4

CHAPTER

VIRTUALIZATION

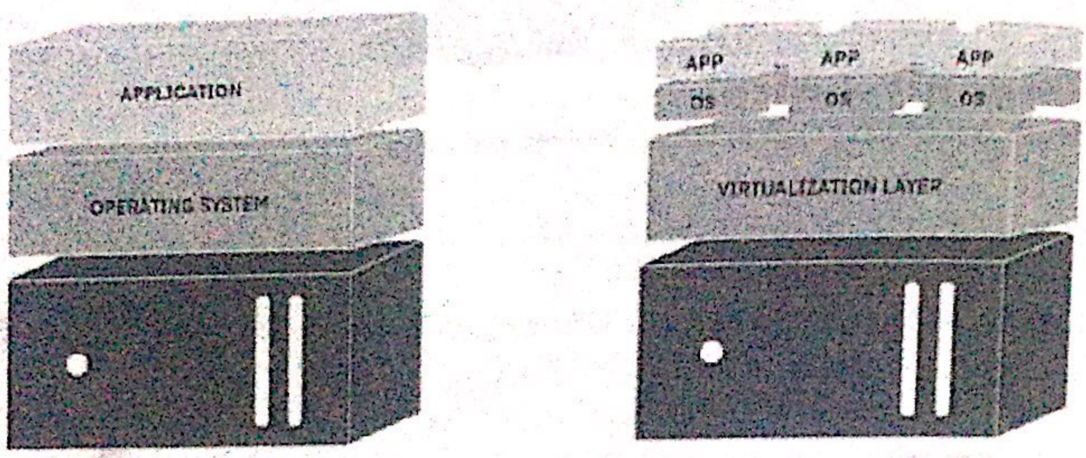
CHAPTER OUTLINE

After studying this chapter, students will be able to understand the:

- Traditional and Virtual Environment
- Overview of Virtualization
- Virtual Machine
- Types of Virtualizations
- TAXONOMY OF VIRTUAL MACHINES
- Hypervisor Management Software

TRADITIONAL AND VIRTUAL ENVIRONMENT

In a typical physical computing environment, software like an operating system (OS) or corporate application has direct access to the underlying computer hardware and components, such as the CPU, memory, storage, specific chipsets, and OS driver versions. This caused significant problems with program setup and made it impossible to relocate or reinstall the software on new hardware, such as while restoring backups after a breakdown or disaster.Virtualization involves the installation of a hypervisor, which acts as an intermediary between the program and the underlying hardware. Once a hypervisor is installed, the software uses virtual representations of computer components, such as virtual processors, rather than actual processors.



Traditional Architecture   Traditional Architecture

Figure 4.1 Traditional and Virtual Architecture

Virtualized computing resources are supplied as separate instances known as Virtual Machines (VMs), into which operating systems and applications can be loaded. Virtualized systems may host numerous VMs at the same time, but each VM is logically separated from the others. This implies that a malware attack or a VM crash will not impact the other VMs. Support for numerous VMs significantly improves system usage and efficiency. Instead of purchasing ten different servers to host ten physical applications, a single virtualized server might support the same ten applications deployed on ten virtual machines on the same system. This increased hardware utilization is a significant benefit of virtualization, as it provides great potential for system consolidation, decreasing the number of servers and power consumption in business data centers.

OVERVIEW OF VIRTUALIZATION

The formation of a virtual version of something, such as a server, a desktop, a storage device, an operating system, or network resources is referred to as virtualization. Virtualization is a technology that allows numerous consumers and organizations to share a single physical instance of a resource or application. It accomplishes this by giving a logical name to a physical storage device and delivering a reference to that physical resource when needed.

Usually, business data centers include a large number of servers, the majority of which are inactive since the responsibility is fulfilled by only a few servers on the network. This wastes expensive resources like hardware, electricity, maintenance, and cooling requirements. By dividing a real server into numerous virtual servers, virtualization helps to enhance resource utilization. These virtual servers seem and behave as if they were independent physical servers, each with its operating system and applications. Virtualization is a concept that is utilized in practically every IT architecture to assist double the capacity of physical devices. It aids in making the most use of current resources, lowering total corporate costs. Virtualization software (hypervisor) is used by businesses to construct virtual computers, networks, desktops, and servers.

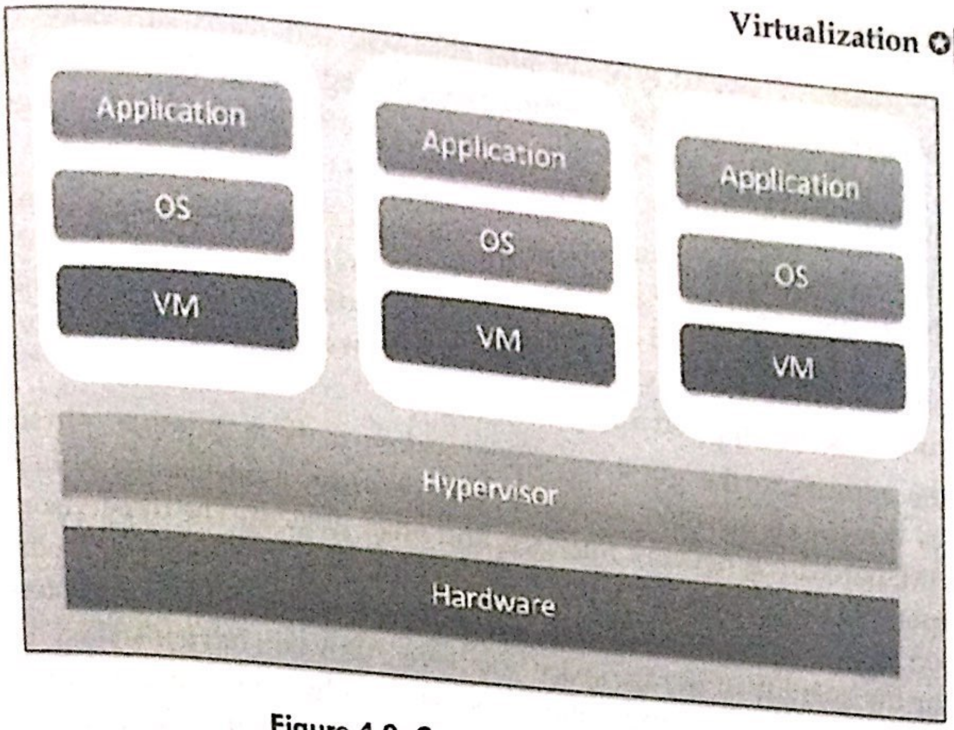


Figure 4.2: Concept of Virtualization

Virtualization software simplifies IT management and makes it more cost-effective to buy and run. It brings about a variety of favorable changes, such as lower hardware costs, improved disaster recovery solutions, higher IT agility, improved performance, and faster resource availability. Understanding the various forms of virtualization is essential for integrating it. Businesses can select the sort of virtualization they needed based on their needs.

In a virtualized data center, software known as the hypervisor is put on real hardware which serves as a platform for virtual machines. In a **vSphere** environment, for example, the hypervisor is *ESXi*. The hypervisor dynamically allocates physical hardware resources to virtual computers as needed to enable their operation. The hypervisor enables virtual computers to run independently of the underlying physical hardware. A virtual machine, for example, can be relocated from one physical host to another, or its virtual disks can be switched from one kind of storage to another, without impacting the virtual machine's operation.

Because virtual machines are detached from the underlying physical hardware, virtualization enables you to pool physical computing resources like CPUs, memory, storage and networking into pools of resources that can be made dynamically and flexibly accessible to virtual machines. You may also leverage a variety of features that boost the availability and security of your virtual infrastructure with proper management tools, such as *vCenter Server*.

VIRTUAL MACHINE

A virtual machine is a computer program that, like a physical computer, runs an operating system and applications. The virtual machine is made up of a set of specification and configuration files and is supported by a host's physical resources. Every virtual machine has virtual devices that perform the same functions as actual hardware while providing extra mobility, management, and security benefits.

A virtual machine (VM) is a software program that not only behaves like a separate computer but can also do functions such as executing apps and programs like a separate computer. A virtual computer sometimes referred to as a "guest," is constructed within another computer environment known as a "host." A single host may support several virtual machines at the same time.

Examples:

- VirtualBox (Windows/Mac/Linux, Free)
- Parallels (Windows/Mac/Linux, $79.99*)
- VMware (Windows/Linux, Basic: Free, Premium: $189*)
- QEMU (Linux, Free)
- Windows Virtual PC (Windows, Free)

A virtual machine consists of several types of files that you store on a supported storage device. The configuration file, virtual disk file, NVRAM setting file, and log file are the primary files that comprise a virtual machine. If you use *vSphere*, for example, you configure virtual machine settings using the vSphere Web Client or the vSphere Client. You do not need to make any changes to the key files.

Virtual machines (VMs) enable you to run other operating systems alongside your present one. The virtual OS will function as if it were a separate software on your machine. This is perfect for trying out various operating systems, such as Windows 10 or alternative Linux distributions. Virtual machines can also be used to execute software on operating systems for which it was not developed. A virtual machine, for example, may execute Windows apps on a Mac.

The virtual machine appears to the guest operating system to be a genuine, physical computer. The emulation engine of the virtual machine, known as a hypervisor, manages the virtual hardware, which includes a CPU, RAM, hard drive, network interface, and other devices. The hypervisor's virtual hardware components correspond to real hardware on your physical machine.A virtual machine's virtual hard disk, for example, is saved as a file on your hard drive. You may run many virtual computers on your PC. You are only restricted by the quantity of storage space you have. After you have installed numerous operating systems, launch your virtual machine application, and select which virtual machine to boot. The guest operating system launches and operates as a window on your host operating system.

Virtual Machine Technology

In virtual machine technology, the hypervisor is an important component. A hypervisor is a specialized software that perfectly emulates the CPU, memory, hard drive, network, and other hardware resources of a PC client or server, allowing virtual computers to share the resources. The hypervisor may replicate various separated virtual hardware platforms, allowing virtual machines to run Linux and Windows Server operating systems on the same underlying physical host. Virtualization saves money by eliminating the requirement for actual hardware devices. Virtual machines use hardware more effectively, which decreases hardware quantities and related maintenance costs, as well as power and cooling consumption. They also make administration easier since virtual hardware never fails. Virtual environments can help administrators ease backups, disaster recovery, new installations, and fundamental system management duties.

Virtual machines do not require the use of specialized, hypervisor-specific hardware. Virtualization does require more bandwidth, storage, and processing capacity than a traditional server or desktop if the physical hardware is going to host multiple running virtual machines. To improve hardware resource use, VMs may be readily moved, cloned, and transferred across host servers. Because VMs on a physical host might consume uneven amounts of resources – one may occupy all of the available physical storage while another store very little – IT professionals must balance VMs with available resources.

The usage of virtual machines brings many critical management issues, many of which may be addressed through basic systems administration best practices and VM management tools. Consolidation has various dangers, such as overtaxing resources or even suffering outages on several VMs owing to a single physical hardware failure. While the cost savings grow as more virtual machines use the same hardware platform, the danger increases. It is conceivable to run hundreds of virtual machines on the same hardware, but if the hardware platform breaks, dozens or hundreds of virtual machines may be lost.

Although some other companies also provide virtual machine software, two major vendors dominate the market: VMware and Microsoft. VMware offers a mature product range that has been used in the IT industry for many years. Despite being a latecomer to virtualization, Microsoft is making significant progress. Many IT departments run non-critical apps on Microsoft virtual machines because the virtualization environment is less expensive than VMware's solutions. Several open-source alternatives are fast emerging, with new features and better stability, but lack the maturity and support choices of these vendor services.

System virtual machines serve as a substitute for physical machines. They provide the capability required to run whole operating systems. A hypervisor employs native execution to share and control hardware, allowing several environments to operate on the same physical computer while being isolated from one another. Modern hypervisors employ hardware-assisted virtualization, which makes use of virtualization-specific hardware, typically from host CPUs. Process virtual machines are intended to run computer applications in a platform-independent environment.

TYPES OF VIRTUALIZATIONS

The most important virtualization types are listed here, which have their importance in the virtualization environment.

