Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

CET4034B: Cloud Infrastructure and Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. CSE(CYBERSECURITY AND FORENSICS)

CET4034B: Cloud Infrastructure and Security

Teaching Scheme
Theory: 2 Hrs. / Week

Credits: 02 + 01 = 03
Practical: 2 Hrs./Week

Course Objectives

1) Knowledge

i. To study basic cloud computing concepts and its operational environment.

2) Skills

i. To acquire skills of using various Virtualization Techniques and Platforms
ii. To understand challenges in cloud computing

3) Attitude

i. To select and use cloud computing platform

Course Outcomes

After completion of this course students will be able to

i. Setup a cloud environment
ii. Deploy web services efficiently on a cloud platform
iii. Manage cloud services efficiently and effectively
iv. Design, deploy and address the cloud security aspects

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Module 2
Understanding Virtualization

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

MIT-WPU

।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

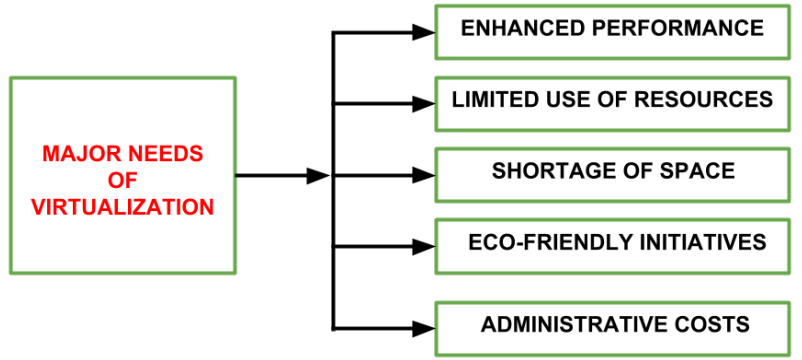
Points to be covered

- Introduction to Virtualization
- Concept of Hypervisor
- Types of Hypervisor
- Taxonomy of Virtualization
- Virtualization- A machine reference model
- Hardware virtualization techniques
- Pros and Cons of Virtualization
- Live migration
- Technology examples: Xen, KVM, VMware, Microsoft Hyper-V.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

What is virtualization in cloud computing?

- It is a process that allows a computer to share its hardware resources with multiple digitally separated environments.
- Each virtualized environment runs within its allocated resources, such as memory, processing power, and storage.
- Virtualization is a proved technology that makes it possible to run multiple operating system and applications on the same server at same time.
- It is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources.
- It is the enabling technology and creates virtual machines that allows a single machine to act as if it were many machines.
- Virtualization creates virtual hardware by cloning physical hardware.
- The hypervisor uses virtual hardware to create a virtual machine (VM).

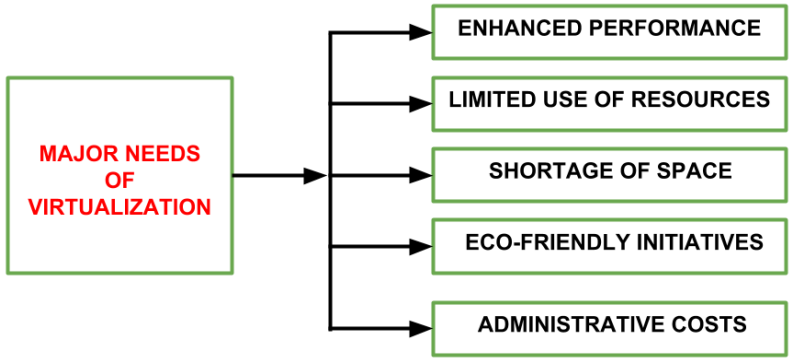


Need of Virtualization

- There are five major needs of virtualization which are described below.

1. **ENHANCED PERFORMANCE-** Currently, the end user system i.e. PC is sufficiently powerful to fulfil all the basic computation requirements of the user, with various additional capabilities which are rarely used by the user. Most of their systems have sufficient resources which can host a virtual machine manager and can perform a virtual machine with acceptable performance so far.

2. **LIMITED USE OF HARDWARE AND SOFTWARE RESOURCES-** The limited use of the resources leads to under-utilization of hardware and software resources. As all the PCs of the user are sufficiently capable to fulfil their regular computational needs that's why many of their computers are used often which can be used 24/7 continuously without any interruption. The efficiency of IT infrastructure could be increase by using these resources after hours for other purposes. This environment is possible to attain with the help of Virtualization.



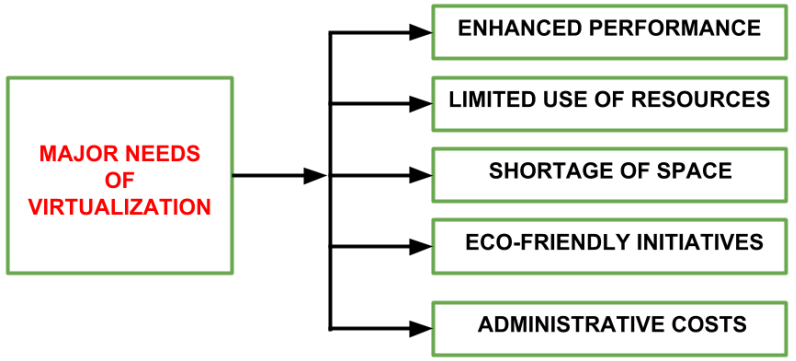
Need of Virtualization

3. **SHORTAGE OF SPACE-** The regular requirement for additional capacity, whether memory storage or compute power, leads data centers raise rapidly. Companies like Google, Microsoft and Amazon develop their infrastructure by building data centers as per their needs. Mostly, enterprises unable to pay to build any other data center to accommodate additional resource capacity. This heads to the diffusion of a technique which is known as server consolidation.

4. **ECO-FRIENDLY INITIATIVES-** At this time, corporations are actively seeking for various methods to minimize their expenditures on power which is consumed by their systems. Data centers are main power consumers and maintaining a data center operations needs a continuous power supply as well as a good amount of energy is needed to keep them cool for well-functioning. Therefore, server consolidation drops the power consumed and cooling impact by having a fall in number of servers. Virtualization can provide a sophisticated method of **server consolidation.**

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

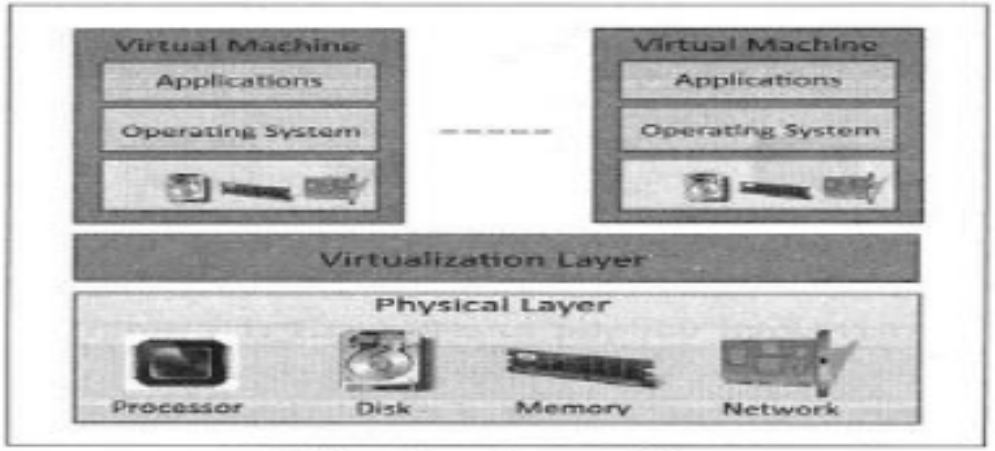
Need of Virtualization



5. **ADMINISTRATIVE COSTS-** Furthermore, the rise in demand for capacity surplus, that convert into more servers in a data center, accountable for a significant increase in administrative costs. Hardware monitoring, server setup and updates, defective hardware replacement, server resources monitoring, and backups are included in common system administration tasks. These are personnel-intensive operations. The administrative costs is increased as per the number of servers. Virtualization decreases number of required servers for a given workload, hence reduces the cost of administrative employees.

Virtualization

- Virtualization refers to **the partitioning the resources of a physical system** (such as computing, Storage, Network and Memory) **into multiple virtual resources**.
- In cloud computing, **resources are pooled to serve multiple users using Multi-Tenancy**.
- Multi-Tenant aspects of the cloud **allow multiple users to be served by the same physical hardware**.
- The below figure shows the architecture of a virtualization technology in cloud computing.
- The physical resources such as **computing, storage, memory and network resources are virtualized**.
- The **virtualization layer partitions the physical resources into multiple virtual machines**.



