UNIT – 4 : VIRTUALIZATION TECHNOLOGY

Definition:

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.

Understanding of Virtualization:

Virtualization, as a computing concept, has existed for over six decades. Its first instance appeared in the late 1960s to facilitate the sharing of computing resources within organisations using mainframe computers. The goal was to utilise the processing power of the mainframe by allowing multiple sub-systems to access its resources.

Since then, the definition of virtualization has undergone several changes, although the fundamental premise remains the same.

Today, virtualization is a term almost synonymous with cloud computing. Cloud service providers are now offering on-demand customised and user-centric virtual environments via the cloud. All these environments share a single physical cloud server that houses all the processing and storage hardware. The users, however, experience these environments as if they are localised.

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**

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.

Characteristics of Virtualization:

Virtualization offers several features or characteristics as listed below: –

- **Distribution of resources:** Virtualization and Cloud Computing technology ensure end-users develop a unique computing environment. It is achieved through the creation of one host machine. Through this host machine, the end-user can restrict the number of active users. By doing so, it facilitates easy of control. They can also be used to bring down power consumption.
- **Accessibility of server resources:** Virtualization delivers several unique features that ensure no need for physical servers. Such features ensure a boost to uptime, and there is less fault tolerance and availability of resources.
- **Resource Isolation:** Virtualization provides isolated virtual machines. Each virtual machine can have many guest users, and guest users could be either operating systems, devices, or applications. The virtual machine provides such guest users with an isolated virtual environment. This ensures that the sensitive information remains protected, and, at the same time, guest users remain inter-connected with one another.
- **Security and authenticity:** The virtualization systems ensure continuous uptime of systems, and it does automatic load balancing and ensures there is less disruption of services.
- **Aggregation:** Aggregation in Virtualization is achieved through cluster management software. This software ensures that the homogenous sets of computers or networks are connected and act as one unified resource.

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.

Drawback of Virtualization:

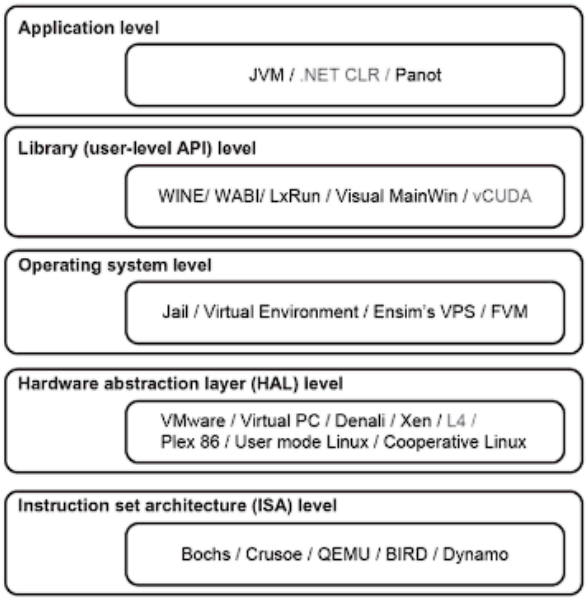
- **High Initial Investment:** Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
- **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud 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.

Implementation Level of Virtualization:

Virtualization is not that easy to implement. A computer runs an OS that is configured to that particular hardware. Running a different OS on the same hardware is not exactly feasible.

To tackle this, there exists a hypervisor. What hypervisor does is, it acts as a bridge between virtual OS and hardware to enable its smooth functioning of the instance.

There are five levels of virtualizations available that are most commonly used in the industry. These are as follows:



1. Instruction Set Architecture Level (ISA):

ISA virtualization can work through ISA emulation. This is used to run many legacy codes written for a different hardware configuration. 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. The virtual machine is formed at this level, which manages the hardware using the virtualization process. 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 on the operating system and the physical server, which uses 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 dedicated virtual hardware resource. In this way, there is no question of any conflict.

4. Library Level:

The operating system is cumbersome, and this is when the applications use the API 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.

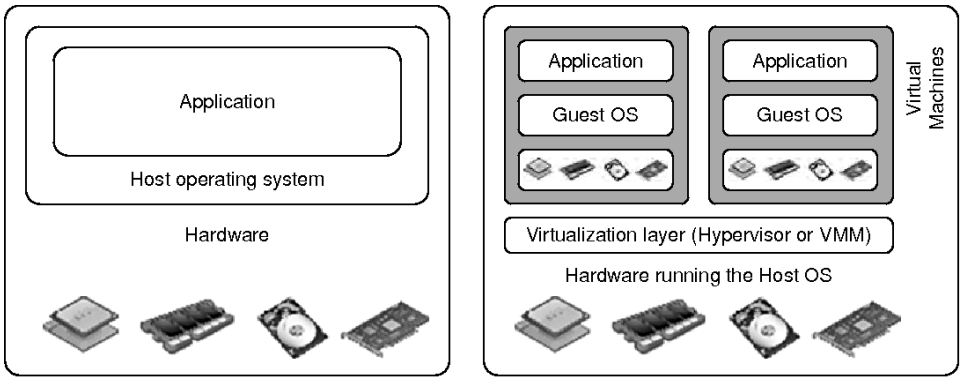
5. Application Level:

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 at the application level of the virtual machine run seamlessly.

