따르면 "McAfee 보고서"사이버 범죄로 인해 발생하는 글로벌 비용은 약 6천억 달러로, 이는 전 세계 GDP의 약 0.8%입니다. 이 액수가 전 세계적으로 4조2000억 달러에 이르는 인터넷 경제 성장세에 비해 14%의 세금에 해당한다.

랜섬웨어는 이러한 재무 비용의 상당 부분을 차지합니다. 2018년에 랜섬웨어 공격으로 인해 발생한 비용은 약 80억 달러이며, 2019년에는 115억 달러에 이를 것으로 예측됩니다.

솔루션이 무엇입니까**?**

최소한의 다운타임으로 랜섬웨어 공격에서 복구하려면 사전 예방적 재해 복구 계획을 구현해야만 합니다. 공격에서 복구할 수 있는 기능을 갖추는 것이 좋지만 공격을 한 번에 차단하는 것이 좋습니다.

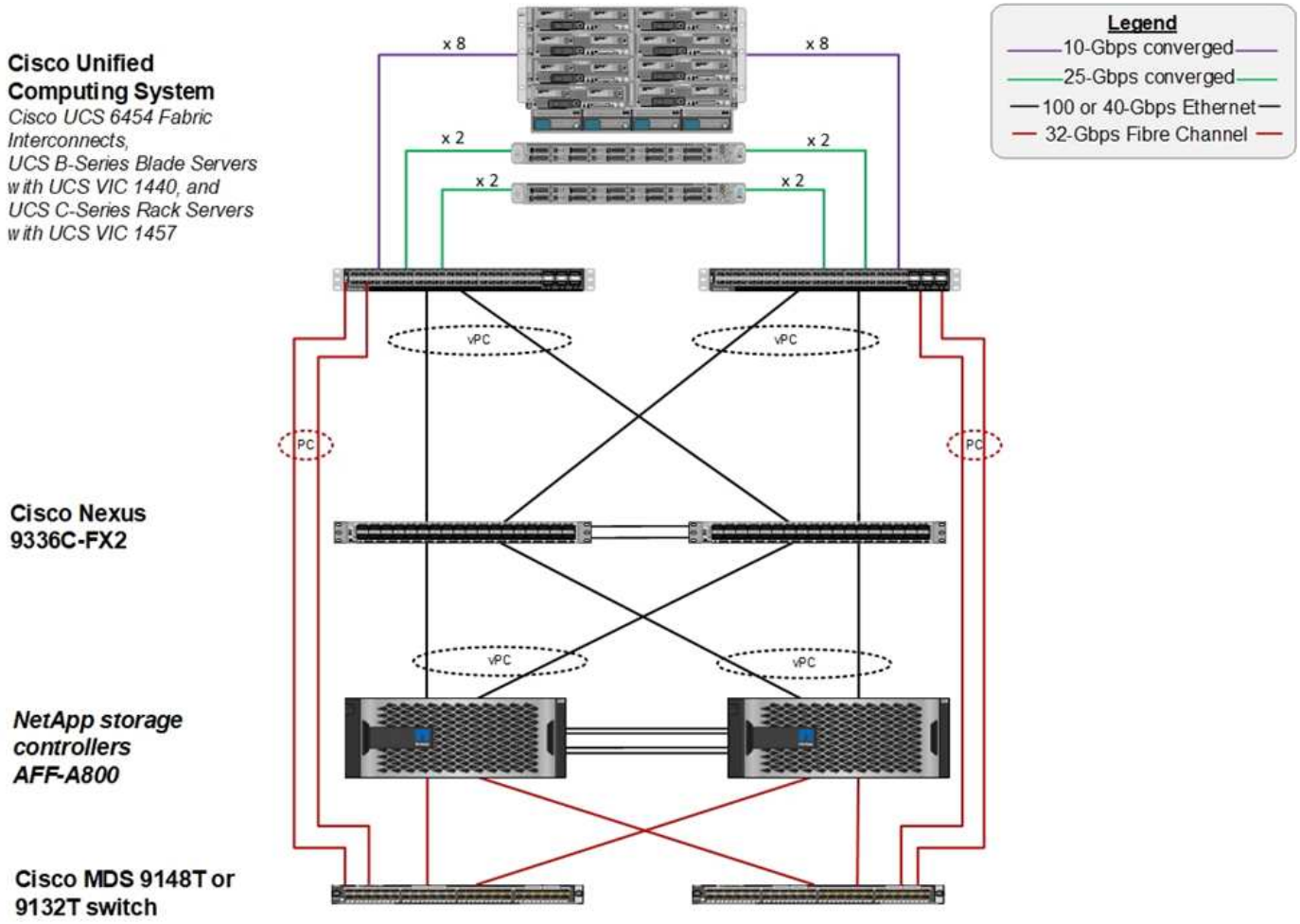
공격을 방지하기 위해 몇 가지 프런트 엔드를 검토하고 수정해야 하지만 공격을 막거나 공격으로부터 복구할 수 있는 핵심 구성 요소는 데이터 센터입니다.

네트워크, 컴퓨팅 및 스토리지 엔드 포인트의 보안을 위해 데이터 센터가 제공하는 설계와 기능은 일상적인 운영을 위한 안전한 환경을 구축하는 데 중요한 역할을 합니다. 이 문서에서는 FlexPod 하이브리드 클라우드 인프라의 기능이 공격 시 데이터를 빠르게 복구하는 데 어떤 도움이 되며 공격을 한 번에 차단하는 데에도 어떤 도움이 되는지를 보여 줍니다.

FlexPod 개요

FlexPod는 Cisco UCS(Unified Computing System) 서버, Cisco Nexus 스위치 제품군, Cisco MDS 패브릭 스위치 및 NetApp 스토리지 어레이를 유연한 단일 아키텍처로 결합하는 사전 설계, 통합 및 검증된 아키텍처입니다. FlexPod 솔루션은 단일 장애 지점 없이 고가용성을 지원하도록 설계되었으며, 비용 효율성과 설계 유연성을 유지하여 다양한 워크로드를 지원합니다. FlexPod 설계는 다양한 하이퍼바이저와 베어 메탈 서버를 지원할 수 있으며 고객의 워크로드 요구사항에 따라 규모 조정 및 최적화할 수 있습니다.

아래 그림은 FlexPod 아키텍처를 보여 주며 스택의 모든 계층에서 고가용성을 보여 줍니다. 스토리지, 네트워크 및 컴퓨팅의 인프라 구성요소는 구성요소 중 하나에 장애가 발생할 경우 정상 작동하는 파트너에게 즉시 페일오버할 수 있도록 구성됩니다.



FlexPod 시스템의 가장 큰 장점은 여러 워크로드를 위해 사전 설계, 통합 및 검증된다는 것입니다. 모든 솔루션 검증에 대한 자세한 설계 및 배포 가이드가 게시되었습니다. 이러한 문서에는 FlexPod에서 원활하게 워크로드를 실행하기 위해 채택해야 하는 모범 사례가 포함되어 있습니다. 이러한 솔루션은 동급 최고의 컴퓨팅, 네트워크 및 스토리지 제품과 전체 인프라의 보안 및 강화를 위한 다양한 기능을 토대로 구축되었습니다.

"IBM의 X-Force 위협 인텔리전스 지수" "과거 424%의 잘못 구성된 클라우드 인프라 점프를 포함하여 손상된 기록의 3분의 2를 책임지는 사람의 실수"

FlexPod 시스템을 사용하면 CVD(Cisco Validated Design)와 NVA(NetApp Verified Architecture)에 설명된 모범 사례에 따라 인프라를 엔드 투 엔드 방식으로 설정하는, Ansible 플레이북을 통해 자동화를 통해 인프라 구성 오류를 방지할 수 있습니다.

랜섬웨어 차단 조치

이 섹션에서는 랜섬웨어 공격을 효과적으로 보호하고 복구할 수 있는 NetApp ONTAP 데이터 관리 소프트웨어의 주요 기능과 Cisco UCS 및 Cisco Nexus용 툴에 대해 설명합니다.

스토리지**: NetApp ONTAP**

ONTAP 소프트웨어는 데이터 보호에 유용한 여러 기능을 제공하며, 대부분의 기능은 ONTAP 시스템을 사용하는 고객에게 무료로 제공됩니다. 다음 기능을 항상 사용하여 공격으로부터 데이터를 보호할 수 있습니다.

- * NetApp 스냅샷 기술. * 스냅샷 복사본은 특정 시점의 파일 시스템 상태를 캡처하는 볼륨의 읽기 전용

이미지입니다. 이러한 복사본은 시스템 성능에 영향을 주지 않고 데이터를 보호하면서 많은 스토리지 공간을 차지하지 않습니다. 스냅샷 복사본을 생성하기 위한 일정을 생성하는 것이 좋습니다. 또한 일부 맬웨어가 휴면 상태가 된 후 감염 후 몇 주 또는 몇 개월 후에 다시 활성화될 수 있기 때문에 보존 기간을 길게 유지해야 합니다. 공격이 발생할 경우 감염 전에 생성된 스냅샷 복사본을 사용하여 볼륨을 롤백할 수 있습니다.

- * NetApp SnapRestore 기술. * SnapRestore 데이터 복구 소프트웨어는 데이터 손상을 복구하거나 파일 내용만 되돌리는 데 매우 유용합니다. SnapRestore은 볼륨의 특성을 되돌리지 않으며 스냅샷 복사본에서 액티브 파일 시스템으로 파일을 복사하여 관리자가 달성할 수 있는 것보다 훨씬 빠릅니다. 많은 파일을 최대한 빨리 복구해야 하는 경우 데이터를 복구할 수 있는 속도가 유용합니다. 이러한 매우 효율적인 복구 프로세스를 통해 공격이 발생할 경우 비즈니스를 신속하게 온라인 상태로 되돌릴 수 있습니다.
- * NetApp SnapCenter 기술. * SnapCenter 소프트웨어는 NetApp 스토리지 기반 백업 및 복제 기능을 사용하여 애플리케이션 정합성을 보장하는 데이터 보호를 제공합니다. 이 소프트웨어는 엔터프라이즈 애플리케이션과 통합되며 애플리케이션, 데이터베이스 및 가상 인프라 관리자의 요구사항에 부합하는 애플리케이션별 워크플로우 및 데이터베이스별 워크플로우를 제공합니다. SnapCenter은 사용하기 쉬운 엔터프라이즈 플랫폼을 제공하여 애플리케이션, 데이터베이스 및 파일 시스템 전반에서 데이터 보호를 안전하게 조율하고 관리합니다. 애플리케이션을 더욱 신속하게 일관된 상태로 복원할 수 있으므로 데이터 복구 중에도 애플리케이션 정합성이 보장된 데이터 보호를 제공하는 기능은 매우 중요합니다.
- NetApp SnapLock 기술 * SnapLock은 파일을 저장한 후 지우거나 쓰기가 불가능한 상태로 커밋하는 특수한 용도의 볼륨을 제공합니다. FlexVol 볼륨에 상주하는 사용자의 운영 데이터는 NetApp SnapMirror 또는 SnapVault 기술을 통해 SnapLock 볼륨으로 미러링하거나 저장할 수 있습니다. SnapLock 볼륨의 파일, 볼륨 자체 및 해당 호스팅 애그리게이트는 보존 기간이 끝날 때까지 삭제할 수 없습니다.
- * NetApp FPolicy 기술. * FPolicy 소프트웨어를 사용하여 특정 확장명의 파일에 대한 작업을 허용하지 않도록 함으로써 공격을 방지하십시오. FPolicy 이벤트는 특정 파일 작업에 대해 트리거될 수 있습니다. 이 이벤트는 정책에 연결되어 있어야 하는 엔진을 호출합니다. 랜섬웨어를 포함할 수 있는 파일 확장자 세트로 정책을 구성할 수 있습니다. 허용되지 않는 확장명을 가진 파일이 무단 작업을 수행하려고 하면 FPolicy가 해당 작업이 실행되지 않도록 합니다.

네트워크**: Cisco Nexus**

Cisco NX OS 소프트웨어는 네트워크 이상 현상 및 보안을 더욱 강화하는 NetFlow 기능을 지원합니다. NetFlow는 네트워크의 모든 대화 메타데이터, 통신 관련 당사자, 사용 중인 프로토콜 및 트랜잭션 기간을 캡처합니다. 정보를 집계 및 분석한 후에는 정상적인 동작에 대한 통찰력을 제공할 수 있습니다.

또한 수집된 데이터를 통해 네트워크를 통해 확산되는 맬웨어와 같은 의심스러운 활동 패턴을 식별할 수 있으며, 그렇지 않을 경우 이를 간과할 수 있습니다.

NetFlow는 흐름을 사용하여 네트워크 모니터링에 대한 통계를 제공합니다. 흐름은 소스 인터페이스(또는 VLAN)에 도착하고 키에 대해 동일한 값을 갖는 패킷의 단방향 스트림입니다. 키는 패킷 내의 필드에 대해 식별된 값입니다. 유동 레코드를 사용하여 유동의 고유 키를 정의하는 유동을 만듭니다. 흐름 내보내기를 사용하여 Cisco Stealthwatch와 같은 원격 NetFlow 수집기로 플로우에 대해 NetFlow에서 수집하는 데이터를 내보낼 수 있습니다. Stealthwatch는 이 정보를 사용하여 네트워크를 지속적으로 모니터링하고 랜섬웨어 발생 시 실시간 위협 탐지 및 사고 대응 법의학 조사를 제공합니다.

컴퓨팅**: Cisco UCS**

Cisco UCS는 FlexPod 아키텍처의 컴퓨팅 엔드포인트입니다. 운영 체제 수준에서 스택의 이 계층을 보호하는 데 도움이 되는 여러 Cisco 제품을 사용할 수 있습니다.

컴퓨팅 또는 애플리케이션 계층에서 다음 주요 제품을 구현할 수 있습니다.

- * 끝점용 Cisco AMP(Advanced Malware Protection).* Microsoft Windows 및 Linux 운영 체제에서 지원되는 이 솔루션은 예방, 검색 및 응답 기능을 통합합니다. 이 보안 소프트웨어는 침입을 방지하고 진입 지점에서 맬웨어를

차단하며 파일 및 프로세스 활동을 지속적으로 모니터링 및 분석하여 일선 방어를 우회할 수 있는 위협을 신속하게 탐지, 억제 및 해결합니다.

AMP의 MAP(Malicious Activity Protection) 구성 요소는 모든 엔드포인트 활동을 지속적으로 모니터링하고 엔드포인트에서 실행 중인 프로그램의 비정상적인 동작을 런타임 감지 및 차단합니다. 예를 들어, 엔드포인트 동작에 랜섬웨어가 표시되면 문제가 되는 프로세스가 종료되어 엔드포인트 암호화가 예방되고 공격이 중지됩니다.

- * Cisco Advanced Malware Protection for Email Security. * 이메일은 맬웨어를 유포하고 사이버 공격을 수행하는 주요 수단으로 자리 잡았습니다. 평균적으로 하루 동안 약 1,000억 개의 이메일이 교환되며, 이를 통해 공격자들은 사용자 시스템에 대한 탁월한 침투 벡터를 얻을 수 있습니다. 따라서 이 공격 라인을 방어하는 것이 절대적으로 중요합니다.

  AMP는 제로 데이 익스플로잇(zero-day exploit) 및 악성 첨부 파일에 숨겨진 악성 맬웨어와 같은 위협에 대한 이메일을 분석합니다. 또한 업계 최고의 URL 인텔리전스를 사용하여 악성 링크를 차단합니다. 스피어 피싱, 랜섬웨어 및 기타 정교한 공격에 대한 고급 보호 기능을 제공합니다.

- * NGIPS(Next-Generation Intrusion Prevention System). * Cisco firepower NGIPS는 데이터 센터에서 물리적 어플라이언스로 구축하거나 VMware(NGIPSv for VMware)에서 가상 어플라이언스로 구축할 수 있습니다. 이 고효율 침입 방지 시스템은 안정적인 성능과 낮은 총 소유 비용을 제공합니다. AMP, 애플리케이션 가시성 및 제어, URL 필터링 기능을 제공하기 위해 선택적 구독 라이센스로 위협 보호를 확장할 수 있습니다. 가상화된 NGIPS는 VM(가상 시스템) 간의 트래픽을 검사하고 리소스가 제한된 사이트에서 NGIPS 솔루션을 쉽게 배포 및 관리할 수 있도록 하여 물리적 자산과 가상 자산 모두의 보호를 강화합니다.

FlexPod에서 데이터 보호 및 복구

이 섹션에서는 공격 발생 시 최종 사용자의 데이터를 복구하는 방법과 FlexPod 시스템을 사용하여 공격을 방지하는 방법을 설명합니다.

테스트 베드 개요

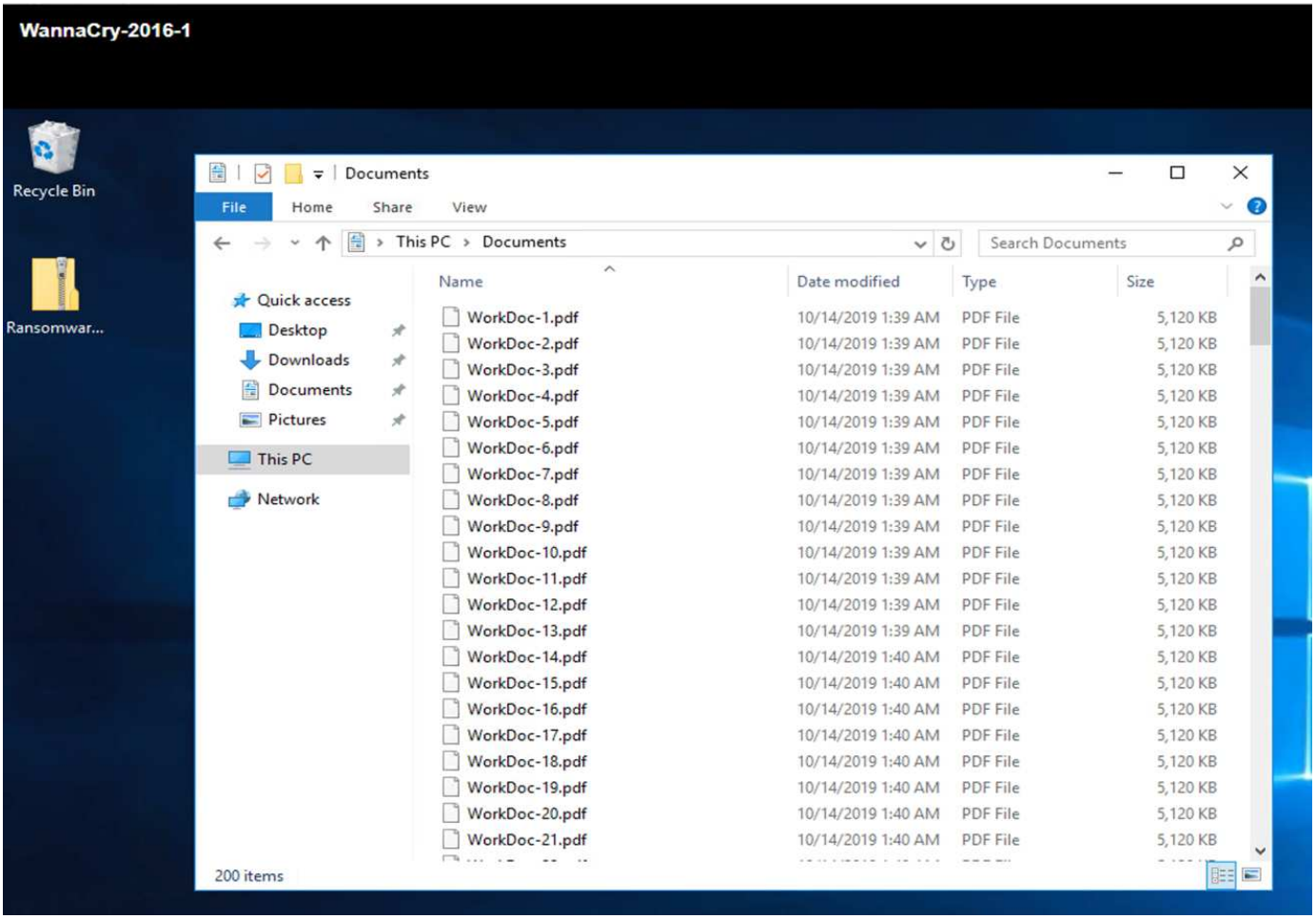
FlexPod 감지, 개선 및 예방을 보여주기 위해 이 문서가 작성된 시점에 제공되는 최신 플랫폼 CVD에 지정된 지침에 따라 테스트베드가 구축되었습니다. "VMware vSphere 6.7 U1, Cisco UCS 4세대 및 NetApp AFF A-Series CVD를 지원하는 FlexPod 데이터 센터".