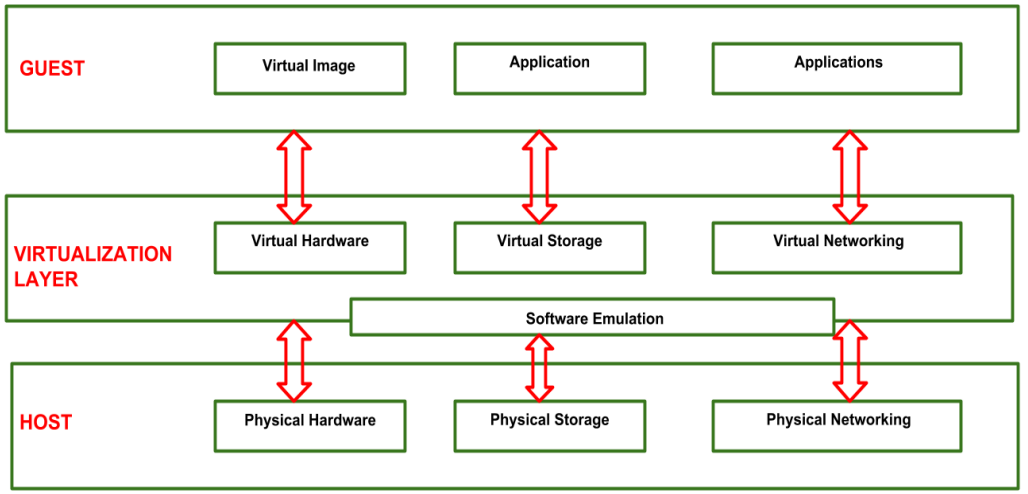
Virtualization architecture

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

VIRTUALIZATION REFERENCE MODEL

Three major Components falls under this category in a virtualized environment:

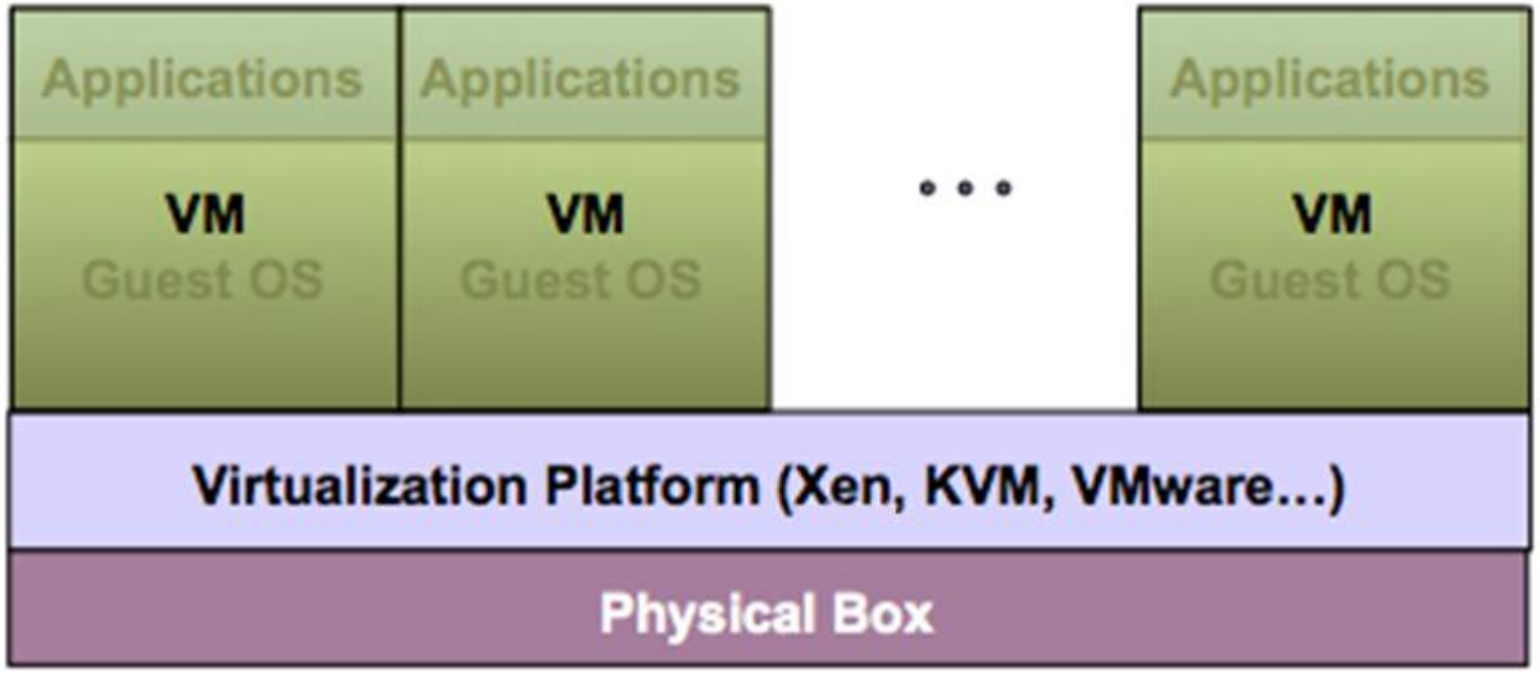
1. **GUEST:** The guest represents the system component that interacts with the virtualization layer rather than with the host, as would normally happen. Guests usually consist of one or more virtual disk files, and a VM definition file. Virtual Machines are centrally managed by a host application that sees and manages each virtual machine as a different application.
2. **HOST:** The host represents the original environment where the guest is supposed to be managed. Each guest runs on the host using shared resources donated to it by the host. The operating system, works as the host and manages the physical resource management, and the device support.
3. **VIRTUALIZATION LAYER:** The virtualization layer is responsible for recreating the same or a different environment where the guest will operate. It is an additional abstraction layer between a network and storage hardware, computing, and the application running on it. Usually it helps to run a single operating system per machine which can be very inflexible compared to the usage of virtualization.



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

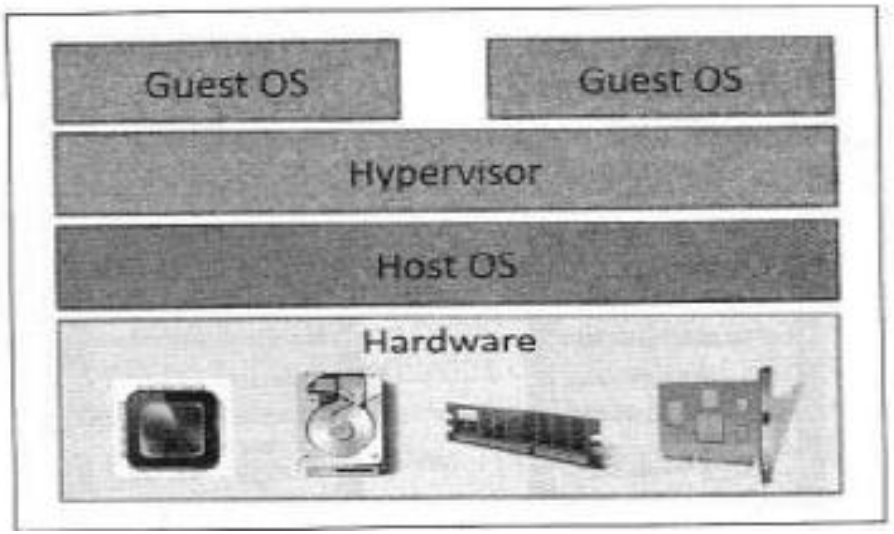
Virtualization Architecture

- A Virtual Machine (VM) is an isolated runtime environment (guest OS and applications).
- Multiple virtual systems (VMs) can run on a single physical system.



Virtualization: Guest Operating System

- A **guest OS is an operating system that is installed in a virtual machine** in addition to the host OS.
- In virtualization, the **guest OS can be different from the host OS.**



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

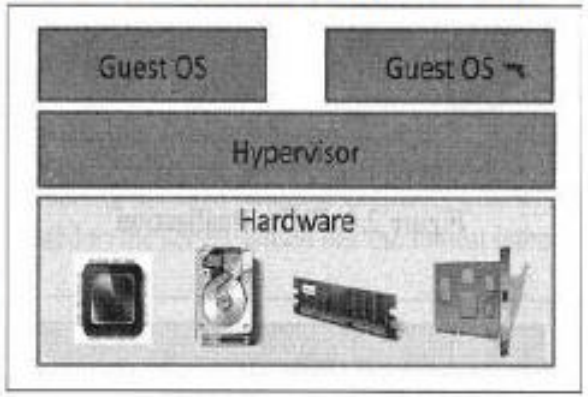
Hypervisor

- A hypervisor, a.k.a. a virtual machine manager/monitor (VMM), or virtualization manager, is a program that allows multiple operating systems to share a single hardware host.
- Each guest operating system appears to have the host's processor, memory, and other resources all to itself.
- However, the hypervisor is actually controlling the host processor and resources,
- Allocating what is needed to each operating system in turn
- Making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

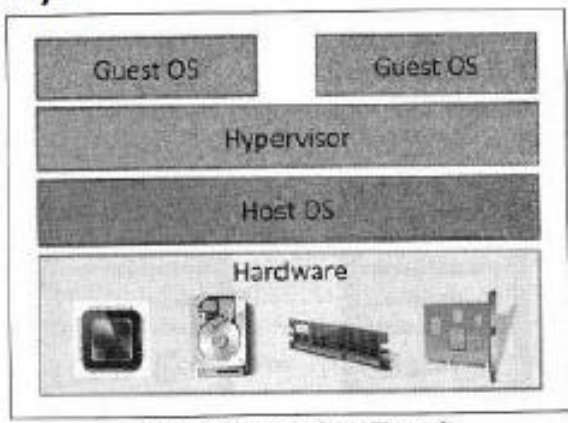
MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Types of Hypervisors

- The **virtualization layer consists of a hypervisor or a Virtual Machine Monitor (VMM).**
- There are two types of hypervisors
  - **Type-1 Hypervisors or Native Hypervisors**
  - **Type-2 Hypervisors or Hosted Hypervisors**



Hypervisor design: Type-1



Hypervisor design: Type-2

Type-1 Hypervisors or Native Hypervisors

- **Type-1 Hypervisors or Native Hypervisors run directly on the host hardware** and **control the hardware** and **monitor the guest operating system.**

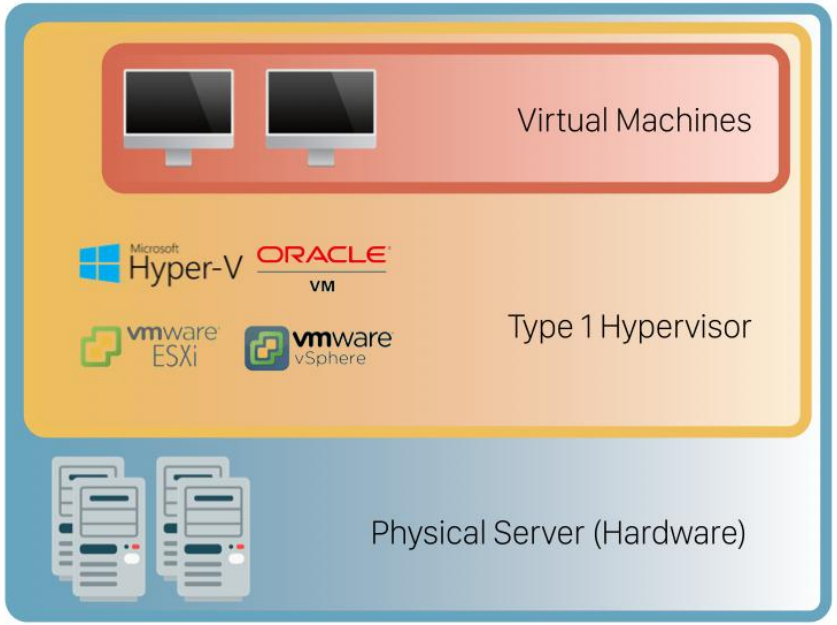
Type 2 Hypervisors or Hosted Hypervisors

- **Type 2 Hypervisors or Hosted Hypervisors run on top of a conventional** (main or Host) **operating system** and **monitor the guest operation systems.**

Type 1 Hypervisors or Bare metal hypervisor

- A Type 1 hypervisor is a layer of software installed directly on top of a physical server and its underlying hardware.
- Since no other software runs between the hardware and the hypervisor, it is also called the **bare-metal hypervisor.**
- Provides excellent performance and stability since it does not run inside Windows or any other operating system.