Virtualization Structure/Tools and Mechanisms:



(a) Traditional computer (b) After virtualization

In general, there are three typical classes of VM architecture. Above Figure showed the architectures of a machine before and after virtualization.

Before virtualization, the operating system manages the hardware. After virtualization, a virtualization layer is inserted between the hardware and the operating system.

In such a case, the virtualization layer is responsible for converting portions of the real hardware into virtual hardware.

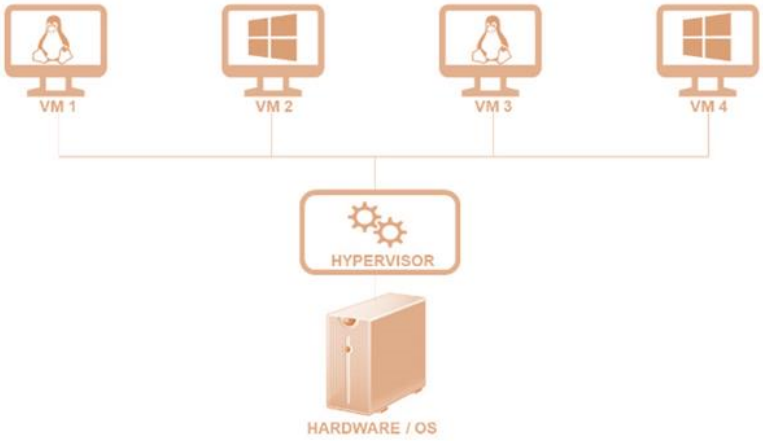
Therefore, different operating systems such as Linux and Windows can run on the same physical machine, simultaneously.

Depending on the position of the virtualization layer, there are several classes of VM architectures, namely the hypervisor architecture, para-virtualization, and host-based virtualization. The hypervisor is also known as the VMM (Virtual Machine Monitor). They both perform the same virtualization operations.

Hypervisor VMware:

Hypervisor is a program that allows multiple Operating Systems to share a single physical hardware. Each operating system will share the host's processor, memory, file storage, and other resources. The hypervisor controls the host processor and resources, allocating what is needed to each operating system. This ensures that he the guest operating systems (called virtual machines) cannot interrupt each other.

Since Hypervisors help create and manage virtual machines (VMs), they are also known as Virtual Machine Monitors or **VMMs**.



Hypervisors help you retain control over a cloud environment's processes and infrastructure and protect sensitive data. It makes cloud-based applications accessible to users in a virtual environment.

Types of Hypervisors:

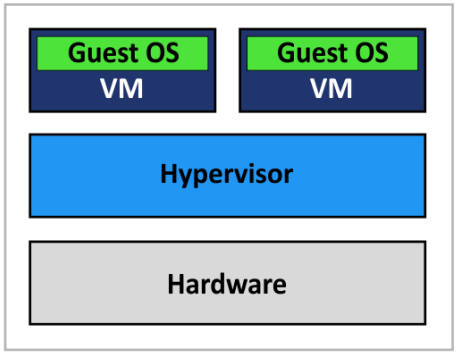
There are 2 types of Hypervisors, as detailed below:

Type 1 Hypervisor:

Type 1 Hypervisor is installed directly on the physical server, also called a **"Native Hypervisor" or "Bare Metal Hypervisor"**. You can also have direct access to the resource of the physical server, which makes the Type 1 Hypervisor highly effective. Furthermore, the design of the Type 1 Hypervisor is highly secure, as it limits the attack surface and the potential for compromise.

Type 1 Hypervisors are the most common choice within the enterprise IT context as it offers strong security, stability, and performance.

Popular Type 1 hypervisors are Nutanix AHV, VMware ESXi, Citrix Hypervisor amongst others.



Type 1 Hypervisor
(Bare-Metal Architecture)

Pros & Cons of Type-1 Hypervisor:

Pros: Such kinds of hypervisors are very efficient because they have direct access to the physical hardware resources (like Cpu, Memory, Network, and Physical storage). This causes the empowerment of the security because there is nothing any kind of the third-party resource so that attacker couldn't compromise with anything.

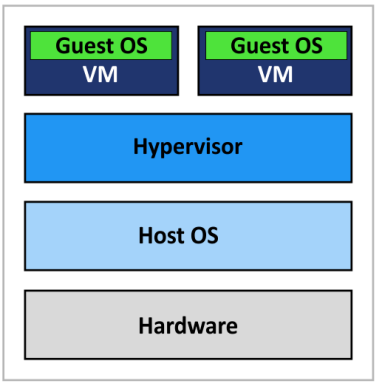
Cons: One problem with Type-1 hypervisors is that they usually need a dedicated separate machine to perform their operation and to instruct different VMs and control the host hardware resources.

