MET's Institute of Engineering

Bhujbal Knowledge City, Adgaon, Nashik.

Computer Engineering

"Virtualization in Cloud Computing"

Prepared By

Prof. Anand N. Gharu

(Assistant Professor)

Computer Engineering Departement

CLASS : TE COMPUTER 2019
SUBJECT : CC (SEM-II)
UNIT : III

25 May 2022

SYLLABUS

Introduction: Definition of Virtualization, Adopting Virtualization, Types of Virtualization, Virtualization Architecture and Software, Virtual Clustering, Virtualization Application, Pitfalls of Virtualization. **Grid, Cloud and Virtualization**: Virtualization in Grid, Virtualization in Cloud, Virtualization and Cloud Security. **Virtualization and Cloud Computing**: Anatomy of Cloud Infrastructure, Virtual infrastructures, CPU Virtualization, Network and Storage Virtualization

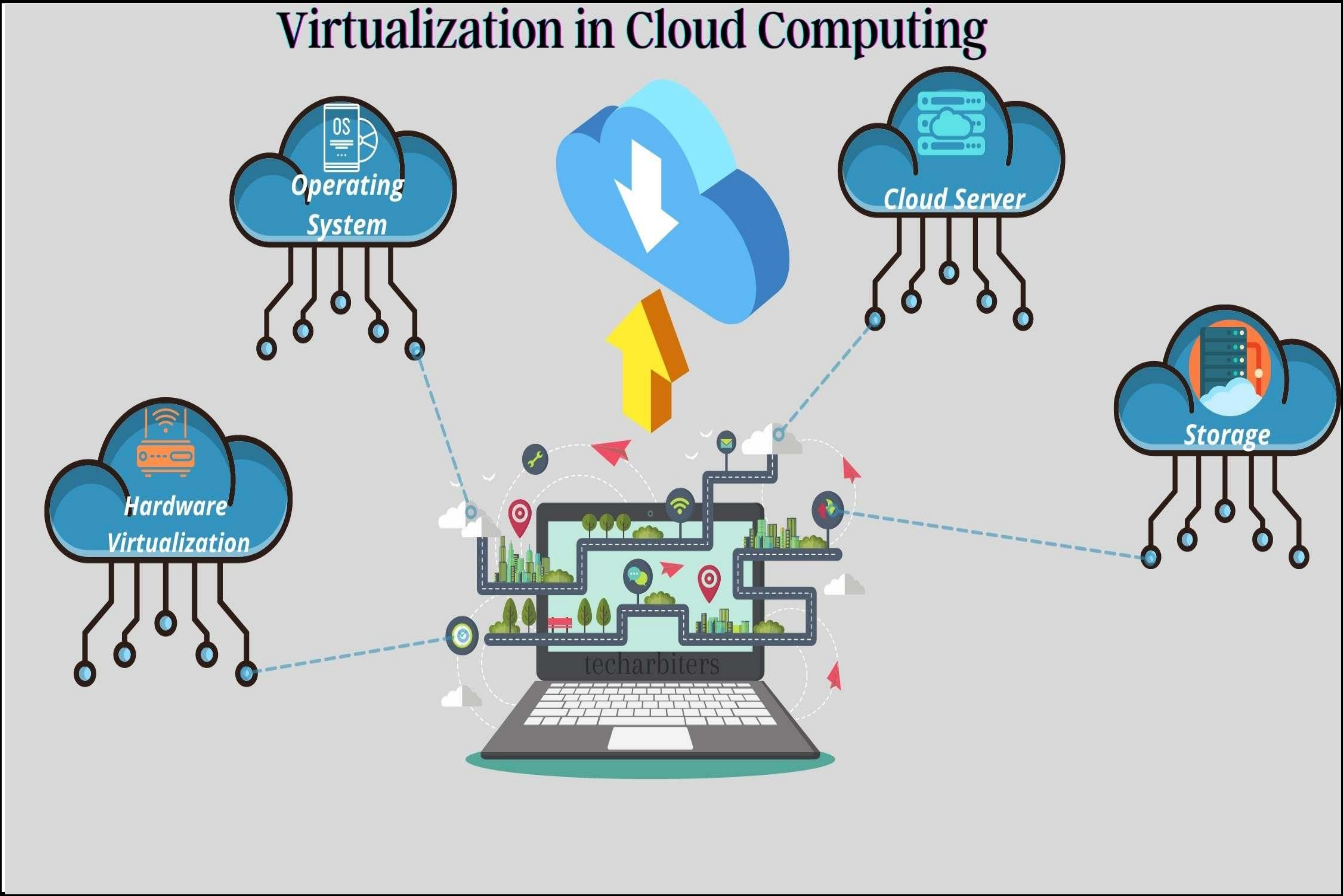
Introduction

Virtualization in Cloud Computing

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

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

Virtualization in Cloud Computing



Basic Terminologies for Virtualization

Virtual machine: A virtual machine can be defined as the computer of a virtual type that operates beneath a hypervisor.

Hypervisor: This can be defined as the operating system that runs on actual hardware. A virtual counterpart of the operating system is a subpart that executes or emulates the virtual process. They are defined as Domain 0 or Dom0.

Basic Terminologies for Virtualization

Container: These can be defined as virtual machines of lightweight nature that are a subset of the same operating system instance or the hypervisor. They are a collection of processes that executes along with corresponding namespace or identifiers of process.

Virtual network: This is defined as the network being separated logically and is present inside the servers. Such networks can be expanded across multiple servers.

Virtualization software: This type of software helps deploy Virtualization on the computer device.

Virtualization in Cloud Computing

What is the concept behind the Virtualization?

