Virtualization in Cloud Computing

Chapter 4

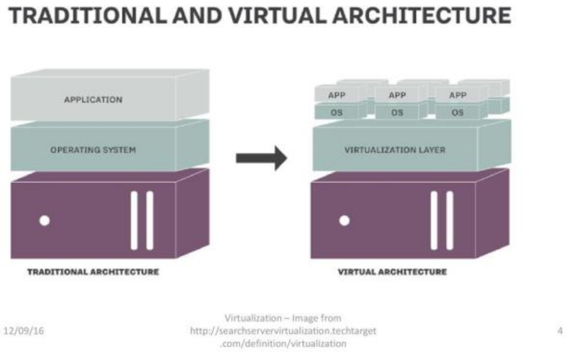
Outline

1. Virtualization
   - Virtualization reference model
   - Virtual machine (VM)
     - Hypervisor
2. Categories of Hypervisor-Based Virtualization
   - Full Virtualization
   - Para-virtualization
3. Types of virtualizations
   - Hardware virtualization
   - Software virtualization
   - Server Virtualization
   - Storage virtualization
4. Containerization

Virtualization

- Process of creating a virtual version of something like - storage, network resource etc
- A technique which allows to share single physical instance of a resource among multiple users or organizations
    - It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand
- With the help of virtualization, multiple operating system and applications can run on same machine and its same hardware at same time increasing the utilization and flexibility of hardware
- Virtualization is **not cloud computing**, but rather a *technology that enables cloud computing* (e.g. resource pooling)

Virtualization



TRADITIONAL AND VIRTUAL ARCHITECTURE

APPLICATION

OPERATING SYSTEM

TRADITIONAL ARCHITECTURE

APP APP APP

OS OS OS

VIRTUALIZATION LAYER

VIRTUAL ARCHITECTURE

12/09/16

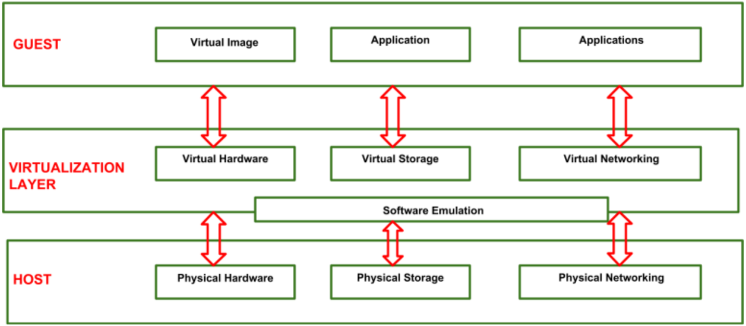
Virtualization – Image from
http://searchservervirtualization.techtarget
.com/definition/virtualization

4

Needs of virtualization

- Purchasing Many Machines For Different purposes (costly)
- Setting up them on Network and connecting them (Adding the new machine or server)
    - no need of any installation process
- No need to provide extra
    - Electricity
    - Networking facility
    - Floor space

Virtualization reference model



Three major components fall under this category in a virtualized environment:

- Guest
- Host
- Virtualization layer

Virtualization reference model

Host

- The host represents the original environment where the guest is supposed to be managed
- Each guest runs on the host using shared resources donated to it by the host
- The operating system, works as the host and manages the physical resource management, and the device support

Virtualization layer

- The virtualization layer is responsible for recreating the same or a different environment where the guest will operate
- It is an additional abstraction layer between a network and storage hardware, computing, and the application running on it
- Usually it helps to run a single operating system per machine which can be very inflexible compared to the usage of virtualization.

