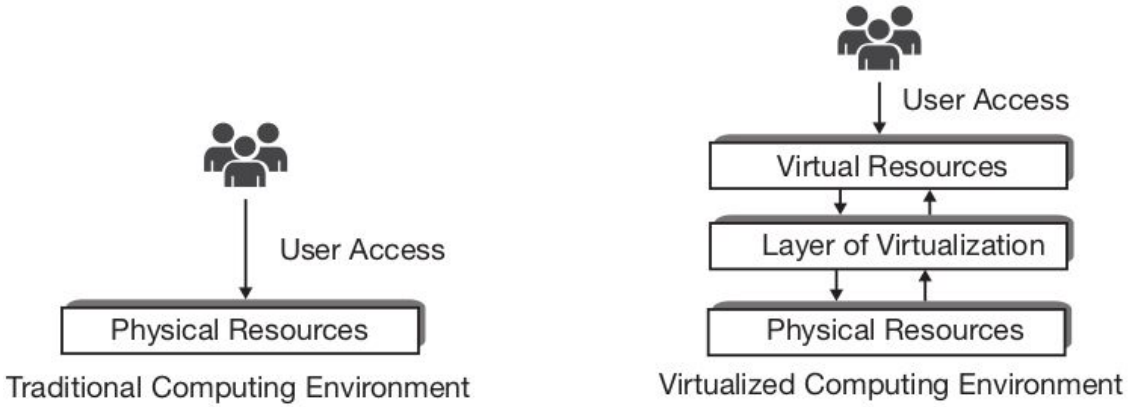
Open Source Software Development

Resource Virtualization

Thái Minh Tuấn - Email: minhtuan@ctu.edu.vn

What Is Virtualization

- The most significant among several enabling technologies of cloud computing
- The representation of physical computing resources in simulated form having made through the software
  - The logical separation of physical resources from direct access of users to fulfill their service needs. Decouples the physical computing resources from direct access of users.

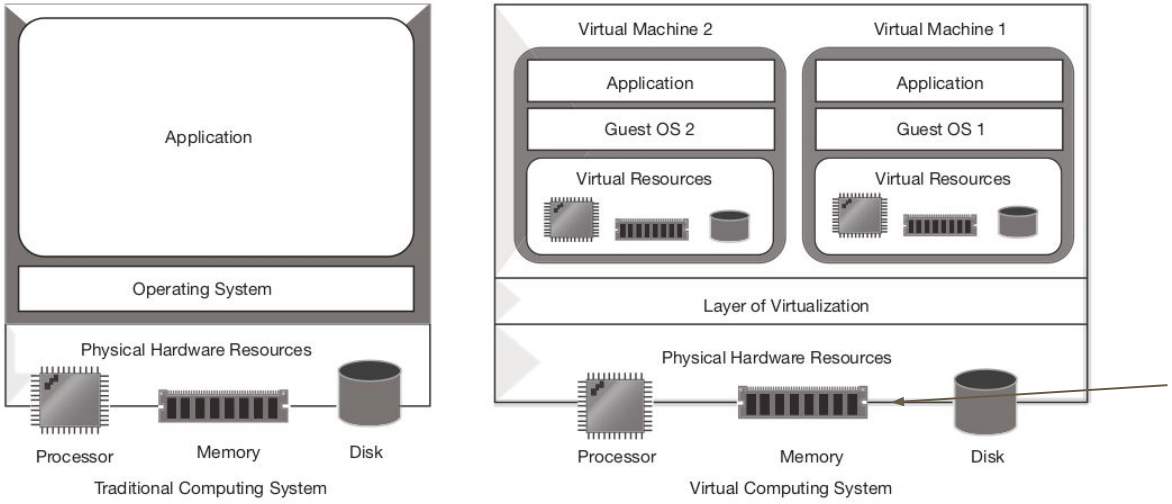


What Is Virtualization

- Any kind of computing resources can be virtualized
  - Processor, memory, storage, network devices, peripheral devices (like keyboard, mouse, printer), etc.
  - In case of core computing resources, a virtualized component can only be operational when a physical resource empowers it from the back end
- The simulated devices produced through virtualization may or may not resemble the actual physical components (in quality, architecture or in quantity)
- Virtual computers (virtual machines) can be built using virtual computing resources produced by virtualization
- Business benefits: Lower hardware cost and improvement in server utilization ratio