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as Host Machine and that virtual machine is referred as a Guest Machine

Benefit of Virtualization in Cloud Computing

1. More flexible and efficient allocation of resources.

2. Enhance development productivity.

3. It lowers the cost of IT infrastructure.

4. Remote access and rapid scalability.

5. High availability and disaster recovery.

6. Pay peruse of the IT infrastructure on demand.

7. Enables running multiple operating systems

Drawback of Virtualization in Cloud Computing

1. The transition of the existing hardware setup to a virtualized setup requires an extensive time investment, and hence this can be regarded as a time-intensive process.
2. There is a lack of availability of skilled resources that helps in terms of transition of existing or actual setup to virtual setup.
3. Since there is a limitation in terms of having less skilled resources, the implementation of Virtualization calls for high-cost implementations.
4. If the transition process is not handled meticulously, it also poses a security risk to sensitive data.

Types of Virtualization

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

1) Hardware Virtualization:

When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization.
The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.
After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:
Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server

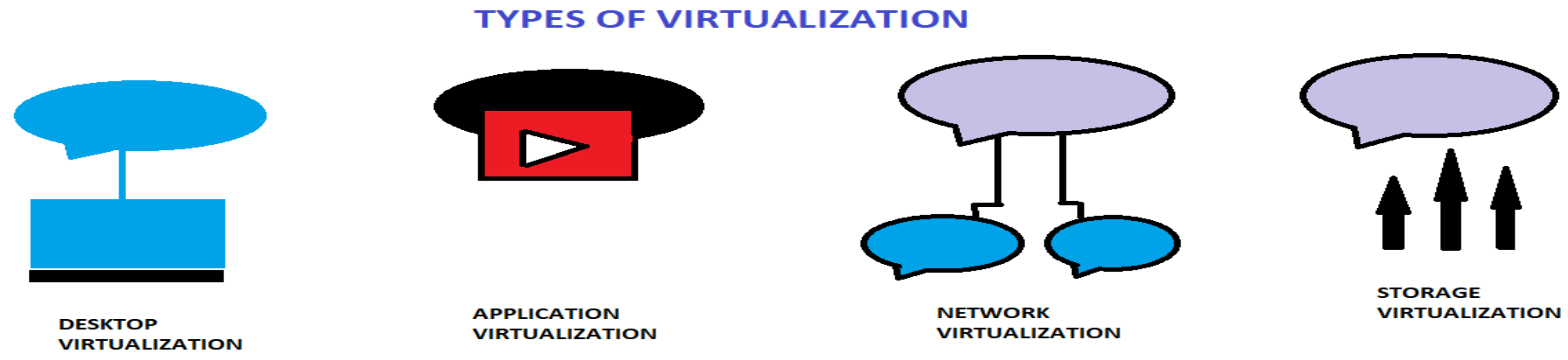
Types of Virtualization

2) Operating System Virtualization:

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

Usage:

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



Types of Virtualization

3) Server Virtualization:

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

Usage:

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

Types of Virtualization

4) Storage Virtualization:

Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device.

Storage virtualization is also implemented by using software applications**.**

Usage:

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

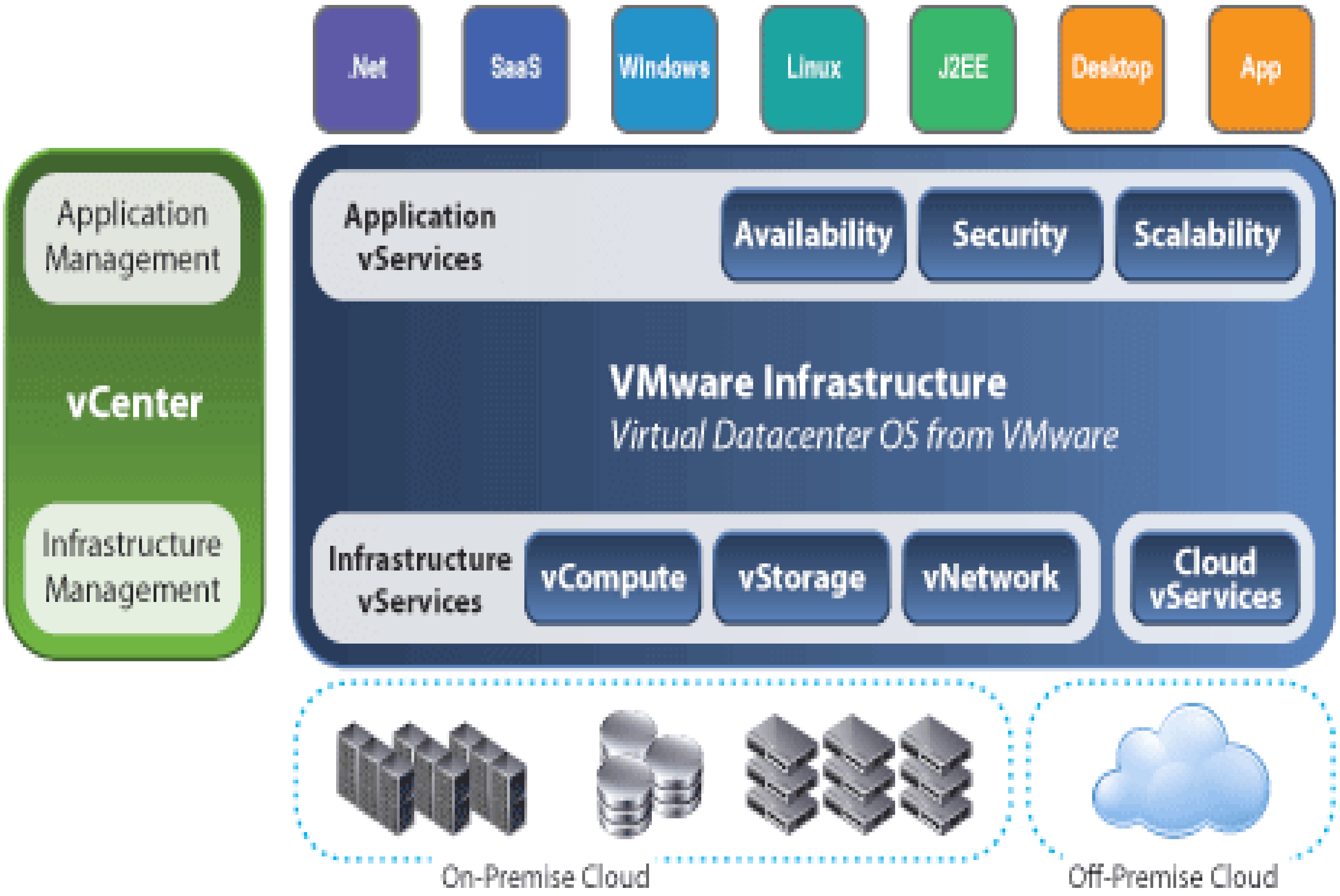
How does virtualization work in cloud computing?

