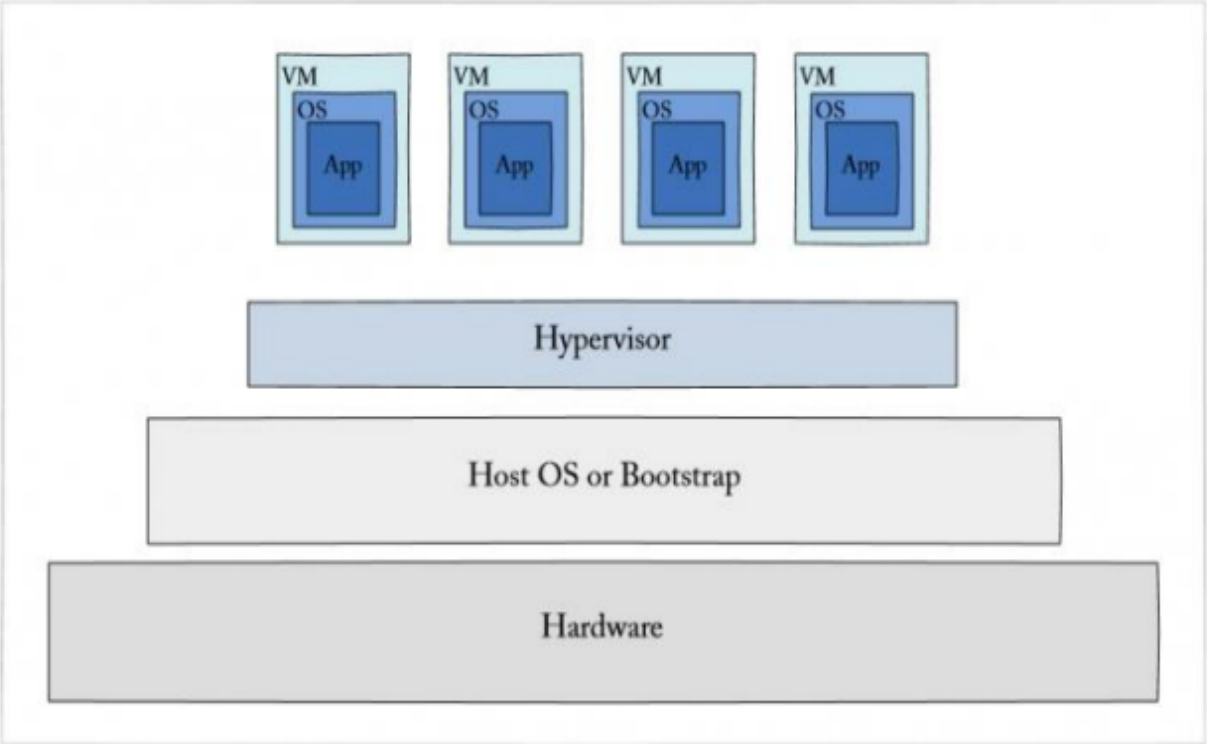
Unit 3

Cloud Virtualization technology

Overview of Virtualization techniques

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.



What is the concept behind the Virtualization?

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

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.**

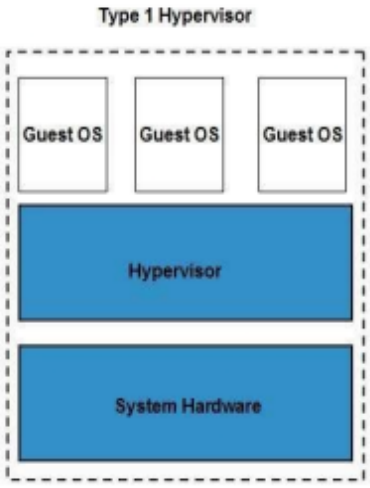
Difference between virtualization and cloud

- Essentially there is a gap between these two terms, though cloud technology requires the concept of virtualization. Virtualization is a technology - it can also be treated as software that can manipulate hardware. At the same time, cloud computing is a service that is the result of manipulation.
- Virtualization is the foundation element of cloud computing, whereas Cloud technology is the delivery of shared resources as a service-on-demand via the internet.
- Cloud is essentially made-up of the concept of virtualization.

