보안 강화

3.5배 더 많은 보안 기능

iDRAC9을 통한 2단계 인증 및 외부 키 관리 포함

에너지 효율성 최적화

6배 이상의 소비 전력 보고서

Dell OME의 보고서 20개 vs. Supermicro SSM의 보고서 3개

1시간 50분의 관리 시간을 절약하여 운영 효율성 향상

서버 100대당

Dell iDRAC9에서는 자동 업데이트 사용 vs. Supermicro IPMI에서는 자동 업데이트 사용 불가능

강력한 Dell 서버 관리 툴을 사용하여 보안, 지속 가능성 및 효율성 강화

Supermicro 관리 포트폴리오 대비

데이터 센터의 새로운 서버에 투자할 때는 하드웨어를 선택하는 데 그치는 것이 아니라 관리 용이성 솔루션까지 선택하게 된다. 관리자가 인프라스트럭처를 구축, 모니터링, 유지 관리 및 보호하면서 에너지 효율성을 개선할 수 있는 효율적이고 기능이 풍부한 툴을 사용할 수 있으면 일상적인 관리를 쉽게 처리하고 조직을 발전시키는 혁신에 더 많은 시간을 할애할 수 있다. 강력한 관리 용이성 툴을 갖춘 공급업체에서 구매하면 시간과 비용을 절약할 수 있다.

본 연구에서는 Dell의 세 가지 툴과 Supermicro의 두 가지 툴을 비교하여 Dell™과 Supermicro®의 서버 관리 포트폴리오를 평가했다.

표 1: 테스트한 관리 툴. *Dell CloudIQ는 클라우드 기반 모니터링 및 분석 툴이다. Supermicro는 이에 상응하는 툴을 제공하지 않는다.
출처: Principled Technologies.

	Dell Technologies	Supermicro
내장형/원격 서버 관리	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
일대다 디바이스 관리 콘솔	Dell OME (OpenManage™ Enterprise) Dell CloudIQ*	SSM (Supermicro Server Manager)

지속 가능성, 보안 및 일상적인 관리 경험 측면에서 Dell은 지속적으로 관리자가 더 많은 옵션과 기능을 활용할 수 있도록 지원하는 기능이 더 풍부한 툴 세트를 제공하는 것으로 확인되었다.

서버 관리를 자동화하고 용이하게 하는 더 다양하고 풍부한 기능

IT 팀은 일상적인 업무에 소요되는 시간을 절약하고 보안 및 효율성 표준을 준수할 수 있는 기능이 풍부한 최신 관리 툴이 필요하다. 평가한 Dell 관리 툴에는 Supermicro 관리 포트폴리오에는 없는 다양한 기능이 포함되어 있다.

지속 가능성

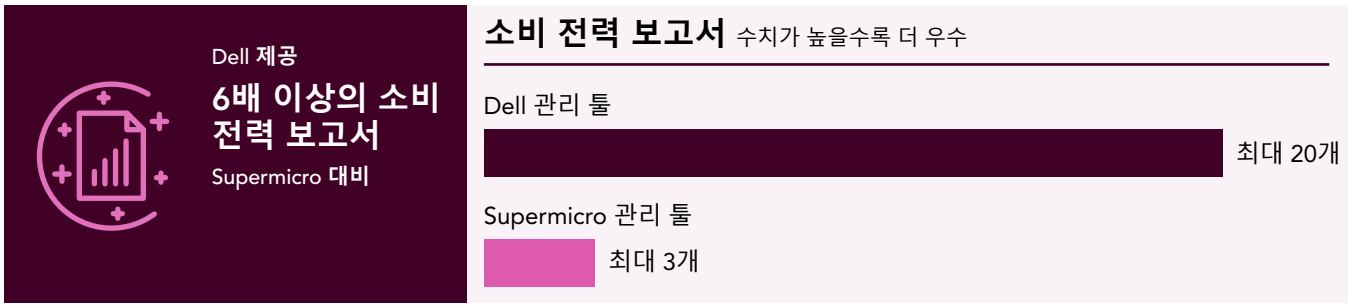
에너지 비용이 상승하고 환경 규제가 증가함에 따라 많은 조직이 지속 가능성에 중점을 두고 있다. 데이터 센터에는 본질적으로 많은 양의 전력이 필요하지만, 열과 소비 전력을 신중하게 관리하면 조직이 소비하는 전력량을 줄일 수 있다. Dell OpenManage Enterprise에는 소비 전력을 면밀히 모니터링하고 관리할 수 있는 여러 기능이 통합되어 있어 지속 가능성 목표 달성에 도움이 될 수 있다. 표 2와 3에 이러한 기능의 주요 이점이 요약되어 있으며, 이에 대해서는 아래에서 자세히 설명한다.

