DELL Technologies

백서

기술 백서:
사이버 회복탄력성을 갖춘 Dell EMC PowerEdge 서버의 보안

2020년 12월

개정

날짜	설명
2018년 1월	최초 릴리즈
2020년 11월	개정된 버전

미국에서 게시됨 [11/12/20] [기술 백서]

목차

목차

핵심 요약

보안에 대한 Dell Technologies의 접근 방식은 본질적으로 내재적 보안입니다. 즉, 보안 기능이 추가되는 게 아니라 내장된 상태로 제공되며 Dell의 SDL(Secure Development Lifecycle)의 모든 단계에 통합됩니다. Dell Technologies는 계속해서 늘어나는 위협 상황에 맞춰 PowerEdge 보안 제어, 기능 및 솔루션을 지속적으로 발전시키기 위해 노력하고 있으며, 칩 내장형 RoT(Root of Trust)를 통해 보안을 지속적으로 강화하고 있습니다. 이 백서에서는 대부분 iDRAC9(Dell Remote Access Controller)에서 지원되는, 사이버 회복탄력성을 갖춘 PowerEdge 플랫폼에 기본 제공되는 보안 기능에 대해 자세히 설명합니다. 이전 PowerEdge 보안 백서 이후 액세스 제어부터 데이터 암호화 및 공급망 보증에 이르기까지 새로운 기능이 많이 추가되었으며, 여기에는 라이브 BIOS 스캔, UEFI 보안 부팅 맞춤 구성, RSA Secure ID MFA, SEKM(Secure Enterprise Key Management), SCV(Secured Component Verification), 향상된 System Erase, 자동 인증서 등록 및 갱신, Cipher-Select 및 CNSA 지원이 포함됩니다. 모든 기능은 인텔리전스와 자동화를 광범위하게 활용하여 위협 상황에 미리 대비할 수 있도록 돕고 지속적으로 확장하는 사용 모델에서 요구되는 확장을 지원합니다.

1. 소개

위협 상황이 진화함에 따라 IT 및 보안 전문가는 데이터와 리소스에 대한 위험을 관리하는 데 어려움을 겪고 있습니다. 데이터는 온프레미스 및 클라우드에서 실행되는 여러 디바이스에서 사용되고 있으며 영향력이 큰 데이터 침해는 계속 늘어나고 있습니다. 예전에는 OS, 애플리케이션, 방화벽, IPS 및 IDS 시스템에 대한 보안이 강조되었으며, 지금도 여전히 해결해야 할 중요한 요소들입니다. 그러나 지난 1~2년 동안 하드웨어를 위협한 이벤트를 고려할 때 펌웨어, BIOS, BMC 및 기타 하드웨어 보호(예: 공급망 보증)와 같은 하드웨어 기반 인프라스트럭처를 보호해야 할 필요성이 중요하게 제기되고 있습니다.

Dell Technologies 2020 Digital Transformation Index에 따르면 데이터 프라이버시와 사이버 보안 문제가 디지털 혁신을 가로막는 가장 큰 장애물인 것으로 나타났습니다.[1] 63%의 기업이 악용된 취약성으로 인해 데이터 손상을 경험했습니다.[2] 사이버 범죄와 관련된 글로벌 피해는 2021년에 6조 달러에 달할 것으로 전망됩니다.[3]

소프트웨어 정의 데이터 센터 아키텍처에서 서버의 중요성이 커짐에 따라 서버 보안은 전반적인 엔터프라이즈 보안의 기반으로 대두되고 있습니다. 서버 보안은 하드웨어 및 펌웨어 수준 모두에 중점을 두어야 하며, 이를 위해 변경 불가능한 RoT(Root of Trust)를 사용하여 서버 내에서 이루어지는 후속 작업을 검증해야 합니다. 이를 통해 구축에서 유지 보수, 그리고 폐기에 이르는 서버 수명주기 전반에 걸쳐 신뢰 체인이 구축됩니다.

iDRAC9이 탑재된 14세대 및 15세대 Dell EMC PowerEdge 서버는 이러한 신뢰 체인에 보안 제어 및 포괄적인 관리 툴을 결합하여 하드웨어 및 펌웨어 전반에 걸쳐 강력한 다중 계층 보안을 제공합니다. 그 결과 내장된 서버 펌웨어, 시스템에 저장된 데이터, 운영 체제, 주변 기기, 서버 관리 작업을 비롯한 서버의 모든 측면에 걸쳐 사이버 회복탄력성을 갖춘 아키텍처가 구현됩니다. 조직에서는 중요한 서버 인프라스트럭처와 서버 내의 데이터를 보호하고 모든 이상 징후, 보안 침해 또는 무단 작업을 탐지하여 의도하지 않은 이벤트나 악의적인 이벤트로부터 복구하는 프로세스를 구축할 수 있습니다.

[1] Dell Technologies 2020 Digital Transformation Index

[2] Match Present-Day Security threats with BIOS-Level Control. Dell의 의뢰로 작성된 Forrester Consulting의 사고 리더십 백서, 2019년

[3] Ransomware Attacks Predicted to Occur... The National Law Review, 2020년

2. 안전한 서버 인프라스트럭처를 구축하는 방법

Dell EMC PowerEdge 서버는 칩 내장형의 혁신적인 데이터 보안 기술을 비롯하여 여러 세대에 걸쳐 강력한 보안을 제공하고 있습니다. Dell EMC 14G PowerEdge 서버는 칩 내장형 보안을 확대하여 서버 부팅 과정에서 암호화 RoT(Root of Trust)로 BIOS와 펌웨어를 인증합니다. Dell EMC 제품 팀은 현대 IT 환경에서 직면할 수 있는 보안 위협에 대응하여 14세대 및 15세대 PowerEdge 서버를 설계할 때 다음과 같은 몇 가지 주요 요구 사항을 염두에 두었습니다.

- **보호:** BIOS, 펌웨어, 데이터 및 물리적 하드웨어를 포함하여 수명주기의 모든 측면에서 서버 보호
- **탐지:** 악의적인 사이버 공격 및 승인되지 않은 변경 탐지, 사전 예방적 IT 관리자 개입
- **복구:** BIOS, 펌웨어 및 운영 체제를 알려진 정상 상태로 복구, 서버를 안전하게 폐기 또는 용도 변경

Dell EMC PowerEdge 서버는 이 백서 전반에서 자세히 설명한 것처럼 암호화 및 보안과 관련된 주요 업계 표준을 준수하며 새로운 취약성을 지속적으로 추적하고 관리합니다.

Dell EMC는 개발, 구매, 제조, 운송 및 지원의 모든 측면에서 보안을 핵심 요소로 포함하여 SDL(Security Development Lifecycle) 프로세스를 구축함으로써 사이버 회복탄력성을 갖춘 아키텍처를 구현했습니다.

2.1 SDL(Security Development Lifecycle)

사이버 회복탄력성을 갖춘 아키텍처를 구현하기 위해서는 개발의 각 단계에서 보안 의식과 원칙이 필요합니다. SDL(Security Development Lifecycle) 모델이라고 하는 이 프로세스에서는 보안을 나중에 생각하는 것이 아니라 전체 서버 설계 프로세스의 핵심 요소로 포함합니다. 이 설계 프로세스에는 아래 글머리 기호와 그림 1에 나와 있는 것처럼 전체 서버 수명주기에서 보안 요구 사항이 반영됩니다.

- 보안을 핵심 우선 순위에 두고 기능 구상, 설계, 프로토타입 제작, 구현, 운영, 구축 및 유지 보수
- 제품 개발 수명주기의 모든 단계에서 악성 코드 유입을 방지하고 차단하며 이에 대응하도록 서버 펌웨어 설계
  - » 설계 프로세스에 위협 모델링 및 침투 테스트 포함
  - » 펌웨어 개발의 각 단계에서 보안 코딩 방법 적용
- 중요한 기술의 경우 외부 감사를 통해 내부 SDL 프로세스를 보강하여 펌웨어가 알려진 보안 모범 사례를 준수하는지 확인
- 최신 보안 진단 툴을 사용하여 새로운 잠재적 취약성을 지속적으로 테스트 및 진단
- 필요한 경우 문제 해결 권장 조치를 비롯하여 중대한 CVE(Common Vulnerabilities and Exposures)에 신속하게 대응

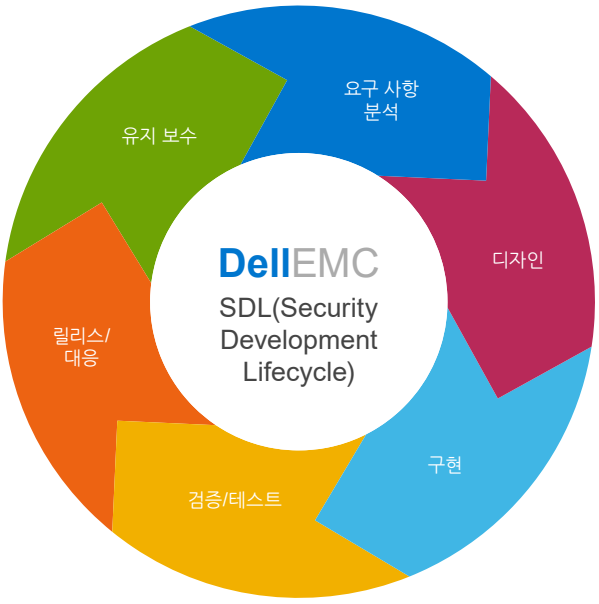


그림 1: Dell EMC SDL(Security Development Lifecycle)

2.2 사이버 회복탄력성을 갖춘 아키텍처

Dell EMC 14세대 및 15세대 PowerEdge 서버는 사이버 공격으로부터 보호, 탐지 및 복구할 수 있도록 서버 설계를 강화한 사이버 회복탄력성을 갖춘 아키텍처를 사용합니다. 이 아키텍처의 주요 기능은 다음과 같습니다.

- **공격으로부터 효과적으로 보호**
  - » 칩 내장형 RoT(Root of Trust)
  - » 보안 부팅
  - » 서명된 펌웨어 업데이트
  - » 유연한 시스템 잠금
  - » 하드 드라이브 암호화 및 엔터프라이즈 키 관리
- **신뢰할 수 있는 공격 탐지**
  - » 구성 및 펌웨어 변동 탐지
  - » 지속적인 이벤트 로깅
  - » 감사 로깅 및 알림
  - » 섀시 침입 감지
- **업무 중단이 거의 또는 전혀 없이 신속하게 복구**
  - » 자동화된 BIOS 복구
  - » 빠른 OS 복구
  - » 펌웨어 롤백
  - » 신속한 시스템 삭제

2.3 오늘날의 보안 위협

끊임없이 변화하는 오늘날의 환경에는 많은 위협 요소가 있습니다. 표 1에는 Dell EMC에서 중요한 백엔드 보안 위협을 관리하는 방법이 요약되어 있습니다.