Type 2 Hypervisor:

Type 2 Hypervisors run as applications on a physical server's pre-existing OS. The host operating system, sits between the physical server and the Hypervisor. So, it is also called "hosted" Hypervisors.

However, Type 2 Hypervisors are not a good choice for server-based environments, as they have higher latency and risk exposure than Type 1. Type 2 Hypervisors are easy to install. It can work well in specific use cases, like individual PC users who want to run only one OS. In such cases, performance and security are not principal concerns.

Example: Installing Linux over Windows using VirtualBox



Type 2 Hypervisor
(Hosted Architecture)

Pros & Cons of Type-2 Hypervisor:

Pros: Such kind of hypervisors allows quick and easy access to a guest Operating System alongside the host machine running. These hypervisors usually come with additional useful features for guest machines. Such tools enhance the coordination between the host machine and the guest machine.

Cons: Here there is no direct access to the physical hardware resources so the efficiency of these hypervisors lags in performance as compared to the type-1 hypervisors, and potential security risks are also there an attacker can compromise the security weakness if there is access to the host operating system so he can also access the guest operating system.

Choosing the Right Hypervisor:

Type 1 hypervisors offer much better performance than Type 2 ones because there's no middle layer, making them the logical choice for mission-critical applications and workloads. But that's not to say that hosted hypervisors don't have their place – they're much simpler to set up, so they're a good bet if, say, you need to deploy a test environment quickly. One of the best ways to determine which hypervisor meets your needs is to compare their performance metrics. These include CPU overhead, the amount of maximum host and guest memory, and support for virtual processors. The following factors should be examined before choosing a suitable hypervisor:

1. Understand your needs: The company and its applications are the reason for the data center (and your job). Besides your company's needs, you (and your co-workers in IT) also have your own needs. Needs for a virtualization hypervisor are:

a. Flexibility
b. Scalability
c. Usability
d. Availability
e. Reliability
f. Efficiency
g. Reliable support

2. The cost of a hypervisor: For many buyers, the toughest part of choosing a hypervisor is striking the right balance between cost and functionality. While a number of entry-level solutions are free, or practically free, the prices at the opposite end of the market can be staggering. Licensing frameworks also vary, so it's important to be aware of exactly what you're getting for your money.

3. Virtual machine performance: Virtual systems should meet or exceed the performance of their physical counterparts, at least in relation to the applications within each server. Everything beyond meeting this benchmark is profit.

4. Ecosystem: It's tempting to overlook the role of a hypervisor's ecosystem – that is, the availability of documentation, support, training, third-party developers and consultancies, and so on – in determining whether or not a solution is cost-effective in the long term.

5. Test for yourself: You can gain basic experience from your existing desktop or laptop. You can run both VMware vSphere and Microsoft Hyper-V in either VMware Workstation or VMware Fusion to create a nice virtual learning and testing environment.

HYPERVISOR REFERENCE MODEL:

There are 3 main modules coordinates in order to emulate the underlying hardware:

1. **Dispatcher:** The dispatcher behaves like the entry point of the monitor and reroutes the instructions of the virtual machine instance to one of the other two modules.
2. **Allocator:** The allocator is responsible for deciding the system resources to be provided to the virtual machine instance. It means whenever a virtual machine tries to execute an instruction that results in changing the machine resources associated with the virtual machine, the allocator is invoked by the dispatcher.
3. **Interpreter:** The interpreter module consists of interpreter routines. These are executed, whenever a virtual machine executes a privileged instruction.

Kernel-Based Virtual Machine (KVM):

Kernel-based Virtual Machine (KVM) is a software feature that you can install on physical Linux machines to create virtual machines. A virtual machine is a software application that acts as an independent computer within another physical computer. It shares resources like CPU cycles, network bandwidth, and memory with the physical machine. KVM is a Linux operating system component that provides native support for virtual machines on Linux. It has been available in Linux distributions since 2007.

Why is KVM important?

Kernel-based Virtual Machine (KVM) can turn any Linux machine into a bare-metal hypervisor. This allows developers to scale computing infrastructure for different operating systems without investing in new hardware. KVM frees server administrators from manually provisioning virtualization infrastructure and allows large numbers of virtual machines to be deployed easily in cloud environments.

Businesses use KVM because of the following advantages.

High performance: KVM is engineered to manage high-demanding applications seamlessly. All guest operating systems inherit the high performance of the host operating system—Linux. The KVM hypervisor also allows virtualization to be performed as close as possible to the server hardware, which further reduces process latency.

Security: Virtual machines running on KVM enjoy security features native to the Linux operating system, including Security-Enhanced Linux (SELinux). This ensures that all virtual environments strictly adhere to their respective security boundaries to strengthen data privacy and governance.