- Desktop Virtualization
- Network Virtualization
- Server and Machine Virtualization
- Storage Virtualization
- System-level or Operating Virtualization
- Application Virtualization
- Compute Virtualization

Desktop Virtualization

Desktop Virtualization, which is also known as client virtualization, is a virtualization technology that is used to isolate a computer's desktop environment from the actual machine. Because the "virtualized" desktop is kept on a centralized, or remote server rather than the actual computer being virtualized. Desktop virtualization is considered a form of client-server computing architecture.

Desktop virtualization occurs when a hypervisor is used to run virtual machines on the host server. A hypervisor can be installed directly on the host computer or over the operating system (like Windows, Mac, and Linux). Virtualized desktops do not use the hard drive of the host machine; instead, they operate on a distant central server. This form of virtualization is beneficial for development and testing teams who need to build or test programs on many operating systems. Another advantage of desktop virtualization is that it allows you to access your desktop from any location by allowing you to log in remotely.

Virtual Desktop Infrastructure or Interface (VDI) is a common desktop virtualization technique. This sort of desktop virtualization employs the server computing model, as desktop virtualization is supported in this situation via hardware and software. The desktop environment is hosted by VDI in a virtual machine (VM) that runs on a centralized or remote server.

Desktop virtualization allows users to keep their desktops on a single, central server. Users can connect to the central server through a LAN, WAN, or the Internet. There are several advantages to using desktop virtualization, including lower total cost of ownership, improved security, lower energy costs, less downtime, and centralized administration.

Network Virtualization

Network Virtualization is a means of combining available network resources by dividing available bandwidth into channels, each of which is independent of the others and may be given to a specific server or device in real-time. Each channel is safeguarded in its way. From a single computer, each subscriber gets shared access to all network resources.

For a human administrator, network administration may be a time-consuming and difficult task. Network virtualization is meant to increase the administrator's productivity, efficiency, and job satisfaction by automating many of these duties, masking the underlying complexity of the network. Network virtualization allows the complete computer network to be managed and monitored as a single administrative unit. Admins can monitor diverse network infrastructure parts such as routers and switches from a single software-based administrator's panel. Network virtualization contributes to network optimization in terms of data transmission speeds, flexibility, dependability, security, and scalability. It raises the overall productivity and efficiency of the network. Administrators may more easily manage and distribute resources while maintaining high and consistent network performance.

The goal of network virtualization is to improve network performance, dependability, flexibility, scalability, and security. Network virtualization is believed to be highly useful in networks that undergo unexpected, substantial, and rapid spikes in consumption.

Server and Machine Virtualization

Server and machine virtualization, often known as 'Hardware virtualization,' is a virtualization approach that includes splitting a physical server into several tiny, virtual servers using virtualization software. Each virtual server in server virtualization runs many operating system instances at the same time.

A typical business data center has a massive number of servers. Many of these servers are inactive since the burden is spread to only a subset of the network's servers. This wastes expensive hardware resources as well as power, maintenance, and cooling needs. Server virtualization divides a single server's resources into many virtual servers. These virtual servers can function as standalone devices. Server virtualization enables enterprises to run many independent operating systems (guests or virtual) with varying settings on a single (host) server. The approach also lowers the hardware costs associated with maintaining a large number of physical servers, allowing firms to optimize their server architecture.

> The practice of separating a physical server into numerous unique and separated virtual servers using a software application is known as server virtualization. Each virtual server is capable of running its operating system.

Server virtualization aims to enhance resource usage by dividing real servers into several virtual servers, each with its operating system and applications. Server virtualization makes each virtual server seem and behave like a real server, thus increasing the capacity of each actual system. The concept of server virtualization is frequently used in IT infrastructure to save costs by making better use of existing resources. For small to medium-scale applications, virtualizing servers is frequently a useful choice. This technology is commonly utilized to provide low-cost web hosting services as well.

Key Benefits of Server Virtualization

- Higher server ability
- Cheaper operating costs
- Eliminate server complexity
- Increased application performance
- Deploy workload quicker

Types Of Server Virtualization

- Paravirtualization
- Full Virtualization
- Hardware-Assisted Virtualization
- Kernel level Virtualization
- System-Level or OS Virtualization

Paravirtualization

Paravirtualization (PV) is a virtualization technology in which a guest operating system (guest OS) is tweaked and recompiled before installation inside a virtual machine (VM) to allow all guest OS within the system to share resources and successfully collaborate, rather than attempting to emulate an entire hardware environment. It is based on the Hypervisor and this paradigm handles a large portion of the emulation and trapping overhead in software-implemented virtualization. The update made to the Guest operating system improves speed since the redesigned guest operating system communicates directly with the hypervisor, removing emulation overhead.

HYPERVISOR

The goal of virtualizations is to separate a computer's physical resources from the software that uses them. A hypervisor is a software application that is installed on the host system to offer a layer of abstraction. Hypervisor directly communicates with a physical server's disk space and CPU. OS and programs interact with the virtualized resources abstracted by the hypervisor rather than the physical resources of the real host computer.

The hypervisor monitors the physical server's resources and keeps each virtual server independent and unaware of the other virtual servers. It also relays resources from the physical server to the correct virtual server as it runs applications. The details of the hypervisor will be discussed later in this unit.

With paravirtualization, the virtual machine is no longer required to catch privileged instructions. Trapping, a method of dealing with unexpected or unacceptable circumstances, can be time-consuming and have a negative influence on performance in systems that use full virtualization.

For Example, Paravirtualization is an expansion of a technology that has existed for years in the IBM operating system. Xen, an open-source software project, incorporates PV. Xen virtualizes the memory and processor using an altered Linux kernel. It also virtualizes the I/O using custom guest OS device drivers.

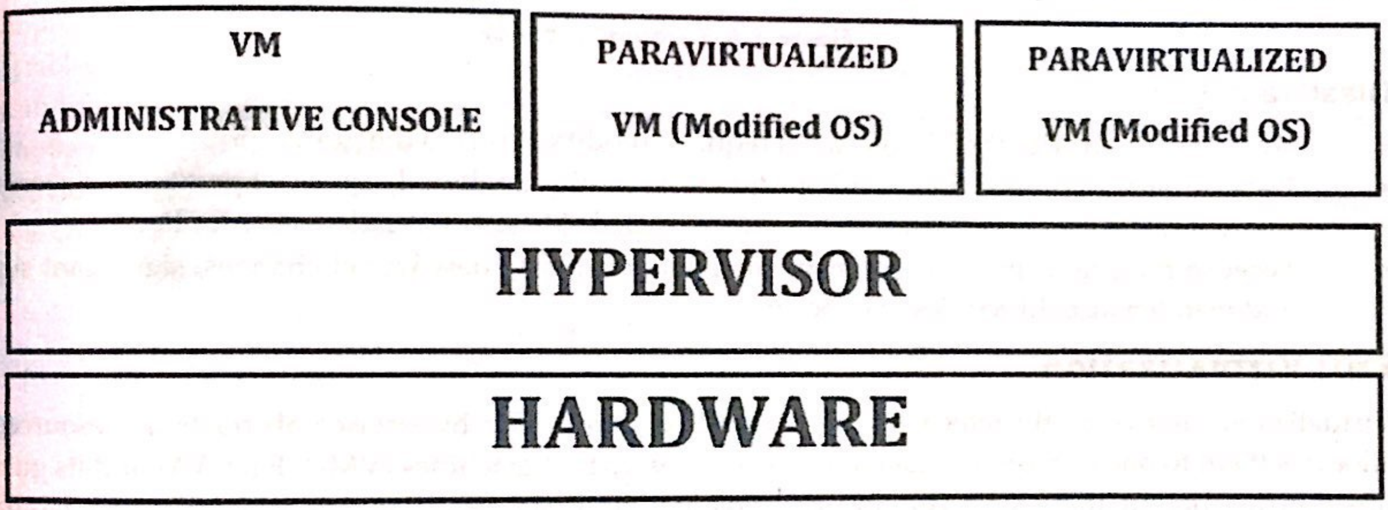


Figure 4.3: Paravirtualization

Advantages:

- Direct communication between the guest kernel and the hypervisor enhances overall performance.
- The thin software layer developed in PV manages virtual server traffic by enabling a single guest OS to have access to the physical hardware device while blocking access to all other guest OS.
- There is less virtualization overhead since PV does not attempt to entirely reconstruct the hardware.
- PV does not provide device drivers since it makes use of the drivers that are already available in the guest OS. Therefore, organizations can take full advantage of the hardware in the server instead of being limited to hardware with available drivers, as is the case in full virtualization.

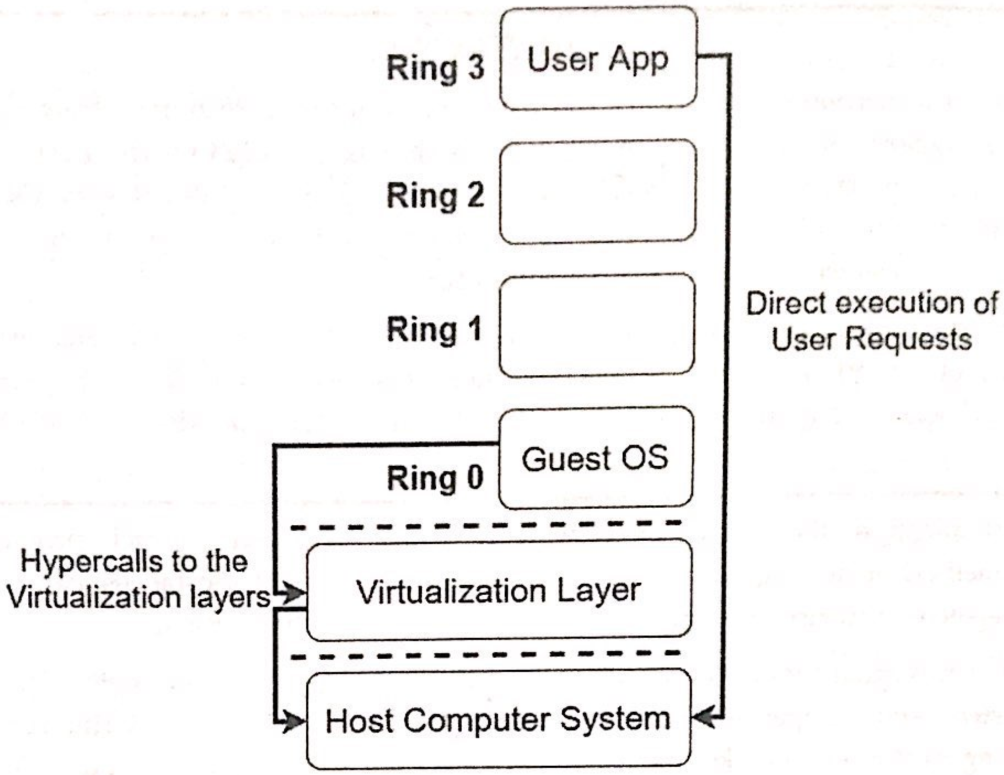


Figure 4.4: Paravirtualization

Disadvantages:

- Any interaction with the PV interfaces requires modifications to the guest OS
- Because paravirtualization cannot function with unaltered guest operating systems, its interoperability and portability with systems such as Microsoft Windows are limited.
- Because the production environment requires extensive guest kernel changes, significant support and maintenance difficulties may occur.

Full Virtualization

Virtualization is frequently referred to as full virtualization. The hypervisor abstracts all resources and allocates them to one or more logical entities known as virtual machines (VMs). Each VM and its guest OS function as though they were running on separate machines, and the OS and programs require no additional adjustments or adaptations to function in a conventional VM. Each VM is logically separated from the others. Unless specifically configured, VMs do not interact or share resources. The hypervisor intercepts the machine actions that the operating system uses to execute I/O or change the system status. Following trapping, these actions are mimicked in software, and the status codes provided are remarkably similar to what the real hardware would produce. As a result, an unmodified operating system can operate on top of the hypervisor.

For example, the *VMWare ESX* server uses this method. A customized Linux version known as Service Console is used as the administrative operating system. It is not as fast as Paravirtualization.