표 1: Dell EMC가 일반적인 위협 요소에 대처하는 방법

서버 플랫폼 계층		
보안 계층	**위협 요소**	**Dell EMC 솔루션**
물리적 서버	서버/구성 요소 변조	SCV(Secured Component Verification), 섀시 침입 탐지
펌웨어 및 소프트웨어	펌웨어 손상, 멀웨어 주입	칩 내장형 RoT(Root of Trust), 인텔 Boot Guard, AMD Secure Root-of-Trust, UEFI 보안 부팅 맞춤 구성 암호화 방식으로 서명되고 검증된 펌웨어
	소프트웨어	CVE 보고, 필요에 따라 패치 적용
증명 신뢰 기능	서버 ID 스푸핑	TPM, TXT, 신뢰 체인
서버 관리	악의적 구성 및 업데이트, 개방 포트에 대한 무단 공격	iDRAC9, 원격 증명

서버 환경 계층		
보안 계층	**위협 요소**	**Dell EMC 솔루션**
데이터	데이터 유출	SED(Self-Encrypting Drive) – FIPS 또는 Opal/TCG 보안 엔터프라이즈 키 관리 ISE(Instant Secure Erase) 전용 드라이브 안전한 사용자 인증
공급망 무결성	위조 구성 요소 멀웨어 위협	전 세계 모든 서버 제조 사이트에서 ISO9001 인증, SCV(Secured Component Verification), 소유 증명 SDL(Secure Development Lifecycle) 프로세스의 일환으로 보안 조치 구현
공급망 보안	제조 사이트의 보안 관제 운송 중 도난 및 변조	TAPA(Transported Asset Protection Association)의 시설 보안 요건 C-TPAT(Customs-Trade Partnership Against Terrorism), SCV

3. 보호

"보호" 기능은 NIST 사이버 보안 프레임워크의 핵심 구성 요소로서 사이버 보안 공격을 방지하는 역할을 합니다. 이 기능은 액세스 제어, 데이터 보안, 유지 보수, 보호 기술을 비롯한 여러 범주로 구성됩니다. 핵심 원칙은 인프라스트럭처 자산이 포괄적인 보안 설치 및 컴퓨팅 환경의 일부로 리소스와 데이터에 대한 무단 액세스를 방지하는 강력한 보호 기능을 제공해야 한다는 것입니다. 여기에는 BIOS 및 펌웨어와 같은 중요한 구성 요소의 무단 수정을 방지하는 것이 포함됩니다. 플랫폼은 NIST SP 800-193의 최신 권장 사항을 따릅니다.

PowerEdge 서버의 사이버 회복탄력성을 갖춘 아키텍처는 다음 기능을 비롯하여 높은 수준의 플랫폼 보호 기능을 제공합니다.

- 암호화 방식으로 검증된 신뢰할 수 있는 부팅
- 사용자 액세스 보안
- 서명된 펌웨어 업데이트
- 암호화된 데이터 스토리지
- 보안 관제
- 공급망 무결성 및 보안

3.1 암호화 방식으로 검증된 신뢰할 수 있는 부팅

서버 보안의 가장 중요한 측면 중 하나는 부팅 프로세스가 안전한지 검증하는 것입니다. 이 프로세스는 OS 부팅 또는 펌웨어 업데이트와 같은 모든 후속 작업의 신뢰성을 보장할 수 있는 기반이 됩니다. PowerEdge 서버는 기밀 데이터를 저장하는 데 사용되는 iDRAC의 암호화된 보안 메모리인 iDRAC Credential Vault와 같은 칩 내장형 보안 기능을 여러 세대에 걸쳐 사용하고 있습니다. 칩 내장형 RoT(Root of Trust)를 사용하여 부팅 프로세스가 NIST SP 800-147B("BIOS Protection Guidelines for Servers") 및 NIST SP 800-155("BIOS Integrity Measurement Guidelines")의 권장 사항을 따르는지 검증됩니다.

3.1.1 칩 내장형 RoT(Root of Trust)

14세대 및 15세대 PowerEdge 서버(인텔 또는 AMD 기반)는 이제 변조 불가능한 칩 내장형 RoT(Root of Trust)를 사용하여 암호화 방식으로 BIOS 및 iDRAC 펌웨어의 무결성을 증명합니다. 이 RoT(Root of Trust)는 프로그래밍 가능한 일회용의 읽기 전용 공개 키를 기반으로 하여 멀웨어 변조를 방지합니다. BIOS 부팅 프로세스에서는 인텔 Boot Guard 기술 또는 AMD Root-of-Trust 기술을 활용하여 부팅 이미지 암호화 해시의 디지털 서명이 Dell EMC가 제조 시설에서 칩에 저장한 서명과 일치하는지 검증합니다. 검증에 실패할 경우 서버가 종료되고 Lifecycle Controller Log에 사용자 알림이 표시되며, 이때 사용자가 BIOS 복구 프로세스를 시작할 수 있습니다. Boot Guard가 검증에 성공할 경우 신뢰 체인 절차를 사용하여 나머지 BIOS 모듈이 검증된 후 OS 또는 하이퍼바이저로 제어가 넘어갑니다.

Boot Guard의 검증 메커니즘 외에도 iDRAC9 4.10.10.10 이상에서는 호스트 부팅 시 BIOS 이미지를 확인하는 RoT(Root of Trust) 메커니즘을 제공합니다. BIOS 이미지가 성공적으로 검증된 후에만 호스트를 부팅할 수 있습니다. iDRAC9은 런타임, 온디맨드 또는 사용자가 예약한 간격으로 BIOS 이미지를 검증하는 메커니즘도 제공합니다.

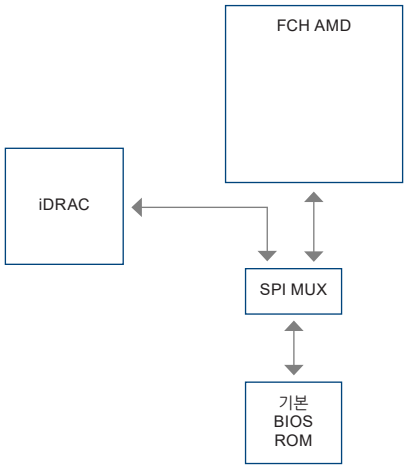
신뢰 체인에 대해 자세히 살펴보겠습니다. 각 BIOS 모듈에는 체인의 다음 모듈에 대한 해시가 포함되어 있습니다. BIOS의 핵심 모듈은 IBB(Initial Boot Block), SEC(Security), PEI(Pre-EFI Initialization), MRC(Memory Reference Code), DXE(Driver Execution Environment) 및 BDS(Boot Device Selection)입니다. 인텔 Boot Guard가 IBB(Initial Boot Block)를 인증하는 경우 IBB는 제어를 넘기기 전에 SEC+PEI를 검증합니다. SEC+PEI는 PEI+MRC를 검증하고 PEI+MRC는 DXE+BDS 모듈을 추가로 검증합니다. 그러면 다음 섹션에서 설명하는 UEFI 보안 부팅으로 제어가 넘어갑니다.

마찬가지로, AMD EPYC 기반의 Dell EMC PowerEdge 서버도 AMD Secure Root-of-Trust 기술을 통해 서버가 신뢰할 수 있는 펌웨어 이미지에서 부팅되도록 보장합니다. 또한 AMD Secure Run 기술은 주 메모리를 암호화하여 비공개로 유지함으로써 해당 하드웨어에 액세스하는 악의적인 침입자로부터 보호합니다. 이 기능을 사용하기 위해 애플리케이션을 수정할 필요가 없으며 암호화 키는 보안 프로세서의 외부에 전혀 노출되지 않습니다.

iDRAC는 하드웨어 기반 보안 기술 역할도 수행하며, AMD의 FCH(Fusion Controller Hub) 외에도 SPI를 통해 기본 BIOS ROM에 액세스하여 RoT 프로세스를 수행합니다.

다음과 같은 조건에서 iDRAC9은 BIOS를 복구합니다.

1. BIOS 무결성 검사에 실패했습니다.
2. BIOS 자체 검사에 실패했습니다.
3. RACADM 명령 사용 - **racadm recover BIOS.Setup.1-1**



iDRAC 부팅 프로세스는 독립적인 칩 내장형 RoT(Root of Trust)를 사용하여 iDRAC 펌웨어 이미지를 검증합니다. 또한 iDRAC RoT(Root of Trust)는 Dell EMC 펌웨어 업데이트 패키지(DUP)의 서명을 인증하는 데 중요한 트러스트 기반을 제공합니다.

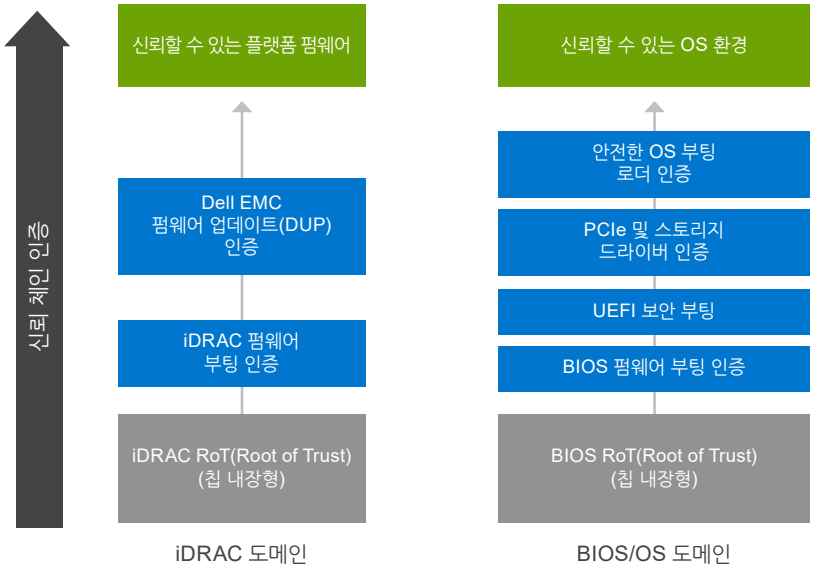


그림 2: PowerEdge 서버의 칩 내장형 RoT(Root of Trust) 도메인

3.1.2 BIOS 라이브 검사

BIOS 라이브 검사는 POST 프로세스가 아닌 호스트의 전원을 켤 때 기본 ROM에서 BIOS 이미지의 무결성 및 신뢰성을 검증합니다. AMD 전용 기능으로 Datacenter 라이선스가 포함된 iDRAC9 4.10.10.10 이상에서만 사용할 수 있습니다. 이 작업을 수행하려면 관리자 권한 또는 "디버그 명령 실행" 디버그 권한이 있는 운영자 권한이 있어야 합니다. iDRAC UI, RACADM 및 Redfish 인터페이스를 통해 검사를 예약할 수 있습니다.

