백서

IBM LinuxONE: 보안 데이터 서비스 및 하이브리드 클라우드 인프라

후원: IBM

Peter Rutten Ashish Nadkarni

2019년 9월

IDC 제언

디지털 트랜스포메이션(DX) 같은 기술 구현 비즈니스 전략 덕분에 기업들은 시장에서 경쟁 우위를 확대해 나갈 수 있습니다. 파격적인 DX는 기업들이 (기술) 플랫폼, (비즈니스) 프로세스, (데이터) 거버넌스 및 (개인) 인재를 효과적이고 효율적으로 결합하여 데이터에서 심층적이고 시기적절한 통찰력을 수집하고, 이러한 통찰력을 바탕으로 비즈니스 운영 방식을 최적화하며, 혁신(새롭고 혁신적인 제품과 서비스 개발)을 가속화하고, 고객 참여를 변혁하도록 요구합니다.

대규모의 다양한 데이터에서 심층적이고 시기 적절하며 조치 가능한 통찰력을 얻기 위해서는 기업들이 기술 플랫폼에 대한 혁신적인 접근 방식을 취해야 합니다. 권장되는 접근 방식은 최신 인프라 플랫폼에 현재 및 차세대 애플리케이션(앱)을 배포하는 방식입니다. 현 세대의 앱 대부분은 기성품으로 조달되고, 인프라에 대한 기존 접근 방식을 필요로 하며 수립된 수익 창출 비즈니스 운영 기법을 지원합니다. 차세대 앱은 특히 미래 지향적인 DX 이니셔티브를 위해 개발되고, 클라우드 네이티브로 설계될 뿐만 아니라 보다 새로운 개발 방법을 활용하면서 컨테이너 같은 최신의 컴퓨팅 기술을 기반으로 구현되곤 합니다. 즉, 현재는 물론 차세대 앱을 호스팅할 수 있는 최신 인프라 솔루션은 최상의 성능과 확장성을 지원해야 하고, 데이터 통합 및 서비스를 위해 최적화되어야할 뿐만 아니라 포괄적인 보안 기능을 지원하고, 민첩하고 신뢰할 수 있으며, 컴퓨팅, 개발, 배포 모델에 있어서 전통적인 것부터 차세대까지 모두 지원하고, 기본적으로 최신 오픈 소스 프레임워크를 지원할 수 있어야 합니다.

IBM의 LinuxONE은 보안 데이터 서비스 인프라 플랫폼으로 현재는물론 차세대 앱의 요구 사항을 충족하도록 설계되었습니다. IBM LinuxONE은 다음과 같은 역량이 요구되는 기업에 이상적입니다.

- 탁월한 보안 유지: 자신들의 요구 사항 목록 상단에 데이터 프라이버시와 규제 우려 사항을 두고 있는 기업들을 위해 LinuxONE 은 EAL5+ 격리, 암호화 키 보호 및 SSC(Secure Service Container) 프레임워크와 같은 동급 최고의 보안 기능을 내장하고 있습니다.
- 타협 없는 데이터 서비스 기능: LinuxONE은 정형 및 비정형 데이터 통합을 위해 설계되었으며 최신 관계형 및 비관계형 데이터베이스를 실행하도록 최적화되었습니다. 기업들은 "통합된 단일의 데이터 소스"로부터 심층적이고 시기적절한 통찰력을 얻을 수 있습니다.
- 특유의 균형잡힌 시스템 아키텍처: 고유한 공유 메모리 및 수직 스케일 아키텍처 덕분에 LinuxONE의 성능 유지(nondegrading performance) 및 확장 기능은 데이터베이스 및 기록 시스템과 같은 워크로드 그리고 블록체인과 같은 안전한 트랜잭션 앱에 적합합니다.

LinuxONE은 DX 이니셔티브에 중요한 현재 및 차세대 앱과 워크로드를 실행하기 위해 고성능 그리고 탁월한 확장성, 매우 안전한 데이터 서비스 및 통합 인프라 플랫폼이 필요한 하이브리드 클라우드 및 클라우드 서비스 제공 업체뿐만 아니라 일반 기업에게도 적합합니다.

상황 개요

기업들은 현재와 미래의 시장에서 경쟁력 차별화를 확대하기 위해 디지털 트랜스포메이션 이니셔티브를 시작합니다. DX는 기술 기반 비즈니스 전략이지만 기업들이 "평소와 같이 비즈니스를 계속 운영하면서 정기적으로 자신을 재창조"(즉, 현재 방식을 유지하면서 동시에 새로운 수익원과 차별화를 찾는 것)해야 하므로 종종 매우 파격적입니다. DX는 가능한 한 많은 데이터를 기업에 제공할 뿐만 아니라 (기술) 플랫폼, (비즈니스) 프로세스, (데이터) 거버넌스 및 (개인) 인재를 효과적이고 효율적으로 결합하여 이 데이터에서 심도 있고 시기 적절한 통찰력을 수집할 수 있습니다. 또한 이러한 통찰력을 발휘하여 비즈니스 운영 기법을 최적화하고, 새롭고 혁신적인 제품 및 서비스를 개발하며, 고객 참여를 변화시킬 수 있습니다. 대부분의 기업에게 있어, DX는 시기의 차이일 뿐 누구나 준비해야하는 것으로 더 이상 큰 대기업만의 이니셔티브가 아닙니다. 그것은 금융 및 보험 서비스, 제조, 소매 및 헬스케어와 같은 산업의 비즈니스에 동등하게 적용됩니다. 데이터 중심 전략의 부재는 제품이나 서비스를 제공하는 대기업이나 중소기업에 실질적인 위협이 됩니다.

