CLOUD COMPUTING VIRTUALIZATION

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

Virtualization Concept

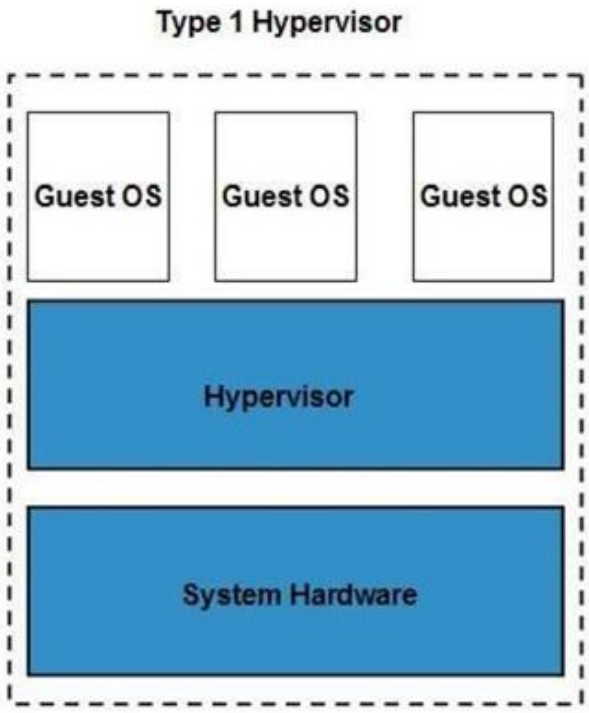
Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is created is known as host machine and virtual machines referred as a guest machine. This virtual machine is managed by a software or firmware, which is known as hypervisor.

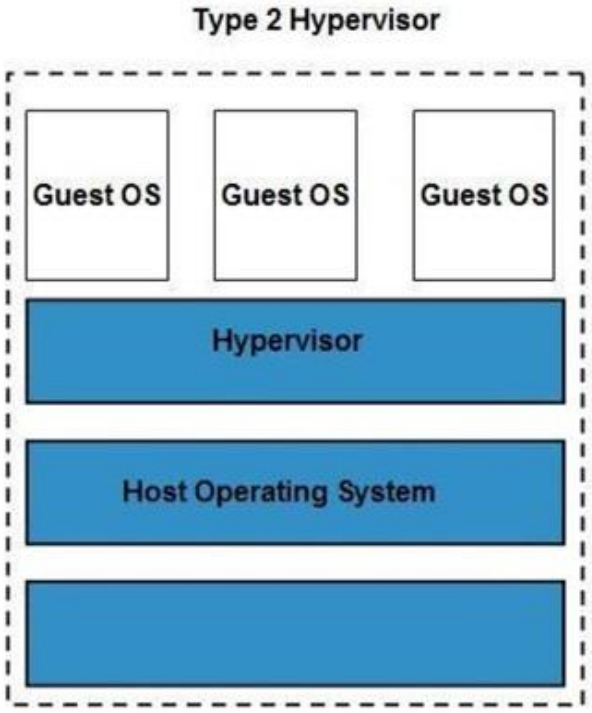
HYPERVISOR

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

Type 1 hypervisor runs 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 **Type 1 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 Hardware Virtualization

Here are the three types of hardware virtualization:

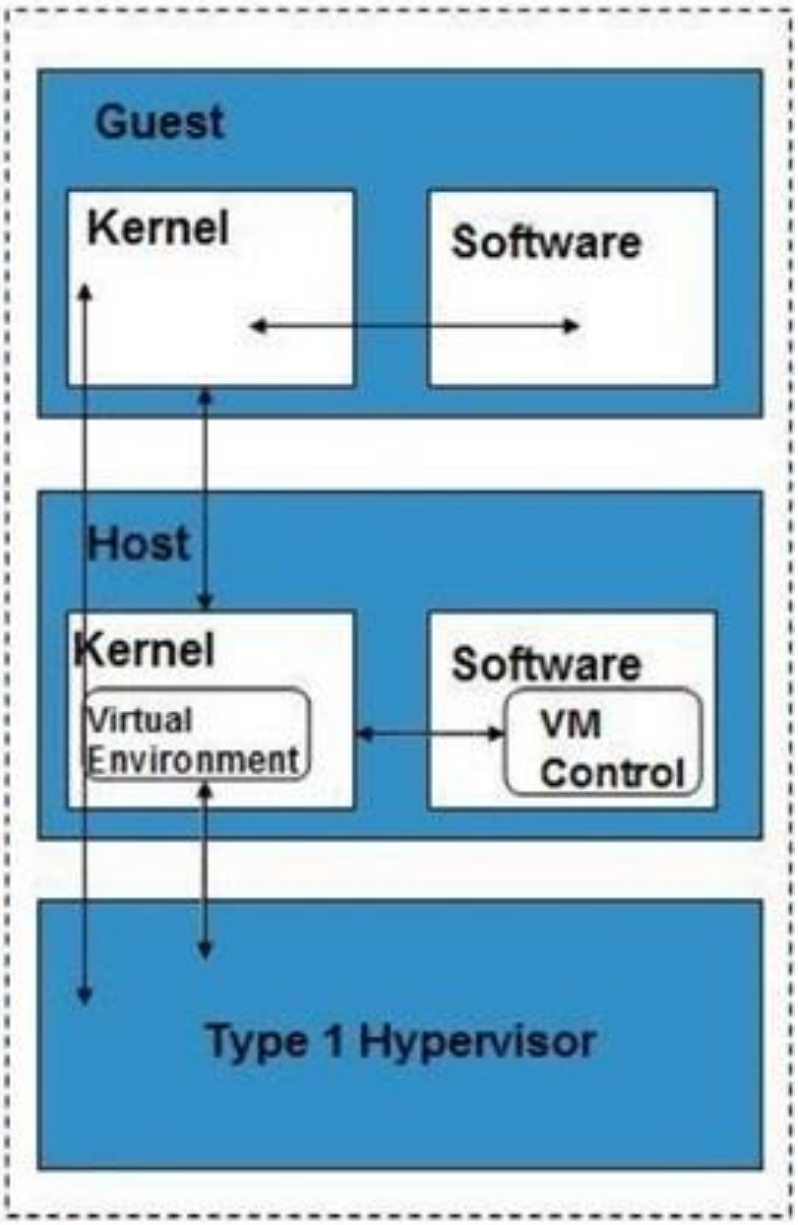
a) Full Virtualization

b) Paravirtualization

c) Emulation Virtualization

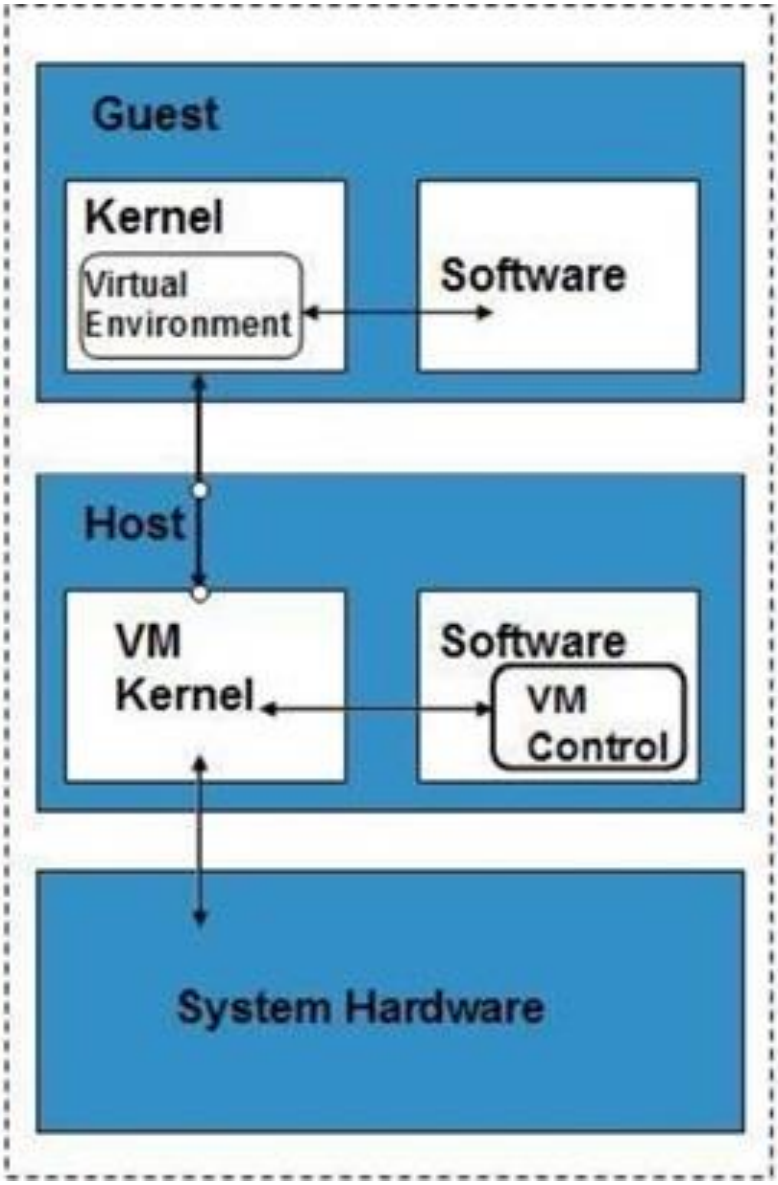
FULL VIRTUALIZATION

In Full Virtualization, the underlying hardware is completely simulated. Guest software does not require any modification to run.