2: Dell OpenManage Enterprise와 SSM 간의 지속 가능성 차이. 출처: Principled Technologies.

기능	Dell 관리 툴	Supermicro 관리 툴
탄소 배출 사용량 계산기 및 용량 계획 툴	✓	x
탄소 발자국 분석	✓	x
온도 트리거 전원 관리 정책	✓	x
정적 전원 관리 정책	✓	✓

3: Dell OME와 Supermicro SSM 및 IPMI 간 비교 요약. 출처: Principled Technologies.

기능	Dell 관리 툴의 주요 이점	Supermicro 관리 툴의 단점
탄소 배출 사용량 계산기 및 용량 계획 툴	지속 가능성 목표를 달성할 수 있도록 **온실가스 배출량**을 맞춤 구성 가능한 값으로 추산할 수 있다.	**유사한 기능 없음**. 지속 가능성 목표를 달성하는 데 도움이 되는 계획을 수립하기 어렵다.
탄소 발자국 분석	OpenManage Enterprise Power Manager를 통해 **사용할 수 있으며**, 지속 가능성 목표 달성에 도움이 될 수 있는 탄소 배출량에 대한 데이터를 제공한다.	**유사한 기능 없음**: 지속 가능성 목표 달성 모니터링에 도움이 되는 탄소 발자국을 추적할 방법이 없다.
자동 전원 및 방열 관리	서버가 소비 전력 또는 온도 임계값을 초과할 때 트리거하는 옵션이 있는 **정적 및 온도 트리거 정책** 옵션	연결된 트리거 옵션이 없는 **하나의 정적 정책 유형**
소비 전력 보고서	이메일 예약 배포 및 맞춤 구성 옵션이 있는 **20개의 기본 제공** 보고서가 포함된 **6배 이상의** 보고서	SSM에는 **2개의 기본 제공 보고서**가 있고, Supermicro IPMI에는 내보낼 수 없는 1개의 보고서가 있다.
전원 관리 메트릭	최대 **15배 더 많은 메트릭**을 제공하여 소비 전력 관리에 대한 더욱 세분화된 통찰력을 제공한다.	**1개만** 제공하므로 소비 전력에 대한 통찰력과 제어 수준이 낮다.



1: Dell OME와 Supermicro SSM에서 사용할 수 있는 소비 전력 보고서 수. 출처: Principled Technologies.

2: Dell OME와 Supermicro SSM에서 사용할 수 있는 전원 관리 메트릭 수. 출처: Principled Technologies.

자동 전원 및 방열 관리

OpenManage Enterprise Power Manager는 정적 전원 및 온도 트리거 정책 옵션을 통해 자동 전원 및 방열 관리를 제공함으로써 관리자가 소비 전력 또는 온도 임계값에 대한 제한을 설정하여 냉각 비용을 절감할 수 있도록 한다. 반면, SSM은 소비 전력에 대한 정적 한도인 단일 정책을 사용하는데, 이는 서버가 한도를 초과해도 자동으로 트리거되지 않아 에너지 비용이 상승할 수 있다.

최적화를 위해 데이터 센터의 소비 전력을 심층적으로 분석하려는 조직은 OpenManage Enterprise Power Manager가 제공하는 **20가지 기본 제공 소비 전력 보고서**의 이점을 누릴 수 있다. 이러한 보고서는 효율성 극대화를 위한 용량 계획 및 전력 관리에 유용하다. SSM의 보고 옵션은 훨씬 더 제한적이다. 관리자는 서비스 보고서가 있는 단일 호스트만 실행하거나 모니터링 화면에서 소비 전력 추세를 확인할 수 있다. Supermicro IPMI를 사용하면 BMC에서 구성 요소 수준 전력 그래프를 볼 수 있지만 그래프의 데이터를 분석용으로 내보낼 수는 없고 이미지로만 저장할 수 있다.

OpenManage Enterprise Power Manager 플러그인을 사용하면 관리자가 개별 구성 요소별 전력 사용량, 공기 흐름 및 구성 요소 활용도를 포함한 **최대 15가지 메트릭을 볼 수 있는** 반면, SSM은 총 전력 사용량만 제공한다.

