Virtualization in Cloud Computing

Tessema Mengistu (Ph.D.)

mengistu@vt.edu

Outline

- Operating System Overview
- Virtualization: What is it?
- Virtualization in the Cloud

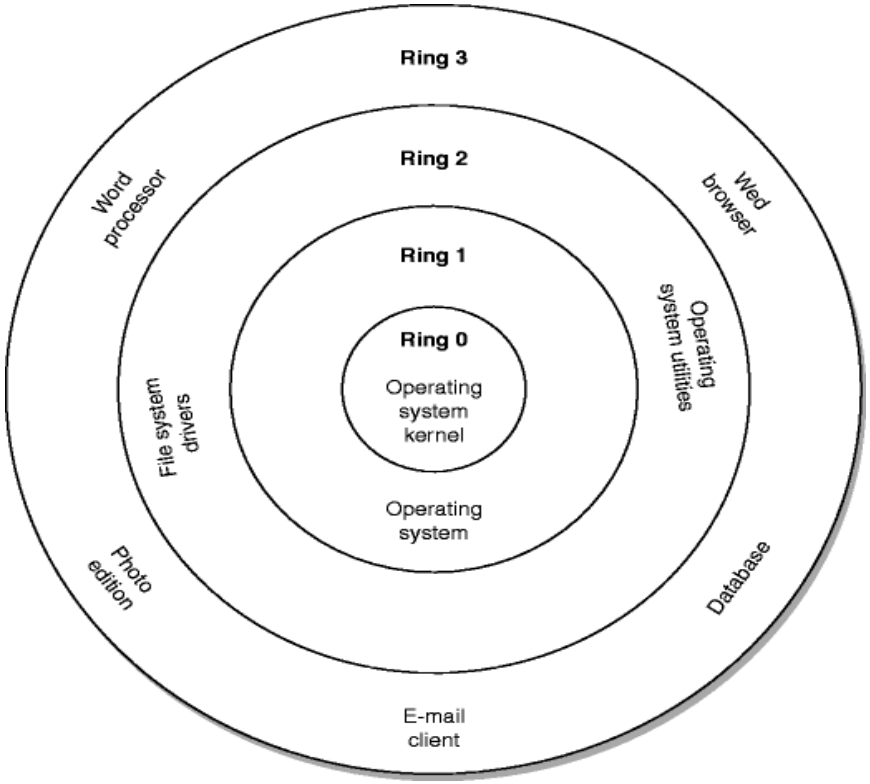
Operating System

- A program that controls the execution of application programs and acts as an interface between applications and the computer hardware
- Manages resources (CPU, Memory, Disk, I/O, …)
- A **microkernel architecture**
  - Few essential functions to the **kernel**, including address spaces, IPC, and basic scheduling
  - Other OS services are provided by processes, sometimes called servers, that run in **user mode** and are treated like any other application
    - System calls

Operating System

- To manage the complexity of operating systems
  - Modular
  - Hierarchical layers and information abstraction
- Modern operating system uses **protection rings**
  - Provides different privilege levels
  - Isolates the OS from untrusted user applications
- In protection ring architecture, the rings are arranged in hierarchical order from ring 0 to ring 3

