Virtualization

- Introduction
- Virtualization and Cloud Computing
- Pros and Cons of Virtualization
- Technology Examples

- Virtualization technology is one of the fundamental components of cloud computing, especially in case of infrastructure based services.
- It allows creation of secure, customizable and isolated execution environment for running applications, even if they are untrusted, without affecting other users applications.

- At the base of this technology , there is the ability of a computer program- or more in general a combination of software and hardware- to emulate an executing environment separate from the one that host such program.
- E.g: running windows OS on top of virtual machine, which itself is running on Linux OS.

- Virtualization provides s great opportunity to build elastically scalable systems, which are capable of provisioning additional capability with minimum costs.
- Moreover , virtualization technologies not only provide a virtual environment for executing applications, but also for storage, memory, and networking.

- **Virtualization** is the creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources.
- Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations.
- It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

- Virtualization is a technique how to separate a service from the underlying physical delivery of that service.
- It is the process of creating a virtual version of something .
- It involves using specialized software to create a virtual or software-created version of a computing resource.
- With the help of Virtualization multiple operating systems and applications can run on same Machine and its same hardware at the same time increasing the utilization and flexibility of hardware.

- One of the main cost effective, hardware reducing, energy saving techniques used by cloud providers is virtualization.
- Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time.
- virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.

Situations that lead to virtualization

- Virtualization technology have gained renewed interest recently due to the following phenomena:

1. Increased performance and computing capacity.

   Now a days, the average end user desktop PC is powerful enough to fulfil almost all the needs of everyday computing, and there is an extra capacity that is rarely used. Almost all these PCs have resources enough to host a virtual machine manager (VMM)and execute a virtual machine with a by far acceptable performance.

And also super computers can provide an immense compute power that can accommodate the execution of hundreds or thousands of virtual machines.

2. Underutilized hardware and software resources.

Hardware and software underutilization is occurring due to (a). The increased performance and computing capacity and (b). Effect of limited or sporadic use of resources.

computers today are so powerful that in most cases only a fraction of their capacity is used by an application or the system.

e.g: desktop PCs mostly required by administrative staff for office automation tasks are only used during work hours , while overnight they remain completely unused. Using these resources for other purposes after work hours could improve the efficiency of the IT infrastructure. In order to provide such a service , it would be necessary to deploy a completely separate environment, which can be achieved through virtualization.

3. Lack of space.

The continuous need for additional capacity , whether this is storage or compute power, makes data centers grow quickly.

Companies like Google and microsoft expand their infrastructure by building data centers, as large as football fields, that are able to host thousands of nodes. Although this is viable for IT giants , in most cases enterprises cannot afford building another data center to accommodate additional resource capacity. This condition along with hardware under utilization led to the diffusion of a technology called server consolidation.

4. Green initiative.

   Recently , companies are increasingly looking for ways to reduce the amount of energy they consume and reduce their carbon footprint. Data centers are one of the major power consumers. Maintaining a data cente operational does not only involve keeping servers on, but a lot of energy is consumed for keeping them cool. Hence reducing the number of servers through server consolidation will definitely reduce the impact of cooling and power consumption of a data center. Virtualization technology can provide an efficient way of consolidating servers.

5. Rise of administrative costs.

Power consumption and cooling costs have now become higher than the cost of the IT equipment. Moreover the increased demand for additional capacity which translates into more servers in data center, is also responsible for a significant increment in the administrative costs. Computers, in particular servers , do not operate all on their own, but they require care and feeding from system administrators. Their tasks include : hardware monitoring , defective hardware replacement, server setup and updates, server resources monitoring, and backups. These are labour intensive operations. Higher the number of servers higher the administrative costs. Virtualization help in reducing the number of required servers for a given workload, thus reducing the cost of the administrative personnel.

