2016 OpenStack Study Class-A

Hardware Virtualization

2016-04-22

IBM Korea - Global Technology Services

JeSam Kim

목차

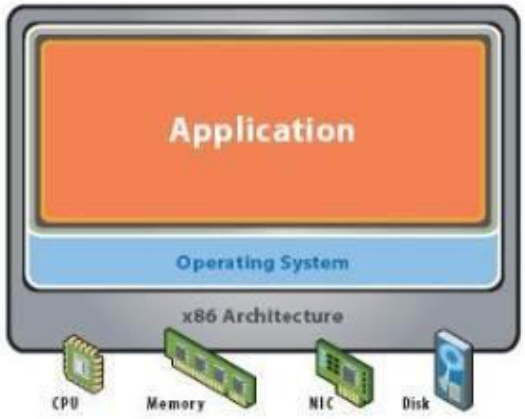
❖ 3주차

1. Hardware Virtualization
2. Intel VT
3. Intel VT-x detail
4. AMD-V
5. CPU ring level

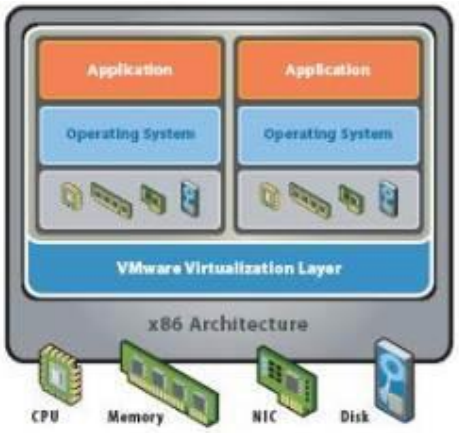
1. Hardware Virtualization

가상화란?
- 컴퓨팅 리소스의 추상화를 일컫음.
- 서버나 스토리지 같은 물리적인 리소스를 이용해 다중의 논리적인 리소스를 만들어 냄.

하드웨어 가상화란?
- 가상화 솔루션의 VMM(Virtualization Machine Monitor = Hypervisor)의 구동에서 CPU overhead를 줄이기 위한 기술
- 인텔/AMD는 VMM 기술에서 사용되는 가상화 구현 관련 명령어 패턴을 하드웨어 기술로 구현함



Before Virtualization:



After Virtualization:

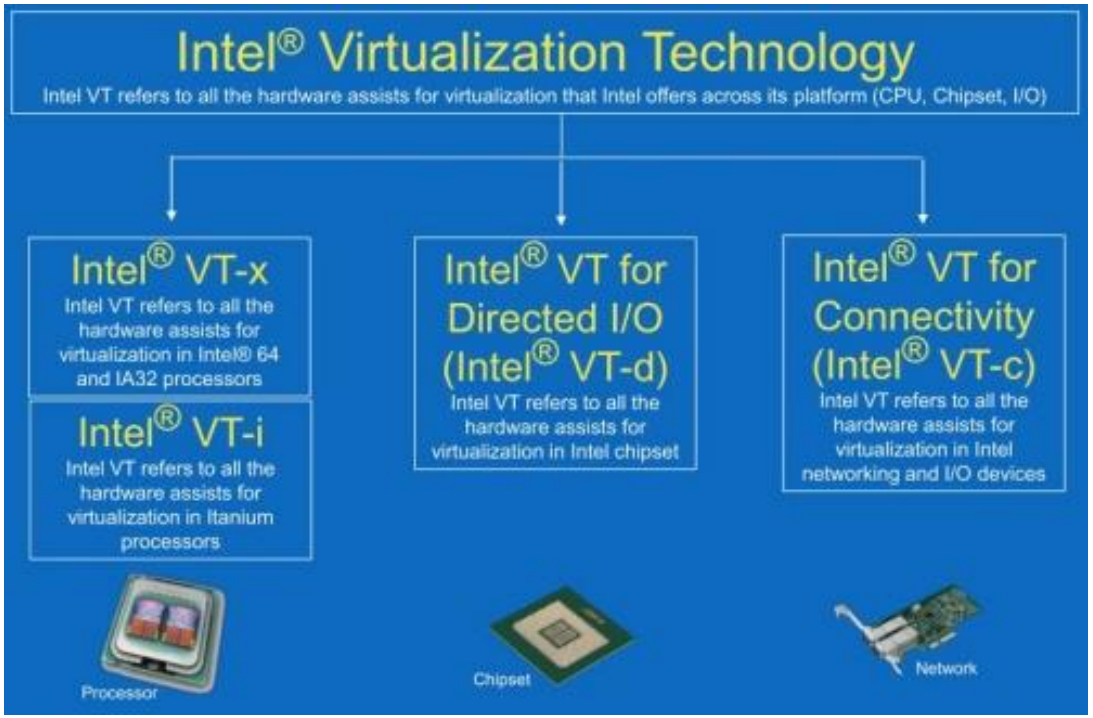
2. Intel VT

Intel VT(Virtualization Technology)