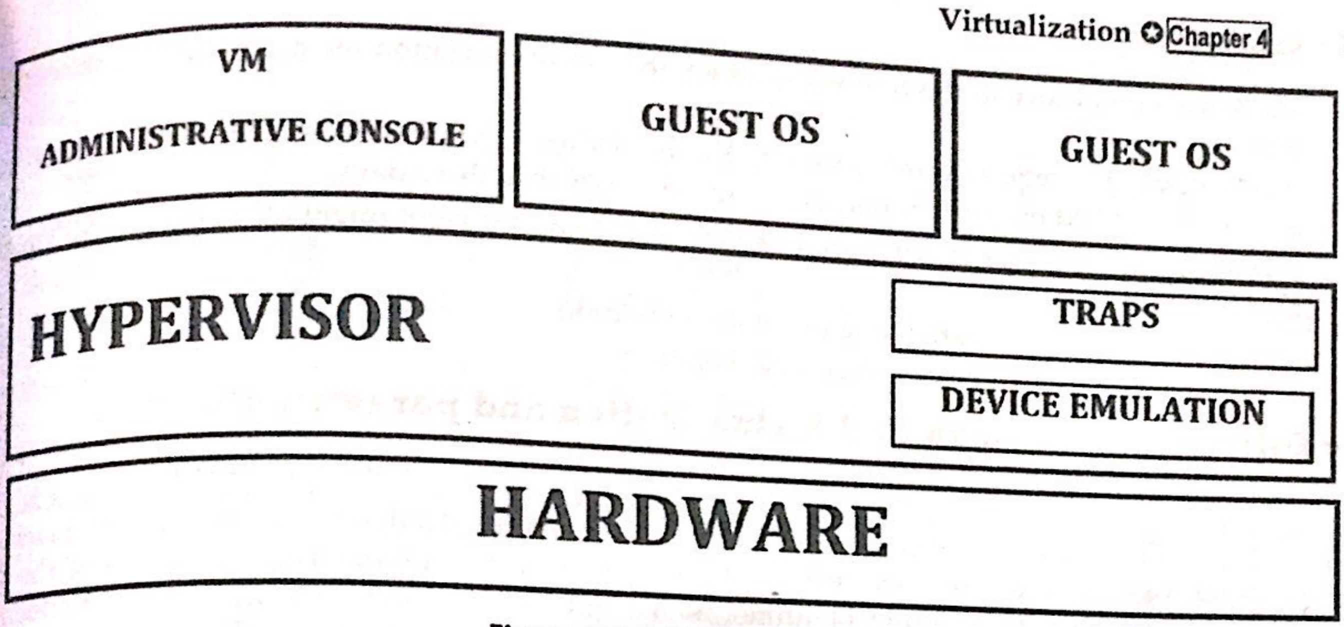


Figure 4.5: Full Virtualization

Advantages

- Full virtualization does not require OS assistance to virtualize a computer or create VMs so no modification to the Guest operating system is required. The hypervisor manages resources and translates instructions quickly and it also enables the OS to emulate new hardware, which can improve reliability, security, and productivity in a system.
- Enables admins to run applications on a completely isolated guest OS, which provides support for multiple OS simultaneously - such as Windows Server 2016 in one VM, Windows Server 2019 in another VM, and Ubuntu in another VM, and so on - all on the same computer.
- Provides features, such as easy VM backups and migrations, enabling VMs to be easily moved from one computer to another without disrupting the VM and its workload.

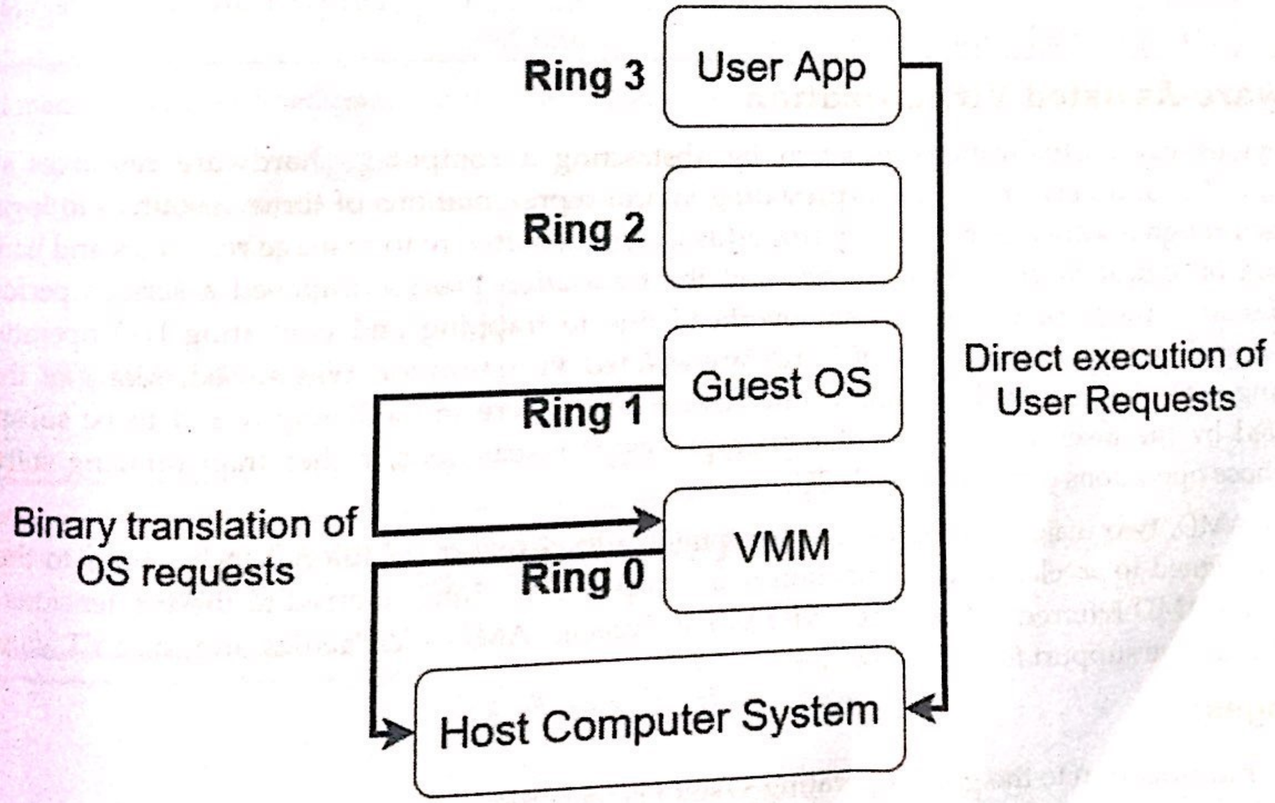


Figure 4.6: Full Virtualization

Disadvantages:

- The use of hypervisors and hardware-assisted processors offers excellent performance compared to non-virtualized OS and application deployments, but the hypervisor itself adds a layer of additional complexity to the technology stack that an organization must pay for, implement, and manage.

- Applications that require direct access to the hardware of the underlying machine will not work effectively in a VM but such applications are extremely rare these days.
- A physical server problem or failure in a virtualized environment might affect every VMs running on the system.
- Slower than paravirtualization due to device emulation.
- Installation of the new device driver is challenging.

Key Differences Between Full Virtualization and paravirtualization

S. N.	Full Virtualization	Paravirtualization
1.	In Full virtualization, the virtual machine permits the execution of the instructions with running of unmodified OS in an entirely isolated way.	In paravirtualization, the virtual machine does not implement full isolation of the OS but rather provides a different API which is utilized when the OS is subjected to alteration.
2.	Full Virtualization is less secure.	Paravirtualization is more secure than Full Virtualization.
3.	Full Virtualization uses binary translation and a direct approach as a technique for operations.	Paravirtualization uses *hypercalls* at compile time for operations.
4.	Full Virtualization is slower than paravirtualization in operation.	Paravirtualization is faster in operation as compared to full virtualization.
5.	Full Virtualization is more portable and compatible.	Paravirtualization is less portable and compatible.
6.	Examples of full virtualization are Microsoft and Parallels systems.	Examples of paravirtualization are VMware and Xen.

Hardware-Assisted Virtualization

The previous two virtualizations function by abstracting a computer's hardware resources such as memory, CPUs, and network I/O and providing logical representations of those resources to logical VM instances through a software hypervisor.This adds a layer of software to manage resources and handle the translation of logical to physical resources and the translation process imposed a serious performance issue. Similarly, much of the hypervisor overhead due to trapping and emulating I/O operations. To overcome such issues, the concept of hardware-assisted virtualization was raised. Many of the time-consuming activities required to handle full virtualization were immediately found to be substantially accelerated by the insertion of particular microprocessor instructions, rather than utilizing software to imitate those operations outside of the CPU.

Intel and AMD, two major microprocessor suppliers, added sets of additional instructions to their CPU families designed to accelerate virtualization-related operations. Intel referred to these extensions as Intel VT, whereas AMD referred to them as AMD-V. *For Example,* AMD – V Pacifica and Intel VT Vanderpool provide hardware support for virtualization.

Advantages:

- No modification to the guest operating system is required
- Very less hypervisor overhead

Disadvantages:

- Hardware support required

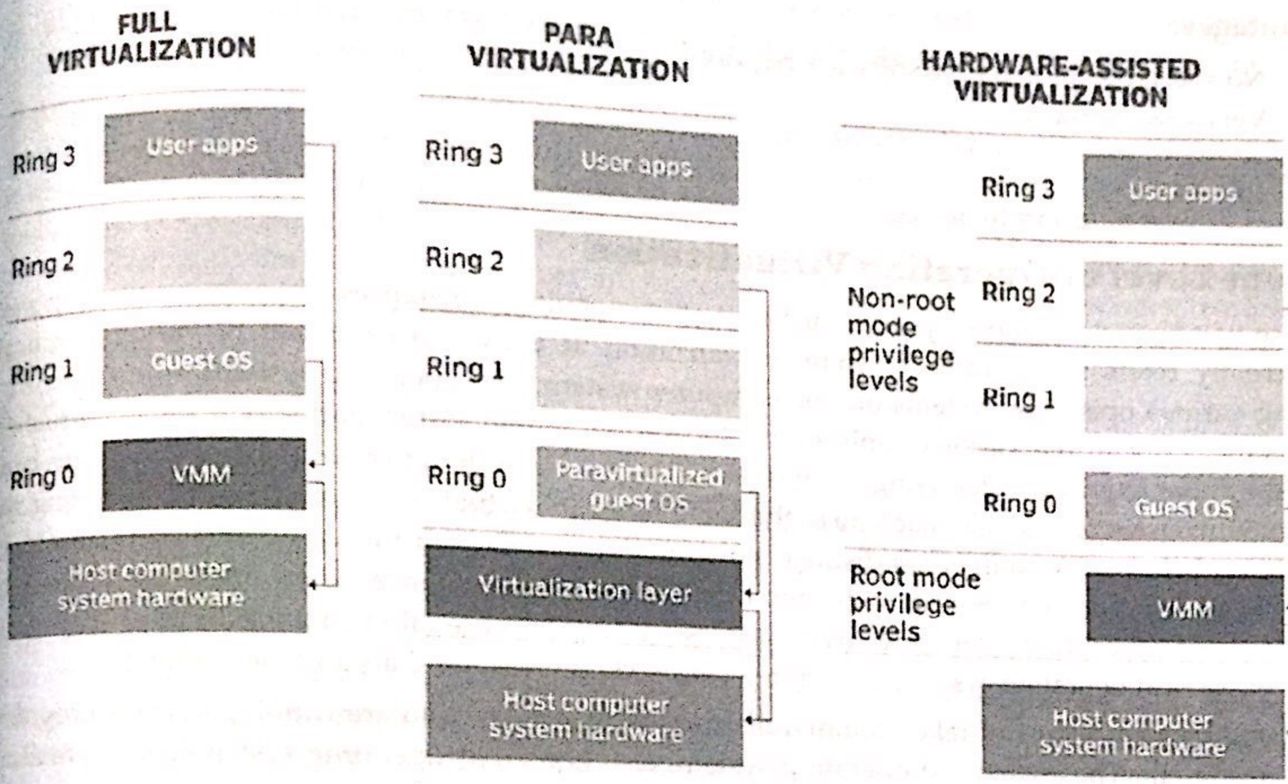


Figure 4.7: Full Virtualization, Paravirtualization, and Hardware-Assisted Virtualization

Kernel Level Virtualization

It does not employ a hypervisor and instead runs a different version of the Linux kernel that views the associated virtual machine as a user-space process on the physical host. This makes running numerous virtual machines on a single host simple. A device driver is used to connect the core Linux kernel to the virtual machine. Kernel-level virtualization is a type of server virtualization that is more specialized.