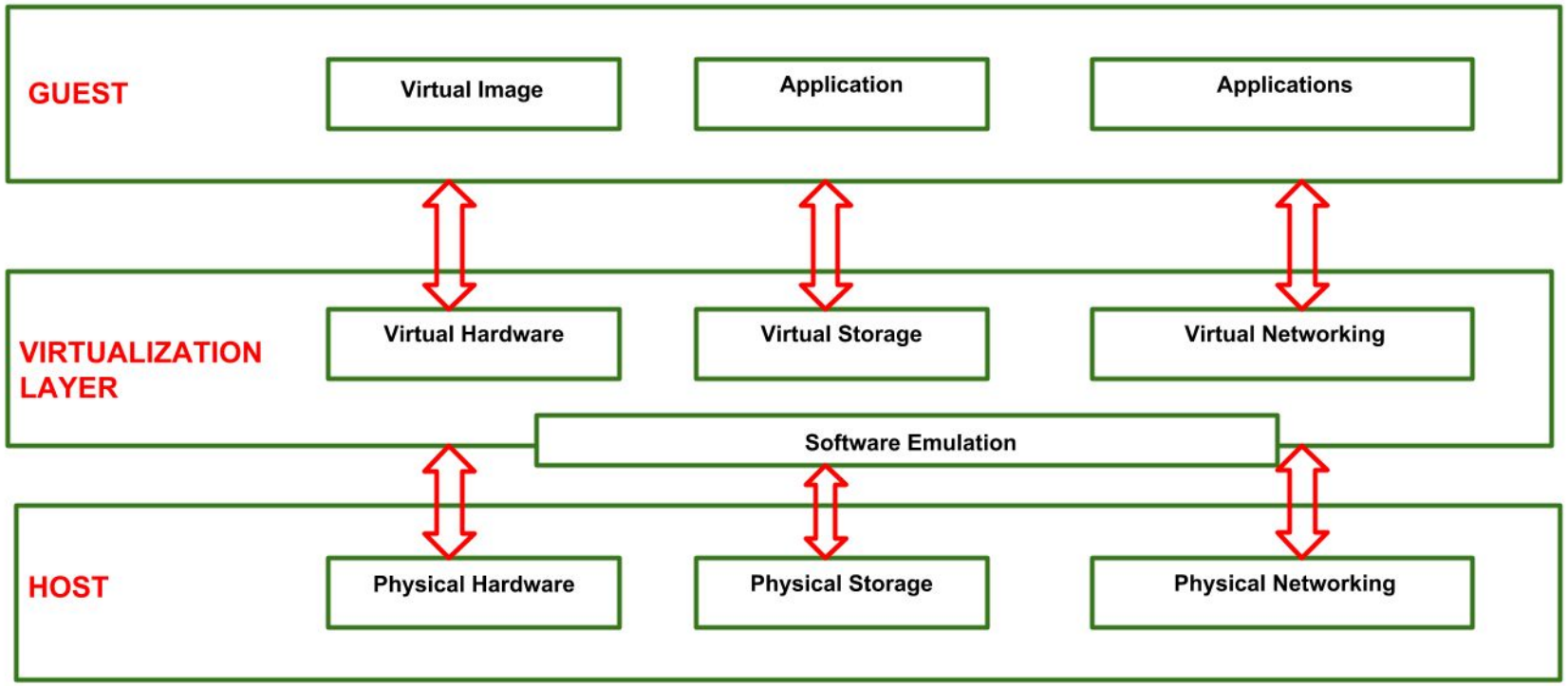
Characteristics of virtualized environments

- Virtualization is a broad concept and it refers to the creation of a virtual version of something, whether this is hardware, software environment , storage, or network.
- In a virtualized environment , there are three major components: gust, host and virtualization layer.

  1. Guest: represents the system component that interact with the virtualization layer .

  2. Host: represents the original environment where the guest is supposed to be managed.

  3. Virtualization layer : is responsible for recreating the same or a different environment where the guest will operate.