Virtualization reference model

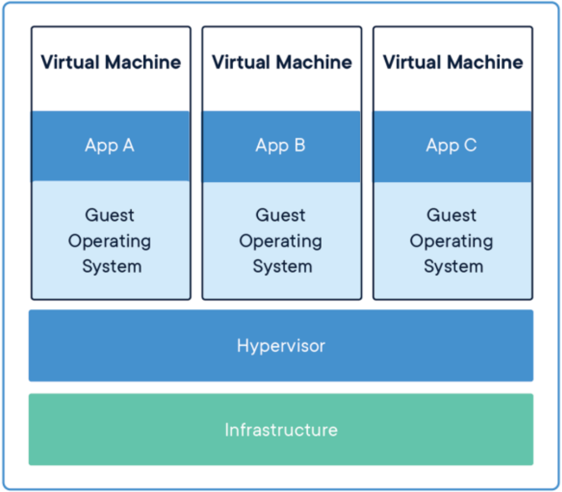
Guest

- The guest represents the system component that interacts with the virtualization layer rather than with the host
- Guests usually consist of one or more virtual disk files, and a VM definition file
- Virtual Machines are centrally managed by a host application that sees and manages each virtual machine as a different application

Virtual machine (VM)

- A virtual machine (VM) is a virtual representation of a physical computer
- Virtualization allows an organization to create multiple virtual machines - *each with their own operating system (OS) and applications* on a single physical machine
- A virtual machine can't interact directly with a physical computer
    - It requires a lightweight software layer called a **hypervisor** to coordinate with the physical hardware upon which it runs
- **Public cloud** services are using virtual machines to provide virtual application resources to multiple users at once, for even more cost efficient and flexible compute
- VMs can perform specific tasks considered **too risky** to carry out in a <u>host environment</u>, such as accessing virus-infected data or testing operating systems
    - The VM is separated from the rest of the system, the software inside the virtual machine cannot tamper with the host computer

Virtual Machine



Virtual Machine
App A
Guest Operating System

Virtual Machine
App B
Guest Operating System

Virtual Machine
App C
Guest Operating System

Hypervisor

Infrastructure

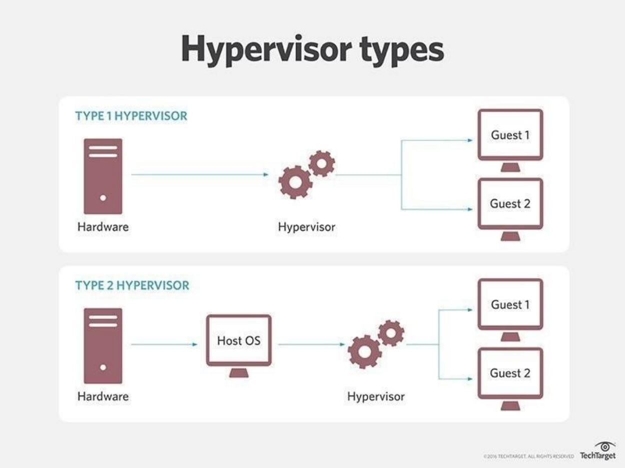
Benefits of Virtual Machine

- Save energy (less servers are running), go green
- Reduce the data center footprint
- Create virtual lab environments
- Reduce hardware vendor lock-in
- Improve disaster recovery
- Isolate applications (from each other)
- Extend the life of older applications
- Easy migrate (Help move things to the cloud)

Hypervisor

- It is a software layer that can supervisor and virtualize the resources of a host machine conferring to the user requirements
- It is an middling layer between operating system and hardware
- The hypervisor allocates only the amount of necessary resources for an instance to be fully functional
- Classified as
  - **Native (Bare Metal or Type 1):** based hypervisor runs directly on the hardware
  - **Host (Type 2):** based hypervisor runs on the host operating system