Machine Or Server Level Virtualization

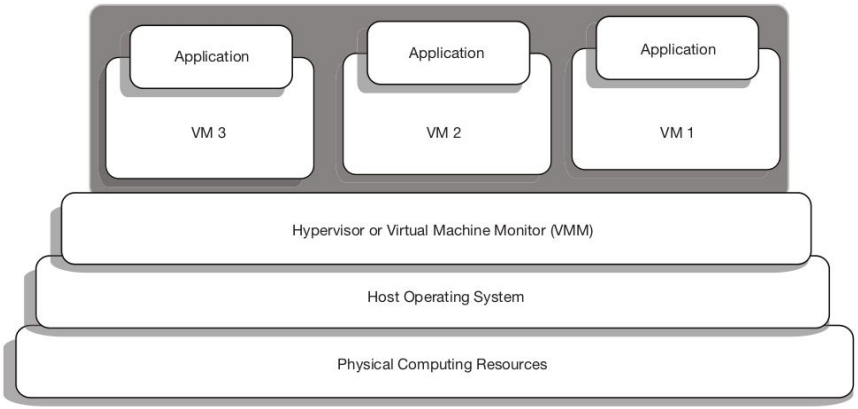
- Machine/server virtualization is the concept of creating virtual machine (guest systems) on actual physical machine (host system)
  - Virtual machines running over a single host system, remain independent of each other
  - Operating systems are installed into those virtual machines

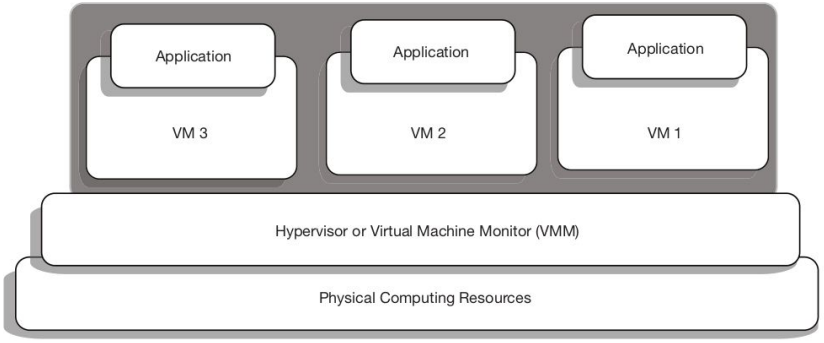


Machine Virtualization Techniques (1/2)

- Hosted approach (Type-2 hypervisor / Hosted hypervisor)
  - VMWare Workstation, VirtualBox, Microsoft Virtual PC, .etc
  - An operating system is first installed on the physical (host) machine
  - The hypervisor is then installed over host OS
  - Compatible for a wide variety of hardware platform, degrade the performance of the virtual machines
- Bare-metal approach: Removal of the Host OS (Type-1 hypervisor / Native Hypervisor)
  - VMware's ESX and ESXi Servers, Microsoft's Hyper-V, Xen
  - The hypervisor is directly installed over the physical machine
  - Provide better performance, advanced features for resource and security management
  - Have limited hardware support and cannot run on a wide variety of hardware platform

Machine Virtualization Techniques (2/2)





Hypervisor Or Virtual Machine Monitor

- Presents a virtual operating platform before the guest systems
- Monitors and manages the execution of guest systems and the VMs
- Allows the sharing of the underlying physical resources among VMs
- Hypervisor-Based Virtualization Approaches:
  - Full Virtualization (native virtualization)
  - Para-Virtualization or OS-Assisted Virtualization
  - Hardware-Assisted Virtualization

Full Virtualization

- The hypervisor fully simulates or emulates the underlying hardware. Virtual machines run over these virtual set of hardware.
- The guest operating systems assume that they are running on actual physical resources and thus remain unaware that they have been virtualized.
- This enables the unmodified versions of available operating systems (like Windows, Linux and else) to run as guest OS over hypervisor.
- In full virtualization technique, the guest operating systems can directly run over hypervisor.

Para(beside/alongside)-Virtualization (1/2)

- Para-virtualization requires hypervisor-specific modifications of guest operating systems.
- A portion of the virtualization management task is transferred (from the hypervisor) towards the guest operating systems. Normal versions of available operating systems need special modification (porting) for this capability inclusion.
  - Each guest OS needs to have prior knowledge that it will run over the virtualized platform, has to know on which particular hypervisor they will have to run.
- Best known example of para-virtualization hypervisor is the open-source Xen project which uses a customized Linux kernel

Para(beside/alongside)-Virtualization (2/2)