- It is a simple operating system designed to run virtual machines.
- The physical machine the hypervisor runs on serves virtualization purposes only.
- Most cloud service providers use Type 1 hypervisors, mainly found in enterprise environments.
- Basically, you would install a Type 1 hypervisor before anything else on a physical host, so it sort of acts like that host's operating system.
- A Type 1 hypervisor has direct access to the underlying physical host's resources—e.g., CPU, RAM, storage, and network interface.
- e.g. Type 1 hypervisors are VMware ESXi and Microsoft Hyper-V.



Type 1 Hypervisors or Bare metal hypervisor

- Once you boot up a physical server with a bare-metal hypervisor installed, it displays a command prompt-like screen with some of the hardware and network details.
- They include the CPU type, the amount of memory, the IP address, and the MAC address.
- Example of a VMware ESXi type 1 hypervisor screen after the server boots up.
- Type 1 hypervisors offer important benefits in terms of performance and security, while they lack advanced management features.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Pros & Cons of Type 1 Hypervisor

Pros

1. VM Mobility

- Type 1 hypervisors enable moving virtual machines between physical servers, manually or automatically.
- This move is based on the resource needs of a VM at a given moment and happens without any impact on the end-users.
- In case of a hardware failure, management software moves virtual machines to a working server as soon as an issue arises.
- The detection and restoration procedure takes place automatically and seamlessly.

2. Security

- The type 1 hypervisor has direct access to hardware without an additional OS layer. This direct connection significantly decreases the attack surface for potential malicious actors.

3. Resource Over-Allocation

- With type 1 hypervisors, you can assign more resources to your virtual machines than you have.
- For example, if you have 128GB of RAM on your server and eight virtual machines, you can assign 24GB of RAM to each.
- This totals 192GB of RAM, but VMs themselves will not consume all 24GB from the physical server. The VMs detect they have 24GB when they only use the amount of RAM they need to perform particular tasks.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Pros & Cons of Type 1 Hypervisor

Cons

1. Limited functionality

- Type 1 hypervisors are relatively simple and do not offer many features.
- The functionalities include basic operations such as changing the date and time, IP address, password, etc.

2. Complicated management

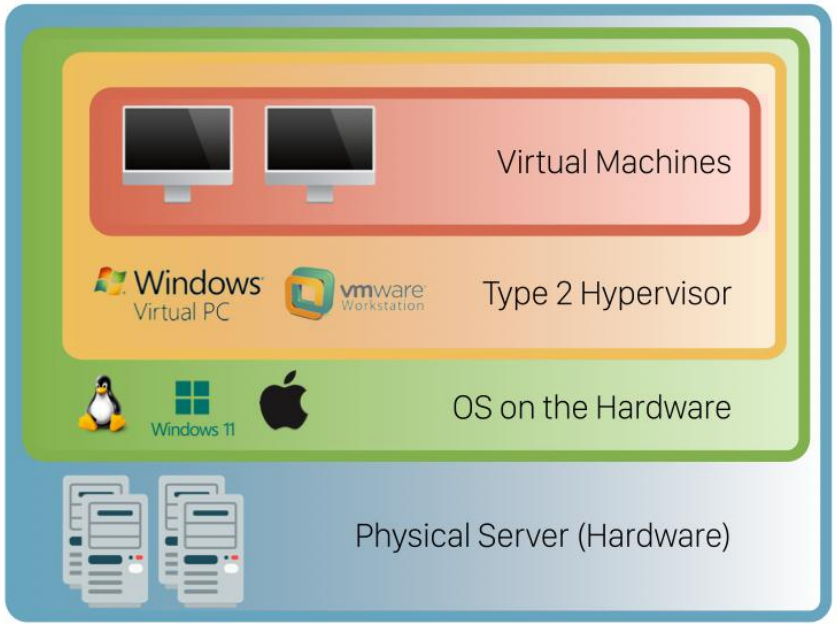
- To create virtual instances, you need a management console set up on another machine.
- Using the console, you can connect to the hypervisor on the server and manage your virtual environment.

3. Price

- Depending on what functionalities you need, the license cost for management consoles varies substantially

Type 2 Hypervisor or hosted hypervisor

- Type 2 hypervisors run inside the physical host machine's operating system, which is why they are called **hosted hypervisors.**
- Unlike bare-metal hypervisors that run directly on the hardware, hosted hypervisors have one software layer in between.
- So, you would have to install a host OS on your physical host before you can install a Type 2 hypervisor.
- When a Type 2 hypervisor needs to communicate with the underlying hardware or access hardware resources, it must go through the host OS first.
- **The system with a hosted hypervisor contains:**
  a. A physical machine
  b. An OS installed on the hardware (Windows, Linux, macOS).
  c. A type 2 hypervisor software within that operating system
  d. Guest virtual machine instances.
- A Type 2 hypervisor runs on top of a host OS.
- Type 2 hypervisors are usually easier to set up and use.
- Hence, they're more common among end users.
- VMware Workstation Pro/ VMware Fusion, VirtualBox and Parallels® Desktop, the most popular solution for running Windows on Macs, are Type 2 hypervisors..

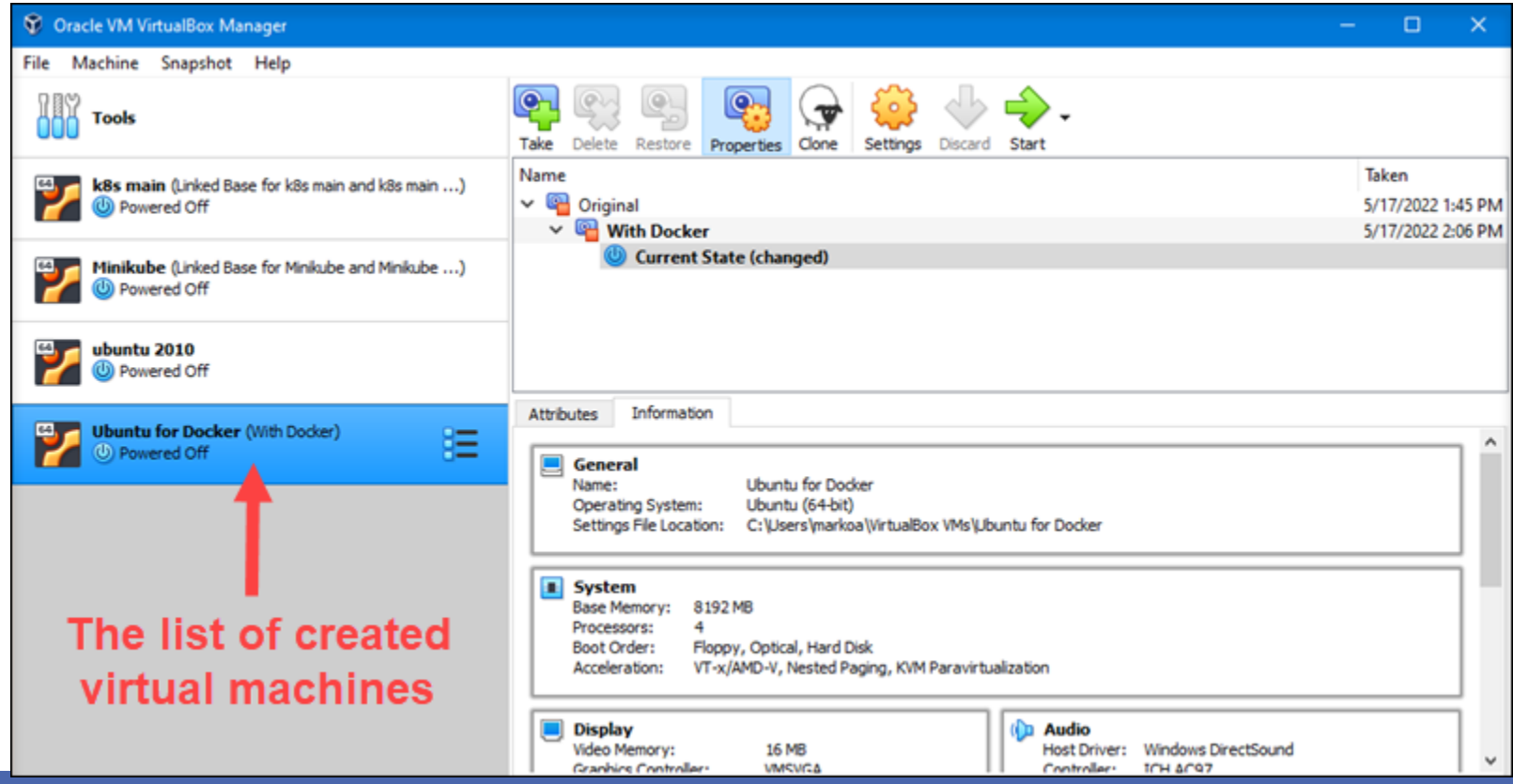


Type 2 Hypervisor or hosted hypervisor

- Type 2 hypervisors are typically found in environments with a small number of servers.
- What makes them convenient is that they do not need a management console on another system to set up and manage virtual machines.