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

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

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

Virtualization Architecture and Software

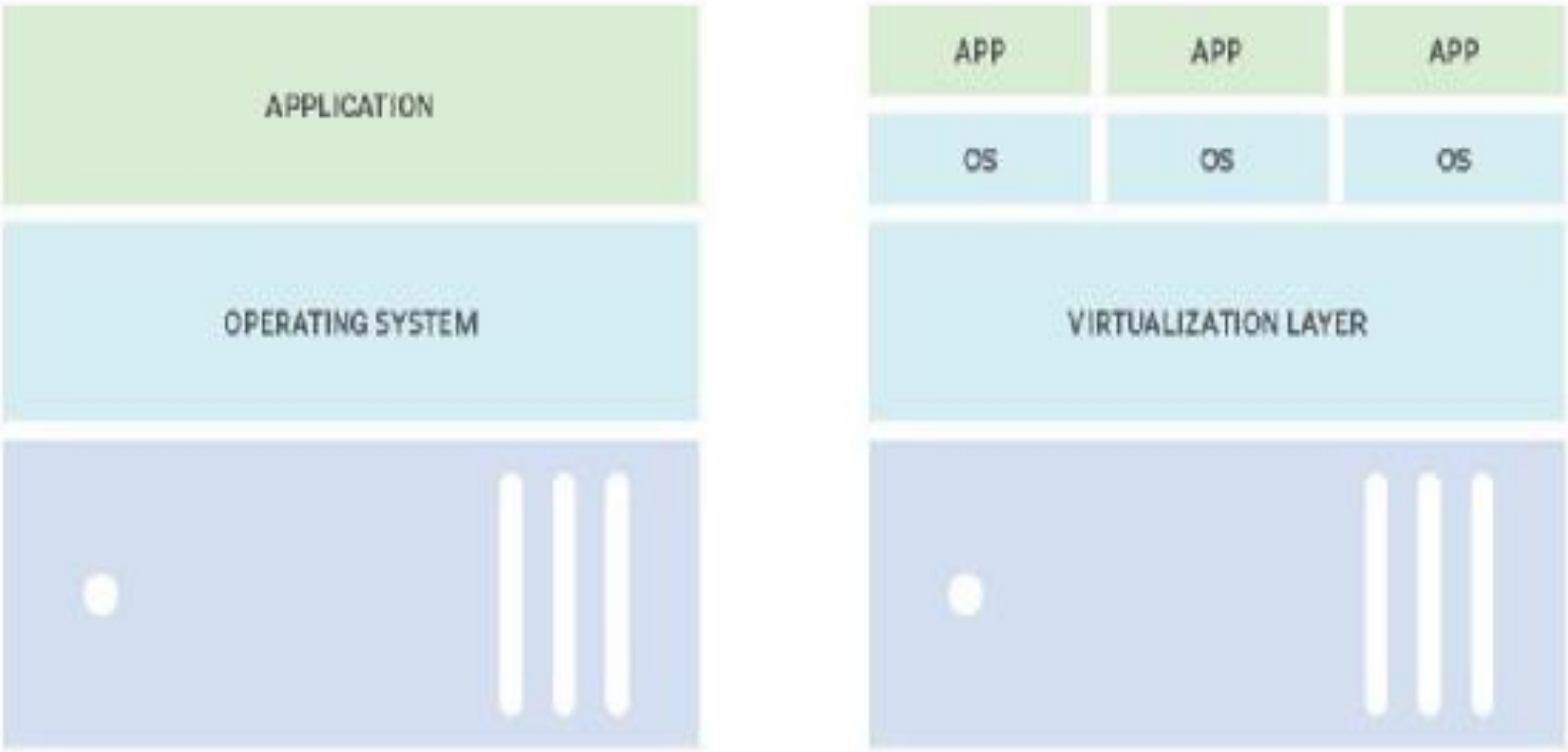


Virtualization Architecture and Software

A virtualization architecture is a conceptual model specifying the arrangement and interrelationships of the particular components involved in delivering a virtual -- rather than physical -- version of something, such as an operating system (OS), a server, a storage device or network resources.