NetApp ONTAP 소프트웨어의 CIFS 공유를 제공하는 Windows 2016 VM이 VMware vSphere 인프라에 구축했습니다. 그런 다음 CIFS 공유에서 NetApp FPolicy를 구성하여 특정 확장 유형의 파일이 실행되지 않도록 했습니다. 또한 NetApp SnapCenter 소프트웨어는 애플리케이션 정합성을 보장하는 스냅샷 복사본을 제공하기 위해 인프라에서 VM의 스냅샷 복사본을 관리하기 위해 구축되었습니다.

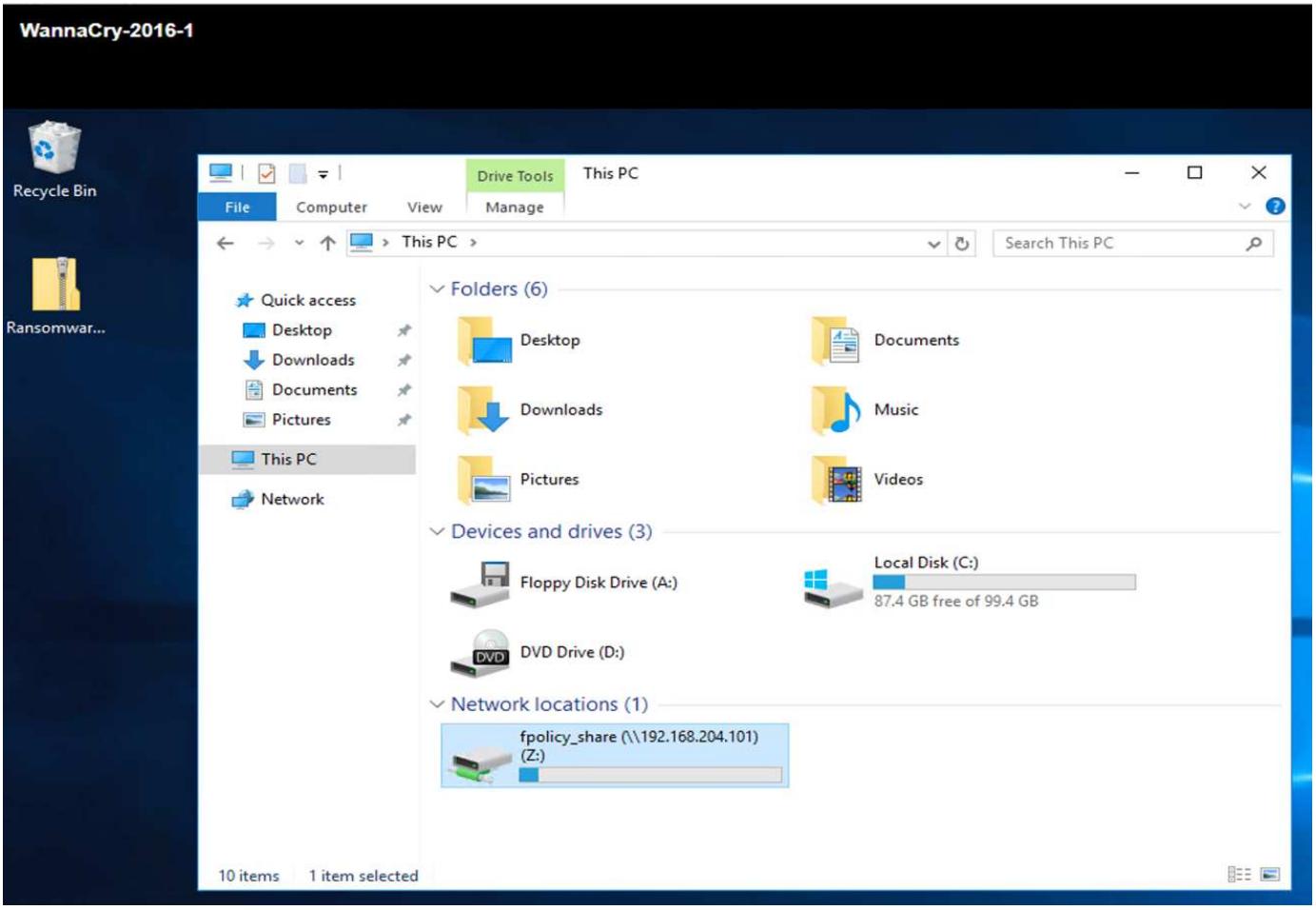
공격 전의 **VM** 및 파일 상태

이 섹션에서는 VM에 대한 공격 전의 파일 상태와 매핑된 CIFS 공유를 보여 줍니다.

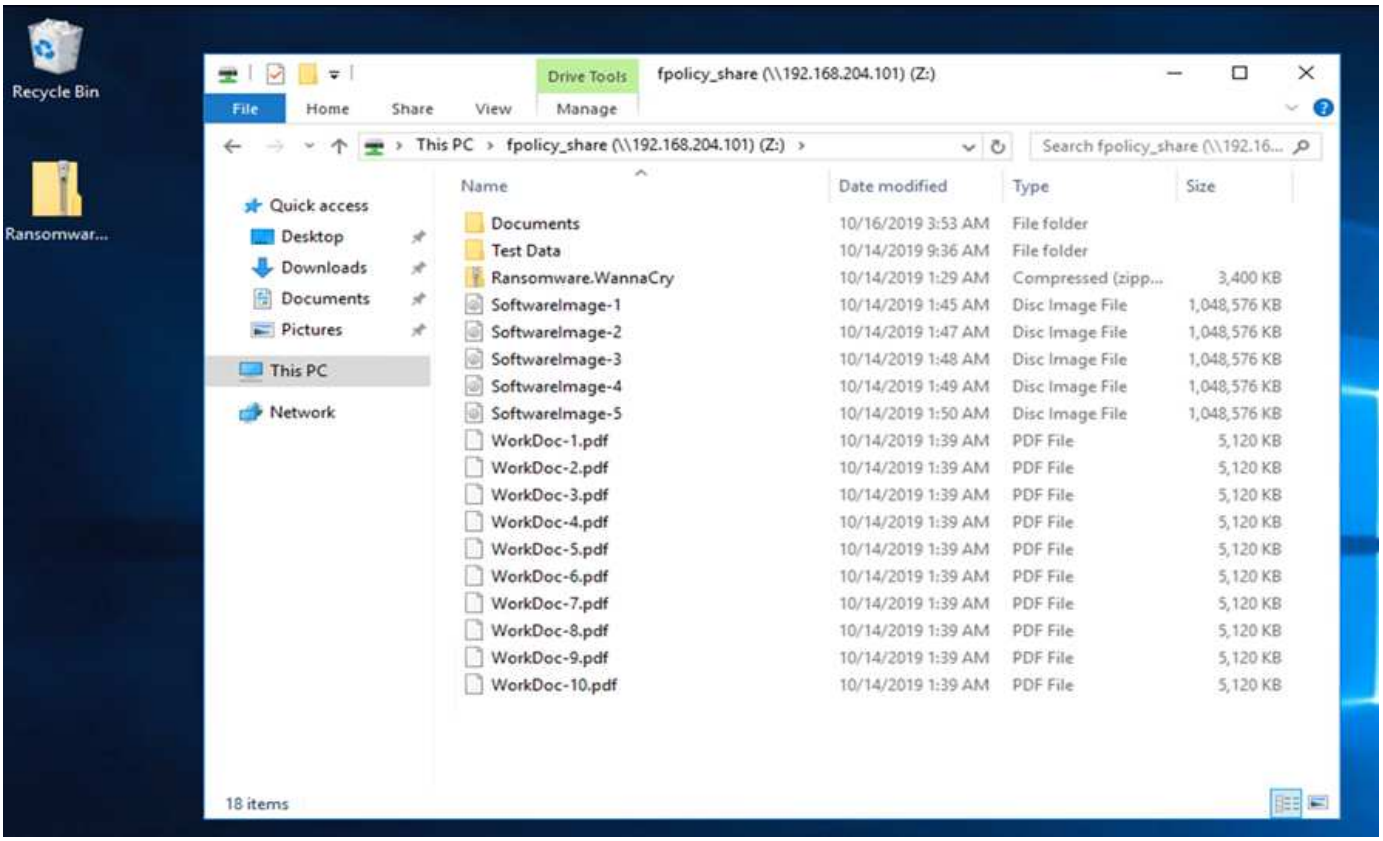
VM의 Documents 폴더에는 WannaCry 맬웨어에 의해 아직 암호화되지 않은 PDF 파일 세트가 있습니다.



다음 스크린샷은 VM에 매핑된 CIFS 공유를 보여 줍니다.



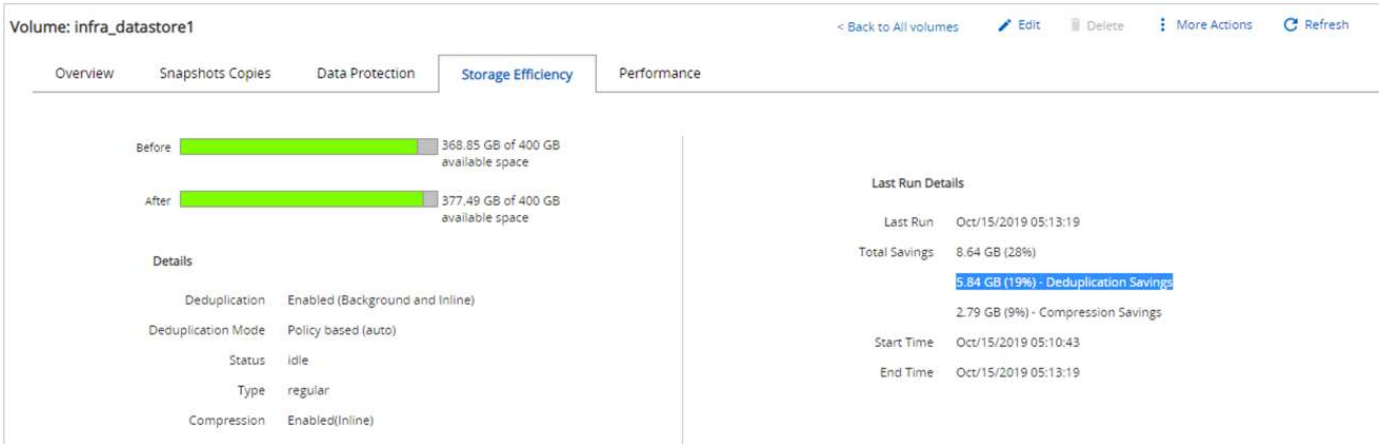
다음 스크린샷은 WannaCry 맬웨어가 아직 암호화하지 않은 CIFS 공유 'FPolicy_share'의 파일을 보여 줍니다.



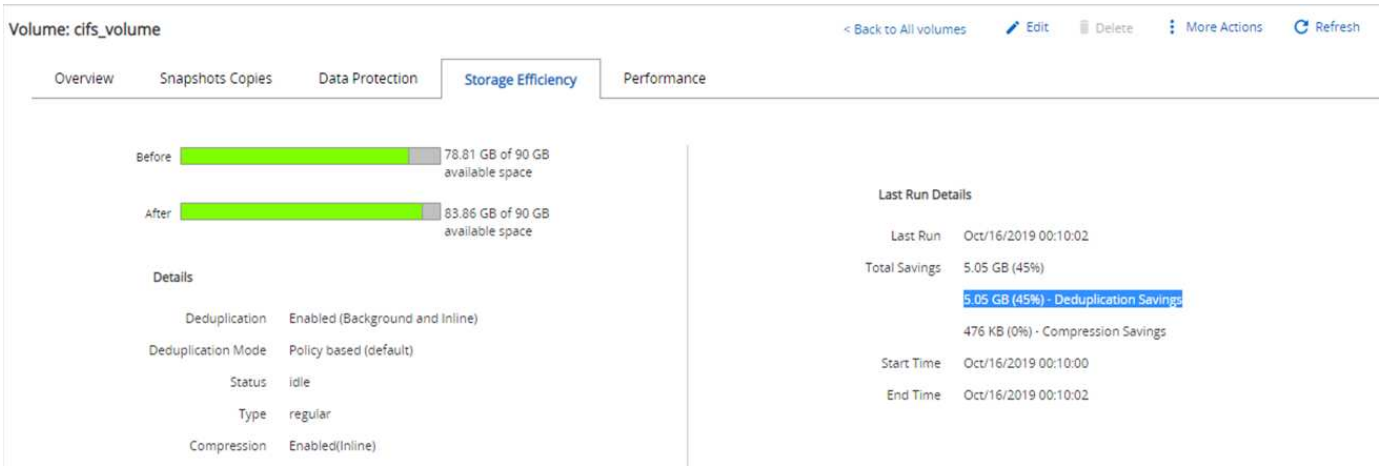
공격 전에 데이터 중복 제거 및 스냅샷 정보

공격 전의 스냅샷 복사본의 스토리지 효율성 세부 정보와 크기는 검색 단계 중에 참조로 표시되고 사용됩니다.

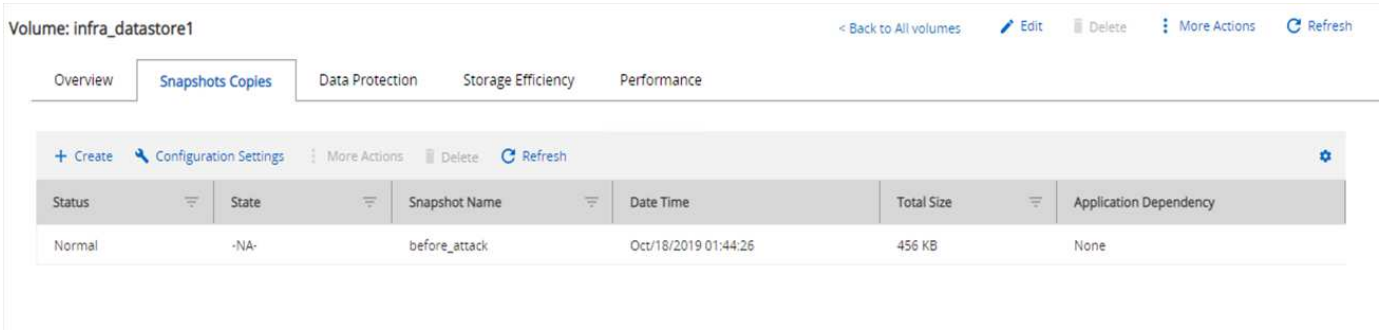
VM을 호스팅하는 볼륨에서 중복 제거를 통해 스토리지를 19%나 절감할 수 있었습니다.



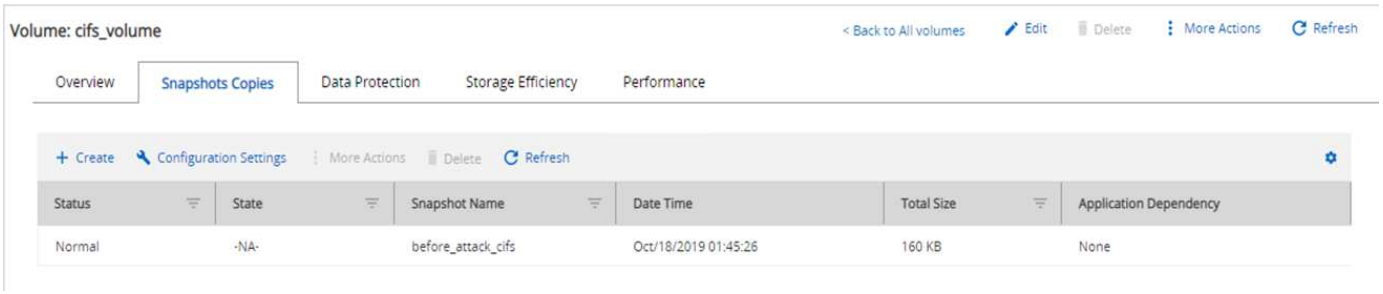
CIFS 공유 'FPolicy_share'의 중복제거 기능으로 스토리지를 45% 절약할 수 있었습니다.



VM을 호스팅하는 볼륨에서 456KB의 스냅샷 복사본 크기가 관찰되었습니다.



CIFS 공유 'FPolicy_share'에 대해 160KB의 스냅샷 복사본 크기가 관찰되었습니다.



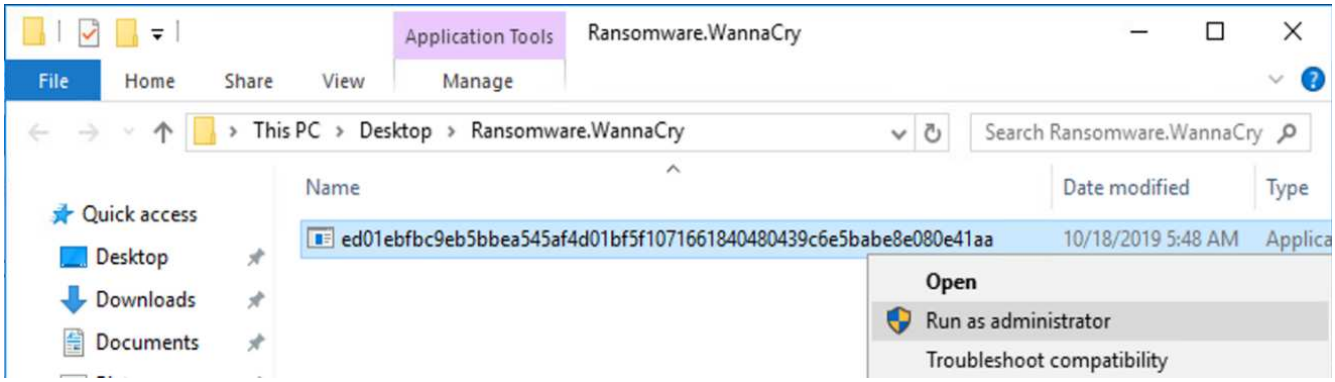
VM 및 **CIFS** 공유에서 **WannaCry** 감염

이 섹션에서는 WannaCry 맬웨어가 FlexPod 환경에 도입된 방식과 관찰된 시스템에 대한 후속 변경 사항을 보여 줍니다.