Stability: KVM has been widely used in business applications for more than a decade. It enjoys excellent support from a thriving open-source community. The source code that powers KVM is mature and provides a stable foundation for enterprise applications.

Cost efficiency: KVM is free and open source, which means businesses do not have to pay additional licensing fees to host virtual machines.

Flexibility: KVM provides businesses many options during installations, as it works with various hardware setups. Server administrators can efficiently allocate additional CPU, storage, or memory to a virtual machine with KVM. KVM also supports thin provisioning, which only provides the resources to the virtual machine when needed.

How does KVM work?

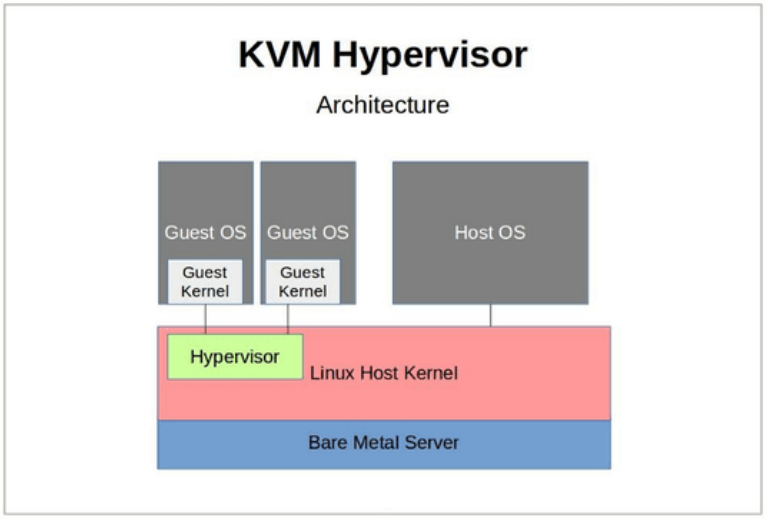
Kernel-based Virtual Machine (KVM) requires a Linux kernel installation on a computer powered by a CPU that supports virtualization extensions. Specifically, KVM supports all x86 CPUs, a family of computer chips capable of processing the Intel x86 instruction language.

How to enable KVM:

Once you have installed the Linux kernel, you need to install the following additional software components on the Linux machine:

- A host kernel module
- A processor-specific module
- An emulator
- A range of other Linux packages for expanding KVM’s capabilities and performance

Once loaded, the server administrator creates a virtual machine via the command line tool or graphical user interface. KVM then launches the virtual machine as an individual Linux process. The hypervisor allocates every virtual machine with virtual memory, storage, network, CPU, and resources.



What is the difference between KVM and VMware?

VMware is the software company that produces VMware ESXi, a commercially licensed virtualization solution. VMware hypervisors are used for enterprise applications, with virtual machines capable of handling heavy workloads.

Kernel-based Virtual Machine (KVM) and VMware ESXi both provide virtualization infrastructure to deploy type 1 hypervisors on the Linux kernel. However, KVM is an open-source feature while VMware ESXi is available via commercial licenses.

Organizations using VMware's virtualization components enjoy professional support from its technical team. Meanwhile, KVM users rely on a vast open-source community to address potential issues.

Xen:

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.

Architecture of Xen:

The Xen hypervisor consists of a small amount of code that runs directly on the host's hardware. This code provides the basic virtualization services, including memory management, CPU scheduling, and I/O device virtualization. Above the hypervisor is the domain 0 operating system, which is a privileged guest operating system that has direct access to the physical hardware. Domain 0 is responsible for managing the other guest operating systems, allocating resources to them, and providing virtualized I/O services.

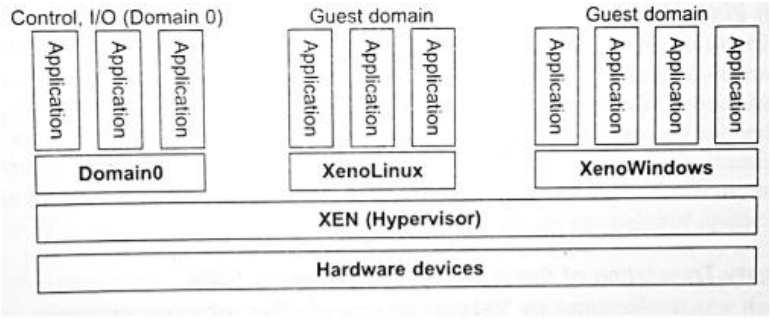


Fig. Xen Architecture

The guest operating systems run in domains that are completely isolated from each other and from domain 0. Each guest operating system is assigned a certain amount of memory and CPU resources, and can access virtualized I/O devices provided by domain 0. Xen supports a wide range of operating systems, including Linux, Windows, and various flavors of BSD.