디지털 혁신을 위한 인프라

대규모의 다양한 데이터에서 심층적이고 시기 적절하며 조치 가능한 통찰력을 얻기 위해서는 기업들이 애플리케이션과 인프라로 구성된 기술 플랫폼에 대한 혁신적인 접근 방식을 취해야 합니다. 애플리케이션 측면에서:

- 기업의 개혁이란 새롭고 진보한 앱(차세대 앱)을 개발한다는 의미입니다. 차세대 앱은 특히 미래 지향적인 DX 이니셔티브를 위해 개발되고, 클라우드 네이트브로 설계되며, 보다 새로운 개발 방법을 활용하고, 컨테이너 같은 최신의 컴퓨팅 기술을 기반으로 구현되곤 합니다.
- 기존 수익원을 유지 관리한다는 것은 비즈니스 앱(현 세대 애플리케이션)의 유지를 의미합니다. 현 세대의 앱 대부분은 기성품으로 조달되고, 인프라에 대한 기존 접근 방식을 필요로 하며 수립된 수익 창출 비즈니스 운영 기법을 지원합니다.

기업들은 애플리케이션 포트폴리오의 특성과 DX 이니셔티브의 특성 및 목표에 맞는 데이터 관리와 인프라에 대한 현대적이고 공유된 접근 방식에 투자함으로써 이익을 얻습니다. 이러한 인프라는 다음과 같은 기능들을 지원합니다:

- 최상의 성능, 유연성 및 확장 가능성
- 데이터 통합 및 앱 간의 공유
- 엄격한 서비스 수준의 목표
- 데이터 암호화를 넘어선 포괄적인 보안 기능
- 베어 메탈, 가상화 및 컨테이너와 같은 다중 컴퓨팅 모델
- DevOps와 같은 보다 새로운 개발 및 배포 모델
- OpenStack과 같은 오픈 소스 클라우드 프레임워크 그리고 Puppet 및 Chef와 같은 자동화 도구
- 컨테이너 및 컨테이너 오케스트레이션
- 하이브리드 클라우드

암호화 등을 포함하는 인프라 보안

다양한 IDC 설문조사에 따르면 데이터 및 인프라와 관련하여 보안 문제가 경영진의 가장 큰 우려 사항으로 나타나고 있습니다. 최신 인프라의 보안 패러다임은 단순한 데이터 암호화 그 이상입니다. 이 패러다임은 인프라 전반에 걸쳐 매순간 위험을 식별하고 내부 및 외부 위협으로부터 보호하는 데 그 목적이 있습니다. 기업들은 최근 몇 년 동안 발생한 잘 알려진 사고로부터 보안에 대한 총체적 접근 방식을 취하는 것이 외부 위협과 함께 내부 위협을 제어한다는 것을 의미하는데 익숙해졌습니다. 이는 인프라의 일부에 대한 무단 액세스 권한을 가진 사람이 "민감한 데이터를 가지고 빠져나가지" 못하도록 한다는 것을 의미합니다. 기업의 인프라 보안은 복잡한 점검 및 균형 시스템이 되어야 하며 아래와 같은 기능을 포함해야 합니다:

- **다층 보안(Multilayer security)** – 내부 및 외부 사용자, 애플리케이션 또는 네트워크 수준의 액세스를 실시간으로 가로 채거나 허용 및/또는 차단하는 권한 부여 및 인증 체계
- **수평 격리(Horizontal isolation)** – VM(가상 머신), 컨테이너, 서버 인스턴스, 백업 및 스냅샷 내에 있거나 액세스할 수 있는 데이터에 대한 관리 액세스 제한(현재의 관행과 기술 제한으로 인해 관리 권한이 부여될 경우 VM 관리자에게 잠재적으로 매우 중요한 정보에 대한 광범위한 액세스를 제공)
- **수직 격리(Vertical isolation)** – 피어 환경뿐 아니라 피어 환경 이상의 관리자 환경으로부터 데이터 보호
- **액세스 매칭(Access matching)** – "알 필요성"을 데이터의 "민감성 지수" 그리고 이 데이터에 액세스할 수 있는 시스템에 대한 "실제 액세스"와 매칭
- **상시 감사 매커니즘(Always-on auditing mechanisms)** – 패턴을 감지하고 관리자에게 시스템 또는 데이터 침해 사례를 경고함으로써 침해 시도를 신속하게 억제
- **데이터 암호화(Data encryption)** – 사용자, 앱 및 네트워크 인증과 분리된 엄격한 키 관리 체계 및 권한 부여 체계가 함께 하는 데이터 보안
- **데이터 보호(Data protection)** – 데이터가 플랫폼 밖으로 이동했을 때까지도 지원