다음 단계에서는 WannaCry 맬웨어 바이너리가 VM에 도입된 방법을 보여 줍니다.

1. 보안 맬웨어가 추출되었습니다.

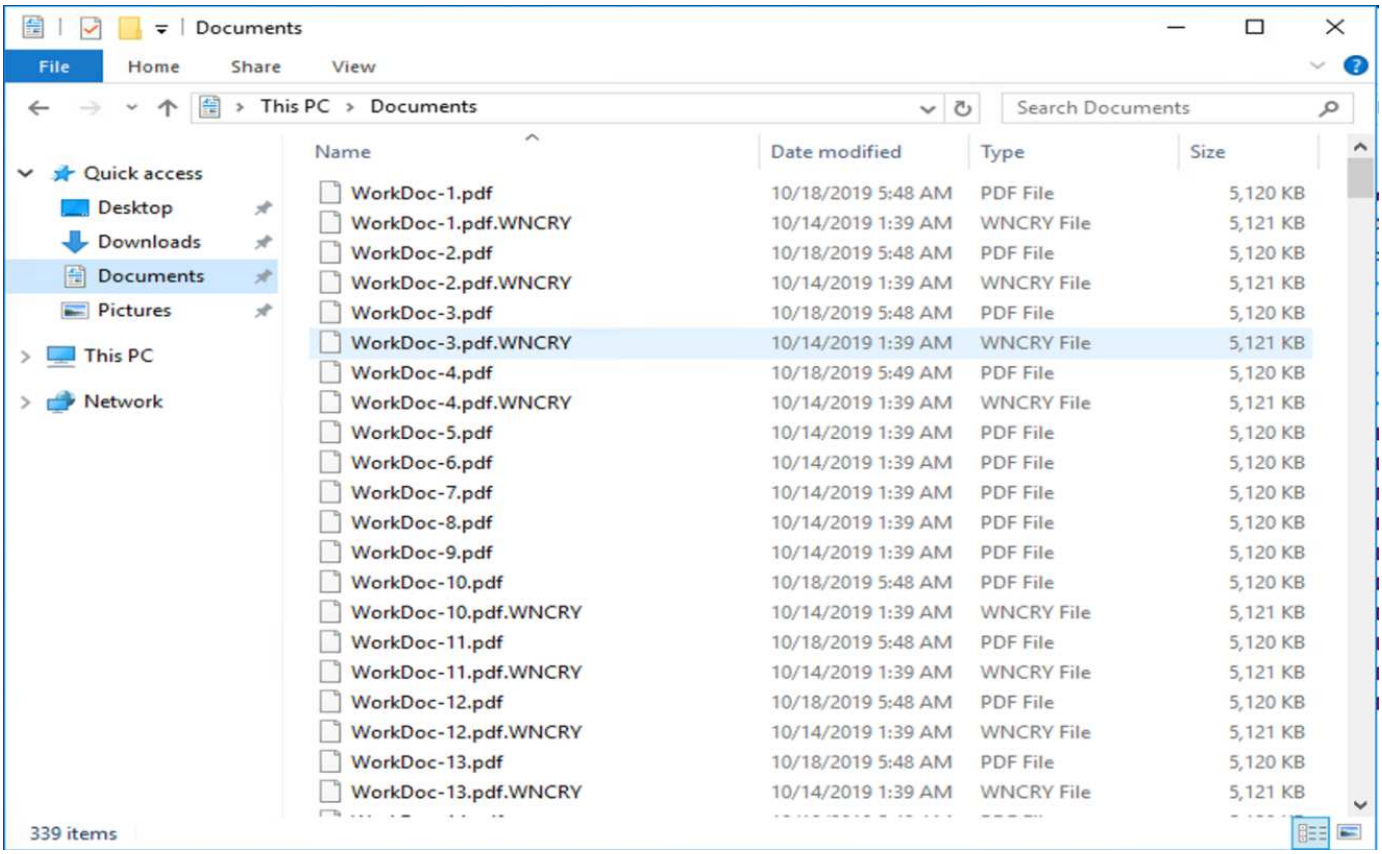
2. 바이너리가 실행되었습니다.



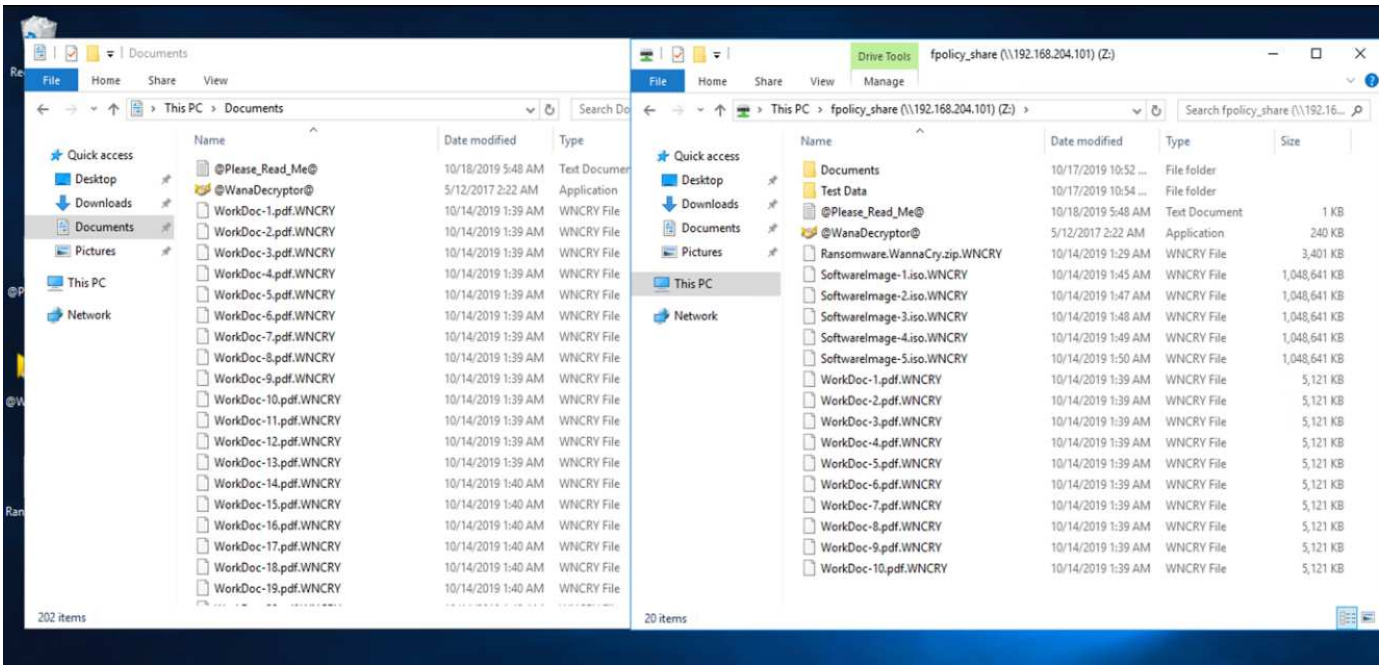
사례 **1: WannaCry**는 **VM** 및 매핑된 **CIFS** 공유 내의 파일 시스템을 암호화합니다

로컬 파일 시스템과 매핑된 CIFS 공유는 WannaCry 멀웨어에 의해 암호화되었습니다.

맬웨어가 WNCRY 확장명으로 파일을 암호화하기 시작합니다.



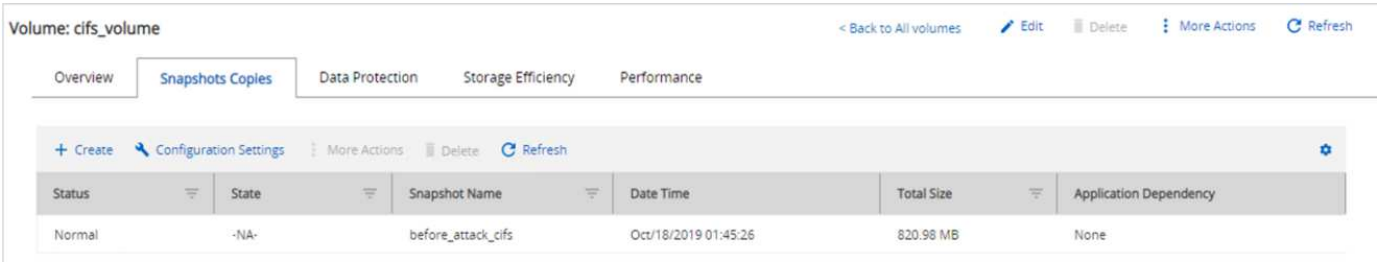
맬웨어는 로컬 VM 및 매핑된 공유의 모든 파일을 암호화합니다.



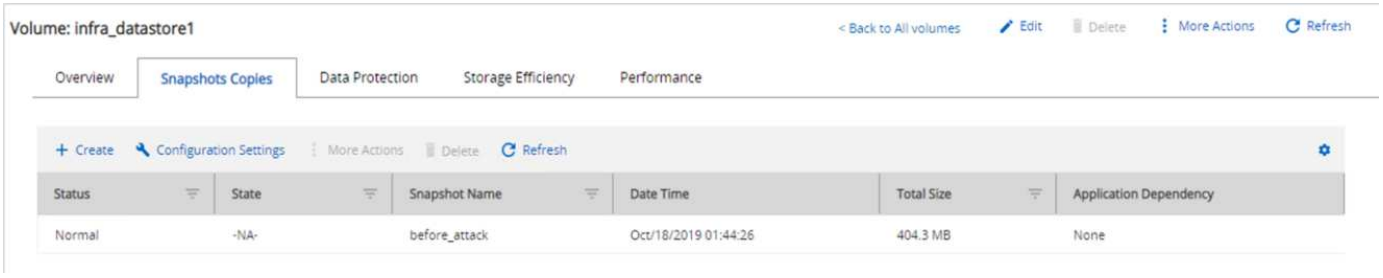
탐지

맬웨어가 파일을 암호화하기 시작한 순간부터 스냅샷 복사본의 크기가 기하급수적으로 증가하고 스토리지 효율성 백분율이 기하급수적으로 감소하게 되었습니다.

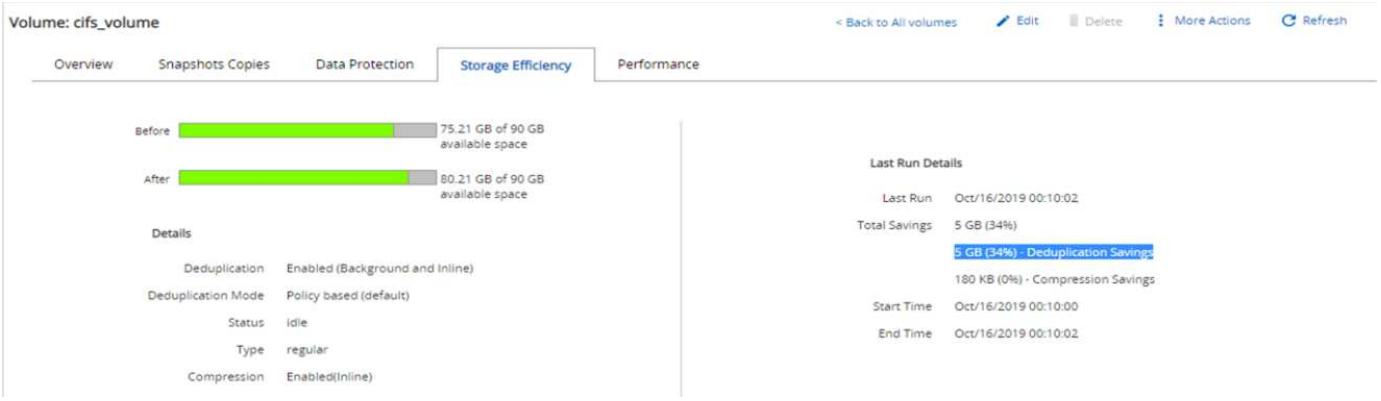
공격 중에 CIFS 공유를 호스팅하는 볼륨에서 스냅샷 크기가 820.98MB로 대폭 증가되는 것을 발견했습니다.



VM을 호스팅하는 볼륨에서 스냅샷 복사본 크기가 404.3MB로 증가되는 것을 발견했습니다.



CIFS 공유를 호스팅하는 볼륨의 스토리지 효율성이 34%로 감소했습니다.



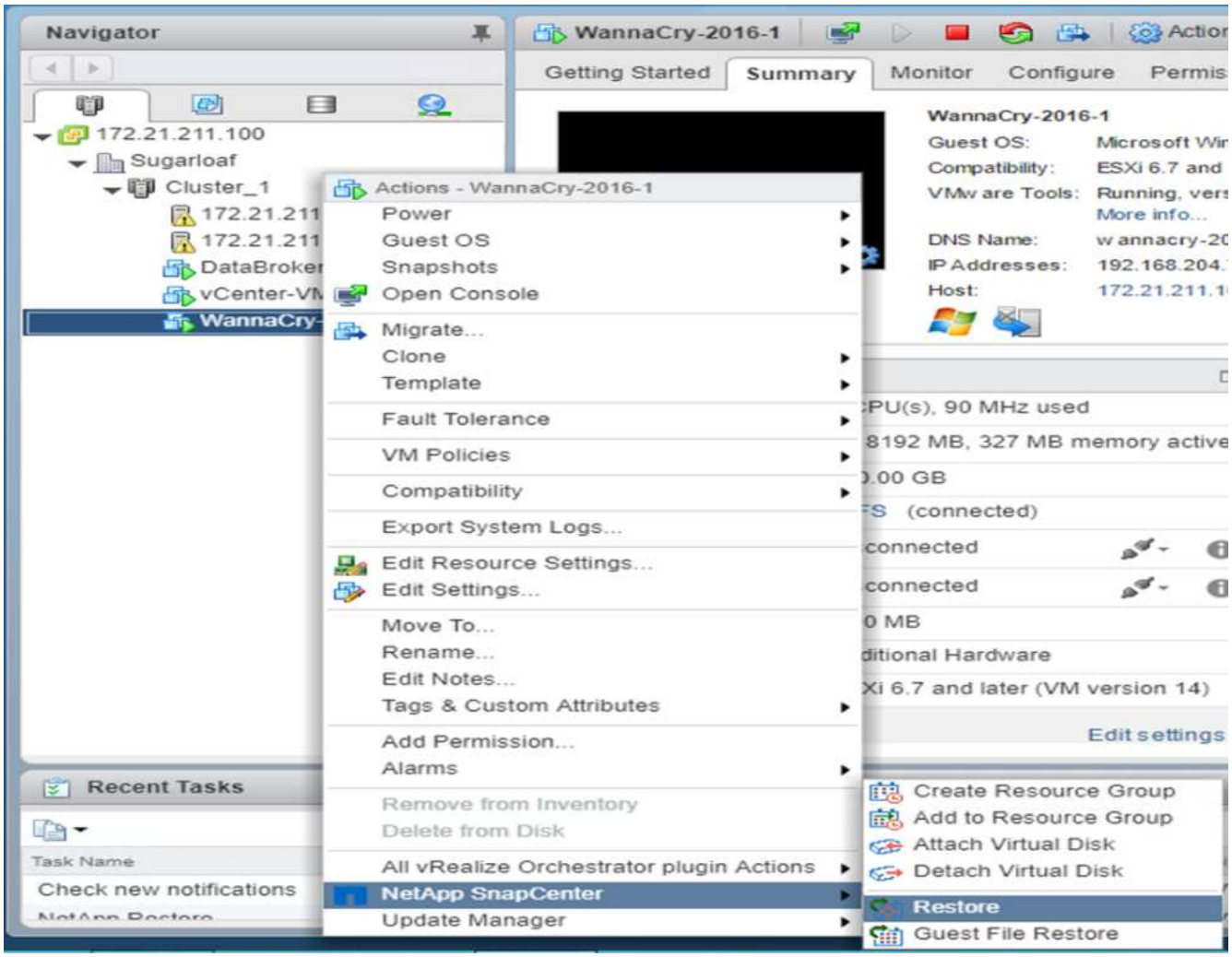
해결

공격 전에 생성된 클린 스냅샷 복사본을 사용하여 VM 및 매핑된 CIFS 공유를 복구합니다.

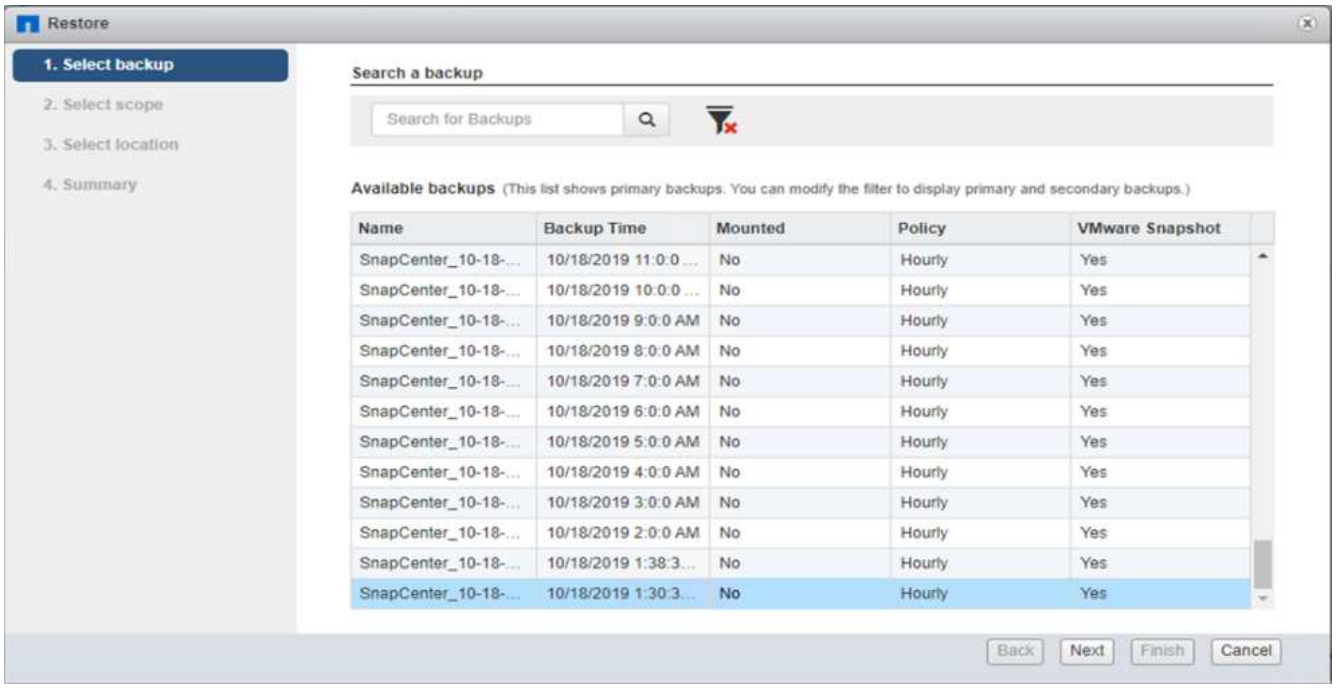
- VM 복원 *

VM을 복원하려면 다음 단계를 완료하십시오.