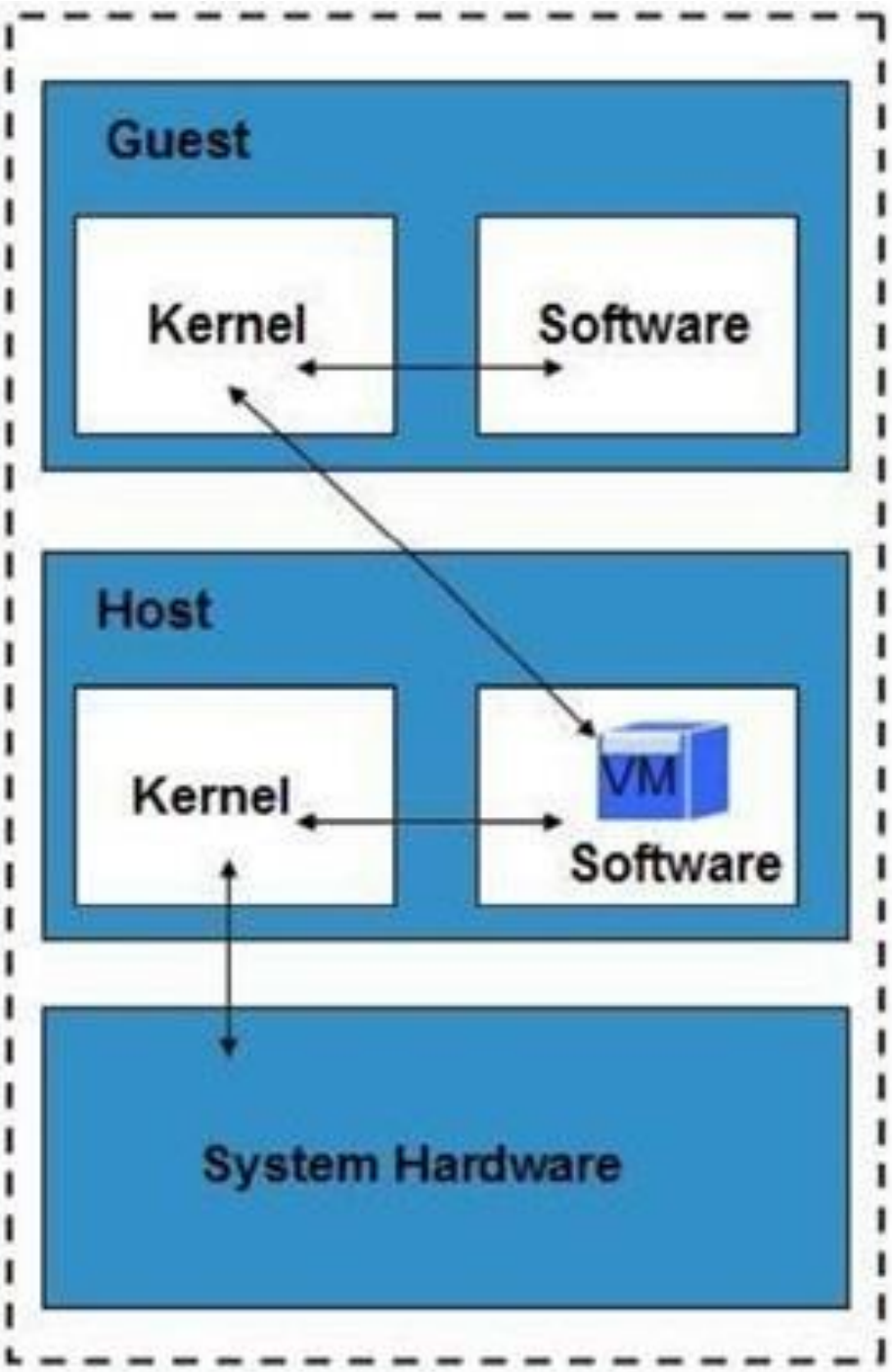
PARAVIRTUALIZATION

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



EMULATION VIRTUALIZATION

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



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

VIRTUALIZATION IN CLOUD COMPUTING

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**

TYPES OF VIRTUALIZATION

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

1) HARDWARE VIRTUALIZATION:

When the virtual machine software or virtual machine manager (VMM) 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: Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2) OPERATING SYSTEM VIRTUALIZATION:

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

Usage: Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) SERVER VIRTUALIZATION:

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

Usage: Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) STORAGE VIRTUALIZATION:

Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device.
Storage virtualization is also implemented by using software applications.

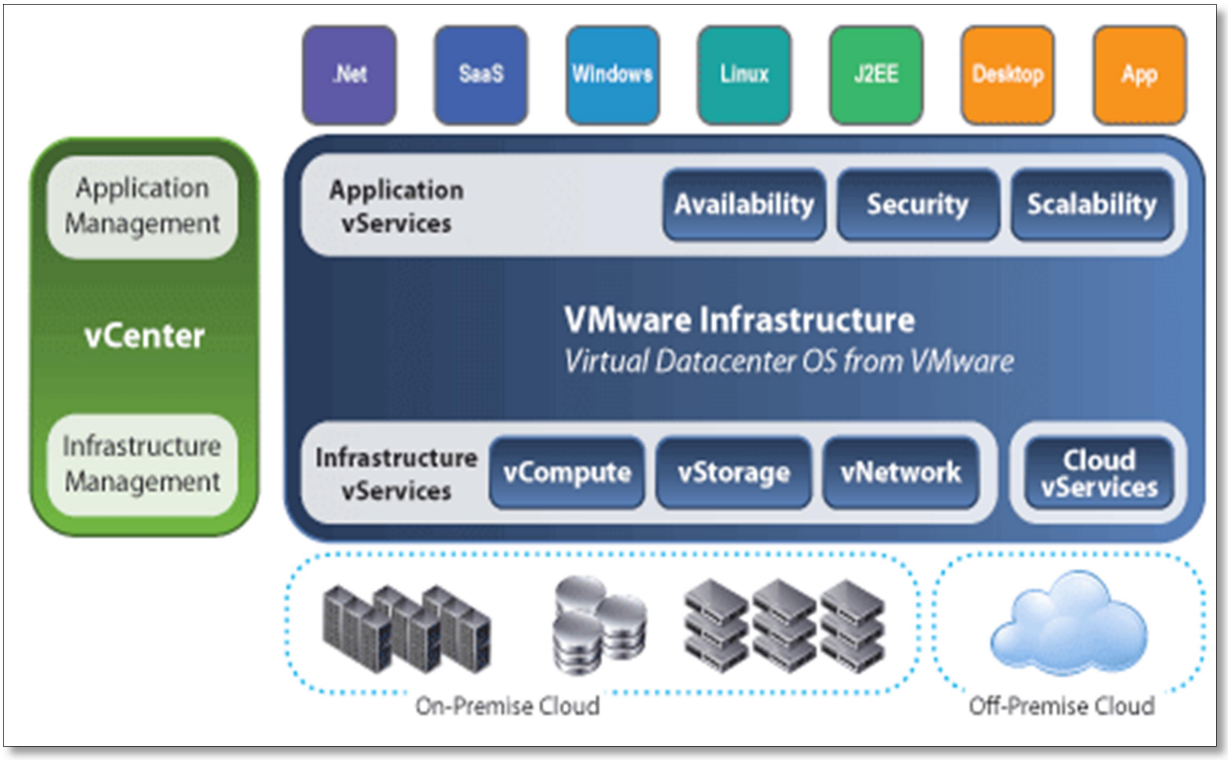
Usage: Storage virtualization is mainly done for back-up and recovery purposes.