- Everything is performed on the server with the hypervisor installed, and virtual machines launch in a standard OS window.

- Hosted hypervisors also act as management consoles for virtual machines.
- Any task can be performed using the built-in functionalities.
- Here is one example of a type 2 hypervisor interface (VirtualBox by Oracle).
- Type 2 hypervisors are simple to use and offer significant productivity-related benefits but are less secure and performant.



Pros & Cons of Type 2 Hypervisor

Pros

1. Easy to manage

- There is no need to install separate software on another machine to create and maintain your virtual environment.
- Install and run a type 2 hypervisor as any other application within your OS.
- Create snapshots or clone your virtual machines, import or export appliances, etc.

2. Convenient for testing

- Type 2 hypervisors are convenient for testing new software and research projects.
- It is possible to use one physical machine to run multiple instances with different operating systems to test how an application behaves in each environment or to create a specific network environment.
- You only need to ensure that there are enough physical resources to keep the host and virtual machines running.

3. Allows access to additional productivity tools

- The users of type 2 hypervisors can use the tools available on other operating systems alongside their primary OS.
- For example, Windows users can access Linux applications by creating a Linux virtual machine.

Pros & Cons of Type 2 Hypervisor

Cons

1. Less flexible resource management

- Allocating resources with this type of hypervisor is more difficult than with type 1.
- Bare-metal hypervisors can dynamically allocate available resources depending on the current needs of a particular VM.
- A type 2 hypervisor occupies whatever the user allocates to a virtual machine.
- When a user assigns 8GB of RAM to a VM, that amount will be taken up even if the VM is using only a fraction of it.
- If the host machine has 32GB of RAM and the user creates three VMs with 8GB each, they are left with 8GB of RAM to keep the physical machine running.
- Creating another VM with 8GB of ram would bring down the system.

2. Performance

- The host OS creates additional pressure on physical hardware, which may result in VMs having latency issues.

3. Security

- Type 2 hypervisors run on top of an operating system.
- This fact introduces a potential vulnerability since attackers may use potential vulnerabilities of the OS to gain access to VMs

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Taxonomy of Virtualization

- Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines.
- Virtual software mimics the functions of physical hardware to run multiple virtual machines simultaneously on a single physical machine.
- Virtualization is mainly used to emulate the **execution environment**, **storage**, and **networks**. Among these categories, **execution virtualization** constitutes the oldest, most popular, and most developed area.
- Therefore, it deserves major investigation and a further categorization. The execution environment is classified into two:

  1. Process-level — implemented on top of an existing operating system, , which has full control of the hardware.

  2. System-level — implemented directly on hardware and do not require or require a minimum of support from an existing operating system.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Taxonomy of Virtualization

Virtualization is mainly used to emulate:

1] Execution Environments: To provide support for the execution of the programs example OS, and Application.

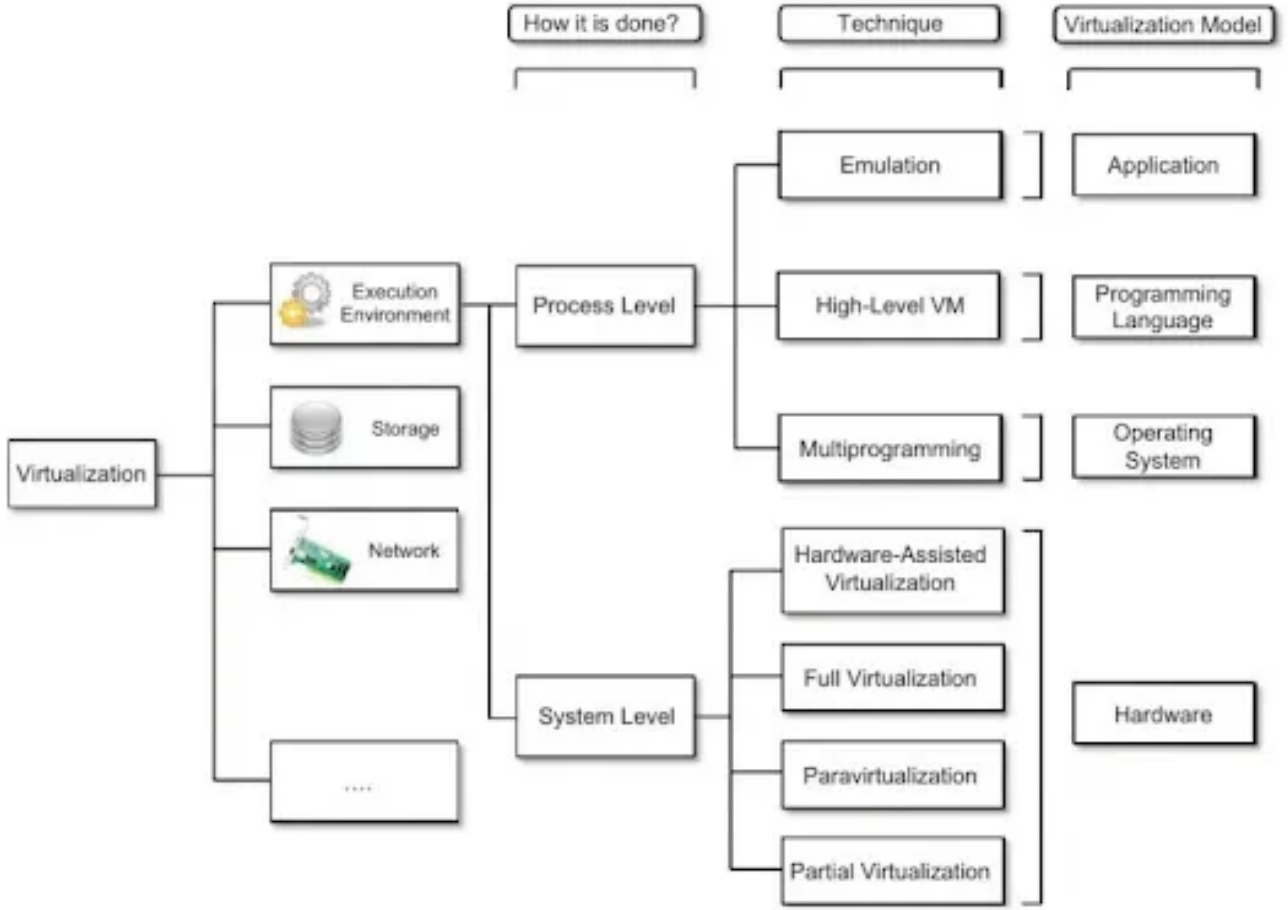
Process Level: Implemented on top of an existing OS that has full control of the hardware

System Level: Implemented directly on Hardware and do not require support from existing OS.

2] Storage: Storage virtualization is a system administration practice that allows decoupling the physical organization of the hardware from its logical representation.

3] Networks: Network virtualization combines hardware appliances and specific software for the creation and management of a virtual network.

Taxonomy of Virtualization



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Virtualization Categories

1. Application Virtualization
2. Network Virtualization
3. Desktop Virtualization
4. Storage Virtualization
5. Server Virtualization
6. Data virtualization

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Execution virtualization

- Includes all techniques that aim to emulate an execution environment that is separate from the one hosting the virtualization layer.
- All these techniques concentrate their interest on providing support for the execution of programs, whether these are the operating system, a binary specification of a program compiled against an abstract machine model, or an application.
- Therefore, execution virtualization can be implemented directly on top of the hardware by the operating system, an application, or libraries dynamically or statically linked to an application image

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Hardware-level virtualization

- It is a virtualization technique that provides an abstract execution environment in terms of computer hardware on top of which a guest operating can be run.
- It is also called system virtualization, since it provides ISA (Instruction Set Architecture) to virtual machines, which is the representation of the hardware interface of a system.
- Hardware-level virtualization is also called system virtualization .
- A fundamental element of hardware virtualization is the hypervisor, or virtual machine manager (VMM).
- It recreates a hardware environment in which guest operating systems are installed.

Hardware Virtualization Techniques

1. Full virtualization:

- It refers to the ability to run a program, most likely an operating system, directly on top of a virtual machine and without any modification, as though it were run on the raw hardware.
- To make this possible, virtual machine manager are required to provide a complete emulation of the entire underlying hardware .

2. Para-virtualization:

- This is a not-transparent virtualization solution that allows implementing within virtual machine managers.
- **Paravirtualization** techniques expose a software interface to the virtual machine that is slightly modified from the host and, as a consequence, guests need to be modified.
- The aim of para virtualization is to provide the capability to demand the execution of performance-critical operations directly on the host.

3. Partial virtualization :

- It provides a partial emulation of the underlying hardware, thus not allowing the complete execution of the guest operating system in complete isolation.
- It allows many applications to run transparently, but not all the features of the operating system can be supported, as happens with full virtualization

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Operating System-Level Virtualization

- It offers the opportunity to create different and separated execution environments for applications that are managed concurrently.
- Differently from hardware virtualization, there is no **virtual machine manager or hypervisor**, and the virtualization is done within a single operating system, where the OS kernel allows for multiple isolated user space instances.