Hypervisor

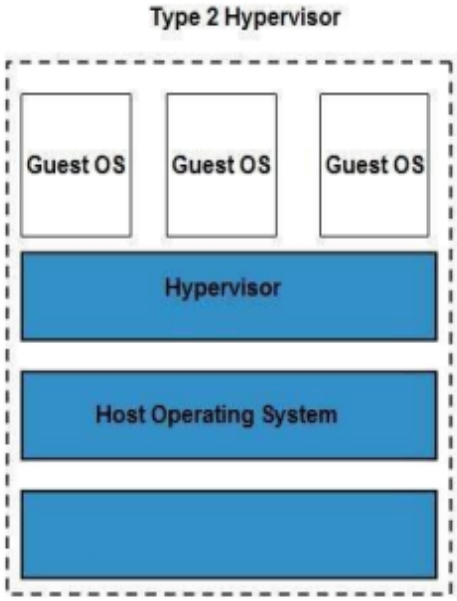
The **hypervisor** is a firmware or low-level program that acts as a Virtual Machine Manager. There are two types of hypervisor:

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.



Types of Virtualizations:

1. Hardware Virtualization.
2. Software Virtualization.
3. Operating system Virtualization.
4. Server Virtualization.
5. Storage Virtualization.

Hardware Virtualization

Previously, there was *"one to one relationship"* between physical servers and operating system. Low capacity of CPU, memory, and networking requirements were available. So, by using this model, the costs of doing business increased. The physical space, amount of power, and hardware required meant that costs were adding up.

The **hypervisor** *manages shared the physical resources of the hardware between the guest operating systems and host operating system*. The physical resources become abstracted versions in standard formats regardless of the hardware platform. The abstracted hardware is represented as actual hardware. Then the virtualized operating system looks into these resources as they are physical entities.

Virtualization means abstraction. Hardware virtualization is accomplished by abstracting the physical hardware layer by use of a hypervisor or VMM (Virtual Machine Monitor).

When the virtual machine software or virtual machine manager (VMM) or hypervisor software is directly installed on the hardware system is known as hardware virtualization.

The main **job of hypervisor** is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system, we can install different operating system on it and run different applications on those OS.

Usage of Hardware Virtualization

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

The main benefits of hardware virtualization are more efficient resource utilization, lower overall costs as well as increased uptime and IT flexibility.

1) More Efficient Resource Utilization:

Physical resources can be shared among virtual machines. Although the unused resources can be allocated to a virtual machine and that can be used by other virtual machines if the need exists.

2) Lower Overall Costs Because Of Server Consolidation:

Now it is possible for multiple operating systems can co-exist on a single hardware platform, so that the number of servers, rack space, and power consumption drops significantly.

3) Increased Uptime Because Of Advanced Hardware Virtualization Features:

The modern hypervisors provide highly arranged operations that maximize the abstraction of the hardware and help to ensure the maximum uptime. These functions help to migrate a running virtual machine from one host to another dynamically, as well as maintain a running copy of virtual machine on another physical host in case the primary host fails.

4) Increased IT Flexibility:

Hardware virtualization helps for quick deployment of server resources in a managed and consistent ways. That results in IT being able to adapt quickly and provide the business with resources needed in good time.

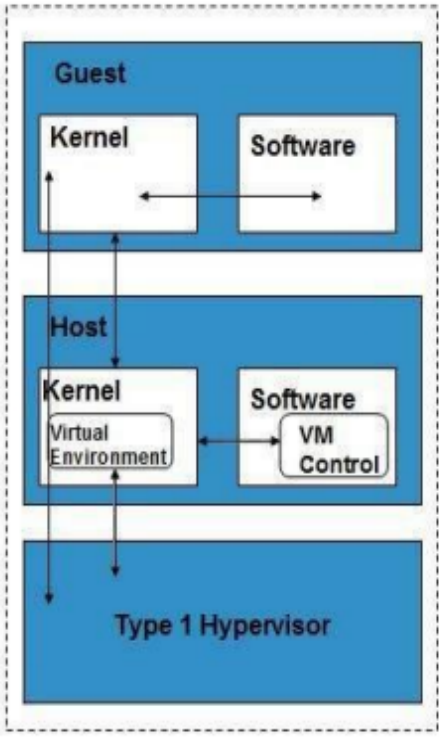
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