Virtualization Architecture and Software

Traditional and virtual architecture



APPLICATION

OPERATING SYSTEM

APP

APP

APP

OS

OS

OS

VIRTUALIZATION LAYER

Traditional architecture

Virtual architecture

Virtualization Architecture and Software

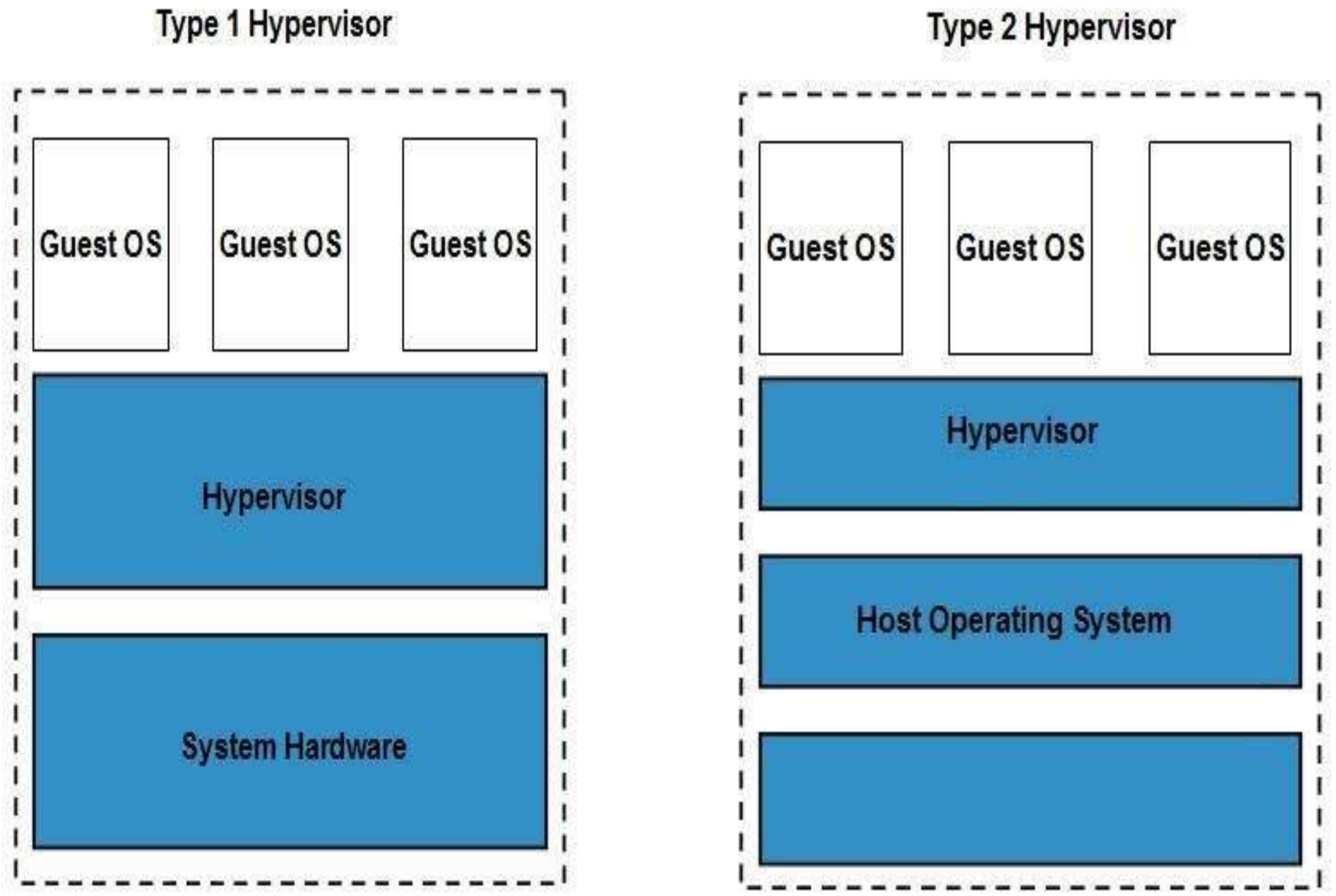
Virtualization is commonly hypervisor-based. The hypervisor isolates operating systems and applications from the underlying computer hardware so the host machine can run multiple virtual machines (VM) as guests that share the system's physical compute resources, such as processor cycles, memory space, network bandwidth and so on.

Type 1 hypervisors, sometimes called bare-metal hypervisors, run directly on top of the host system hardware. Bare-metal hypervisors offer high availability and resource management. Their direct access to system hardware enables better performance, scalability and stability. Examples of type 1 hypervisors include Microsoft Hyper-V, Citrix XenServer and VMware ESXi.

Virtualization Architecture and Software

A type 2 hypervisor, also known as a hosted hypervisor, is installed on top of the host operating system, rather than sitting directly on top of the hardware as the type 1 hypervisor does. Each guest OS or VM runs above the hypervisor. The convenience of a known host OS can ease system configuration and management tasks. However, the addition of a host OS layer can potentially limit performance and expose possible OS security flaws. Examples of type 2 hypervisors include VMware Workstation, Virtual PC and Oracle VM VirtualBox.

Virtualization Architecture and Software



Virtualization Architecture and Software

The main alternative to hypervisor-based virtualization is containerization. Operating system virtualization, for example, is a container-based kernel virtualization method. OS virtualization is similar to partitioning. In this architecture, an operating system is adapted so it functions as multiple, discrete systems, making it possible to deploy and run distributed applications without launching an entire VM for each one. Instead, multiple isolated systems, called containers, are run on a single control host and all access a single kernel.

Software Virtualization

Software Virtualization is a technique that allows one computer server to work with more than one virtual system.

The primary function of software Virtualization is to develop virtual Software and make the work easier. It produces a simple virtual machine on which the system can work as regularly.

Software Virtualization: It is precisely the same as the virtualization bit. It is capable of abstracting the software installation procedure and building virtual software installations.

Virtualized Software: Basically, it is a program installed inside its self-contained unit.

Software Virtualization

The concept behind Software Virtualization

Software Virtualization will build a virtual environment and allows the user to use more than one Operating System.

Suppose the user wants to use Windows and Linux at the same time. Virtualization can help build a virtual environment, and it will enable the use of more than one Operating System.

Types of Software Virtualization

1. OS Virtualization

In OS Virtualization, more than the Operating system wants to work individually to complete the task without affecting others. Thus, a particular Operating system can perform its specified job.

2. Application Virtualization

Application Virtualization is the second Virtualization method where users can remotely access their applications on the central server. It helps to run multiple applications at the same time by building a virtual environment.

3. Service Virtualization

Service Virtualization is a technique to simulate the Behaviors of components in the form of combination component-based applications.

Types of Software Virtualization

1. OS Virtualization

In OS Virtualization, more than the Operating system wants to work individually to complete the task without affecting others. Thus, a particular Operating system can perform its specified job.

2. Application Virtualization

Application Virtualization is the second Virtualization method where users can remotely access their applications on the central server. It helps to run multiple applications at the same time by building a virtual environment.

3. Service Virtualization

Service Virtualization is a technique to simulate the Behaviors of components in the form of combination component-based applications.

Benefits of Software Virtualization

1. Time-Saving

Software Virtualization helps organizations to complete the task efficiently, and also it helps to save time.

2. Quick Changes

The user is capable of making quick changes in the Software according to the requirements. According to the demand, the Software can be altered and run.

