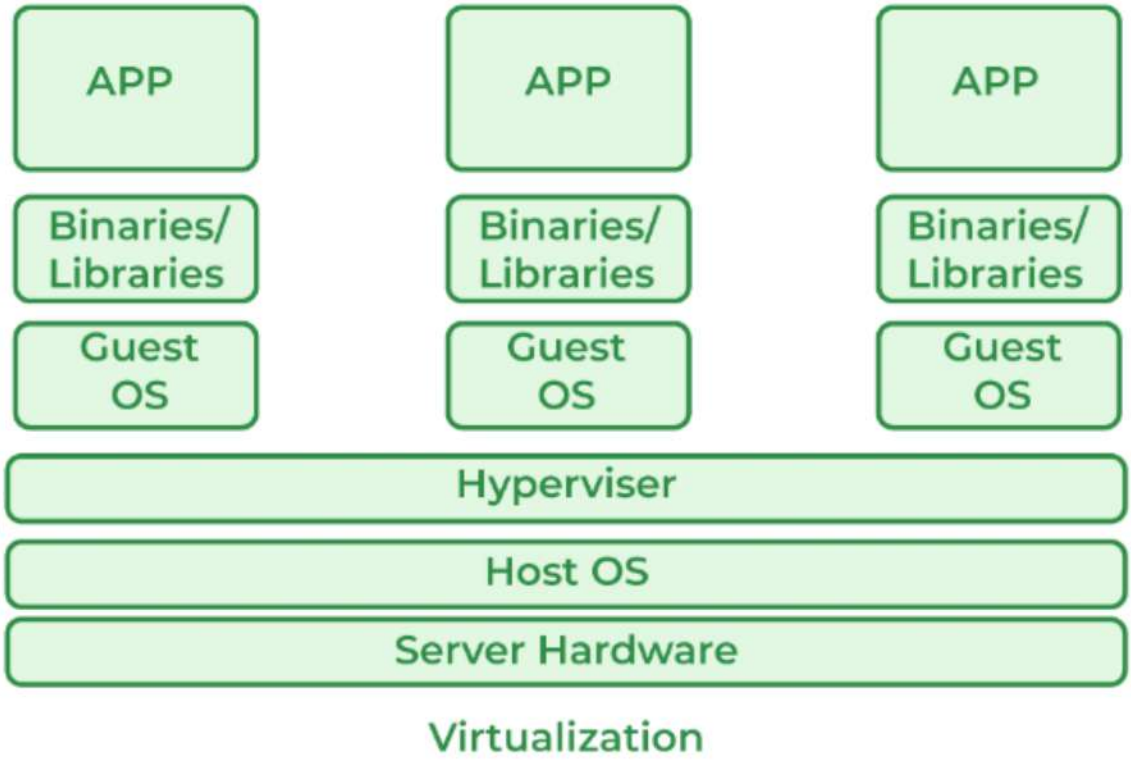
3 Cloud Virtualization Technology

3.1 Overview of Virtualization Techniques

- Virtualization is the "creation of a virtual (rather than actual) version of something, such as aserver, a desktop, a storage device, an operating system or network resources".
- Virtualization is a technique, which allows to share a single physical instance of aresource or an application among multiple customers and organizations. It does by assigning alogical name to a physical storage and providing a pointer to that physical resource when demanded.
- Virtualization is a technique how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.
- In other words, one of the main cost-effective, hardware-reducing, and energy-saving techniques used by cloud providers is Virtualization. Virtualization allows sharing of a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.

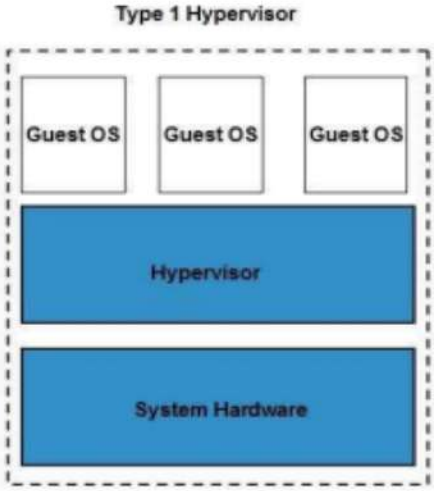


Virtualization

- The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine.**
- This virtual machine is managed by a software or firmware, which is known as **hypervisor**.