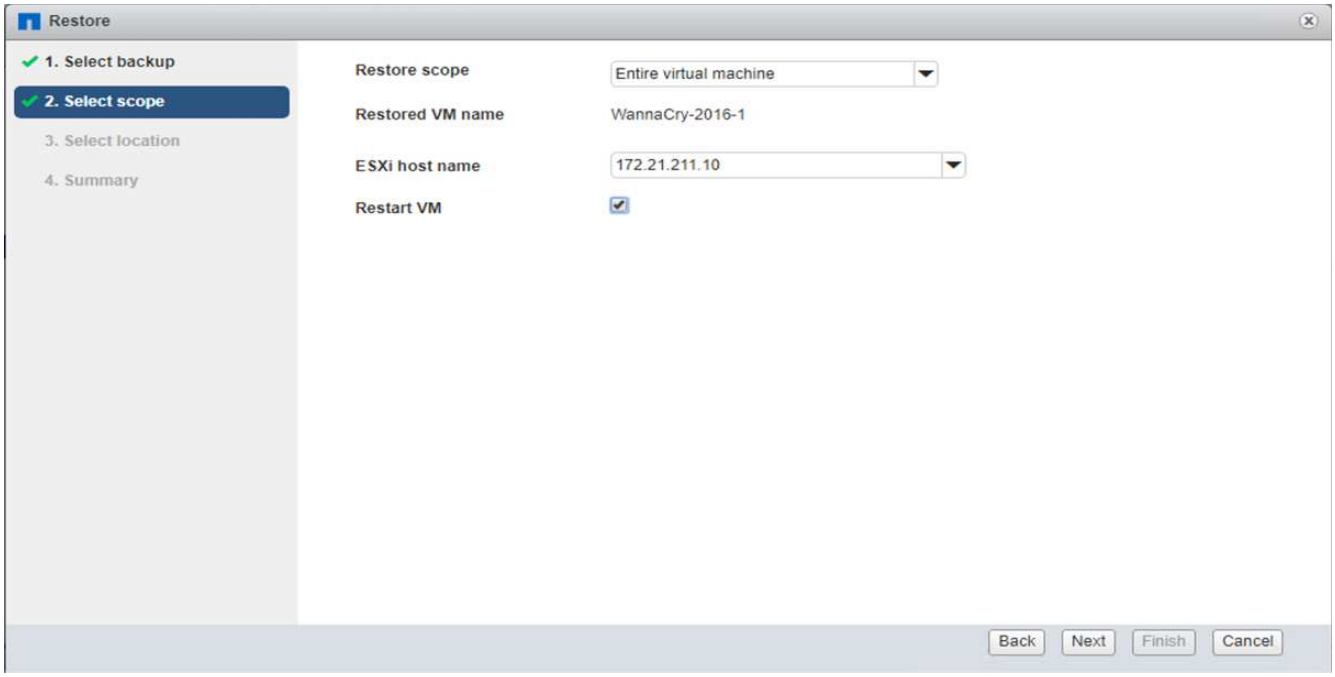
1. SnapCenter에서 생성한 스냅샷 복사본을 사용하여 VM을 복원합니다.



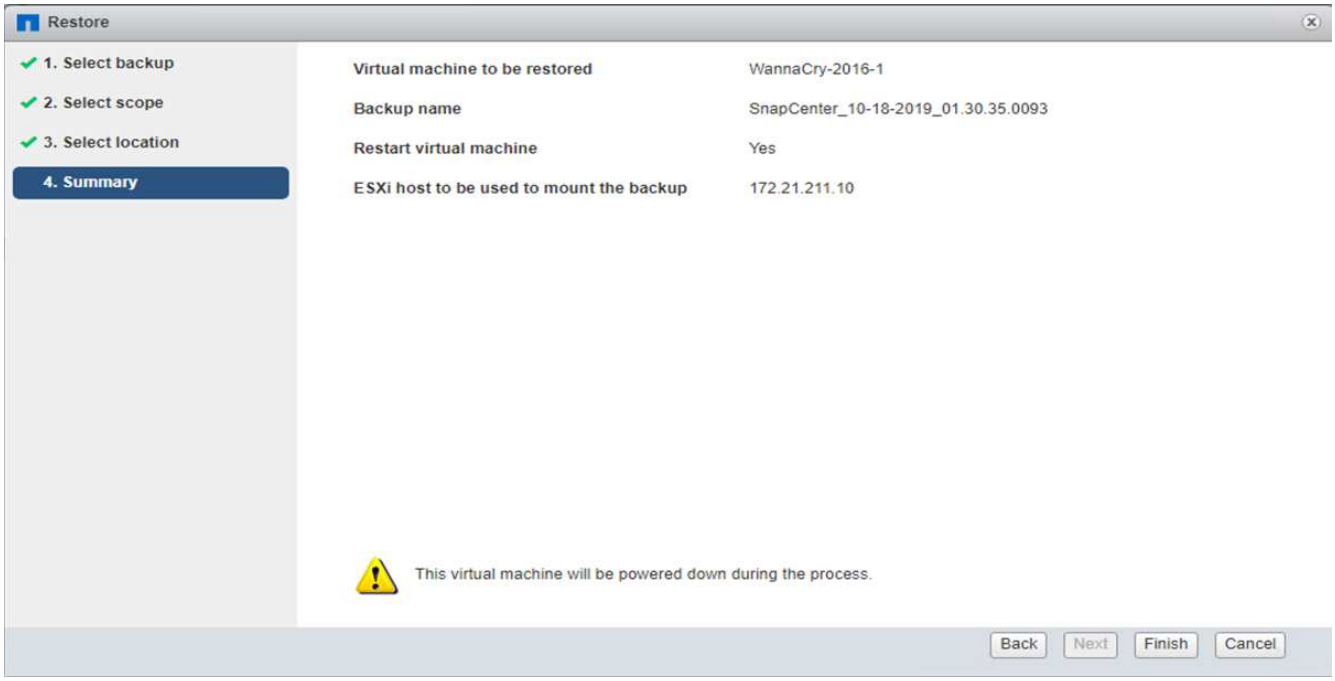
2. 복구할 VMware 정합성 보장 스냅샷 복사본을 선택합니다.



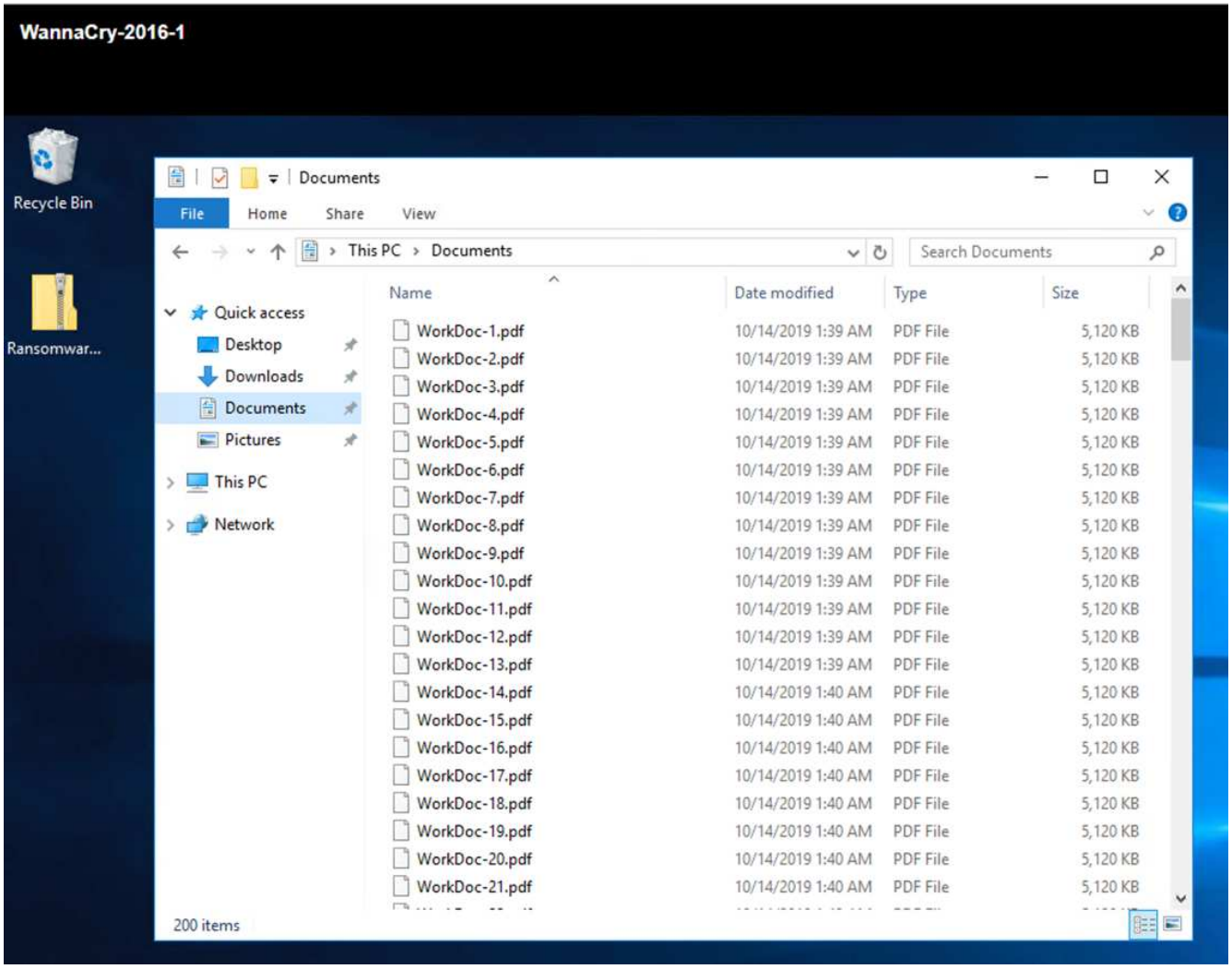
3. 전체 VM이 복원되고 다시 시작됩니다.



4. 마침 을 클릭하여 복원 프로세스를 시작합니다.



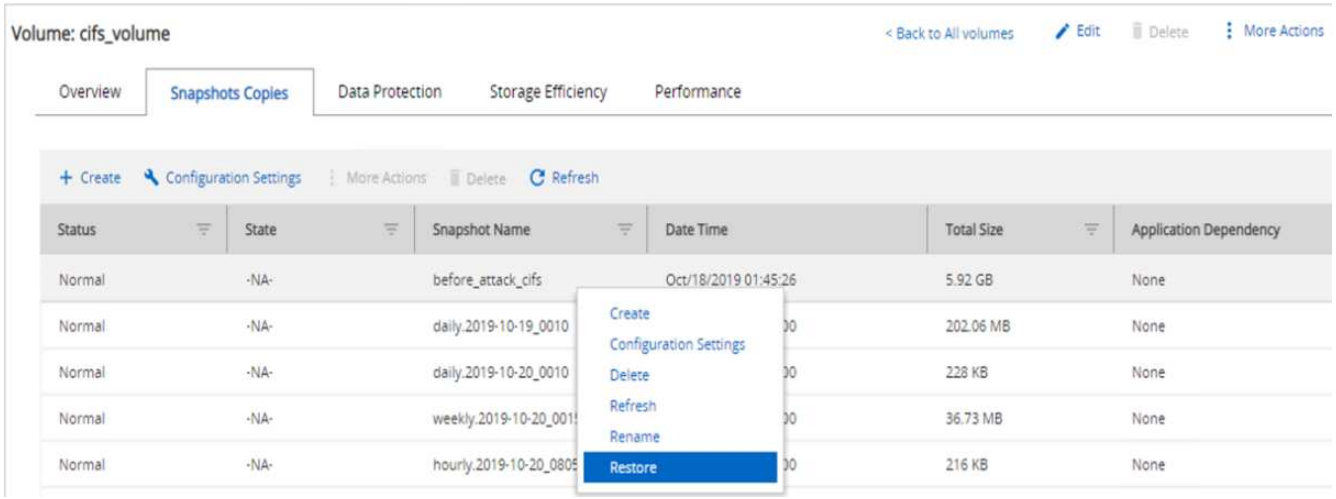
5. VM 및 해당 파일이 복원됩니다.



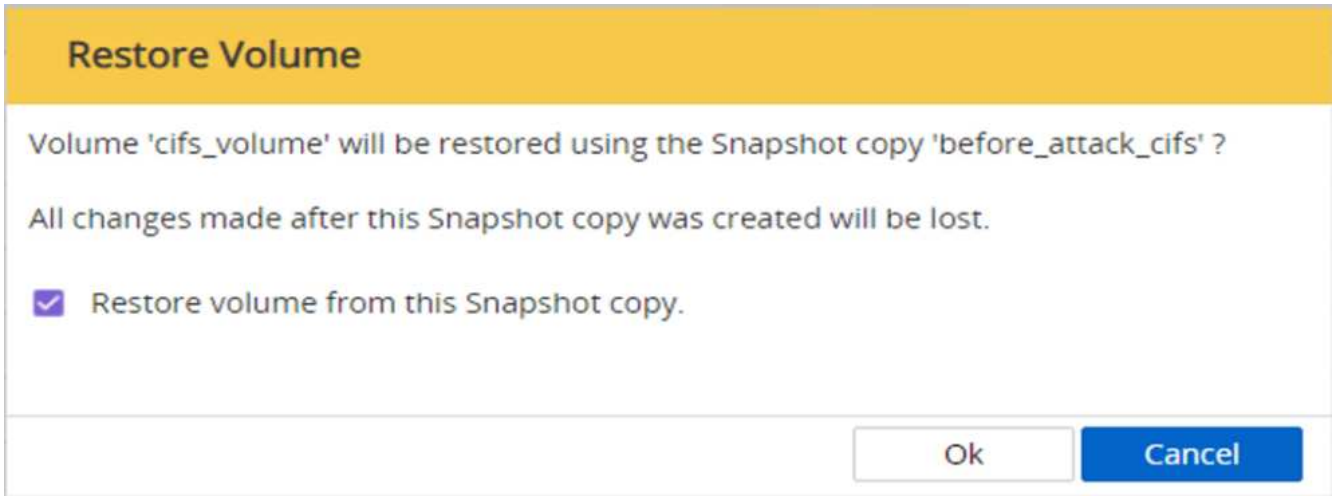
◦ CIFS 공유 복원 *

CIFS 공유를 복구하려면 다음 단계를 수행하십시오.

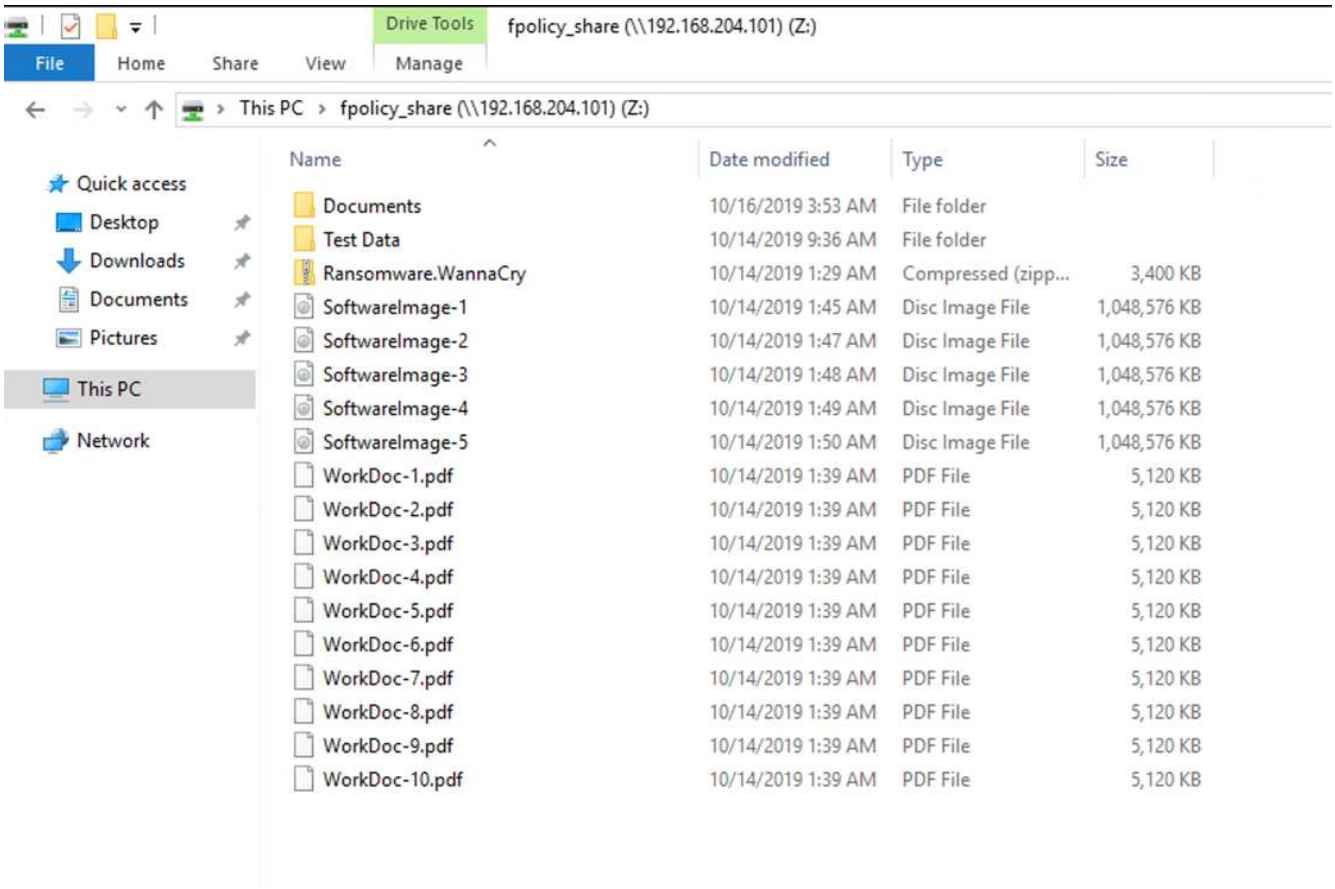
1. 공격 전에 생성된 볼륨의 스냅샷 복사본을 사용하여 공유를 복구합니다.



2. 확인 을 클릭하여 복원 작업을 시작합니다.



3. 복구 후 CIFS 공유를 봅니다.