탄소 배출량 및 탄소 발자국 분석

OME에는 특히 온실가스 배출량을 추산하는 데 도움이 될 수 있는 탄소 배출 사용량 계산기와 용량 계획 툴이 포함되어 있다. 에너지 소비 단위의 전력 비용 및 탄소 배출량에 대한 기본값을 제공하지만, 해당 지역의 전력 비용과 데이터 센터의 소비 모델에 맞게 이러한 값을 맞춤 구성할 수 있다. SSM은 유사한 기능을 제공하지 않으므로 조직이 지속 가능성 목표를 향한 진행 상황을 계획하고 모니터링하기가 어려울 수 있다.

보안

사이버 범죄가 기하급수적으로 증가하면서 기업을 "데이터 손상 및 파괴, 금전 도난, 생산성 손실, 지적 재산 도난, 개인 및 금융 데이터 도난, 횡령, 사기, 공격 후 정상적인 비즈니스 운영 중단, 포렌식 조사, 해킹된 데이터 및 시스템의 복원 및 삭제, 평판 훼손"으로 위협하고 있다.[1] 이러한 환경에서 의사 결정권자는 모든 서버 구매 시 보안을 고려해야 한다. Dell OpenManage Enterprise에는 Supermicro 툴에는 없는, 데이터를 안전하게 보호하는 데 도움이 되는 여러 기능이 통합되어 있는 것으로 확인되었다(표 4 및 5 참조).

4: Dell 관리 툴과 Supermicro 관리 툴 간의 보안 차이점. 출처: Principled Technologies.

기능	Dell 관리 툴	Supermicro 관리 툴
다단계 인증	✓	x
외부 키 관리	✓	x
범위 기반 액세스 제어	✓	x
정책 기반 보안 구성	✓	x
사이버 보안 권고	✓	x
역할 기반 액세스 제어	✓	✓
동적 USB 포트 비활성화	✓	✓

5: Dell 관리 툴과 Supermicro 관리 툴 간의 보안 기능 비교 요약. 출처: Principled Technologies.

기능	Dell 관리 툴의 주요 이점	Supermicro 관리 툴의 단점
MFA(Multi-factor authentication)	**이메일 또는 RSA SecurID**를 통한 iDRAC의 **2단계 인증**으로 권한이 없는 사용자가 기밀 데이터에 액세스하는 것을 방지한다.	**유사한 기능이 없어** 권한이 없는 사용자가 기밀 데이터에 액세스할 수 있는 보안 격차가 발생한다.
외부 키 관리	iDRAC의 **Secure Enterprise Key Manager**를 통해 보안 계층을 한 단계 더 강화하여 드라이브 암호화 및 중앙 집중식 관리로 서버의 저장 상태 데이터를 보호한다.	**유사한 기능이 없어** 또 다른 보안 격차가 발생한다.
액세스 제어	OME는 **RBAC**(Role-Based Access Control)와 **SBAC**(Scope-Based Access Control)를 **모두** 제공하여 디바이스 관리자가 액세스할 수 있는 디바이스 그룹을 제한한다.	**RBAC만** 제공하여 관리자가 액세스를 제한하는 기능을 제한한다.
정책 기반 보안 구성	CloudIQ를 통한 **정책 기반 보안 구성** 설정으로 관리자에게 불일치를 알린다.	**유사한 기능이 없어** 위반 조치 및 문제 해결에 지연이 발생할 수 있다.
사이버 보안 권고	취약성 세부 정보와 적용 가능한 문제 해결 제안 사항이 포함된 Dell CloudIQ 보안을 통한 **보안 권고 보고**로 신속한 조치를 취할 수 있다.	**유사한 기능이 없어** 악의적인 행위자가 악용할 수 있는 보안 격차가 발생한다.

다단계 인증

MFA(Multi-Factor Authentication)는 권한이 없는 사용자와 악의적인 행위자가 기밀 데이터에 액세스하는 것을 방지하는 데 도움이 될 수 있다. Dell iDRAC은 여러 업계에서 사용되는 외부 다단계 인증 기술 세트인 RSA SecurID와 이메일을 통한 2단계 인증을 지원한다는 것으로 확인되었다.[2] 또한 Supermicro IPMI와 SSM은 모두 이 기능을 제공하지 않아 보안 격차가 발생한다는 사실도 확인되었다.