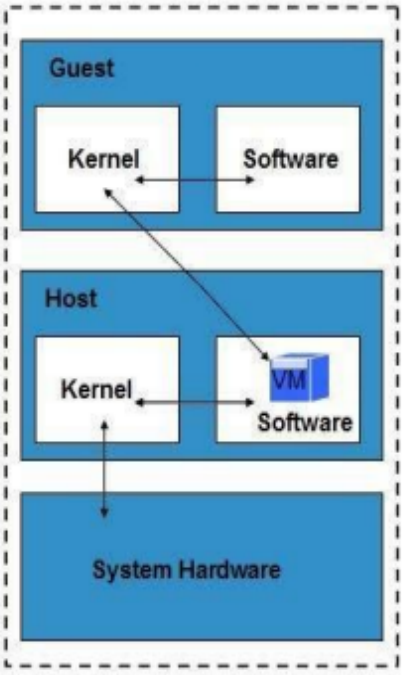
Full Virtualization

In **full virtualization,** the underlying hardware is completely simulated. Guest software does not require any modification to run.



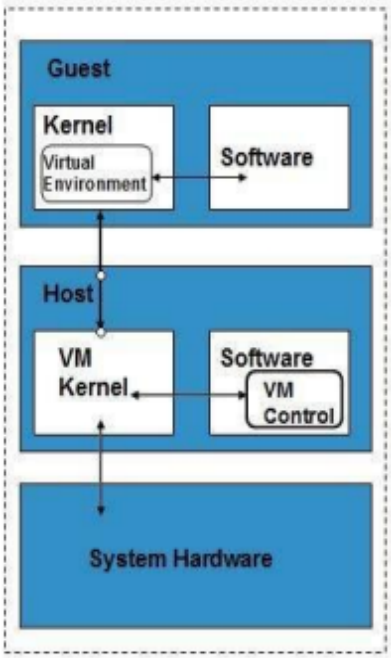
Emulation Virtualization

In **Emulation,** the virtual machine simulates the hardware and hence becomes independent of it. In this, the guest operating system does not require modification.



Paravirtualization

In **Paravirtualization,** the hardware is not simulated. The guest software run their own isolated domains.



VMware vSphere is highly developed infrastructure that offers a management infrastructure framework for virtualization. It virtualizes the system, storage and networking hardware.

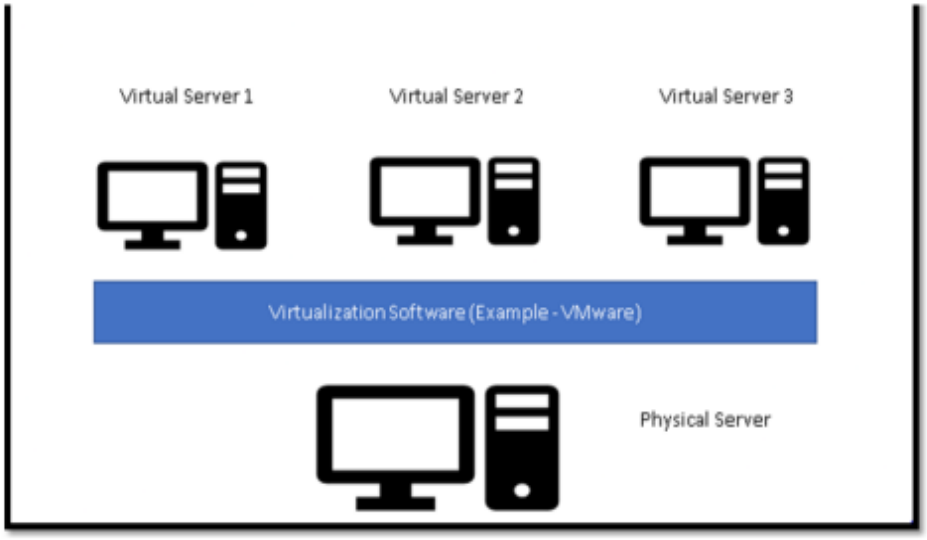
Software Virtualization

Managing applications and distribution becomes a typical task for IT departments. Installation mechanism differs from application to application. Some programs require certain helper applications or frameworks and these applications may have conflict with existing applications.

Software virtualization is just like a virtualization but *able to abstract the software installation procedure and create virtual software installations*.

Virtualized software is an application that will be "installed" into its own self-contained unit.

Example of software virtualization is *VMware software, virtual box* etc.