데이터 중심 접근 방식의 인프라를 위한 수직 확장 기능

IT 산업에는 차세대 애플리케이션 아키텍처에 대한 수평적 확장 접근 방식이 온-프레미스이든 퍼블릭 클라우드이든 현재 애플리케이션이 직면한 모든 성능 및 확장 문제에 대한 가장 포괄적인 솔루션이라는 믿음이 있습니다. 수평 확장은 고유한 이점을 가지고 있지만 비즈니스 주체에 다음과 같은 위험도 안겨주고 있습니다:

- 데이터 일관성 및 리소스 활용: 서버 기반 스토리지를 활용하는 앱과 클라우드에서 실행하는 앱 등을 비롯한 여러 가지 수평 확장 앱은 비동기 복제본 또는 소거 코딩 사본(erasure-coded copies)의 형태로 구현된 최종 데이터 일관성 체계(eventual data consistency scheme)를 활용합니다. 즉, 보안 사고와 같은 일종의 중단 또는 오류로 인해 어떤 시간의 어떤 스냅샷에 대해서 다중의 데이터 소스가 존재할 수 있습니다. 또한 이러한 애플리케이션은 서로 별개인 확장 기능과 성능을 위한 노드를 추가하도록 요구하며 이로써 리소스 활용도가 낮아져 장기적인 측면에서 운영 비용이 추가로 발생합니다.
- 클러스터의 한계: 내장형 또는 외부 클러스터링 소프트웨어를 사용하게 되면 데이터 일관성과 리소스 활용 상황이 추가로 복잡해지기 마련입니다. 네트워크 노드는 자동화된 액티브-패시브 또는 액티브-액티브 운영 모드에서 연결되며 소프트웨어가 정상 조건에서는 시정 조치를 취할 것으로 기대되지만 종종 실패하기도 합니다.

또한 사람에 의해 야기된 실수의 경우 오히려 빠른 조치가 예기치 않은 복잡한 문제를 유발해 상황을 악화시킬 수도 있습니다.

중요한 기록 시스템과 고성능 데이터 서비스 플랫폼의 특정한 애플리케이션 구성 요소를 호스팅하는 시스템에 대해 수직 확장 접근 방식을 취하는 것은 장점이 있습니다. 이러한 시스템을 통해 보다 쉽게 수행할 수 있는 것은 다음과 같습니다:

- 최종 데이터 일관성을 기반으로 설계된 데이터베이스와 애플리케이션을 구현한 경우라도 데이터 일관성 및 보안의 관점에서 통합된 단일의 데이터 소스로 관리
- 더 많은 "코어"를 추가하여 매우 빠른 반응 시간을 제공할 수 있으며, 특정한 외부 프로비저닝 활동 없이 요구 성능을 구현하여 전체 시스템에서 하나의 보안 패러다임을 보다 쉽게 구현
- 모든 가상 머신에서 리소스를 공유할 수 있는 역량을 통해 시스템을 보다 효과적으로 활용

IBM LINUXONE

IBM은 고유한 밸런스드 멀티테넌트 시스템 아키텍처와 데이터 서비스 및 미션 크리티컬 워크로드 그리고 애플리케이션에 맞게 최적화된 업계 최고의 퍼베이시브 보안 기능을 갖춘 엔터프라이즈급 플랫폼 솔루션을 원하는 조직을 위해 LinuxONE 브랜드의 Linux 전용 기술을 도입했습니다. 따라서 LinuxONE은 다음과 같은 조직에 매우 적합합니다:

- 데이터 프라이버시 및 규제 요구 사항 때문에 또는 퍼블릭 클라우드 서비스 제공업체 역량의 한계 때문에 온-프레미스로 비즈니스 애플리케이션을 운영하여 엄격한 가용성, 성능 및 확장 가능성 확보를 목표로 선택한 기업
- 애플리케이션을 호스팅하기 위해 안전한 멀티테넌트 플랫폼이 필요하고 우수한 품질의 서비스를 제공함으로써 대규모 퍼블릭 클라우드 서비스 제공업체(SP)와 자신들을 차별화하기 원하는 관리형 SP 및 클라우드 SP
- 하이브리드 클라우드를 구축하고 하이브리드 클라우드에서 실행하기 위해 클라우드 네이티브 애플리케이션을 개발하고 있는 기업(프로세서 확장 기능, 플랫폼 보안 기능, 클라우드 네이티브 애플리케이션을 데이터가 있는 시스템에서 함께 운영할 수 있는 역량, 데이터와 애플리케이션 간의 지연을 감소시킬 수 있는 역량 덕분에 LinuxONE은 수직적/수평적 확장성을 모두 제공)

또한 IBM은 온-프레미스 및 클라우드에서 블록체인을 실행하기 위한 엔터프라이즈급 플랫폼으로서 LinuxONE의 기능을 선보이고 있습니다. 예를 들어, IBM Cloud에서 운영되는 LinuxONE 시스템은 블록체인을 위한 안전하고 강력한 데이터 서비스 클라우드 플랫폼으로서 LinuxONE의 적합성을 보여줍니다. LinuxONE을 사용하여 데이터 또는 비즈니스 요구 사항에 따라 온-프레미스로 블록체인 애플리케이션을 구축하고 확장할 수도 있습니다.