3.1.3 UEFI 보안 부팅 맞춤 구성

또한 PowerEdge 서버는 업계 표준 UEFI(Unified Extensible Firmware Interface) 보안 부팅을 지원하며, 이 기능은 OS가 실행되기 전에 UEFI 드라이버와 로드된 다른 코드의 암호화 서명을 확인합니다. 보안 부팅은 부팅 전 환경의 보안을 위한 업계 표준입니다. 컴퓨터 시스템 공급업체, 확장 카드 공급업체 및 운영 체제 공급업체는 상호 운용성을 증진하기 위해 이 사양과 관련해 긴밀히 협력합니다.

UEFI 보안 부팅이 활성화되면 서명되지 않은, 즉 신뢰할 수 없는 UEFI 디바이스 드라이버는 로드되지 않고 오류 메시지가 표시되며 디바이스가 작동되지 않습니다. 서명되지 않은 디바이스 드라이버를 로드하려면 보안 부팅을 비활성화해야 합니다.

또한 14세대 및 15세대 PowerEdge 서버는 Microsoft에서 서명하지 않은 맞춤 구성된 부팅 로더 인증서를 사용할 수 있는 독보적인 유연성을 제공합니다. 이 기능은 기본적으로 고유한 OS 부팅 로더에 서명하려는 Linux 환경 관리자를 위한 기능입니다. 기본 iDRAC API를 통해 맞춤형 인증서를 업로드하여 고객의 고유한 OS 부팅 로더를 인증할 수 있습니다. 이 PowerEdge UEFI 맞춤 구성 방법은 서버의 Grub2 취약성을 완화하기 위해 NSA가 인용했습니다.

3.1.4 TPM 지원

PowerEdge 서버는 3가지 버전의 TPM을 지원합니다.

- TPM 1.2 FIPS + Common Criteria+ TCG 인증 획득(Nuvoton)
- TPM 2.0 FIPS + Common Criteria+ TCG 인증 획득(Nuvoton)
- TPM 2.0 China(NationZ)

TPM을 사용하여 공개 키 암호화 기능을 수행하고, 해시 함수를 연산하고, 키를 생성,관리 및 안전하게 저장하고, 증명을 수행할 수 있습니다. 인텔의 TXT(Trusted Execution Technology) 기능과 Windows Server 2016의 Microsoft Platform Assurance 기능도 지원됩니다. TPM을 사용하여 Windows Server 2012/2016의 BitLocker™ 하드 드라이브 암호화 기능을 활성화할 수 있습니다.

증명 및 원격 증명 솔루션은 TPM을 사용하여 서버의 하드웨어, 하이퍼바이저, BIOS 및 OS의 부팅 시 측정을 수행하고 암호화된 안전한 방식으로 해당 측정치를 TPM에 저장된 기본 측정치와 비교할 수 있습니다. 측정치가 동일하지 않다면 서버 ID가 유출되었을 가능성이 있으며 시스템 관리자는 로컬 또는 원격으로 서버를 비활성화하여 연결을 해제할 수 있습니다.

서버 주문 시 TPM을 포함하거나 포함하지 않을 수 있지만, TPM은 많은 OS 및 기타 보안 조항에서 표준이 되고 있습니다. TPM은 BIOS 선택 사항을 통해 활성화되며 플러그인 모듈 솔루션으로 제공되고 플레이너에 이 플러그인 모듈을 위한 커넥터가 있습니다.

3.1.5 보안 인증

Dell EMC는 NIST FIPS 140-2 및 Common Criteria EAL-4와 같은 표준에 대해 인증을 받았습니다. 이러한 인증은 미국 DoD 및 기타 정부 요건을 준수한다는 측면에서 중요합니다. PowerEdge 서버는 다음과 같은 인증을 획득했습니다.

- 서버 플랫폼: RHEL 사용에 대한 Common Criteria EAL4+ 인증. 파트너 CC 인증을 지원하는 데도 사용됨
- iDRAC 및 CMC FIPS 140-2 Level 1 인증
- OpenManage Enterprise – 모듈에 대한 EAL2+ 인증
- TPM 1.2 및 2.0에 대한 FIPS 140-2 및 Common Criteria 인증

3.2 사용자 액세스 보안

적절한 인증 및 권한 부여는 최신 액세스 제어 정책의 핵심 요구 사항입니다. PowerEdge 서버의 기본 액세스 인터페이스는 API, CLI 또는 내장형 iDRAC의 GUI입니다. 서버 관리 자동화를 위한 기본 API 및 CLI는 다음과 같습니다.

- iDRAC RESTful API with Redfish
- RACADM CLI
- SELinux

이러한 각 인터페이스는 필요한 경우 HTTPS 등의 암호화된 연결을 통해 전송되는 사용자 이름 및 암호 보안과 같은 강력한 자격 증명을 제공합니다. SSH는 일치하는 암호화 키 세트를 사용하여 사용자를 인증하므로 보안 수준이 더 낮은 암호를 입력할 필요가 없습니다. IPMI와 같은 오래된 프로토콜도 지원되지만 최근 몇 년간 발견된 다양한 보안 문제로 인해 신규 구축에는 권장되지 않습니다. 현재 IPMI를 사용 중인 경우 iDRAC RESTful API with Redfish를 평가하고 이 프로토콜로 전환하는 것이 좋습니다.

TLS/SSL 인증서를 iDRAC에 업로드하여 웹 브라우저 세션을 인증할 수 있습니다. 세 가지 선택이 가능합니다.

- **Dell EMC 자체 서명된 TLS/SSL 인증서 –** 인증서가 자동으로 생성되고 iDRAC에서 자체 서명됩니다.
  - » 장점: 별도의 인증 기관을 유지할 필요가 없습니다(X.509/IETF PKIX 표준 참조).
- **맞춤 서명된 TLS/SSL 인증서 –** 인증서가 자동으로 생성되고 iDRAC에 이미 업로드된 개인 키를 사용하여 서명됩니다.
  - » 장점: 모든 iDRAC에 신뢰할 수 있는 단일 CA가 사용됩니다. 내부 CA가 관리 스테이션에서 이미 신뢰되어 있을 수 있습니다.
- **CA 서명된 TLS/SSL 인증서 –** CSR(Certificate Signing Request)이 생성되고 서명을 위해 내부 CA에 제출되거나 VeriSign, Thawte, Go Daddy와 같은 타사 CA에 의해 제출됩니다.
  - » 장점: 커머셜 인증 기관을 사용할 수 있습니다(X.509/IETF PKIX 표준 참조). 모든 iDRAC에 신뢰할 수 있는 단일 CA가 사용됩니다. 커머셜 CA가 사용되는 경우 관리 스테이션에서 이미 신뢰되어 있을 가능성이 매우 높습니다.

iDRAC9은 이미 PowerEdge 서버에 대한 안전한 액세스를 제공하는 고객의 기존 인증 및 권한 부여 스키마를 활용하여 **Active Directory** 및 **LDAP**과의 통합을 지원합니다. 또한 **RBAC(Role-based Access Control)**를 지원하여 서버 운영 담당자의 역할에 맞춰 필요한 만큼 적절한 수준의 액세스 권한(Administrator, Operator 또는 Read Only)을 부여합니다. 모든 사용자에게 가장 높은 수준의 액세스 권한(즉, Administrator)을 부여하기 보다는 이 방식으로 RBAC를 사용할 것을 적극 권장합니다.

또한 iDRAC9은 **IP 차단 및 필터링**을 비롯하여 무단 액세스를 방지하는 추가적인 방법을 제공합니다. IP 차단은 특정 IP 주소에서 과도한 로그인 실패가 발생할 경우 이를 동적으로 파악하여 사전 선택된 기간 동안 해당 주소에서 iDRAC9에 로그인하지 못하도록 차단합니다. IP 필터링은 iDRAC에 액세스하는 클라이언트의 IP 주소 범위를 제한합니다. 들어오는 로그인의 IP 주소를 지정된 범위와 비교하여 소스 IP 주소가 지정된 범위에 속한 관리 스테이션에서 이루어지는 iDRAC 액세스만 허용하고 다른 모든 로그인 요청은 거부합니다.

사용자 이름 및 암호에 기반한 1단계 인증 스키마의 취약성이 증가함에 따라 **MFA(Multi-Factor Authentication)**가 더욱 널리 사용되고 있습니다. iDRAC9은 원격 GUI 액세스 시 스마트 카드의 사용을 허용하고, RSA 토큰도 지원합니다. 두 경우 모두 MFA에서 디바이스 또는 카드의 실제 존재 여부와 관련 PIN을 확인합니다.

3.2.1 RSA SecurID MFA

RSA SecurID는 시스템에서 사용자를 인증하는 또 다른 수단으로 사용할 수 있습니다. iDRAC9은 또 다른 2단계 인증 방법으로 Datacenter 라이선스 및 펌웨어 4.40.00.00을 사용하여 RSA SecurID를 지원합니다.

3.2.2 간소화된 2FA

제공되는 또 다른 인증 방법은 iDRAC에 로그인할 때 임의로 생성된 토큰을 사용자의 이메일 수신함으로 보내는 Easy 2FA입니다.