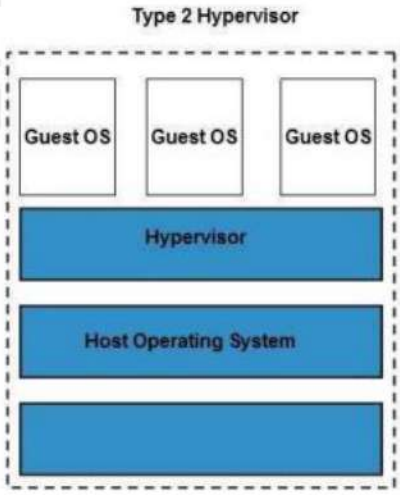
Hypervisor

- The hypervisor is a firmware or low-level program that acts as a Virtual Machine Manager. There are two types of hypervisor:
  - Type 1 hypervisor executes on bare system. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogic VLX are examples of Type 1 hypervisor. The following diagram shows the Type 1 hypervisor.



The type1 hypervisor does not have any host operating system because they are installed on a bare system.

  - Type 2 hypervisor is a software interface that emulates the devices with which a system normally interacts. Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMWare workstation 6.0 are examples of Type 2 hypervisor. The following diagram shows the Type 2 hypervisor.



Work of Virtualization in Cloud Computing

- Virtualization has a prominent impact on Cloud Computing. In the case of cloud computing, users store data in the cloud, but with the help of Virtualization, users have the extra benefit of sharing the infrastructure. Cloud Vendors take care of the required physical resources, but these cloud providers charge a huge amount for these services which impacts every user or organization. Virtualization helps Users or Organizations in maintaining those services which are required by a company through external (third-party) people, which helps in reducing costs to the company. This is the way through which Virtualization works in Cloud Computing.

3.1.1 Benefits of Virtualization

- More flexible and efficient allocation of resources.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.
- Remote access and rapid scalability.
- High availability and disaster recovery.
- Pay peruse of the IT infrastructure on demand.
- Enables running multiple operating systems.

3.1.2 Drawback of Virtualization

- **High Initial Investment:** Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
- **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
- **Risk of Data:** Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.

3.1.3 Characteristics of Virtualization

- **Increased Security:** The ability to control the execution of a guest program in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment. All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
- **Managed Execution:** In particular, sharing, aggregation, emulation, and isolation are the most relevant features.
- **Sharing:** Virtualization allows the creation of a separate computing environment within the same host.
- **Aggregation:** It is possible to share physical resources among several guests, but virtualization also allows aggregation, which is the opposite process.

3.2 Types of Virtualization

- There are various types of virtualization in cloud computing, each serving different purposes. Here are the some main types of virtualization in cloud computing:

1. **Server Virtualization:**
   - Server virtualization involves running multiple virtual machines (VMs) on a single physical server. Each VM operates independently and can run different operating systems and applications. Hypervisors, such as VMware vSphere, Microsoft Hyper-V, and KVM, manage these VMs. Server virtualization is widely used in IaaS (Infrastructure as a Service) cloud environments.
   - Benefits:
     - Improved server utilization.
     - Isolation between VMs.
     - Easy backup and migration.
     - Resource allocation and scaling.
2. **Network Virtualization:**
   - Network virtualization abstracts the physical network infrastructure, allowing multiple virtual networks to coexist on the same physical network. Software-defined networking (SDN) and network virtualization platforms like VMware NSX and Cisco ACI enable network virtualization. This is essential for multi-tenancy and network isolation in cloud environments.
   - Benefits:
     - Isolation of network traffic.
     - Dynamic network provisioning.

- Simplified network management.
- Improved security and quality of service.

3. **Storage Virtualization:**

- Storage virtualization abstracts physical storage devices and presents them as a single, virtualized storage pool. This enables efficient storage management, data replication, and disaster recovery. Technologies like Storage Area Networks (SAN) and Network Attached Storage (NAS) often employ storage virtualization.
- Benefits:
  - Better storage utilization.
  - Simplified data management.
  - Data redundancy and fault tolerance.
  - Efficient backup and recovery.

4. **Desktop Virtualization (VDI - Virtual Desktop Infrastructure):**

- Desktop virtualization allows users to access their desktop environments remotely from various devices. It involves running multiple virtual desktops on a centralized server or cloud infrastructure. Popular desktop virtualization solutions include VMware Horizon, Citrix Virtual Apps and Desktops, and Microsoft Remote Desktop.
- Benefits:
  - Centralized management and updates.
  - Enhanced security and data protection.
  - Support for remote work and BYOD.
  - Efficient resource allocation.

5. **Application Virtualization:**

- Application virtualization decouples software applications from the underlying operating system, making them portable across different platforms. This allows applications to run in isolation without interfering with other applications or the host OS. Popular application virtualization technologies include Docker and Kubernetes containers.
- Benefits:
  - Simplified application deployment.
  - Portability and consistency.
  - Resource efficiency.
  - Scalability.