Hypervisor type

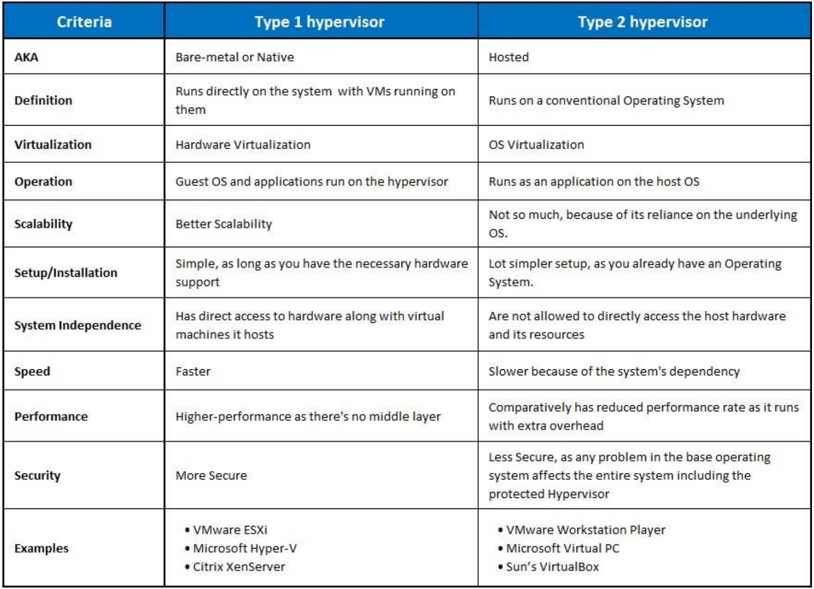


Type 1 Hypervisor

- A bare-metal hypervisor is a layer of software, which is install directly on top of a physical server and its underlying hardware
  - On top of type 1 hypervisors, virtual machines run
- There is no software or any operating system in between, hence the name bare-metal hypervisor
- Proven in providing **excellent performance** and stability since it does not run inside any operating system
- The physical machine with Type 1 hypervisor: serves virtualization purposes only
  - cannot use it for anything else
- Type 1 hypervisors are mainly found in enterprise environments
- Highly secure: an attack on a guest VM is logically isolated to that VM and can't spread to others running on the same hardware

Type 2 Hypervisor

- A Type 2 hypervisor is typically installed on top of an existing OS of host machine.
- Mainly used for personal use and small development
  - not used for data center computing
  - used where performance and security are lesser concerns



Criteria	Type 1 hypervisor	Type 2 hypervisor
AKA	Bare-metal or Native	Hosted
Definition	Runs directly on the system with VMs running on them	Runs on a conventional Operating System
Virtualization	Hardware Virtualization	OS Virtualization
Operation	Guest OS and applications run on the hypervisor	Runs as an application on the host OS
Scalability	Better Scalability	Not so much, because of its reliance on the underlying OS.
Setup/Installation	Simple, as long as you have the necessary hardware support	Lot simpler setup, as you already have an Operating System.
System Independence	Has direct access to hardware along with virtual machines it hosts	Are not allowed to directly access the host hardware and its resources
Speed	Faster	Slower because of the system's dependency
Performance	Higher-performance as there's no middle layer	Comparatively has reduced performance rate as it runs with extra overhead
Security	More Secure	Less Secure, as any problem in the base operating system affects the entire system including the protected Hypervisor
Examples	• VMware ESXi • Microsoft Hyper-V • Citrix XenServer	• VMware Workstation Player • Microsoft Virtual PC • Sun's VirtualBox

How Hypervisors Enable the Benefits of Virtualization?

- As software, hypervisors decouple the OS and apps from the physical host
  - This decoupling provides an array of benefits, including the ability to easily and **quickly migrate** the VM from one host to another without disruption
- Virtualization enables cost savings through reducing physical footprint, which in turn reduces costs for electricity, cooling, and maintenance
- Virtualization also greatly improves agility and speed in delivering IT services
  - For example, it is far easier to spin up a VM than to provision new environments to satisfy customer requests