Advantages of Software Virtualization

1) Client Deployments Become Easier:

Copying a file to a workstation or linking a file in a network then we can easily install virtual software.

2) Easy to manage:

To manage updates becomes a simpler task. You need to update at one place and deploy the updated virtual application to the all clients.

3) Software Migration:

Without software virtualization, moving from one software platform to another platform takes much time for deploying and impact on end user systems. With the help of virtualized software environment, the migration becomes easier.

Operating System Virtualization

With the help of OS virtualization nothing is pre-installed or permanently loaded on the local device and no-hard disk is needed. Everything runs from the network using a kind of virtual disk. This virtual disk is actually a disk image file stored on a remote server, SAN (Storage Area Network) or NAS (Non-volatile Attached Storage). The client will be connected by the network to this virtual disk and will boot with the Operating System installed on the virtual disk.

How does OS Virtualization work?

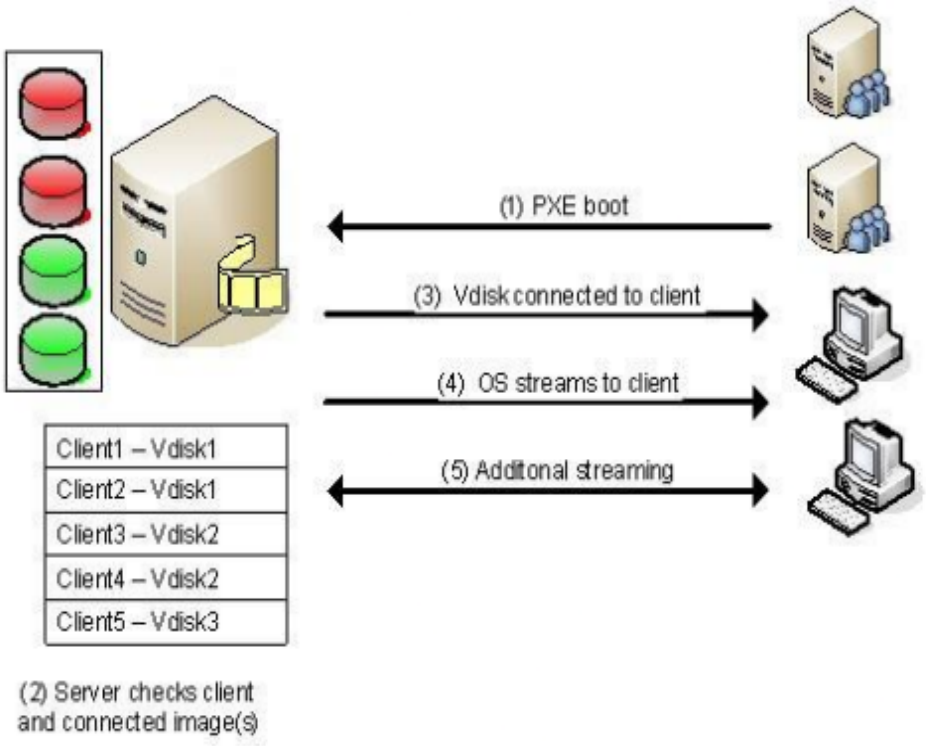
Components needed for using OS Virtualization in the infrastructure are given below:

The first component is the OS Virtualization server. This server is the center point in the OS Virtualization infrastructure. The server manages the streaming of the information on the virtual disks for the client and also determines which client will be connected to which virtual disk (using a database, this information is stored). Also, the server can host the storage for the virtual disk locally or the server is connected to the virtual disks via a SAN (Storage Area Network). In high availability environments there can be more OS Virtualization servers to create no redundancy and load balancing. The server also ensures that the client will be unique within the infrastructure.

Secondly, there is a client which will contact the server to get connected to the virtual disk and asks for components stored on the virtual disk for running the operating system.

The available supporting components are database for storing the configuration and settings for the server, a streaming service for the virtual disk content, a (optional) TFTP service and a (also optional) PXE boot service for connecting the client to the OS Virtualization servers.