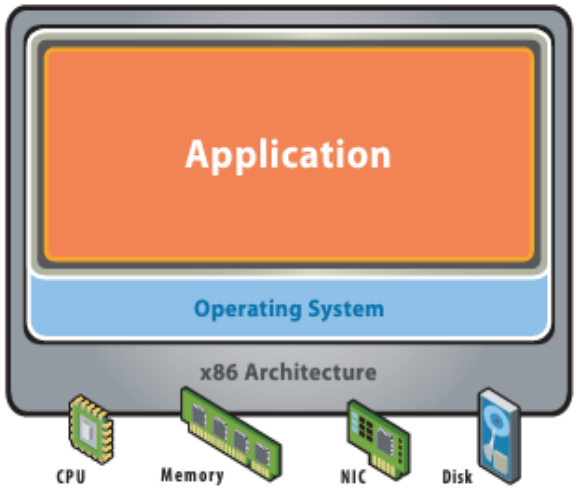
Operating System



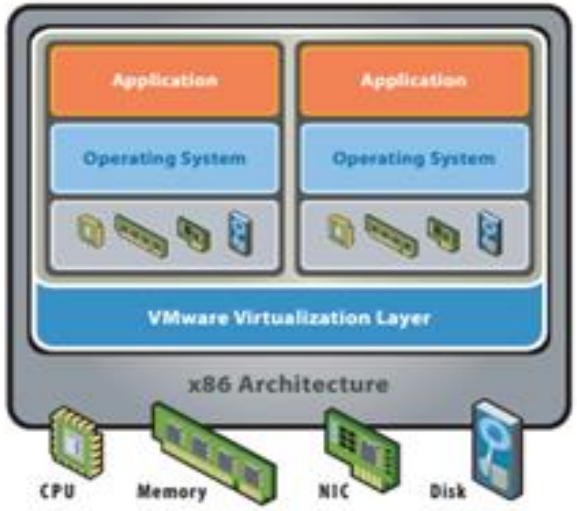
https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_788

Virtualization

- Virtualization
  - The ability to run multiple operating systems on a single physical system and share the underlying hardware resources
  - Provides a layer of abstraction between computing, storage and networking hardware, and the applications running on it



Traditional Stack



Virtualized Stack

https://www.vmware.com/pdf/virtualization.pdf

Virtualization

- Resources that can be virtualized:
  - Memory, CPU
  - Storage
  - Network
    - SDN, NFV
  - Server
  - Application
    - JVM
- Advantages of Virtualization
  - Efficient resource utilization
  - Cost reduction
  - Fault Isolation
  - Green computing
- Disadvantage
  - May lead to lower performance

Virtualization

- Virtual Machine (VM)
  - A virtual representation, or emulation, of a physical computer
  - An isolated environment with access to a subset of physical resources of the computer system
  - Communicates with the physical machine (hardware) through a layer of software - hypervisor

Hypervisor

- Also called a Virtual Machine Monitor - VMM
- The software that securely partitions the resources of a computer system into one or more VMs
  - Sits in between VMs and physical infrastructure and provides the required virtual infrastructure for VMs
- A hypervisor runs in kernel mode, while a guest OS runs in user mode

Hypervisor

- A hypervisor :
  - Guarantees the **isolation** of the individual VMs and thus, ensures security and encapsulation
  - Enables Multiple services to **shar**e the same platform
  - Monitors the system performance and takes corrective actions to avoid performance degradation
  - The movement of a service from one platform to another
    - VM **migration**
  - System modification, while maintaining backward compatibility with the original system