Features of Xen:

1. **Hypervisor Architecture**: Xen employs a lightweight hypervisor architecture directly on physical hardware, enabling efficient virtualization.
2. **Paravirtualization**: Xen supports paravirtualization, enhancing performance by modifying guest operating systems to cooperate with the hypervisor.
3. **Hardware Virtualization**: Xen leverages hardware virtualization extensions for near-native performance and compatibility with unmodified guest operating systems.
4. **Live Migration**: Xen facilitates live migration, allowing seamless movement of running virtual machines between physical hosts without service interruption.
5. **Strong Isolation**: Xen provides robust isolation between guest domains, ensuring security, stability, and independence of operation for each virtual machine.
6. **Resource Management**: Xen offers tools and mechanisms for efficient allocation and management of physical resources (CPU, memory, disk, network) among virtualized instances, optimizing performance and scalability.

Virtualization of CPU, Memory, I/O Devices:

To support virtualization, processors such as the x86 employ a special running mode and instructions, known as hardware-assisted virtualization. In this way, the VMM and guest OS run in different modes and all sensitive instructions of the guest OS and its applications are trapped in the VMM. To save processor states, mode switching is completed by hardware. For the x86 architecture, Intel and AMD have proprietary technologies for hardware-assisted virtualization.

Hardware Support for Virtualization:

Hardware support for virtualization encompasses features and extensions integrated into modern CPUs and chipsets to enhance the performance, security, and efficiency of virtualized environments.

These features include hardware virtualization extensions like Intel VT-x and AMD-V, which enable CPU virtualization and I/O virtualization, enhancing the ability to run multiple virtual machines concurrently while improving resource allocation and isolation. Memory management unit (MMU) virtualization facilitates memory isolation between virtual machines, while I/O virtualization features such as SR-IOV and VT-d optimize access to physical I/O devices.

CPU Virtualization:

Virtual Machine is a copy of existing system and instructions of it are executed on the host processor in native mode. Unprivileged instructions of Virtual Machine runs directly on the host machine for higher efficiency.

CPU is virtualized if it executes the Virtual Machine's privileged and unprivileged instructions in the CPU user mode and VMM executes in supervisor mode. Privileged instructions like control and behavior instructions of a VM are executed by securing in the VMM. Here VMM works like a unified mediator for hardware access from different VMs to guarantee the correctness and stability of the whole system. But all CPU's not support virtualization. As RISC CPU can be virtualized but x86 CPU not support virtualization.

Memory Virtualization:

The traditional operating systems supports virtualization by making page tables. All modern CPUs contains memory management unit (MMU) and translation look-a-side buffer (TLB) to perform virtualization. The memory of the physical system is virtualized and allocated to the virtual machine as its physical memory. So that means two stage mapping is implemented by the guest OS and VMM for virtual memory to

physical memory and physical memory to machine memory. Virtual OS of virtual machine controls the mapping of virtual memory with the physical memory but it cannot directly access the machine memory. VMM performs the mapping of the physical memory with the machine memory.

I/O Virtualization:

I/O virtualization manages the I/O requests between virtual machine and the physical machine. There are three ways to implement I/O virtualization:

Full device emulation: It provides the emulation of the well-known real-world devices.

Para-virtualization: It is also known as the split driver model which contains frontend driver and backend driver. They both works on different domains and they interact with each other by using block of shared memory. Frontend driver manages the I/O requests of the virtual OS and the backend driver manages the real I/O devices. So, para virtualization is better than full device emulation.

Direct I/O virtualization: It allows Virtual machine to access devices directly.

Virtual Cluster and Resources Management:

In cloud computing, virtual clusters and resource management play crucial roles in optimizing resource utilization and providing efficient and scalable services. Here's an overview of virtual clusters and resource management in the context of cloud computing:

1. Virtual Clusters:

- Virtual clusters are logical groupings of virtual machines (VMs) or containers within a cloud environment.

- They provide a way to create isolated and dedicated environments for specific applications or workloads.

- Virtual clusters allow organizations to achieve better resource utilization by consolidating multiple workloads on a shared infrastructure.

- They enable flexibility and scalability as virtual clusters can be easily provisioned, scaled up or down, and managed independently.

2. Resource Management:

- Resource management involves efficiently allocating and managing the computing resources (e.g., CPU, memory, storage) in a cloud environment.

- It aims to optimize resource utilization, performance, and cost-effectiveness while meeting the demands of various applications and users.

- Resource management techniques and tools are employed to ensure fair resource allocation, load balancing, and scalability.

Key aspects of resource management in cloud computing include:

- **Resource provisioning:** Automatically provisioning resources (VMs, containers, storage) based on demand to ensure efficient utilization and avoid resource shortages.

- **Load balancing:** Distributing workloads across available resources to optimize performance and avoid bottlenecks.

- **Elasticity:** Dynamically scaling resources up or down based on demand to ensure optimal performance and cost efficiency.

- **Performance monitoring:** Continuously monitoring resource utilization and performance metrics to identify and resolve performance issues.

- **Prioritization and scheduling:** Managing resource allocation and scheduling tasks based on priority, deadlines, and policies.