6. **Hardware Virtualization:**

- Hardware virtualization is an essential component of server virtualization. It involves the use of a hypervisor to create multiple virtual instances (VMs) on a single physical server. Each VM is isolated and has its own virtualized hardware resources, including CPU, memory, and storage.
- Benefits:
  - Efficient resource allocation.
  - Isolation and security.
  - Improved hardware utilization.
  - Simplified management.

7. **Storage Virtualization:**

- Storage virtualization abstracts physical storage resources into a virtual storage pool, which can be allocated and managed dynamically. This technology simplifies storage management, improves scalability, and enhances data protection and disaster recovery.
- Benefits:
  - Centralized and simplified storage management.
  - Dynamic provisioning of storage resources.
  - Enhanced data redundancy and failover capabilities.

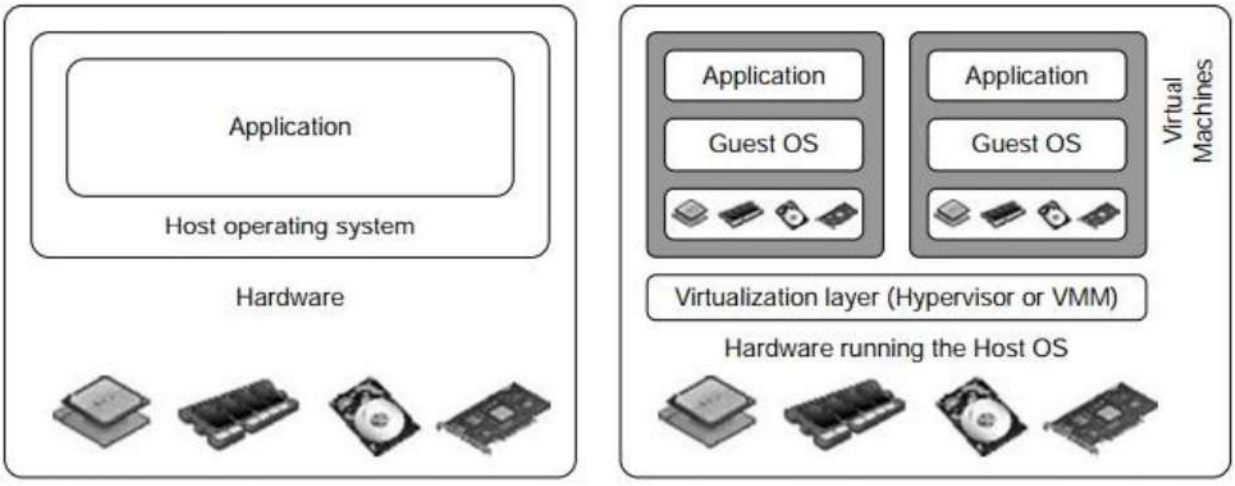
- Efficient data backup and recovery.

8. Security Virtualization:

- Security virtualization involves isolating security functions and policies into separate virtual instances. This helps improve security and compliance, especially in multi-tenant cloud environments. Virtualized security components can include firewalls, intrusion detection systems, and encryption services.
- Benefits:
  - Enhanced security for cloud services and applications.
  - Isolation of security policies and controls.
  - Scalability and adaptability of security measures.
  - Improved compliance and auditing capabilities.

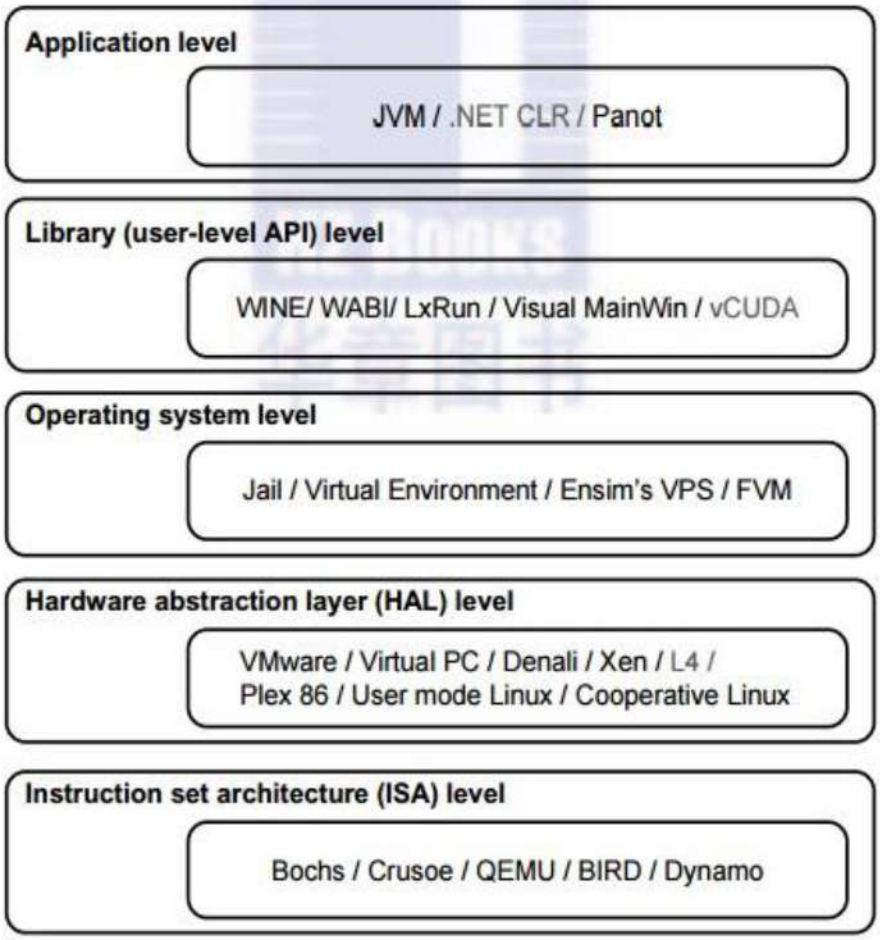
3.3 Implementation Level of Virtualization