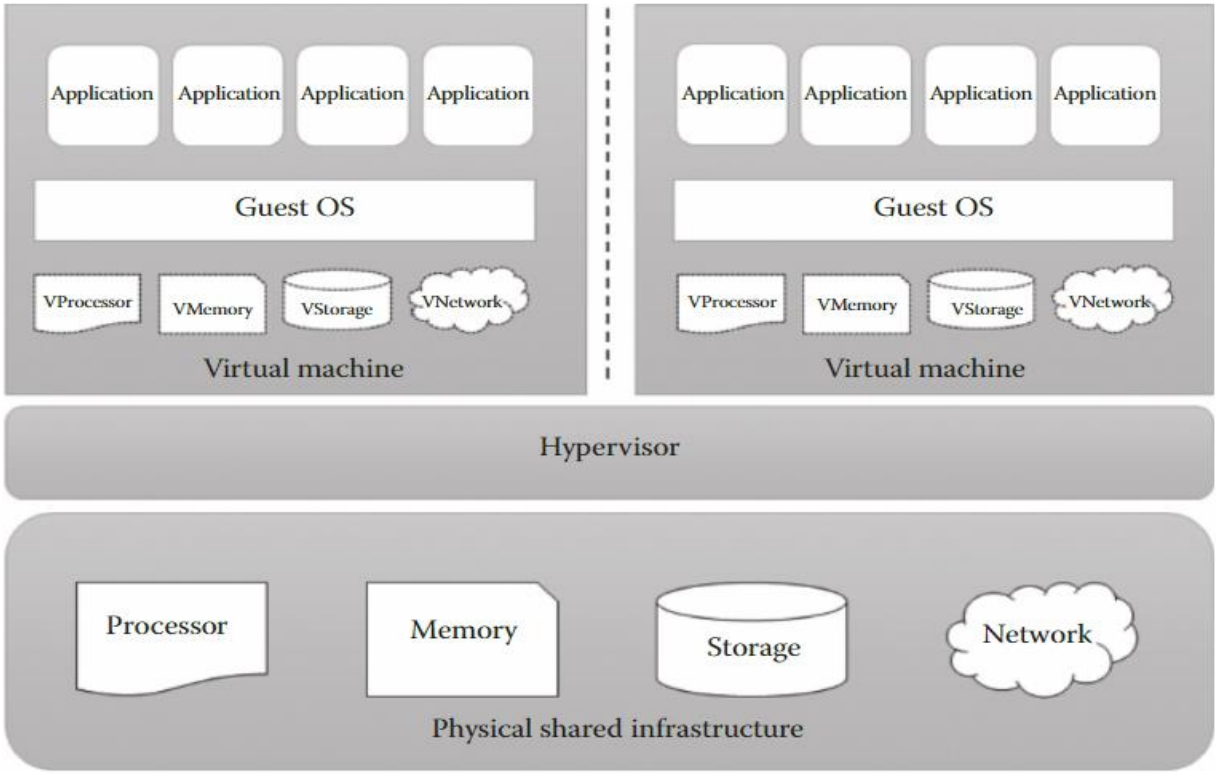
Hypervisor

- Two types of hypervisors
  - Type I
  - Type II

Hypervisor

- Type I hypervisor
  - Runs directly on the host computer's hardware in order to control the hardware resources and also to manage the guest OSs
  - Also known as **native** or **bare-metal** hypervisors
  - Suitable for servers that handle heavy load and require more security
  - Examples: VMware ESXi, Citrix XenServer, and Microsoft Hyper-V