Examples: User – Mode Linux (UML) and Kernel Virtual Machine (KVM)

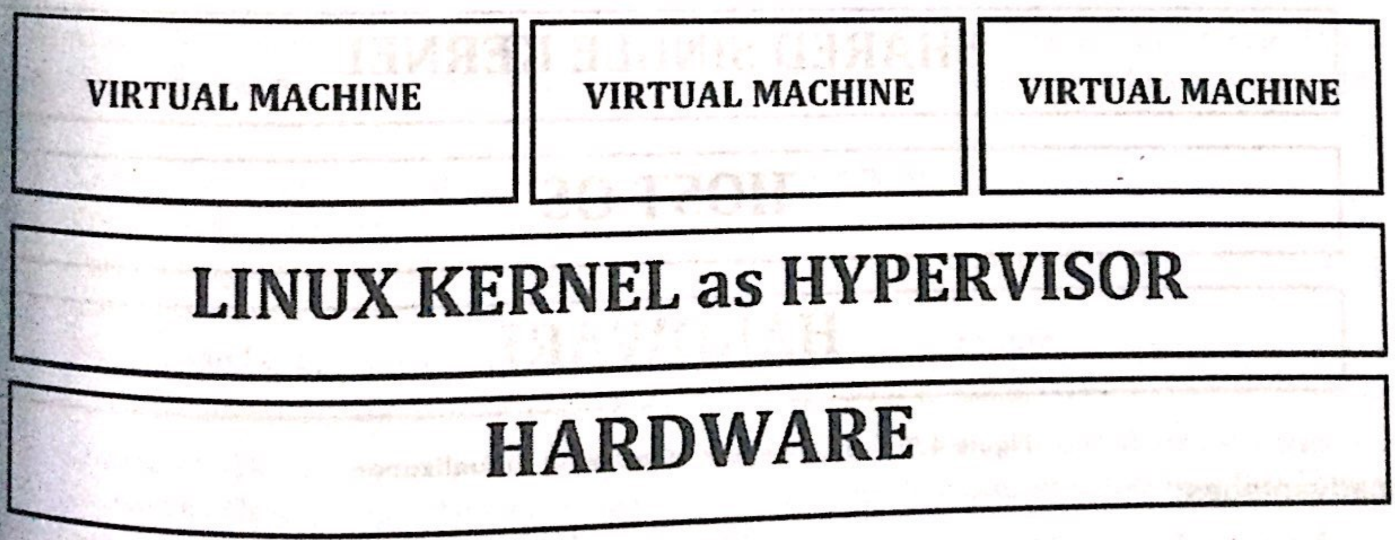


Figure 4.8: Kernel Level Virtualization

Kernel-based Virtual Machine (KVM) is an open-source virtualization technology built into Linux. Specifically, KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs).

Advantages:

- No special administrative software required,
- Very less overhead

Limitations:

- Hardware Support Required

System-Level or Operating Virtualization

The use of software to allow system hardware to run multiple instances of various operating systems concurrently refers to Operating System virtualization. It allows to execution of various applications needing various operating systems on one computer system. The operating systems do not conflict with one another or with the various applications. Operating system virtualization is a server virtualization technology that requires customizing a conventional operating system to run numerous programs handled by numerous users on a single machine at the same time. OS virtualization modifies the operating system such that it behaves like numerous distinct, separate systems. Even if they are on the same machine, the operating systems do not interact with each other. On a single instance of the operating system kernel, numerous but conceptually separate environments are run. Because all virtual machines share a common kernel of the host operating system, this strategy is also known as the shared kernel method.

The virtualized environment takes commands from several users who are running various programs on the same system. The virtualized operating system, also known as operating system-level virtualization, handles users and their demands independently.

*Examples:*FreeVPS, Linux Vserver, and OpenVZ, etc.

Advantages:

- Significantly lightweight than complete machines
- Can host many virtual servers
- Enhanced Security and Isolation

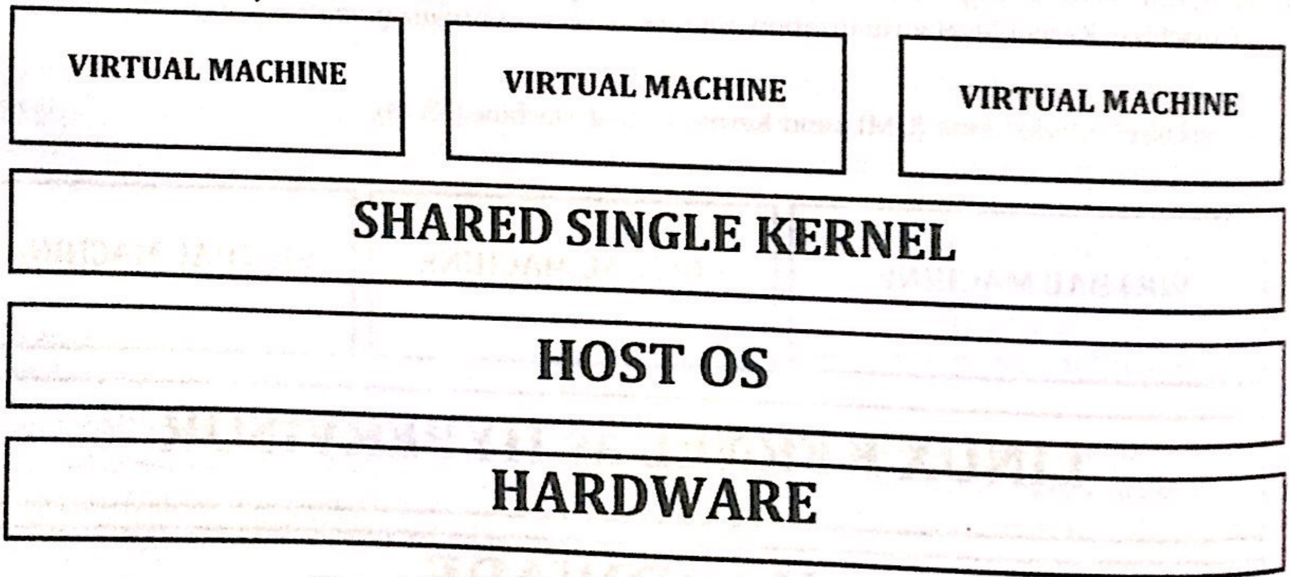


Figure 4.9: System-Level or Operating Virtualization

Disadvantages:

- Kernel or driver problem can take down all virtual servers.

Storage Virtualization

Storage Virtualization is the technique of combining physical storage from numerous network storage devices to appear as a single storage unit. To simplify application and network-independent storage management, the procedure entails abstracting and covering the core functions of a storage device from the host application, host servers, or a general network. Storage virtualization is the consolidation of physical storage from several network storage devices into what appears to be a single storage device administered from a centralized interface.

Storage virtualization, which is also known as cloud storage, enables storage administrators to conduct backup, archiving, and recovery operations more quickly - and in less time - by masking the true complexity of a storage area network (SAN). Administrators can use software programs to deploy virtualization, or they can use hardware and software hybrid appliances. It also enables administrators to efficiently distribute, relocate, update, and set up resources throughout the corporate infrastructure. There are two types of Storage Virtualization - Block Level Storage Virtualization and File Level Storage Virtualization.

Block-Level Storage Virtualization

Block-level storage is a form of storage that is extensively used in Storage Area Networks (SANs) and other large-scale storage systems by big corporations and companies. A block-level storage system allows each block to be handled as an independent hard drive, and the blocks are handled by a server operating system.

Storage at the block level Virtualization is a storage solution that offers applications and users a flexible, logical arrangement of storage capacity while abstracting its physical location. It intercepts I/O requests to that logical capacity as a software layer and translates them to the relevant physical locations. As a result, virtualization enables administrators to supply storage capacity when and where it is required while shielding users from potentially disruptive aspects like expansion, data protection, and system mainfenance.

- Block-level storage is usually deployed in the SAN environment.
- Block-level storage offers boot-up of systems that are connected to them.
- Block-level storage can be used to store files and can work as storage for special applications like databases, Virtual machine file systems, and so on.
- Block-level storage data transportation is more efficient and reliable.
- Block-level storage supports individual formatting of file systems like NFS, NTFS, VMFS (VMware) which are required by the applications.
- Each storage volume can be treated as an independent disk drive, and it can be controlled by an external server operating system.

In terms of administrative complexity, block-based storage systems are more difficult than file-based storage systems; this is the price you pay for the extra flexibility. Administrators of block storage devices must:

- Carefully manage and distribute storage on a per-server basis.
- Control storage security levels (i.e., RAID).
- Track storage device performance to verify that it continues to satisfy the demands of the server and applications.
- Manage and keep an eye on the storage communications infrastructure.

This block-level shared storage is used by a variety of applications, including:

1. **Databases** - When clustering the databases, the clustered databases require shared storage.
2. **Exchange** - Despite significant advancements to Exchange, Microsoft still does not offer file-level or network-based storage. Only block-level storage is available.
3. **VMware** - Although VMware may utilize file-level storage using Network File System (NFS), it is far more typical to install VMware servers with shared VMFS volumes on block-level storage.
4. **Server boot** - Servers can be configured to boot from block-level storage with the correct storage device.

File-level Storage Virtualization

File virtualization is a type of storage virtualization that works at the computer file level. It entails combining various storage devices into a single logical file pool. The establishment of an abstraction layer between file servers and the clients that use those file servers is referred to as file virtualization. Once installed, the file virtualization layer maintains files and file systems across servers, allowing administrators to provide clients with a single logical file mount for all servers. File data and metadata are still stored on the file servers.

While this setup may appear to add unnecessary IT complexity, file virtualization offers numerous major benefits, including a global namespace for indexing files on network file servers. Furthermore, this virtual file storage consolidation enables the sharing of surplus storage space among file servers. Data migrations across file servers may be performed invisibly to end-users and applications, which is suitable in a tiered storage environment.

In a nutshell, file virtualization enables businesses to have access to separated storage space on network file servers and execute smooth file migrations between them. File virtualization can be implemented as an appliance or as a commercially available server running file virtualization software. The decision is usually influenced by the expense as well as the amount of management and disruption involved.

- The File-level storage is simple to use and implement.
- It stores files and folders, and the visibility is the same to the clients accessing and to the system which stores it.
- This level of storage is inexpensive to be maintained when it is compared to its counterpart i.e., block-level storage.
- Network-attached storage systems usually depend on this file-level storage.
- File-level storage can handle access control, integration with corporate directories; and so on.

Scalability, which might include the number of file systems, files, servers, or I/O performance, might restrict file virtualization. To function with existing storage systems and switches, the file virtualization platform must be compatible with the present infrastructure. A file virtualization platform should always be validated for proper scalability and compatibility to avoid potential issues.

File-level use cases include:

- **Mass File Storage**: When your customers only require a location to save data, file-level devices can be quite useful.
- VMware: In addition to block-level storage, VMware hosts may connect to the storage offered through NFS.

Application Virtualization

Application virtualization refers to the technique of placing an application on a central server and that application can be run virtually on many platforms. The virtualized program behaves precisely like a native program installed on a real workstation for end users. Application virtualization makes it easier for enterprises to centrally update, manage, and repair applications. Admins may control and alter program access rights without signing into the user's desktop. Portability is another advantage of application virtualization. It enables users to utilize virtualized programs on non-Windows devices such as iOS and Android.

Application virtualization can also be called Application Service Virtualization and it also lets users execute the application on a thin client, which is a terminal or network workstation with few resident programs that access the majority of applications on a connected server.

Application virtualization deceives the computer into thinking the application is running on the local machine while, in reality, it is running on a virtual machine (such as a server) at another place, running its operating system (OS), and being accessible by the local machine. By executing virtual apps, incompatibility issues with the local machine's operating system, as well as flaws or low-quality code in the program, maybe resolved.

Application virtualization seeks to isolate application programs from an operating system with which they are incompatible, leading computers to halt or crash.

Application virtualization also has the following advantages:

- Running fewer resources than using a separate virtual computer.
- Allowing incompatible apps to operate on the same system at the same time.
- Maintaining a consistent, more efficient, and cost-effective OS setup across several devices in a particular enterprise, regardless of the applications utilized.
- Allowing for faster application deployment.
- Improving security by separating apps from the local operating system.
- Easier tracking of license usage, potentially saving money on license expenses.
- Enabling apps to be transferred to portable media and utilized by other client computers without requiring local installation.
- Increasing the capacity to manage a huge number of diverse/variable tasks.