3.2.3 SELinux 프레임워크

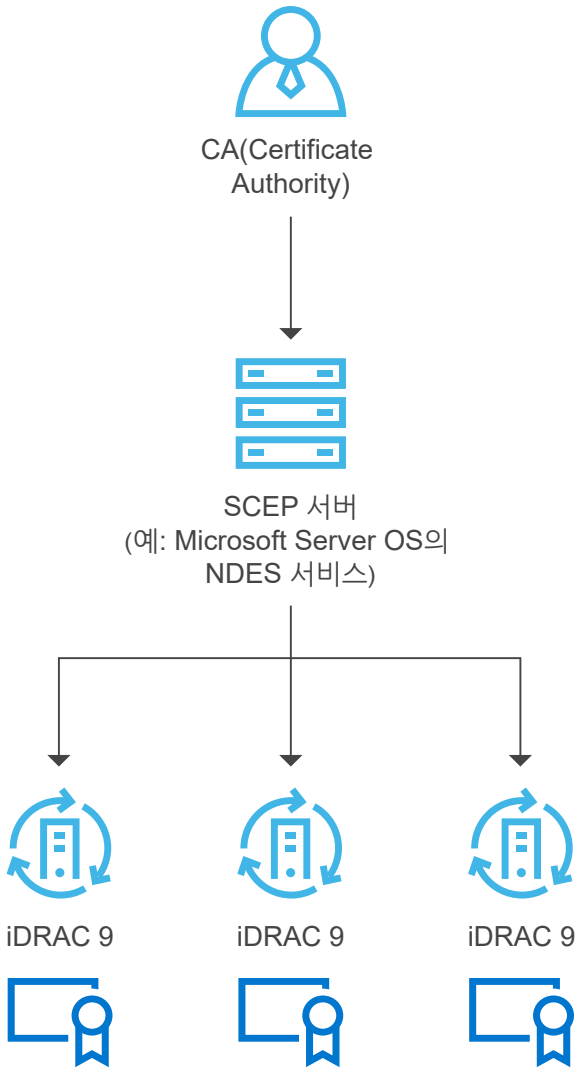
SELinux는 iDRAC의 핵심 커널 수준에서 작동하며 사용자의 입력이나 구성이 필요하지 않습니다. SELinux는 공격이 탐지되면 보안 메시지를 기록합니다. 이러한 로그 메시지는 공격자가 시스템에 대한 침입을 시도한 시기와 방법을 나타냅니다. 현재 이러한 로그는 이 새로운 기능에 등록한 고객이 SupportAssist를 통해 사용할 수 있으며, iDRAC의 향후 릴리스에서는 Lifecycle Controller Log로 제공됩니다.

3.2.4 최소 필수 권한

iDRAC 내에서 실행되는 모든 내부 프로세스는 최소한의 권한으로 실행되며, 이는 Unix 보안의 핵심적 개념입니다. 이렇게 하면 공격 대상인 시스템의 프로세스가 해당 프로세스의 범위를 벗어난 파일 또는 하드웨어에 액세스할 수 없게 됩니다. 예를 들어 가상 KVM을 지원하는 프로세스는 팬 속도를 변경할 수 없어야 합니다. 이 두 프로세스를 별도의 기능으로 실행하면 공격이 프로세스 간에 전파되는 것을 방지하여 시스템을 보호할 수 있습니다.

3.2.5 자동 인증서 등록 및 갱신

iDRAC9 v4.0에는 SCEP(Simple Certificate Enrollment Protocol) 지원을 위한 클라이언트가 추가되었으며 Datacenter 라이선스가 필요합니다. SCEP는 자동 등록 프로세스를 사용하여 다수의 네트워크 디바이스에 대한 인증서를 관리하는 데 사용되는 프로토콜 표준입니다. iDRAC는 이제 Microsoft ServerNDES 서비스와 같은 SCEP 호환 서버와 통합되어 SSL/TLS 인증서를 자동으로 유지 관리할 수 있습니다. 이 기능은 만료 예정인 웹 서버 인증서를 등록하고 갱신하는 데 사용할 수 있으며, iDRAC GUI에서 일대일 방식으로 수행하거나 서버 구성 프로파일을 통해 설정하거나 RACADM과 같은 툴을 통해 스크립팅할 수 있습니다.



3.2.6 출고 시 생성된 기본 암호

기본적으로 모든 14G PowerEdge 서버에는 보안을 강화하기 위해 사전 생성된 고유한 iDRAC 암호가 제공됩니다. 이 암호는 출고 시 생성되어 섀시 전면의 서버 자산 레이블 옆에 있는 풀아웃 정보 태그에 기재되어 있습니다. 이 기본 방법을 선택하는 사용자는 이 암호를 확인하여 iDRAC에 처음으로 로그인할 때 범용 기본 암호 대신 사용해야 합니다. Dell EMC는 보안을 위해 기본 암호를 변경할 것을 적극 권장합니다.

3.2.7 유연한 시스템 잠금

iDRAC9은 한 대 이상의 서버 하드웨어 및 펌웨어 구성을 '잠그는' 새로운 기능을 제공하며 Enterprise 또는 Datacenter 라이선스가 필요합니다. 이 모드는 GUI 또는 RACADM과 같은 CLI를 사용하거나 서버 구성 파일의 일부로 활성화할 수 있습니다. 관리자 권한이 있는 사용자가 시스템 잠금 모드를 설정하면 보다 낮은 권한을 가진 사용자가 서버를 변경하지 못하게 됩니다. 이 기능은 IT 관리자가 활성화 또는 비활성화할 수 있습니다. 시스템 잠금이 비활성화된 상태에서 이루어진 모든 변경 사항은 Lifecycle Controller Log에서 추적됩니다. 잠금 모드를 활성화하면 Dell EMC 툴 및 에이전트를 사용할 때 데이터 센터의 구성 변경을 방지할 수 있고 Dell EMC 업데이트 패키지를 사용할 때 펌웨어에 대한 악의적 공격을 방지할 수 있습니다. 잠금 모드는 시스템을 재부팅하지 않고도 동적으로 활성화할 수 있습니다. iDRAC9 v4.40에는 DUP(Dell Update Package)를 사용하여 업데이트만 제어하는 현재의 시스템 잠금 외에도 이 기능이 일부 NIC로 확장되는 개선 기능이 포함됩니다. (참고: NIC의 강화된 잠금에는 펌웨어 업데이트 방지를 위한 펌웨어 잠금만 포함됩니다.) 구성(x-UEFI) 잠금은 지원되지 않습니다. 고객이 지원되는 인터페이스에서 속성을 활성화 또는 설정하여 시스템을 잠금 모드로 설정하면 iDRAC에서 시스템 구성에 따라 추가 조치를 취합니다. 이러한 조치는 iDRAC 검색 프로세스의 일환으로 탐지된 타사 디바이스에 따라 다릅니다.

3.2.8 도메인 격리

14세대 및 15세대 PowerEdge 서버는 멀티 테넌트 호스팅 환경에서 중요한 기능인 **도메인 격리**를 통해 보안을 강화합니다. 서버 하드웨어 구성의 보안을 유지하기 위해 호스팅 공급업체는 테넌트에 의한 재구성을 차단하는 것이 좋을 수 있습니다. 도메인 격리는 호스트 OS의 관리 애플리케이션이 아웃오브밴드 iDRAC나 ME(Management Engine) 또는 IE(Innovation Engine) 같은 인텔 칩셋 기능에 액세스할 수 없도록 선택할 수 있는 구성 방법입니다.

3.3 서명된 펌웨어 업데이트

PowerEdge 서버는 여러 세대 동안 펌웨어 업데이트에 디지털 서명을 사용하여 신뢰할 수 있는 펌웨어만 서버 플랫폼에서 실행되도록 보장하고 있습니다. 2048비트 RSA 암호화를 사용한 SHA-256 해싱을 통해 모든 펌웨어 패키지를 디지털로 서명하여 iDRAC, BIOS, PERC, I/O 어댑터 및 LOM, PSU, 스토리지 드라이브, CPLD 및 백플레인 컨트롤러용 펌웨어를 비롯한 주요 서버 구성 요소에 서명합니다. iDRAC는 펌웨어 업데이트를 검색하여 해당 서명을 칩 내장형 RoT(Root of Trust)를 사용한 서명과 비교하여, 검증에 실패한 펌웨어 패키지는 중단되고 오류 메시지가 LCL(LifeCycle Log)에 기록되어 IT 관리자가 이를 확인할 수 있습니다.

대다수 타사 디바이스에 향상된 펌웨어 인증 기능이 내장되어 있어 자체 RoT(Root-of-Trust) 메커니즘을 사용한 서명 검증을 제공합니다. 이를 통해 침해된 타사 업데이트 툴을 이용하여 악성 펌웨어를 NIC 또는 스토리지 드라이브 등에 로드하거나 서명된 Dell EMC 업데이트 패키지를 사용하는 것을 우회할 수 있는 가능성을 차단합니다. PowerEdge 서버와 함께 제공되는 대다수의 타사 PCIe 및 스토리지 디바이스는 하드웨어 RoT(Root of Trust)를 사용하여 해당 펌웨어 업데이트를 검증합니다.

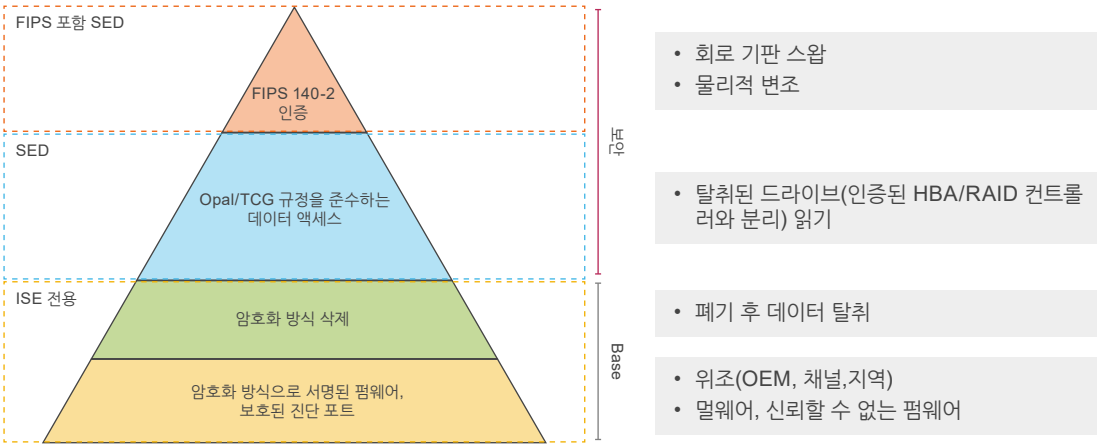
특정 디바이스 펌웨어의 악의적인 변조가 의심될 경우 IT 관리자는 대부분의 플랫폼 펌웨어 이미지를 iDRAC에 저장된 신뢰할 수 있는 이전 버전으로 롤백할 수 있습니다. PowerEdge 서버에는 기존 운영 버전("N")과 이전의 신뢰할 수 있는 버전("N-1")으로 두 가지 버전의 디바이스 펌웨어가 유지됩니다.