GUEST
Virtual Image
Application
Applications
VIRTUALIZATION LAYER
Virtual Hardware
Virtual Storage
Virtual Networking
Software Emulation
HOST
Physical Hardware
Physical Storage
Physical Networking

The advantages that are characterized by virtualized solutions are

1. Increased security
2. Managed execution
   - 2.1.sharing
   - 2.2.Aggreation
   - 2.3.Emulation
   - 2.4.isolation
3. Portability

1. Increased security

- The ability to control the execution of a gust in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment.
- Resources exposed by the host can then be hidden or simply protected from the guest. Moreover , sensitive information that is contained in the host can be naturally hidden without the need of installing complex security policies. Increased security is a requirement when dealing with untrusted code.
- E.g: applets downloaded from the internet run in a sandboxed version of the ‘java virtual machine (JVM)’ , which provides them with limited access to the hosting operating system resources.
- Both the JVM and .NET runtime provide extensive security policies for customizing the execution environment of applications.

- Hardware virtualization solutions such as ‘Vmware Desktop’, ‘VirtualBox’ and ‘Parallels’ provide the ability to create a virtual computer with customized virtual hardware on top of which a new OS can be installed.
- By default the file system exposed by the virtual computer is completely separate from the one of the host machine. This becomes the perfect environment for running applications without affecting other users in the environment.

2. Managed execution.

Virtualization of the execution environment allow increased security and provide a wide range of features :

i. Sharing : virtualization allows the creation of a separate computing environment within the same host. In this way , it is possible to fully exploit the capabilities of a powerful host , which would be otherwise underutilized.

ii. Aggregation: A group of separate hosts can be tied together and represented to gusts as a single virtual host. This function is naturally implemented in middleware for distributed computing .

iii. Emulation : A complete different environment with respect to the host can be emulated, allowing the execution of guests requiring specific characteristics that are not present in the physical host.

This feature becomes very useful for testing purpose where a specific guest has to be validated against different platforms and the wide range of options is not easily accessible during the development.

Again hardware virtualization solutions are able to provide virtual hardware and emulate a particular kind of device such as Small Computer System Interface (SCSI)devices for file IO, without the hosting machine having such hardware installed.

old and legacy software, which does not meet the requirements of current systems, can be run on emulated hardware without any need of changing their code.

An example of emulation is represented by arcade game emulators allowing playing arcade games on a normal personal computer.

iv. Isolation : virtualization allows providing guests- whether they are OS, applications or other entities- with a complete environment , in which they are executed.

The guest performs its activity by interacting with an abstraction layer , which provides access to the underlying resources.

Isolation allows multiple guests to run on the same host without each of them interfering with the other and it provide a separation between the host and the guest.

isolation allows virtual machine managers such as Xen Hypervisor to stop the execution of a gust OS , to move its virtual image into another machine, and to resume its execution in a completely transparent manner. This technique is called virtual machine migration.