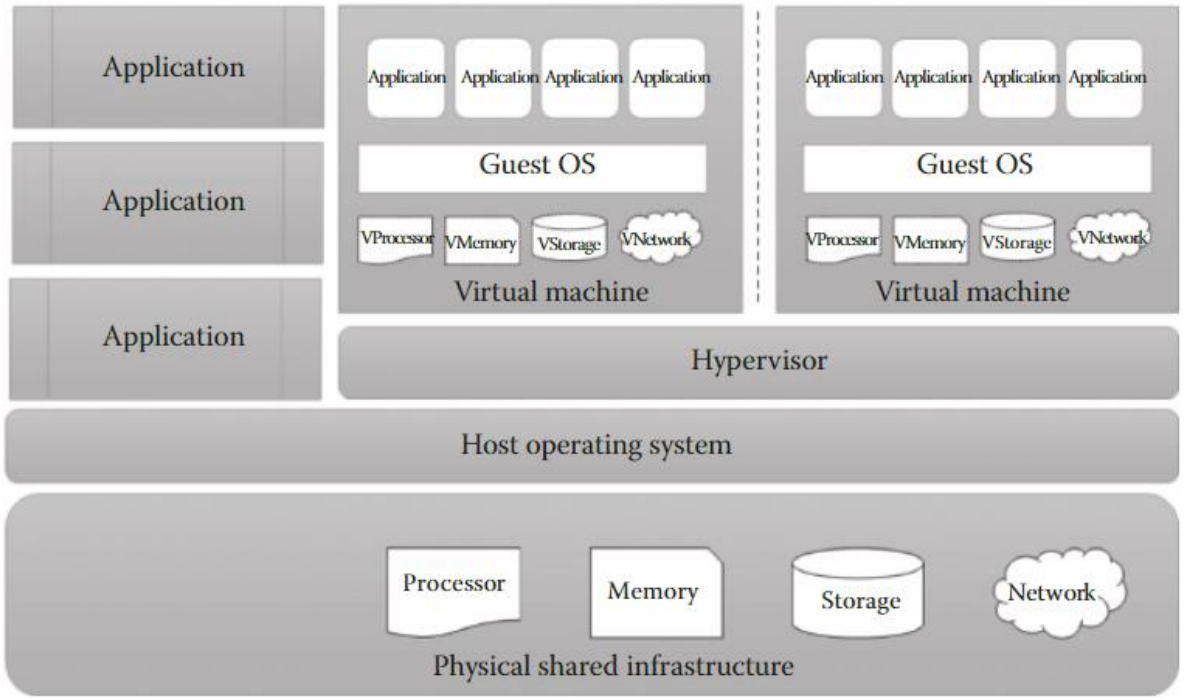
Hypervisor



Hypervisor

- Type II hypervisor
  - Runs within a formal OS environment
  - In this type, the hypervisor runs as a distinct second layer while the guest OS runs as a third layer above the hardware
  - Recommended for client systems where efficiency is less critical
  - Also known as the **hosted** hypervisors
  - Examples: VMware Workstation and VirtualBox

Hypervisor



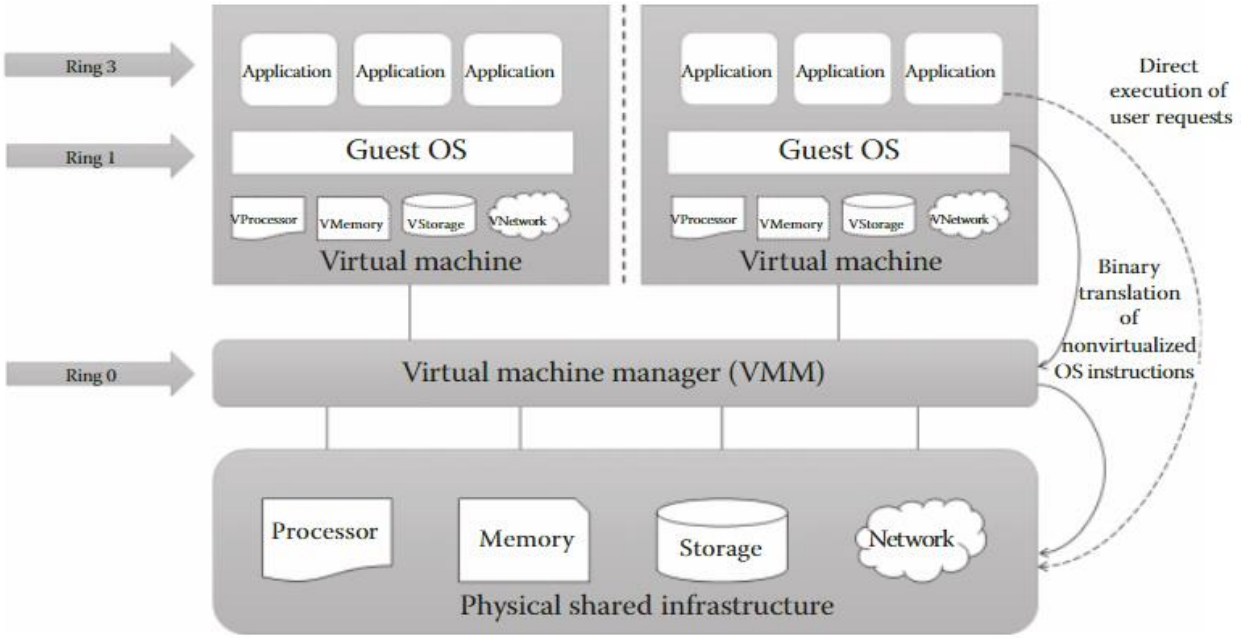
Types of Virtualization

- There are **three** types of approaches followed for virtualization:
  1. Full virtualization
  2. Paravirtualization
  3. Hardware-assisted virtualization

Types of Virtualization

- Full virtualization
  - The guest OS is completely abstracted from the underlying infrastructure
  - The virtualization layer or virtual machine manager (VMM) fully decouples the guest OS from the underlying infrastructure
  - The hypervisor or VMM resides at ring 0 and provides all the virtual infrastructures needed for VMs