3.4 암호화된 데이터 스토리지

14세대 및 15세대 PowerEdge 서버는 데이터 보호를 위해 다양한 스토리지 드라이브 선택 사항을 제공합니다. 아래에 나와 있는 것처럼 이러한 선택 사항은 ISE(Instant Secure Erase)를 지원하는 드라이브에서 시작합니다. ISE는 사용자 데이터를 즉시 안전하게 삭제하는 새로운 기술입니다. 14세대 및 15세대 서버는 기본적으로 ISE 지원 드라이브를 제공합니다. ISE에 대해서는 System Erase 기능 설명의 일부로 이 백서의 뒷부분에서 자세히 설명합니다.

다음으로 높은 수준의 보안 선택 사항은 SED(Self-Encrypting Drive)입니다. 이는 스토리지 드라이브를 사용되는 서버 및 RAID 카드에 바인딩하는 잠금 보호 기능을 제공합니다. 이를 통해 소위 "스매시 앤드 그랩(smash and grab)"이라는 수법으로 드라이브 탈취 및 드라이브에 저장되어 있는 중요한 사용자 데이터의 손실 위험을 방지합니다. 탈취자가 드라이브를 사용하려고 할 때 필요한 잠금 키 암호를 모르기 때문에 암호화된 드라이브 데이터에 액세스하지 못하게 됩니다. 고객은 이 백서의 뒷부분에서 설명하는 SEKM(Secure Enterprise Key Manager)을 사용하여 전체 서버의 탈취 위험을 방지할 수 있습니다.

가장 높은 수준의 보호는 NIST FIPS 140-2 인증을 획득한 SED를 통해 제공됩니다. 이 표준을 준수하는 드라이버는 테스트 연구소의 인증을 획득했으며 변조 방지 스티커가 드라이브에 부착되어 있습니다. Dell EMC SED 드라이브는 기본적으로 FIPS 140-2 인증을 획득했습니다.



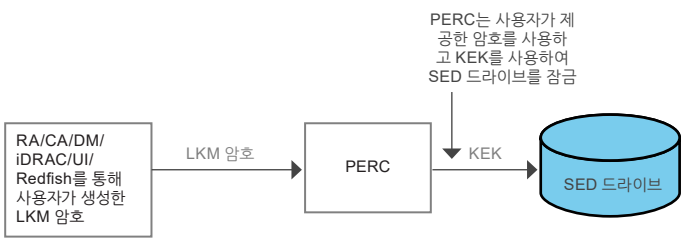
3.4.1 iDRAC Credential Vault

iDRAC 서비스 프로세서는 iDRAC 사용자 자격 증명 및 자체 서명된 SSL 인증서의 개인 키와 같은 다양한 기밀 데이터를 보호하는 안전한 스토리지 메모리를 제공합니다. 칩 내장형 보안의 한 가지 예인 이 메모리는 제조 시 각 iDRAC 칩에 프로그래밍되는 변경 불가능한 고유 루트 키로 암호화됩니다. 이를 통해 공격자가 데이터에 액세스하기 위해 칩의 땜납을 제거하는 물리적 공격으로부터 보호할 수 있습니다.

3.4.2 LKM(Local Key Management)

현재 PowerEdge 서버는 LKM(Local Key Management)을 사용하여 PERC 컨트롤러에 연결된 SED 드라이브를 보호하는 기능을 제공합니다.

드라이브 탈취 시 사용자 데이터 보호를 보장하려면 키가 제공되지 않는 한 사용자 데이터를 복호화하지 않도록 별도의 키로 SED를 잠가야 합니다. 이 키를 KEK(Key Encryption Key)라고 합니다. 이를 위해 사용자가 SED가 연결된 PERC 컨트롤러에 키 ID/암호를 설정하면, PERC 컨트롤러에서 암호를 사용하여 KEK를 생성하고 이를 사용하여 SED를 잠급니다. 이제 드라이브의 전원이 켜지면 잠긴 SED가 표시되고 잠금 해제를 위해 KEK가 제공된 경우에만 사용자 데이터를 암호화/복호화할 수 있습니다. PERC는 드라이브에 KEK를 제공하여 잠금을 해제합니다. 이때 탈취된 드라이브가 "잠김" 상태로 표시되고 공격자가 KEK를 제공할 수 없으면 사용자 데이터가 보호됩니다. 이를 암호로 Local이라고 하며 KEK는 PERC에 로컬로 저장됩니다. 다음 다이어그램은 LKM 솔루션을 보여줍니다.

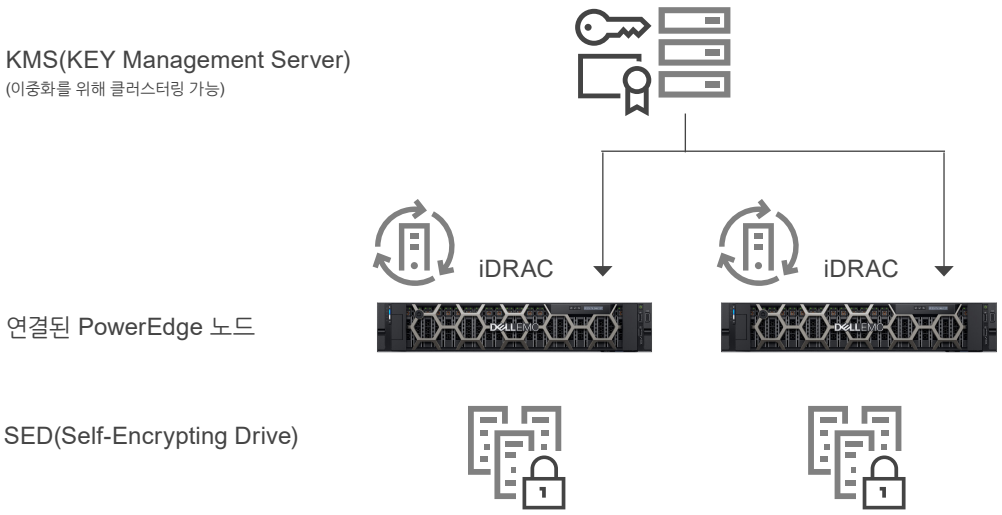


3.4.3 SEKM(Secure Enterprise Key Manager)

OpenManage SEKM은 조직 전체에서 저장 데이터를 관리하기 위한 중앙 키 관리 솔루션을 제공합니다. 이를 통해 고객은 외부 KMS(Key Management Server)를 사용하여 iDRAC에서 Dell EMC PowerEdge 서버의 스토리지 디바이스를 잠그고 잠금 해제하는 데 사용할 수 있는 키를 관리할 수 있습니다. iDRAC는 특별 라이선스로 활성화되는 내장 코드를 사용하여 KMS에 각 스토리지 컨트롤러에 대한 키를 생성하도록 요청합니다. 그런 다음 이 키를 가져와 호스트를 부팅할 때마다 스토리지 컨트롤러에 제공하여 스토리지 컨트롤러가 SED(Self-Encrypting Drive)의 잠금을 해제할 수 있도록 합니다.

LKM(Local Key Management)과 비교해 SEKM을 사용할 때의 이점은 다음과 같습니다.

- 키가 서버에 저장되지 않고 외부에 저장되고 iDRAC를 통해 연결된 PowerEdge 서버 노드에서 검색되므로 "서버 탈취"를 방지
- 암호화된 디바이스에 중앙 집중식 확장 가능한 키 관리 기능을 제공하여 높은 가용성 유지
- 업계 표준 KMIP 프로토콜을 지원하므로 다른 KMIP 호환 디바이스 사용 지원
- 드라이브 또는 전체 서버 공격 시 저장 데이터 보호
- 드라이브 수에 따라 드라이브 내 암호화 성능 확장



3.5 하드웨어 보안

하드웨어 보안은 포괄적인 보안 솔루션의 핵심적인 부분입니다. 일부 고객은 USB 같은 진입 포트에 대한 액세스를 제한하길 원합니다. 운영을 개시한 후에는 일반적으로 서버 섀시를 열 필요가 없습니다. 모든 고객은 최소한 그러한 활동을 추적하고 로그로 남기길 원합니다. 전반적인 목적은 물리적인 침입을 방지하고 제한하는 것입니다.

3.5.1 섀시 침입 알림

PowerEdge 서버는 하드웨어 침입 탐지 및 로깅 기능을 제공하며, AC 전원이 공급되지 않는 경우에도 탐지 기능이 작동합니다. 운송 중인 경우를 포함하여 섀시를 열거나 변조하려고 할 경우 섀시에 있는 센서를 통해 해당 활동이 탐지됩니다. 운송 중에 서버가 열린 경우 전원이 공급된 후에 iDRAC LCL(LifeCycle Log)에 관련 내용의 항목이 생성됩니다.

3.5.2 동적 USB 포트 관리

보안 강화를 위해 USB 포트를 완전히 비활성화할 수 있습니다. 또는 전면에 있는 USB 포트만 비활성화할 수도 있습니다. 예를 들어 USB 포트를 운영 환경에서 비활성화한 후 디버깅을 위해 크래시 카트에 액세스하도록 일시적으로 활성화할 수 있습니다.

3.5.3 iDRAC Direct

iDRAC Direct는 서버 전면(냉기 통로)에서 서버 디버깅 및 관리를 수행하기 위해 iDRAC 서비스 프로세서에 유선으로 연결된 특수 USB 포트입니다. 표준 Micro-AB USB 케이블을 이 포트에 연결하고 케이블의 다른 쪽 끝(Type A)을 노트북 컴퓨터에 연결할 수 있습니다. 그런 다음 표준 웹 브라우저로 iDRAC GUI에 액세스하여 서버에 대한 광범위한 디버깅 및 관리 작업을 수행할 수 있습니다. iDRAC Enterprise 라이선스가 설치된 경우 iDRAC의 가상 콘솔 기능을 통해 OS 데스크탑에도 액세스할 수 있습니다.

iDRAC Direct는 로그인하는 데 일반 iDRAC 자격 증명이 사용되므로 안전한 크래시 카트 역할을 하며, 광범위한 하드웨어 관리 및 서비스 진단을 수행할 수 있는 추가적인 이점을 제공합니다. iDRAC Direct는 원격 사이트의 서버에 대한 물리적 액세스의 보안을 유지하기 위한 훌륭한 방법이 될 수 있습니다(이 경우 호스트 USB 포트와 VGA 출력을 비활성화할 수 있음).

3.5.4 지리적 위치를 포함한 iDRAC 연결 뷰

연결 뷰는 iDRAC가 서버 I/O에 연결된 외부 스위치 및 포트를 보고하는 기능을 제공합니다. 일부 네트워킹 디바이스에서 지원되는 기능으로 연결된 스위치에서 LLDP(Link Layer Discovery Protocol)가 활성화되어 있어야 합니다.