키 관리

외부 KMS(Key Management System)를 사용하면 IT 팀이 별도의 타사 서버를 사용하여 서버의 스토리지를 잠그고 잠금 해제하는 데 사용하는 키를 관리함으로써 보안 계층을 추가할 수 있다. iDRAC에는 모든 새로운 Dell PowerEdge 서버에 대한 LKM(Local Key Manager)이 포함되어 있다. 일부 라이선스는 전체 디스크 암호화 및 외부 키 관리를 통해 추가적인 보안을 지원하는 SEKM(Secure Enterprise Key Manager)도 제공한다. SEKM은 업계 표준 OASIS KMIP 프로토콜을 지원하여 조직이 해당 표준을 사용하는 외부 KMS 공급업체를 선택할 수 있도록 한다. Supermicro는 이 보안 기능이나 이와 동등한 기능을 제공하지 않는다.

액세스 제어

RBAC(Role-Based Access Control)는 사용자의 역할에 따라 액세스할 수 있는 시스템 부분과 해당 부분에서 수행할 수 있는 작업을 결정하며, 많은 서버 보안 전략의 필수 구성 요소이다. OpenManage Enterprise에서 RBAC는 관리자, 장치 관리자 및 뷰어의 세 가지 기본 제공 역할에 대한 사용자 권한을 정의한다.[3] 또한 SBAC(Scope-Based Access Control)를 제공하여 디바이스 관리자가 액세스할 수 있는 디바이스 그룹을 관리자가 제한할 수 있도록 한다.[4] 이를 통해 관리자는 디바이스 하위 세트에 대한 액세스 권한을 제공할 수 있다. Supermicro는 RBAC를 제공하지만 SBAC는 제공하지 않는다.

자격 증명 관리

iDRAC 비밀번호 순환은 여러 가지 용도로 사용된다. 보안 정책에 따른 OpenManage Enterprise에 대한 액세스를 월별 기본값을 사용하여 순환하고, 외부 비밀번호 처리기와 함께 작동하며, 비밀번호를 관리하기 위해 CyberArk를 지원한다.[5,6]

OpenManage Enterprise를 통해 관리자는 알려진 정적 관리자 계정을 OME에서 관리하는 서비스 계정으로 대체하여 iDRAC 비밀번호 순환을 관리할 수 있다. SSM에는 이 기능이 없다.

정책 기반 보안 구성

Dell은 PowerEdge AIOps용 CloudIQ 솔루션에서 정책 기반 사이버 보안 기능을 제공한다. 이 기능은 구축된 PowerEdge 서버의 구성을 가져와 Dell 모범 사례에 따른 보안 관련 구성 정책과 비교한다. CloudIQ가 불일치를 감지하면 관리자에게 알리고 문제 해결 단계를 제공한다.[7] SSM은 동등한 기능을 제공하지 않으므로 위반 탐지가 지연될 수 있다.

사이버 보안 권고

보안 권고는 보안 문제를 공지한다. Dell에 따르면, CloudIQ의 Dell Security Advisor 페이지에서는 적용 가능한 보안 권고의 전체 목록과 해당 권고의 영향, 영향을 받는 시스템 수, 게시 날짜를 제공한다.[8] Dell CloudIQ는 취약성 세부 정보 및 문제 해결 제안 사항이 포함된 보안 권고 보고를 제공한다. SSM은 유사한 기능을 제공하지 않아 시스템이 취약해질 수 있다.

Dell CloudIQ 소개

Dell CloudIQ는 서버, 스토리지, 데이터 보호 어플라이언스 및 하이퍼컨버지드 인프라스트럭처를 비롯한 수많은 Dell 제품 및 서비스에 대해 "사전 예방적 모니터링, 머신 러닝 및 예측 분석"을 제공하는 클라우드 기반 AIOps 툴이다.[9] 2022년 Principled Technologies 연구에 따르면, CloudIQ가 네트워크 대역폭에 미치는 영향은 미미하지만, 이를 통해 단일 콘솔에서 텔레메트리, 상태, 알림 및 인벤토리를 모니터링할 수 있는 것으로 나타났다.[10]

CloudIQ에 대한 자세한 내용은 https://www.dell.com/en-us/dt/solutions/cloudiq.htm 에서 확인할 수 있다.

동적 USB 포트 비활성화

USB 포트를 비활성화하거나 활성화하면 관리자가 USB 포트를 통해 서버에 대한 액세스를 제어할 수 있으므로 악의적인 사용과 금지된 애플리케이션 설치 또는 바이러스의 위험을 방지할 수 있다.