- A traditional computer runs with a host operating system specially tailored for its hardware architecture, as shown in Figure a. After virtualization, different user applications managed by their own operating systems (guest OS) can run on the same hardware, independent of the host OS. This is often done by adding additional software, called a virtualization layer as shown in Figure b. This virtualization layer is known as hypervisor or virtual machine monitor (VMM). The VMs are shown in the upper boxes, where applications run with their own guest OS over the virtualized CPU, memory, and I/O resources.



(a) Traditional computer (b) After virtualization

- The main function of the software layer for virtualization is to virtualize the physical hardware of a host machine into virtual resources to be used by the VMs, exclusively. This can be implemented at various operational levels, as we will discuss shortly. The virtualization software creates the abstraction of VMs by interposing a virtualization layer at various levels of a computer system. Common virtualization layers include the instruction set architecture (ISA) level, hardware level, operating system level, library support level, and application level.



1. **Instruction Set Architecture Level (ISA)**

- ISA virtualization can work through ISA emulation. This is used to run many legacy codes that were written for a different configuration of hardware. These codes run on any virtual machine using the ISA. With this, a binary code that originally needed some additional layers to run is now capable of running on the x86 machines. It can also be tweaked to run on the x64 machine. With ISA, it is possible to make the virtual machine hardware agnostic. For the basic emulation, an interpreter is needed, which interprets the source code and then converts it into a hardware format that can be read. This then allows processing. This is one of the five implementation levels of virtualization in cloud computing.

2. **Hardware Abstraction Level (HAL)**

- True to its name HAL lets the virtualization perform at the level of the hardware. This makes use of a hypervisor which is used for functioning. At this level, the virtual machine is formed, and this manages the hardware using the process of virtualization. It allows the virtualization of each of the hardware components, which could be the input-output device, the memory, the processor, etc. Multiple users will not be able to use the same hardware and also use multiple virtualization instances at the very same time. This is mostly used in the cloud-based infrastructure.

3. **Operating System Level**

- At the level of the operating system, the virtualization model is capable of creating a layer that is abstract between the operating system and the application. This is an isolated container that is on the operating system and the physical server, which makes use of the software and hardware. Each of these then functions in the form of a server. When there are several users, and no one wants to share the hardware, then this is where the virtualization level is used. Every user will get his virtual environment using a virtual hardware resource that is dedicated. In this way, there is no question of any conflict.

4. **Library Level**

- The operating system is cumbersome, and this is when the applications make use of the API that is from the libraries at a user level. These APIs are documented well, and this is why the library virtualization level is preferred in these scenarios. API hooks make it possible as it controls the link of communication from the application to the system.

5. **Application Level**

- The application-level virtualization is used when there is a desire to virtualize only one application and is the last of the implementation levels of virtualization in cloud computing. One does not need to virtualize the entire environment of the platform.
- This is generally used when you run virtual machines that use high-level languages. The application will sit above the virtualization layer, which in turn sits on the application program.
- It lets the high-level language programs compiled to be used in the application level of the virtual machine run seamlessly.

3.4 Server Virtualization

- Server Virtualization is the process of dividing a physical server into several virtual servers, called virtual private servers. Each virtual private server can run independently.
- The concept of Server Virtualization widely used in the IT infrastructure to minimizes the costs by increasing the utilization of existing resources.
- Server Virtualization is the partitioning of a physical server into a number of small virtual servers, each running its own operating system. These operating systems are known as guest operating systems. These are running on another operating system known as the host operating system. Each guest running in this manner is unaware of any other guests running on the same host. Different virtualization techniques are employed to achieve this transparency.