연결 뷰의 이점을 다음과 같습니다.

- 서버 I/O 모듈(LOM, NDC 및 추가 기능 PCIe 카드)이 올바른 스위치 및 포트에 연결되어 있는지 원격으로 빠르게 확인할 수 있습니다.
- 배선 오류를 수정하기 위해 비용이 많이 드는 원거리 기사 파견이 필요하지 않습니다.
- 서버실의 열기 통로에서 케이블을 확인할 필요가 없습니다.
- GUI를 통해 이 기능을 사용하거나, RACADM 명령을 통해 모든 14G 연결에 대한 정보를 확인할 수 있습니다.

시간과 비용을 크게 절감할 수 있는 것 외에도 연결 뷰를 사용하면 물리적 서버 또는 가상 머신의 지리적 위치를 실시간으로 파악할 수 있다는 이점이 있습니다. iDRAC 연결 뷰를 통해 관리자는 서버에 연결되는 스위치와 포트를 정확하게 파악하여 회사 보안 지침 또는 모범 사례를 따르지 않는 네트워크 및 디바이스에는 서버를 연결하지 않도록 할 수 있습니다.

연결 뷰는 서버에 연결된 스위치 ID를 보고하므로 간접적으로 서버의 위치를 확인할 수 있습니다. 스위치 ID를 통해 지리적 위치를 파악하여 서버가 승인되지 않은 사이트의 악성 서버가 아니라는 점을 확인할 수 있으므로 보안 관제가 한층 향상됩니다. 또한 애플리케이션 또는 VM이 해외에 있지 않으며, 승인되고 안전한 환경에서 실행되고 있는지 확인할 수 있습니다.

3.6 공급망 무결성 및 보안

공급망 무결성은 두 가지 주요 당면 과제에 중점을 둡니다.

1. 하드웨어 무결성 유지: 제품이 고객에게 배송되기 전에 제품이 변조되거나 위조 구성 요소가 삽입되지 않도록 보장합니다.
2. 소프트웨어 무결성 유지: 제품이 고객에게 배송되기 전에 펌웨어 또는 디바이스 드라이버에 멀웨어가 삽입되지 않도록 보장하며 코딩 취약성을 방지합니다.

Dell EMC의 공급망 보안은 물리적 자산, 인벤토리, 정보, 지적 재산 및 사용자를 보호하는 방지/탐지 제어 조치 적용을 의미합니다. 또한 이러한 보안 조치는 공급망에 멀웨어 및 위조 구성 요소가 악의적으로 또는 부주의로 유입될 가능성을 줄임으로써 공급망에 대한 보증과 무결성을 제공합니다.

3.6.1 하드웨어 및 소프트웨어 무결성

Dell EMC는 위조 구성 요소가 공급망에 유입될 가능성을 최소화하기 위해 품질 관리 프로세스를 갖추는 데 중점을 두고 있습니다. 공급업체 선택, 조달, 생산 프로세스, 감사 및 테스트를 통한 거버넌스에 모두 Dell EMC의 품질 관리가 적용됩니다. 공급업체를 선택한 후에는 새로운 제품 도입 프로세스를 통해 전체 제작 단계에서 사용된 모든 자재가 승인된 공급업체에서 공급된 것인지, 그리고 해당하는 경우 BOM(Bill of Materials)과 일치하는지 확인합니다. 생산 중 자재 검수를 통해 표시가 잘못되었거나 정상 성능 매개변수를 이탈했거나 잘못된 전자 식별자가 포함된 구성 요소를 식별합니다.

부품은 가능하면 ODM(Original Design Manufacturer) 또는 OCM(Original Component Manufacturer)에서 직접 조달됩니다. 새로운 제품 도입 프로세스 중에 이루어지는 자재 검수를 통해 공급망에 유입되었을 수 있는 위조 구성 요소나 손상된 구성 요소를 재차 확인할 수 있습니다.

또한 Dell EMC는 전 세계 모든 제조 사이트에서 ISO 9001 인증을 유지하고 있습니다. 이러한 프로세스 및 제어 조치를 엄격하게 준수함으로써 위조 구성 요소가 Dell EMC 제품에 유입되거나 멀웨어가 펌웨어 또는 디바이스 드라이버에 삽입될 위험이 최소화됩니다. 이러한 조치는 SDL(Software Development Lifecycle) 프로세스의 일환으로 구현됩니다.

3.6.2 보안 관제

Dell EMC는 제조 시설과 물류망에서 보안을 구현하고 유지하는 다양한 핵심 프로세스를 장기적으로 시행하고 있습니다. 예를 들어 주요 구역에 모니터링되는 폐쇄 회로 카메라를 사용하고, 액세스 제어를 적용하고, 24시간 출입구 경비를 수행하는 것을 비롯하여 Dell EMC 제품을 제작하는 특정 공장들에 지정된 TAPA(Transported Asset Protection Association) 시설 보안 요건을 준수하도록 요구하고 있습니다. 또한 업계를 선도하는 물류 프로그램을 통해 운송 중 제품 도난과 변조를 방지하기 위한 보호 조치가 구현되어 있습니다. 이 프로그램은 24시간 유인 관제 센터를 통해 전 세계적으로 특정 인바운드 및 아웃바운드 운송을 모니터링하여 목적지 간에 중단 없이 운송이 이루어지도록 보장합니다.

또한 Dell EMC는 여러 자발적 공급망 보안 프로그램 및 이니셔티브에 적극 참여하고 있습니다. 이러한 이니셔티브의 한 가지 예는 미국 정부가 9/11 이후 강화된 국경 및 공급망 보안 조치를 통해 테러 가능성을 줄이기 위해 도입한 C-TPAT(Customs-Trade Partnership Against Terrorism)입니다. 이 이니셔티브의 일환으로 미국 관세 및 국경 보호국은 회원 조직이 각자의 보안 프로세스의 무결성을 보장하고 공급망 내 비즈니스 파트너에게 보안 지침을 전달하도록 요구하고 있습니다. Dell EMC는 2002년 이후로 이 이니셔티브에 적극 참여하고 있으며 최상의 멤버십 자격을 유지하고 있습니다.

3.6.3 PowerEdge용 Dell Technologies SCV(Secured Component Verification)

PowerEdge용 Dell Technologies SCV(Secured Component Verification)는 Dell EMC 고객이 배송받은 PowerEdge 서버가 공장에서 제조된 것과 일치하는지 검증할 수 있는 공급망 보증 오퍼링입니다. 암호화 방식으로 구성 요소를 검증하기 위해, 제조 프로세스 중에 특정 서버에 대한 고유한 구성 요소 ID를 포함하는 인증서가 생성됩니다. 이 인증서는 Dell Technologies 공장에서 서명되어 iDRAC에 저장되며, 이후 SCV 애플리케이션에서 사용됩니다. 고객은 SCV 애플리케이션을 사용하여 고유한 구성 요소 ID를 비롯한 현재 시스템 인벤토리를 수집하고, 수집한 인벤토리를 SCV 인증서의 인벤토리를 기준으로 검증합니다.

SCV 애플리케이션에서 생성된 보고서는 출고 시 설치된 구성 요소와 비교하여 일치하는 구성 요소와 일치하지 않는 구성 요소를 확인합니다. 또한 iDRAC용 SCV 개인 키의 소유 증명과 함께 인증서 및 신뢰 체인도 확인합니다. 현재 구현에서는 직접 발송 고객을 지원하며, VAR 또는 부품 교체 시나리오는 포함하지 않습니다.

4. 탐지

서버 시스템의 구성, 상태 및 변경 이벤트를 포괄적으로 파악할 수 있는 탐지 기능을 갖추는 것이 중요합니다. 이러한 탐지 기능을 통해 부팅 및 OS 런타임 프로세스 내의 BIOS, 펌웨어 및 선택 사항인 ROM에 대한 악의적인 변경이나 기타 변경을 파악해야 합니다. 사전 예방적 폴링과 함께 시스템 내 모든 이벤트에 대한 알림을 전송하는 기능이 필요하며, 서버에 대한 액세스 및 변경 내역과 관련된 완전한 정보가 로그에 기록되어야 합니다. 그리고 무엇보다 이러한 기능이 서버의 모든 구성 요소에 적용되어야 합니다.

4.1 iDRAC를 통한 포괄적인 모니터링

iDRAC는 OS 에이전트 대신 각 디바이스에 대한 직접 사이드 밴드(Side-Band) 경로를 사용하여 서버의 관리되는 리소스와 통신합니다. Dell EMC는 PERC RAID 컨트롤러,이더넷 NIC, Fibre Channel HBA, SAS HBA 및 NVMe 드라이브와 같은 주변 기기와 통신할 때 MCTP, NC-SI, NVMe-MI 등의 업계 표준 프로토콜을 활용했습니다. 이 아키텍처는 PowerEdge 서버에 에이전트 없는 디바이스 관리를 제공하기 위해 수 년에 걸쳐 업계를 선도하는 공급업체와 장기적으로 파트너십을 맺은 결과입니다. 구성 및 펌웨어 업데이트 작업에도 Dell EMC 및 파트너가 지원하는 강력한 UEFI 및 HII 기능이 활용됩니다.

이 기능을 통해 iDRAC는 시스템의 구성 이벤트, 침입 이벤트(예: 이 백서의 앞부분에서 언급한 섀시 침입 탐지) 및 상태 변경을 모니터링할 수 있습니다. 구성 이벤트의 경우, 변경을 시작한 사용자(GUI 사용자, API 사용자 또는 콘솔 사용자)의 ID를 바로 확인할 수 있습니다.

4.1.1 LCL(LifeCycle Log)

LCL(LifeCycle Log)은 일정 기간 동안 서버에서 발생하는 이벤트의 모음입니다. LCL(LifeCycle Log)에는 이벤트에 대한 설명과 타임스탬프, 심각도, 사용자 ID 또는 소스, 권장 조치 및 기타 추적 또는 알림에 유용한 기술 정보가 나와 있습니다.

LCL(LifeCycle Log)에는 다음과 같은 다양한 유형의 정보가 기록됩니다.