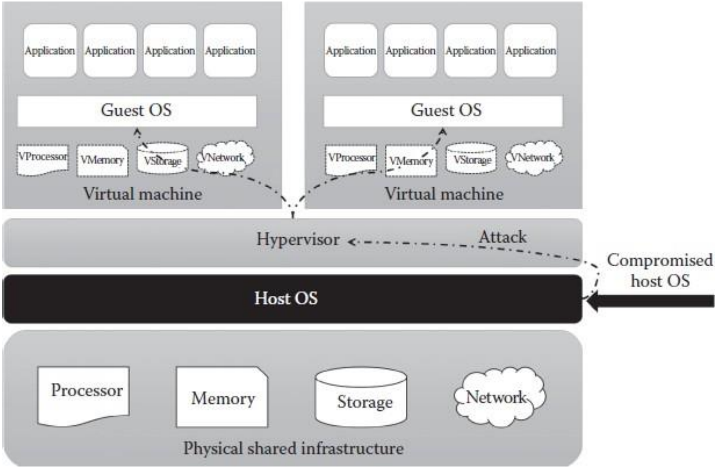
Security Issues and Recommendations

- The hypervisor creates a virtual environment in the data centers
- In a virtualized environment, hypervisor is the higher authority entity that has the direct access to the hardware
  - most of the attackers will target the hypervisor as an entry point to attack the system
- In bare metal hypervisor: very difficult to perform the attack as it is deployed directly on the hardware
- In hosted hypervisors: more vulnerable to the attacks as hypervisors are running on top of the host OSs.
- There are two possibilities of attacking the hypervisor:
  1. Through the host OS
  2. Through the guest OS

Through the host OS

- Attacks from the host OS can be performed by **exploiting the vulnerabilities** of the host OS
- Once the OS gets compromised, the attackers have full control over
  - actual hardware
  - the applications running on top of the OS
- The attacker can do the following malicious activities:
  - Denial of service attack, where the attacker can deny the virtual resources when there is a request from the new VM
  - Stealing the confidential information that is stored in the VMs

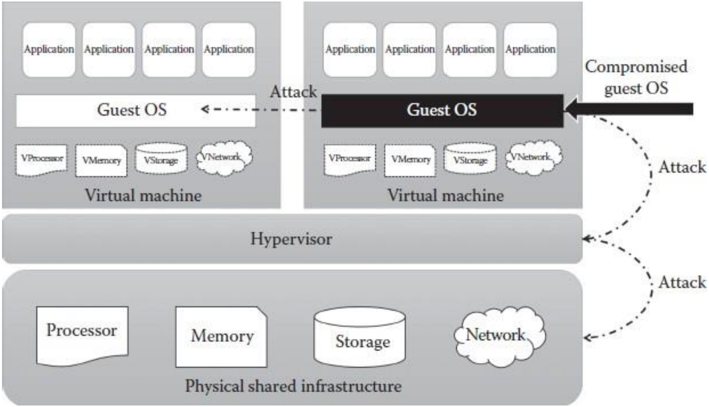
Through the host OS



Through the guest OS

- The guest OS is communicating with the hypervisor to get virtual resources, any malicious code from the guest OS or VMs can compromise the hypervisor
- The attacker will try to attack or compromise the hypervisor from the malicious VMs
- Once the hypervisor gets compromised by the guest OS or malicious VMs, it can misuse the hypervisor’s high privilege on the hardware
- After the hypervisor gets compromised, the attacker can do the following malicious activities:
    - Get unauthorized access to the other VMs that share the physical hardware
    - Attacker can utilize the hardware resources fully to launch resource exhaustion attacks, etc

Through the guest OS



Recommendations to avoid hypervisor attacks

- Update the hypervisor software and the host OS regularly.
- Disconnect the unused physical resources from the host system or hypervisor.
- Enable the least privilege to the hypervisor and guest OS to avoid attacks through unauthorized access.
- Deploy the monitoring tools in the hypervisor to detect/prevent malicious activities.
- Strong guest isolation.
- Employ mandatory access control policies.

Virtualization as a Concept of Cloud Computing

Virtualization is considered to be the backbone of cloud computing because of the following features:

- **Partitioning:** Virtualization technology divides the available resources into multiple partitions and provides the allocation of resources and applications in the virtual form among multiple users or organizations.
- **Isolation:** Virtualization keeps all virtual versions isolated from each other on single physical resources
    - crashing of one VM doesn't affect another one
- **Scalability:** The feature of scaling up and down the resources as per the demands of the customers
    - essential characteristic of virtualization
    - enables the efficient growth of a business
- **Flexibility:** Enables the availability of resources or applications to multiple clients or organizations at the same time.