Types of Server virtualization :

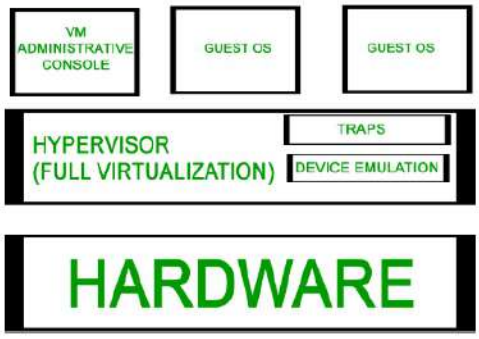
1. **Hypervisor**

- In the Server Virtualization, Hypervisor plays an important role. It is a layer between the operating system (OS) and hardware. There are two types of hypervisors.
  - Type 1 hypervisor (also known as bare metal or native hypervisors)
  - Type 2 hypervisor (also known as hosted or Embedded hypervisors)
- The hypervisor is mainly used to perform various tasks such as allocate physical hardware resources (CPU, RAM, etc.) to several smaller independent virtual machines, called "guest" on the host machine.
- A Hypervisor or VMM(virtual machine monitor) is a layer that exists between the operating system and hardware. It provides the necessary services and features for the smooth running of multiple operating systems.
- It identifies traps, responds to privileged CPU instructions, and handles queuing, dispatching, and returning the hardware requests. A host operating system also runs on top of the hypervisor to administer and manage the virtual machines.

2. **Full Virtualization**

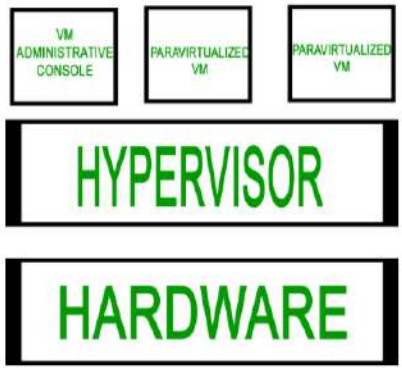
- Full Virtualization uses a hypervisor to directly communicate with the CPU and physical server. It provides the best isolation and security mechanism to the virtual machines.
- The biggest disadvantage of using hypervisor in full virtualization is that a hypervisor has its own processing needs, so it can slow down the application and server performance.
- **VMWare ESX** server is the best example of full virtualization.
- Advantages:
  - No modification to the Guest operating system is required.
- Limitations:
  - Complex

- Slower due to emulation
- Installation of the new device driver is difficult.



3. Para Virtualization

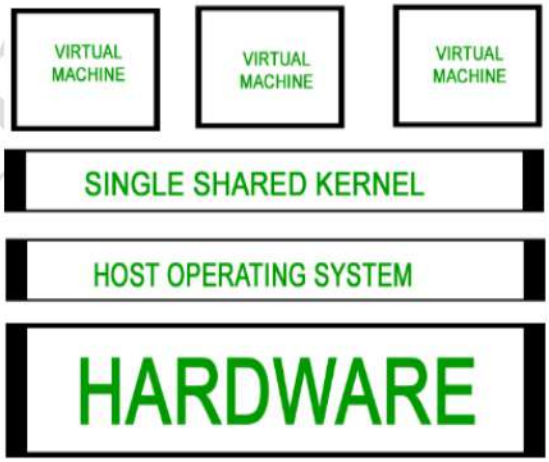
- Para Virtualization is quite similar to the Full Virtualization. The advantage of using this virtualization is that it is easier to use, Enhanced performance, and does not require emulation overhead. Xen primarily and UML use the Para Virtualization.
- The difference between full and pare virtualization is that, in para virtualization hypervisor does not need too much processing power to manage the OS.
- It is based on Hypervisor. Much of the emulation and trapping overhead in software implemented virtualization is handled in this model. The guest operating system is modified and recompiled before installation into the virtual machine.
- Due to the modification in the Guest operating system, performance is enhanced as the modified guest operating system communicates directly with the hypervisor and emulation overhead is removed.
- Example: Xen primarily uses Paravirtualization, where a customized Linux environment is used to support the administrative environment known as domain 0.
- Advantages:
  - Easier
  - Enhanced Performance
  - No emulation overhead
- Limitations:
  - Requires modification to a guest operating system



4. Operating System Virtualization

- Operating system virtualization is also called as system-lever virtualization. It is a server virtualization technology that divides one operating system into multiple isolated user-space called virtual environments. The biggest advantage of using server visualization is that it reduces the use of physical space, so it will save money.
- Linux OS Virtualization and Windows OS Virtualization are the types of Operating System virtualization.
- FreeVPS, OpenVZ, and Linux Vserver are some examples of System-Level Virtualization.