COMPUTE VIRTUALIZATION

Compute Virtualization is the process of creating a simulated version of computing hardware, operating systems, computer networks, or other resources. It is a reduction in the number of physical devices by the simplicity of traditional designs.

Compute virtualization is a method of increasing efficiency and lowering the cost of IT infrastructure. It offers a flexible approach for virtual machines in which actual servers are regarded as a resource pool. It works by combining servers, decreasing the demand for computer equipment and other related infrastructure, and thereby lowering expenses. It streamlines licensing-related business operations, making them more manageable. It establishes a centralized infrastructure that can be shared and accessible by several people working in different places at the same time.

Advantages of Compute Virtualization:

1. **Increased Security:** Data security improves as data is distributed across several systems and resources are hidden from users. In the event of an emergency, the lost data can be recovered from another virtual server. This boosts network flexibility and makes it easier to deal with virus and malware issues.
2. **Improved Administration:** Because the server is separated into numerous virtual servers, it is significantly easier to administer. Business procedures and server licenses are also simplified.
3. **Financial Savings:** The virtual servers can be housed in easily accessible places. As the management cost decreases, so do the hardware and power expenses.
4. **The centralized server:** Compute virtualization centralizes the company's information technology infrastructure. The network becomes extremely efficient, and data may be accessible by a large number of people at any time and from any location.
5. **A More Convenient Software Testing Environment:** A sophisticated testing environment may be built to allow testing in a variety of environments and operating systems.

IMPLEMENTATION LEVELS OF VIRTUALIZATION STRUCTURES

Virtualization is a computer architecture method that multiplexes multiple virtual machines (VMs) on the same physical system. A VM's objective is to increase computer efficiency in terms of resource usage and program flexibility by allowing several users to share resources. In various functional levels, hardware resources (CPU, memory, I/O devices, etc.) or software resources (operating system and software libraries) can be virtualized. As the need for distributed and cloud computing has expanded dramatically in recent years, this virtualization technique has been strengthened. The goal of virtualization is to separate the hardware from the software to improve system efficiency. When the concept of virtual memory was established, computer users had access to much-increased memory space. Likewise virtualization techniques may be used to improve the efficiency of computing engines, networks, and storage.

A typical computer runs a host operating system that is specifically customized to its hardware architecture. Following virtualization, distinct user applications controlled by their operating system (guest OS) can operate independently of the host OS on the same hardware. This is frequently accomplished by including extra software known as a virtualization layer. The hypervisor or virtual machine monitor (VMM) is the name given to this virtualization layer. The primary role of the virtualization software layer is to virtualize the actual hardware of a host computer into virtual resource that are only used by the VMs. This may be done at a variety of operational levels, which include the Instruction Set Architecture (ISA) level, Hardware-level, Operating System level, Library Support level and Application level.

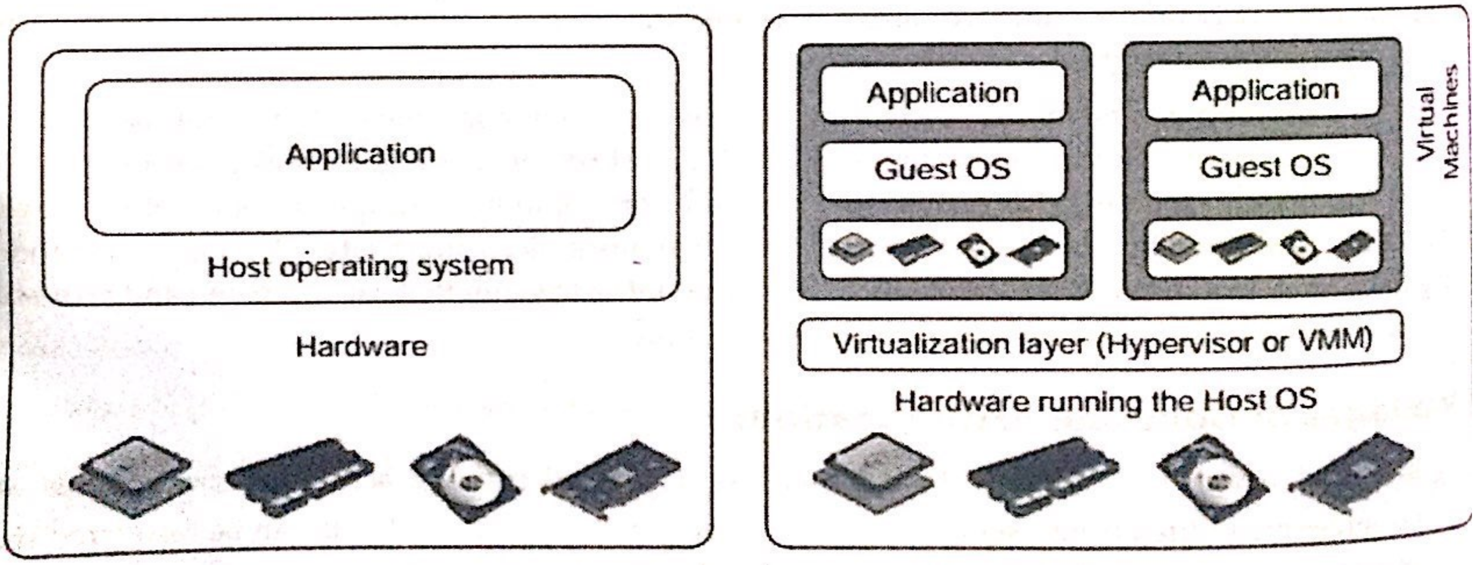


Figure 4.10: Traditional and Virtualized Environment.

The Five Levels Of Implementing Virtualization

There are five levels of implementing virtualizations, which are as follows:

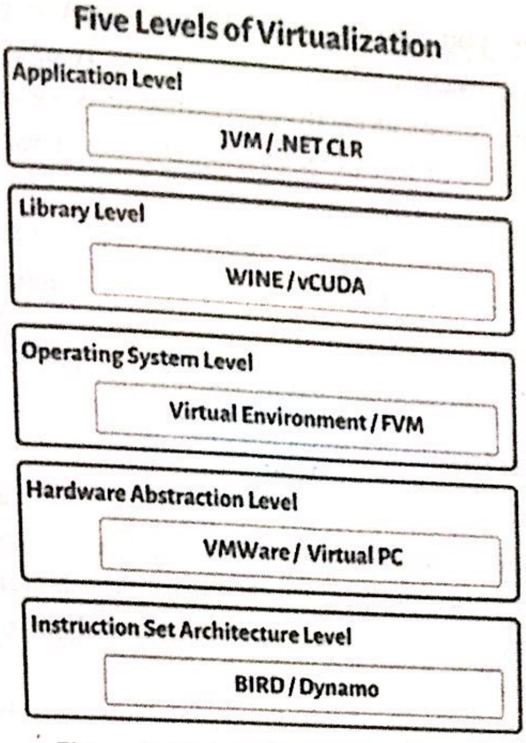


Figure 4.11: Levels of virtualization.

1. **Instruction Set Architecture Level (ISA):** Virtualization in ISA is accomplished by ISA emulation. This is useful for running large amounts of legacy code that was originally developed for various hardware configurations. These programs can be executed on the virtual machine through an ISA.A binary code that previously required extra layers to operate may now be executed on an x86 processor or, with little altering, even on an x64 computer. ISA contributes to this virtual machine's hardware independence. The fundamental emulation, on the other hand, requires the use of an interpreter. This translator translates the source code and turns it into a hardware-readable format for processing.
2. **Hardware Abstraction Level (HAL):** Hardware-level virtualization occurs directly on top of the hardware. This method creates a virtual hardware environment for a virtual machine as well as handles the underlying hardware through virtualization. The goal is to virtualize the resources of a computer, such as its processors, memory, and I/O devices. The goal is for several users to enhance the hardware usage rate at the same time. In the 1960s, the notion was realized in the IBM VM/370. Recently, the Xen hypervisor has been used to virtualize x86-based workstations to run Linux or other guest operating systems.
3. **Operating System Level:** The virtualization paradigm, at the operating system level, establishes an abstract layer between the programs and the OS. It functions as a separate container on the actual server and operating system, utilizing hardware and software. To allocate hardware resources among a large number of mutually distrusting users, OS-level virtualization is often utilized in the creation of virtual environments. Every user gets their virtual environment with their virtual hardware resources.
4. **Library Support Level:** Instead of the OS's long system calls, most programs use APIs revealed by user-level libraries as most systems have well-documented APIs. Virtualization using library interfaces is achieved by using API hooks to regulate the communication channel between programs and the rest of the system. This concept has been applied by the software utility *WINE* to support Windows programs on top of UNIX hosts. Another example is *vCUDA*, which enables programs running within virtual machines to make use of GPU hardware acceleration.

5. **Application Level:** When you simply want to virtualize a single program, application-level virtualization needs to be considered. In this case, the entire environment of the platform does not need to be virtualized. As applications run as a single process on a computer's operating system, this can also be referred to as process-level virtualization. It is beneficial when operating virtual machines that employ high-level languages. In this case, the virtualization layer sits on top of the operating system as an application program, and the layer exports an abstraction of a VM that can run programs written and compiled to a certain abstract machine specification. Any HLL based software that has been built for this VM will be able to execute on it. This type of VM is exemplified by the Microsoft.NET CLR and the Java Virtual Machine (JVM).

Advantages of Virtualization

1. **It is cheaper:** Because virtualization does not need the usage or installation of physical hardware components, IT infrastructures find it to be a less expensive technology to employ. There is no longer a need to allocate significant amounts of space and substantial sums of money to build an on-site resource. You just buy the license or access it from a third-party source and start working as if the gear were installed locally.
2. **It keeps costs predictable:** Individuals and corporations can have predictable costs for their information technology needs because third-party providers typically provide virtualization options.
3. **It reduces the workload** :The majority of virtualization service providers immediately update the hardware and software that will be used. The third-party vendor installs these upgrades instead of sending individuals to perform them locally. This allows local IT specialists to focus on other responsibilities and saves even more money for individuals or organizations.
4. **It offers a better uptime:** Thanks to virtualization technology as uptime has increased considerably. Some service providers guarantee a 99.9999% uptime. Even low-cost companies now guarantee 99.99% uptime.
5. **It allows for** faster **deployment of resources:**When virtualization is implemented, resource provisioning is quick and easy. There is no longer a requirement to establish physical machines, local networks, or other information technology components. It may be propagated throughout the rest of the company as long as there is at least one point of entry to the virtual environment.
6. **It promotes digital entrepreneurship:** Before the widespread adoption of virtualization, digital entrepreneurship was virtually impossible for the average person. Almost anybody can start their side hustle or become a company owner today, thanks to the many platforms, servers, and storage devices that are accessible.
7. **It provides energy savings:** Virtualization is an energy-efficient technology for the vast majority of consumers and businesses. Energy consumption rates can be reduced because no local hardware or software alternatives are used. Instead of paying for data center cooling and equipment operating costs, monies can be repurposed for other operational expenses over time to increase virtualization's total ROI.
8. **Easier backup and disaster recovery** :You may do backups and snapshots of your virtual machines in addition to complete backups of your virtual server. These virtual computers may be easily and quickly relocated from one server to another. Throughout the day, snapshots may be collected, resulting in significantly more up-to-date data. Furthermore, because launching a snapshot is faster than running a conventional server, downtime is drastically reduced. Disasters strike quickly and unexpectedly. Leaks, floods, power outages, cyber-attacks, robbery, and even snowstorms all wipe away critical data in seconds. Virtualization allows for considerably faster and more accurate recovery with less labor and a fraction of the equipment — it is all virtual.

9. **Better business continuity:** With an increasingly mobile workforce, company continuity is critical. Files become inaccessible without it, work remains unfinished, procedures stall, and employees are less productive. Virtualization allows employees to access software, data, and communications from anywhere, and it can allow several people to access the same information for greater continuity.
10. **More efficient IT operations:** Moving to a virtual environment may make everyone's job easier, particularly the IT workers. Virtualization simplifies the installation and maintenance of software, the distribution of updates, and the maintenance of a more secure network. In comparison to a non-virtual environment, they can accomplish this with less downtime, fewer outages, faster recovery, and rapid backup.