3. Portability .

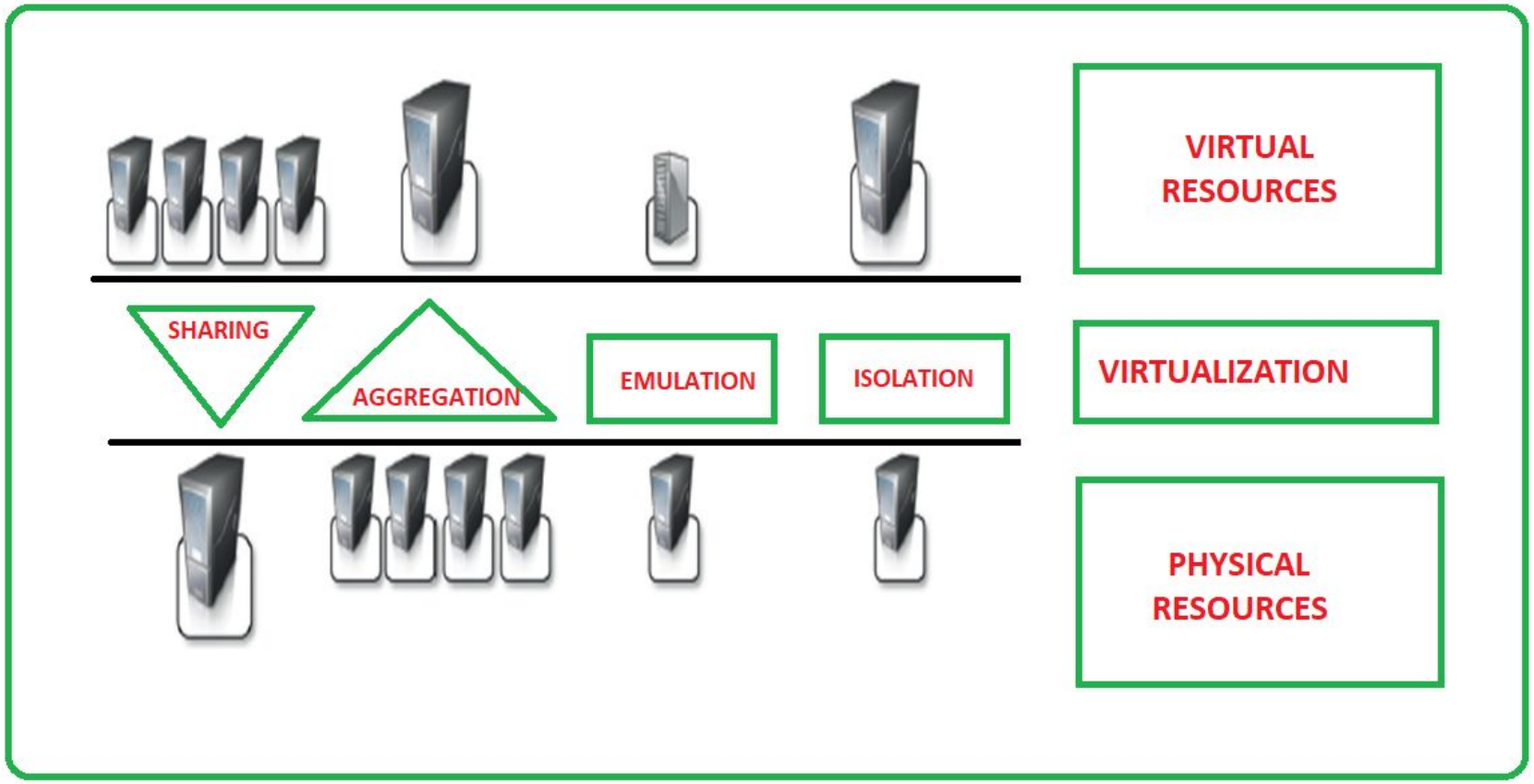
   Portability applies in different ways in different type of virtualization.

   In the case of hardware virtualization the guest is packaged into a virtual image that can be safely moved and executed on top of different virtual machines.

   In case of programming level virtualization the binary code representing application components can be run without any recompilation on any implementation of the corresponding virtual machine.

   Portability allows having our own system always with us and ready to use.

Functions enabled by managed execution



Types of virtualization

1. Hardware level virtualization (system virtualization)
   1.1. Hypervisors
   1.2. Hardware virtualization techniques
      1.2.1. Hardware assisted virtualization
      1.2.2. full virtualization
      1.2.3. para virtualization
      1.2.4. partial virtualization
2. Operating system level virtualization
3. Programming language level virtualization
4. Application level virtualization
5. Storage virtualization
6. Network virtualization
7. Desktop virtualization
8. Application server virtualization

- 1. Hardware level virtualization (system virtualization)

 Hardware –level virtualization is a virtualization technique that provides an abstract execution environment in terms of computer hardware , on top of which a guest O.S can be run.

 The guest is represented by the O.S, the host by the physical computer hardware, the

virtual machine manager by the hypervisor.