사례 **2: WannaCry**는 **VM** 내의 파일 시스템을 암호화하고 **FPolicy**를 통해 보호되는 매핑된 **CIFS** 공유를 암호화합니다

예방

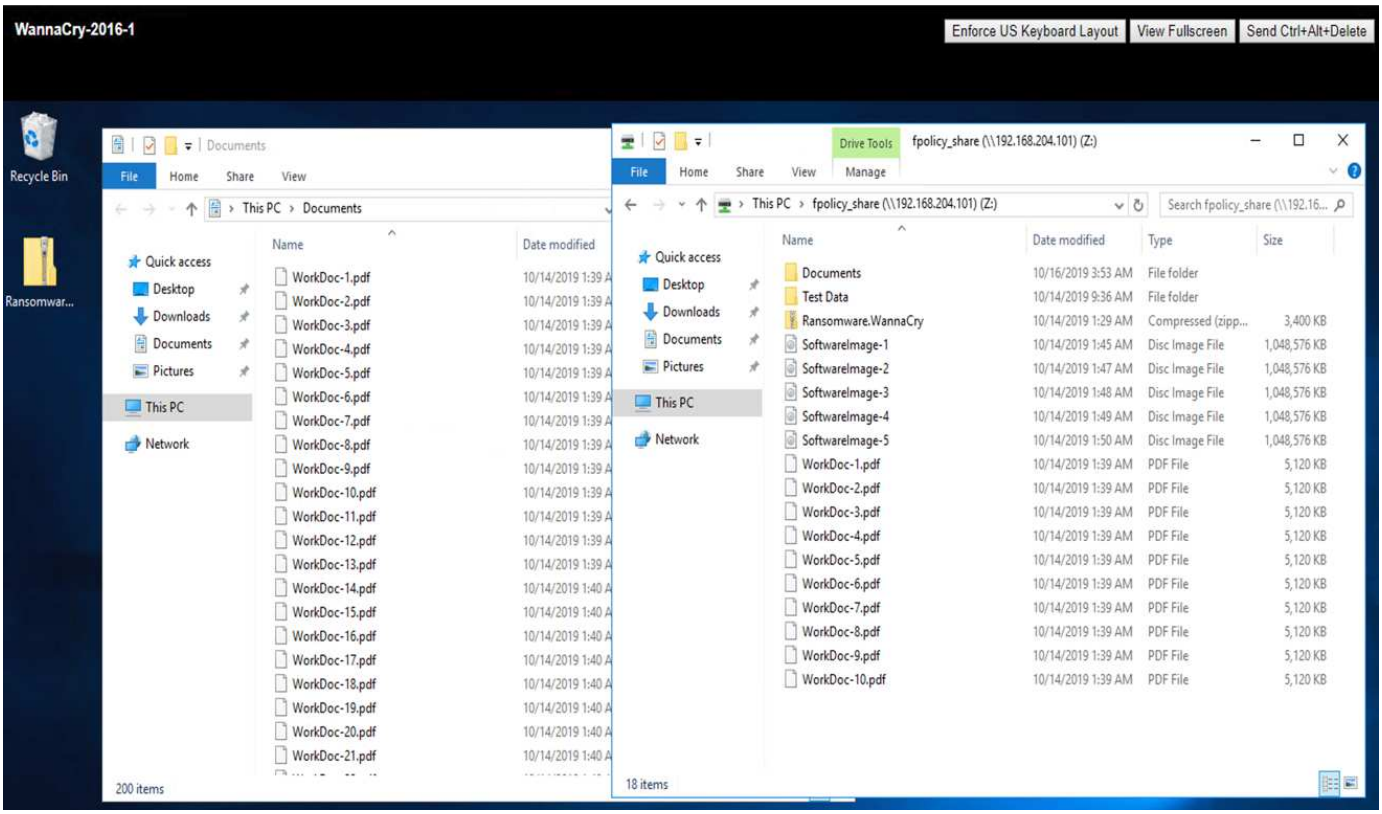
- FPolicy 구성 * 을 참조하십시오

CIFS 공유에서 FPolicy를 구성하려면 ONTAP 클러스터에서 다음 명령을 실행하십시오.

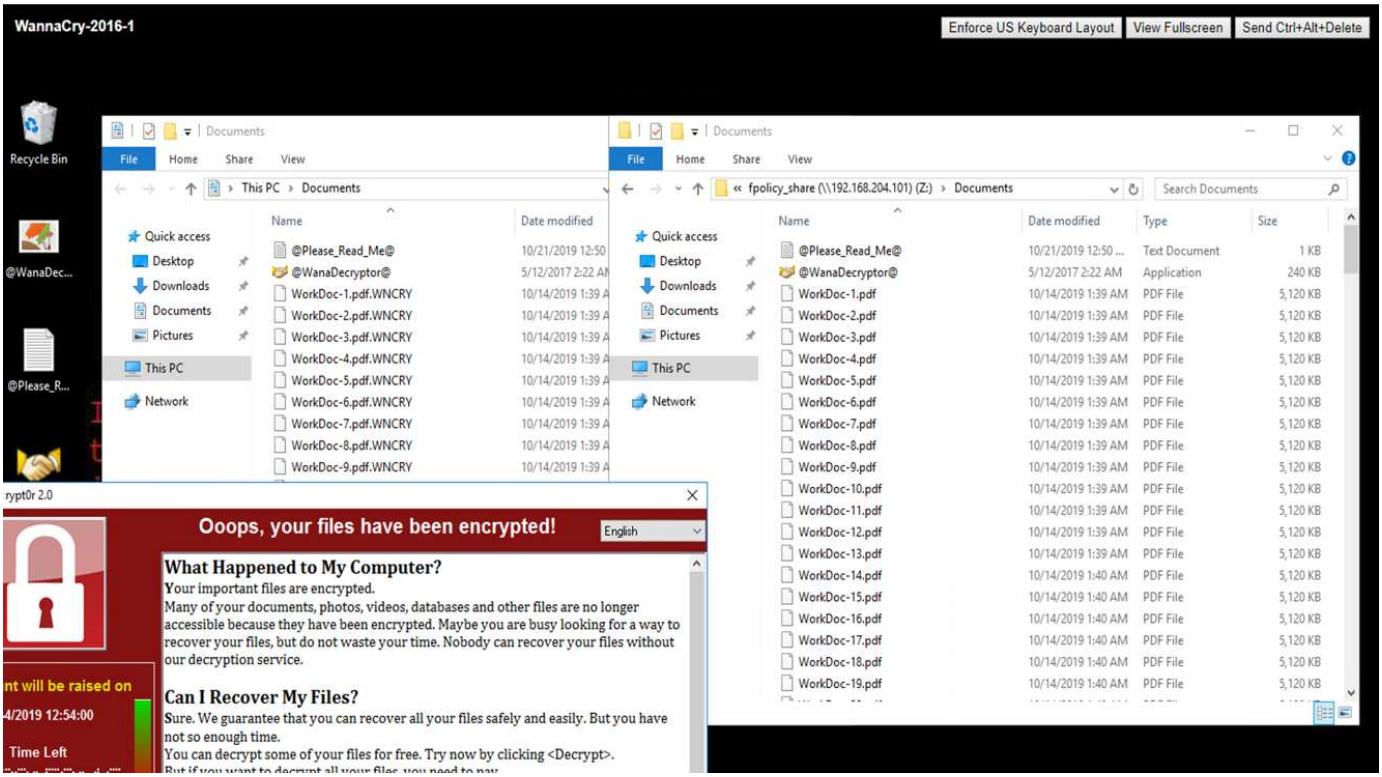
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

이 정책을 사용하면 WNCRY, Locky 및 ad4c 확장명을 가진 파일은 파일 생성, 이름 바꾸기, 쓰기 또는 열기 작업을 수행할 수 없습니다.

공격하기 전에 파일의 상태를 확인합니다. 암호화되지 않은 상태로 깨끗한 시스템에 있습니다.



VM의 파일은 암호화됩니다. WannaCry 맬웨어는 CIFS 공유의 파일을 암호화하려고 하지만 FPolicy는 파일이 영향을 받지 않도록 합니다.



대가를 지불하지 않고 비즈니스 운영을 지속하십시오

이 문서에 설명된 NetApp 기능은 공격 후 몇 분 내에 데이터를 복구하고 공격을 차단함으로써 비즈니스 운영을 방해받지 않고 계속할 수 있도록 합니다.

원하는 RPO(복구 시점 목표)를 충족하도록 스냅샷 복사본 스케줄을 설정할 수 있습니다. 스냅샷 복사본 기반 복원 작업은 매우 빠르게 수행되므로 RTO(복구 시간 목표)를 매우 짧게 달성할 수 있습니다.

무엇보다, 공격으로 인한 대가를 지불하지 않아도 되며, 신속하게 정상 운영으로 돌아갈 수 있습니다.

결론

랜섬웨어는 조직 범죄의 산물이며 공격자는 윤리적으로 행동하지 않습니다. 이들은 돈을 받은 후에도 암호 해독 키를 제공하지 않을 수 있습니다. 피해자는 데이터를 잃을 뿐만 아니라 상당한 금액의 돈까지 잃게 되고 운영 데이터의 손실로 인한 결과에 직면하게 됩니다.

에 따르면 "Forbes 기사를 참조하십시오"랜섬웨어 피해자 중 오직 19%만 대가를 지불한 후 데이터를 돌려받습니다. 따라서 공격자는 공격 시 대가를 지불하지 않는 것이 좋습니다. 대가를 지불하면 비즈니스 모델에 대한 믿음을 강화할 수 있기 때문입니다.

데이터 백업 및 복원 작업은 랜섬웨어 복구의 중요한 부분입니다. 따라서 비즈니스 계획의 필수 요소로 포함되어야 합니다. 이러한 작업의 구현 예산을 책정하여 공격 발생 시 복구 기능에 영향을 주지 않도록 해야 합니다.

중요한 것은 이 과정에서 올바른 기술 파트너를 선택하는 것입니다. FlexPod은 기본적으로 All-Flash FAS 시스템에서 추가 비용 없이 필요한 기능을 대부분 제공합니다.

감사의 말

저자는 이 문서 작성에 도움을 주신 다음 분들께 감사 드립니다.

- Jorge Gomez Navarrete, NetApp
- NetApp, Ganesh Kamath

추가 정보

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NetApp Snapshot 소프트웨어

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter 백업 관리

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock 데이터 규정 준수

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- NetApp 제품 설명서

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco AMP(Advanced Malware Protection)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

FIPS 140-2 Security-호환 FlexPod 솔루션을 통한 의료 서비스 지원

TR-4892: FIPS 140-2 Security-compliant FlexPod solution for healthcare

Cisco의 NetApp John McAbel, JayaKishore Esanakula

경제 및 임상 보건법(HITECH)을 위한 의료 정보 기술(Health Information Technology for Economic and Clinical Health Act, HITECH)에는 전자 보호 건강 정보(ePHI)에 대한 FIPS(Federal Information Processing Standard) 140-2의 검증된 암호화가 필요합니다. Hit(Health Information Technology) 애플리케이션 및 소프트웨어는 FIPS 140-2를 준수하여 프로모션 상호 운용성 프로그램(이전의 의미 있는 사용 인센티브 프로그램) 인증을 취득해야 합니다. 자격을 갖춘 제공자 및 병원은 Medicare 및 Medicaid 인센티브를 받을 때 FIPS 140-2(Level 1) 준수 히트(Hit)를 사용하고 중앙 의료보험 및 메디케이드(Center for Medicare and

Medicaid, CMS)에서 보상금 부과를 방지해야 합니다. FIPS 140-2 인증 암호화 알고리즘은 에 따라 필요한 기술 보호 수단으로서 제공됩니다 "보안 규칙" HIPAA(Health Information Portability and Accountability Act).

FIPS 140-2는 미국 중요한 정보를 보호하는 하드웨어, 소프트웨어 및 펌웨어의 암호화 모듈에 대한 보안 요구 사항을 설정하는 정부 표준입니다. 표준 준수는 미국 정부가 사용하도록 규정하고 있습니다 금융 서비스 및 의료와 같은 규제 대상 산업에서도 자주 사용됩니다. 이 기술 보고서를 통해 독자는 FIPS 140-2 보안 표준을 높은 수준에서 이해할 수 있습니다. 또한 의료 기관이 직면한 다양한 위협을 청중이 이해하는 데 도움이 됩니다. 마지막으로, 기술 보고서를 통해 FlexPod 통합 인프라에 FIPS 140-2 규격 FlexPod 시스템을 구축하여 의료 자산을 보호하는 방법을 파악할 수 있습니다.

범위

이 문서는 FIPS 140-2 보안 규정을 준수해야 하는 하나 이상의 의료 IT 애플리케이션 또는 솔루션을 호스팅하기 위한 Cisco Unified Computing System(Cisco UCS), Cisco Nexus, Cisco MDS 및 NetApp ONTAP 기반 FlexPod 인프라의 기술 개요입니다.

대상

이 문서는 의료 산업의 기술 리더 및 Cisco와 NetApp 파트너 솔루션 엔지니어 및 프로페셔널 서비스 직원을 위한 것입니다. NetApp은 사용자가 컴퓨팅 및 스토리지 사이징 개념을 잘 이해하고 있을 뿐만 아니라 의료 위협, 의료 보안, 의료 IT 시스템, Cisco UCS 및 NetApp 스토리지 시스템에 대한 기술적 지식을 갖추고 있다고 가정합니다.

"다음은 의료 분야의 사이버 보안 위협입니다."

의료 분야의 사이버 보안 위협

"이전: 소개."

모든 문제는 새로운 기회를 제공합니다. COVID 범세계적 확산으로 인해 이러한 기회 중 하나가 발생할 수 있습니다. 에 따르면 "보고서" HHS(Department of Health and Human Services) 사이버 보안 프로그램을 통해 COVID 대응은 랜섬웨어 공격 횟수를 늘렸습니다. 2020년 3월 셋째 주에 등록된 새로운 인터넷 도메인은 6,000개에 달했습니다. 도메인 중 50% 이상이 맬웨어를 호스팅했습니다. 랜섬웨어 공격은 2020년 전체 의료 데이터 침해의 거의 50%를 차지하여 630개 이상의 의료 조직과 약 2,900만 개의 의료 기록에 영향을 주었습니다. 19개의 침공자/현장은 갈취의 두 배가 되었습니다. 24.5%에 의료 산업에서는 2020년에 데이터 유출 사고가 가장 많이 발생하였습니다.

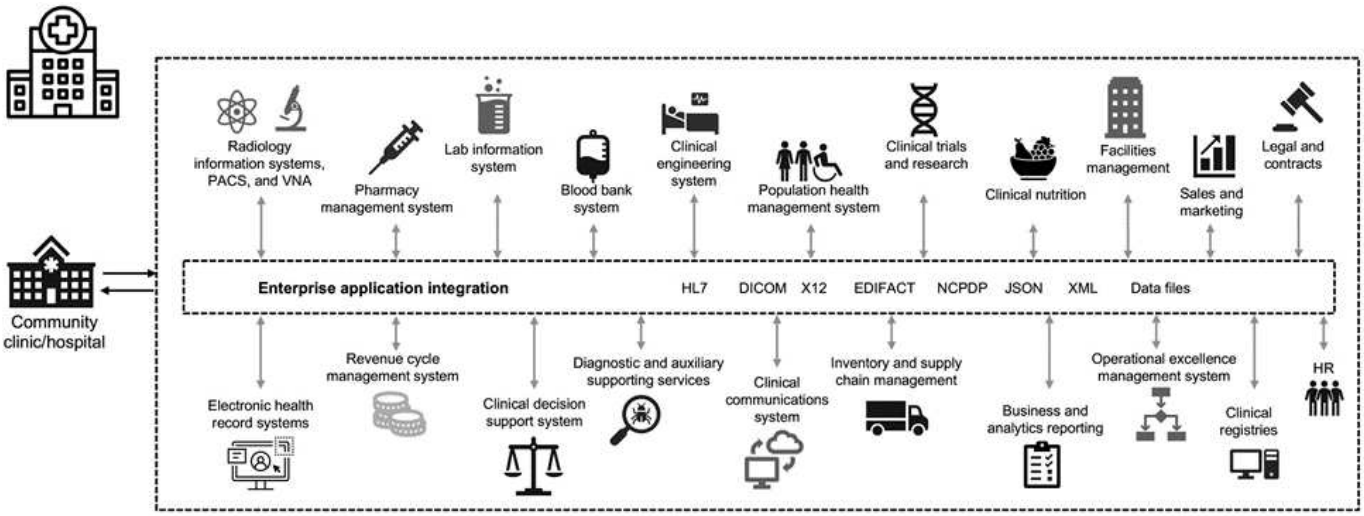
악의적인 요원들이 정보를 판매하거나 이를 파괴하거나 노출시키겠다고 위협하여 PHI(Protected Health Information)의 보안 및 개인 정보를 침해하려고 시도했습니다. ePHI에 대한 무단 접근을 위해 대상 및 대량 방송 시도가 자주 이루어집니다. 2020년 하반기에 노출된 환자 기록의 약 75%는 업무 관계자가 피해를 본 덕분이었습니다.

다음 의료 조직 목록은 악의적인 에이전트의 표적이 되었습니다.

- 병원 시스템
- 생명 과학 연구소
- 연구 랩
- 재활 시설

- 지역 병원 및 클리닉

의료 기관을 구성하는 애플리케이션의 다양성은 부인할 수 없으며 복잡성이 증가하고 있습니다. 정보 보안 사무소는 방대한 IT 시스템 및 자산에 대한 거버넌스를 제공해야 하는 과제를 안고 있습니다. 다음 그림은 일반적인 병원 시스템의 임상적 기능을 보여줍니다.



환자 데이터가 이 영상의 중심에 있습니다. 환자 데이터 손실 및 민감한 의학적 상태와 관련된 오인은 매우 현실적입니다. 기타 중요한 문제로는 사회적 부담보, 협박메일, 프로파일링, 대상 마케팅, 악용, 지불자의 특권 이외의 의료 정보에 대한 지불자에 대한 잠재적인 재정적 책임 등이 있습니다.

의료에 대한 위협은 본질적으로 다차원적이며 영향을 줍니다. 전 세계 정부들은 ePHI를 보호하기 위해 다양한 규정을 제정했습니다. 의료 위협 요소의 해로운 영향과 진화하는 특성으로 인해 의료 기관은 모든 위협을 방어하기가 어렵습니다.

다음은 의료 분야에서 확인된 일반적인 위협 목록입니다.

- 랜섬웨어 공격
- 민감한 정보가 있는 장비 또는 데이터의 손실 또는 도난
- 피싱 공격
- 환자 안전에 영향을 줄 수 있는 연결된 의료 기기에 대한 공격
- 전자 메일 피싱 공격
- 장비 또는 데이터의 손실 또는 도난
- 원격 데스크톱 프로토콜 손상
- 소프트웨어 취약점

의료 조직은 디지털 에코시스템과 같이 복잡한 법률 및 규정 환경에서 사업을 운영하고 있습니다. 이 환경에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 국립보건조정관(의료 기술용) ONC 인증 전자보건정보기술상호운용성 표준
- Medicare 액세스 및 아동 건강 보험 프로그램 재허가 법(MACRA)/의미 있는 사용
- FDA(Food and Drug Administration)에 따른 다수의 의무
- 공동 위원회 인증 프로세스

- HIPAA 요구 사항
- HITECH 요구 사항
- 지불자의 최소 허용 위험 기준
- 개인 정보 보호 및 보안 규칙
- 연방 정보 보안 현대화 법안 요구 사항 연방 계약 및 연구 보조금은 국가 보건원 등의 기관을 통해 통합됩니다
- PCI-DSS(Payment Card Industry Data Security Standard)
- 약물 남용 및 정신 건강 서비스 관리(SAMHSA) 요건
- 재무 처리를 위한 Gramm-Leach-Bliley Act
- Stark 법률은 제휴 조직에 서비스를 제공하는 것과 관련이 있습니다
- 고등 교육에 참여하는 기관을 위한 가족교육권 및 개인정보보호법(FERPA)
- 유전정보차별금지법(GINA)
- EU의 새로운 GDPR(General Data Protection Regulation)

악의적 행위자가 의료 정보 시스템에 영향을 주지 않도록 보안 아키텍처 표준이 빠르게 발전하고 있습니다. 이러한 표준 중 하나는 NIST(National Institute of Standards and Technology)에서 정의한 FIPS 140-2입니다. FIPS 140-2 은 미국에 대해 자세히 설명합니다 암호화 모듈에 대한 정부 요구 사항 보안 요구 사항은 암호화 모듈의 보안 설계 및 구현과 관련된 영역을 다루며, 보안 요구 사항을 적용하여 보안 기능을 강화할 수 있습니다. 잘 정의된 암호화 경계를 통해 암호화 모듈을 최신 상태로 유지하면서 보안 관리를 쉽게 수행할 수 있습니다. 이러한 경계는 악의적인 행위자가 쉽게 악용할 수 있는 약한 암호화 모듈을 방지하는 데 도움이 됩니다. 또한 표준 암호화 모듈을 관리할 때 인적 오류를 방지할 수 있습니다.