LinuxONE 아키텍처

IBM은 LinuxONE을 Linux를 실행하는 매우 확장성이 뛰어난 데이터 서비스 및 트랜잭션 처리 플랫폼으로 설계함으로써 x86 기반 Linux 서버와 크게 차별화하고 있습니다. 이를 위해 LinuxONE은 단일 설치 공간에서 최대 8,000개의 Linux 서버를 지원합니다. 또한 LinuxONE은 세계 최고의 IBM Z 플랫폼의 엔터프라이즈 품질과 Linux 및 오픈 소스 소프트웨어의 개방성을 결합하고 있습니다.

IBM 엔터프라이즈 플랫폼 기술을 기반으로 설계

LinuxONE은 독창적인 공유 메모리 및 수직 확장 아키텍처를 갖춘 검증된 미션 크리티컬 하드웨어 플랫폼(IBM Z 기반)입니다. I/O 채널의 전용 전원 및 RAS 코어와 I/O 오케스트레이션용 SAP는 플랫폼이 지연시간의 증가 없이도 엄청난 양의 I/O를 처리하고 손쉽게 초당 수백만 건의 트랜잭션을 처리할 수 있도록 해줍니다. 이러한 특징 덕분에 LinuxONE은 데이터베이스 및 기록 시스템과 같은 상태 저장 워크로드를 실행하는 데 훨씬 우수합니다.

칩에서 데이터 압축

IBM Z에 기반한 LinuxONE의 새로운 기능은 프로세서 칩의 하드웨어 기반 데이터 압축 기능입니다. 이전 버전에서는 별도의 압축 카드 하드웨어나 소프트웨어를 사용하여 데이터를 압축할 수 있었습니다. 사용자들은 최신 LinuxONE을 사용하여 칩에서 보다 신속하게 데이터를 압축할 수 있습니다.

IBM은 IBM z14 I/O 카드(zEnterprise Data Compression [zEDC] Express)의 기능을 zEnterprise 데이터 압축을 위한 통합된 가속 기능에 포함시켰습니다. 이 명령은 공개적으로 사용 가능한 설계 명령이므로 소프트웨어 개발의 문을 열어줍니다. 또한 이 명령은 사용하기 위해 권한을 부여 받거나 커널 모드에 있을 필요가 없습니다. 결과적으로, 모든 사용자 애플리케이션은 특별한 권한없이 이러한 가속 기능을 활용할 수 있습니다. 커널 지원이 필요하지 않는다는 것은 특히 LinuxONE에서 중요합니다. 이 가속 기능은 사용자 공간에 전체적으로 배포될 수 있고 명령 아키텍처의 일부이므로 가상화 요구 사항이 없는 모든 게스트가 새로운 명령을 사용할 수 있습니다.

이 가속기는 산업 전반과 여러 프로토콜에서 사용되는 매우 일반적인 압축 형식인 DEFLATE와 완벽하게 호환됩니다. 이것은 오픈 소스 소프트웨어가 이를 활용할 수 있도록 한다는 점에서 중요합니다. 예상되는 이점으로는 데이터를 압축 및 압축 해제하는 시간이 크게 단축되고 해당 작업을 수행하는 데 CPU 사용량이 줄어드는 것을 들 수 있습니다. 또한 고속 압축은 시스템을 통한 데이터 흐름을 크게 최적화합니다.

오픈 소스 Linux 기반 소프트웨어 스택

LinuxONE의 강화된 Linux 기반 소프트웨어 스택은 데이터베이스 및 데이터 관리(예: MariaDB, PostgreSQL, MongoDB 및 Apache Spark), 가상화 및 컨테이너 플랫폼(예: KVM, Docker), 자동화 및 오케스트레이션 소프트웨어(예: Kubernetes, OpenStack, Puppet, Node.js, Juju 및 Chef) 그리고 블록체인 같은 컴퓨팅 집약적인 워크로드와 같이 대부분의 오픈 소스 소프트웨어 패키지를 실행할 수 있습니다.

대부분의 IT 설계자들은 50% 이상의사용율을 성능 저하의 요인으로 간주합니다. 하지만 LinuxONE은 100%에 이르는 사용율에서 조차도 저해되지 않은 성능 및 확장 가능성을 통해 솔루션을 간소화하고 추가 비용을 절감해줍니다. 또한 LinuxONE 시스템의 Ubuntu 덕분에 엔터프라이즈급 스케일 아웃 클러스터 및 확장 가능한 클라우드 아키텍처를 쉽게 구축하고 모델링하며 배포하고 관리할 수 있습니다. 마지막으로 IBM은 LinuxONE을 회사의 사양에 맞게 주문할 수 있도록 설계했으며 LinuxONE은 지진, 화재 및 홍수와 같은 위험에 견딜 수 있도록 완벽하게 테스트되었습니다.