- Runs multiple but logically distinct environments on a single instance of the operating system kernel. Also called shared kernel approach as all virtual machines share a common kernel of host operating system. Based on the change root concept "chroot".
- chroot starts during bootup. The kernel uses root filesystems to load drivers and perform other early-stage system initialization tasks. It then switches to another root filesystem using chroot command to mount an on-disk file system as its final root filesystem and continue system initialization and configuration within that file system.
- The chroot mechanism of system-level virtualization is an extension of this concept. It enables the system to start virtual servers with their own set of processes that execute relative to their own filesystem root directories.
- The main difference between system-level and server virtualization is whether different operating systems can be run on different virtual systems. If all virtual servers must share the same copy of the operating system it is system-level virtualization and if different servers can have different operating systems (including different versions of a single operating system) it is server virtualization.
- Examples: FreeVPS, Linux Vserver, and OpenVZ are some examples.
- Advantages:
  - Significantly lightweight than complete machines(including a kernel)
  - Can host many more virtual servers
  - Enhanced Security and isolation
  - Virtualizing an operating system usually has little to no overhead.
  - Live migration is possible with OS Virtualization.
  - It can also leverage dynamic container load balancing between nodes and clusters.
  - On OS virtualization, the file-level copy-on-write (CoW) method is possible, making it easier to back up data, more space-efficient, and easier to cache than block-level copy-on-write schemes.
- Limitations:
  - Kernel or driver problems can take down all virtual servers.



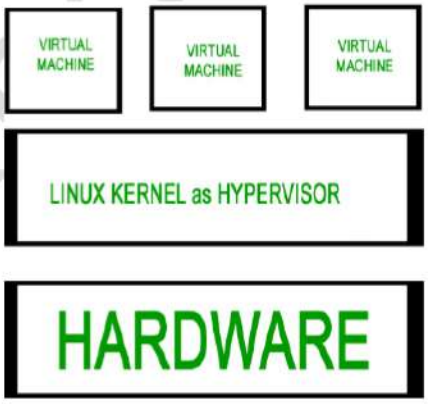
5. Hardware Assisted Virtualization

- Hardware Assisted Virtualization was presented by AMD and Intel. It is also known as Hardware virtualization, AMD virtualization, and Intel virtualization. It is designed to increase the performance of the processor. The advantage of using Hardware Assisted Virtualization is that it requires less hypervisor overhead.
- It is similar to Full Virtualization and Paravirtualization in terms of operation except that it requires hardware support. Much of the hypervisor overhead due to trapping and emulating I/O operations and status instructions executed within a guest OS is dealt with by relying on the hardware extensions of the x86 architecture.
- Unmodified OS can be run as the hardware support for virtualization would be used to handle hardware access requests, privileged and protected operations, and to communicate with the virtual machine.

- Examples: AMD – V Pacifica and Intel VT Vanderpool provide hardware support for virtualization.
- Advantages:
  - No modification to a guest operating system is required.
  - Very less hypervisor overhead
- Limitations:
  - Hardware support Required

6. Kernel-Level Virtualization

- Kernel-level virtualization is one of the most important types of server virtualization. It is an opensource virtualization which uses the Linux kernel as a hypervisor.
- The advantage of using kernel virtualization is that it does not require any special administrative software and has very less overhead.
- User Mode Linux (UML) and Kernel-based virtual machine are some examples of kernel virtualization.
- Instead of using a hypervisor, it runs a separate version of the Linux kernel and sees the associated virtual machine as a user-space process on the physical host. This makes it easy to run multiple virtual machines on a single host. A device driver is used for communication between the main Linux kernel and the virtual machine.
- Processor support is required for virtualization (Intel VT or AMD – v). A slightly modified QEMU process is used as the display and execution containers for the virtual machines. In many ways, kernel-level virtualization is a specialized form of server virtualization.
- Examples: User – Mode Linux(UML) and Kernel Virtual Machine(KVM)
- Advantages:
  - No special administrative software is required.
  - Very less overhead
- Limitations:
  - Hardware Support Required



Advantages of Server Virtualization

- Independent Restart:
  In Server Virtualization, each server can restart independently and does not affect the working of other virtual servers.
- Low Cost:
  Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.
- Disaster Recovery:
  Disaster Recovery is one of the best advantages of Server Virtualization. In Server Virtualization, data can easily and quickly move from one server to another and these data can be stored and retrieved from anywhere.