- Intel VT-x, VT-i
  : CPU 단에서 제공되는 기술이며, 인텔의 가상화 기술 중 x86서버에 탑재되는 Xeon processor에 대한 기술을 VT-x 라고 하며, 유닉스 서버용 프로세서인 Itanium processor에 대한 기술을 VT-i 라 부름.

- Intel VT-d
  : Virtualization Technology for Directed I/O 를 의미하며, I/O가 사용하는 DMA 주소를 물리 서버와 VM에 매핑하는 것을 하드웨어로 구현한 것

- Intel VT-c
  : Virtualization Technology for Connectivity 를 의미하며, 가상화 환경에서 네트워크 카드의 성능을 향상시킴.



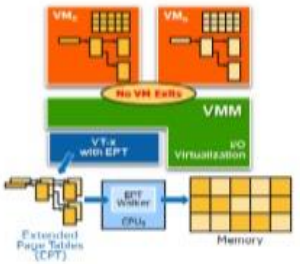
3. Intel VT-x : detail

Intel VT-x

- Physical Host 위에 생성된 여러 개의 VM들의 하드웨어 리소스 사용에 대한 주도권 다툼으로 인한 병목 현상을 줄이는 것이 핵심.
- FlexPriority : VM들에 우선순위를 지정하여 처리하는 기술
- FlexMigration : 코어 마이크로 아키텍쳐 기반의 플랫폼으로부터 VM 마이그레이션 지원
  => DR, Load Balancing, Reducing Downtime
- EPT : VM의 메모리를 Physical 메모리의 어느 부분을 사용하는지 고속으로 계산
- VPID : VM의 변경이 있을 때, Physical 메모리와 VM의 메모리 공간 매핑 테이블을 VM 마다 보존

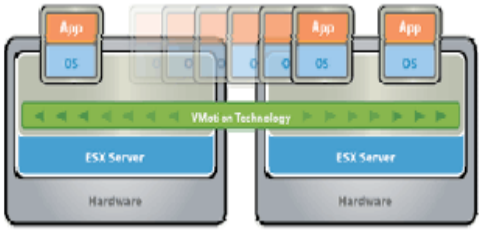
Intel® Virtualization Technology Review - HW Virtualization

Extended Page Tables (EPT)



Virtual Processor ID (VPID)

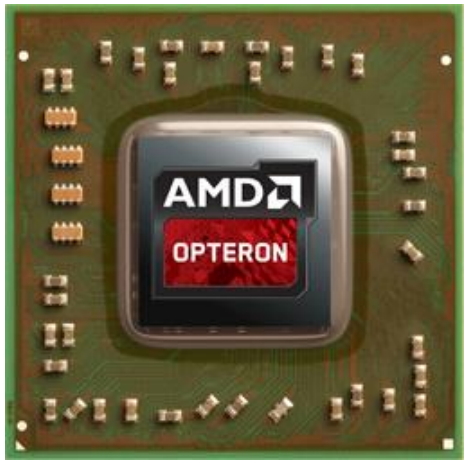
FlexMigration

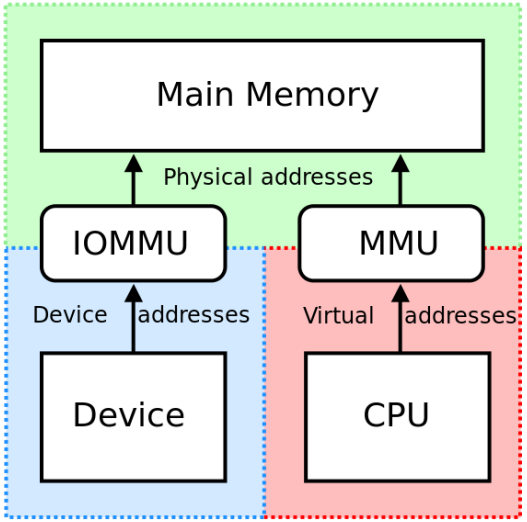


4. AMD-V

AMD-V(Virtualization)

- 64bit x86-architecture에 대한 AMD의 가상화 기술을 AMD-V 라 부름.
- AMD-V는 애슬론 64 및 튜리온 64 X2, 옵테론 2세대 및 페넘 이후의 프로세서에 존재함.
- AMD는 입출력 메모리 관리 장치(IOMMU) 기술을 AMD-V에 추가함.