- 시스템 하드웨어 구성 요소에 대한 구성 변경
- iDRAC, BIOS, NIC 및 RAID 구성 변경
- 모든 원격 작업의 로그
- 디바이스, 버전 및 날짜 기준의 펌웨어 업데이트 기록
- 교체된 부품에 대한 정보
- 고장난 부품에 대한 정보
- 이벤트 및 오류 메시지 ID
- 호스트 전원 관련 이벤트
- POST 오류
- 사용자 로그인 이벤트
- 센서 상태 변경 이벤트

4.1.2 알림

iDRAC는 다양한 이벤트 알림과 특정 LCL(LifeCycle Log) 이벤트가 발생할 경우 수행할 조치를 구성하는 기능을 제공합니다. 이벤트가 발생하면 선택된 알림 유형 메커니즘을 사용하여 구성된 대상에게 전달됩니다. iDRAC 웹 인터페이스, RACADM 또는 iDRAC 설정 유틸리티를 통해 알림을 활성화하거나 비활성화할 수 있습니다.

iDRAC는 다음과 같은 유형의 알림을 지원합니다.

- 이메일 또는 IPMI 알림
- SNMP 트랩
- OS 및 원격 시스템 로그
- Redfish 이벤트

또한 알림을 심각도(심각, 경고 또는 정보)별로 분류할 수 있습니다.

다음과 같은 필터를 알림에 적용할 수 있습니다.

- 시스템 상태(예: 온도, 전압 또는 디바이스 오류)
- 스토리지 상태(예: 컨트롤러 오류, 물리적 또는 가상 디스크 오류)
- 구성 변경(예: RAID 구성 변경, PCIe 카드 제거)
- 감사 로그(예: 암호 인증 실패)
- 펌웨어/드라이버(예: 업그레이드 또는 다운그레이드)

마지막으로 IT 관리자는 알림에 대한 다양한 조치(재부팅, 전원 순환, 전원 끄기 또는 조치 없음)를 설정할 수 있습니다.

4.2 변경 탐지

표준화된 구성을 적용하고 변경에 대한 "무관용" 정책을 채택함으로써 취약점 공격의 가능성을 줄일 수 있습니다. Dell EMC OpenManage Enterprise 콘솔을 통해 고객은 고유한 서버 구성 기준을 정의한 후 운영 서버가 해당 기준에서 변경되는 것을 모니터링할 수 있습니다. 기준은 보안 및 성능과 같은 운영 환경에 적합한 다양한 조건을 사용하여 정의할 수 있습니다. OpenManage Enterprise는 기준에서 벗어난 사항을 보고하고 필요에 따라 간단한 워크플로를 통해 iDRAC 아웃오브밴드에서 변경 사항을 스테이징하여 변경 사항을 복구할 수 있습니다. 그러면 다음번 유지 보수 기간에 서버가 재부팅될 때 복구를 위한 변경이 이루어져 운영 환경이 다시 기준을 준수하게 됩니다. 이 단계별 프로세스를 통해 유지 보수 기간이 아니더라도 서버 다운타임 없이 운영 환경에 구성 변경 사항을 적용할 수 있습니다. 따라서 서비스 가용성과 보안이 저해되지 않고 서버 가용성이 향상됩니다.

5. 복구

서버 솔루션은 다양한 이벤트에 대응하여 알려진 정합성 상태로의 복구를 지원해야 합니다.

- 새로 발견된 취약성
- 악의적 공격 및 데이터 변조
- 메모리 장애 또는 잘못된 업데이트 절차로 인한 펌웨어 손상
- 서버 구성 요소 교체
- 서버 폐기 또는 용도 변경

아래에서는 Dell EMC가 새로운 취약성 및 손상 문제에 대응하는 방법과 필요한 경우 원래 상태로 서버를 복구하는 방법을 자세히 설명합니다.

5.1 새로운 취약성에 신속하게 대응

CVE(Common Vulnerabilities and Exposures)는 소프트웨어 및 하드웨어 제품의공격에 사용되는 새롭게 발견된 공격 요소입니다. CVE에 적시에 대응하여 신속하게 공격 노출을 진단하고 적절한 조치를 취하는 것이 대부분의 기업에서 매우 중요합니다.

CVE는 다음을 비롯한 다수의 항목에서 식별된 새로운 취약성에 대응하여 발표될 수 있습니다.

- OpenSSL 등의 오픈 소스 코드
- 웹 브라우저 및 기타 인터넷 액세스 소프트웨어
- 공급업체의 하드웨어 및 펌웨어 제품
- 운영 체제 및 하이퍼바이저

Dell EMC는 PowerEdge 서버에 존재하는 새로운 CVE에 신속하게 대응하고 다음을 비롯한 정보를 적시에 고객에게 제공하고자 적극 노력하고 있습니다.

- 영향을 받는 제품
- 문제 해결 조치
- CVE를 해결하기 위한 업데이트 제공 시점(필요한 경우)

5.2 BIOS 및 OS 복구

Dell EMC 14세대 및 15세대 PowerEdge 서버에는 두 가지 유형의 복구, 즉 BIOS 복구와 빠른 OS(Operating System) 복구 기능이 포함되어 있습니다. 이러한 기능을 통해 손상된 BIOS 또는 OS 이미지에서 신속하게 복구할 수 있습니다. 두 경우에 모두 특수한 스토리지 영역이 런타임 소프트웨어(BIOS, 운영 체제, 디바이스 펌웨어 등)에서 숨겨져 있습니다. 이러한 스토리지 영역에는 손상된 기본 소프트웨어를 대체하여 사용할 수 있는 온전한 이미지가 들어 있습니다.

빠른 OS 복구 기능을 통해서는 손상된 OS 이미지(또는 악의적인 변조가 의심되는 OS 이미지)를 신속하게 복구할 수 있습니다. 복구 미디어로는 내부 SD 카드, SATA 포트, M.2 드라이브 또는 내부 USB를 사용할 수 있습니다. 선택한 디바이스를 부팅 목록과 OS에 표시하여 복구 이미지를 설치한 후 비활성화하고 부팅 목록과 OS에서 숨길 수 있습니다. 숨겨진 상태에서는 BIOS가 디바이스를 비활성화하므로 OS에서 액세스할 수 없습니다. OS 이미지가 손상될 경우 부팅을 위해 복구 위치를 활성화할 수 있습니다. 이러한 설정은 BIOS 또는 iDRAC 인터페이스를 통해 액세스할 수 있습니다.

악의적인 공격, 업데이트 중 전원 손실 또는 기타 예상치 못한 이벤트로 인해 BIOS가 손상되는 극단적인 경우 BIOS를 원래 상태로 복구하는 방법을 제공하는 것이 중요합니다. iDRAC에는 백업 BIOS 이미지가 저장되므로 필요한 경우 이 이미지를 사용하여 BIOS 이미지를 복구할 수 있습니다. iDRAC는 전체 복구 프로세스를 조정합니다.

- 자동 BIOS 복구는 BIOS 자체에서 시작됩니다.
- 필요 시 BIOS 복구는 RACADM CLI 명령을 사용하여 사용자가 시작할 수 있습니다.

5.3 펌웨어 롤백

최신 기능과 보안 업데이트를 사용하도록 펌웨어를 지속적으로 업데이트하는 것이 좋습니다. 그러나 업데이트 후 문제가 발생할 경우 업데이트를 롤백하거나 이전 버전을 설치해야 할 수 있습니다. 이전 버전으로 롤백하는 경우 해당 서명과 비교하여 검증됩니다.

기존 운영 환경 버전 "N"에서 이전 버전 "N-1"로의 펌웨어 롤백은 현재 다음 펌웨어 이미지에 대해 지원됩니다.

- BIOS
- Lifecycle Controller가 포함된 iDRAC
- NIC(Network Interface Card)
- PowerEdge RAID Controller(PERC)
- 전원 공급 장치(PSU)
- 후면판

다음 방법 중 하나를 사용하여 펌웨어를 이전에 설치된 버전("N-1")으로 롤백할 수 있습니다.

- iDRAC 웹 인터페이스
- CMC 웹 인터페이스
- RACADM CLI – iDRAC 및 CMC
- Lifecycle Controller GUI
- Lifecycle Controller - 원격 서비스

이전에 다른 인터페이스로 업그레이드를 수행한 경우에도 iDRAC 또는 Lifecycle Controller가 지원하는 모든 디바이스용 펌웨어를 롤백할 수 있습니다. 예를 들어 이전에 Lifecycle Controller GUI를 사용하여 펌웨어를 업그레이드했더라도 iDRAC 웹 인터페이스를 사용하여 롤백할 수 있습니다. 한 번의 시스템 재부팅으로 여러 디바이스에 대한 펌웨어 롤백을 수행할 수 있습니다.

단일 iDRAC 및 Lifecycle Controller 펌웨어가 있는 14세대 및 15세대 PowerEdge 서버에서 iDRAC 펌웨어를 롤백할 경우 Lifecycle Controller 펌웨어도 롤백됩니다.

5.4 하드웨어 서비스 후 서버 구성 복원

서비스 이벤트를 해결하는 것은 IT 운영의 중요한 부분입니다. RTO(Recovery Time Objective) 및 RPO(Recovery Point Objective)를 충족하는 것은 솔루션의 보안에 직접적인 영향을 미칩니다. 서버 구성 및 펌웨어를 복원하면 서버 운영에 대한 보안 정책이 자동으로 충족됩니다.

PowerEdge 서버는 다음과 같은 경우에 서버 구성을 신속하게 복원하는 기능을 제공합니다.

- 개별 부품 교체
- 마더보드 교체(전체 서버 프로파일 백업 및 복원)
- 마더보드 교체(Easy Restore)

5.4.1 부품 교체

iDRAC는 NIC 카드, RAID 컨트롤러 및 PSU(Power Supply Unit)에 대한 펌웨어 이미지와 구성 설정을 자동으로 저장합니다. 이러한 부품의 현장 교체 시 iDRAC는 자동으로 새 카드를 감지하고 펌웨어와 구성을 교체된 카드에 복원합니다. 이 기능을 통해 상당한 시간이 절감되고 일관된 구성과 보안 정책을 유지할 수 있습니다. 지원되는 부품을 교체한 후 시스템 재부팅 시 업데이트가 자동으로 수행됩니다.

5.4.2 Easy Restore(마더보드 교체 시)

마더보드 교체는 시간이 오래 걸리고 생산성에 영향을 미칠 수 있습니다. iDRAC는 PowerEdge 서버의 구성 및 펌웨어를 백업하고 복원하는 기능을 제공하여 장애가 발생한 마더보드를 교체하는 데 필요한 작업을 최소화합니다.

PowerEdge 서버는 다음 두 가지 방법으로 백업 및 복원을 수행할 수 있습니다.

1. PowerEdge 서버가 시스템 구성 설정(BIOS, iDRAC, NIC), 서비스 태그, UEFI 진단 애플리케이션 및 기타 라이선스가 부여된 데이터를 플래시 메모리에 자동으로 백업합니다.

   서버에서 마더보드를 교체한 후 Easy Restore에서 이 데이터를 자동으로 복원하라는 메시지를 표시합니다.