하이브리드 클라우드 배포

컨테이너, Kubernetes 및 마이크로서비스로의 광범위한 이동으로 인해 IBM과 Red Hat은 RedHat의 컨테이너 및 Kubernetes 소프트웨어인 OpenShift®에 대한 LinuxONE의 플랫폼 및 클라우드 전반의 지원 계획을 2019년 8월에 발표했습니다. LinuxONE는 이미 컨테이너와 Kubernetes를 지원했지만 OpenShift를 통해 특히 Java 및 Python을 위한 하이브리드 클라우드에서 애플리케이션의 이식성을 구현할 수 있게 될 예정입니다. 사용자들은 애플리케이션을 컨테이너화한 다음, 다중 아키텍처 지원 기능을 통해 컨테이너화된 애플리케이션을 다른 아키텍처로 전환할 수 있습니다. 예를 들어, x86 플랫폼에 구축된 컨테이너를 LinuxONE에 배포할 수 있습니다. 또한 사용자들은 애플리케이션을 마이크로서비스로 분해한 다음, 컨테이너화하거나 그 반대로 할 수 있습니다.

LinuxONE에서 OpenShift를 사용하는 하이브리드 클라우드의 이점은 LinuxONE 사용자가 플랫폼의 보안 기능을 활용하면서 클라우드 네이티브 애플리케이션을 개발 및 배포하고, 대규모 애플리케이션을 컨테이너화할 때 플랫폼의 확장성을 활용하며, 다양한 온-프레미스 및 클라우드 플랫폼에서 단일 지점 관리를 활용하고, 클라우드 에코시스템에서 민첩성을 구현하며, 개방형 기술 및 툴링을 사용하고, 하이브리드 클라우드 에코시스템에서 워크로드, 서비스 및 데이터의 모빌리티를 지원할 수 있다는 데 있습니다.

LinuxONE 보안

LinuxONE은 보안 기능이 내장되어 바로 사용 가능한 플랫폼으로 일반적으로 이와 같은 솔루션은 많지 않습니다. 기업은 시스템을 도입하면서 바로 보안 기능의 이점을 누릴 수 있습니다. 펌웨어 수준에서 보안 기능을 활용할 수 있다는 것은 위험이 발생하기 전에 보안 조치를 취할 수 있다는 것을 의미합니다. 다음 섹션에서 논의될 기능은 여러 가지 면에서 LinuxONE을 독보적인 플랫폼으로 만듭니다.

LPAR 레벨에서의 EAL5+ 격리

안전한 이 멀티테넌시 기능은 피어 환경 간의 격리 기능을 제공하므로 기업뿐 아니라 서비스 제공업체에도 상당한 이점을 제공합니다. 또한 LinuxONE의 Crypto Express 어댑터는 레벨 4 FIPS 140-2 인증을 받도록 설계되었습니다. 즉, 암호화 키의 변조 방지 인클로저가 손상되면 시스템은 데이터를 자동으로 0으로 작성하여 키를 보호합니다.

IBM Secure Service Container

IBM Secure Service Container는 소프트웨어 어플라이언스를 LinuxONE에 안전하게 배포하기 위한 프레임워크이며 Secure Service Container 어플라이언스는 "SSC 모드"로 구성된 LinuxONE LPAR에 배포됩니다. Secure Service Container 기술은 다음과 같은 기능을 제공합니다:

- **업계 최고의 피어 격리:** Secure Service Container 기술은 LinuxONE의 EAL5+ 인증 LPAR 격리 기능을 활용하여 단일 설치 공간에서 어플라이언스 환경을 거의 망분리(Air Gap) 수준으로 분리하여 다른 인프라에서 어플라이언스 워크로드를 볼 수 없도록 해줍니다.
- **권한있는 사용자로부터 데이터를 수직으로 격리 및 보호:** "SSC 모드" LPAR로 구성된 어플라이언스의 경우 설계 상 쉘 또는 명령 행 인터페이스를 통한 직접(SSH) 운영 체제 액세스가 사용 불가능합니다. 시스템 권한이 상승된 사용자의 액세스를 금지하는 효과적으로 정립된 RESTful API와 웹 인터페이스를 통해서만 어플라이언스 관리 및 통신이 허용됩니다. Secure Service Container LPAR 및 내부에서 실행되는 어플라이언스에 대한 액세스 권한이 부여된 사용자만 어플라이언스에 액세스할 수

있으므로 부주의하거나 악의적인 내부자 위협으로부터 어플라이언스 데이터와 실행 환경이 보호됩니다.

- **사용 및 대기 중 데이터 혹은 코드의 기밀 유지:** Secure Service Container 어플라이언스에 대한 직접 메모리 액세스는 비활성화되어 있으며 암호화되지 않은 상태에서 어플라이언스 메모리를 떠나는 데이터가 없도록 다양한 암호화 및 서명 계층이 구현되어 있습니다.
- **변조 또는 멀웨어의 위험을 줄이기 위한 어플라이언스 코드의 유효성 검사:** Secure Service Container 어플라이언스는 소프트웨어 배포 전에 신뢰할 수 있는 펌웨어 부팅 절차를 통한 생성과 서명 확인을 통한 변조 방지를 기반으로 보호됩니다.