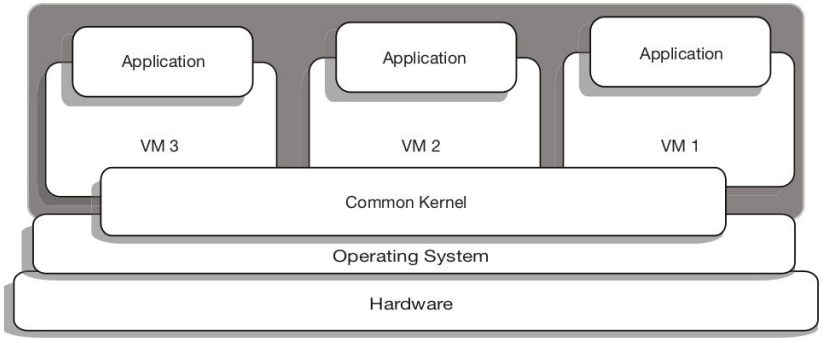
- Reduces the virtualization overhead of the hypervisor as compared to the full virtualization
- The system is not restricted by the device drivers provided by the virtualization software layer
  - Unmodified versions of available operating systems (like Windows or Linux) are not compatible with para-virtualization hypervisors.
  - Modifications are possible in Open-source operating systems (like Linux) by the user. But for proprietary operating systems (like Windows), it depends upon the owner
- Security is compromised in this approach as the guest OS has a comparatively more control of the underlying hardware

Hardware-Assisted Virtualization

- Inspired by software-enabled virtualization, hardware vendors later started manufacturing devices tailored to support virtualization
  - Intel and AMD started this by including new virtualization features in their processors
- The AMD-Virtualization (AMD-V) and Intel Virtualization Technology (Intel-VT): allows some privileged CPU calls from the guest OS to be directly handled by the CPU
- Hardware-assisted virtualization requires explicit features in the host machine's CPU.

Operating System Level Virtualization

- No hypervisor is used and the virtual servers are enabled by the kernel of the operating system of physical machine
- The kernel of the operating system installed over physical system is shared among all of the virtual servers running over it
- Create multiple logically-distinct user-space instances (virtual servers) over a single instance of an OS kernel
- Examples: FreeBSD's jail, Linux VServer (Docker/LXC), OpenVZ



- Advantages: lighter in weight since all of the virtual servers share a single instance of an OS kernel.
- Limitations: All VMs have to use the OS.

Major Server Virtualization Products And Vendors

- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V Server
- Oracle VM VirtualBox
- KVM
- etc.

High-level Language Virtual Machine

- Also known as application VM or process VM
- Against the idea of conventional computing environment where a compiled application is firmly tied to a particular OS and ISA (instruction set architecture)
- Use the porting of compiler by rendering HLLs to intermediate representation targeted towards a*bstract machines*. The abstract machine then translates the intermediate code to physical machine's instruction set
  - Java Virtual Machine (JVM)
  - Microsoft's Common Language Runtime (CLR)

Advantages Of Virtualization

- Better utilization of existing resources
- Reduction in hardware cost
- Reduction in computing infrastructure costs
- Improved fault tolerance or zero downtime maintenance
- Simplified system administration
- Simplified capacity expansion
- Simplified system installation
- Support for legacy systems and applications
- Simplified system-level development
- Simplified system and application testing
- Security

  The benefits of virtualization directly propagate into cloud computing and have empowered it as well.

Downsides Of Virtualization

- Single point of failure problem
- Lower performance issue
- Difficulty in root cause analysis

  The positive impulse of virtualization prevails over the negatives by far

Virtualization Security Threats

- The single point host
- Threats to hypervisor
- Complex configuration
- Privilege escalation
- Inactive virtual machines
- Consolidation of different trust zones

Any virtualization threats can be mitigated by maintaining security recommendations while designing a computing system

Virtualization Security Recommendations

- Hardening virtual machines
- Hardening the hypervisor
- Hardening the host operating system
- Restrictive physical access to the host
- Implementation of single primary function per vm
- Use of secured communications
- Use of separate nic for sensitive vm

Guest OS, hypervisor, host OS and the physical system are the four layers in the architecture of virtualized environment, and for security measures all of these should be considered separately.

Virtualization and Cloud computing (1/2)

- The resources at data center are virtualized and it is usually referred as data center virtualization
  - Pools of resources are created at data centers and a layer of abstraction is created over the pools of various types of physical resources using virtualization
  - Consumers of cloud services can only access the virtual computing resources from the data center
- Data center virtualization provides a way to the cloud system for managing resources efficiently

  Data center virtualization is one foundation of cloud computing.

  Accesses to pooled resources is provided using resource virtualization.

Virtualization and cloud computing (2/2)

- Virtualization is the key enabler of most of the fundamental attributes of cloud computing
  - Shared service: Users remain unaware about the actual physical resources and cannot occupy any specific resource unit while not doing any productive work.
  - Elasticity: With virtualized resources, the underlying capacity of actual resources can be easily altered to meet the varying demand of computation
  - Service orientation: The implementation of service-oriented the architecture becomes easier when virtualization is in place.
  - Metered usage: In cloud computing, the services are billed on usage basis. The accurate measurement of resource consumption has been possible due to use of virtualized resources