- **Reservation and isolation:** Providing mechanisms to guarantee resources for specific applications or users and ensure isolation between workloads.

3. Resource Management Techniques:

Cloud platforms employ various resource management techniques to optimize resource utilization and performance:

- **Virtualization:** Virtualization technologies, such as hypervisors, enable the creation and management of virtual machines, allowing better resource sharing and isolation.

- **Orchestration and automation:** Tools and frameworks like Kubernetes, OpenStack, and Apache Mesos help automate resource provisioning, scheduling, and management tasks.

- **Auto-scaling:** Automated scaling mechanisms dynamically adjust resource capacity based on predefined rules or thresholds.

- **Policy-based management:** Applying policies and rules to govern resource allocation, prioritization, and access control.

- **Predictive analytics:** Utilizing historical data and machine learning algorithms to predict resource demands and optimize resource allocation.

Physical vs Virtual Clusters:

Aspect	Physical Clusters	Virtual Clusters
Resource Management	Managed at hardware level	Managed at software level (hypervisor)
Hardware Dependency	Dependent on physical servers	Abstracted from underlying hardware
Isolation	Limited isolation between applications	Strong isolation between virtual clusters
Scalability	Limited scalability, requires adding hardware	Dynamic scalability, can scale resources up or down as needed
Flexibility	Limited flexibility, fixed hardware resources	Flexible, can adjust resources dynamically
Resource Utilization	Typically, lower due to fixed allocation	Higher due to dynamic resource allocation
Maintenance	Hardware maintenance required	Software-based maintenance, easier updates
Cost	Higher initial hardware investment	Lower initial investment, pay-as-you-go model
Disaster Recovery	Complex disaster recovery processes	Easier disaster recovery with virtualization
Overhead	Lower overhead due to direct hardware access	Higher overhead due to virtualization layer

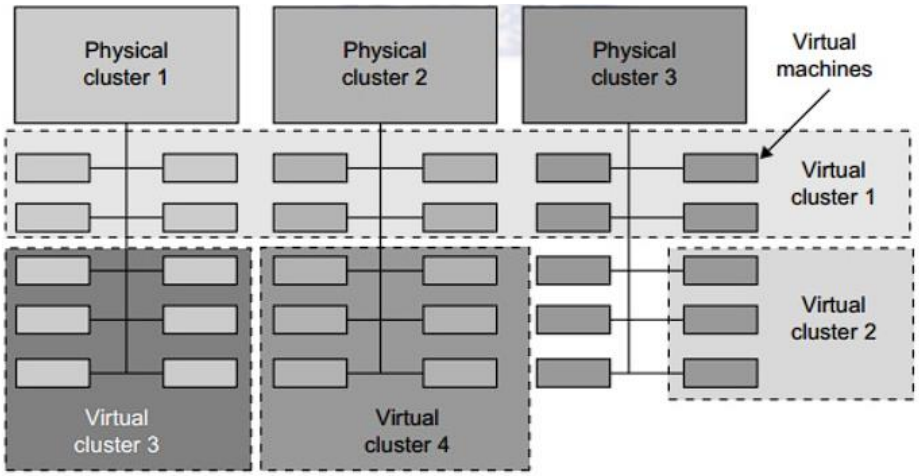
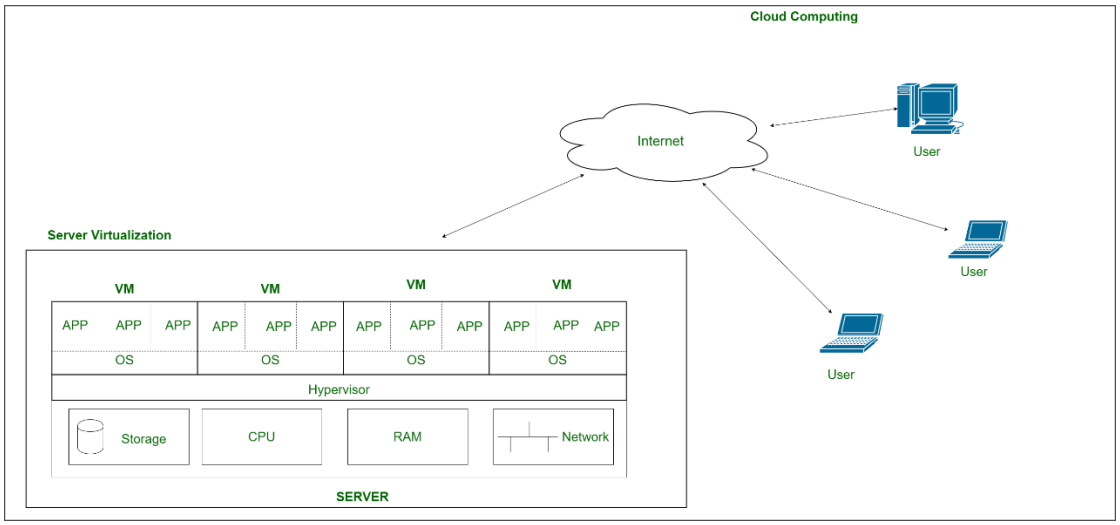


FIGURE 3.18

A cloud platform with four virtual clusters over three physical clusters shaded differently.