3. High Security

The Software can be kept secure from any viruses and security attacks as the firewall is available as a bodyguard and prevents from entering the viruses. Thus the resided data remains highly secure. **are minimal.**

Benefits of Software Virtualization

4. Effective Utilization

With the help of Software Virtualization, the available resources are used best by building a virtual environment. It results in making use of multiple operating systems in one computer.

5. Easy Manage

Managing updates is a simple task. The user can update applications at one location and deploy the updated virtual applications to all client systems.

6. Software Migration

In previous scenarios, getting switched from one platform to another was a time-consuming and challenging task, impacting the end-user systems. But with the help of Software Virtualization, the migration process is simplified.

Virtual Cluster in Cloud Computing

Virtual cluster is a many-to-one virtualization technology, which can form a routing system from multiple common devices connected through a switching network, while performing the same as a single logical router to all external appearances.

Virtual clusters are built with VMs installed at distributed servers from one or more physical clus-ters. The VMs in a virtual cluster are interconnected logically by a virtual network across several physical networks. Figure 3.18 illustrates the concepts of virtual clusters and physical clusters. Each virtual cluster is formed with physical machines or a VM hosted by multiple physical clusters. The virtual cluster boundaries are shown as distinct boundaries

Virtual Cluster in Cloud Computing

The provisioning of VMs to a virtual cluster is done dynamically to have the following interest-ing properties:

- The virtual cluster nodes can be either physical or virtual machines. Multiple VMs running with different OSes can be deployed on the same physical node.
- A VM runs with a guest OS, which is often different from the host OS, that manages the resources in the physical machine, where the VM is implemented.
- The purpose of using VMs is to consolidate multiple functionalities on the same server. This will greatly enhance server utilization and application flexibility.
- VMs can be colonized (replicated) in multiple servers for the purpose of promoting distributed parallelism, fault tolerance, and disaster recovery

Virtual Cluster in Cloud Computing

- The size (number of nodes) of a virtual cluster can grow or shrink dynamically, similar to the way an overlay network varies in size in a peer-to-peer (P2P) network.
- The failure of any physical nodes may disable some VMs installed on the failing nodes. But the failure of VMs will not pull down the host system.

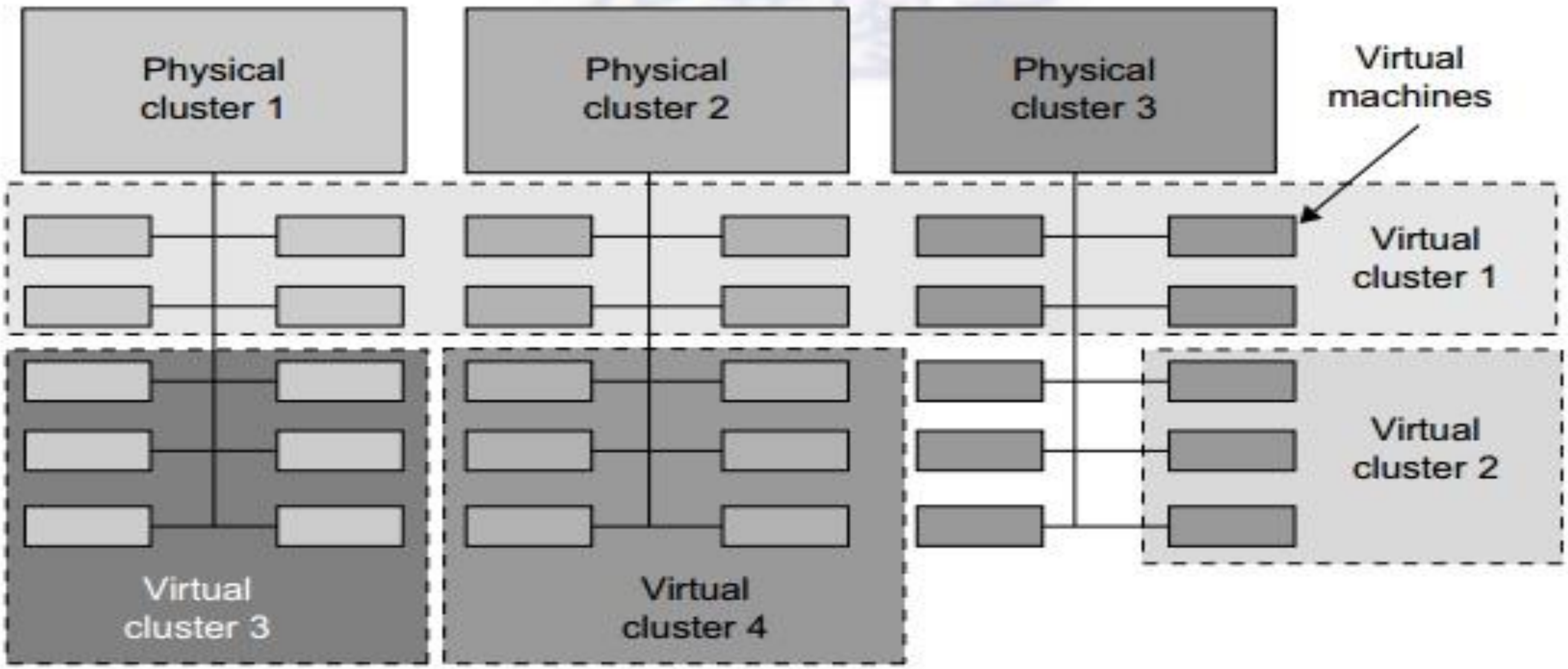


FIGURE 3.18

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

Virtualization Application

Application virtualization is technology that allows users to access and use an application from a separate computer than the one on which the application is installed. Using application virtualization software, IT admins can set up remote applications on a server and deliver the apps to an end user’s computer. For the user, the experience of the virtualized app is the same as using the installed app on a physical machine

Virtualization Application

How does it works?