Programming language-level virtualization

- Programming language-level virtualization is mostly used to achieve ease of deployment of applications, managed execution, and portability across different platforms and operating systems
- The main advantage of programming-level virtual machines, also called **process virtual machines**, is the ability to provide a uniform execution environment across different platforms.
- Programs compiled into bytecode can be executed on any operating system and platform for which a virtual machine able to execute that code has been provided.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Application-level virtualization

- The application-level virtualization is used when there is a desire to virtualize only one application
- Application virtualization software allows users to access and use an application from a separate computer than the one on which the application is installed

Other types of virtualizations

- Other than execution virtualization, other types of virtualizations provide an abstract environment to interact with.
- These mainly cover storage, networking, and client/server interaction.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Benefits of Virtualization

- Flexible and efficient resource allocation
- Improved productivity in development
- Reduced IT infrastructure costs
- Remote access and
- Quick scalability
- High availability and
- Disaster recovery
- Pay-per-use of IT infrastructure on demand, and
- The ability to run multiple operating systems

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Benefits of Virtualization

- Sharing of resources helps cost reduction
- **Isolation:** Virtual machines are isolated from each other as if they are physically separated
- **Encapsulation:** Virtual machines encapsulate a complete computing environment
- **Hardware Independence:** Virtual machines run independently of underlying hardware
- **Portability:** Virtual machines can be migrated between different hosts.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Virtualization in Cloud Computing

Cloud computing takes virtualization one step further:

- You don’t need to own the hardware
- Resources are rented as needed from a cloud
- Various providers allow creating virtual servers:
  - Choose the OS and software each instance will have
  - The chosen OS will run on a large server farm
  - Can instantiate more virtual servers or shut down existing ones within minutes
- You get billed only for what you used

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Virtualization Security Challenges

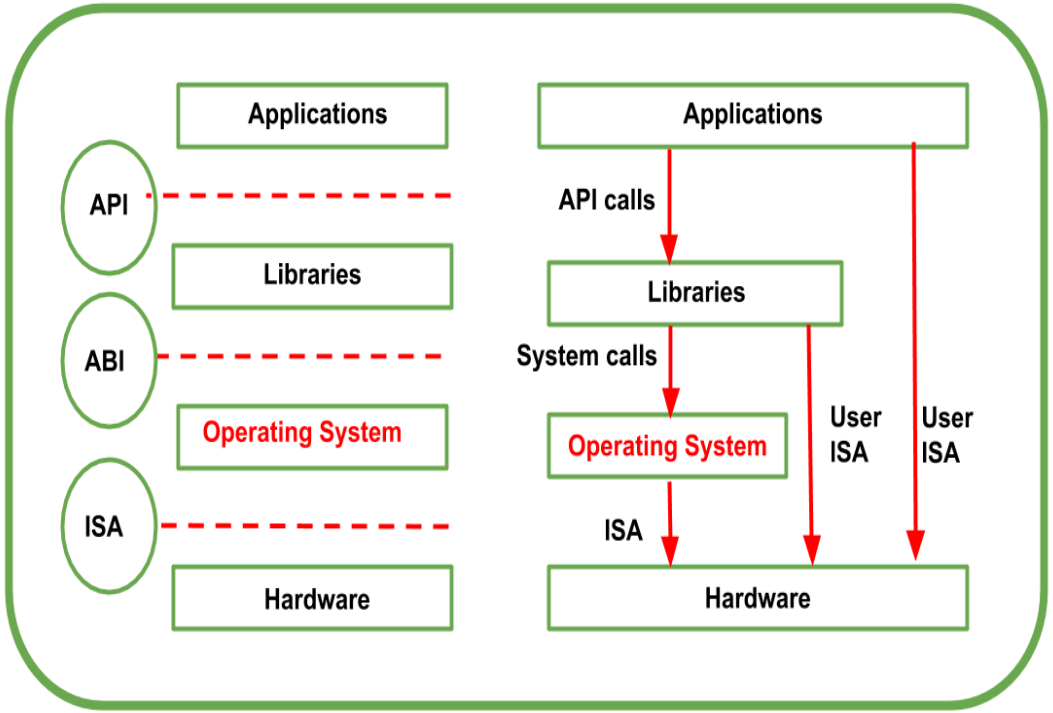
The trusted computing base (TCB) of a virtual machine is too large.

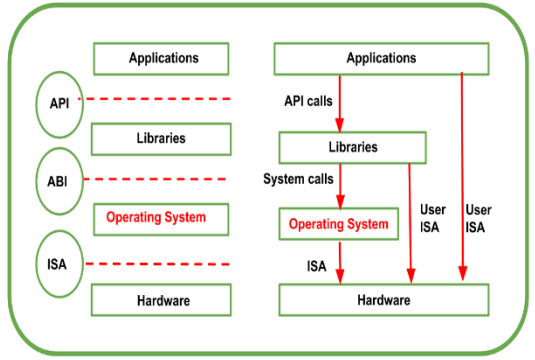
- The Trusted Computing Base (TCB) refers to all of a system's hardware, firmware, and software components that provide a secure environment.
- TCB is everything in a computing system that provides a secure environment for operations.
- This includes its hardware, firmware, software, operating system, physical locations, built-in security controls, and prescribed security and safety procedures.
- The components inside the TCB are considered "critical." If one component inside the TCB is compromised, the entire system's security may be jeopardized.
- A small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security*
- Smaller TCB → more security

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Virtualization | A Machine Reference Model

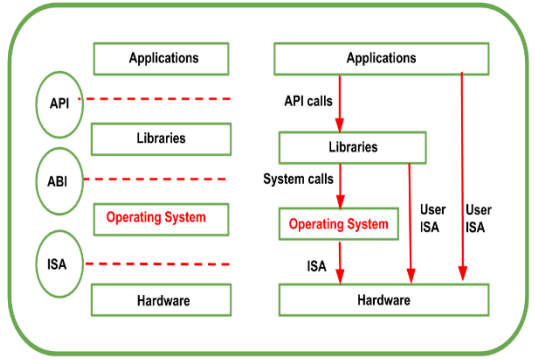
- When an execution environment is virtualized at unlike levels of the stack of computation then it requires a reference model which defines the **interfaces** within the level of abstractions, and this level of abstraction hides the details of implementations.
- Virtualization techniques can substitute any one layer and can intercept the calls which are directed to it.
- A clear separation within the layers can simplify their implementations, which only need an emulation of the interfaces and a proper response with the underlying layer.
- At the base layer, the model for the hardware is declared or manifested on terms of an architecture i.e. Instruction Set Architecture (ISA).





Virtualization | A Machine Reference Model

- **Instruction Set Architecture (ISA)** defines the instruction set for the processor, registers, memory, and interrupt management.
- It is an interface between software and hardware and It is mandatory for the operating system (OS) developer (system ISA) developers of applications who directly manages core hardware (user ISA).
- The operating system layer is separated by the application binary interface (ABI) from the application and libraries, which are managed by operating system.
- **Application Binary Interface (ABI)** covers facts such as low-level data types and call conventions and it also defines a format for many programs. Mainly, system calls are defined at this level.
- Moreover, this type of interface enables portability of various applications and libraries across OS which employ the same ABI.
- **Application programming interface (API)** is represented by the highest level of abstraction.
- This API interfaces applications to libraries and/or the core OS. For an action is to be performed in the application level API, ABI and the two which are responsible to make it done.



Virtualization | A Machine Reference Model

Mainly, CPU runs on two privilege levels:

1. User Mode:

- In this mode, memory access is restricted up to some limit whereas access to peripherals is denied.

2. Kernel Mode:

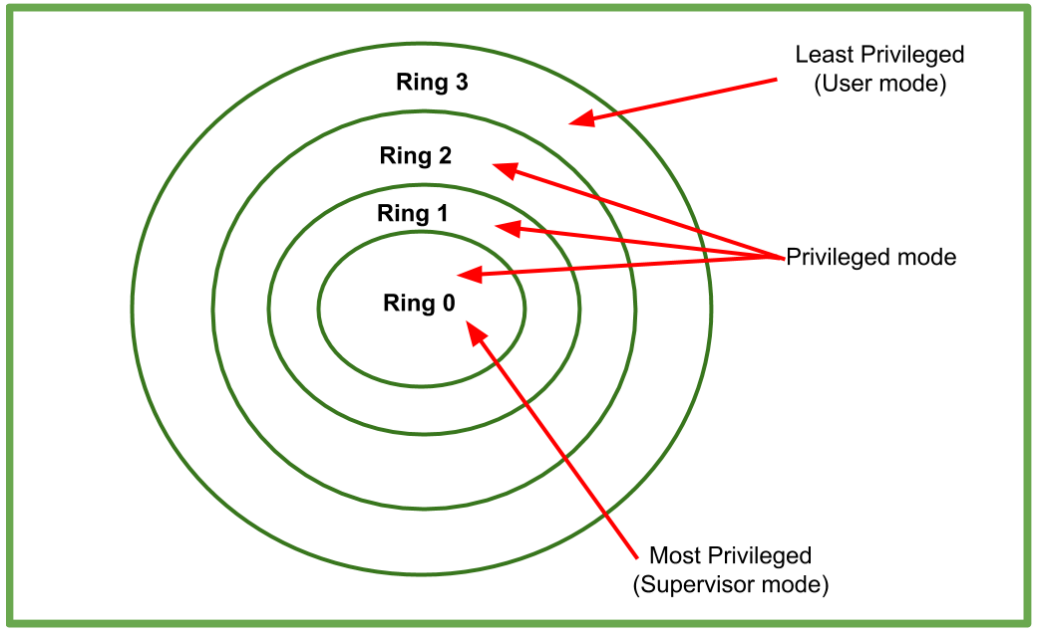
- In this mode, CPU has instructions which manage memory and how to be accessed and it also has instructions which enable access of the peripherals like disks and network cards.
- From one running program to another running program, CPU switches automatically.
- The expansions and applications of computing system are simplified by this layered approach.
- Application of multitasking and co-existence of multiple executing is simplified by this layered approach.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Virtualization | A Machine Reference Model

Privileged Mode

- Those instructions which can be used with interrupting with another task are known as **Non-privileged instruction**. They are also called so because shared resources are not accessed.
- **Example:** All the fixed points, floating and arithmetic instructions
- The instructions which are executed under particular restrictions and which are frequently used for sensitive operations (which expose behaviour-sensitive or modify control sensitive) are known as **privileged instructions**.
- It is expected that in a hyper visor-managed environment, code of guest OS runs in user to prevent it from the direct access of OS's status.
- It is no longer possible to completely isolate the guest OS when non-privileged instructions are implemented.