Types of Virtualization



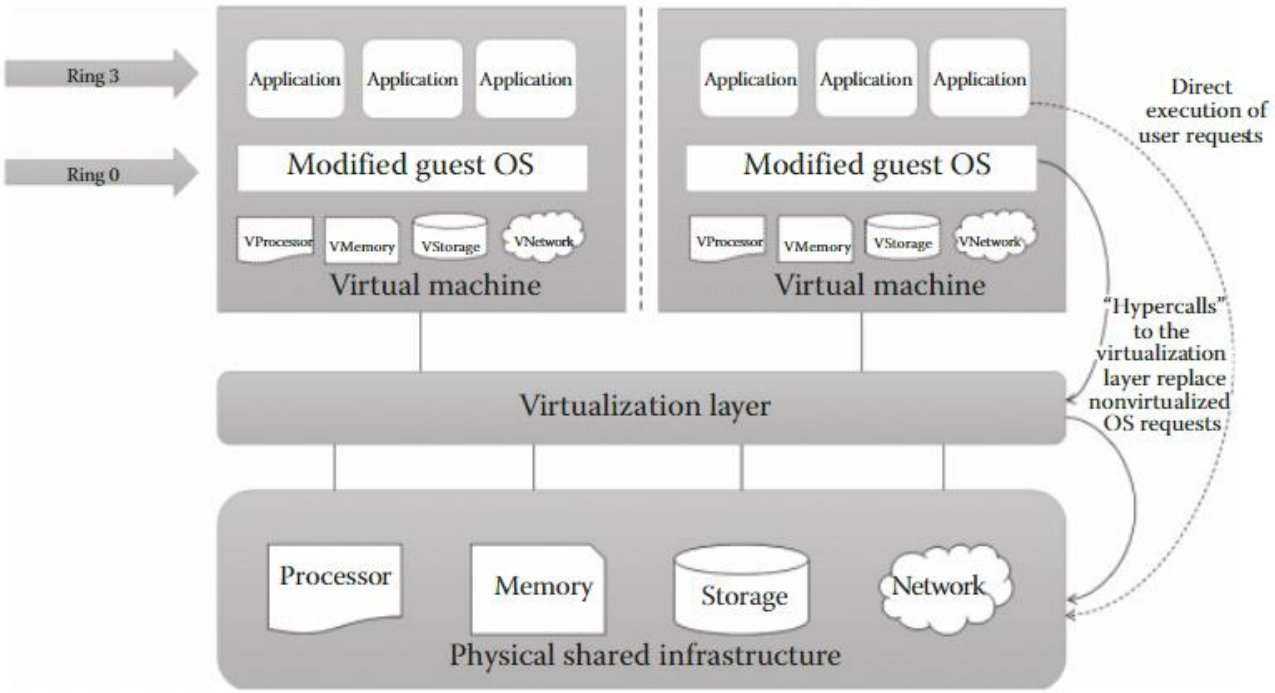
Types of Virtualization

- Pros
  - Best isolation and security for the VMs
  - Different OSs can run simultaneously
  - The virtual guest OS can be easily migrated to work in native hardware
  - It is easy to install and use and does not require any change in the guest OS
- Cons
  - Binary translation is an additional, overhead, and it reduces the overall system performance
  - There is a need for correct combination of hardware and software

Types of Virtualization

- Partial virtualization
  - Also called OS-assisted virtualization, paravirtualization
  - Provides partial simulation of the underlying infrastructure
  - Uses hypercalls
    - Similar to system calls and used for the direct communication between OS and hypervisor