Dell iDRAC은 다운타임 없이 독립적인 동적 USB 포트 비활성화를 제공한다. Supermicro는 BIOS 내에서 동적 전면 USB(및 후면 USB) 비활성화를 제공하지만, 이를 활성화하려면 노드 라이선스 키별 Supermicro DataCenter Management Suite가 필요하다. IT 부서에서 시스템 잠금 명령을 구현하여 이를 트리거할 수 있는데, 이 명령은 BMC 또는 Supermicro IPMI 콘솔에서 실행할 수 있지만 시스템 잠금 모드와 독립적이지 않다.[11]

그림 3에서 볼 수 있듯이, Dell iDRAC을 사용하여 포트를 비활성화하는 작업은 **41초, 4단계만 소요되는** 간단한 프로세스인 반면, Supermicro IPMI에서는 **그보다 4배 이상인 2분 50초, 6단계**가 소요되었다. 이러한 시간 절감 효과를 100대의 시스템에 적용하면 시간 절감 효과는 3시간 35분으로 늘어난다. 즉, 관리자가 Supermicro IPMI를 사용하면 하루 업무 시간의 거의 절반이 소요되는데, Dell iDRAC을 사용하면 1시간이 조금 넘게 소요되는 것이다.

그림 3: 단일 서버의 전면 USB 포트 비활성화 소요 시간과 서버 100대의 전면 USB 포트 비활성화 추정 소요 시간. 낮을수록 더 우수. 출처: Principled Technologies.

Dell OpenManage Enterprise 소개

OpenManage Enterprise는 데이터 센터를 위한 일대다 시스템 관리 콘솔입니다. 이 콘솔은 최신 HTML5 그래픽 사용자 인터페이스를 제공하며 VMware ESXi™, Microsoft Hyper-V 및 KVM(Kernel-based Virtual Machine) 환경을 위한 Virtual Appliance로 구축된다. OpenManage Enterprise는 Dell 랙 서버, Dell 타워 서버, Dell 블레이드 및 섀시를 포함하여 최대 8,000대의 디바이스에 대한 IPv4 및 IPv6 네트워크를 검색하고 인벤토리를 생성할 수 있다.[12] 최근 PT 연구에 따르면 OpenManage Enterprise와 OME-M(OpenManage Enterprise Modular)을 사용하는 Dell 환경에서는 VLAN 변경 소요 시간이 절약될 수 있고 예약된 펌웨어 업데이트 중에 개입이 방지될 수 있는 것으로 확인되었다.[13]

OpenManage Enterprise에 대한 자세한 내용은 https://www.dell.com/en-us/lp/dt/open-manage-enterprise 에서 확인할 수 있다.

모니터링, 분석 및 사용 편의성

관리 용이성 툴은 관리자가 모니터링 및 분석 작업은 물론 업데이트 예약과 같은 기타 일상적인 작업을 수행하도록 지원하는 방식이 매우 다양하다. 이 섹션에서는 연구한 Dell 관리 툴과 Supermicro 관리 툴 간 이러한 영역에서의 차이를 살펴본다. 지속 가능성 및 보안 기능을 조사했을 때 알게 된 것처럼, Dell 관리 툴 제품군은 관리자의 업무를 더욱 편리하게 만들어 주는 수많은 기능을 제공하는데 Supermicro 도구에는 이러한 기능이 없다. 표 6에는 툴이 제공해야 하는 관리 이점이 비교되어 있다.

6: Dell 관리 툴과 Supermicro 관리 툴 간의 비교 요약. 출처: Principled Technologies.