Disadvantages of Virtualization

1. **It can have a high cost of implementation:** When considering virtualization, the ordinary individual or corporation will incur relatively minimal costs. However, the installation expenses for virtualized environment providers might be fairly substantial. At some point, hardware and software are necessary, which implies devices must be designed, made, or acquired for implementation.
2. **It still has limitations:** Not every program or server will function properly in a virtualized environment. This indicates that a hybrid system may be required for an individual or company to function successfully. This still saves time and money in the long term, but because not every manufacturer supports virtualization and some may discontinue support after the initial implementation, there is always a sense of uncertainty when completely installing this sort of system.
3. **It creates a security risk:** Information is our modern currency. You can make money if you have it. You will be disregarded if you do not have it. Because data is critical to a company's success, it is regularly targeted.
4. **It creates an availability issue:** The main issue that many people have about virtualization is what will happen to their job if their assets are unavailable. If a company is unable to connect to its data for a lengthy length of time, it will struggle to compete in its field. Furthermore, because availability is controlled by third-party providers, the capacity to stay connected with virtualization is out of one's hands.
5. **It creates a scalability issue:** Because of virtualization, you can develop a business or opportunity rapidly, but you may not be able to develop as much as you would like. When you initially start, you may be compelled to be bigger than you want to be. Growth causes slowness inside a virtualized network since numerous entities share the same resources. There is little anybody can do if a huge presence diverts resources away from multiple smaller enterprises.
6. **It requires several links in a chain that must work together cohesively:** If you have access to local equipment, you have complete control over what you can accomplish. Because numerous connections must collaborate to complete the same activity, you lose control with virtualization. As an example, consider saving a document file. You may save the file immediately and even generate a backup with a local storage device, such as a flash drive or HDD. Your ISP connection must be active to use virtualization. Your LAN or Wi-Fi must be operational. Your online storage choice must be accessible. If any of these don't work, you're not saving that file.
7. **It takes time:** Although virtualization saves time during the installation phases, it costs users time in the long run when compared to local systems. This is because more procedures must be taken to get the desired result.

TAXONOMY OF VIRTUAL MACHINES

Virtual machines are broadly classified into two types: System Virtual Machines (also known as Hardware Virtual Machines) and Process Virtual Machines (also known as Application Virtual Machine). The classification is based on their usage and degree of similarity to the linked physical machine. The system VM mimics the whole system hardware stack and allows for the execution of the whole operating system. Process VM, on the other hand, provides a layer to an operating system that is used to replicate the programming environment for the execution of specific processes.

A **Process Virtual Machine**, also known as an application virtual machine, operates as a regular program within a host OS and supports a single process. It is formed when the process begins and deleted when it terminates. Its goal is to create a platform-independent programming environment that abstracts away features of the underlying hardware or operating system, allowing a program to run on any platform. With Linux, for example, Wine software aids in the execution of Windows applications.

A **System Virtual Machine**, such as VirtualBox, offers a full system platform that allows the operation of a whole operating system (OS).

Virtual Machines are used to distribute and designate suitable system resources to software (which might be several operating systems or an application), and the software is restricted to the resources provided by the VM. The actual software layer that allows virtualization is the Virtual Machine Monitor (*also known as Hypervisor*). Hypervisors are classified into two groups based on their relationship to the underlying hardware. Native VM is a hypervisor that takes direct control of the underlying hardware, whereas hosted VM is a different software layer that runs within the operating system and so has an indirect link with the underlying hardware.

The system VM abstracts the Instruction Set Architecture, which differs slightly from that of the actual hardware platform. The primary benefits of system VM include consolidation (it allows multiple operating systems to coexist on a single computer system with strong isolation from each other), application provisioning, maintenance, high availability, and disaster recovery, as well as sandboxing, faster reboot, and improved debugging access.

The process VM enables conventional application execution inside the underlying operating system to support a single process. To support the execution of numerous applications associated with numerous processes, we can construct numerous instances of process VM. The process VM is formed when the process starts and terminates when the process is terminated. The primary goal of process VM is to provide platform independence (in terms of development environment), which implies that applications may be executed in the same way on any of the underlying hardware and software platforms.Process VM, as opposed to system VM, abstracts high-level programming languages. Although Process VM is built using an interpreter, it achieves comparable speed to compiler-based programming languages using the just-in-time compilation mechanism.

Java Virtual Machine (JVM) and Common Language Runtime are two popular examples of Process VMs; they are used to virtualize the Java programming language and the.NET Framework programming environment, respectively.

HYPERVISOR MANAGEMENT SOFTWARE

A hypervisor is a function that abstracts, or separates, operating systems and applications from the underlying computer hardware. This abstraction enables the underlying host machine hardware to run one or more virtual machines as guests independently, allowing numerous guest VMs to effectively share the system's physical computational resources like processor cycles, memory space, network bandwidth, and so on. A hypervisor is also known as a virtual machine monitor.

A hypervisor, often known as a VMM (Virtual Machine Monitor), is a software layer that sits between the operating system and the hardware. It provides the services and functionality required for the seamless operation of several operating systems. It detects traps, reacts to privileged CPU instructions, and manages hardware request queuing, dispatching, and return. To administer and control the virtual machines, a host operating system runs on top of the hypervisor.

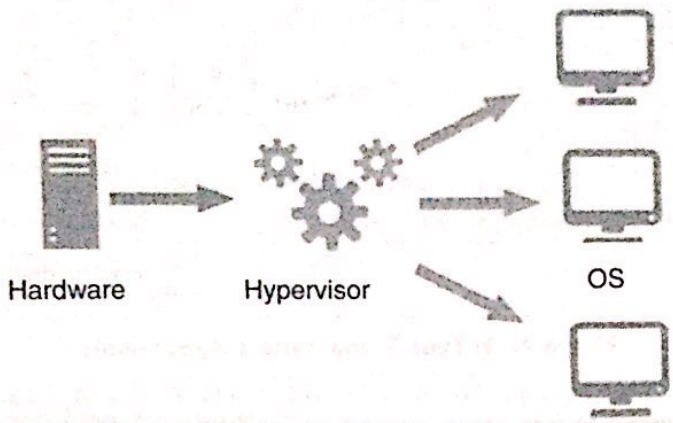


Figure 4.12: Hypervisor Concept

Hypervisors offer various advantages to the business data center. First, the capacity of a physical host system to operate numerous guest VMs may dramatically enhance resource usage. Whereas physical (non-virtualized) servers may only host one operating system and application, a hypervisor virtualizes the server, allowing the system to host multiple VM instances, each running an independent operating system and application, on the same physical system while utilizing far more of the system's available compute resources.

The abstraction that occurs in a hypervisor also allows the VM to be independent of the underlying hardware. Traditional software is often tightly connected to the underlying server hardware, which means that relocating the application to a different server necessitates time-consuming and error-prone reinstallation and customization. A hypervisor, on the other hand, renders the underlying hardware specifics irrelevant to the VMs. This enables VMs to be transferred or migrated between any local or distant virtualized servers with appropriate computational capacity nearly at whim, with virtually no disturbance to the VM; a capability known as live migration.

> Using hypervisor-based virtualization software to provide isolation between different customer environments can lead to increased utilization of system resources such as CPU and memory. Using native virtualization technologies offered by hardware vendors, such as *Solaris Zones* when using the *Oracle Solaris operating system*, can be much more effective and efficient depending on the customer environment. Native virtualization technologies offered by hardware vendors are more restrictive in terms of what is supported than hypervisor-based virtualization software.

Even though they operate on the same physical computer, VMs are logically segregated from one another. In practice, a VM has no innate awareness of or reliance on other VMs. A mistake, crash, or virus attack on one virtual machine does not spread to other virtual machines on the same or different computers. As a result, hypervisor technology is incredibly secure.

Hypervisors are classified into two types: TYPE 1 and TYPE 2

Type 1 hypervisors are those that operate directly on the system hardware. In vendor literature, they are frequently referred to as "native," "bare metal," or "embedded" hypervisors. A host operating system is used by type 2 hypervisors. Type 2 hypervisors were the most popular when the virtualization trend initially took off. Administrators may purchase the program and install it on an existing server.

If you have heterogeneous systems in your service network, you must choose a hypervisor that supports the operating systems you are currently running. If you run a Windows or Linux-based homogenous network, support for a lower number of guest operating systems may be sufficient.

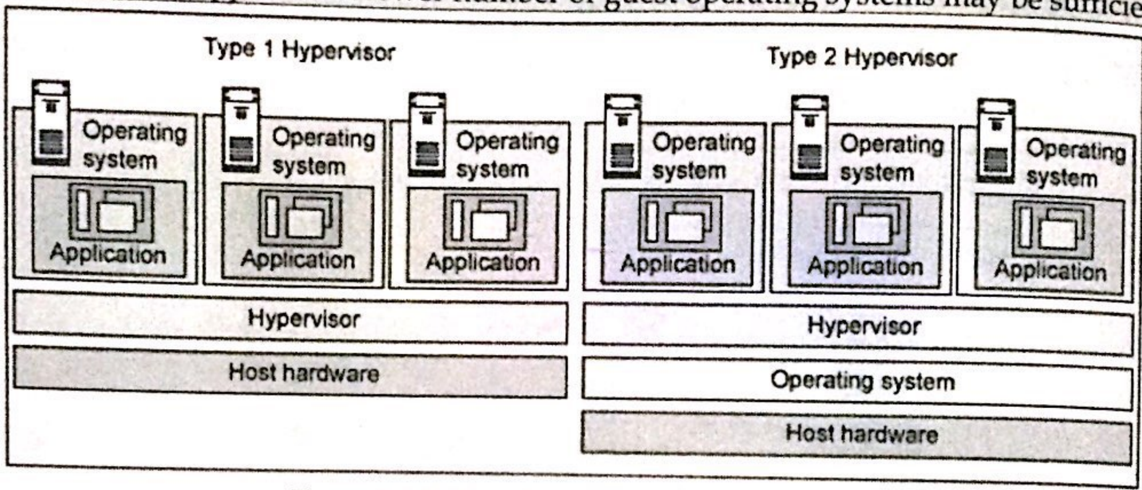


Figure 4.13: Type 1 and Type 2 Hypervisors

Type 1 hypervisors are becoming more prevalent these days because incorporating the hypervisor into the firmware is more efficient. Type 1 hypervisors, according to IBM, provide better performance, availability, and security than Type 2 hypervisors. IBM advises that Type 2 hypervisors be used primarily on client systems where efficiency is not as important, or on systems where support for a wide range of I/O devices is required and may be supplied by the host operating system.

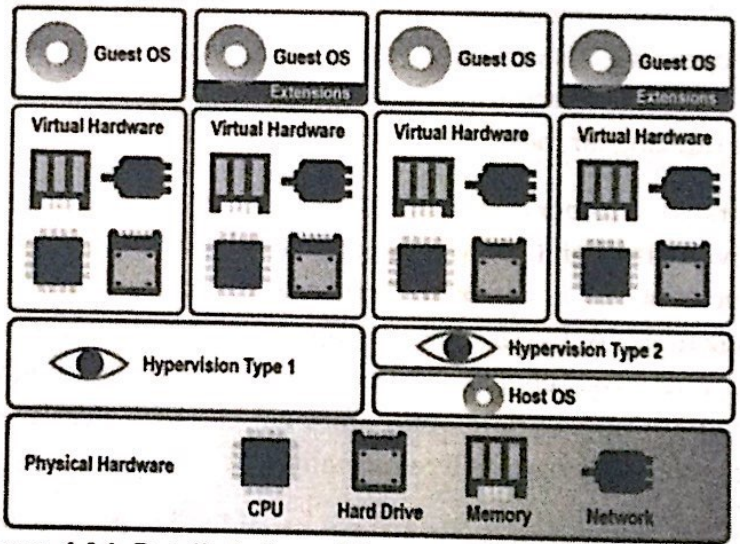


Figure 4.14: Detailed view of Type 1 and Type 2 hypervisors

Examples of Type 1 Hypervisor

1. **VMware ESX and ESXi:** These hypervisors provide extensive functionality and scalability, but they need a license, which raises the expenses. VMware provides certain low-cost bundles that might make hypervisor technology more economical for small infrastructures. VMware is the market leader in Type-1 hypervisors. Their vSphere/ESXi product is offered in five commercial variants as well as a free edition.
2. **Microsoft Hyper-V:** The Microsoft hypervisor, Hyper-V, lacks many of the sophisticated capabilities seen in VMware's solutions. Hyper-V, along with XenServer and vSphere, is one of the top three Type-1 hypervisors.
3. Citrix XenServer: It started as an open-source project. The underlying hypervisor technology is free, but it lacks advanced functionality, much to VMware's free ESXi. Xen is a bare-metal hypervisor of type 1. Just as Red Hat Enterprise Virtualization uses KVM, Citrix uses Xen in the commercial XenServer.