Types of Virtualization



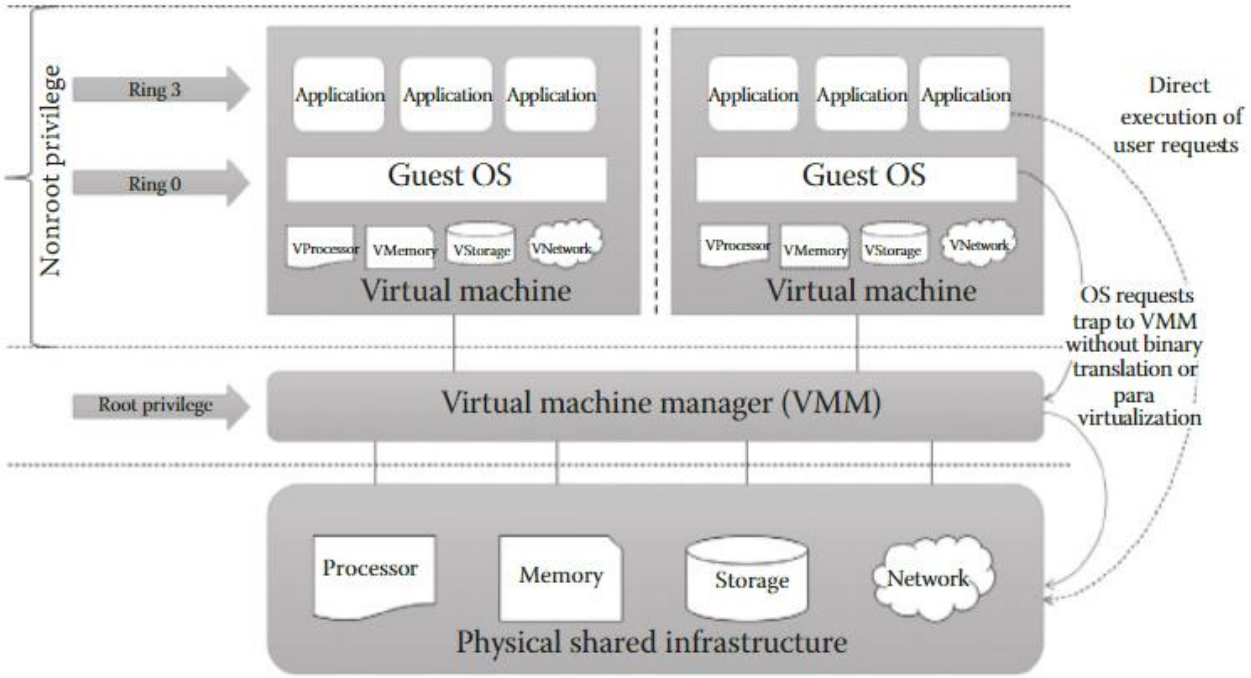
Types of Virtualization

- Pros
  - Eliminates the additional overhead of binary translation
    - Improves the overall system efficiency and performance
  - Easier to implement than full virtualization
    - No need for special hardware
- Cons
  - There is an overhead of guest OS kernel modification
  - The modified guest OS cannot be migrated to run on physical hardware
  - VMs suffer from lack of backward compatibility and are difficult to migrate to other hosts

Types of Virtualization

- Hardware Assisted Virtualization
  - Virtualization supported by processors
    - Example: Intel (VT-x) and AMD (AMD-v)
  - Eliminates much overhead involved in the binary translation and guest OS modification
  - In hardware-assisted virtualization, the VMM has the highest privilege (root privilege) level