NIST는 CSE(Communications Security Establishment)와 함께 FIPS 140-2 검증 수준에 대한 암호화 모듈을 인증하기 위해 CMVP(Cryptographic Module Validation Program)를 설립했습니다. FIPS 140-2 인증 모듈을 사용하는 연방 조직은 이동 중에도 기밀 또는 가치 있는 데이터를 보호해야 합니다. 민감하거나 중요한 정보를 보호하는 데 성공했기 때문에 많은 의료 시스템이 법적으로 요구되는 최소 보안 수준 이상으로 FIPS 140-2 암호화 모듈을 사용하여 ePHI를 암호화하기로 결정했습니다.

FlexPod FIPS 140-2 기능을 활용하여 구현하는 데 몇 시간(며칠이 아님)만 걸립니다. FIPS를 준수하는 것은 규모와 관계없이 대부분의 의료 조직에서 가능합니다. 암호화 경계가 명확하게 정의되고 문서화되고 간단한 구현 단계를 통해 FIPS 140-2 규격 FlexPod 아키텍처는 인프라를 위한 견고한 보안 기반을 마련하고 보안 위협에 대한 보호 수준을 더욱 높이기 위해 간단한 개선 기능을 제공할 수 있습니다.

"다음: FIPS 140-2의 개요"

FIPS 140-2 개요

"이전: 의료 분야의 사이버 보안 위협"

"FIPS 140-2" 컴퓨터 및 통신 시스템의 중요한 정보를 보호하는 보안 시스템 내에서 사용되는 암호화 모듈에 대한 보안 요구 사항을 지정합니다. 암호화 모듈은 하드웨어, 소프트웨어, 펌웨어 또는 조합 세트여야 합니다. FIPS는 암호화 경계 내에 포함된 암호화 알고리즘, 키 생성 및 키 관리자에 적용됩니다. FIPS 140-2는 제품, 아키텍처, 데이터 또는 에코시스템이 아닌 암호화 모듈에 특히 적용된다는 점을 이해하는 것이 중요합니다. 이 문서의 뒷부분에 나오는 주요 용어로 정의된 암호화 모듈은 승인된 보안 기능을 구현하는 특정 구성 요소(하드웨어, 소프트웨어 및 /또는 펌웨어)입니다. 또한 FIPS 140-2는 네 가지 레벨을 지정합니다. 승인된 암호화 알고리즘은

모든 수준에 공통적입니다. 각 보안 수준의 주요 요소 및 요구 사항은 다음과 같습니다.

- * 보안 수준 1 *
  - 암호화 모듈에 대한 기본 보안 요구 사항을 지정합니다(하나 이상의 승인된 알고리즘 또는 보안 기능이 필요함).
  - 운영 등급 구성 요소의 기본 요구 사항을 초과하는 수준 1에는 지정된 물리적 보안 메커니즘이 필요하지 않습니다.
- * 보안 수준 2 *
  - 코팅 또는 봉인, 탈착식 커버 또는 암호화 모듈의 도어에 잠금 장치와 같은 변조 방지 솔루션을 사용하여 변조 증거에 대한 요구 사항을 추가하여 물리적 보안 메커니즘을 강화합니다.
  - 최소한 역할 기반 액세스 제어(RBAC)가 필요하며, 이 경우 암호화 모듈은 운영자 또는 관리자의 권한을 인증하여 특정 역할을 수행하고 해당 기능 세트를 수행해야 합니다.
- * 보안 수준 3 *
  - 레벨 2의 변조 가능한 요구 사항을 기반으로 암호화 모듈 내의 중요 보안 매개 변수(CSP)에 대한 추가 액세스를 방지합니다.
  - 수준 3에 필요한 물리적 보안 메커니즘은 물리적 액세스 시도 또는 암호화 모듈의 사용 또는 수정 시도를 감지하고 이에 대응할 가능성이 높은 것을 목적으로 합니다. 암호화 모듈의 이동식 덮개가 열릴 때 모든 일반 텍스트 CSP를 제로화하는 강력한 인클로저, 변조 감지 및 응답 회로가 이러한 예에 포함될 수 있습니다.
  - 레벨 2에 지정된 RBAC 메커니즘의 보안을 강화하기 위해 ID 기반 인증 메커니즘이 필요합니다. 암호화 모듈은 운영자의 ID를 인증하고 운영자가 역할을 사용하고 역할의 기능을 수행할 권한이 있는지 확인합니다.
- * 보안 수준 4 *
  - FIPS 140-2의 최고 보안 수준.
  - 물리적으로 보호되지 않는 환경에서 작업을 수행하는 데 가장 유용한 레벨입니다.
  - 이 수준에서 물리적 보안 메커니즘은 물리적 액세스에서 승인되지 않은 시도를 감지하고 대응하는 책임을 지고 암호화 모듈에 대한 완벽한 보호를 제공하기 위한 것입니다.
  - 암호화 모듈의 침투 또는 노출은 감지 가능성이 높으며 모든 비보안 또는 일반 텍스트 CSP의 즉각적인 제로로 이어질 수 있습니다.

"다음: 컨트롤 플레인 대 데이터 플레인"

컨트롤 플레인 대 데이터 플레인

"이전: FIPS 140-2의 개요"

FIPS 140-2 전략을 구현할 때는 어떤 것이 보호되고 있는지 이해하는 것이 중요합니다. 컨트롤 플레인과 데이터 플레인의 두 영역으로 쉽게 나눌 수 있습니다. 제어 계층이란 FlexPod 시스템 내에서 구성 요소의 제어 및 운영에 영향을 미치는 측면, 예를 들어 NetApp 스토리지 컨트롤러, Cisco Nexus 스위치, Cisco UCS 서버에 대한 관리 액세스 권한을 말합니다. 이 계층의 보호는 관리자가 장치에 연결하고 변경할 때 사용할 수 있는 프로토콜과 암호화 사이퍼를 제한함으로써 제공됩니다. 데이터 플레인은 FlexPod 시스템 내의 PHI와 같은 실제 정보를 나타냅니다. 이는 저장된 데이터를 암호화하고 FIPS를 위해 다시 암호화하여 보호하므로 사용 중인 암호화 모듈이 표준을 충족하도록 합니다.

"다음으로, FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2를 살펴보겠습니다."

FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2

"이전: 컨트롤 플레인 대 데이터 플레인"

FlexPod 아키텍처는 FIPS 140-2를 준수하는 Cisco UCS 서버로 설계할 수 있습니다. 미국 S. NIST, Cisco UCS 서버는 FIPS 140-2 레벨 1 준수 모드에서 작동할 수 있습니다. FIPS 호환 Cisco 구성 요소의 전체 목록은 을 참조하십시오 "Cisco의 FIPS 140 페이지". Cisco UCS Manager는 FIPS 140-2 검증을 거쳤습니다.

Cisco UCS 및 패브릭 인터커넥트

Cisco UCS Manager는 Cisco Fabric Interconnect(FI)에서 구축 및 실행됩니다.

Cisco UCS 및 FIPS 활성화 방법에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS Manager 설명서".

각 패브릭 A 및 B의 Cisco 패브릭 인터커넥트에서 FIPS 모드를 활성화하려면 다음 명령을 실행합니다.

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

Cisco UCS Manager 릴리즈 3.2(3)의 클러스터에서 Cisco UCS Manager 릴리즈 3.2(3) 이전 릴리즈의 FI로 FI를 교체하려면 교체 FI를 클러스터에 추가하기 전에 기존 FI에서 FIPS 모드(FIPS 모드 비활성화)를 비활성화하십시오. Cisco UCS Manager의 부팅 과정에서 클러스터가 구성되면 FIPS 모드가 자동으로 설정됩니다.

Cisco는 컴퓨팅 또는 애플리케이션 계층에서 구현할 수 있는 다음과 같은 주요 제품을 제공합니다.

- * 엔드포인트용 Cisco AMP(Advanced Malware Protection).* Microsoft Windows 및 Linux 운영 체제에서 지원되는 이 솔루션은 예방, 검색 및 응답 기능을 통합합니다. 이 보안 소프트웨어는 침입을 방지하고 진입 지점에서 맬웨어를 차단하며 파일 및 프로세스 활동을 지속적으로 모니터링 및 분석하여 일선 방어를 우회할 수 있는 위협을 신속하게 탐지, 억제 및 해결합니다. AMP의 MAP(Malicious Activity Protection) 구성 요소는 모든 엔드포인트 활동을 지속적으로 모니터링하고 엔드포인트에서 실행 중인 프로그램의 비정상적인 동작을 런타임 감지 및 차단합니다. 예를 들어, 엔드포인트 동작에 랜섬웨어가 표시되면 문제가 되는 프로세스가 종료되어 엔드포인트 암호화가 예방되고 공격이 중지됩니다.
- 이메일 보안을 위한 * AMP. * 이메일은 맬웨어를 유포하고 사이버 공격을 수행하는 주요 수단으로 자리 잡았습니다. 평균적으로 하루 동안 약 1,000억 개의 이메일이 교환되며, 이를 통해 공격자들은 사용자 시스템에 대한 탁월한 침투 벡터를 얻을 수 있습니다. 따라서 이 공격 라인을 방어하는 것이 절대적으로 중요합니다. AMP는 제로 데이 익스플로잇(zero-day exploit) 및 악성 첨부 파일에 숨겨진 악성 맬웨어와 같은 위협에 대한 이메일을 분석합니다. 또한 업계 최고의 URL 인텔리전스를 사용하여 악성 링크를 차단합니다. 스피어 피싱, 랜섬웨어 및 기타 정교한 공격에 대한 고급 보호 기능을 제공합니다.
- * NGIPS(Next-Generation Intrusion Prevention System). * Cisco firepower NGIPS는 데이터 센터에서 물리적 어플라이언스로 구축하거나 VMware(NGIPSv for VMware)에서 가상 어플라이언스로 구축할 수 있습니다. 이 고효율 침입 방지 시스템은 안정적인 성능과 낮은 총 소유 비용을 제공합니다. AMP, 애플리케이션 가시성 및 제어, URL 필터링 기능을 제공하기 위해 선택적 구독 라이센스로 위협 보호를 확장할 수 있습니다. 가상화된 NGIPS는 VM(가상 시스템) 간의 트래픽을 검사하고 리소스가 제한된 사이트에서 NGIPS 솔루션을 쉽게 배포 및 관리할 수 있도록 하여 물리적 자산과 가상 자산 모두의 보호를 강화합니다.

"다음으로, FlexPod Cisco 네트워킹 및 FIPS 140-2가 있습니다."

FlexPod Cisco 네트워킹 및 FIPS 140-2

"이전: FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2가 지원됩니다."

Cisco MDS를 참조하십시오

소프트웨어 8.4.x가 포함된 Cisco MDS 9000 시리즈 플랫폼은 "FIPS 140-2 규격 준수". Cisco MDS는 SNMPv3 및 SSH에 대해 암호화 모듈 및 다음 서비스를 구현합니다.

- 각 서비스를 지원하는 세션 설정
- 각 서비스 키 파생 기능을 지원하는 모든 기본 암호화 알고리즘
- 각 서비스에 대한 해싱입니다
- 각 서비스의 대칭 암호화

FIPS 모드를 활성화하기 전에 MDS 스위치에서 다음 작업을 완료합니다.

1. 암호의 길이는 최소 8자 이상이어야 합니다.
2. 텔넷을 비활성화합니다. 사용자는 SSH만 사용하여 로그인해야 합니다.
3. RADIUS/TACACS+를 통해 원격 인증을 비활성화합니다. 스위치에 로컬로 있는 사용자만 인증을 받을 수 있습니다.
4. SNMP v1 및 v2를 비활성화합니다. SNMPv3에 대해 구성된 스위치의 기존 사용자 계정은 인증을 위해 SHA 와 개인 정보 보호를 위해 AES/3DES 로만 구성해야 합니다.
5. VRRP를 비활성화합니다.
6. 인증을 위해 MD5가 있거나 암호화를 위해 DES가 있는 모든 IKE 정책을 삭제합니다. 인증에 SHA를 사용하고 암호화에 3DES/AES를 사용하도록 정책을 수정합니다.
7. 모든 SSH 서버 RSA1 키 쌍을 삭제합니다.

FIPS 모드를 활성화하고 MDS 스위치에 FIPS 상태를 표시하려면 다음 단계를 수행하십시오.

1. FIPS 상태를 표시합니다.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048비트 SSH 키를 설정합니다.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS 모드를 활성화합니다.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. FIPS 상태를 표시합니다.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. 실행 중인 구성에 구성을 저장합니다.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. MDS 스위치를 다시 시작합니다

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. FIPS 상태를 표시합니다.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

자세한 내용은 을 참조하십시오 "FIPS 모드 활성화".

Cisco Nexus를 참조하십시오

Cisco Nexus 9000 시리즈 스위치(버전 9.3)는 "FIPS 140-2 규격 준수". Cisco Nexus는 SNMPv3 및 SSH에 대해 암호화 모듈 및 다음 서비스를 구현합니다.

- 각 서비스를 지원하는 세션 설정
- 각 서비스 키 파생 기능을 지원하는 모든 기본 암호화 알고리즘
- 각 서비스에 대한 해싱입니다
- 각 서비스의 대칭 암호화

FIPS 모드를 활성화하기 전에 Cisco Nexus 스위치에서 다음 작업을 완료하십시오.

1. 텔넷을 비활성화합니다. 사용자는 SSH(Secure Shell)만 사용하여 로그인해야 합니다.
2. SNMPv1 및 v2를 비활성화합니다. SNMPv3에 대해 구성된 장치의 기존 사용자 계정은 인증을 위해 SHA 와 개인 정보 보호를 위해 AES/3DES 로만 구성해야 합니다.
3. 모든 SSH 서버 RSA1 키 쌍을 삭제합니다.
4. Cisco TrustSec 보안 연결 프로토콜(SAP) 협상 중에 사용할 HMAC-SHA1 메시지 무결성 검사(MIC)를 활성화합니다. 이렇게 하려면 CTS-MANUAL 또는 CTS-dot1x 모드에서 SAP hash-algorithm HMAC-SHA-1 명령을 입력한다.

Nexus 스위치에서 FIPS 모드를 활성화하려면 다음 단계를 수행하십시오.

1. 2048비트 SSH 키를 설정합니다.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048비트 SSH 키를 설정합니다.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS 모드를 활성화합니다.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer             1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Nexus 스위치를 다시 시작합니다.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. FIPS 상태를 표시합니다.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

또한 Cisco NX OS 소프트웨어는 네트워크 이상 및 보안 검색을 향상시키는 NetFlow 기능을 지원합니다. NetFlow는 네트워크의 모든 대화 메타데이터, 통신 관련 당사자, 사용 중인 프로토콜 및 트랜잭션 기간을 캡처합니다. 정보를 집계 및 분석한 후에는 정상적인 동작에 대한 통찰력을 제공할 수 있습니다. 또한 수집된 데이터를 통해 네트워크를 통해 확산되는 맬웨어와 같은 의심스러운 활동 패턴을 식별할 수 있으며, 그렇지 않을 경우 이를 간과할 수 있습니다. NetFlow는 흐름을 사용하여 네트워크 모니터링에 대한 통계를 제공합니다. 흐름은 소스 인터페이스(또는 VLAN)에 도착하고 키에 대해 동일한 값을 갖는 패킷의 단방향 스트림입니다. 키는 패킷 내의 필드에 대해 식별된 값입니다. 유동 레코드를 사용하여 유동의 고유 키를 정의하는 유동을 만듭니다. 흐름 내보내기를 사용하여 Cisco Stealthwatch와 같은 원격 NetFlow 수집기로 플로우에 대해 NetFlow에서 수집하는 데이터를 내보낼 수 있습니다. Stealthwatch는 이 정보를 사용하여 네트워크를 지속적으로 모니터링하고 랜섬웨어 발생 시 실시간 위협 탐지 및 사고 대응 법의학 조사를 제공합니다.

"다음으로, FlexPod NetApp ONTAP 스토리지와 FIPS 140-2를 살펴보겠습니다."

FlexPod NetApp ONTAP 스토리지 및 FIPS 140-2

"이전: FlexPod Cisco 네트워킹 및 FIPS 140-2."

NetApp은 다양한 하드웨어, 소프트웨어 및 서비스를 제공하며, 여기에는 표준에 따라 검증된 암호화 모듈의 다양한 구성요소가 포함될 수 있습니다. 따라서 NetApp은 제어 플레인 및 데이터 플레인을 위해 FIPS 140-2 규정 준수를 위한 다양한 접근 방식을 사용합니다.

- NetApp에는 전송 중인 데이터 및 유휴 데이터의 암호화에 대한 레벨 1 검증을 획득한 암호화 모듈이 포함되어 있습니다.
- NetApp은 FIPS 140-2 검증을 거친 하드웨어 및 소프트웨어 모듈을 모두 인수합니다. 예를 들어, NetApp Storage Encryption 솔루션은 FIPS 레벨 2 인증 드라이브를 활용합니다.
- NetApp 제품은 제품 또는 기능이 검증 범위 내에 있지 않더라도 표준을 준수하는 방법으로 검증된 모듈을 사용할 수 있습니다. 예를 들어, NetApp Volume Encryption(NVE)은 FIPS 140-2 규정을 준수합니다. 이 솔루션은 개별적으로 검증되지 않았지만 레벨 1의 검증된 NetApp 암호화 모듈을 활용합니다. 사용 중인 ONTAP 버전에 대한 규정 준수 사항을 자세히 알아보려면 FlexPod SME에게 문의하십시오.
- NetApp 암호화 모듈은 FIPS 140-2 레벨 1의 검증을 거쳤습니다 *
- NetApp CSM(Cryptographic Security Module)은 FIPS 140-2 레벨 1의 검증을 거쳤습니다.
- NetApp 자체 암호화 드라이브는 FIPS 140-2 레벨 2의 검증을 거쳤습니다 *

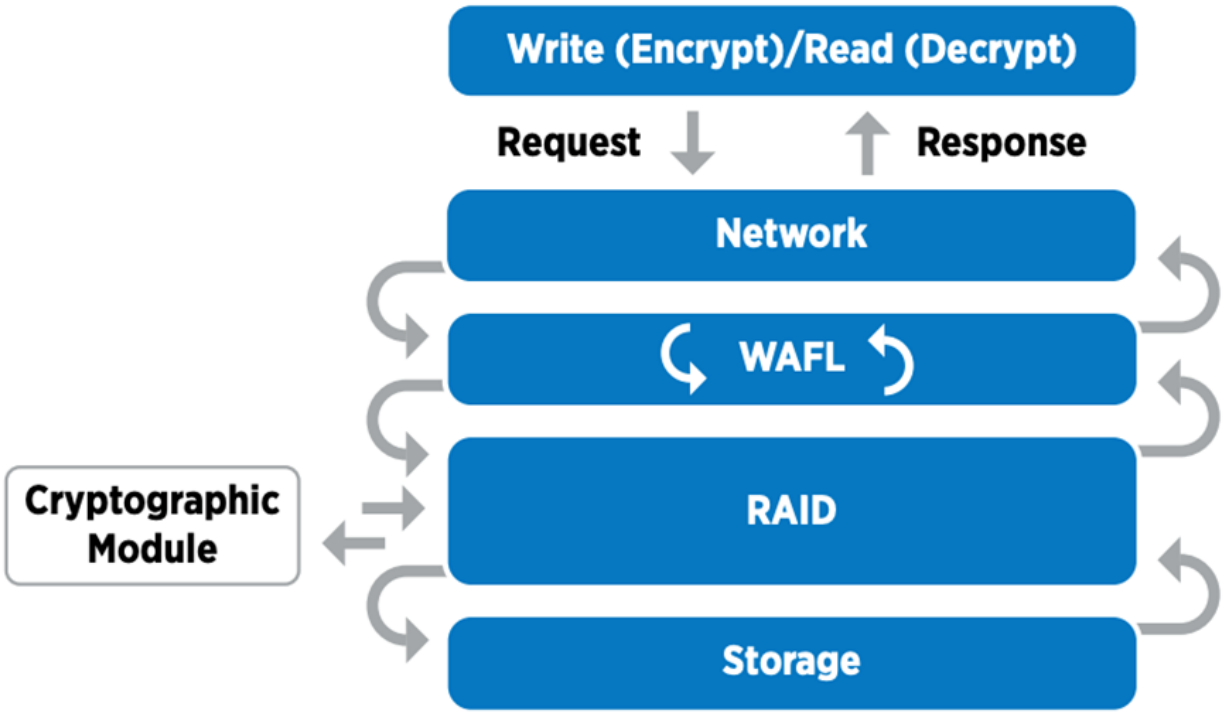
NetApp은 FIPS 140-2 검증을 거친 SED(자체 암호화 드라이브)를 OEM(Original Equipment Manufacturer)에서 구입합니다. 이러한 드라이브를 찾는 고객은 주문 시 드라이브를 지정해야 합니다. 드라이브는 레벨 2에서 검증됩니다. 다음 NetApp 제품은 검증된 SED를 활용할 수 있습니다.