Virtualization in Cloud Computing

- **Security:** Virtualization provides a high level of security and protection for guest machines
  - uses firewalls and encryption to ensure the security of data and applications
  - protects the host machine from any harm or damage caused by the guest machines

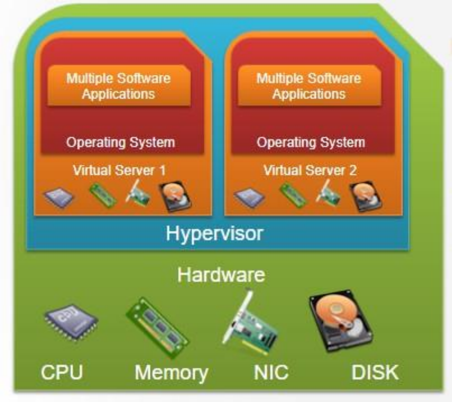
Categories of Hypervisor-Based Virtualization

1. Full Virtualization
2. Para-virtualization
3. Hardware-assisted Virtualization

Full Virtualization

- Hypervisor that fully simulates or emulates the simulation of the underlying hardware
- In this VM, the application runs on the top of the guest operating system
  - Each guest server runs on its own operating system
- Guest OS is not aware that it is being virtualized
  - It sends commands directly to the simulated hardware
- In this model, it is the responsibility of the hypervisor to handle all guest OS to physical hardware requests during running of guest machines
- Provides the features of isolation and security to virtual machines and provides the virtual machines with all the services of a physical system
- Very popular and cost-efficient virtualization
- Complex and lower due to emulation
- Installation of the new device driver is difficult.

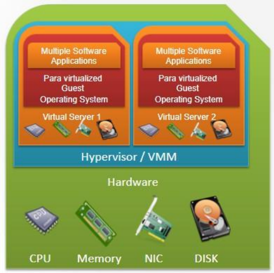
Full virtualization



OS assisted/Para-virtualization

- A modified and recompiled version of the guest operating system is made to run in the virtual machine
- A portion of the virtualization management task is transferred (from the hypervisor) towards the guest operating systems
  - Need for modifying the guest operating system is to minimize the execution time performing operations
  - Hardware uses an application known as **Application Programming Interface (API)** that helps in modifying guest OSs.
- Guest OS is aware of the fact that it is a guest
- Para-virtualization allows calls from guest OS to directly communicate with hypervisor (without any binary translation of instructions)
  - 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
  - guest operating systems contain the required device drivers

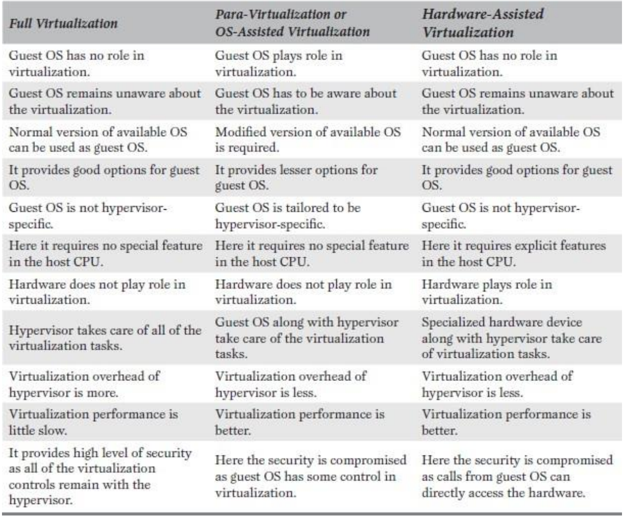
Para-virtualization


Multiple Software Applications
Para virtualized Guest Operating System
Virtual Server 1
Multiple Software Applications
Para virtualized Guest Operating System
Virtual Server 2
Hypervisor / VMM
Hardware
CPU
Memory
NIC
DISK

- 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
- Security is compromised in this approach as the guest OS has comparatively more control of the underlying hardware

Hardware assisted virtualization

- Virtualization that makes use of the computer’s hardware as architectural support to build and manage a fully virtualized virtual machine
- The virtual machines are created using hardware instead of software as it is more efficient to implement virtualization functions using hardware capabilities.
- Many Hypervisors are overhead because of trapping and Emulation of I/O Operations, and status instructions get executed and processed within the guest OS
- In hardware-assisted type, the hypervisor sends the call to the processor.
    - processor’s job is to create and maintain the virtual machines
    - which reduces the overhead on the system and enables the host system to host a large number of VMs
- increases the performance of VMs