2. 보다 포괄적인 백업을 위해 사용자가 BIOS, RAID, NIC, iDRAC, Lifecycle Controller 및 NDC(Network Daughter Card)와 같은 다양한 구성 요소에 설치된 펌웨어 이미지와 이러한 구성 요소의 설정을 포함하여 시스템 구성을 백업할 수 있습니다. 또한 백업 작업에는 하드 디스크 구성 데이터, 마더보드 및 교체된 부품도 포함됩니다. 백업을 통해 단일 파일이 생성되며 이를 vFlash SD 카드 또는 네트워크 공유(예: CIFS, NFS, HTTP 또는 HTTPS)를 통해 저장할 수 있습니다.

   이 프로파일 백업은 사용자가 언제든지 복원할 수 있습니다. 향후 복원이 필요할 수 있는 모든 시스템 프로파일에 대해 백업 작업을 수행하는 것이 좋습니다.

5.5 System Erase

수명주기가 끝나면 시스템을 폐기하거나 용도를 변경해야 합니다. System Erase의 목적은 기밀 정보가 의도치 않게 유출되지 않도록 서버 스토리지 디바이스와 캐시 및 로그와 같은 서버 비휘발성 저장소에서 기밀 데이터와 설정을 삭제하는 것입니다. System Erase는 Lifecycle Controller의 유틸리티로서 로그, 구성 데이터, 스토리지 데이터, 캐시 및 내장된 애플리케이션을 삭제합니다.

System Erase 기능을 사용하여 다음과 같은 디바이스, 구성 설정 및 애플리케이션을 삭제할 수 있습니다.

- iDRAC(기본값으로 재설정)
- LC(Lifecycle Controller) 데이터
- BIOS
- 내장된 진단 및 OS 드라이버 팩
- iSM
- SupportAssist Collection 보고서

또한 다음과 같은 구성 요소도 삭제할 수 있습니다.

- 하드웨어 캐시(PERC NVCache 삭제)
- vFlash SD 카드(카드 초기화) (참고: vFlash는 15G 이상의 서버에서 사용할 수 없습니다.)

아래에 설명된 대로 다음과 같은 구성 요소의 데이터가 System Erase를 통해 암호화 방식으로 폐기됩니다.

- SED(Self-Encrypting Drive)
- ISE(Instant Secure Erase) 전용 드라이브
- NVM 디바이스(Apache Pass, NVDIMMs)

또한 ISE SATA 이외의 하드 드라이브는 데이터 덮어쓰기를 사용하여 삭제할 수 있습니다.

참고로 ISE(Instant Secure Erase)는 14세대 및 15세대 드라이브에 사용되는 내부 암호화 키를 파기하여 사용자 데이터를 복구 불가능하게 만듭니다. ISE는 스토리지 드라이브의 데이터를 삭제하는 방법으로 NIST Special Publication 800-88 "Guidelines for Media Sanitization"에 언급될 만큼 인정받고 있습니다.

System Erase가 포함된 새로운 ISE 기능의 장점은 다음과 같습니다.

- **속도:** DoD 5220.22-M과 같은 데이터 덮어쓰기 방법보다 훨씬 빠릅니다(몇 시간이 아닌 몇 초).
- **효과:** ISE는 예약된 블록을 포함하여 드라이브의 모든 데이터를 전혀 읽을 수 없게 만듭니다.
- **더 나은 TCO:** 스토리지 디바이스를 손상시키거나 물리적으로 파기하지 않으므로 재사용할 수 있습니다.

System Erase는 다음과 같은 방법으로 수행할 수 있습니다.

- Lifecycle Controller GUI(F10)
- RACADM CLI
- Redfish

5.6 iDRAC9 Cipher Select

Cipher Suite Select를 사용하여 웹 브라우저가 iDRAC와 통신하는 데 사용할 수 있는 암호를 제한할 수 있습니다. 또한 연결의 안전성을 판단할 수 있습니다. 이러한 설정은 iDRAC 웹 인터페이스, RACADM 및 Redfish를 통해 구성할 수 있습니다. 이 기능은 iDRAC7, iDRAC8(2.60.60.60 이상), 최신 iDRAC9(3.30.30.30 이상) 등 여러 iDRAC 릴리스에서 사용할 수 있습니다.

5.7 CNSA 지원

TLS 1.2비트 및 256비트 암호화가 포함된 iDRAC9에서 사용할 수 있는 암호가 아래 스크린샷 이미지에 나와 있습니다. 사용 가능한 암호에는 CNSA 승인 세트의 암호가 포함되어 있습니다.

5.8 전체 전원 순환

전체 전원 순환에서는 서버와 서버의 모든 구성 요소가 재부팅됩니다. 서버 및 모든 구성 요소에서 주 전원과 보조 전원이 끊깁니다. 휘발성 메모리의 모든 데이터도 삭제됩니다.

물리적 전체 전원 순환에서는 AC 전원 케이블을 뽑고 30초 동안 기다린 후 다시 꽂아야 합니다. 이는 원격 시스템에 대한 작업 시 문제가 됩니다. 14G 및 15G 서버의 새로운 기능을 사용하면 iSM, IDRAC GUI, BIOS 또는 스크립트에서 실제 전체 전원 순환을 수행할 수 있습니다. 전체 전원 순환은 다음번 전원 순환에서 적용됩니다.

전체 전원 순환 기능은 데이터 센터에 인력이 있어야 할 필요성을 없애므로 문제 해결 시간을 줄일 수 있습니다. 예를 들어 여전히 메모리에 상주하는 멀웨어를 제거할 수 있습니다.

6. 요약

데이터 센터의 보안은 비즈니스 성공을 위한 핵심이며 기본 서버 인프라스트럭처의 보안은 매우 중요합니다. 사이버 공격이 발생하면 장시간의 시스템 및 비즈니스 다운타임, 매출 및 고객 손실, 법적 손해 배상, 기업 평판 훼손 등의 결과를 초래할 수 있습니다. 하드웨어를 대상으로 이루어지는 사이버 공격을 방지 및 탐지하고 공격에서 복구하기 위해서는 보안을 사후에 추가하는 것이 아니라 서버 하드웨어 설계에 구현해야 합니다.

Dell EMC는 PowerEdge 서버에서 펌웨어 보안을 유지하고 중요한 사용자 데이터를 보호하기 위해 칩 내장형의 보안을 선도적으로 활용하고 있습니다. 14세대 및 15세대 PowerEdge 제품군은 칩 내장형 RoT(Root of Trust)를 사용하며 사이버 회복탄력성을 갖춘 아키텍처를 바탕으로 다음 기능을 비롯한 서버 보안을 한층 강화합니다.

- **암호화 방식으로 검증된 신뢰할 수 있는 부팅** - 포괄적인 서버 안전과 전반적인 데이터 센터 보안을 위한 기반으로, 칩 내장형 RoT(Root of Trust), 디지털 서명된 펌웨어 및 자동 BIOS 복구 기능이 포함됩니다.
- **보안 부팅** - OS가 실행되기 전에 UEFI 드라이버와 로드된 다른 코드의 암호화 서명을 확인합니다.
- **iDRAC Credential Vault** - 자격 증명, 인증서 및 기타 기밀 데이터를 위한 안전한 스토리지 공간으로 모든 서버에 고유한 칩 내장형 키로 암호화되어 있습니다.
- **동적 시스템 잠금** - PowerEdge만의 독보적인 기능으로, 모든 시스템 구성과 펌웨어를 악의적 변경이나 의도치 않은 변경에서 보호하고 모든 시스템 변경 시도를 사용자에게 알립니다.
- **엔터프라이즈 키 관리** - 조직 전체에서 저장 데이터를 관리하기 위한 중앙 집중식 키 관리 솔루션을 제공합니다.
- **System Erase** - 스토리지 드라이브와 기타 내장된 비휘발성 메모리의 데이터를 안전하고 빠르게 삭제하여 14세대 및 15세대 PowerEdge 서버를 간편하게 폐기하거나 용도 변경할 수 있도록 지원합니다.
- **공급망 보안** - 제품이 고객에게 배송되기 전에 제품이 변조되거나 위조 구성 요소가 삽입되지 않도록 보장하여 공급망을 보증합니다.

결론적으로 탁월한 보안을 자랑하는 14세대 및 15세대 PowerEdge 서버는 IT 혁신을 위한 신뢰할 수 있는 기반을 제공하여 고객이 IT 작업 및 워크로드를 안전하게 실행할 수 있습니다.

A. 부록: 추가 정보

보안 백서 및 보충 자료

- (Direct from Dev) Power Edge 서버의 System Erase 기능
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- System Erase 기능을 통한 14세대 Dell EMC Power Edge 서버 보안
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direct from Dev) 서버 설계에 구현된 보안
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Direct from Dev) 칩셋 및 BIOS에 구현된 사이버 회복탄력성
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- 출고 시 생성된 기본 iDRAC9 암호
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- CVE-2017-1000251 "BLUEBORNE"에 대한 Dell EMC iDRAC의 대응
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (비디오) RACADM을 사용한 보안 부팅 구성 및 인증서 관리
  https://youtu.be/mrIIN4X380c
- Dell EMC PowerEdge 서버의 보안 부팅 관리
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- 14세대 및 15세대 이상 Dell EMC PowerEdge 서버의 보안 부팅 기능을 위한 UEFI 이미지 서명
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- 빠른 운영 체제 복구
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- 14세대(14G) Dell EMC PowerEdge 서버에 대한 iDRAC9 이벤트 알림 관리
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFI 보안 부팅 맞춤 구성
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

PowerEdge 백서

- iDRAC 개요
  http://www.DellTechCenter.com/iDRAC
- OpenManage Console 개요
  http://www.DellTechCenter.com/OME
- OpenManage Mobile 개요
  http://www.DellTechCenter.com/OMM
- Lifecycle Controller 부품 교체
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- 마더보드 교체
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC 자동 인증서 등록
  https://www.dellemc.com/resources/en-us/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- SELinux를 사용한 iDRAC9의 서버 보안 기능 강화
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 Cipher Select - Dell EMC PowerEdge 서버의 보안 강화
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

PowerEdge 서버에 대해 자세히 알아보기

PowerEdge 서버에 대한 자세한 정보

시스템 관리 솔루션에 대한 자세한 정보

리소스 라이브러리 검색

Twitter에서 PowerEdge 서버 팔로우

Dell Technologies 영업 및 지원 전문가에게 문의

DELL Technologies