- Faster deployment of resources:
  Server virtualization allows us to deploy our resources in a simpler and faster way.
- Security:
  It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

- The biggest disadvantage of server virtualization is that when the server goes offline, all the websites that are hosted by the server will also go down.
- There is no way to measure the performance of virtualized environments.
- It requires a huge amount of RAM consumption.
- It is difficult to set up and maintain.
- Some core applications and databases are not supported virtualization.
- It requires extra hardware resources.

Uses of Server Virtualization

- Server Virtualization is used in the testing and development environment.
- It improves the availability of servers.
- It allows organizations to make efficient use of resources.
- It reduces redundancy without purchasing additional hardware components.

3.5 Hypervisor Management Software

Hypervisor management software, also known as virtualization management software, plays a critical role in cloud computing environments. It is responsible for overseeing and controlling the virtualization layer (the hypervisor) and the virtualized resources, such as virtual machines (VMs) or containers, in order to ensure efficient, secure, and scalable operation.

- **Hypervisor Management:**

Hypervisor Installation and Configuration: Hypervisor management software helps install and configure hypervisors on physical servers. It can deploy various types of hypervisors, such as VMware vSphere, Microsoft Hyper-V, KVM, and Xen, depending on the specific requirements of the cloud infrastructure.

Hypervisor Monitoring: It continuously monitors the health and performance of hypervisors, ensuring they are running optimally. This includes tracking CPU and memory usage, network traffic, and storage capacity.

- **Resource Management:**

Resource Allocation: Hypervisor management software allocates CPU, memory, storage, and network resources to virtual machines and containers. It ensures that resources are distributed fairly and efficiently among multiple VMs.

Dynamic Resource Scaling: The software allows for dynamic resource scaling, automatically adjusting resource allocation based on the workloads and requirements of VMs or containers. This ensures that applications can scale up or down as needed.

Overcommitment: In some cases, the software supports overcommitment, where it assigns more virtual resources than are physically available, relying on statistical analysis to avoid resource contention.

- **VM and Container Management:**

VM Lifecycle Management: Hypervisor management software assists in creating, cloning, starting, stopping, and deleting virtual machines. It provides tools for managing the entire VM lifecycle, including creating snapshots and templates.

Container Orchestration: In environments that use containers, the software may provide container orchestration features, such as deploying containers, scaling them, and managing their networking and storage.

- **Storage and Network Management:**

Storage Virtualization: It abstracts physical storage devices, creating a virtualized storage pool that can be dynamically allocated to VMs or containers. It may also manage features like storage snapshots, replication, and backup.

- Network Virtualization: Hypervisor management software can create virtual networks, configure network settings for VMs, and enforce network policies. Software-defined networking (SDN) may be integrated to provide advanced network management capabilities.

- **Security and Isolation:**
- Access Control: The software enforces access controls and permissions, ensuring that only authorized users or applications can access VMs, containers, or other virtualized resources.
- Isolation: It enforces strong isolation between VMs and containers, preventing interference or unauthorized access between different virtualized workloads.

- **High Availability and Fault Tolerance:**
- High Availability (HA): Hypervisor management software often includes features for HA, allowing it to automatically restart VMs on healthy hosts in the event of a host failure.
- Fault Tolerance (FT): Some software supports FT, where VMs are simultaneously active on two hosts, providing continuous service even in the event of a hardware failure.

- **Reporting and Analytics:**
- Performance Metrics: The software collects performance data, generates reports, and provides analytics that can help in optimizing resource allocation and capacity planning.
- Cost Analysis: It may offer insights into resource costs, helping cloud administrators make informed decisions about resource usage and billing.

- **Integration and APIs:**
- Integration with Cloud Management Platforms: Hypervisor management software can integrate with higher-level cloud management platforms, such as OpenStack or VMware vRealize, to enable a unified cloud management experience.
- APIs and Automation: APIs allow for programmatic control of the virtualization environment, facilitating automation and orchestration of cloud resources.

Hypervisor management software is a critical component of cloud infrastructure, enabling efficient resource utilization, scalability, security, and high availability. Its role is to abstract the complexities of virtualization, providing a user-friendly interface for cloud administrators to manage virtualized resources and ensuring the seamless operation of cloud services.

3.6 Virtual Infrastructure

- Virtual infrastructure is a collection of software-defined components that make up an enterprise IT environment. A virtual infrastructure provides the same IT capabilities as physical resources, but with software, so that IT teams can allocate these virtual resources quickly and across multiple systems, based on the varying needs of the enterprise.
- By decoupling physical hardware from an operating system, a virtual infrastructure can help organizations achieve greater IT resource utilization, flexibility, scalability and cost savings. These benefits are especially helpful to small businesses that require reliable infrastructure but can't afford to invest in costly physical hardware.