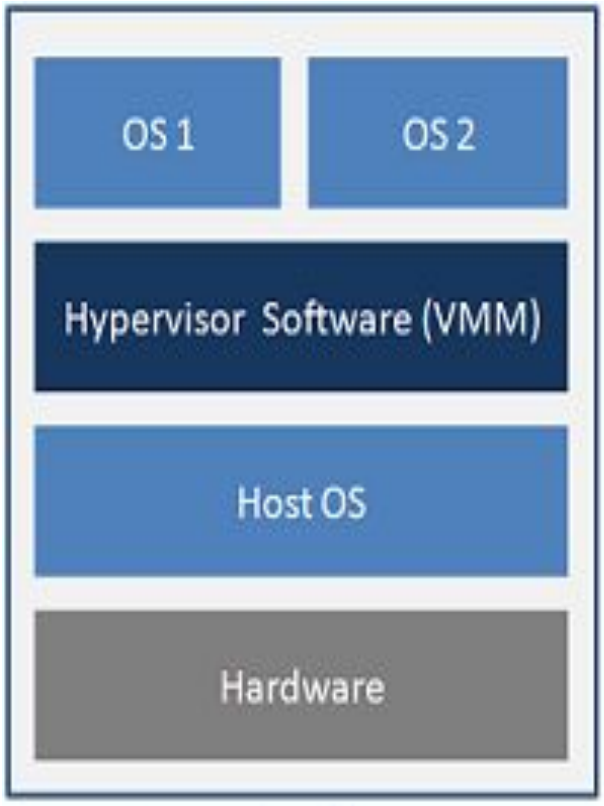
 The hypervisor is generally a program ,or a combination of software and hardware , that allows the abstraction of the underlying physical hardware.

1.1. Hypervisors (virtual machine manager)

- A fundamental element of hardware virtualization.
- It recreates a hardware environment, where gust OS are installed.
- Two types

  1. type 1 (hosted)- hypervisors run directly on top of the hardware.

  2. type 2 (native)- require the support of an OS to provide virtualization.



Hosted Architecture

Bare-Metal Architecture

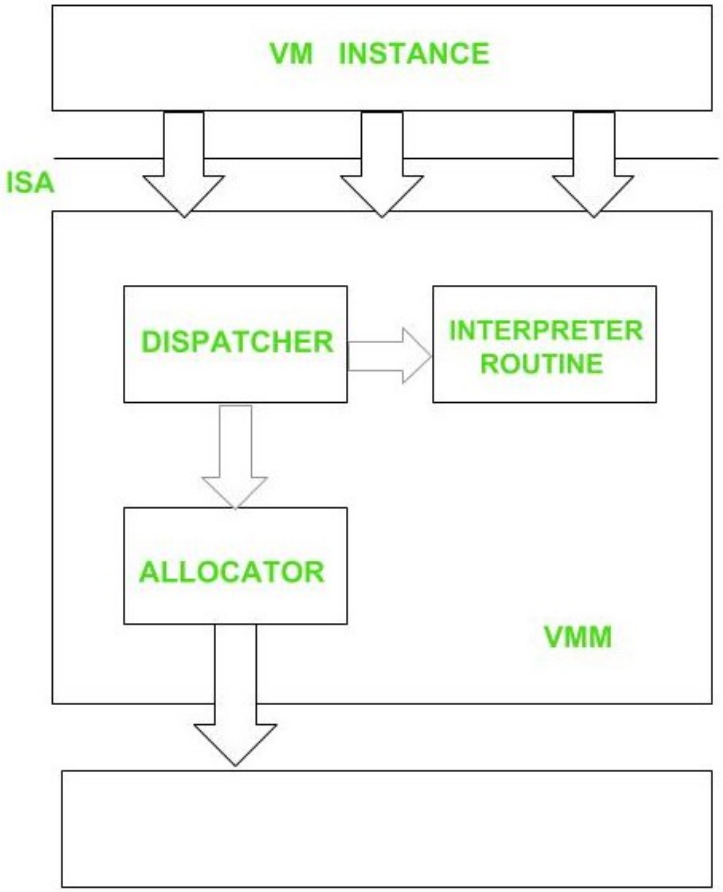
- Type I
- Run directly on top of the hardware
- They take the place of the O.S
- Interact directly with the ISA (instruction set architecture, is the interface between hardware and software) .
- Also called native virtual machine – since it runs natively on hardware.