HOW DOES VIRTUALIZATION WORK IN CLOUD COMPUTING?

Virtualization plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like application etc, but actually with the help of virtualization users shares the Infrastructure.

The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.

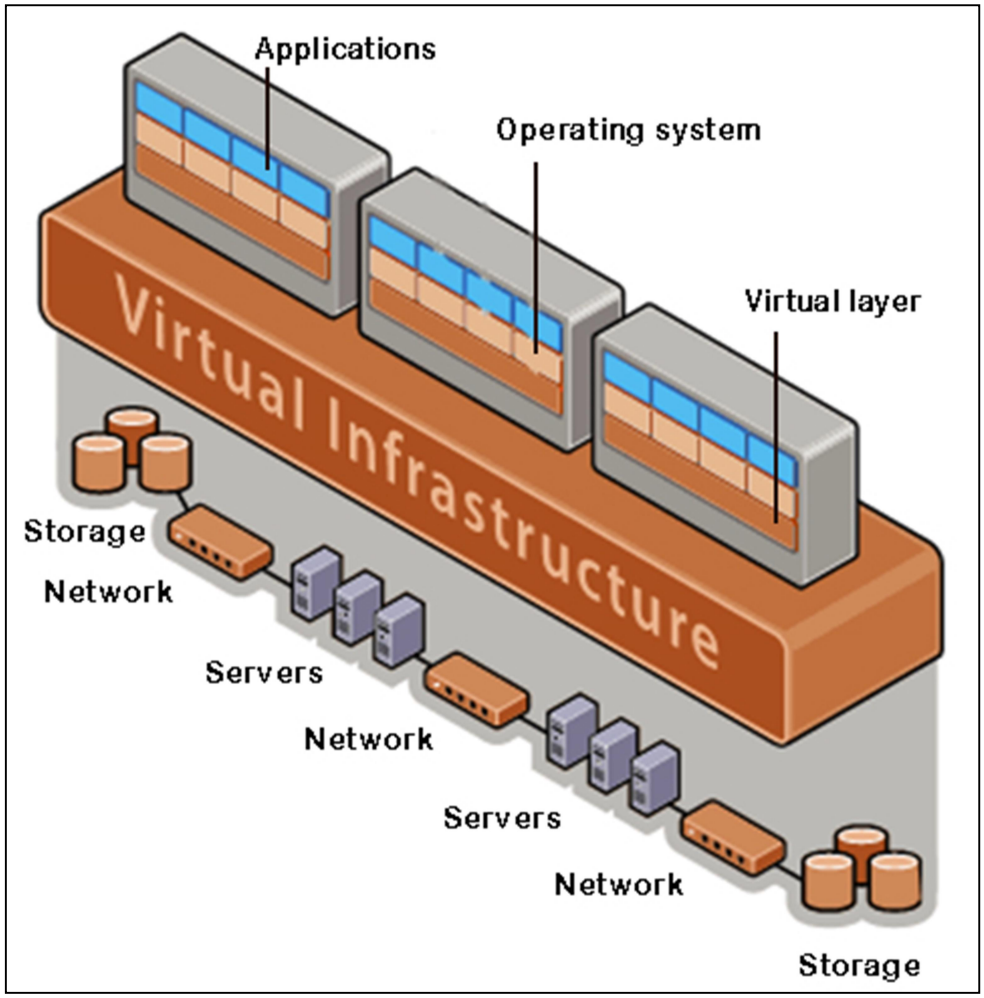
To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.



Mainly Virtualization means, running multiple operating systems on a single machine but sharing all the hardware resources. And it helps us to provide the pool of IT resources so that we can share these IT resources in order get benefits in the business.

HOW VIRTUALIZATION WORKS?