Virtual infrastructure components

- By separating physical hardware from operating systems, virtualization can provision compute, memory, storage and networking resources across multiple virtual machines (VMs) for greater application performance, increased cost savings and easier management. Despite variances in design and functionality, a virtual infrastructure typically consists of these key components:
  - **Virtualized compute:** This component offers the same capabilities as physical servers, but with the ability to be more efficient. Through virtualization, many operating systems and applications can run on a single physical server, whereas in traditional infrastructureservers were often underutilized. Virtual compute also makes newer technologies likecloud computing and containers possible.
  - **Virtualized storage:** This component frees organizations from the constraints and limitations of hardware by combining pools of physical storage capacity into a single, more manageable repository. By connecting

storage arrays to multiple servers using storage area networks, organizations can bolster their storage resources and gain more flexibility in provisioning them to virtual machines.

- **Virtualized networking and security:** This component decouple networking services from the underlying hardware and allows users to access network resources from a centralized management system. Key security features ensure a protected environment for virtual machines, including restricted access, virtual machine isolation and user provisioning measures.
- **Management solution:** This component provides a user-friendly console for configuring, managing and provisioning virtualized IT infrastructure, as well automating processes. A management solution allows IT teams to migrate virtual machines from one physical serverto another without delays or downtime, while enabling high availability for applications running in virtual machines, disaster recovery and back-up administration.

Benefits of virtual infrastructure

➢ The benefits of virtualization touch every aspect of an IT infrastructure, from storage and server systems to networking tools. Here are some key benefits of a virtual infrastructure:

- **Cost savings:** By consolidating servers, virtualization reduces capital and operating costs associated with variables such as electrical power, physical security, hosting and server development.
- Scalability: A virtual infrastructure allows organizations to react quickly to changing customer demands and market trends by ramping up on CPU utilization or scaling back accordingly.
- **Increased productivity:** Faster provisioning of applications and resources allows IT teams to respond more quickly to employee demands for new tools and technologies. The result: increased productivity, efficiency and agility for IT teams, and an enhanced employee experience and increased talent retention rates without hardware procurement delays.
- **Simplified server management:** From seasonal spikes in consumer demand to unexpected economic downturns, organizations need to respond quickly. Simplified server management makes sure IT teams can spin up, or down, virtual machines when required and re-provision resources based on real-time needs. Furthermore, many management consoles offer dashboards, automated alerts and reports so that IT teams can respond immediately to server performance issues.

Virtual infrastructure requirements

➢ From design to disaster recovery, there are certain virtual infrastructure requirements organizations must meet to reap long-term value from their investment.

- **Plan ahead:** When designing a virtual infrastructure, IT teams should consider how business growth, market fluctuations and advancements in technology might impact their hardware requirements and reliance on compute, networking and storage resources.
- **Look for ways to cut costs:** IT infrastructure costs can become unwieldy if IT teams don't take the time to continuously examine a virtual infrastructure and its deliverables. Cost-cutting initiatives may range from replacing old servers and renegotiating vendor agreements to automating time-consuming server management tasks.
- Prepare for failure: Despite its failover hardware and high availability, even the most resilient virtual infrastructure can experience downtime. IT teams should prepare for worst-case scenarios by taking advantage of monitoring tools, purchasing extra hardware and relying on clusters to better manage host resources.

Virtual infrastructure architecture

➢ A virtual infrastructure architecture can help organizations transform and manage their IT system infrastructure through virtualization. But it requires the right building blocks to deliver results. These include:

- **Host:** A virtualization layer that manages resources and other services for virtual machines. Virtual machines run on these individual hosts, which continuously perform monitoring and management activities in the background. Multiple hosts can be grouped together to work on the same network and storage subsystems, culminating in combined computing and memory resources to form a cluster. Machines can be dynamically added or removed from a cluster.

- **Hypervisor:** A software layer that enables one host computer to simultaneously support multiple virtual operating systems, also known as virtual machines. By sharing the same physical computing resources, such as memory, processing and storage, the hypervisor stretches available resources and improves IT flexibility.
- **Virtual machine:** These software-defined computers encompass operating systems, software programs and documents. Managed by a virtual infrastructure, each virtual machine has its own operating system called a guest operating system. The key advantage of virtual machines is that IT teams can provision them faster and more easily than physical machines without the need for hardware procurement. Better yet, IT teams can easily deploy and suspend a virtual machine, and control access privileges, for greater security. These privileges are based on policies set by a system administrator.
- **User interface:** This front-end element means administrators can view and manage virtual infrastructure components by connecting directly to the server host or through a browserbased interface