Types of Virtualization



Hypervisor

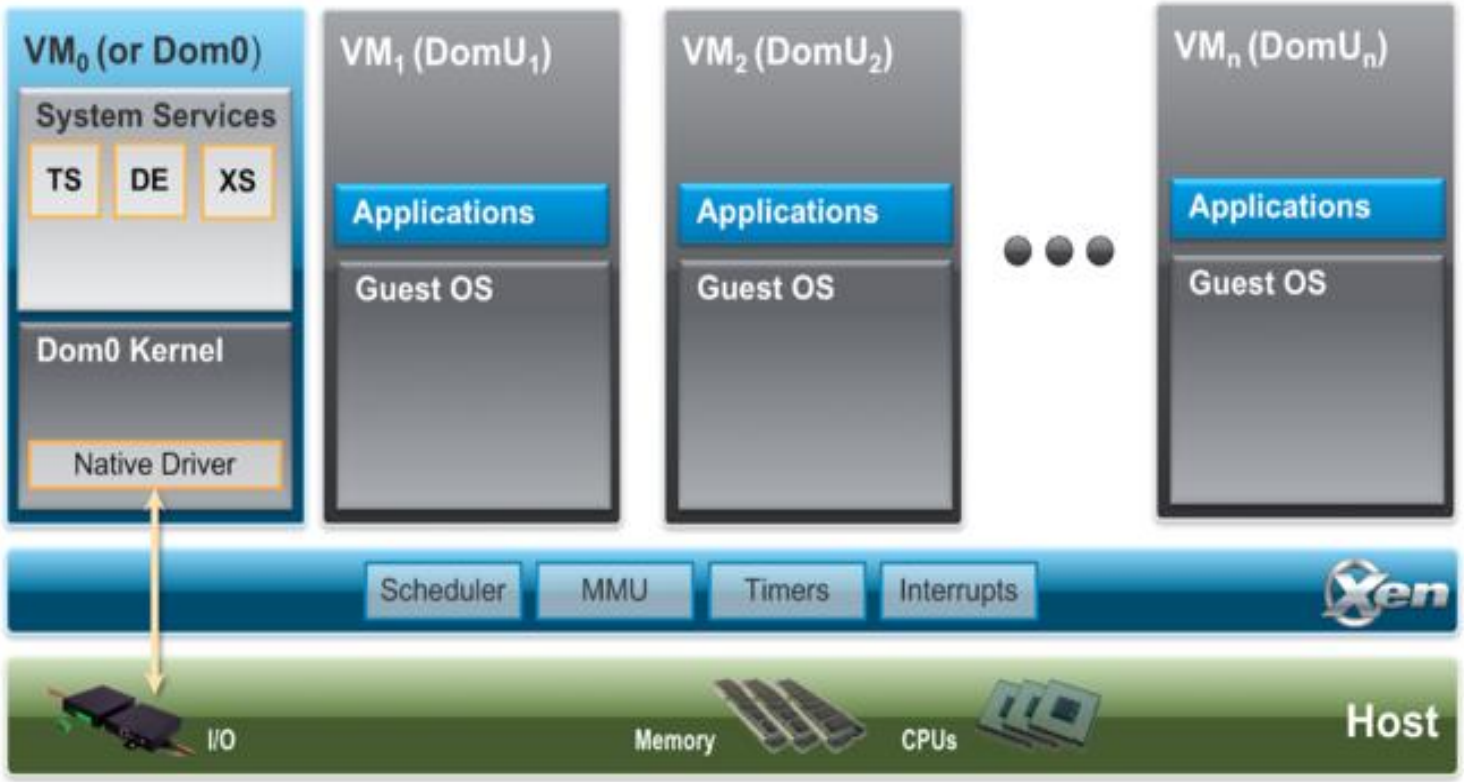
- XEN
  - Type I hypervisor and opensource
  - Used in commercial products
    - XenServer, Oracle VM for x86, CitriXen of AWS
  - Some of Xen's features:
    - Small memory footprint
    - Operating system agnostic
    - Driver isolation
    - Paravirtualization

https://xenproject.org/

Hypervisor

- Xen Architecture
  - Xen hypervisor runs directly on the hardware
    - Responsible for handling CPU, Memory, timers and interrupts
  - The **Control Domain (or Domain 0)** is a specialized Virtual Machine that has special privileges
    - contains the drivers for all the devices in the system, Toolstack, etc.
  - Guest domains/virtual machines