4. **Oracle VM:** The Oracle hypervisor is built on the open-source Xen platform. However, if you require hypervisor support or product upgrades, you will be charged. Many of the sophisticated functionality present in competing for bare-metal virtualization hypervisors are missing from Oracle VM.

> As there is no intermediary layer in Type 1 hypervisors, they provide far superior performance than Type 2 hypervisors, making them the obvious choice for mission-critical applications and workloads. But that is not to say that hosted hypervisors are not useful; they are considerably easier to set up, so they are a smart pick if you need to rapidly install a test environment. Comparing their performance is one of the greatest methods to discover which hypervisor best matches your requirements. These include CPU overhead, the amount of maximum host and visitor RAM, and virtual processor support.

Examples Of Type 2 Hypervisor

1. **VMware Workstation/Fusion/Player:** VMware Player is a virtualization hypervisor that is available for free. It is designed to operate only one virtual machine (VM) and does not support the creation of new VMs. VMware Workstation is a more powerful hypervisor that includes sophisticated capabilities like record-and-replay and VM snapshot support. VMware Workstation offers three key use cases: running various operating systems or versions of one operating system on a single desktop, for developers who require sandbox environments and snapshots, and for laboratories and demonstration's purpose.
2. **VMware Server:** VMware Server is a free, hosted virtualization hypervisor that functions similarly to VMware Workstation.
3. **Microsoft Virtual PC:** Windows Virtual PC is the most recent virtualization technology from Microsoft. It enables you to run a wide range of productivity programs in a virtual Windows environment with a single click, directly from a Windows 7-based PC.
4. **Oracle VM VirtualBox:** If you wish to virtualize on a budget, VirtualBox hypervisor technology delivers enough performance and functionality. Although it is a free, hosted solution with a tiny footprint, VirtualBox has several features in common with VMware vSphere and Microsoft Hyper-V.
5. **Red Hat Enterprise Virtualization:** Red Hat's Kernel-based Virtual Machine (KVM) combines the advantages of a hosted and bare-metal virtualization hypervisor. It is capable of converting the Linux kernel into a hypervisor, allowing VMs direct access to physical hardware.

Features to look for in a Virtualization Platform

1. **Reduction of Capital Expenditures (CAPEX):** Server usage levels are typically modest, averaging approximately 15%. Virtualization has the potential to double throughput. This implies that a corporation may utilize less hardware and save money on electricity. It is important to note that this must be balanced against the total cost of ownership of the virtualization platform.
2. **System Consolidation:** An organization decreases the number of physical servers necessary by running numerous applications and operating systems. This is a method of utilizing computer server resources efficiently to decrease the total number of servers or server locations required by a company.
3. **Ease of System Management:** Easy administration in this sense refers to how quickly new services such as platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS) can be implemented. It also refers to the agility and rapidity with which new application stacks are deployed.
4. **Platform Maturity:** Virtualization is a costly long-term investment that will be squandered if suppliers are swapped. As a result, new market entrants may not be a good option for mission-critical data centers.
5. **Hardware Compatibility:** Hardware challenges with virtualizing platforms include outright incompatibility and sub-optimal performance. Hosted hypervisors often support the widest range of hardware types, whereas bare-bonesvirtualizers are often picky about supported hardware. If you intend to reuse existing gear, be sure that your platform of choice supports it.

6. **Total Cost of Ownership:** The total cost of ownership includes more than simply the cost of acquiring a virtualization platform. Additional costs should be considered, such as guest OS licensing, training and support, and hardware. The acquisition of sophisticated management tools is one expense component that is frequently overlooked. These are typically not included in the initial purchase price.

SELECTING SERVER VIRTUALIZATION PLATFORM (CHOOSING THE RIGHT HYPERVISOR)

Before selecting a good hypervisor, the following criteria should be considered:

1. **Understand your needs:** The data center exists because of the company and its applications. You may have personal demands in addition to the demands of the organization. The following are the required features in a virtualization hypervisor.
   - Flexibility
   - Scalability
   - Usability
   - Availability
   - Reliability
   - Efficiency
2. **The cost of a hypervisor:** The most difficult aspect of selecting a hypervisor for many consumers is achieving the correct balance between cost and capability. While many entry-level solutions are free or almost so, the cost at the other end of the market might be shocking. Licensing regimes differ as well, so it is critical to understand exactly what you are receiving for your money.
   - **Memory management:** Look for hardware-assisted memory virtualization capability. Memory overcommits and big page table support in the VM guest and hypervisor are recommended features; memory page sharing is an optional bonus feature worth considering.
3. **Virtual machine performance:** Virtual systems should perform as well as or better than their physical equivalents, at least in terms of the applications running on each server. Everything above and beyond this criterion is profit. Ideally, each hypervisor should be able to manage resources on the fly to maximize performance for each virtual machine. The question is, how much are you prepared to pay for this optimization? The value of this optimization is often determined by the size or mission-criticality of your project.
4. **Ecosystem:** It is easy to underestimate the significance of a hypervisor's ecosystem – that is, the availability of documentation, support, training, third-party developers, and consultants, among other things – in evaluating whether or not a solution is cost-effective in the long run.
   - **High availability:** Each major manufacturer has its high availability solution, and the methods used to accomplish it might vary greatly, ranging from quite sophisticated to extremely simple. It is vital to understand both catastrophe prevention and disaster recovery procedures for any system. You should never put a virtual machine online until you fully understand the protection and recovery procedures in place.
   - **Live migration:** Live migration is critical for users; in addition to supporting live migration between platforms and the ability to live to migrate two or more VMs at the same time, you should carefully assess what each hypervisor offers in this area.
   - **Networking, storage, and security:** In terms of networking, hypervisors should provide network interface card teaming and load balancing, Unicast isolation, and standard virtual local area network compatibility (VLAN). Each hypervisor should be able to support iSCSI and Fibre Channel as well.

- **Management features:** Look for management features like Simple Network Management Protocol (SNMP) capability, interaction with other management software, and management server fault tolerance – these are vital to a hypervisor.
- **Test for yourself:** You can get started with your existing desktop or laptop. To build a great virtual learning and testing environment, you may run both VMware vSphere and Microsoft Hyper-V in VMware Workstation or VMware Fusion.

BUSINESS CASES FOR SERVER VIRTUALIZATION

Understanding how server virtualization technologies may be applied to business objectives is the first step in preparing to adopt them. We will explore the important areas of information technology where server virtualization may be effectively implemented, as well as how it connects to common business goals, in this section. It also demonstrates how typical short-term and long-term problems may be solved with server virtualization technology, as well as when it should not be employed.

Aside from the novelty of running many operating systems on a single machine at the same time, server virtualization technology was created to aid in the resolution of business difficulties. Virtualization may be utilized in a straightforward fashion, similar to physical servers, and when done so, it may assist minimize physical server hardware expenses by combining several servers into a single server. Server consolidation is a term used to describe this type of utilization.

Virtualization introduces new functionality that was previously inaccessible or unattainable on traditional server hardware. One of the most significant advantages of virtualization is the separation of virtual machines from the actual hardware, which allows virtual machines to be portable. As a result, virtualization simplifies and improves legacy server and application support while opening up new possibilities in disaster recovery and high-availability scenarios. Since virtual machines are significantly easier to deploy than physical servers, and because virtualization technology's software nature lends itself well to provisioning automation, on-demand and adaptive computing are more readily achieved. Server Consolidation, Legacy server, and application support, Disaster Recovery, High availability, Adaptive computing, On-demand computing, etc. are some areas where server virtualization provides business value.

SERVER CONSOLIDATION

Many businesses may have many servers, each serving a specific function. These servers include file servers, print servers, e-mail servers, Web servers, database servers, and other application servers. It is fairly rare for apps to demand or highly advise the usage of a dedicated server, generally because the program does not live well with other apps installed on the same operating system. In these cases, organizations will buy small, dedicated servers to host these applications, many of which have a low utilization rate because the application has a small number of users or is only used infrequently, such as once a month. The difficulty with this scenario is that the firm must incur a capital cost of, for example, $6,000 or more, and the new dedicated server's CPU, RAM, and disk storage are significantly underused and virtually squandered. Over time, the data center may house a large number of tiny, underused servers supporting dedicated applications, incurring data center hosting fees (ping, power, and bandwidth) for each server. Server virtualization can help firms save money in the data center by consolidating servers.

Server consolidation is the practice of reducing the number of servers or server locations in order to use compute resources more efficiently and reduce costs. This involves moving multiple, heterogeneous workloads to a single server or combining workloads under a single operating system.

Server consolidation is a method of optimizing the use of computer server resources to decrease the total number of servers or server locations required by an organization. The technique evolved in reaction to the issue of server sprawl, which occurs when many, underutilized servers take up more space and demand more resources than their workload justifies. Servers in many businesses often run at 15-20% of their capacity, which may not be a sustainable ratio in the present economic environment. Server consolidation is increasingly being used by businesses to reduce needless expenditures and maximize return on investment (ROI) in the data center.

Server Sprawl

Server sprawl occurs when many, underutilized servers take up more space and demand more resources than their workload justifies. The procurement of a large number of inexpensive, low-end servers, as well as the practice of devoting servers to particular applications, are two common sources of server sprawl. Server sprawl may be restricted to a single server room, but it can also be distributed across many facilities in widely dispersed geographical areas, particularly when one firm acquires another, or two organizations combine.

While consolidation can significantly enhance the effective use of server resources, it can also result in complicated data, application, and server settings that are difficult for the typical user to deal with. To address this issue, server virtualization may be utilized to hide server resource specifics from consumers while maximizing resource sharing. Another way to server consolidation is to deploy blade servers to enhance space efficiency.

Advantages of Consolidation

- Lower hardware and running costs (such as cooling and electricity).
- Reduce the time it takes to set up new servers.
- Warranty and software licensing fees will be reduced.
- Business agility through the use of cloud and shared infrastructure
- With business continuity and built-in disaster recovery, you can reduce downtime and increase dependability.
- Provide on-demand IT services independent of hardware, operating systems, applications, or infrastructure providers.

VIRTUAL LAN (VLAN)

A virtual local area network (VLAN) is a logical set of workstations, servers, and network devices that seem to be on the same local area network (LAN) despite their geographical separation. A VLAN enables a network of computers and users to connect in a simulated environment as if they were part of a single LAN with a single broadcast and multicast domain. VLANs are used to accomplish scalability, security, and network administration ease, and they can swiftly adapt to changes in network needs and the migration of workstations and server nodes. Higher-end switches provide VLAN functionality and implementation. The goal of creating a VLAN is to increase network speed or to add necessary security measures.

Local Area Networks (LANs) and Wide Area Networks (WANs) are two types of computer networks (WANs). LANs are network equipment such as switches, hubs, bridges, workstations, and servers that are linked to each other in the same network at a given place. A LAN is often referred to as a broadcast domain. A VLAN enables many networks to function as though they are part of the same LAN. One of the most advantageous aspects of a VLAN is that it eliminates network latency, which saves network resources and improves network efficiency. Furthermore, VLANs are designed to enable segmentation and to aid with concerns such as security, network administration, and scalability. VLANs can also be used to simply regulate traffic flows.