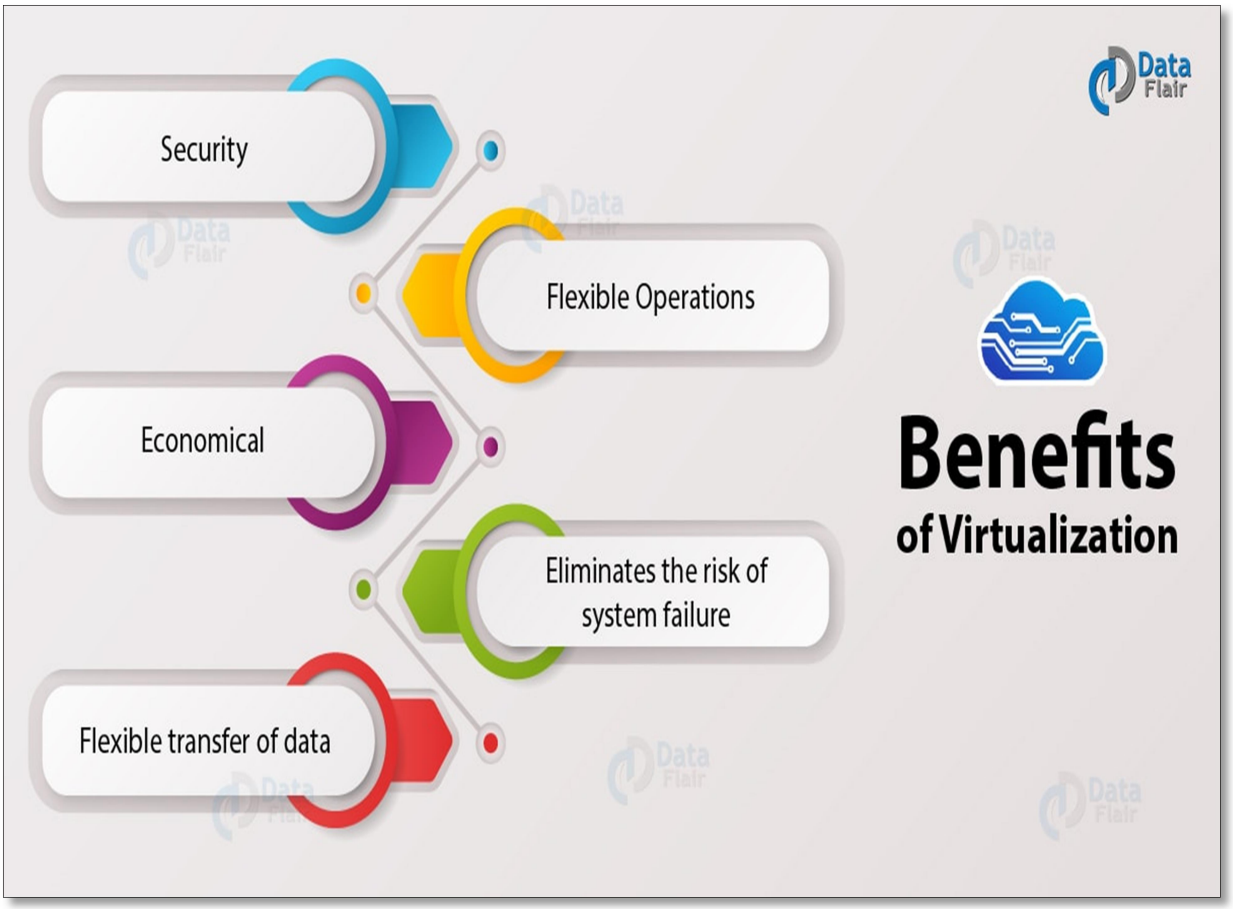
Virtualization in Cloud Computing is a process in which the user of cloud shares the data present in the cloud which can be application software etc. It provides a virtual environment in the cloud which can be software hardware or any other thing. In virtualization, the server and the software application which are required by the **cloud providers** maintain by the third party and in this, the cloud provider please some amount to the third party. It is done because it will be costly if a new version of an application is released and it has to be introduced to the customers.



It can be also explained in a way that with the help of Hypervisor which is software the cloud customer can access server. A hypervisor is connectivity between the server and the virtual environment and distributes the resources between different virtual environments.

Benefits of Virtualization

Virtualizations in **Cloud Computing has numerous benefits**, let's discuss them one by one:



SECURITY

During the process of virtualization **security** is one of the important concerns. The security can be provided with the help of firewalls, which will help to prevent unauthorized access and will keep the data confidential. Moreover, with the help of firewall and security, the data can protect from harmful viruses malware and other cyber threats. Encryption process also takes place with protocols which will protect the data from other threads. So, the customer can virtualize all the data store and can create a backup on a server in which the data can store.

FLEXIBLE OPERATIONS

With the help of a virtual network, the work of it professional is becoming more efficient and agile. The network switch implement today is very easy to use, flexible and saves time. With the help of virtualization in Cloud Computing, technical problems can solve in physical systems. It eliminates the problem of recovering the data from crashed or corrupted devices and hence saves time.

ECONOMICAL

Virtualization in **Cloud Computing**, save the cost for a physical system such as hardware and servers. It stores all the data in the virtual server, which are quite economical. It reduces the wastage, decreases the electricity bills along with the maintenance cost. Due to this, the business can run multiple operating system and apps in a particular server.

ELIMINATES THE RISK OF SYSTEM FAILURE

While performing some task there are chances that the system might crash down at the wrong time. This failure can cause damage to the company but the virtualizations help you to perform the same task in multiple devices at the same time. The data can store in the cloud it can retrieve anytime and with the help of any device. Moreover, there is two working server side by side which makes the data accessible every time. Even if a server crashes with the help of the second server the customer can access the data.

FLEXIBLE TRANSFER OF DATA

The data can transfer to the virtual server and retrieve anytime. The customers or cloud provider don't have to waste time finding out hard drives to find data. With the help of virtualization, it will very easy to locate the required data and transfer them to the allotted authorities. This transfer of data has no limit and can transfer to a long distance with the minimum charge possible. Additional storage can also provide and the cost will be as low as possible.

PROS OF VIRTUALIZATION

1. It can lower overall capital expenditures

With virtualization, you will no longer need to purchase a server for each of the applications you are going to implement in your organization. You will be able to host multiple virtual servers on a single physical machine, which means that you will have lower overall capital expenditures.