As it is already mentioned that the virtual disk contains an image of a physical disk from the system that will reflect to the configuration and the settings of those systems which will be using the virtual disk. When the virtual disk is created then that disk needs to be assigned to the client that will be using this disk for starting. The connection between the client and the disk is made through the administrative tool and saved within the database. When a client has a assigned disk, the machine can be started with the virtual disk using the following process as displayed in the given below Figure:



1) Connecting to the OS Virtualization server:

First we start the machine and set up the connection with the OS Virtualization server. Most of the products offer several possible methods to connect with the server. One of the most popular and used methods is using a PXE service, but also a boot strap is used a lot (because of the disadvantages of the PXE service). Although each method initializes the network interface card (NIC), receiving a (DHCP-based) IP address and a connection to the server.

2) Connecting the Virtual Disk:

When the connection is established between the client and the server, the server will look into its database for checking the client is known or unknown and which virtual disk is assigned to the client. When more than one virtual disk are connected then a boot menu will be displayed on the client side. If only one disk is assigned, that disk will be connected to the client which is mentioned in step number 3.

3) VDisk connected to the client:

After the desired virtual disk is selected by the client, that virtual disk is connected through the OS Virtualization server. At the back-end, the OS Virtualization server makes sure that the client will be unique (for example computer name and identifier) within the infrastructure.

4) OS is "streamed" to the client:

As soon the disk is connected the server starts streaming the content of the virtual disk. The software knows which parts are necessary for starting the operating system smoothly, so that these parts are streamed first. The information streamed in the system should be stored somewhere (i.e. cached). Most products offer several ways to cache that information. For examples on the client hard disk or on the disk of the OS Virtualization server.

5) Additional Streaming:

After that the first part is streamed then the operating system will start to run as expected. Additional virtual disk data will be streamed when required for running or starting a function called by the user (for example starting an application available within the virtual disk).

Advantages of OS virtualization

- OS virtualization usually imposes little or no overhead.
- OS Virtualization is capable of live migration
- It can also use dynamic load balancing of containers between nodes and a cluster.
- The file level copy-on-write (CoW) mechanism is possible on OS virtualization which makes easier to back up files, more space-efficient and simpler to cache than the block-level copy-on-write schemes.

Virtual disks in OS virtualization

The client will be connected via the network to the virtual disk & will boot the OS installed on virtual disk. Two types of virtual disks are there for implementation.
These are:

1. Private Virtual Disk: is used by one client only like that of a local hard disk. Users can save information on the virtual disk based on the rights assigned. So as the client restart the system, the settings are retained just like working with physical local hard disk.
2. Shared/Common Virtual Disk: It is used by multiple clients at the same time. The changes are saved in a special cache & these caches gets cleaned as the user restarts or shutdowns the system. In other words, when a client is booting up, it will use the default configuration available on the virtual disk.

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.

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.

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.

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.

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.

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.

6. Kernel-Level Virtualization

Kernel-level virtualization is one of the most important types of server virtualization. It is an **open-source 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.

Advantages of Server Virtualization

There are the following advantages of Server Virtualization -

1. Independent Restart

In Server Virtualization, each server can restart independently and does not affect the working of other virtual servers.

2. Low Cost

Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.

3. 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.

4. Faster deployment of resources

Server virtualization allows us to deploy our resources in a simpler and faster way.

5. Security

It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

There are the following disadvantages of Server Virtualization -

1. 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.
2. There is no way to measure the performance of virtualized environments.
3. It requires a huge amount of RAM consumption.
4. It is difficult to set up and maintain.
5. Some core applications and databases are not supported virtualization.
6. It requires extra hardware resources.