The most common way to virtualize applications is the server-based approach. This means an IT administrator implements remote applications on a server inside an organization's datacenter or via a hosting service. The IT admin then uses application virtualization software to deliver the applications to a user's desktop or other connected device. The user can then access and use the application as though it were locally installed on their machine, and the user's actions are conveyed back to the server to be executed.

Application virtualization is an important part of digital workspaces and desktop virtualization.

Virtualization Application

Benefits of Application Virtualization :

1. Simplified Management

2. Scalability

3. Security

Pitfalls of Virtualization

1. Capacity and costs fail to meet expectations.
2. Application fails to run (or fails to run adequately) in a virtual environment.
3. Licensing cost increase and some software is not supported.
4. Managers, executives, users and other “server huggers” resist virtualization.
5. Virtualization exposes unforeseen security risks.

Grid, Cloud and Virtualization

Virtualization in Grid

The primary focus in Grid Computing lies in secure resource sharing in terms of access to computers, software and data in a dynamic environment. Sharing of those resources has to be fine grained and highly controlled. Moreover, Foster proposed a three point checklist which characterizes a Grid more in detail:

- Delivery of nontrivial qualities of service;
- Usage of standard, open, general-purpose protocols and interfaces e.g. for inter-communication;
- Coordination of resources that are not subject to centralized control.

Virtualization in Grid

Operating System virtualizations are just a use of software which allows the hardware of a system to run multiple operating systems concurrently. This further provides the benefit to run multiple applications requiring a different operating system on a single computer.

How virtualization is different from Grid Computing?

Whereas a grid has many systems in a network and hence multiple people can have ownership. Virtualization helps in providing cloud better security. Grid computing is more economical. It splits the work and distributes it over the network on computers increasing the efficiency as well

Virtualization in Grid

What is an example of virtualization?

Examples of virtualization in the IT world include: Running multiple Windows VM servers on an Intel box, or running different IBM i, Linux, and AIX partitions on an IBM POWER machine are well known implementations of server virtualization.

Why grid computing is required?

Grid computing enables the virtualization of distributed computing resources suchas processing, network bandwidth,and storage capacity to create a single system image, granting users and applications seamless access to vast IT capabilities.

Virtualization in Cloud

Note : As we have already studied this part in Unit No – 02 as Virtualization in Cloud Computing

Virtualization and Cloud Security

Virtualized security, or security virtualization, refers to security solutions that are software-based and designed to work within a virtualized IT environment. This differs from traditional, hardware-based network security, which is static and runs on devices such as traditional firewalls, routers, and switches.

In contrast to hardware-based security, virtualized security is flexible and dynamic. Instead of being tied to a device, it can be deployed anywhere in the network and is often cloud-based. This is key for virtualized networks, in which operators spin up workloads and applications dynamically; virtualized security allows security services and functions to move around with those dynamically created workloads

Virtualization and Cloud Security

Cloud security considerations (such as isolating multitenant environments in public cloud environments) are also important to virtualized security. The flexibility of virtualized security is helpful for securing hybrid and multi-cloud environments, where data and workloads migrate around a complicated ecosystem involving multiple vendors.

What are the benefits of virtualized security?

1. **Cost-effectiveness:** Virtualized security allows an enterprise to maintain a secure network without a large increase in spending on expensive proprietary hardware. Pricing for cloud-based virtualized security services is often determined by usage, which can mean additional savings for organizations that use resources efficiently.

2. **Flexibility:** Virtualized security functions can follow workloads anywhere, which is crucial in a virtualized environment. It provides protection across multiple data centers and in multi-cloud and hybrid cloud environments, allowing an organization to take advantage of the full benefits of virtualization while also keeping data secure.

What are the benefits of virtualized security?

3. **Operational efficiency :** Quicker and easier to deploy than hardware-based security, virtualized security doesn’t require IT teams to set up and configure multiple hardware appliances. Instead, they can set up security systems through centralized software, enabling rapid scaling. Using software to run security technology also allows security tasks to be automated, freeing up additional time for IT teams.

4. **Regulatory compliance :** Traditional hardware-based security is static and unable to keep up with the demands of a virtualized network, making virtualized security a necessity for organizations that need to maintain regulatory compliance.

How does virtualized security work?

Virtualized security can take the functions of traditional security hardware appliances (such as firewalls and antivirus protection) and deploy them via software. In addition, virtualized security can also perform additional security functions. These functions are only possible due to the advantages of virtualization, and are designed to address the specific security needs of a virtualized environment.

For example, an enterprise can insert security controls (such as encryption) between the application layer and the underlying infrastructure, or use strategies such as micro-segmentation to reduce the potential attack surface.

Virtualized security can be implemented as an application directly on a bare metal hypervisor (a position it can leverage to provide effective application monitoring) or as a hosted service on a virtual machine. In either case, it can be quickly deployed where it is most effective, unlike physical security, which is tied to a specific device.

How is physical security different from virtualized security?

Traditional physical security is hardware-based, and as a result, it’s inflexible and static. The traditional approach depends on devices deployed at strategic points across a network and is often focused on protecting the network perimeter (as with a traditional firewall). However, the perimeter of a virtualized, cloud-based network is necessarily porous and workloads and applications are dynamically created, increasing the potential attack surface.

Traditional security also relies heavily upon port and protocol filtering, an approach that’s ineffective in a virtualized environment where addresses and ports are assigned dynamically. In such an environment, traditional hardware-based security is not enough; a cloud-based network requires virtualized security that can move around the network along with workloads and applications

What are the different types of virtualized security?

Segmentation, or making specific resources available only to specific applications and users. This typically takes the form of controlling traffic between different network segments or tiers.

Micro-segmentation, or applying specific security policies at the workload level to create granular secure zones and limit an attacker's ability to move through the network. Micro-segmentation divides a data center into segments and allows IT teams to define security controls for each segment individually, bolstering the data center's resistance to attack.

Isolation, or separating independent workloads and applications on the same network. This is particularly important in a multitenant public cloud environment, and can also be used to isolate virtual networks from the underlying physical infrastructure, protecting the infrastructure from attack.