2. It can reduce IT costs

This is one of the biggest advantages associated with using this technology in your IT infrastructure, where you do not have to invest in equipment that are incredibly expensive and in-house IT professionals to be able to easily access various software and servers. Also, virtualization is contrived to be affordable, as you do not have to purchase hardware outright, which means more savings. You simply pay a third party, who own and maintain all servers, for their virtualization services without having to spend additional costs.

3. It automates routine tasks

This technology allows you to automate your important routine IT tasks. Something that is as simple as patches for your operating system will become simpler and quicker.

4. It makes a business energy-efficient

Virtualization is seen as revolutionary advancement due to a number of reasons, and one of those having the most impact is energy savings. By implementing such a technology in your business, you will be able to lessen your carbon footprint immensely, which would eventually make a big difference overall. If your organization is environmentally conscious, then virtualization is the way to go.

5. It promotes greater redundancy

Virtualization technologies can help you improve your uptime by allowing greater security and safety while reducing points of contact.

6. It greatly helps with development

This technology is observed to be very helpful in development environments. For example, if you are running several websites, you can make the coding process of these sites easier by using a virtualized server.

7. It allows for faster deployment

In a virtualized environment, provisioning would become quick and simple. You should know that deploying virtual machines is simpler than deploying the older physical versions.

LIST OF CONS OF VIRTUALIZATION

1. It requires high upfront expenditures

Though it was stated that virtualization is cost-effective, when you implement such a strategy from the ground up, it would mean that are you are going to have to invest more money in hardware in the near future. Nevertheless, you will definitely save in the long run, but take note that implementation can get costly.

2. It comes with limitations

One major disadvantage of using virtualization is that it involves various limitations. Take note that not all servers and applications are virtualization-friendly, which means that some aspects of the IT infrastructure of your business might not be compatible with virtualized solutions. You should consider the fact that there are still vendors that do not fully support virtualized environments.

3. It puts data at risk

Since data is crucial to your business, it is of utmost importance that you only choose virtualization solutions that offer adequate data protection. Remember that not having your own server can put your data at risk, making it vulnerable.

4. It comes with the danger of server sprawl

While virtualization is very easy to deploy, there is always the risk that new servers would be added even if they are not necessary. For instance, instead of having 10 virtual servers that you really need, you might have 20 or more.

5. It comes with issues of availability and scalability

Most of the time, the terms availability and scalability are intertwined when it comes to networking, as both are relevant to server virtualization after all. Availability would become a problem if virtualized servers go offline and every website they host would also fail. Scalability is even trickier, considering that virtualization offers a means for several small businesses to share the costs associated with hosting. As you can see, while a business may start out small, there is always the possibility that it could grow big and easily dominate a virtualized server, robbing resources from other websites.

6. It has security flaws

The process of virtualization is designed to separate virtualized resources, but there are still cases where servers were accidentally visible to other people who were not supposed to see them.

7. It comes with the risk of bleed-overs

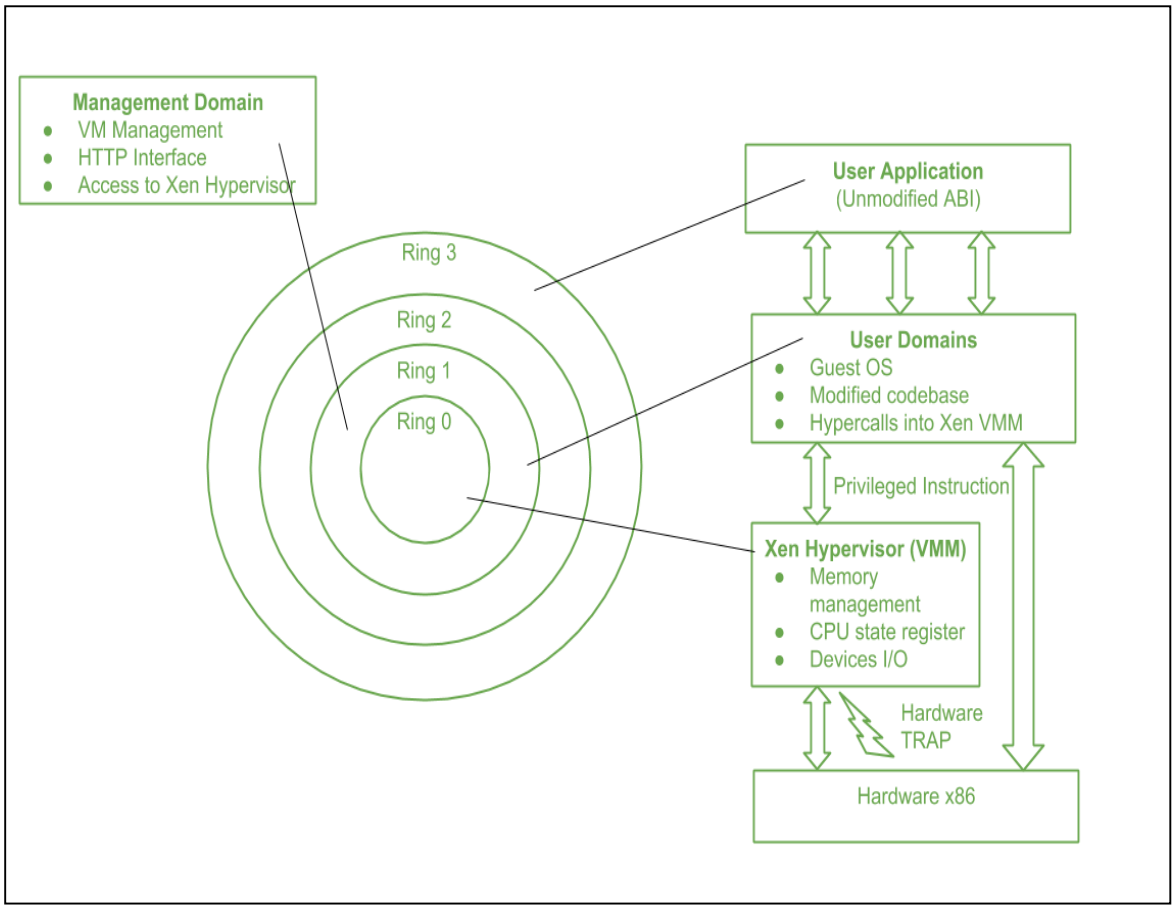
Bleed-overs are possible issues to be aware of when subscribing to a virtualized server, occurring when the contents of a certain server affect other servers. For instance, a chat room that occasionally hosts live discussions with IT industry professionals would experience its chat members receiving a pop-up window stating that they already exceeded the total bandwidth allocation and being booted out of the chat room. What's worse, this can still happen even if your internet service provider (ISP) was not limiting bandwidth consumption. The thing is, there might be another site that is hosted on the same server implementing a shareware bandwidth limitation program, which can limit bandwidth for the server as a whole.