초기 단계에서 Secure Service Container 프레임워크는 비즈니스 네트워크가 미션 크리티컬, 엔터프라이즈급 블록체인 데이터 및 체인 코드를 호스팅하는 데 필요한 암호화 및 데이터 프라이버시를 통해 온-프레미스 및 IBM Cloud 모두에서 IBM Blockchain Platform과 같이 IBM이 제공한 솔루션을 구현했습니다.

다음 단계에서는 Secure Service Container 프레임워크 사용자가 온-프레미스에서 컨테이너 기반 애플리케이션을 LinuxONE의 Secure Service Container 인스턴스에 배포하는 데 사용할 수 있도록 만들어졌습니다. 이를 통해 사용자의 애플리케이션이 구현되어 Secure Service Container 기술의 기능을 활용하면서 단일의 LinuxONE 설치 공간에 수백만 개에 이르는 컨테이너까지 동적으로 확장하고 이를 사용자의 엔터프라이즈 전역, 교차 플랫폼 컨테이너 및 DevOps 전략과 통합할 수 있게 됩니다.

IBM은 최신 LinuxONE 배포판에 다음과 같은 기능을 추가했습니다:

- 부팅 프로세스 동안의 취약성을 대상으로 하는 루트-레벨 공격 및 바이러스로부터 보호하는 안전한 부팅 보호 시스템
- Fibre Channel 엔드포인트 보안에 대한 계획된 지원, 데이터센터 내부 및 데이터센터에 걸쳐 Fibre Channel 링크의 사용 중 엔드-투-엔드 데이터 보호 기능을 제공하여 무단 액세스 제거

Data Privacy Passports

IBM은 최신 LinuxONE 배포판과 함께 본래의 플랫폼 영역을 벗어난 범위까지 데이터 보호 범위를 확장하는 Data Privacy Passports도 발표했습니다. 예를 들어, 사용자가 LinuxONE 서버에서 데이터를 추출하여 분산 컴퓨팅 시스템에서 이러한 데이터를 사용할 경우, Data Privacy Passports는 분산 시스템까지 데이터 보호 범위를 확장할 수 있습니다. 데이터가 신뢰할 수 있는 데이터 개체의 일부로 암호화된 상태로 추출되면 중심화된 데이터 액세스 정책에 따라 액세스할 수 있습니다. 데이터 액세스 권한이 철회되면 사용자는 Data Privacy Passports 인프라의 정책에 따라 분산 시스템에 있는 데이터에 더 이상 액세스할 수 없습니다.

Data Privacy Passports는 IBM이 Data Privacy Passport Controller라 언급하는 도구를 사용하며 이는 Secure Service Container에 배포되고 특정한 JDBC(Java Database Connectivity) 소스에서 데이터를 수집할 수 있습니다. 이 도구는 LinuxONE의 JDBC, Z 기반의 Linux, z/OS, Power Systems 또는 x86을 통해 액세스 가능한 데이터를 보호합니다. Data Privacy Passports는 데이터 중심 접근 방식을 통해 플랫폼 안팎의 데이터에 대한 프라이버시를 제공한다는 점에서 퍼베이시브 암호화를 보완하는 한편 퍼베이시브 암호화는 데이터 소스에서 데이터베이스 또는 애플리케이션 데이터를 보호합니다.

이러한 보호 시나리오에서는 기록 시스템에서 시작된 데이터가 보호된 다음, 조직의 중앙 집중식 데이터 액세스 정책을 통해 계속 보호되면서 엔터프라이즈를 통해 이동합니다. 이것이 작동하는 방식은 데이터가 메타데이터 및 암호화 데이터가 포함된 신뢰할 수 있는 데이터 개체로 묶여 있다는 것입니다. 문제없는 상태에서 데이터에 액세스하기 위해서는 신뢰할 수 있는 이러한 데이터 개체를 Data Privacy Passports 인프라를 통해 처리해야 합니다. 달리 말해, 데이터가 신뢰할 수 있는 데이터 개체로 보호되어 있으며 이 상태에서 암호화된 데이터가 이동하고 시스템을 이동할 수 있습니다.

혁신적인 LinuxONE 사용 사례

LinuxONE은 고도의 공학적 설계에 기반한 솔루션으로 데이터 서비스 및 상태 유지가 필요한 애플리케이션(stateful application)에 매우 적합하며, 범용 Linux 서버 또는 가상 머신의 수평 확장 클러스터에서 실행되는 것에 비해 내부 고속 패브릭에서 공유된 메모리와 공유된 프로세싱을 통해 수직 확장 환경으로부터 더 많은 혜택을 누릴 수 있습니다. 다음 섹션에 설명되어 있는 사용 사례는 LinuxONE의 진정한 성능을 보여줍니다.