Virtualization of Server:

This is a kind of virtualization in which the masking of server resources takes place. Here, the central server (physical server) is divided into multiple different virtual servers by changing the identity number, and processors. So, each system can operate its operating systems in an isolated manner. Where each sub-server knows the identity of the central server. It causes an increase in performance and reduces the operating cost by the deployment of main server resources into a sub-server resource. It's beneficial in virtual migration, reducing energy consumption, reducing infrastructural costs, etc.



Server Virtualization

To implement Server Virtualization, hypervisor is installed on server which manages and allocates host hardware requirements to each virtual machine. This hypervisor sits over server hardware and regulates resources of each VM. A user can increase or decrease resources or can delete entire VM as per his/her need. This servers with VM created on them is called server virtualization and concept of controlling this VM by users through internet is called Cloud Computing.

Advantages of Server Virtualization:

- Each server in server virtualization can be restarted separately without affecting the operation of other virtual servers.
- Server virtualization lowers the cost of hardware by dividing a single server into several virtual private servers.
- One of the major benefits of server virtualization is disaster recovery. In server virtualization, data may be stored and retrieved from any location and moved rapidly and simply from one server to another.
- It enables users to keep their private information in the data centers.

Disadvantages of Server Virtualization:

- The major drawback of server virtualization is that all websites that are hosted by the server will cease to exist if the server goes offline.
- The effectiveness of virtualized environments cannot be measured.
- It consumes a significant amount of RAM.
- Setting it up and keeping it up are challenging.
- Virtualization is not supported for many essential databases and apps.

Virtualization of Desktop:

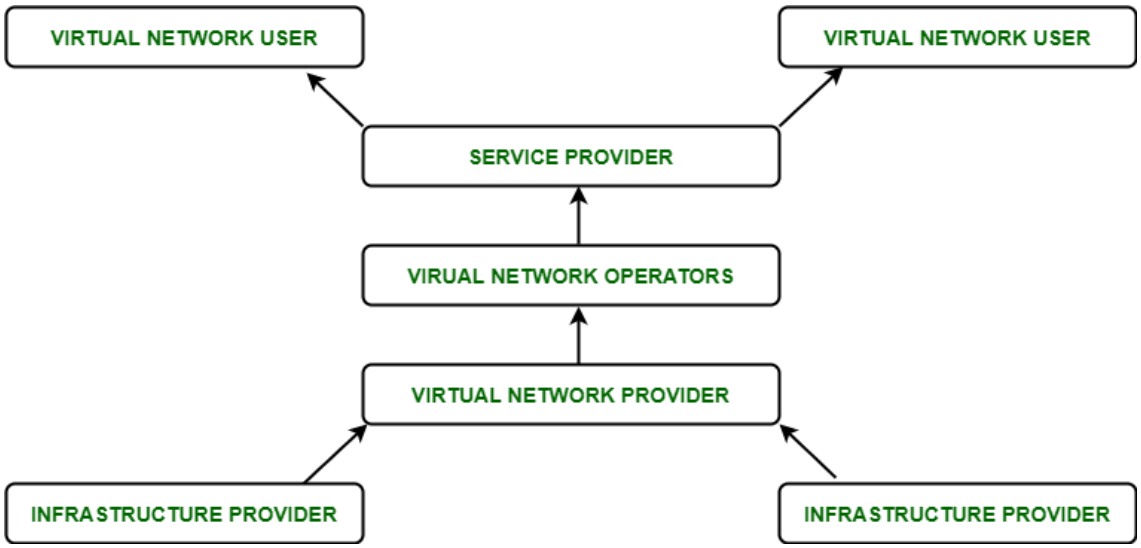
Desktop virtualization allows the users' OS to be remotely stored on a server in the data center. It allows the user to access their desktop virtually, from any location by a different machine. Users who want specific operating systems other than Windows Server will need to have a virtual desktop. The main benefits of desktop virtualization are user mobility, portability, and easy management of software installation, updates, and patches.

Types of Desktop Virtualization:

1. **Hosted Virtual Desktops (HVD)**:
   - Desktop environments run on servers in a data center.
   - Users access their virtual desktops using thin clients, web browsers, or dedicated client software.
2. **Virtual Desktop Infrastructure (VDI)**:
   - A centralized infrastructure hosts multiple virtual desktop instances.
   - Each user is assigned a dedicated virtual machine or session.
3. **Shared Session/Desktop Virtualization**:
   - Multiple users share the same virtual desktop environment.
   - Each user gets a session within the same operating system instance.