Cloud Security

Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection. They also support regulatory data compliance. Cloud security is employed in cloud environments to protect a company's data from distributed denial of service (DDoS) attacks, malware, hackers, and unauthorized user access or use.

Cloud Security

Planning of security in Cloud Computing :

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

Types of Cloud Computing Security

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls :** Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls :** Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls :** It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls :** In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of Cloud Security

- **Centralized security :** Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- **Reduced costs :** Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration.
- **Reduced Administration :** It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- **Reliability :** These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

Virtualization and Cloud Computing

Anatomy of Cloud Infrastructure

Cloud computing is changing itself to meet the demands of customers in terms of software and hardware. These changes have benefitted developments in web-based applications and facilitated decisions-making in business.

Thomas J. Watson of IBM has said ‘there may be a demand for five in world market for computers.’ IBM designed computers for 20 companies, expecting to get orders only from five companies. Surprisingly, IBM got order for 18 companies for the IBM 701 system. Operations in terms of hardware and data are the main players and they are not cost effective. Cloud’s on-demand infrastructure will make it cheaper and efficient.

Anatomy of Cloud Infrastructure

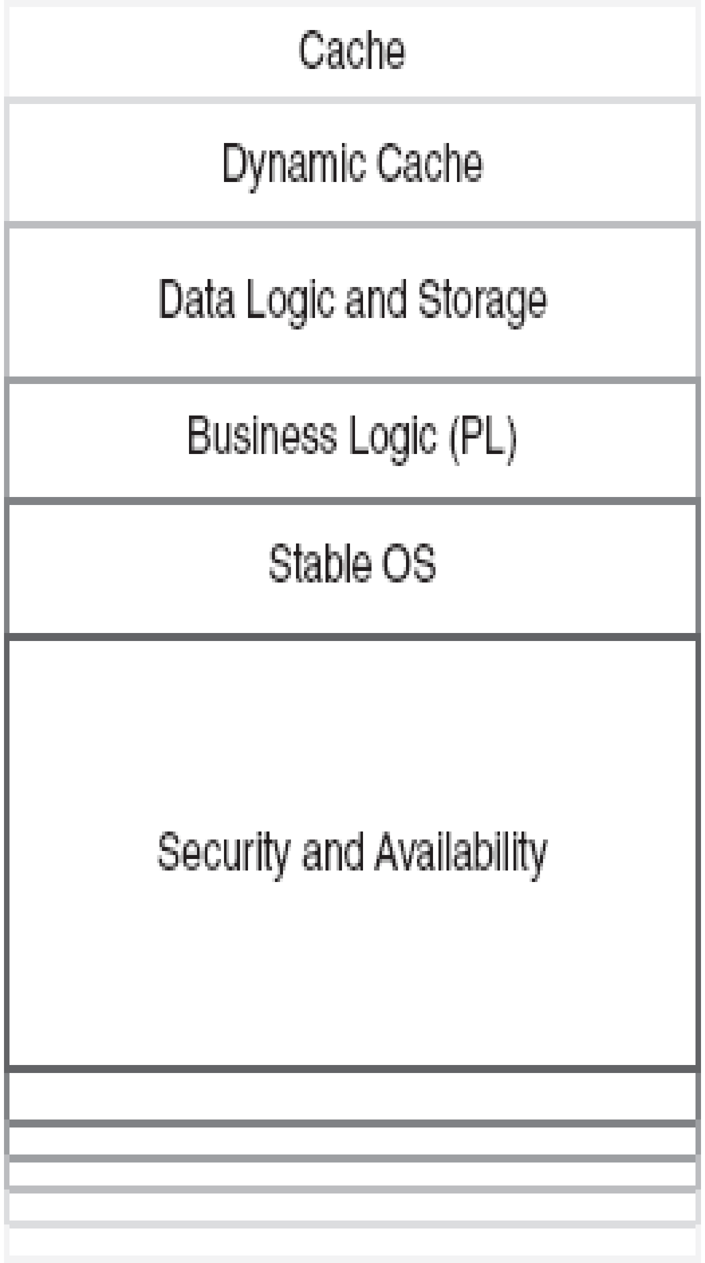
Microsoft and Google are the new players using cloud computing technology. Microsoft’s Windows Azure platform will provide best results for C# and ASP.Net development. Google’s App Engine and its Python language has powered distributed web applications.

The most famous cloud computing provider is Amazon’s EC2. AMI (Amazon Machine Image) is the block used in EC2 virtualization and is the point of interaction to users of Amazon’s EC2.

Anatomy of Cloud Infrastructure

1. Cloud Stack :

Infrastructure stack for delivering web applications by the providers of cloud computing. Figure shows the managed cloud stack consisting of two parts: first part consists of cache, dynamic code and attached storage and logic for the dynamic code; second part consists of stable and efficient OS, security features and business logic written using some programming language. Cloud computing environment separates the computing environment away from the developers and helps them focus on improving their application.



Anatomy of Cloud Infrastructure

1. Cloud Stack :

Every cloud platform includes a virtual machine language and a gateway for web services. Language functions are closely linked with parent OS and their native libraries are taken away. External tools and ordinary compilers will not function in the cloud language layer. Cloud services always bundles language runtime dynamically for efficient interpretation across many application instances.

Dynamic applications resides in application state and logic through database and file storage. In cloud computing, the database and the file server are placed inside cloud services, which are operated in an isolated and specialized layer. This isolation layer makes the storage layer inter-changeable from cloud stack.

Anatomy of Cloud Infrastructure

1. Cloud Stack :

Static files are categorized based on their size. Files <1 MB can be consumed in a single request. File >1 MB need to be chopped into parts for an easier and sequenced download. Static cloud storage can be broken up according to their file size and type, thus providing best solution for storage and delivery.

Anatomy of Cloud Infrastructure

2. Cloud Consumers :

Web Application Developers

New small web applications may experience exponential growth. Web developers use cloud computing stack for faster web performance and their applications. Enterprise applications have deployed different cloud models. SMBs and large-sized IT companies are replacing their in-house maintenance and relying on IaaS. Project management, employee tracking, payroll and some common functions are deployed as SaaS.