- Type II
- Require the support of an O.S to provide virtualization services.
- They are programs managed by the O.S , which interact with it through the ABI (application binary interface) and emulate the ISA of virtual hardware for guest O.S.
- Also called hosted virtual machine , since it is hosted within an O.S

- Three main modules coordinate their activity in order to emulate the underlying hardware

1. Dispatcher
2. Allocator
3. Interpreter

Hypervisor reference architecture (VMM internal organization)



- Dispatcher – constitutes the entry point of the monitor and reroutes the instructions issued by the virtual machine instance to one of the two other modules.
- Allocator – is responsible for deciding the system resources to be provided to the VM.
- Interpreter – consists of interpreter routines . These are executed whenever a virtual machine executes a privileged instruction : a trap is triggered and the corresponding routine is executed .

- The criteria that need to be met by a VMM to efficiently support virtualization (or the properties that have to be satisfied) is ..

1. Equivalence : a gust running under a VMM should exhibit the same behaviour as when executed directly on the physical host.
2. Resource control : The VMM should be in complete control of virtualized resources.
3. Efficiency : A statistically dominant fraction of the machine instructions should be executed without intervention from the VMM.

1.2. Hardware virtualization techniques

1.2.1. Hardware-assisted virtualization : this term refers to a scenario in which the hardware provides architectural support for building a VMM able to run a gust OS in complete isolation.

1.2.2. Full virtualization

- Refers to the ability of running a program, most likely an OS , on top of a VM directly and without any modification, as if it were run on the raw hardware.
- In order to make this possible VMMs are required to provide a complete emulation of the entire underlying hardware.
- The advantages are complete isolation ,which leads to enhanced security, ease of emulation of different architectures, and coexistence of different systems on the same platform.

1.2.3. Paravirtualization

- 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 is to provide the capability to demand the execution of performance critical operation directly on the host.

1.2.4.Partial virtualization .

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

2. Operating system level virtualization

- Offers the opportunity to create different and separated execution environments for applications that are managed concurrently.
- The difference from hardware virtualization is there is no VMM or hypervisor, the virtualization is done within a single OS.
- This is an evolution of chroot mechanism in Unix.
- Examples are FreeBSD jails, IBM Logical Partition(LPAR), Free Virtual Private Server(FreeVPS)

3. Programming language level virtualization

- It is mostly used to achieve ease of deployment of application ,managed execution and portability across different platform and OS.
- It consists of a virtual machine executing the byte code of a program
- Example

  java platform – java virtual machine (jvm)

  .Net provides common language infrastructure
- They are stack based virtual machines.

4. Application level Virtualization.

- This technique allows applications to be run on runtime environments, which do not natively support all the features required by such applications.
- this is a good solution in the case of missing libraries in the host OS: in this case a replacement library can be linked with the application , or library calls can be remapped to existing functions available in the host system.
- This technique allows incompatible applications to run together.
- Examples:

  Wine: which is a software application allowing unix like os to execute programs written for the microsoft windows platform

  CrossOver : allows running Windows applications directly on the Mac OS X .

  Vmware ThinApp,

5. Storage Virtualization.

- Storage virtualization is an array of servers that are managed by a virtual storage system.
- The servers aren’t aware of exactly where their data is stored.
- storage virtualization software maintains smooth operations, consistent performance and a continuous suite of advanced functions despite changes, break down and differences in the underlying equipment.

6. Network Virtualization

The ability to run multiple virtual networks that each has a separate control and data plan.

It co-exist together on top of one physical network.

It can be managed by individual parties that potentially confidential to each other.
Network virtualization, provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security.