Security Rings and Privileged Mode

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Virtualization Security Requirements

Scenario: A client uses the service of a cloud computing company to build a remote VM

- A secure network interface
- A secure secondary storage
- A secure run-time environment
  - ✓ Build, save, restore, destroy

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Virtualization Security Requirements

- A secure run-time environment is the most fundamental
- The first two problems already have solutions:
  - Network interface: Transport layer security (TLS)
  - Secondary storage: Network file system (NFS)
- The security mechanism in the first two rely on a secure run-time environment
  - All the cryptographic algorithms and security protocols reside in the run-time environment

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Pros and Cons of Virtualization

- Virtualization is the creation of Virtual Version of something such as server, desktop, storage device, operating system etc.
- Virtualization is a technique which allows us to share a single physical instance of a resource or an application among multiple customers and an organization.
- Virtualization often creates many virtual resources from one physical resource.

Pros of Virtualization in Cloud Computing :

1. Utilization of Hardware Efficiently
2. Availability increases with Virtualization
3. Disaster Recovery is efficient and easy
4. Virtualization saves Energy
5. Quick and Easy Set up
6. Cloud Migration becomes easy
7. Encourages digital entrepreneurship

Cons of Virtualization:

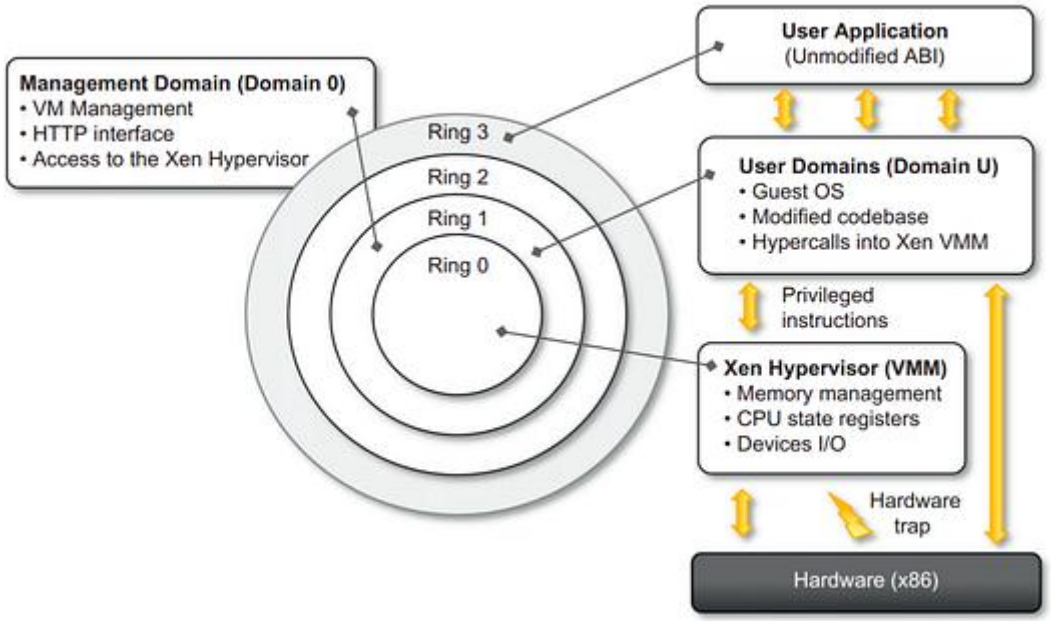
1. Data can be at Risk
2. Not all hardware or software can be virtualized
3. Learning New Infrastructure
4. High Initial Investment
5. Problems with scalability
6. A Number of links must interact
7. Threats to security

Technology Examples

Case Studies

Xen Architecture and Guest OS Management

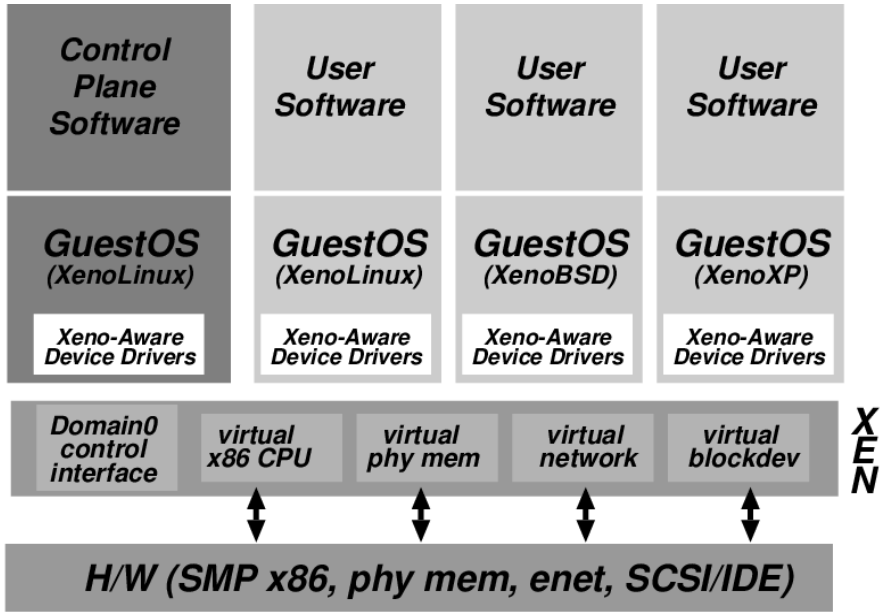
- *Xen is an open-source virtualization platform*
- *It was initially developed at the University of Cambridge and is now maintained by the Xen Project, a collaborative community of developers.*
- *It is either used for desktop or server virtualization.*
- *It employs para-virtualization, which involves modifying guest operating systems for better efficiency.*
- *Para-virtualization is a virtualization technique that involves modifying the operating system (OS) running inside a virtual machine (VM) to make it aware of its virtualized environment.*
- *Para-virtualization requires changes to the guest OS to improve performance, security, and efficiency*
- *Strong isolation and performance, used by cloud providers like Amazon Web Services.*
- *Xen is cost-effective as it's open source, but it can have a steeper learning curve.*
- Example: **XenoLinux** is a modified Linux OS that runs on Xen hypervisor.



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Xen Virtualization Architecture and the Threat Model

- Management VM – Dom0
- Guest VM – Dom
- Dom0 may be malicious
  - Vulnerabilities
  - Device drivers
  - Careless / malicious administration
- Dom0 is in the TCB of DomU because it can access the memory of DomU, which may cause information leakage/ modification



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Pros of Xen:

- **High Performance**
  - Xen's paravirtualization approach often results in better performance compared to full virtualization methods. By modifying the guest operating systems, Xen reduces the overhead associated with virtualization, making it suitable for high-performance computing workloads.
- **Strong Isolation**
  - Xen offers strong isolation between virtual machines, which enhances security and stability. Each VM runs in its own isolated environment, preventing one VM from affecting others even in the case of system failures or security breaches.
- **Open Source**
  - Xen is open-source software, making it a cost-effective choice for organizations looking to implement virtualization without significant licensing costs. This open nature also encourages a community of developers to contribute and improve the platform continually.
- **Live Migration**
  - Xen supports live migration, allowing virtual machines to be moved between physical hosts with minimal downtime. This is essential for load balancing, hardware maintenance, and fault tolerance.
- **Compatibility:** Xen supports a wide range of operating systems as both guests and hosts, making it versatile and suitable for various use cases.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Cons of Xen

- **Complex Configuration:** Xen can be complex to set up and configure, especially for beginners. Managing and configuring VMs in a Xen environment may require a steeper learning curve compared to some other virtualization solutions.
- **Limited Desktop Virtualization Support:** While Xen can be used for desktop virtualization, it is not as well-optimized for this purpose as some other virtualization platforms like VMware Horizon or Citrix XenDesktop.
- **Hardware Support:** Hardware support can be a limitation. Xen relies on hardware virtualization extensions (Intel VT-x or AMD-V) for certain features. Older hardware or systems lacking these extensions may not work optimally with Xen.
- **Community Support:** While Xen has an active open-source community, it may not have as extensive support and resources as some commercial virtualization solutions like VMware.
- **Integration and Compatibility:** Integrating Xen with certain management tools or integrating Xen-based VMs with other virtualization platforms may be more challenging due to the specific paravirtualization features.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Technology Example: VMware

- VMware is built upon the principle of **full virtualization**, which involves duplicating the underlying hardware and presenting it to the guest OS.
- The guest OS operates without any awareness of this abstraction layer and requires no modifications.
- Full virtualization is a virtualization technique that allows multiple virtual machines (VMs) to run on a single physical host without modifications to the guest operating systems.
- In a fully virtualized environment, each virtual machine operates as if it has its own dedicated physical hardware, even though it shares resources with other VMs on the same host.
- VMware is a leading company in the field of virtualization and cloud computing.
- They provide a range of virtualization and cloud management solutions that allow organizations to create and manage virtualized IT environments.
- VMware's most notable product is VMware vSphere, which includes the ESXi hypervisor, vCenter Server for centralized management, and various other components for virtual infrastructure management.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Pros of VMware

1. **Highly Reliable**

   VMware has a strong reputation for reliability. It's widely used in enterprise environments where system uptime is critical. Their products undergo rigorous testing and are known for their stability.

2. **Mature Ecosystem**

   VMware has a large and mature ecosystem with a vast number of third-party integrations, tools, and resources. This makes it easier to find solutions that fit specific needs.

3. **Performance:** VMware's virtualization technology is known for its high performance. Their hypervisor, ESXi, is designed for efficiency and speed.

4. **Security:** VMware provides security features to protect virtualized environments. This includes features like vSphere Security, which enhances the security of VMs and their communication.

5. **Management Tools:** VMware offers a comprehensive set of management tools. VMware vCenter Server allows administrators to manage and monitor virtual environments from a central location, providing a robust set of features for resource management and performance optimization.

6. **Live Migration:** VMware supports live migration of virtual machines, enabling seamless movement of workloads from one host to another with minimal downtime, which is essential for load balancing and hardware maintenance.

7. **Wide Guest OS Support:** VMware supports a wide range of guest operating systems, making it versatile for different types of workloads and applications.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Cons of VMware

1. **Cost:** One of the significant drawbacks of VMware is the cost. VMware's products can be expensive, especially for smaller organizations. Licensing costs can add up quickly.