Windows Azure, Salesforce’s Force.com and Google App Engine has strong support for back office add-ons. Microsoft and Google support Exchange Online and Google Apps, respectively. Force.com tied to the popular Salesforce CRM application for sales and marketing teams.

Companies such as Aptana, CohesiveFT, RightScale are some examples for cloud hosting providers.

Virtual Infrastructure

In the present scenario, the Internet provides services such as research, mining, e-mail and maps. In the near future, it will converge communication and computation as a single service.

Hence the Internet cannot be considered as a huge shared and unreliable communication enabling data exchanges between users. Instead, it will become a pool of interconnected resources that can be shared.

Grid’5000, an experimental facility, gathers clusters and gives access to nearly 5,000 CPUs distributed over remote sites and inter-connected by super fast networks.

Virtual Infrastructure

Virtualization abstracts services and physical resources. It simplifies the job of managing the resources and offers a great flexibility in resource usage.

The vitrual machine

- Provides an environment where non-trusted applications can be run
- Adopts isolation techniques
- Allows dynamic deployment of application (portability)
- Applied optimization in OS
- Manages as a single service

CPU Virtualization

Virtualizing a CPU is an easy job. For virtualizing a CPU, the following points are to adhered:

- Privileged instructions runs only in privileged mode.
- Control sensitive instructions that tend to change memory mappings, communicating with other devices.
- Behavior-sensitive instructions that tend to change resource configuration.

By adopting CPU virtualization, two separate CPUs resemble a single CPU, i.e., two systems running in a single system. By adopting this concept, user can run two OS in a single system. The most important part of the computer is the central processing unit(CPU).

CPU Virtualization

The main objective of CPU virtualization is to make a CPU function similar to that of two separate CPUs. CPU virtualization allows the users to run different operating systems simultaneously. For example, Apple Mac can be virtualized to run Windows as well.

CPU virtualization is not multitasking or multi-threading. Multitasking is concept of running multiple applications at a time. Multi-threading is where more than one CPUs can run applications in a way that carries out two actions at the same time.

Network and Storage Virtualization

1. Network Virtualization :

Network virtualization facilitates running of multiple networks, multiple consumers over a shared substrate.

Network virtualization is a method which combines the available resources by splitting up the bandwidth into channels and assigned to device or user in real time. Each channel is independently secured. Every consumer will have shared access to all the resources on the network.

By adopting network virtualization, managing the network will be an easier job and less time-consuming for network administrators. Productivity and efficiency are improved using network virtualization. Files, images, programs and folders can be managed centrally.

Network and Storage Virtualization

1. Network Virtualization :

Network virtualization facilitates running of multiple networks, multiple consumers over a shared substrate.

Network virtualization is a method which combines the available resources by splitting up the bandwidth into channels and assigned to device or user in real time. Each channel is independently secured. Every consumer will have shared access to all the resources on the network.

By adopting network virtualization, managing the network will be an easier job and less time-consuming for network administrators. Productivity and efficiency are improved using network virtualization. Files, images, programs and folders can be managed centrally.

Network and Storage Virtualization

1. **Network Virtualization :**

Storage media such as hard drives and tape drives can be added, removed and shared easily. Network virtualization is categorized as: external and internal.

External format: In this format, multiple local networks are combined or subdivided into virtual networks to improve the efficiency. VLAN and network switch are the components of this format.

Internal format: In this format, a single system is configured with containers or hypervisors, such as the Xen/KVM domain to control VNIC. By adopting this format, overall efficiency of a single system is improved since applications are isolated.

Network and Storage Virtualization

1. **Network Virtualization :**

Components of a virtual network consists of:

- Network hardware components such as network switch, adapters (NIC)
- Network elements e.g., firewalls
- VLANs and VMs
- Network storage devices
- Network mobile elements e.g., tablets, mobiles
- Network media e.g., ethernet cards and fibre channels

Network and Storage Virtualization

2. Storage Virtualization

1. Storage virtualization is a concept where storage devices are virtualized. As a result of this concept better functionality, proper maintenance of storage devices and efficient backup procedures can be achieved.

2. A storage system is also called as storage array or disk array. Storage systems are complex and are controlled by special systems providing high data protection for the data stored in it.

3. There are two types of storage virtualization : block virtualization and file virtualization.

Network and Storage Virtualization

2. Storage Virtualization :

- **Block virtualization** separates the logical storage from physical storage. Accessing can be done without the knowledge of where the physical storage is located and its nature (heterogeneous). Storage virtualization allows storage administrators greater flexibility in managing the storage devices and the users.

- **File virtualization** takes care of NAS by eliminating the dependencies between file level and the location. Due to file virtualization, optimization of storage and migrations of storage devices can be done easily.

Network and Storage Virtualization

2. Storage Virtualization :

Benefits of Storage Virtualization

1. **Non-disruptive data migration:** Ability to migrate data without disturbing concurrent I/O access.

2. **Improved utilization:** Utilization can be increased by pooling and migration. When all storage media are pooled, the administrator can easily maintain the devices and also assign disks for the users.

REFERENCES

1. https://www.javatpoint.com/virtualization-in-cloud-computing5

2. https://www.guru99.com/virtualization-cloud-computing.html

3. https://www.techtarget.com/whatis/definition/virtualization-architecture

4. https://www.brainkart.com/article/Virtual-Clusters-and-Resource-Management_11343/

5. https://gzipwtf.com/what-is-virtualization-in-grid-computing/

6. https://www.researchgate.net/publication/226151863_Grids_Clouds_and_Virtualization

7. https://indianjournals.com/ijor.aspx?target=ijor:ijst1&volume=13&issue=4&article=005

8. https://arxiv.org/ftp/arxiv/papers/1807/1807.11016.pdf

9. https://learning.oreilly.com/library/view/cloud-computing/9789332537439/xhtml/chapter010.xhtml#ch10sec4-2

THANK YOU!!!

My Blog : https://anandgharu.wordpress.com/

Email : gharu.anand@gmail.com