7.Desktop Virtualization

Desktop virtualization allows the users' OS to be remotely stored on a server in the data center.

It allows the user to access their desktop virtually, from any location by different machine.

Main benefits of desktop virtualization is user mobility, portability, easy management of software installation, updates.

8. Application server virtualization

abstracts a collection of application servers that provide the same services as a single virtual application server by using load balancing strategies and providing a high availability infrastructure for the services hosted in the application server.

Virtualization and cloud computing

- Virtualization plays an important role in cloud computing , it allows for the appropriate degree of customization , security, isolation, and manageability that are fundamental for delivering IT services on demand.
- Hardware and programming language virtualization are the techniques adopted in cloud computing.
- Hardware virtualization is an enabling factor for solutions in IaaS.
- Programming language virtualization leveraged in PaaS.
- Virtualization simplify the leasing of services and their accountability on the vendor side.

- Server consolidation

  it allows reducing the number of active resources by aggregating virtual machines over smaller number of resources that become fully utilized.

  It allows reducing the power consumption of a data center and resolving hardware underutilization.

- Live migration

Live Migration is the process of moving a running virtual machine (VM) from one physical server to another while not disrupting the availability of the virtual machine to users.

It helps better resource utilization by load balancing.

Live migration & server consolidation

Virtualization

- An example of live migration and server consolidation is shown in fig.

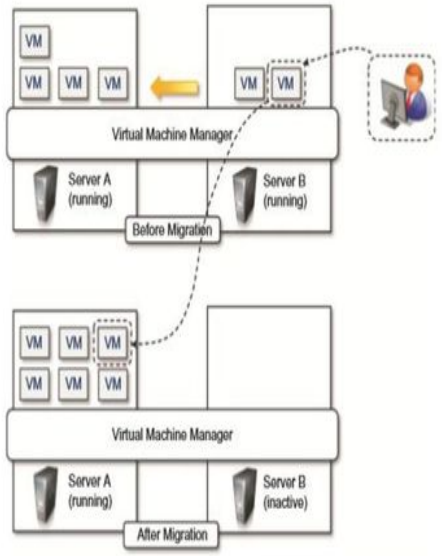


FIGURE 3.10
Live migration and server consolidation.

- ✓ It is important to notice that cloud computing is strongly leveraged for the development of applications that need to scale on demand.
- ✓ This is because applications have to process increased workloads or serve more requests.
- ✓ In this scenario, live migration offers a better solution because it does not create any service interruption during consolidation.

Pros and cons of virtualization

- Advantages:

1. Managed execution and isolation: these characteristics allow building secure and controllable computing environments.

   this enables fine tuning of resources , which is very important in server consolidation scenario.

2. portability: virtual machine instances are normally represented by one or more files that can be easily transported with respect to physical systems. Java programs are “compiled once and run everywhere” –they only require the java virtual machine to be installed on the host.
3. self-containment : contribute to reduce the costs for maintenance , since the number of hosts is expected to be lower than the number of virtual machine instances.
4. Efficient use of resources: multiple systems can securely coexist and share the resources of the underlying host, without interfering with each other. Thus save energy consumption and have less impact on the environment.

- Disadvantages:

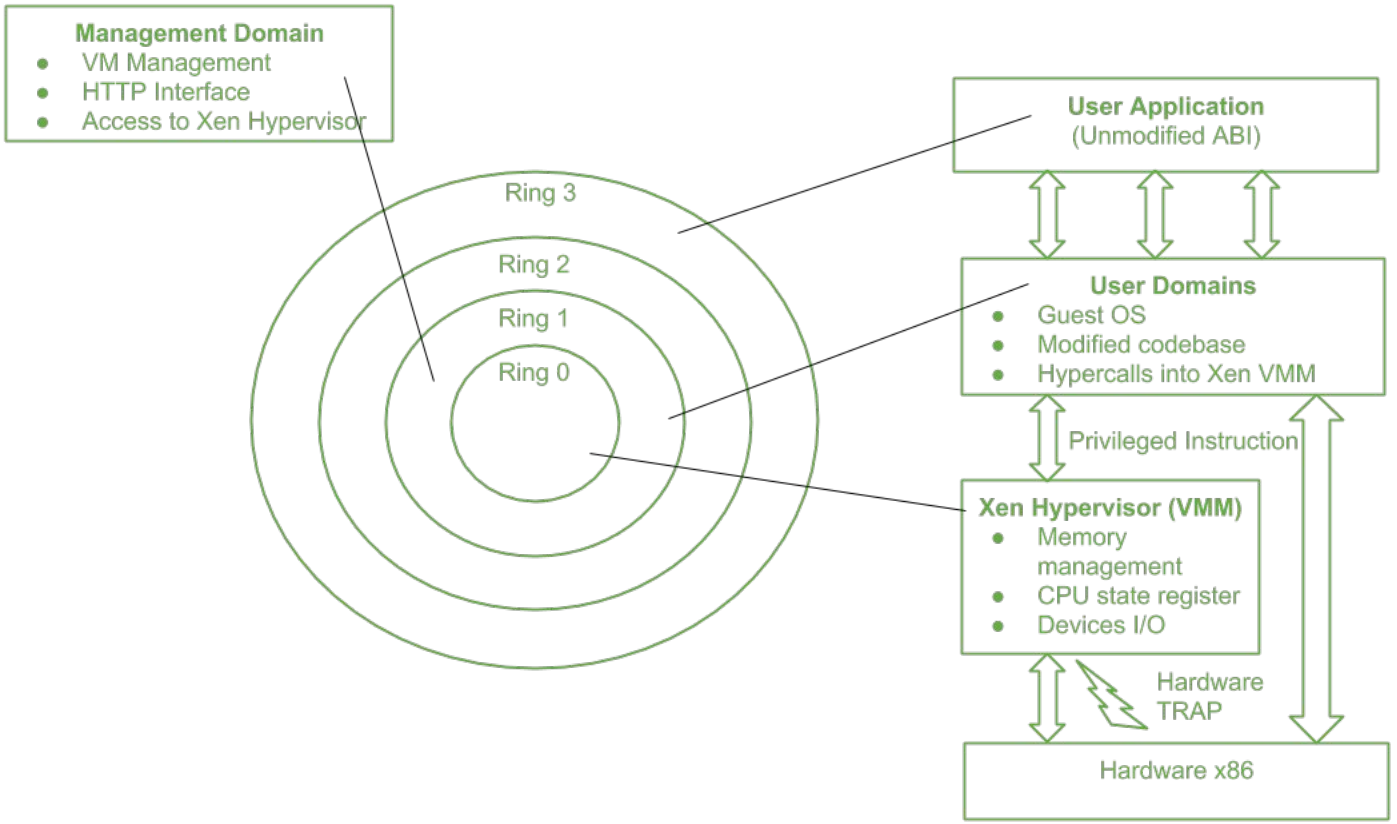
1. Performance degradation: performance is definitely one of the major concerns when using the virtualization technology. Since virtualization interposes an abstraction layer between the gust and the host, increased latencies and delays can be experienced by the guest.
2. Inefficiency and degraded user experience: virtualization can sometimes lead to an inefficient use of the host. Some of the specific features of the host cannot be exposed by the abstraction layer and they become inaccessible.
3. Security holes and new threats: virtualization opens the door to a new and unexpected form of phishing. The capability of emulating a host in a complete transparent manner, has led the way to malicious programs which are designed to extract sensitive information from the guest.

Technology examples

1. Xen : para virtualization

- is a type-1 hypervisor
- **Xen** was developed by XenSource, which was purchased by **Citrix** Systems in 2007.
- It is an open source **hypervisor**.

Xen architecture



2.VMware: full virtualization.

3. Microsoft Hyper-V

- Infrastructure virtualization solution
- Developed by Microsoft
- For server virtualization
- Type 1 hypervisor