Full Virtualization	*Para-Virtualization or OS-Assisted Virtualization*	*Hardware-Assisted Virtualization*
Guest OS has no role in virtualization.	Guest OS plays role in virtualization.	Guest OS has no role in virtualization.
Guest OS remains unaware about the virtualization.	Guest OS has to be aware about the virtualization.	Guest OS remains unaware about the virtualization.
Normal version of available OS can be used as guest OS.	Modified version of available OS is required.	Normal version of available OS can be used as guest OS.
It provides good options for guest OS.	It provides lesser options for guest OS.	It provides good options for guest OS.
Guest OS is not hypervisor-specific.	Guest OS is tailored to be hypervisor-specific.	Guest OS is not hypervisor-specific.
Here it requires no special feature in the host CPU.	Here it requires no special feature in the host CPU.	Here it requires explicit features in the host CPU.
Hardware does not play role in virtualization.	Hardware does not play role in virtualization.	Hardware plays role in virtualization.
Hypervisor takes care of all of the virtualization tasks.	Guest OS along with hypervisor take care of the virtualization tasks.	Specialized hardware device along with hypervisor take care of virtualization tasks.
Virtualization overhead of hypervisor is more.	Virtualization overhead of hypervisor is less.	Virtualization overhead of hypervisor is less.
Virtualization performance is little slow.	Virtualization performance is better.	Virtualization performance is better.
It provides high level of security as all of the virtualization controls remain with the hypervisor.	Here the security is compromised as guest OS has some control in virtualization.	Here the security is compromised as calls from guest OS can directly access the hardware.

Types of virtualization

- Hardware virtualization
- Software Virtualization
- Server Virtualization
- Storage Virtualization

Hardware virtualization

- Creation of virtual physical hardware resources so that multiple users can access the hardware resources at the same time
- In hardware virtualization, the virtual machine software is directly installed on the hardware system: **bare-metal virtualization**
- A virtual machine is created over the existing operating system and hardware: **host virtualization**
- Once the hardware virtualization is done, it is appropriate to install different operating systems and run various applications on them
- **Usage:** Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server

Advantages of Hardware Virtualization

- It is very efficient in utilizing the resources.
- Uptime is significantly increased.
- It is very cost-effective and economical.
- Hardware and software redundancy.

Software virtualization

- Creates a multi-virtual environment on the host machine using the same set of hardware
  - same as virtualization
- Purpose of software virtualization is to emulate the whole computer system and allow the guest operating system to run on it
- An effective way for businesses and organizations to manage and implement applications
  - Administrators install the application on the centralized server instead of locally on each desktop computer
- Ensures the security of sensitive information in case of data is lost or stolen as all the information gets stored on the server

Types of Software Virtualization

1. **OS Virtualization:**
   - Multiple operating systems can run on a single set of hardware resources
   - Each of the operating system perform their task efficiently and do not interfere with each other's work
2. **Application Virtualization:**
   - Virtualization method where users can remotely access their applications on the central server
   - It helps to run multiple applications at the same time by building a virtual environment
3. **Service Virtualization:**
   - Emulates the behaviour of essential components which will be present in the final production environment
   - With the help of service virtualization, the complex application can go through testing much earlier in the development process
     - Technique to simulate the behaviors of components in the form of combination component-based applications

Advantages of Software Virtualization

1. **Testing:**
   - Easier to test the new operating system and software on VMs as it does not require any additional hardware and the testing can do within the same software
2. **Utilization:**
   - VM can modify as per the requirement such as the user can modify ram, drive space, etc
     - higher efficiency in resource utilization
   - It requires very less amount of hardware as compared to the equivalent number of physical machines
3. **Flexible:**
   - It provides flexibility to the user so that the user can modify the software as per their demand
   - The modification can do within minutes and can adjust easily when the workload changes

Advantages of Software Virtualization

4. **Secure:**
   - It can protect from any attacks
     - several firewalls is used to prevent hacking and virus
   - The data in the software virtualization is safe as it stores in several different places so if the disaster takes place the data can retrieve easily.
5. **Less Downtime:**
   - The software is upgrading and the upgrade in the VMs can do when the VM is working
   - VM can modify when it is working or it is not working which means that the downtime of it is very less.
6. **Running multiple operating systems and software:**
   - Enables the system to run more than one operating system by dividing the hard drive into partitions
   - Also allows keeping different versions of software
     - different versions can be placed in one system, it is much easier to migrate from one version of software to another