- AFF A-Series 및 FAS 스토리지 시스템
- E-Series 및 EF-Series 스토리지 시스템을 구축합니다
- NetApp 애그리게이트 암호화 및 NetApp 볼륨 암호화 *

NVE 및 NetApp Aggregate Encryption(NAE) 기술을 사용하면 볼륨 및 애그리게이트 레벨에서 데이터를 암호화할 수 있으므로 솔루션이 물리적 드라이브에 제한되지 않습니다.

NVE는 ONTAP 9.1부터 사용 가능한 소프트웨어 기반의 유휴 데이터 암호화 솔루션이며 ONTAP 9.2 이후 FIPS 140-2를 준수합니다. NVE를 사용하면 ONTAP가 각 볼륨의 데이터를 세부적으로 암호화할 수 있습니다. ONTAP 9.6과 함께 제공되는 NAE는 NVE의 성장이 앞서며, ONTAP가 각 볼륨의 데이터를 암호화할 수 있으며 볼륨이 애그리게이트 전체에서 키를 공유할 수 있습니다. NVE와 NAE는 모두 AES 256비트 암호화를 사용합니다. SED가 없는 디스크에도 데이터를 저장할 수 있습니다. NVE와 NAE를 사용하면 암호화가 사용되는 경우에도 스토리지 효율성 기능을 사용할 수 있습니다. 애플리케이션 계층만 암호화하면 스토리지 효율성의 모든 이점을 누릴 수 없습니다. NVE와 NAE를 사용하면 데이터가 NetApp WAFL를 통해 네트워크에서 RAID 계층으로 전송되기 때문에 스토리지 효율성이 유지되고 데이터의 암호화 여부가 결정됩니다. 스토리지 효율성을 높이기 위해 NAE에서 애그리게이트 중복제거를 사용할 수 있습니다. NVE 볼륨과 NAE 볼륨이 동일한 NAE 애그리게이트에 공존할 수 있습니다. NAE 애그리게이트는 암호화되지 않은 볼륨을 지원하지 않습니다.

프로세스는 다음과 같이 진행됩니다. 데이터가 암호화되면 FIPS 140-2 레벨 1의 유효성이 검증된 암호화 모듈로 전송됩니다. 암호화 모듈은 데이터를 암호화하고 RAID 계층으로 다시 전송합니다. 그런 다음 암호화된 데이터가 디스크로 전송됩니다. 따라서 NVE와 NAE를 결합하여 데이터를 디스크로 이미 암호화할 수 있습니다. 읽기는 반대 경로를 따릅니다. 즉, 데이터가 암호화된 상태로 남아 RAID로 전송되고 암호화 모듈에 의해 해독되며 다음 그림과 같이 스택의 나머지 부분까지 전송됩니다.



NVE는 FIPS 140-2 레벨 1의 검증된 소프트웨어 암호화 모듈을 사용합니다.

NVE에 대한 자세한 내용은 를 "NVE 데이터시트"참조하십시오.

NVE는 클라우드의 데이터를 보호합니다. Cloud Volumes ONTAP 및 Azure NetApp Files는 FIPS 140-2 규격 데이터 암호화를 유휴 상태에서 제공할 수 있습니다.

ONTAP 9.7부터 NVE 라이센스와 온보드 또는 외부 키 관리가 있을 때 새로 생성된 애그리게이트 및 볼륨이 기본적으로 암호화됩니다. ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. Aggregate에서 생성한 볼륨은 기본적으로 암호화됩니다. 볼륨을 암호화할 때 기본값을 재정의할 수 있습니다.

ONTAP NAE CLI 명령

다음 CLI 명령을 실행하기 전에 클러스터에 필요한 NVE 라이센스가 있는지 확인하십시오.

Aggregate를 생성하여 암호화하려면 다음 명령을 실행합니다(ONTAP 9.6 이상의 클러스터 CLI에서 실행 시).

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

NAE가 아닌 애그리게이트를 NAE A aggregate로 변환하려면 다음 명령을 실행합니다(ONTAP 9.6 및 이후 클러스터 CLI에서 실행되는 경우).

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

NAE 애그리게이트를 NAE가 아닌 aggregate로 변환하려면 다음 명령을 실행하십시오(ONTAP 9.6 이상의 클러스터 CLI에서 실행되는 경우).

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE CLI 명령

ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. Aggregate에서 생성한 볼륨은 기본적으로 암호화됩니다.

NAE가 활성화된 애그리게이트에서 볼륨을 생성하려면 다음 명령을 실행합니다(ONTAP 9.6 및 이후 클러스터 CLI에서 실행되는 경우).

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

볼륨 이동 없이 기존 볼륨 "제자리에" 암호화를 활성화하려면 다음 명령을 실행합니다(ONTAP 9.6 이상 클러스터 CLI에서 실행 시).

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

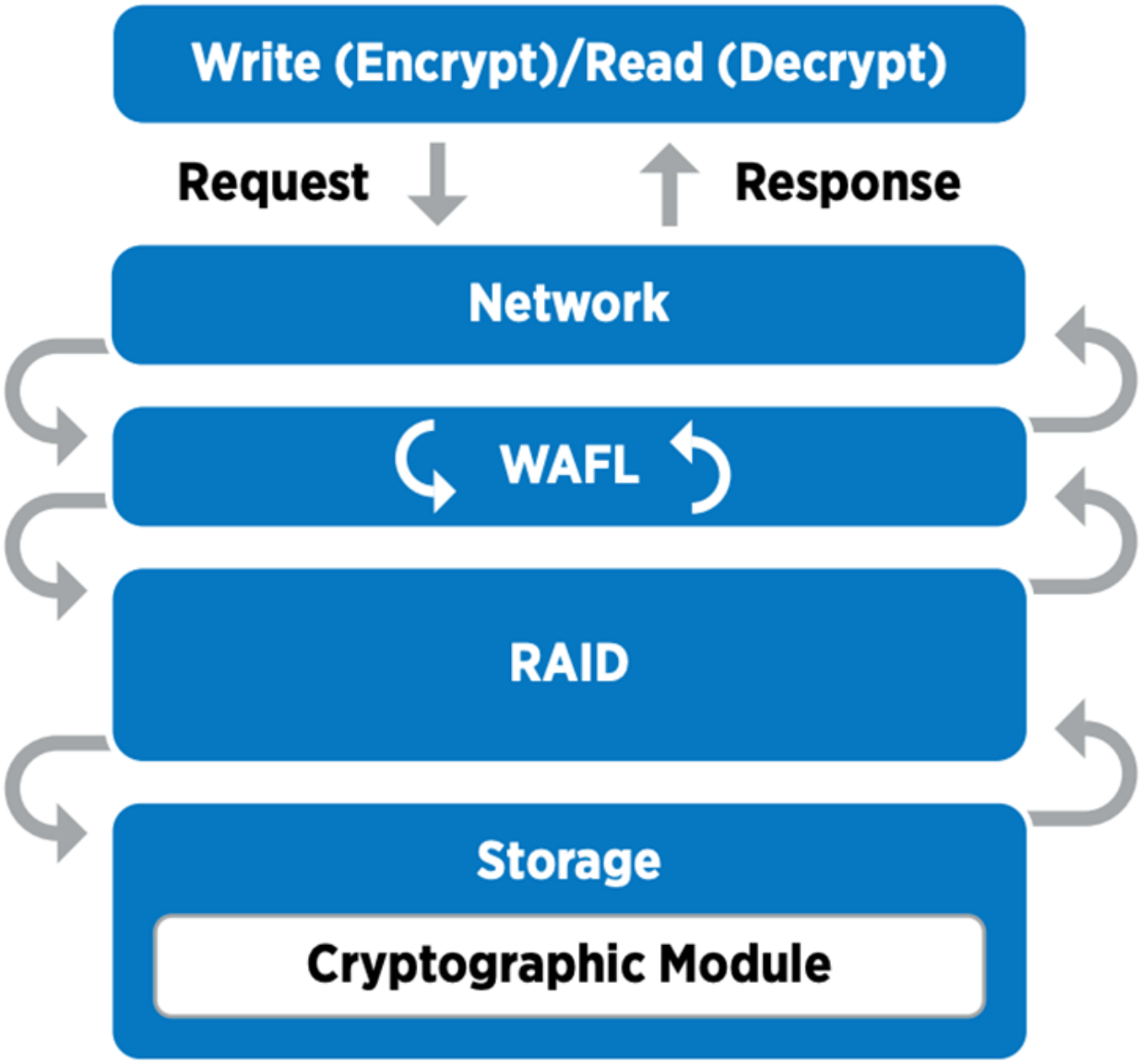
볼륨에 암호화가 설정되어 있는지 확인하려면 다음 CLI 명령을 실행합니다.

```
fp-health::> volume show -is-encrypted true
```

NSE를 선택합니다

NSE는 SED를 사용하여 하드웨어 가속 메커니즘을 통해 데이터 암호화를 수행합니다.

NSE는 AES 256비트 투명 디스크 암호화를 통해 유휴 데이터를 보호하여 규정 준수 및 스페어 반환을 지원하도록 FIPS 140-2 레벨 2 자체 암호화 드라이브를 구성합니다. 드라이브는 암호화 키 생성을 포함하여 다음 그림에 설명된 대로 내부적으로 모든 데이터 암호화 작업을 수행합니다. 데이터에 대한 무단 액세스를 방지하기 위해 스토리지 시스템은 드라이브를 처음 사용할 때 설정된 인증 키를 사용하여 드라이브에서 자체적으로 인증해야 합니다.



NSE는 FIPS 140-2 레벨 2의 검증된 각 드라이브에서 하드웨어 암호화를 사용합니다.

NSE에 대한 자세한 내용은 를 "NSE 데이터시트"참조하십시오.

키 관리

FIPS 140-2 표준은 다음 그림과 같이 경계에서 정의한 암호화 모듈에 적용됩니다.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

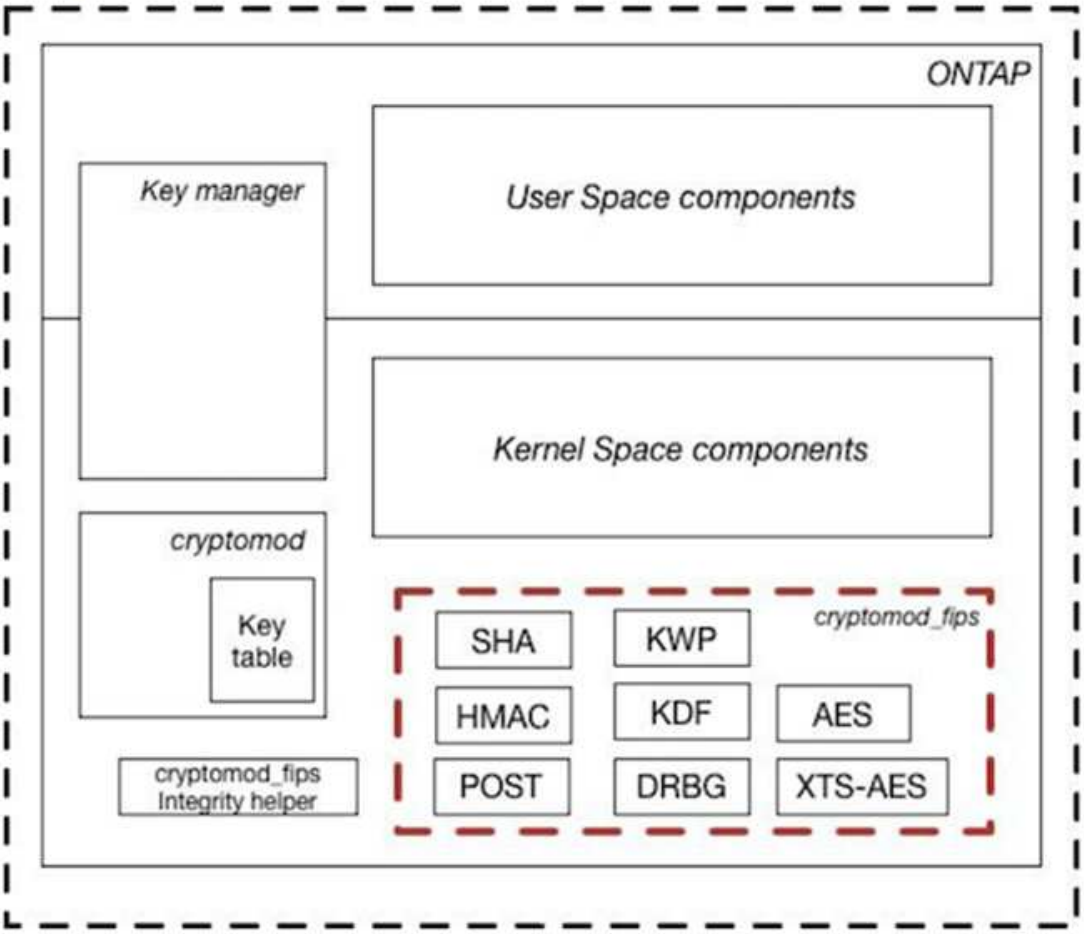


Figure 1 - Block Diagram

키 관리자는 ONTAP에서 사용하는 모든 암호화 키를 추적합니다. NSE SED는 키 관리자를 사용하여 NSE SED의 인증 키를 설정합니다. 키 관리자를 사용할 때 NVE와 NAE의 결합된 솔루션은 소프트웨어 암호화 모듈, 암호화 키 및 키 관리자로 구성됩니다. NVE는 각 볼륨에 대해 키 관리자가 저장하는 고유한 XTS-AES 256 데이터 암호화 키를 사용합니다. 데이터 볼륨에 사용되는 키는 해당 클러스터의 데이터 볼륨에 고유하며 암호화된 볼륨이 생성될 때 생성됩니다. 마찬가지로 NAE 볼륨은 집합당 고유한 XTS-AES 256 데이터 암호화 키를 사용하며 키 관리자도 이 암호화 키를 저장합니다. NAE 키는 암호화된 Aggregate가 생성될 때 생성됩니다. ONTAP는 키를 미리 생성하거나 다시 사용하거나 일반 텍스트로 표시하지 않습니다. 키는 키 관리자에 의해 저장 및 보호됩니다.

외부 키 관리자 지원

ONTAP 9.3부터 외부 키 관리자는 NVE 솔루션과 NSE 솔루션 모두에서 지원됩니다. FIPS 140-2 표준은 특정 공급업체의 구현에 사용되는 암호화 모듈에 적용됩니다. 대부분의 경우 FlexPod 및 ONTAP 고객은 에 따라 다음 검증 중 하나를 사용합니다 "NetApp 상호 운용성 매트릭스") 주요 관리자:

- Gemalto 또는 SafeNet AT
- 보메트릭(목요일)

- IBM SKLM
- Utimaco(이전의 Microfocus, HPE)

NSE 및 NVMe SED 인증 키는 업계 표준 OASIS KMIP(Key Management Interoperability Protocol)를 사용하여 외부 키 관리자에 백업됩니다. 스토리지 시스템, 드라이브 및 키 관리자만이 키에 액세스할 수 있으며, 보안 도메인 외부로 드라이브를 이동하면 드라이브 잠금을 해제할 수 없으므로 데이터 유출을 방지할 수 있습니다. 외부 키 관리자는 NVE 볼륨 암호화 키와 NAE 애그리게이트 암호화 키도 저장합니다. 컨트롤러와 디스크가 더 이상 외부 키 관리자에 액세스할 수 없는 경우, NVE 및 NAE 볼륨은 액세스할 수 없으며 해독할 수 없습니다.

다음 명령 예에서는 외부 키 관리자가 SVM(Store Virtual Machine)의 vmname1"에 사용하는 서버 목록에 두 개의 키 관리 서버를 추가합니다.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

ONTAP는 멀티테넌시 시나리오에서 FlexPod 데이터 센터를 사용 중인 경우 SVM 레벨에서 보안상의 이유로 테넌시를 제공하여 사용자를 지원합니다.

외부 키 관리자 목록을 확인하려면 다음 CLI 명령을 실행합니다.

```
fp-health::> security key-manager external show
```

이중 암호화를 위한 암호화 결합(계층화된 방어)

데이터에 대한 액세스를 격리하고 데이터를 항상 보호해야 하는 경우 NSE SED를 네트워크 또는 패브릭 수준 암호화와 결합할 수 있습니다. NSE SED는 관리자가 상위 수준 암호화를 구성하거나 잘못 구성하는 경우 백스톱처럼 작동합니다. 두 개의 개별 암호화 계층의 경우 NSE SED를 NVE 및 NAE와 결합할 수 있습니다.

NetApp ONTAP 클러스터 전체에서 데이터 제어 플레인 **FIPS** 모드를 지원합니다

NetApp ONTAP 데이터 관리 소프트웨어에는 고객을 위해 추가 보안 수준을 인스턴스화하는 FIPS 모드 구성이 있습니다. 이 FIPS 모드는 컨트롤 평면에만 적용됩니다. FIPS 모드가 활성화되면 FIPS 140-2의 주요 요소에 따라 전송 계층 보안 v1(TLSv1) 및 SSLv3이 비활성화되고 TLS v1.1 및 TLS v1.2만 활성화됩니다.

FIPS 모드의 ONTAP 클러스터 전체 제어 창은 FIPS 140-2 레벨 1을 준수합니다. 클러스터 전체 FIPS 모드는 NCSM에서 제공하는 소프트웨어 기반 암호화 모듈을 사용합니다.

클러스터 전체 컨트롤 플레인을 위한 FIPS 140-2 규정 준수 모드는 ONTAP의 모든 제어 인터페이스를 보호합니다. 기본적으로 FIPS 140-2 전용 모드는 비활성화되어 있지만 '보안 구성 수정' 명령에 대해 'is-FIPS-enabled' 매개 변수를 'true'로 설정하여 이 모드를 활성화할 수 있습니다.