Uses of Server Virtualization

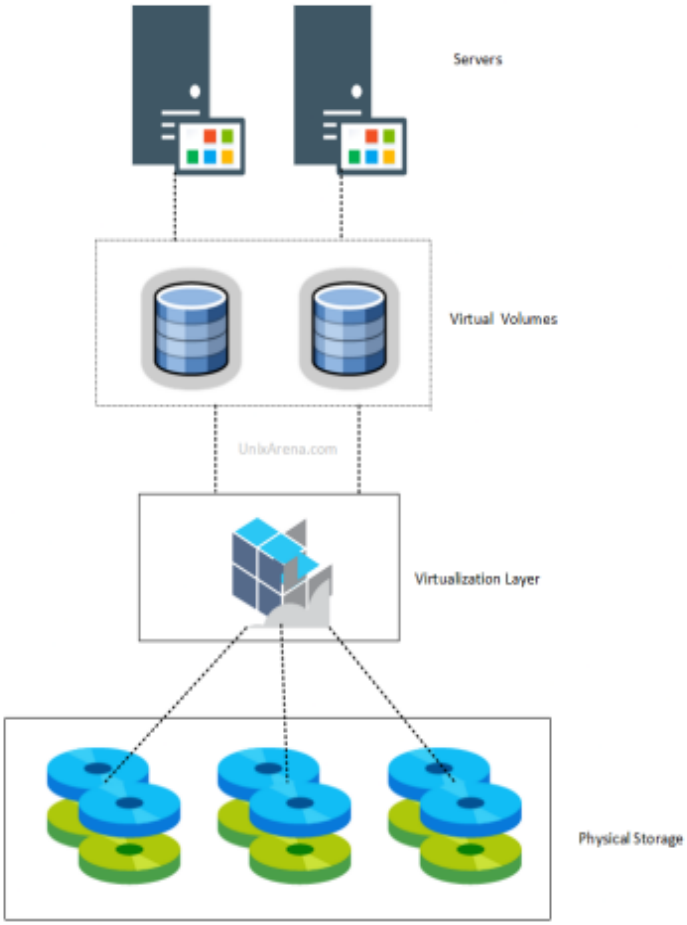
A list of uses of server virtualization is given below -

- 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.

Storage Virtualization

Storage virtualization is a major component for storage servers, in the form of functional RAID (Redundant Array of Independent disks) levels and controllers. Operating systems and applications with device can access the disks directly by themselves for writing. The controllers configure the

local storage in RAID groups and present the storage to the operating system depending upon the configuration. However, the storage is abstracted and the controller is determining how to write the data or retrieve the requested data for the operating system.



Advantages of Storage Virtualization

1. Data is stored in the more convenient locations away from the specific host. In the case of a host failure, the data is not compromised necessarily.
2. The storage devices can perform advanced functions like replication, reduplication, and disaster recovery functionality.
3. By doing abstraction of the storage level, IT operations become more flexible in how storage is provided, partitioned, and protected.

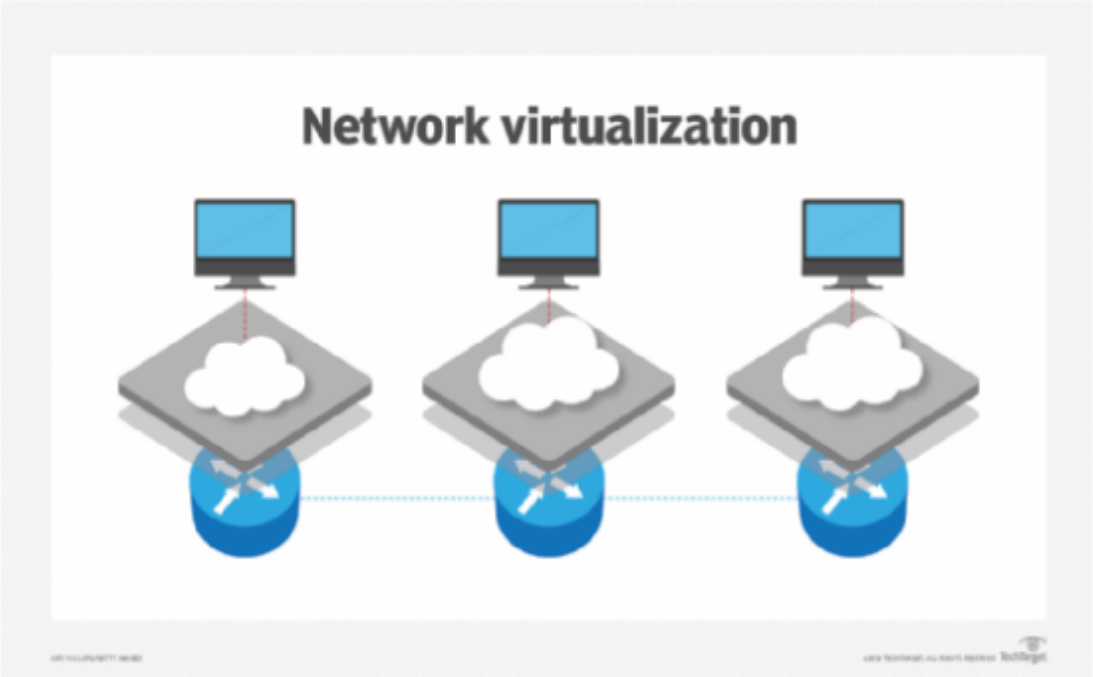
Network Virtualization

Network virtualization is a method of combining the available resources in a network to consolidate multiple physical networks, divide a network into segments or create software networks between virtual machines (VMs). IT managers that use network virtualization can administrate their environment as a single software-based network. Network virtualization is

intended to optimize network speed, reliability, flexibility, scalability and security. It is said to be especially useful in networks that experience sudden, large and unforeseen surges in usage.