Server Virtualization

- Server virtualization means dividing the physical server into multiple virtual servers
    - Server administrators use virtualization software to partition the single physical server into multiple isolated virtual environments
- Each of the virtual environments can run independently without interfering with the working of each other
- Enables organizations to cut down on the hardware resources used by them which leads to cost efficiency

Types of server virtualization

1. **Full Virtualization:** interfaces directly with a physical server
   - The hypervisor **maintains track** of the actual Server's resources while keeping each virtual Server separate and oblivious to the others
   - Also transmits resources from the real Server to the appropriate virtual server as it executes programs
2. **Para-Virtualization:**
   - each operating system on the virtual servers is aware of one another through para-virtualization, the hypervisor can manage the operating systems with less computing power
3. **OS-Level Virtualization:** basic form of server virtualization is OS-level virtualization
   - Using OS-level virtualization, there is no need for a hypervisor
   - The duty of managing resources and separating virtual machines is instead handled by the physical server's operating system
   - drawback: each virtual machine will have to run the same operating system, because the OS is acting as a hypervisor

Advantages of server virtualization

1. **Cost efficient:**
   - Organizations do not need to invest a lot of money in buying physical servers and resources
   - All resources are available virtually
2. **Improved efficiency:**
   - Multiple virtual servers are used in place of one physical server
   - This makes the system more efficient as multiple tasks can be completed at the same time.
3. **Independent environment for users:**
   - Enables each virtual server to run independently of the other
   - Every user is given an isolated environment to work on
   - No interference is made from other users
4. **Reduced need for physical infrastructure**
5. **Reduced energy consumption**

Storage virtualization

- The single storage system is partitioned into multiple logical storage forms and assigned to each customer
- The logical storage works like real physical storage space and appears to the server or the host as physical storage devices
- The data stored by users on this virtual storage devices get stored on the cloud only and ensure the safety and protection of data
- Users do not have any idea about where all their data gets stored on the server but they can access it using the logical path

Containerization

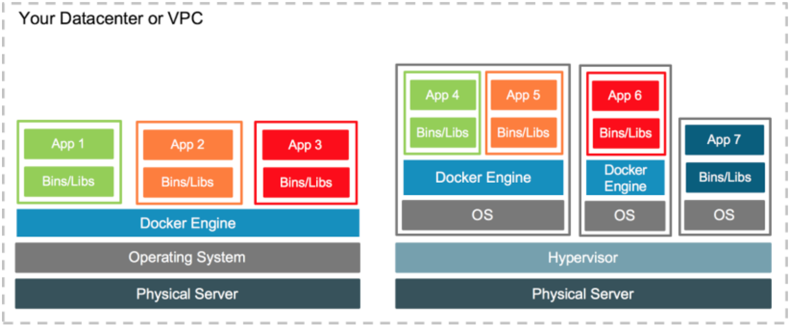
- Containerization is the packaging of software code with just the operating system (OS) libraries and dependencies required to run the code to create a single lightweight executable—called a container—that runs consistently on any infrastructure
- With traditional methods, code is developed in a specific computing environment which, when transferred to a new location, often results in bugs and errors
  - For example, when a developer transfers code from a desktop computer to a VM or from a Linux to a Windows operating system
- Containerization eliminates: by bundling the application code together with the related configuration files, libraries, and dependencies required for it to run
- Containers share the machine's operating system kernel and do not require the overhead of associating an operating system within each application
  - referred as lightweight

Benefits of containerization

- Lighter weight: Containers don't carry the payload of an entire OS instance and hypervisor. They include only dependencies necessary to execute the code
- Portability: A container creates an executable package of software that is abstracted away from the host operating system
- Speed: share the machine's operating system (OS) kernel and speed up start-times as there is no operating system to boot
- Fault isolation: Each containerized application is isolated and operates independently of others

Docker engine

- an open source platform that enables developers to build, deploy, run, update and manage containers



Self-Study

Kubernetes