LinuxONE의 서비스형 데이터베이스*(DB as a Service)*

최근에는 차세대 앱 개발이 가속화되면서 기업에서 오픈 소스 기반 관계형 및 비관계형 데이터베이스 도입이 급증하고 있습니다. IBM은 정형 및 비정형 데이터 관리를 위한 "서비스형" 환경을 구축하려는 기업들에게 LinuxONE을 추천하고 있습니다. LinuxONE의 보안, 확장성 및 성능 덕분에 LinuxONE은 DBaaS(서비스형 데이터베이스) 구축에 이상적인 플랫폼입니다. 고객들은 다양한 형태의 DBaaS를 구현할 수 있습니다:

- 완벽한 제어를 제공하는 DBaaS 환경: 이것은 DIY(do-it-yourself) 방식의 모델입니다. IBM은 Trove를 활용하는 온-프레미스 OpenStack 환경에서 고객이 DBaaS를 설정할 수 있도록 지원하는 레퍼런스 아키텍처를 제공합니다. 고객들은 이 레퍼런스 아키텍처를 활용하여 DB2, SQL 및 MongoDB와 함께 DBaaS를 신속하게 가동하고 실행할 수 있습니다. 또한 고객들은 LinuxONE 플랫폼에서 사용할 수 있는 다른 오픈 소스 및 기술 옵션을 활용하여 DBaaS로의 경로를 직접 생성하는 것을 선택할 수도 있습니다.
- 사전 구성된 온-프레미스 프라이빗 클라우드 환경: 기본적으로 훨씬 빠른 배포를 제공하면서 IBM LinuxONE Secure Service Container 프레임워크를 활용하기 때문에 전자에 비해 보다 사전에 정의된 솔루션 접근 방식이 될 것입니다. IBM은 LinuxONE에서 이를 제공할 수 있는 가능성을 모색하고 있습니다.
- 호스팅된 오프-프레미스 클라우드 환경: 기본적으로 셀프 서비스 모델로서, 뛰어난 확장성 및 보안 기능을 위해 LinuxONE에 데이터가 호스팅됩니다. 이는 현재 서비스형 Hyper Protect 데이터베이스로 제공되고 있으며, 퍼블릭 클라우드 서비스로 IBM Cloud의 LinuxONE에 구축 및 배포되고 있습니다.

LinuxONE의 블록체인

블록체인은 강력한 트랜잭션 보안이 가장 중요하면서 엄격한 규제가 요구되는 산업(예: 핀테크)에서 급부상하고 있습니다. 따라서 이러한 산업에는 엔드-투-엔드 블록체인 배포에 필요한 엄격한 퍼베이시브 보안 체계를 기반으로 설계된 트랜잭션 지향 컴퓨팅 인프라 플랫폼(즉, 확장성이 뛰어난)이 필요합니다.

IBM Blockchain 플랫폼은 IBM Cloud, 다른 클라우드 환경 및 온-프레미스에서 IBM 관리형 블록체인 서비스 형태로 제공됩니다. IBM Blockchain 플랫폼은 엔터프라이즈급 블록체인 서비스로서, IBM이 적극적으로 기여하는 Linux Foundation이 호스팅하는 Hyperledger 프로젝트인 최신 버전의 Hyperledger Fabric을 기반으로 합니다. 이 서비스를 통해 개발자들은 IBM 클라우드에서 보안 기능이 풍부한 프로덕션 블록체인 네트워크를 신속하게 구축하고

호스팅할 수 있습니다. 이 서비스는 온-프레미스 및 IBM Cloud에 기반을 둔 LinuxONE으로 제공되며 보안, 성능 및 데이터 격리 사양 측면에서 업계 최고 중 하나로 간주될 수 있습니다. 이

Cognition Foundry는 스타트업이 혁신을 위해 엔터프라이즈 기술을 활용하는 데 도움을 주고 있습니다.

Cognition Foundry는 스타트업과 중소기업들에게 아키텍처 설계에 대한 통찰력과 애플리케이션 개발을 지원하는 동시에 LinuxONE 기반에서 사용할 수 있는 우수한 컴퓨팅 리소스 액세스를 제공하고 있으며, 유망한 스타트업과 중소 기업들에게 공정한 경쟁의 장을 제공하는 것을 목표로 하고 있습니다.
Cognition Foundry는 이러한 접근 방식을 "엔터프라이즈 IT에 대한 액세스 권한 민주화"라 설명합니다. 이러한 접근 방식을 통해 소규모 사용자들은 정부와 포춘 500대 기업들이 사용하는 기술과 동일한 기술을 사용할 수 있습니다.
Cognition Foundry의 개발자 팀은 스타트업이 코드를 개발하고 테스트할 수 있도록 도와주면서 고도로 공학 설계된 개방형 IT 인프라의 이점을 최대한 활용할 수 있도록 지원합니다. Cognition Foundry는 대규모 네트워크를 활용하여 유망한 스타트업이 경쟁 시장에서 승리할 수 있도록 엔터프라이즈 아키텍처, 설계 및 비즈니스 기술을 연계해 주고 IT 비용도 관리할 수 있도록 도와 줍니다.
LinuxONE이 오픈 소스 소프트웨어를 실행할 수 있는 능력은 스타트업 공간에 오픈 소스 소프트웨어가 얼마나 널리 보급되어 있는지를 고려할 때 Cognition Foundry에게 상당한 경쟁력을 제공합니다. 플랫폼에서 수직으로 확장할 수 있는 능력 덕분에 인프라를 추가하지 않고도 대규모 확장이 가능합니다. 최적의 자원 관리에 중점을 두고 있는 서비스 제공업체인 Cognition Foundry는 고객 기업에게 상당한 도움이 됩니다. 최근 이 기업은 고객들에게 하이브리드 클라우드 플랫폼을 제공하고 있으며 고객들은 이를 통해 온-프레미스 LinuxONE 환경 및 IBM 퍼블릭 클라우드의 LinuxONE 간을 넘나드는 컨테이너화된 애플리케이션으로 전환할 수 있습니다. Cognition Foundry의 고객에는 개발도상국의 커뮤니티와 협력하여 유용한 혜택을 받는 대가로 플라스틱 병을 재활용하는 플라스틱 은행과 같은 조직이 포함되어 있습니다.