Many businesses and organizations of today are already taking advantage of virtualization because most of their operations are highly dependent on IT processes. This is regarded as a wise investment that makes management of data more efficient and convenient. However, for your organization, you must make sure that you are aware of both the advantages and advantages of using virtualization to ensure that you will be able to implement and manage it properly.

Virtualization - Xen: Paravirtualization

Xen is an open source hypervisor based on paravirtualization. It is the most popular application of paravirtualization. Xen has been extended to compatible with full virtualization using hardware-assisted virtualization. It enables high performance to execute guest operating system. This is probably done by removing the performance loss while executing the instructions requiring significant handling and by modifying portion of the guest operating system executed by Xen, with reference to the execution of such instructions. Hence this especially support x86, which is the most used architecture on commodity machines and servers.

Xen Architecture and Guest OSnManagement



Above figure describes the **Xen** Architecture and its mapping onto a classic x86 privilege model. A **Xen** based system is handled by **Xen** hypervisor, which is executed in the most privileged mode and maintains the access of guest operating system to the basic hardware. Guest operating system are run between domains, which represents virtual machine instances.

In addition, particular control software, which has privileged access to the host and handles all other guest OS, runs in a special domain called Domain 0. This the only one loaded once the virtual machine manager has fully booted, and hosts an HTTP server that delivers requests for virtual machine creation, configuration, and termination. This component establishes the primary version of a shared virtual machine manager (VMM), which is a necessary part of Cloud computing system delivering Infrastructure-as-a-Service (IaaS) solution.

Various x86 implementation support four distinct security levels, termed as rings, i.e., Ring 0, Ring 1, Ring 2, Ring 3

Here, Ring 0 represents the level having most privilege and Ring 3 represents the level having least privilege. Almost all the frequently used Operating system, except for OS/2, uses only two levels i.e. Ring 0 for the Kernel code and Ring 3 for user application and non-privilege OS program. This provides a chance to the Xen to implement paravirtualization. This enables Xen to control unchanged the Application Binary Interface (ABI) thus allowing a simple shift to Xen-virtualized solutions, from an application perspective.

Due to the structure of x86 instruction set, some instructions allow code execution in Ring 3 to switch to Ring 0 (Kernel mode). Such an operation is done at hardware level, and hence between a virtualized environment, it will lead to a TRAP or a silent fault, thus preventing the general operation of the guest OS as it is now running in Ring 1.

This condition is basically occurred by a subset of system calls. To eliminate this situation, implementation in operating system requires a modification and all the sensitive system calls needs re-implementation with hypercalls. Here, hypercalls are the particular calls revealed by the virtual machine (VM) interface of Xen and by use of it, Xen hypervisor tends to catch the execution of all the sensitive instructions, manage them, and return the control to the guest OS with the help of supplied handler.

Paravirtualization demands the OS codebase to be changed, and hence all operating systems can not be referred as guest OS in a Xen-based environment. This condition holds where hardware-assisted virtualization can not be free, which enables to run the hypervisor in Ring 1 and the guest OS in Ring 0. Hence, Xen shows some limitations in terms of legacy hardware and in terms of legacy OS.

In fact, these are not possible to modify to be run in Ring 1 safely as their codebase is not reachable, and concurrently, the primary hardware hasn't any support to execute the in a more privileged mode than Ring 0. Open source OS like Linux can be simply modified as its code is openly available, and Xen delivers full support to virtualization, while components of Windows are basically not compatible with Xen, unless hardware-assisted virtualization is available. As new releases of

OS are designed to be virtualized, the problem is getting resolved and new hardware supports x86 virtualization.

Virtualization - VMware: Full Virtualization

In full virtualization primary hardware is replicated and made available to the guest operating system, which executes unaware of such abstraction and no requirements to modify. Technology of VMware is based on the key concept of Full Virtualization. Either in desktop environment, with the help of type-II hypervisor, or in server environment, through type-I hypervisor, VMware implements full virtualization. In both the cases, full virtualization is possible through the direct execution for non-sensitive instructions and binary translation for sensitive instructions or hardware traps, thus enabling the virtualization of architecture like x86.