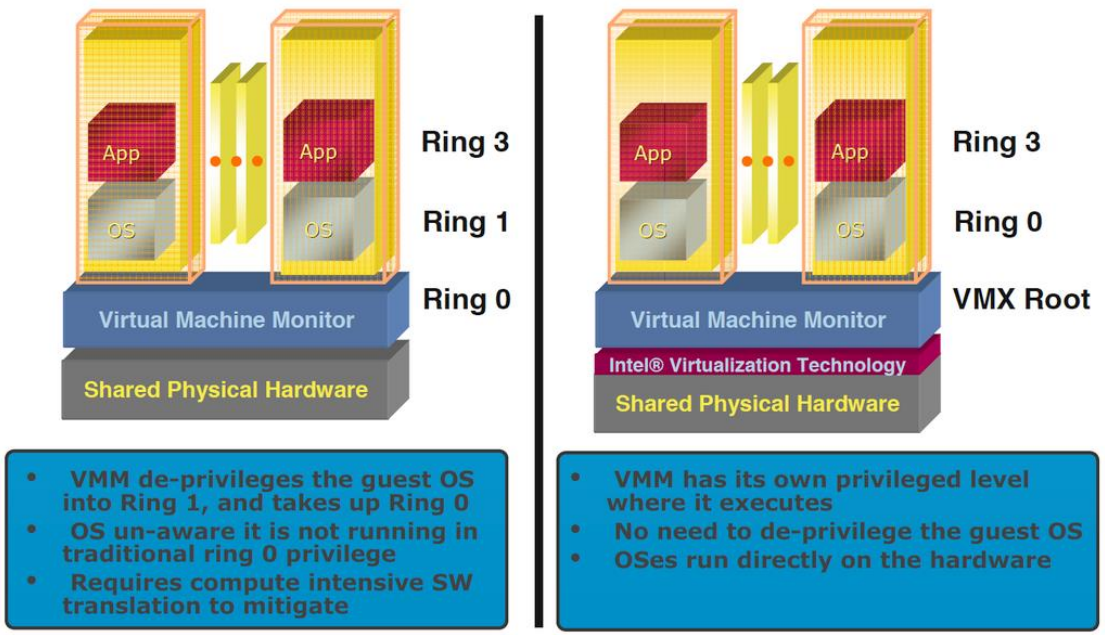


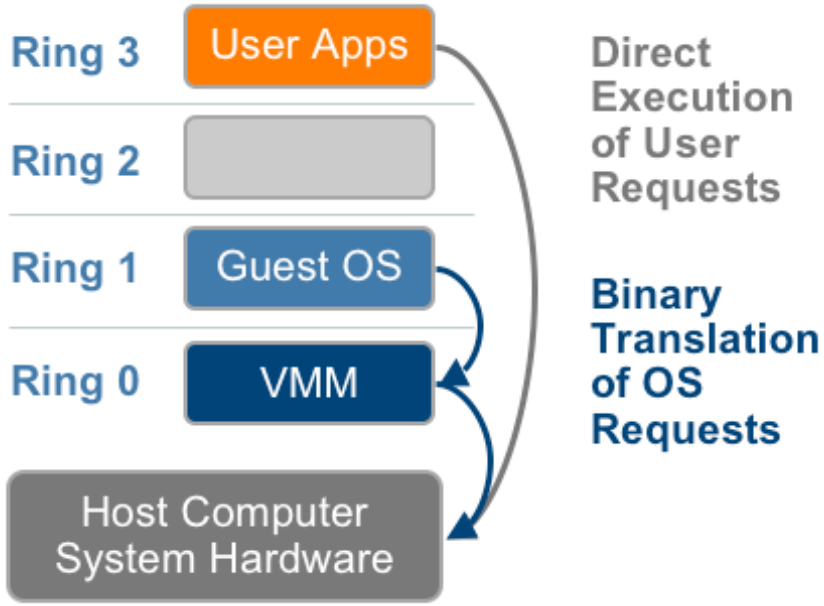


5. CPU ring level

CPU (x86) ring level (without VT-x)

- Privilege level (=protection rings)
- Ring 0 : VMM
- Ring 1 : guest OS
- Ring 3 : User Application





THANK YOU