서비스는 컴플라이언스 및 포렌식 검사를 위한 입증된 감사 환경을 제공합니다.

IBM의 도전과제 및 기회

IBM은 LinuxONE을 통해 미래의 워크로드와 애플리케이션을 위해 설계된 강력한 시스템을 구축했다고 주장할 수 있으며, 블록체인 및 오픈 소스 데이터베이스는 두 가지 핵심 기술입니다. IBM은 LinuxONE을 통하여 IBM Z의 장기적인 성공을 재현하고자 합니다. IBM은 이제 LinuxONE의 가치와 역량을 광범위한 고객, 산업, 지역 및 워크로드로 확대하고자 합니다. 이 모든 가치에는 다음과 같은 공통점이 있습니다.

- 같은 데이터를 공유하는 동일한 머신에서 다양한 프로덕션 및 분석 워크로드를 지원할 수 있는 멀티 테넌트 확장성 제공
- 더 작은 인프라 설치 공간에서 워크로드를 통합할 수 있도록 더 나은 성능과 최적의 보안 기능으로 에너지 소비 및 라이선스 비용 절감

- 기업들이 비즈니스를 수행하고 데이터를 최대한 활용하며 고객에게 더 많은 서비스를 제공할 수 있는 신뢰할 수 있는 상시 데이터 제공 플랫폼 구현

IBM은 LinuxONE과 범용 x86 기반 서버 클러스터를 직접 비교하지 않고도 대화를 유용하게 전환할 수 있었습니다. 이제 LinuxONE은 제한된 수의 워크로드를 지원하는 플랫폼을 넘어서 업계 최고의 보안, 확장성 및 성능을 갖춘 총체적 솔루션 패키지로 정의해야 합니다. 또한 모든 워크로드를 위한 플랫폼으로서의 LinuxONE에서 최고 수준의 보안 기능을 제공하는 단일 소스의 데이터 서비스를 위한 최고의 플랫폼인 LinuxONE으로 논의를 전환해야 합니다.

결론

온-프레미스 또는 클라우드에 배포되었는지 여부에 관계없이 플랫폼 선택은 중요한 문제입니다. 또한 플랫폼은 자격 증명이 보호되고, 피어 환경이 서로 격리되며, 펌웨어 레벨에서 암호화 기능이 기본으로 제공되고, 암호화 키가 하드웨어로 보호되는 보안 멀티테넌시를 제공해야 합니다. 플랫폼은 민감한 고객 기록 및 기밀 정보와 같은 데이터가 내부 및 외부 위협으로부터 보호되는 수직 보안 기능을 제공해야 합니다. 최종적으로, 퍼베이시브 보안 기능을 통해 전체 시스템이 완전히 보호되고 하드웨어 구획들은 서로 격리되어야 합니다.

IBM LinuxONE은 상용(IBM Z) 시스템과 오픈 소스(Linux) 시스템의 장점을 결합해 다른 어떤 제품과도 비교할 수 없는 보안 기능 및 기록 시스템 워크로드의 확장 가능성을 함께 제공하고 있습니다. IBM LinuxONE은 투자할 가치가 있는 플랫폼입니다.

IDC에 대한 소개

IDC(International Data Corporation)는 정보 기술, 통신 및 소비자 기술 시장에 시장 인텔리전스, 자문 서비스 및 이벤트 서비스를 제공하고 있는 세계적인 공급업체입니다. IDC는 IT 전문가, 비즈니스 임원 및 투자 커뮤니티가 기술 구매 및 비즈니스 전략에 대한 사실 기반 의사 결정을 내릴 수 있도록 지원합니다. 1,100명 이상의 IDC 애널리스트가 전 세계 110여 개 국가의 기술 및 업계 기회와 동향에 대한 글로벌, 지역 및 현지 전문 지식을 제공합니다. IDC는 50년 동안 고객이 주요 비즈니스 목표를 달성하는 데 도움이 되는 전략적 통찰력을 제공해 왔습니다. IDC는 세계 최고의 기술 미디어, 리서치 및 이벤트 서비스 제공업체인 IDG의 자회사입니다.

본사

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
트위터: @IDC
idc-community.com
www.idc.com