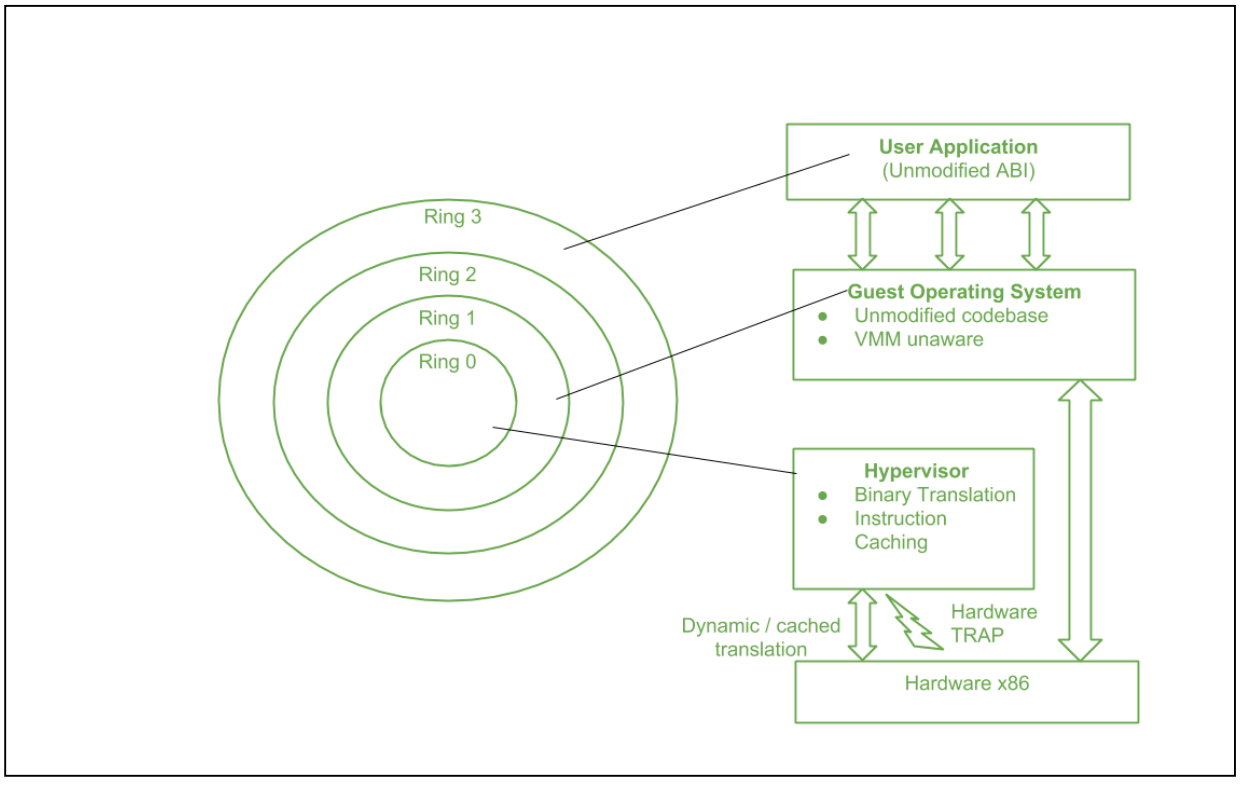
Full Virtualization and Binary Translation

VMware is widely used as it tends to virtualize x86 architectures, which executes unmodified on-top of their hypervisors. With the introduction of hardware-assisted virtualization, full virtualization is possible to achieve by support of hardware. But earlier, x86 guest operating systems unmodified in a virtualized environment could be executed only with the use of dynamic binary translation.

Since the set of sensitive instruction is not a subset of privileged instruction, x86 architecture design is not satisfy the first theorem of virtualization. Due to this different behavior occurs while such instructions are not run in the Ring 0, which is normal in a virtualization environment where the guest OS is run in Ring 1.

Basically, a trap is created, and the method in which it manages differentiation of the solution in which virtualization is applied for x86. In dynamic binary translation, the trap encounters the translation of interrupts or offending instructions into a corresponding set of instructions that establishes the same target without making exceptions. In addition, to expand performance, the corresponding set of instruction is cached, so the translation is not important anymore for further encounters of the same instructions. Below is the figure which demonstrates it.

Full Virtualization Reference Model



The major benefit of this approach is that guests can run unmodified in a virtualized environment, which is an important feature for operating system whose source code does not existed. Binary translation is portable for full virtualization. As well as translation of instructions at

runtime presents an additional overhead that is not existed in other methods like paravirtualization or hardware-assisted virtualization. Contradict, binary translation is only implemented to a subset of the instruction set, while the others are manged through direct execution on the primary hardware. This depletes somehow the impact on performance of binary translation.

Binary Translation: *Binary translation is one specific approach to implementing full virtualization that does not require hardware virtualization features. It involves examining the executable code of the virtual guest for "unsafe" instructions, translating these into "safe" equivalents, and then executing the translated code.*

Advantages of Binary Translation –

1. This kind of virtualization delivers the best isolation and security for Virtual Machine.
2. Truly isolated numerous guest OS can execute concurrently on the same hardware.
3. It is only implementation that needs no hardware assist or operating system assist to virtualize sensitive instruction as well as privileged instruction.

Disadvantages of Binary Translation –

1. It is time consuming at run-time.
2. It acquires a large performance overhead.
3. It employs a code cache to stock the translated most used instructions to enhance the performance, but it increases memory utilization along with the hardware cost.

4. The performance of full virtualization on the x86 architecture is 80 to 95 percent that of the host machine.