기능	Dell 관리 툴의 주요 이점	Supermicro 관리 툴의 단점
텔레메트리 스트리밍	iDRAC9 **텔레메트리 스트리밍**은 원격 syslog 서버에서 **사용 가능**하며, 장애 예측 및 성능 최적화에 도움이 된다. Grafana 및 Splunk와 같은 분석 툴에 서버 메트릭을 스트리밍할 수 있다.	**자동 텔레메트리 스트리밍 없음**
모바일 모니터링 및 관리	기능이 풍부한 iOS 및 Android 용 OpenManage Mobile 앱으로, OME 및 iDRAC9과 통합된다.	SSM과 **통합되지 않는** Supermicro IPMIView 앱
타사 디바이스 및 서버 모니터링	OME는 주요 경쟁업체에 대한 지원을 포함하여 **타사 디바이스 및 서버 모니터링을 지원**한다.	해당 에이전트, 해당 BMC, IPMI 지원 장비의 이전 버전 및 Redfish 지원 디바이스를 **사용하는 타사 디바이스만 지원**한다.
자산 모니터링	OME 및 CloudIQ를 통해 사용 가능. OME는 라이선스가 부여된 관리 서버의 데이터를 CloudIQ로 전송하여 여러 데이터 센터 전반을 모니터링할 수 있다.	데이터 센터 전반에 걸쳐 모니터링 데이터를 집계할 수 있는 **클라우드 기반 포털이 없다**.
알림 기반 작업	알림의 입력을 기반으로 작업을 트리거하는 OME의 정책	**사용 가능한 알림 기반 작업 없음**
더 간편한 서버 구축(시스템 구성 가져오기/ 내보내기 기능)	iDRAC9을 사용하여 서버의 모든 구성 항목을 **가져올/내보낼** 수 있으며, **가져오기에 단 48초와 5 단계, 내보내기에 단 1분 9초와 7단계가 소요된다.**	**BMC(Baseboard Management Controller) 구성만** 가져올/ 내보낼 수 있으며, 각 서버에 대해 상당한 수동 구성이 필요하다.
BIOS 구성 설정 변경 시간 단축	**iDRAC에서 직접 전체 BIOS 설정을** 빠르게 변경하고 유지 보수 기간 동안 업데이트 및 재부팅을 스테이징할 수 있으므로 관리 시간이 크게 절약된다.	BMC에서 **사용 가능한 BIOS 변경 사항이 제한되어 있으며**, 그렇지 않으면 서버를 재부팅해야 한다. 수동 단계와 관리 시간이 더 많이 소요된다.
Virtual Appliance로 실행	OME에서 **사용 가능**하므로 OS 를 업데이트할 필요가 없다.	**유사한 기능이 없어** 관리되는 OS 내에서 실행되어야 한다. 이로 인해 관리자는 구성 요소를 하나 더 패치 및 업데이트해야 한다.
Connection View	iDRAC에서 **사용 가능**하며, LLDP 를 사용하여 케이블 연결, 불량 스위치 포트 등과 같은 네트워킹 문제를 진단하는 문제 해결 툴	**Connection View가 없으며** 업스트림 스위치 포트에 대한 물리적 연결 정보 없음
펌웨어 및 드라이버 업데이트 예약 기능	OME 및 iDRAC에서 **사용 가능**	BIOS 및 BMC 펌웨어 업데이트를 예약할 수 있지만 **드라이버 업데이트는 예약할 수 없음**

BIOS 구성 항목 변경

Dell은 iDRAC에서 직접 전체 BIOS 구성 설정을 변경할 수 있는 기능을 제공하며, 다음 재부팅 시 해당 변경 사항을 스테이징할 수 있는 기능을 제공한다. Supermicro는 BMC에서 제한된 BIOS 설정 세트를 제공한다. 제한된 세트 외에도 단일 구성 항목에 대한 Supermicro 서버의 BIOS 구성을 변경하려면 관리자가 서버를 재부팅하여 부팅 화면에서 BIOS 구성 메뉴에 액세스해야 한다.

그림 4에서는 Dell iDRAC과 Supermicro IPMI를 사용하여 단일 서버에서 BIOS 구성 변경을 수행하는 시간을 보여준다. **Supermicro 툴을 사용하는 수동 프로세스는** iDRAC에서 자동 프로세스를 설정하는 것보다 **2분 6초 또는 4.9배의 시간이 더 걸린다**. 이러한 시간을 동일하게 구성된 서버 100대에 대입하면 iDRAC의 시간 절감 효과는 3.5 시간으로 추정된다. (서버가 동일하게 구성되지 않았다면 이러한 시간 절약 효과가 보이지는 않았을 것이다.)

그림 4: 단일 서버와 동일하게 구성된 서버 100대 모두에서 BIOS 구성 변경을 수행하는 데 걸리는 시간(추정치). 낮을수록 더 우수. 출처: Principled Technologies.

iDRAC9 정보

Dell PowerEdge™ 서버에는 시스템 알림 및 원격 관리 기능을 포함한 시스템 관리 기능을 제공하는 Dell Lifecycle Controller가 탑재된 Integrated Dell Remote Access Controller 9이 포함되어 있다. Dell Technologies에 따르면 iDRAC9의 주요 이점은 다음과 같다.

- API 및 스크립팅 툴을 사용하여 수천 대의 서버를 관리할 수 있는 기능
- 서버 상태 및 수천 개의 매개변수 상태 모니터링에 대한 보기를 제공하는 내장 지원
- 강력한 보안 기능 및 옵션[14]

iDRAC9이 제공하는 기능에 대한 자세한 내용은 https://www.dell.com/en-us/lp/dt/open-manage-idrac에서 확인할 수 있다.