Virtualization of Network:

The ability to run multiple virtual networks with each having a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that are potentially confidential to each other. Network virtualization provides a facility to create and provision virtual networks, logical switches, routers, firewalls, load balancers, Virtual Private Networks (VPN), and workload security within days or even weeks.



Network Virtualization

Types of Network Virtualization:

1. **Virtual Local Area Networks (VLANs)**:
   - Segmenting a physical network into multiple virtual networks, each operating as a separate broadcast domain.
   - Enables isolation and security between different network segments.
2. **Virtual Private Networks (VPNs)**:
   - Creating secure, encrypted connections over a public network (like the internet) to connect remote users or branch offices to a central network.
   - Provides secure access to resources while maintaining privacy and confidentiality.
3. **Software-Defined Networking (SDN)**:
   - Decoupling the network control plane from the data plane and centralizing network intelligence in software-based controllers.
   - Allows for programmable, automated network management and dynamic provisioning of network services.

4. **Network Function Virtualization (NFV)**:
   - Virtualizing network functions such as firewalls, routers, load balancers, and WAN optimization appliances.
   - Running these network functions as software instances on commodity hardware rather than dedicated appliances.
5. **Overlay Networks**:
   - Creating virtual networks (overlays) on top of an existing physical network infrastructure.
   - Enables the deployment of virtual networks with specific characteristics or services independent of the underlying physical network.

Tools for Network Virtualization:

1. **Physical switch OS**: It is where the OS must have the functionality of network virtualization.
2. **Hypervisor:** It is which uses third-party software or built-in networking and the functionalities of network virtualization.

Functions of Network Virtualization:

- It enables the functional grouping of nodes in a virtual network.
- It enables the virtual network to share network resources.
- It allows communication between nodes in a virtual network without routing of frames.
- It restricts management traffic.
- It enforces routing for communication between virtual networks.

Advantages of Network Virtualization:

1. Efficient resource use by abstracting network services from hardware.
2. Improved security with isolated virtual networks.
3. Flexible provisioning for rapid service deployment.
4. Cost-efficient consolidation and automated management.
5. Scalability for dynamic resource allocation.

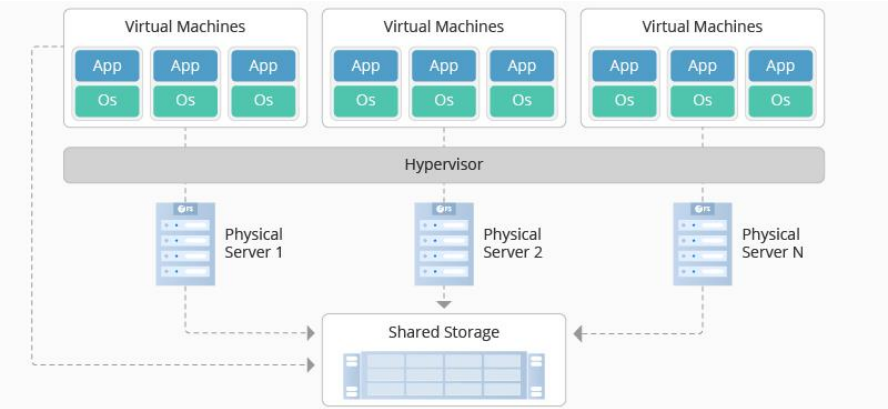
Disadvantages of Network Virtualization:

- It needs to manage IT in the abstract.
- It needs to coexist with physical devices in a cloud-integrated hybrid environment.
- Increased complexity.
- Upfront cost.
- Possible learning curve.

Virtualization of Data-Centre:

Data center virtualization is the transfer of physical data centers into digital data centers using a cloud software platform, so that companies can remotely access information and applications.

In a virtualized data center, a virtual server, also called a software-defined data center (SDDC) is created from traditional, physical servers. This process abstracts physical hardware by imitating its processors, operating system, and other resources with help from a hypervisor. A hypervisor (or virtual machine monitor, VMM, virtualizer) is a software that creates and manages a virtual machine. It treats resources such as CPU, memory, and storage as a pool that can be easily reallocated between existing virtual machines or to new ones.



Benefits of Data Center Virtualization:

1. Data center virtualization optimizes hardware use, reducing costs and energy consumption.
2. Scalability allows quick adjustments to resources based on demand.
3. Robust disaster recovery ensures business continuity during failures or disasters.
4. Simplified management tools streamline IT operations.
5. Enhanced security features isolate virtual machines, reducing security risks.

Drawbacks of Data Center Virtualization:

1. Increased complexity in managing virtualized infrastructure can require specialized skills and training.
2. Virtualization introduces performance overhead due to the hypervisor layer, impacting resource utilization.
3. Security vulnerabilities within the hypervisor or virtualization software can pose risks to the entire virtualized environment.
4. Licensing costs for virtualization software and management tools can add to the overall expenses.
5. Dependency on virtualization technology can lead to vendor lock-in and limit flexibility in adopting alternative solutions.