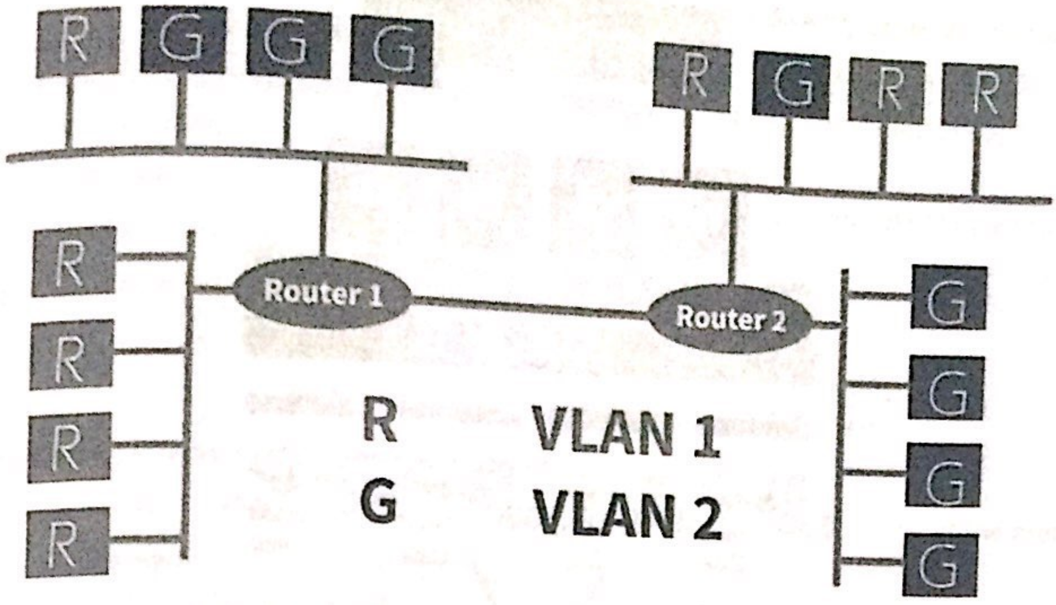


Figure 4.15: Example of VLAN

The key benefits of implementing VLANs include:

- allowing network administrators to add additional security to network communication.
- making network or network device expansion and relocation easier.
- providing flexibility because administrators can configure in a centralized environment while the devices may be located in different geographical locations.
- Reduce latency and traffic strain on the network and network devices, resulting in improved performance

VLANs also have some disadvantages as listed below:

- There is a high danger of virus problems since a single infected machine can transmit a virus over the entire logical network.
- Because extra routers may be required to regulate the workload in very large networks, there may be equipment limits.
- More successful than a WAN at managing latency, but less efficient than a LAN.

Virtual SAN (VSAN)

A logical partition in a physical storage area network (SAN) is referred to as a virtual storage area network (VSAN). This storage virtualization implementation model splits and assigns parts or all of a storage area network into one or more logical SANs for usage by internal or external IT services and solutions. A virtual storage area network is most commonly used in cloud computing and virtualization contexts. Through storage virtualization, a VSAN enables end-users and enterprises to construct a logical storage area network on top of a physical SAN. The virtualized SAN may be used to create a virtual storage pool for numerous services; however, it is often configured to work with virtual machines and virtual servers.

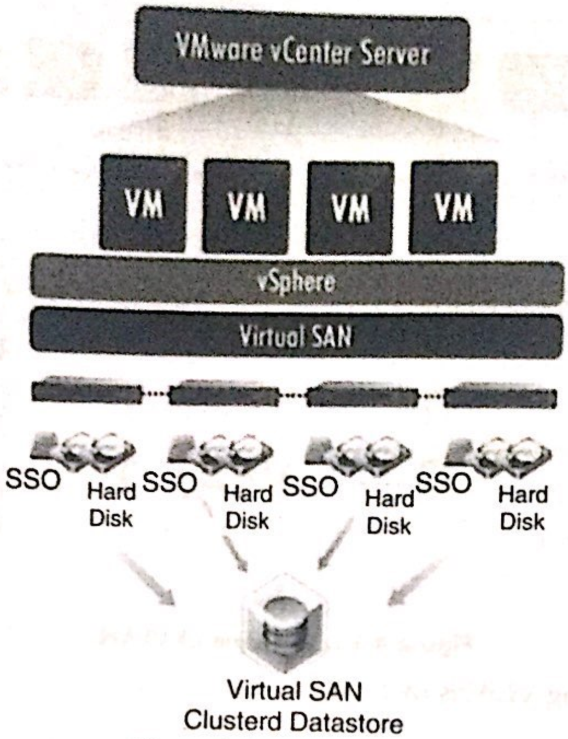


Figure 4.16: Virtual SAN

A VSAN provides identical services and functionality as a traditional SAN, but because it is virtualized, it enables the addition and relocation of subscribers without changing the actual topology of the network. It also has a variable storage capacity that may be raised or lowered over time. VSANs enable traffic to be isolated inside specified areas of a storage area network, allowing a problem in one logical partition to be handled with little disturbance to the rest of the network. The usage of numerous, separated VSANs can also make it easier to set up and scale-out a storage system. Subscribers can be added or moved without altering the physical layout.

OBJECTIVE QUESTIONS

1) **Point out the wrong statement.**
   a. Abstraction enables the key benefit of cloud computing: shared, ubiquitous access
   b. Virtualization assigns a logical name for a physical resource and then provides a pointer to that physical resource when a request is made
   c. All cloud computing applications combine their resources into pools that can be assigned on demand to users
   d. All of the mentioned

2) **Which of the following types of virtualization is also characteristic of cloud computing?**
   a. Storage b. Application c. CPU d. All of the above

3) **The technology used to distribute service requests to resources is referred to as __________**
   a. load performing b. load scheduling c. load balancing d. all of the mentioned

4) **Which of the following is one of the major categories of Amazon Machine Instances that you can create on the Amazon Web Service?**
   a. AMP b. XAMPP c. LAMP d. None of the mentioned

5) **An operating system running on a Type __________ VM is a full virtualization.**
   a. 1 b. 2 c. 3 d. All of the mentioned

6) In a ____________ scheme, the VM is installed as a Type 1 Hypervisor directly onto the hardware.
   a. paravirtualization b. full virtualization c. emulation d. None of the mentioned

7) Which of the following characteristics should you consider when deciding whether to deploy an application or service to a virtual machine?
   a. Hardware requirements
   b. Software support, compatibility and Licensing
   c. Performance and resource requirements
   d. All of the above

8) Which of the following is another name for a system virtual machine?
   a. hardware virtual machine
   b. software virtual machine
   c. real machine
   d. None of the mentioned

9) Which of the following provide system resource access to virtual machines?
   a. VMM b. VMC c. VNM d. All of the mentioned

10) Point out the correct statement:
   a. A virtual machine is a computer that is walled off from the physical computer that the virtual machine is running on
   b. Virtual machines provide the capability of running multiple machine instances, each with its operating system
   c. The downside of virtual machine technologies is that having resources indirectly addressed means there is some level of overhead
   d. All of the mentioned

11) Which of the following is Type 1 Hypervisor?
   a. Wind River Simics
   b. Virtual Server 2005 R2
   c. KVM
   d. LynxSecure

12) Which of the following is Type 2 VM?
   a. VirtualLogixVLX b. VMware ESX c. Xen d. LynxSecure

13) Point out the correct statement:
   a. A client can request access to a cloud service from any location
   b. A cloud has multiple application instances and directs requests to an instance based on conditions
   c. Computers can be partitioned into a set of virtual machines with each machine being assigned a workload
   d. All of the mentioned

14) Which of the following software can be used to implement load balancing?
   a. Apache mod_balancer
   b. Apache mod_proxy_balancer
   c. F6's BigIP
   d. All of the mentioned

15) Which of the following network resources can be load-balanced?
   a. Connections through intelligent switches
   b. DNS
   c. Storage resources
   d. All of the mentioned

16) Point out the wrong statement:
   a. Some hypervisors are installed over an operating system and are referred to as Type 2 or hosted VM
   b. All CPUs support virtual machines
   c. On a Type 2 VM, a software interface is created that emulates the devices with which a system would normally interact
   d. All of the mentioned

17) Which of the following types of virtualizations is found in hypervisor such as Microsoft's Hyper-V?
   a. paravirtualization
   c. full virtualization
   c. emulation
   d. none of the mentioned

18) In ______ the virtual machine simulates hardware, so it can be independent of the underlying syst hardware.

a. paravirtualization b. full virtualization c. emulation d. none of the mentioned

19) Which of the following operating systems support operating system virtualization?

a. Windows NT b. Sun Solaris c. Windows XP d. Compliance

20) Which of the following is a service that aggregates servers into an assignable pool?

a. VMware vStorage b. VMware vNetwork
c. VMware vCompute d. Application services

21) ________ is a service that creates and manages virtual network interfaces.

a. VMware vStorage b. VMware vNetwork
c. VMware vCompute d. Application services

22) Which of the following allows a virtual machine to run on two or more physical processors at the sam time?

a. Virtual SMP b. Distributed Resource Scheduler
c. vNetwork Distributed Switch d. Storage VMotion

23) Which of the following will be the host operating system for Windows Server?

a. VirtualLogixVLX b. Microsoft Hyper-V c. Xen d. All of the above

24) Which of the following runs on Xen Hypervisor?

a. Azure b. AWS EC2 c. C AWS EC3 d. All of the above

25) The software that supports virtual machines is called.

a. VMM b. Hypervisor c. Kernel d. Both A and B

26) _______ consists of servers, storage devices, network, cloud management software, deployment software, and platform virtualization.

a. Computing Planning b. Cloud infrastructure
c. Cloud Computing Technologies d. Cloud Computing Architecture

27) ________ is a firmware that acts as a Virtual Machine Manager.

a. Hypervisor b. Network c. Server d. Storage

28)Hypervisor also known as:

a. high-level program b. simple program
c. complex program d. low-level program

29) Resource allocation and deallocation services provided by?

a. Network b. Server c. Storage d. Software

30) Point out the wrong statement:

a. A cloud is defined as the combination of the infrastructure of a data center with the ability to provision hardware and software

b. High touch applications are best done on-premises

c. The Google App Engine follows IaaS

d. All of the above

31) Which of the following is not a benefit of server virtualization technology?

a. Agile capacity b. More hardware
c. Expanded disaster recovery options d. better utilization of resources

32) When implementing virtualization, a server must provide ample memory space for the ______.

a. Operating system
b. Hypervisor
c. Virtual machines on the server
d. All of the above

33) Server virtualization has proven to reduce data center capital and operational expenses assuming the consolidation ratio offsets the cost of ______.

a. Air-side economizers
b. Virtualization software licensing
c. Implementation
d. Server power supplies

QUESTION

1. What is virtualization and what are its benefits? Explain.
2. Describe the characteristics of virtualized environments.
3. Discuss classification or taxonomy of virtualization at different levels.
4. Discuss the machine reference model of execution virtualization.
5. What are hardware virtualization techniques?
6. List and discuss different types of virtualizations.
7. What is a data center? Describe data center virtualization. Explain the difference between cloud and traditional data centers.
8. What are the benefits of virtualization in the context of cloud computing?
9. What are the disadvantages of virtualization?
10. Discuss the architecture of Hyper-V. Discuss its use in cloud computing.
11. What is Hypervisor in Cloud Computing? Explain its types.
12. Are Type-1 Hypervisors better in performance than Type-2 Hypervisors and Why?
13. What is server virtualization? Explain in Brief.
14. Explain Block Level Storage Virtualization and File Level Storage Virtualization.
15. What is a virtual LAN? What are the benefits and limitations of VLAN? Describe Virtual SAN.
16. What is virtualization? Explain different types of virtualizations.
17. Explain the benefits of virtualization.
18. What are the characteristics of virtualized environments?
19. Discuss classification or taxonomy of virtualization at different levels.
20. Discuss the machine reference model of execution virtualization.
21. List and discuss different types of virtualization.
22. What are the benefits of virtualization in the context of cloud computing?
23. What are the disadvantages of virtualization?
24. Discuss the reference model of full virtualization.
25. Explain block and file-level storage virtualization.

26. What is server and machine Virtualization? Explain types and business cases for Server Virtualization.
27. "Cloud is about how you do computing, not where you do computing." Explain.
28. What do you mean by Hypervisor? Explain its roles in the virtualization process.
29. Describe Virtual LAN and Virtual SAN along with benefits. Explain how VLAN works.
30. What is virtualization? Elaborate on its benefits. Explain block and file-level storage virtualization.
31. What is server and machine Virtualization? Explain types and business cases for Server Virtualization.
32. Explain Server Sprawl and Server Consolidation. Describe the major features to look for in a Virtualizat Platform.
33. What do you mean by Hypervisor? Explain its roles in the virtualization process. Briefly describe the types Hypervisor.