Network virtualization works by combining the available resources in a network and splitting up the available bandwidth into channels, each of which is independent from the others and each of which can be assigned (or reassigned) to a particular server or device in real time. Each channel is independently secured. Every subscriber has shared access to all the resources on the network from a single computer.

Network virtualization is intended to improve productivity, efficiency and job satisfaction of the administrator by performing many of these tasks automatically, thereby disguising the true complexity of the network. Files, images, programs and folders can be centrally managed from a single physical site. Storage media such as hard drives and tape drives can be easily added or reassigned. Storage space can be shared or reallocated among the servers.



Advantages and disadvantages

The use of network virtualization does have its upsides and downsides, including:

Advantages:

- More productive IT environments (i.e., efficient scaling).
- Improved security and recovery times.
- Faster in application delivery.
- More efficient networks.
- Reduced overall costs.

Disadvantages:

- Increased upfront costs (investing in virtualization software).
- Need to license software.
- There may be a learning curve if IT managers are not experienced.
- Not every application and server will work in a virtualized environment.
- Availability can be an issue if an organization can't connect to their virtualized data.

Desktop Virtualization

Desktop virtualization provides a way for users to maintain their individual desktops on a single, central server. The users may be connected to the central server through a LAN, WAN or over the Internet.

Desktop virtualization has many benefits, including a lower total cost of ownership (TCO), increased security, reduced energy costs, reduced downtime and centralized management.

Limitations of desktop virtualization include difficulty in maintenance and set up of printer drivers; increased downtime in case of network failures; complexity and costs involved in VDI deployment and security risks in the event of improper network management.

Benefits of Desktop Virtualization

Resource Management:
Desktop virtualization helps IT departments get the most out of their hardware investments by consolidating most of their computing in a data center. Desktop virtualization then allows organizations to issue lower-cost computers and devices to end users because most of the intensive computing work takes place in the data center. By minimizing how much computing is needed at the endpoint devices for end users, IT departments can save money by buying less costly machines.

Remote work:
Desktop virtualization helps IT admins support remote workers by giving IT central control over how desktops are virtually deployed across an organization's devices. Rather than manually setting up a new desktop for each user, desktop virtualization allows IT to simply deploy a ready-to-go virtual desktop to that user's device. Now the user can

interact with the operating system and applications on that desktop from any location and the employee experience will be the same as if they were working locally.

Security:
Desktop virtualization software provides IT admins centralized security control over which users can access which data and which applications. If a user's permissions change because they leave the company, desktop virtualization makes it easy for IT to quickly remove that user's access to their persistent virtual desktop and all its data—instead of having to manually uninstall everything from that user's devices. And because all company data lives inside the data center rather than on each machine, a lost or stolen device does not post the same data risk. If someone steals a laptop using desktop virtualization, there is no company data on the actual machine and hence less risk of a breach.

Benefits of Virtualization

Virtualization can increase IT agility, flexibility, and scalability while creating significant cost savings. Workloads get deployed faster, performance and availability increase and operations become automated, resulting in IT that's simpler to manage and less costly to own and operate. Additional benefits include:

- Reduce capital and operating costs.
- Minimize or eliminate downtime.
- Increase IT productivity, efficiency, agility and responsiveness.
- Provision applications and resources faster.
- Enable business continuity and disaster recovery.
- Simplify data center management.
- Build a true Software-Defined Data Center

Disadvantages of Virtualization

The disadvantages of virtualization are mostly those that would come with any technology transition. With careful planning and expert implementation, all of these drawbacks can be overcome.

- **Upfront costs.** The investment in the virtualization software, and possibly additional hardware might be required to make the virtualization possible. This depends on your existing network. Many businesses have sufficient capacity to accommodate the virtualization without requiring a lot of cash. This obstacle can also be more readily navigated by working with a Managed IT Services provider, who can offset this cost with monthly leasing or purchase plans.
- **Software licensing considerations**. This is becoming less of a problem as more software vendors adapt to the increased adoption of virtualization, but it is important to check with your vendors to clearly understand how they view software use in a virtualized environment.