ONTAP 클러스터에서 FIPS 모드를 활성화하려면 다음 명령을 실행합니다.

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL을 위해 FIPS 컴플레인 암호화를 사용합니다.

전체 클러스터에 대해 FIPS 상태를 표시하려면 다음 명령을 실행합니다.

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"다음으로, FlexPod 통합 인프라의 솔루션 이점에 대해 알아보십시오."

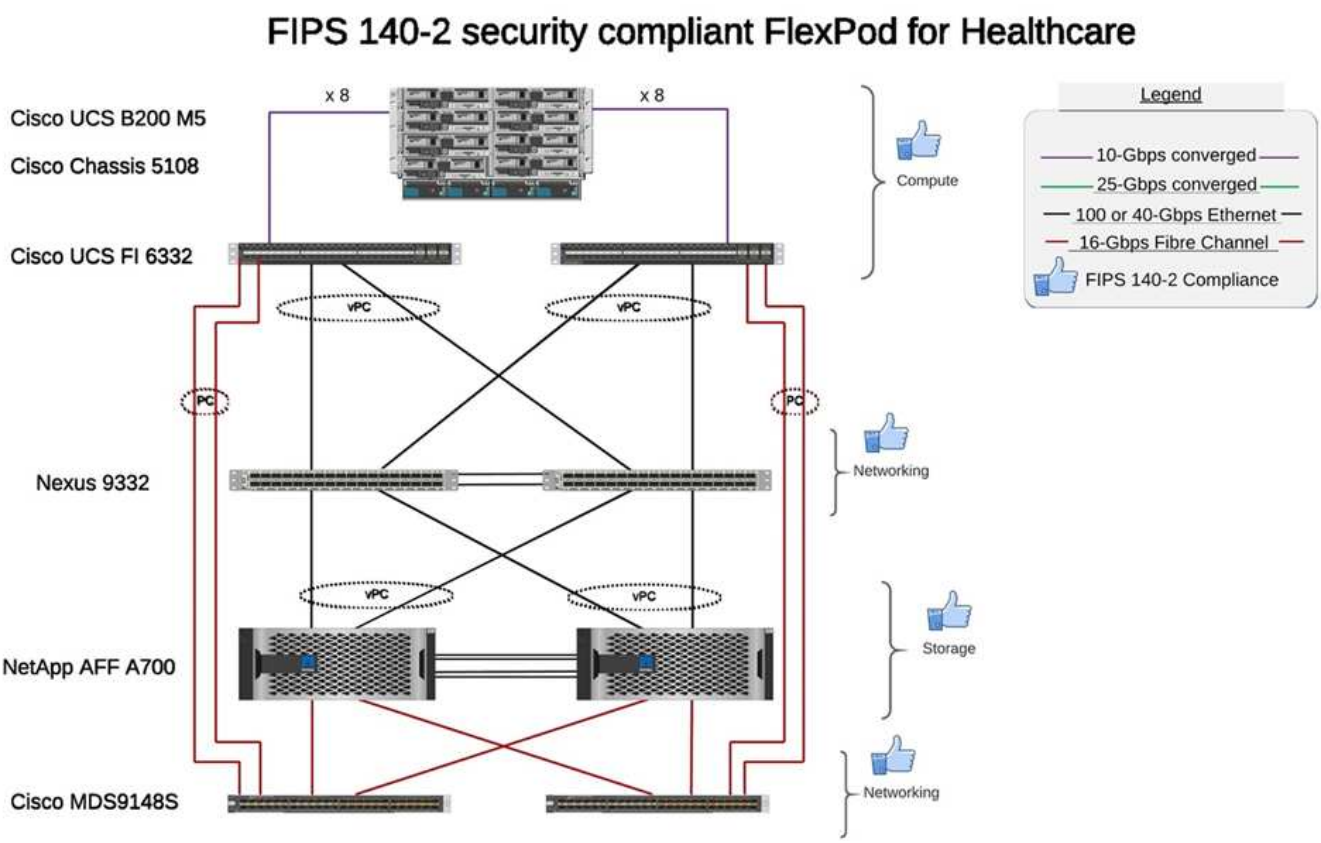
FlexPod 통합 인프라의 솔루션 이점

"이전:FlexPod NetApp ONTAP 스토리지 및 FIPS 140-2가 있습니다."

의료 조직에는 몇 가지 미션 크리티컬 시스템이 있습니다. 가장 중요한 시스템 두 가지는 EHR(전자 건강 기록) 시스템과 의료 영상 시스템입니다. FlexPod 시스템에서 FIPS 설정을 시연하기 위해 FlexPod 시스템에서 랩 설정 및 워크로드 검증을 위해 오픈 소스 EHR과 오픈 소스 사진 아카이빙 및 통신 시스템(PACS) 시스템을 사용했습니다. EHR 기능, EHR 논리적 애플리케이션 구성 요소 및 EHR 시스템을 FlexPod 시스템에 구현할 경우 EHR 시스템이 어떤 이점을 누릴 수 있는지 보려면 을 참조하십시오 "TR-4881: 전자 건강 기록 시스템용 FlexPod". 의료 영상 시스템 기능, 논리적 응용 프로그램 구성 요소 및 의료 영상 시스템이 FlexPod에 구현될 때 어떤 이점을 얻을 수 있는지 전체 목록은 를 참조하십시오 "TR-4865: 의료 영상용 FlexPod".

FIPS 설정 및 워크로드 검증 과정에서 NetApp은 일반적인 의료 기관을 대표하는 워크로드 특성을 실행했습니다. 예를 들어, 오픈 소스 EHR 시스템을 사용하여 현실적인 환자 데이터 액세스 및 변경 시나리오를 포함했습니다. 또한 ' * 에서 디지털 이미징 및 의료(DICOM) 개체 통신 등의 의료 영상 작업 부하를 행사했습니다. DCM의 파일 형식입니다. 메타데이터가 있는 DICOM 객체가 파일 및 블록 스토리지에 모두 저장되었습니다. 또한 가상화된 RedHat Enterprise Linux(RHEL) 서버 내에서 다중 경로 기능을 구현했습니다. NFS에 DICOM 객체, iSCSI를 사용하여 마운트된 LUN 및 FC를 사용하여 마운트된 LUN을 저장했습니다. FIPS 설정 및 검증 중에 FlexPod 통합 인프라가 당사의 기대치를 초과하고 원활하게 수행된다는 것을 확인했습니다.

다음 그림은 FIPS 설정 및 검증에 사용되는 FlexPod 시스템을 보여 줍니다. 우리는 을 활용했습니다 "VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 CVD(Cisco Validated Design)" 설치 프로세스 중



솔루션 인프라 하드웨어 및 소프트웨어 구성 요소

다음 두 그림은 FlexPod에서 FIPS 테스트를 수행할 때 각각 사용되는 하드웨어 및 소프트웨어 구성 요소를 나열합니다. 이러한 표의 권장사항은 예이며, NetApp SME와 협력하여 해당 구성요소가 귀사에 적합한지 확인해야 합니다. 또한 에서 구성 요소 및 버전이 지원되는지 확인합니다 "NetApp 상호 운용성 매트릭스 툴" (IMT) 및 "Cisco HCL(하드웨어 호환 목록)".

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1 또는 2	
	Cisco UCS 블레이드 서버	3 B200 M5	각각 20개 이상의 코어, 2.7GHz 및 128-384GB RAM이 있습니다
	Cisco UCS 가상 인터페이스 카드(VIC)	Cisco UCS 1440	를 참조하십시오
	Cisco UCS Fabric 인터커넥트 2개	6332	-
네트워크	Cisco Nexus 스위치	2x Cisco Nexus 9332	-
스토리지 네트워크	SMB/CIFS, NFS 또는 iSCSI 프로토콜을 통한 스토리지 액세스를 위한 IP 네트워크	위와 동일한 네트워크 스위치	-
	FC를 통한 스토리지 액세스	Cisco MDS 9148S 2개	-

레이어	제품군	수량 및 모델	세부 정보
스토리지	NetApp AFF A700 All-Flash 스토리지 시스템	클러스터 1개	2개의 노드로 클러스터
	디스크 쉘프	DS224C 또는 NS224 디스크 쉘프 1개	24개 드라이브로 완전히 채워집니다
	SSD를 지원합니다	>24, 1.2TB 이상의 용량	-

소프트웨어	제품군	버전 또는 릴리스	세부 정보
다양하다	리눅스	RHEL 7.X를 참조하십시오	-
	Windows	Windows Server 2012 R2(64비트)	-
	NetApp ONTAP를 참조하십시오	ONTAP 9.7 이상	-
	Cisco UCS 6120 패브릭 인터커넥트	Cisco UCS Manager 4.1 이상	-
	Cisco 이더넷 3000 또는 9000 시리즈 스위치	9000 시리즈, 7.0(3) i7(7) 이상(3000 시리즈, 9.2(4) 이상	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) 이상	-
	하이퍼바이저	VMware vSphere ESXi 6.7 U2 이상	-
스토리지	하이퍼바이저 관리 시스템	VMware vCenter Server 6.7 U3(vCSA) 이상	-
네트워크	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	-
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	-
	Cisco UCS Manager를 참조하십시오	4.1(1c) 이상	
하이퍼바이저	ESXi		
관리	하이퍼바이저 관리 시스템 VMware vCenter Server 6.7 U3(vCSA) 이상		
	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	
	Cisco UCS Manager를 참조하십시오	4.1(1c) 이상	

"다음: 추가 FlexPod 보안 고려 사항."

추가 **FlexPod** 보안 고려 사항

"이전: FlexPod 통합 인프라의 솔루션 이점"

FlexPod 인프라는 모듈식, 컨버지드, 선택적으로 가상화, 확장 가능(스케일아웃 및 스케일업) 및 비용 효율적인 플랫폼입니다. FlexPod 플랫폼을 사용하면 컴퓨팅, 네트워크, 스토리지를 독립적으로 확장하여 애플리케이션 구축을 가속할 수 있습니다. 모듈식 아키텍처를 사용하므로 시스템 스케일아웃 및 업그레이드 작업 중에도 무중단으로 운영할 수 있습니다.

HIT 시스템의 여러 구성 요소는 SMB/CIFS, NFS, ext4 및 NTFS 파일 시스템에 데이터를 저장해야 합니다. 즉, 인프라가 NFS, CIFS 및 SAN 프로토콜을 통해 데이터 액세스를 제공해야 합니다. 단일 NetApp 스토리지 시스템에서 이러한 모든 프로토콜을 지원하여 프로토콜 관련 스토리지 시스템의 기존 관행을 제거할 수 있습니다. 또한, 단일 NetApp 스토리지 시스템은 EHR, PACS 또는 VNA, 유전체학, VDI 등 다양한 HIT 워크로드를 지원할 수 있습니다.
보장된 구성 가능한 성능 수준

HIT는 FlexPod 시스템에 배포되면 의료 산업에만 해당되는 여러 가지 이점을 제공합니다. 다음 목록은 이러한 이점에 대한 자세한 설명입니다.

- * FlexPod 보안 *. 보안은 FlexPod 시스템의 기초가 됩니다. 지난 몇 년 동안 랜섬웨어는 위협이 되었습니다. 랜섬웨어는 암호화 바이러스, 암호화를 사용하여 악성 소프트웨어를 빌드하는 일종의 맬웨어입니다. 이 맬웨어는 대칭 키 암호화와 비대칭 키 암호화를 모두 사용하여 피해자의 데이터를 잠그고 데이터 암호를 해독할 키를 제공하는 대가로 금전을 요구합니다. FlexPod 솔루션이 랜섬웨어와 같은 위협을 완화하는 데 어떤 도움이 되는지 알아보려면 를 참조하십시오. "TR-4802: 랜섬웨어에 대한 솔루션" FlexPod 인프라 구성 요소도 "FIPS 140-2를 준수합니다"있습니다.
- Cisco Intersight. * Cisco Intersight는 혁신적인 클라우드 기반의 서비스형 관리 플랫폼으로, 전체 스택 FlexPod 관리 및 오케스트레이션을 위한 단일 창을 제공합니다. Intersight 플랫폼은 FIPS 140-2 보안 호환 암호화 모듈을 사용합니다. 플랫폼의 대역 외 관리 아키텍처는 HIPAA와 같은 일부 표준 또는 감사 범위를 벗어납니다. 네트워크에서 개인 식별 가능한 건강 정보는 Intersight 포털에 전송되지 않습니다.
- * NetApp FPolicy 기술. * 이름 파일 정책의 진화된 FPolicy는 NFS 또는 SMB/CIFS 프로토콜을 통한 파일 액세스를 모니터링하고 관리하기 위한 파일 액세스 알림 프레임워크입니다. 이 기술은 10년 이상 ONTAP 데이터 관리 소프트웨어의 일부였습니다. 랜섬웨어의 탐지에 유용합니다. 이 제로 트러스트 엔진은 ACL(액세스 제어 목록)의 사용 권한 외에 추가적인 보안 조치를 제공합니다. FPolicy는 두 가지 운영 모드, 즉 기본 및 외부 모드를 사용합니다.
  - 기본 모드는 파일 확장명의 블랙리스트와 화이트리스팅을 모두 제공합니다.
  - 외부 모드는 네이티브 모드와 동일한 기능을 제공하지만, ONTAP 시스템 외부에서 실행되는 FPolicy 서버와 SIEM(보안 정보 및 이벤트 관리) 시스템과도 통합됩니다. 랜섬웨어에 대항하는 방법에 대한 자세한 내용은 를 참조하십시오 "랜섬웨어에 대항하기: 3부 – 강력한 기본(무료) 툴인 ONTAP FPolicy" 블로그:
- * 저장된 데이터 *. ONTAP 9 이상에서는 FIPS 140-2를 준수하는 세 가지 유휴 데이터 암호화 솔루션이 있습니다.
  - NSE는 자체 암호화 드라이브를 사용하는 하드웨어 솔루션입니다.
  - NVE는 각 볼륨의 고유 키를 사용해 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.
  - NAE는 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

ONTAP 9.7부터 NAE와 NVE는 VE라는 이름의 NetApp NVE 라이센스 패키지가 설치된 경우 기본적으로 활성화됩니다.

- * 비행 중인 데이터 *. ONTAP 9.8부터 IPsec(인터넷 프로토콜 보안)은 클라이언트와 ONTAP SVM 사이의 모든 IP 트래픽에 엔드 투 엔드 암호화 지원을 제공합니다. 모든 IP 트래픽에 대한 IPsec 데이터 암호화에는 NFS, iSCSI 및 SMB/CIFS 프로토콜이 포함됩니다. IPsec은 iSCSI 트래픽에 대해 전송 중인 유일한 암호화 옵션을 제공합니다.
- * 하이브리드 멀티 클라우드 Data Fabric * 에서 엔드 투 엔드 데이터 암호화 데이터 복제 트래픽에 NSE 또는 NVE, CPE(Cluster 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 IPsec을 사용하여 하이브리드 멀티 클라우드 데이터 패브릭 전체에서 클라이언트와 스토리지 간의 엔드 투 엔드 암호화를 사용할 수 있습니다. ONTAP 9부터는 클러스터 차원의 제어 평면 인터페이스를 위해 FIPS 140-2 규정 준수 모드를 활성화할 수 있습니다. 기본적으로 FIPS 140-2 전용 모드는 비활성화되어 있습니다. ONTAP 9.6부터 CPE는 ONTAP SnapMirror, NetApp SnapVault 및 NetApp FlexCache 기술과 같은 데이터 복제 기능에 TLS 1.2 AES-256 GCM 암호화 지원을 제공합니다. 암호화는 두 클러스터 피어 간에 미리 공유된 키(PSK)를 통해 설정됩니다.
- * 보안 멀티 테넌시 *. 가상화된 서버 및 스토리지 공유 인프라의 증가하는 요구 사항을 지원하여 특히 데이터베이스 및 소프트웨어의 여러 인스턴스를 호스팅할 때 시설별 정보의 안전한 멀티 테넌시를 지원합니다.

"다음: 결론."

결론

"이전: 추가 FlexPod 보안 고려 사항."

FlexPod 플랫폼에서 의료 애플리케이션을 실행하면 FIPS 140-2를 지원하는 플랫폼을 통해 의료 조직을 더욱 안전하게 보호할 수 있습니다. FlexPod은 컴퓨팅, 네트워크, 스토리지 등 모든 단일 구성 요소에서 다계층 보호를 제공합니다. FlexPod 데이터 보호 기능은 사용되지 않는 데이터나 사용 중인 데이터를 보호하고, 필요할 때 백업을 안전하게 보호합니다.

Cisco와 NetApp의 전략적 파트너십을 통해 엄격한 테스트를 거친 FlexPod 사전 검증된 설계를 활용하여 사람의 실수를 방지합니다. FlexPod 시스템은 FIPS 140-2를 컴퓨팅, 네트워킹 및 스토리지 계층에서 사용할 수 있는 경우에도 성능에 거의 영향을 주지 않으면서 예측 가능하고 낮은 대기 시간의 시스템 성능과 고가용성을 제공하도록 엔지니어링 및 설계되었습니다. 이러한 접근 방식은 사용자의 사용 환경이 뛰어나고 사용자의 HIT 시스템 사용자에게 최적의 응답 시간을 제공합니다.

"다음: 감사의 말, 버전 기록 및 추가 정보를 찾을 위치."

감사의 말, 버전 기록 및 추가 정보를 찾을 수 있는 위치

"이전: 결론."

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- Cisco MDS 9000 제품군 NX-OS 보안 구성 가이드

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 시리즈 NX-OS 보안 구성 가이드, 릴리즈 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp 및 FIPS(Federal Information Processing Standard) 간행물 140-2

https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- NetApp ONTAP 9 강화 가이드

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- NetApp 암호화 기능 가이드 를 참조하십시오

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE 및 NAE 데이터시트

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NSE 데이터시트

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- ONTAP 9 문서 센터

  http://docs.netapp.com

- NetApp 및 FIPS(Federal Information Processing Standard) 간행물 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco 및 FIPS 140-2 규정 준수

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp 암호화 보안 모듈

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- 중대형 의료 조직을 위한 사이버 보안 사례

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco 및 CMVP(Cryptographic Module Validation Program)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp 스토리지 암호화, NVMe 자체 암호화 드라이브, NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화

https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp 스토리지 암호화

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- 전자 건강 기록 시스템용 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Data Now:클라우드 연결 플래시 기술로 Epic EHR 환경의 성능 향상

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Epic EHR 인프라용 FlexPod Datacenter

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Epic EHR용 FlexPod 데이터 센터 구축 가이드 를 참조하십시오

  https://www.netapp.com/media/10658-tr-4693.pdf

- MEDITECH 소프트웨어용 FlexPod 데이터 센터 인프라

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- FlexPod 표준은 MEDITECH 소프트웨어로 확장됩니다

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- MEDITECH 방향 사이징 가이드용 FlexPod

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- 의료 영상 촬영용 FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf

- 의료 부문의 AI

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- 의료 분야의 혁신을 지원하는 FlexPod

  https://flexpod.com/solutions/verticals/healthcare/

- Cisco와 NetApp의 FlexPod

  https://flexpod.com/

감사의 말

- Abhinav Singh, NetApp 기술 마케팅 엔지니어

- Brian O는 NetApp의 솔루션 설계자 Healthcare(Epic) 입니다
- Brian Pruitt, NetApp 비즈니스 개발 매니저
- Arvind Ramakrishnan, NetApp 수석 솔루션 설계자
- Michael Hommer, NetApp의 FlexPod 글로벌 현장 CTO

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2021년 4월	최초 릴리스