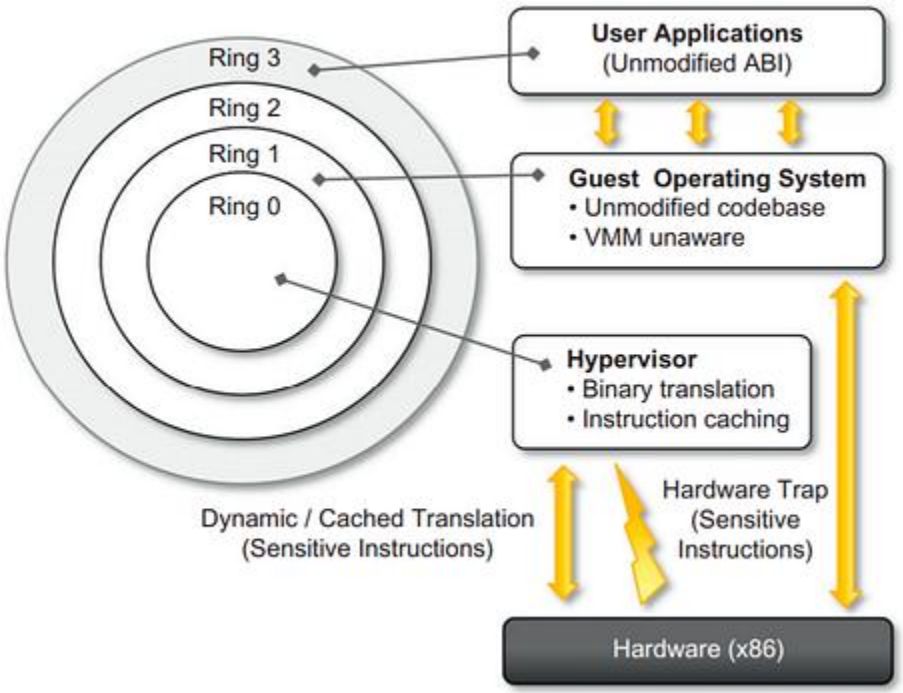
2. **Resource Intensive:** While VMware is known for its performance, it can be resource-intensive. The hypervisor and management tools may require dedicated hardware and resources, which can impact the overall infrastructure costs.

3. **Complexity:** VMware's products can be complex to set up and manage, especially for beginners. This complexity can make it more challenging for organizations without extensive IT expertise.

4. **Vendor Lock-In:** There's a concern that once an organization heavily invests in VMware's ecosystem, it may be challenging to migrate to other virtualization platforms due to vendor lock-in.

5. **Limited Free Options:** VMware offers a limited free version of its hypervisor (VMware vSphere Hypervisor, formerly ESXi), but many advanced features are available only in the paid versions.

The reference model of full virtualization



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Technology Example: Microsoft Hyper-V

- It is a **virtualization technology and hypervisor** developed by **Microsoft**.
- It allows you to create and manage virtual machines (VMs) on Windows-based servers.
- Hyper-V is commonly used in data centers, enterprise environments, and cloud services to consolidate workloads, enhance resource utilization, and provide scalable and flexible virtualization solutions.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Pros of Microsoft Hyper-V

1. **Integration with Windows Ecosystem:** Hyper-V seamlessly integrates with Microsoft's Windows Server operating system and management tools, making it a natural choice for organizations heavily invested in Microsoft technologies.
2. **Cost-Effective:** For Windows-based environments, Hyper-V can be a cost-effective virtualization solution since it's included with Windows Server licenses. This can result in significant cost savings compared to third-party virtualization solutions.
3. **Broad Guest OS Support:** Hyper-V supports a wide range of guest operating systems, including various Windows versions, Linux distributions, and others, making it versatile for different workloads.
4. **Live Migration:** Hyper-V offers features like live migration, which allows VMs to be moved between physical hosts with minimal downtime, enhancing availability and resource optimization.
5. **Clustering and High Availability:** Hyper-V supports clustering and high-availability features, ensuring business continuity by automatically moving VMs to healthy hosts in case of hardware or host failures.
6. **Hyper-Converged Infrastructure:** Microsoft offers solutions like Azure Stack HCI, which combines Hyper-V with storage and networking features for hyper-converged infrastructure deployments.
7. **Management Tools:** Hyper-V is managed using Microsoft's Hyper-V Manager and can be further enhanced with System Center Virtual Machine Manager (SCVMM) for more extensive management capabilities.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Cons of Microsoft Hyper-V

1. **Complexity for Linux Support:** While Hyper-V supports Linux, it may be more challenging to set up and manage Linux VMs compared to other virtualization platforms, which might have better native support for Linux.

2. **Hardware Requirements:** Hyper-V requires specific hardware virtualization extensions (Intel VT-x or AMD-V), which may limit its compatibility with older hardware.

3. **Licensing Costs:** While Hyper-V can be cost-effective in Windows environments, there are licensing costs associated with Windows Server, System Center, and other management tools, which can add to the overall cost.

4. **Ecosystem Limitations:** Hyper-V may not have as extensive a third-party ecosystem as other virtualization solutions like VMware, which may limit the availability of add-on tools and extensions.

5. **Learning Curve:** Hyper-V has a learning curve, and while it's relatively straightforward for Windows administrators, those new to the platform may find it initially complex.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Technology Example: 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.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

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.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

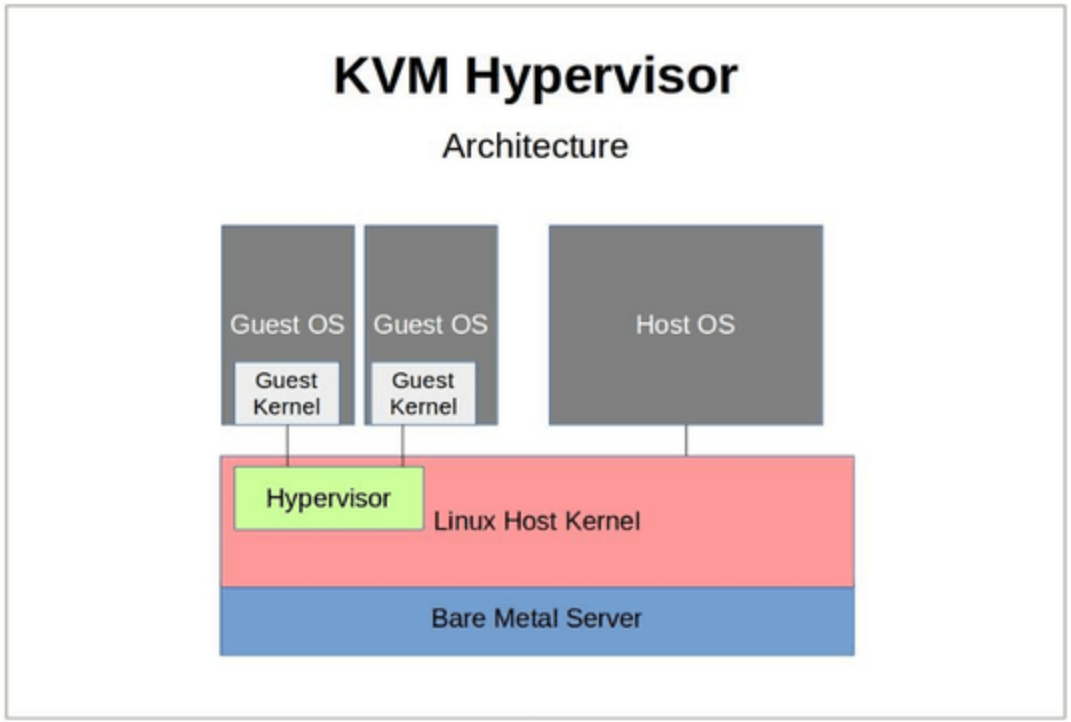
Why is KVM important?

- 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.

KVM architecture

- **Hypervisor:** KVM works as a hypervisor, embedding itself into the Linux kernel and transforming it into a high-performance hypervisor.

- **QEMU (Quick Emulator):** QEMU is used in combination with KVM to emulate virtual machine hardware and provide resource management.



MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

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.
- **Linux kernel:** Linux kernel is the core of the open-source operating system.
  - A kernel is a low-level program that interacts with computer hardware.
  - It also ensures that software applications running on the operating system receive the required computing resources.
  - Linux distributions, such as Red Hat Enterprise Linux, Fedora, and Ubuntu, pack the Linux kernel and additional programs into a user-friendly commercial operating system.

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.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Cons of KVM

1. **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.

2. **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.

3. **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.

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

5. **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.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Cloud Migration

- Cloud migration is the process of moving a company's digital assets, services, databases, IT resources, and applications either partially, or wholly, into the cloud.
- Cloud migration is the process of moving data, applications or other business elements to a cloud computing environment.
- Cloud migration is also about moving from one cloud to another.
- Companies wishing to move on from outdated and increasingly inefficient legacy infrastructures, such as aging servers or potentially unreliable firewall appliances, or to abandon hardware or software solutions that are no longer operating at optimum capacity, are now turning to the cloud to experience the benefits of cloud computing.
- This is why so many organizations are, at the very least, making a partial migration to the cloud.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Various types of cloud migrations

- There are various types of cloud migrations an enterprise can perform.

1. One common model is to transfer data and applications from a local on-premises data center to the public cloud.
2. However, a cloud migration could also entail moving data and applications from one cloud platform or provider to another; this model is known as **cloud-to-cloud (C2C) migration**.
3. A third type of migration is a reverse cloud migration, **cloud repatriation** or **cloud exit**, where data or applications are moved off of the cloud and back to a local data center.

Why is cloud migration important?