자동화된 펌웨어 및 드라이버 업데이트

iDRAC

Supermicro IPMI와 달리 Dell iDRAC에서는 자동 펌웨어 업데이트를 예약할 수 있다. 즉, 일정에 따른 자동 업데이트 구성이 일회성 작업이므로 업데이트 주기마다 시간이 절약된다. 그림 5에서는 Dell iDRAC과 Supermicro IPMI를 사용하여 서버 100대에 대해 처음으로 자동 펌웨어 업데이트를 예약하는 데 걸리는 추정 시간을 보여준다. Supermicro 툴을 사용하는 수동 프로세스는 iDRAC에서 자동 프로세스를 설정하는 것보다 **13분이 더** 소요된다.

관리자가 매월 첫 번째 토요일 밤에 월별 일정을 설정한다고 가정하면 iDRAC을 사용하는 관리자는 서버당 58초의 일회성 시간을 투자하게 된다. 서버 100대를 대상으로 한 경우에는 일회성 설정으로 1시간 36분 40초가 소요된다. 이에 비해 Supermicro IPMI를 사용하는 관리자는 각 유지 보수 기간에 서버 100대에 대해 1시간 50분을 투자하게 된다. iDRAC의 일회성 설정과 Supermicro IPMI의 첫 번째 설정 시간을 비교해보면 Dell 관리 툴로 약 13분 20초가 절약된다. (그림 5 참조.)

그러나 두 번째부터는 **Dell이 110분을 절약하게 된다. 매번 관리자가 작업을 수행할 필요가 없기 때문이다**. (그림 6 참조.) 이러한 시간 절약은 서버 100대가 동일하게 구성되지 않은 경우에도 발생한다. 이 시간에는 BMC에 펌웨어를 업로드하는 데 걸리는 시간만 포함되며 Supermicro 펌웨어의 다운로드 및 압축 풀기 시간은 반영되지 않는다.

OME

Dell OME는 **모든 구성 요소에 대한 펌웨어 업데이트**와 Windows 드라이버 업데이트를 지원한다. SSM은 BIOS 및 BMC 펌웨어 업데이트를 지원하지만 **드라이버 업데이트 또는 기타 구성 요소 업데이트는 지원하지 않는다**.

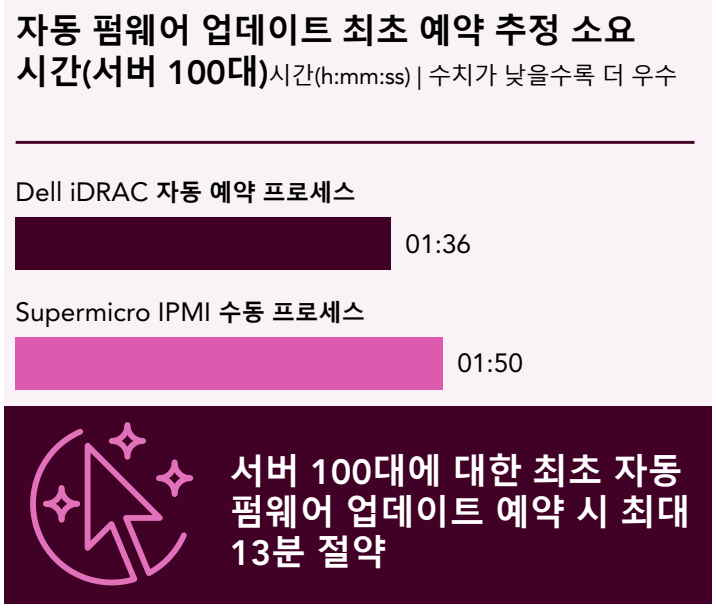
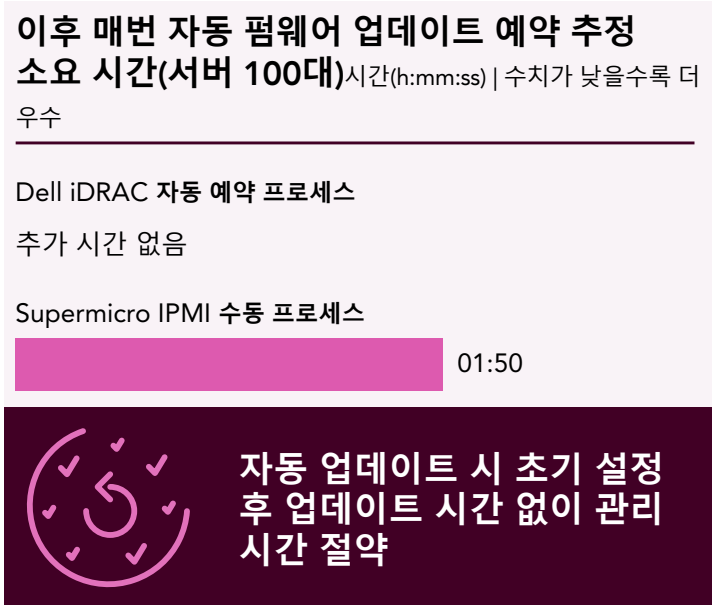