- **Possible learning curve.** Implementing and managing a virtualized environment will require IT staff with expertise in virtualization. On the user side a typical virtual environment will operate similarly to the non-virtual environment. There are some applications that do not adapt well to the virtualized environment – this is something that your IT staff will need to be aware of and address prior to converting.

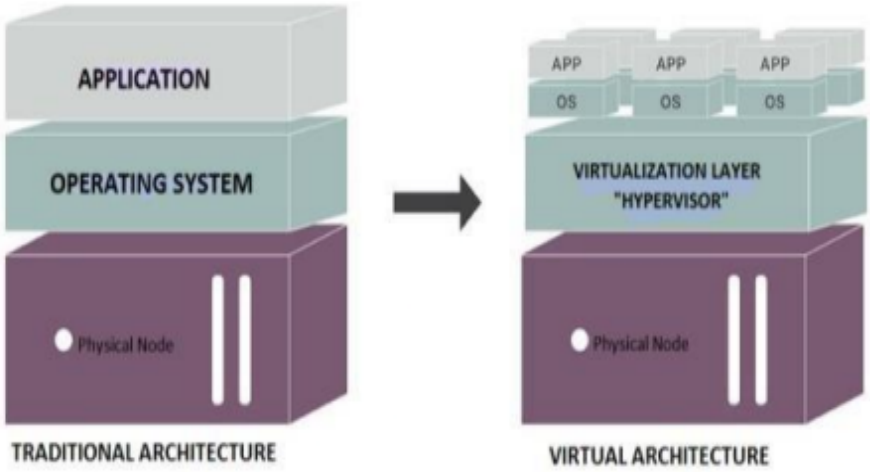
For many businesses comparing the advantages to the disadvantages, moving to a virtual environment is typically the clear winner. Even if the drawbacks present some challenges, these can be quickly navigated with an expert IT team or by outsourcing the virtualization process to a Managed IT Services provider. The seeming disadvantages are more likely to be simple challenges that can be navigated and overcome easily.

IMPLEMENTATION LEVELS OF VIRTUALIZATION

It is not simple to set up virtualization. Your computer runs on an operating system that gets configured on some particular hardware. It is not feasible or easy to run a different operating system using the same hardware.

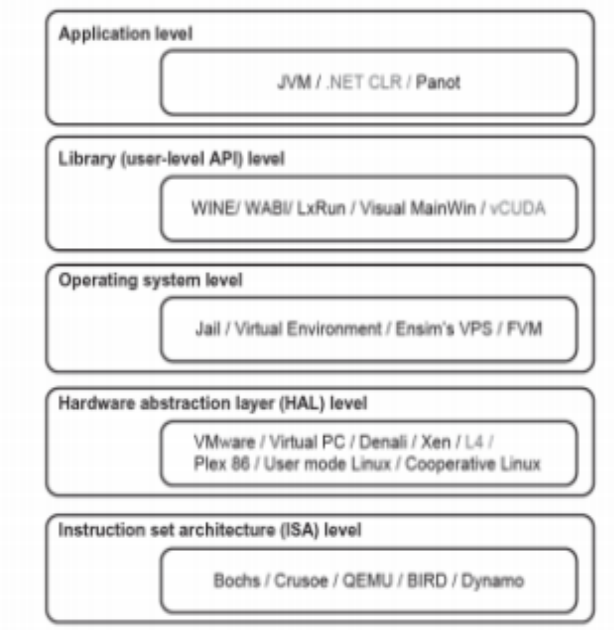
To do this, you will need a hypervisor. Now, what is the role of the hypervisor? It is a bridge between the hardware and the virtual operating system, which allows smooth functioning.

Talking of the Implementation levels of virtualization in cloud computing, there are a total of five levels that are commonly used. Let us now look closely at each of these levels of virtualization implementation in cloud computing.



Virtualization can be implemented at various operational levels, as given below:

- Instruction set architecture (ISA) level
- Hardware level
- Operating system level
- Library support level
- 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.

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 infrastructure servers were often underutilized. Virtual compute also makes newer technologies like cloud 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 server to 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 unwieldly 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 browser-based interface.