- Cloud migration is a process of transition or change.
- When an organization decides to use a cloud service, the goal is to treat computing as a utility -- like electricity, water or natural gas.
- The highly scalable, pay-as-you-go nature of the public cloud provides businesses with the flexibility to use only the resources needed, for only as long as needed, and pay only for those resources that are actually consumed.
- It's an attractive paradigm shift that entices businesses of all sizes and verticals.
- Many organizations migrate on-premises applications and data from their local data center to public cloud infrastructure to take advantage of benefits such as greater elasticity, self-service provisioning, redundancy and a flexible pay-per-use model.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Benefits of cloud migration

- For companies that undertake the process of cloud migration, the cloud can have a massive impact.
- This includes a reduction in the total cost of ownership (TCO), faster time to delivery, and enhanced opportunities for innovation.
- With access to the cloud comes agility and flexibility, both of which are imperative to meet changing consumer and market demands.
- **Benefits of migrating to the cloud include**:

1. Increased agility and flexibility
2. Ability to innovate faster
3. Easing of increasing resource demands
4. Better managing of increased customer expectations
5. Reduction in costs
6. Deliver immediate business results
7. Simplify IT
8. Shift to everything as-a-service
9. Better consumption management
10. Cloud scalability
11. Improved performance

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Types of cloud migration strategies

- Moving workloads to the cloud requires a well-thought-out strategy that includes a complex combination of management and technology challenges, as well as staff and resource realignment.
- There are choices in the type of migration to perform as well as the type of data that should move.
- It's important to consider the cloud migration checklist before taking action.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Types of cloud migration strategies

- There are three fundamental strategies for migrating an enterprise workload from the local data center to a cloud provider's infrastructure:

1. **Lift and shift. This strategy** -- also called rehosting -- is the most direct approach, where a local workload and its data are basically moved (rehosted) to corresponding compute and storage resources within a cloud provider's infrastructure. For example, a workload in a virtual machine (VM) and its storage volume can be redeployed to the cloud with relative ease and speed when there are few dependencies and minor business impact.
2. **Re-platform:** Not all workloads can accommodate simple rehosting. Many enterprise workloads can be complex with numerous dependencies, and a business might choose to make some changes to the workload's deployment schema to improve its performance in a public cloud environment. If a workload requires a database, for example, the business can use a compatible database service already hosted and available through the cloud provider rather than deploying a copy of the corresponding database. Re-platforming a workload can be more difficult and time-consuming -- and require more testing and validation -- than rehosting.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Types of cloud migration strategies

3. **Refactor:** This type of cloud migration involves a fundamental redesign of the workload itself in order to optimize its use of cloud resources and improve its performance in the cloud. For example, consider a single monolithic workload deployed as a large and unwieldly VM that is difficult to scale. This workload can be redesigned as a container-based, Kubernetes-powered microservices application capable of automatically scaling different microservices components in order to enhance performance while minimizing the use of cloud services. Refactoring a workload is often the most time-consuming and complex type of cloud migration project, which is usually reserved for businesses with cloud-first workload design and deployment strategies.

- In terms of the actual migration approach or process, every company has a different reason to move a workload to the cloud, and goals for each organization will vary.
- The first step is to identify the application or workload to move to the cloud.
- Next, figure out how much data needs to be moved, how quickly the work needs to be done and how to migrate that data.
- Take inventory of data and applications, and look for dependencies and how those will be replicated in the cloud or possibly rearchitected to accommodate numerous cloud service options.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Cloud migration deployment models

Enterprises today have more than one cloud model from which to choose:

1. **Public.** The public cloud lets many users access compute resources through the internet or dedicated connections.
2. **Private.** A private cloud keeps data within the data center and uses a proprietary architecture.
3. **Hybrid.** The hybrid cloud model mixes public and private cloud models and transfers data between the two.
4. **Multi-cloud.** In a multi-cloud scenario, a business uses IaaS options from more than one public cloud provider.

Beyond this initial choice of cloud model, there are three major cloud categories that should be considered for cloud deployments as

1. **Infrastructure as a service**
2. **Platform as a service**
3. **Software as a service**

It's important to note that all three cloud categories can be used concurrently in any combination that suits the needs of the particular business.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

How does the cloud migration process work?

(Cloud migration steps or processes)

- The cloud migration steps or processes an enterprise follows will vary based on factors such as the type of migration it wants to perform and the specific resources it wants to move.
- That said, common elements of a cloud migration strategy include the following:

1. Understand the purpose
2. Determine the target application(s)
3. Choose the cloud target
4. Select a proven cloud partner
5. Evaluate migration costs and needs
6. Choose the appropriate architecture
7. Create the migration plan
8. Perform the migration
9. Follow monitoring and reporting
10. Follow-up and organizational changes

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Best practices to ensure cloud migration success

- There are many reasons why an organization chooses to migrate an app or workload to the cloud, and each project will be unique depending on resource allocations, integrations with other services and multiple other factors.
- Here are some general guidelines for a cloud migration that streamline the process and improve changes for success:
  - Get organizational buy-in
  - Define cloud roles and ownership
  - Pick the right cloud services
  - Understand security risks
  - Calculate cloud costs
  - Devise a long-term cloud roadmap

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Common challenges during a cloud migration:

- Interoperability
- Data and application portability
- Data integrity and security
- Business continuity
- Without proper planning, a migration could degrade workload performance and lead to higher IT costs -- thereby negating some of the main benefits of cloud computing.
- As with any major technical endeavor, the business faces potential problems and challenges during and after the application migration process.
- A solid strategy won't completely eliminate all the hurdles and potential problems with a cloud migration.
- These challenges can include the following:

- Uncertain and excessive cloud costs
- Lack of cloud strategy
- Application performance in the cloud
- Application suitability for the cloud
- No cloud exit strategy
- Failure is not permanent
- Poor infrastructure design or provisioning
- Inadequate or ill-trained staff

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Cloud migration tools and services

- Workload management alters significantly when an application moves to the cloud. Enterprises should calculate the cost of a cloud configuration before a migration to avoid unexpected surprises.
- IT staff needs to change their management processes to work as well in the cloud as they do locally.
- This can be achieved by any number of services and tools.
- The big IaaS providers -- AWS, Microsoft and Google -- offer various cloud migration services as well as free tiers. Here are a few examples:

	AWS	Azure	Google Cloud
Database migration	AWS Database Migration Service	Azure Database Migration Service	Database Migration Service (preview)
Data transfer appliance	Snow Family	Data Box	Transfer Appliance
Disaster recovery	CloudEndure Disaster Recovery	Azure Site Recovery	N/A
Online data transfer	AWS DataSync, AWS Transfer Family	Azure File Sync	BigQuery Data Transfer Service, Cloud Data Transfer
On-premises application analysis	AWS Application Discovery Service, Migration Evaluator	Azure Migrate, Movere, Azure Resource Mover	N/A
On-premises and cloud storage integration	Storage Gateway	StorSimple	N/A (offered by partner Cloudian)
Migration tracker	AWS Migration Hub	Azure Migrate	N/A
Server migration	AWS App2Container, AWS Server Migration Service, CloudEndure Migration	Azure Migrate	Migrate for Anthos, Migrate for Compute Engine, VM migration

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Live Migration

- Live migration allows the system to move VMs from one host to another while the VM is turned on without workload interruption, regardless of whether the administrator or an automatic process initiates the movement.
- Live migration is the process of transferring a live virtual machine from one physical host to another without disrupting its normal operation.
- Live migration enables the porting of virtual machines and is carried out in a systematic manner to ensure minimal operational downtime.
- Live migrations occur regularly in the cluster nodes, triggered by maintenance operations, ADS workload balancing, node expansion, or administrator-driven requests.

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Live Migration

- Live migration is generally performed when the host physical computer/server needs maintenance, updating and/or to be switched between different hosts.
- To start off, the data in a virtual machine's memory is first transferred to the target physical machine.
- Once the memory copying process is complete, an operational resource state consisting of CPU, memory and storage is created on the destination machine.
- After that, the virtual machine is suspended on the original site and copied and initiated on the destination machine along with its installed applications.
- The whole process has a minimal downtime of seconds in between migration – specifically in copying memory content.
- However, that can be reduced by a few techniques such as pre-paging and the probability density function of memory.

For more info, visit:

- https://www.unixarena.com/2017/12/virtual-machine-live-migration-works.html/
- https://storware.eu/blog/vm-live-migration/

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Points to Remember

1. Understand your specific needs and requirements when selecting a cloud deployment and service model.
2. Prioritize security measures such as data encryption and access controls to protect against unauthorized access.
3. Plan for disaster recovery and high availability to ensure business continuity.
4. Continuously monitor and optimize resource utilization for optimal performance and cost savings.
5. Regularly assess and adapt your cloud architecture to evolving business needs and emerging technologies.

Learning Resources

Text books

1. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi, “Mastering Cloud Computing”, Tata McGraw Hill, ISBN-13: 978-1-25-02995-0
2. Tim Mather, Subra K, Shahid L, Cloud Security and Privacy, OReilly, ISBN-13 978-81-8404-815-5
3. Rajkumar Buyya, James Broberg, Andrzej Goscinski, “Cloud computing Principles and Paradigms”, Wiley Publication.
4. Barrie Sosinsky, “Cloud Computing", Wiley India, ISBN: 978-0-470-90356-8
5. Kailash Jayaswal, “Cloud computing", Black Book, Dreamtech Press
6. Thomas Erl, Zaigham Mahmood and Ricardo Puttini, “Cloud Computing: Concepts, Technology and Architecture”, Pearson, 1st Edition.

Reference Books

1. Introduction to the Theory of Computation, Michael Sipser.
2. Introduction to Languages and the Theory of Computation, John Martin.
3. Computers and Intractability: A Guide to the Theory of NP Completeness, M. R. Garey and D. S. Johnson

Supplementary Reading:

1. Dr. Kumar Saurabh, “Cloud Computing”, Wiley Publication

Learning Resources

Web Resources:

i. https://www.ibm.com/cloud-computing/files/cloud-for-dummies.pdf

Web links

i. https://docs.aws.amazon.com/

ii. https://docs.microsoft.com/en-us/azure/

MOOCs:

i. https://www.coursera.org/learn/gcp-fundamentals
ii. https://nptel.ac.in/courses/106105167/

MIT-WPU

।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

THANK YOU FOR LISTENING ANY QUESTION?