Hypervisor



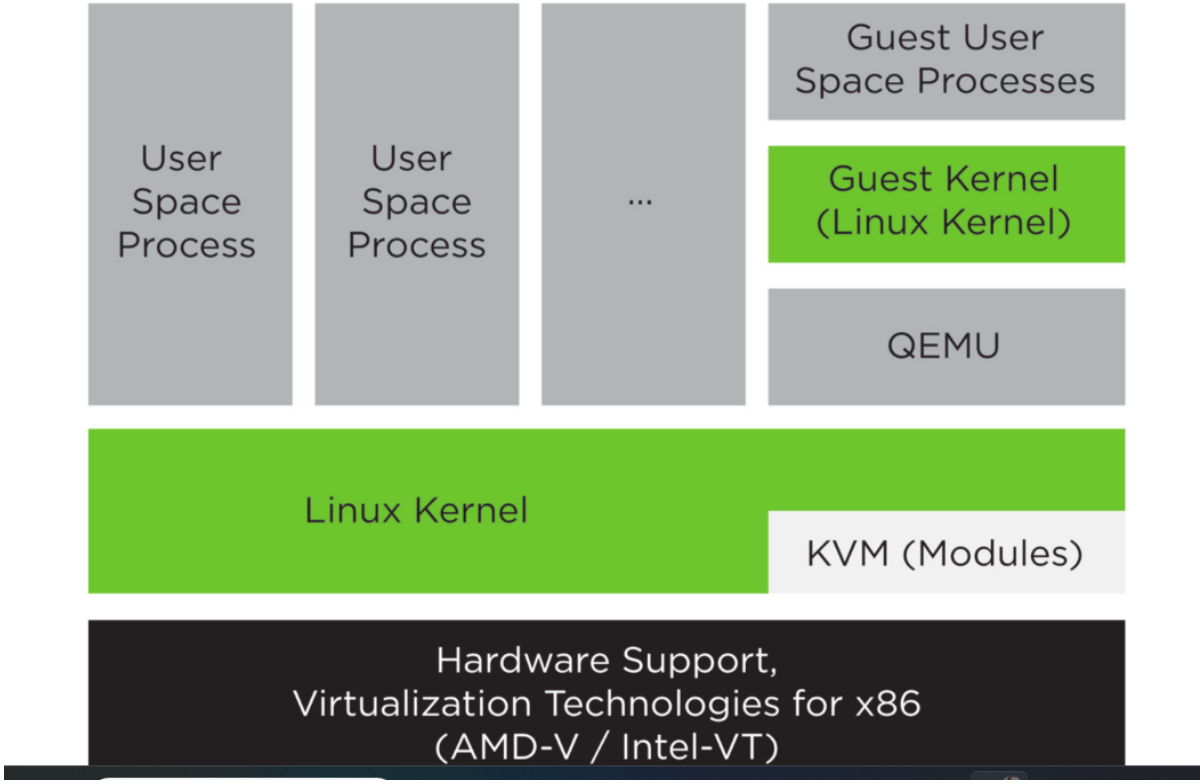
©Xen Wikipage

Hypervisor

- KVM
  - **K**ernel-based **V**irtual **M**achine (KVM) is a virtualization infrastructure of the Linux kernel
  - Supports **full virtualization** and it is **opensource**
  - KVM runs inside Linux as a driver handling the new virtualization instructions exposed by the hardware
  - Requires **hardware assisted** virtualization

http://www.linux-kvm.org

Hypervisor



https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-kvm-intro.html

Hypervisor

- The following packages are usually required for a virtualization host
  - *libvirt:*
    - Provides an interface to KVM, and the libvirtd daemon for managing guest VMs
  - *qemu-kvm:*
    - Installs the QEMU emulator that performs hardware virtualization so that guests can access host CPU and other resources
  - *virt-install:*
    - Provides command line utilities for creating and provisioning guest VMs
  - *virt-viewer:*
    - Provides a graphical utility that can be loaded into a desktop environment to access the graphical console of a guest VM

Virtualization in the Cloud

- Virtualization enables Cloud Computing
- Cloud Virtual Machines run applications inside a guest OS which runs on virtual hardware under the control of a hypervisor
- Issues:
  - VM Configuration
    - Applications to VMs
    - Avoiding over- and under-provisioning
  - VM Placement
    - Also known as VM Scheduling
    - VMs to physical machines

Virtualization in the Cloud

- VM Scheduling
  - Initial placement vs. reallocation
    - Server consolidation
      - Load balancing, increase resource utilization, energy consumption reduction, etc.
    - Live migration
  - NP-hard problem
  - Optimization problem with different objectives
    - Cost, latency, energy, SLA, . . .

Mapping Virtual Machines onto Physical Machines in Cloud Computing: A Survey. ACM, 2016
https://doi.org/10.1145/2983575

References

- Essentials of Cloud Computing, K. Chandrasekaran, Published by CRC Press
  - Chapter 7
- CLOUD COMPUTING TECHNOLOGY. Huawei Technologies Co., Ltd.
  - Chapter 3
- https://www.ibm.com/topics/virtualization
- https://wiki.xenproject.org/wiki/Xen_Project_Software_Overview