그림 5: 서버 100대의 펌웨어를 처음으로 업데이트할 때 걸리는 시간의 추정치. 낮을수록 더 우수. 출처: Principled Technologies.



6: 100개 서버의 펌웨어를 업데이트할 때마다 걸리는 시간의 추정치입니다. 낮을수록 더 우수. 출처: Principled Technologies.

결론

서버 구매를 위한 공급업체를 선택하는 것은 단지 하드웨어 플랫폼만 고려하는 것이 아니다. 의사 결정권자는 시스템/데이터 보안, 에너지 효율성 및 관리 용이성을 비롯한 더 장기적인 우려 사항도 고려해야 한다. 이러한 우려 사항으로 인해 공급업체가 제공하는 시스템 관리 툴이 하드웨어만큼 중요해진다.

본 연구에서는 Dell과 Supermicro의 서버 관리 툴이 가진 특징과 기능을 조사했는데, 내장형 서버 관리 측면에서 Dell iDRAC9과 Supermicro IPMI를 비교했고 일대다 디바이스 및 콘솔 관리와 모니터링 측면에서 Dell OpenManage Enterprise 및 CloudIQ와 Supermicro Server Manager를 비교했다. 그 결과, Dell 관리 툴이 Supermicro 서버보다 더 포괄적인 보안, 지속 가능성 및 관리/모니터링 기능을 제공하는 것으로 확인되었다. 또한 Dell 툴은 서버 관리가 용이하도록 더 많은 작업을 자동화하므로, 관리자가 Supermicro 툴을 사용하면 동일한 작업을 수동으로 수행해야 하는 데 비해 상당한 시간을 절약할 수 있다.

서버를 구매할 때 공급업체의 관련 관리 제품은 데이터를 보호하고, 더욱 지속 가능한 환경을 지원하며, 시스템 유지 보수를 용이하게 하는 데 매우 중요하다. 테스트와 연구에 따르면, PowerEdge 서버용 Dell 관리 포트폴리오는 조직의 목표 달성에 도움이 되는 기능을 유사한 Supermicro 관리 제품보다 더 많이 제공하는 것으로 나타났다.

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025"(2024년 2월 15일 액세스), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, "Using iDRAC9 RSA SecurID 2FA"(2024년 2월 15일 액세스), https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide"(2024년 2월 15일 액세스), https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?.
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide."
5. Dell, "OpenManage Enterprise 4.0: iDRAC 암호 관리 및 순환"(2024년 2월 15일 액세스), https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation.
6. Dell, "OpenManage Portfolio Software Licensing Guide"(2024년 4월 3일 액세스), https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean과 Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation"(2024년 2월 15일 액세스), https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, "Security Advisories"(2024년 2월 15일 액세스), https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights"(2024년 2월 15일 액세스), https://www.dell.com/en-us/dt/solutions/cloudiq.htm
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests"(2024년 1월 17일 액세스), https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, "X13DEM User's Manual"(2024년 2월 16일 액세스), https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, "OpenManage Enterprise"(2023년 12월 20일 액세스), https://www.dell.com/en-us/work/learn/openmanage-enterprise.
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators"(2024년 1월 17일 액세스) https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf
14. "iDRAC(Integrated Dell Remote Access Controller)"(2024년 1월 16일 액세스), https://www.dell.com/en-us/lp/dt/open-manage-idrac.

이 보고서에 숨겨진 과학 확인 ▶

Principled Technologies®

Facts matter.®

Principled Technologies는 Principled Technologies, Inc.의 등록 상표입니다.
다른 모든 제품 이름은 해당 소유주의 상표입니다.
자세한 내용은 '이 보고서에 숨겨진 과학'을 참조하십시오.

이 프로젝트는 Dell Technologies의 의뢰로 진행되었습니다.