CC NOTES:

MOD 1:

VIRTUALIZATION:

* It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era.
* With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.
* Virtualization is the ability that allows sharing the physical instance of a single application or resource among multiple organizations or users.
* It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand
* The machine on which the virtual machine is created is known as host machine
* Virtual machine ->guest machine.
* This virtual machine is managed by a software or firmware, which is known as hypervisor.

**Benefits of Virtualization**

* Virtualization in cloud computing efficiently utilizes hardware resources, reducing costs for both users and service providers. It eliminates the need for physical servers, saving space and reducing hardware costs [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).
* Virtualization improves availability and resilience, allowing for seamless access to information from anywhere and at any time. It also supports live migration of virtual instances between servers, enhancing disaster recovery capabilities [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).
* By reducing the number of physical servers, virtualization lowers energy consumption and associated costs, contributing to a more sustainable IT environment [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).
* Virtualization speeds up the setup process compared to traditional methods, making it more productive and cost-effective [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).
* It simplifies cloud migration for companies with existing server infrastructure, allowing for data and maintenance cost savings

**Drawback of Virtualization**

* **High Initial Investment:**There can be a high initial investment in cloud services, particularly if an organization purchases unnecessary services due to a lack of expertise
* **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
* **Risk of Data:**Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.However, virtualization can pose risks to data security since data is hosted on shared resources, potentially vulnerable to hacking or unauthorized access [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).
* Transitioning to cloud-based virtualization requires skilled personnel or additional training, which can increase costs [**1**](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/).

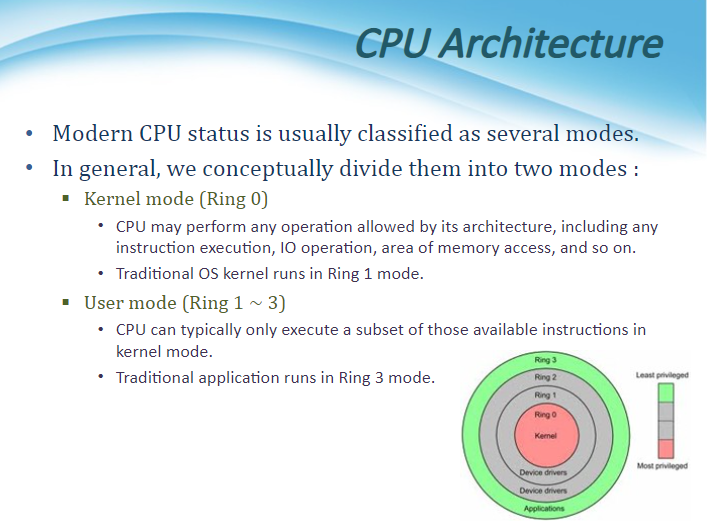
| **Aspect** | **Full Virtualization** | **Paravirtualization** |
| --- | --- | --- |
| Definition | Abstracts entire hardware to create independent VMs | Modifies guest OS to collaborate with hypervisor |
| Hypervisor Requirement | Relies on a hypervisor (e.g., VMware, Hyper-V) | Also requires a hypervisor but with guest OS mods |
| Guest OS Support | Supports unmodified guest OSes (Windows, Linux, etc.) | Requires specially modified guest OSes (e.g., Xen) |
| Isolation | Provides strong isolation between VMs | Provides isolation but may not be as strong |
| Performance Overhead | May incur higher overhead due to emulation | Typically incurs lower overhead due to collaboration |
| Examples | VMware vSphere/ESXi, Hyper-V, KVM | Xen |

Hardware virtualization:

* Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines (VMs).
* It consists of a **hypervisor** which use to control and monitor the process, memory, and other hardware resources.
* After the completion of hardware virtualization process, the user can install the different operating system in it and with this platform different application can use.
* Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.
* Hardware-based virtualization provides good performance as the hypervisor has direct access to the physical hardware, which means that virtual machines can achieve close to native performance.
* Hardware-based virtualization provides strong isolation between virtual machines, which means that any problems in one virtual machine will not affect other virtual machines running on the same physical host.

 CPU Virtualization:

* With CPU Virtualization, all the virtual machines act as physical machine and distribute their hosting resources just like having various processors.
* The virtual machines get a share of the single CPU allocated to it, being a single-processor acting as dual-processor.
* CPU Virtualization adds the amount of overhead based on the workloads and virtualization used. Any application depends mainly on the CPU power waiting for the instructions to get executed first. Such applications require the use of CPU Virtualization that gets the command or executions that are needed to be executed first. This overhead takes the overall processing time and results in an overall degradation in performance and CPU virtualisation execution.



Instructions:

* Unprivileged instructions:
  + without interfering other task, no shared resources,
  + arithmetic instructions
  + Privileged instructions
  + Execute under specific restrictions in a privileged mode and will be trapped if executed outside this mode.
    - Control-sensitive (modify) instructions
      * Attempt to change the configuration of shared resources used. I/O instructions
    - Behavior-sensitive(expose) instructions.
      * Alter the state of CPU registers.

Software based :

1. Application code gets executed:
   * Unprivileged code gets executed directly on the processor.
   * Privileged code gets translated first and that translated code gets executed directly on the processor.
2. This translation is purely known as Binary Translation (BT).
3. The guest programs that are based on unprivileged coding runs very smooth and fast.
4. The code programs or the applications that are based on privileged code components that are significant such as system calls, run at a slower rate in the virtual environment.

**Hardware-Assisted CPU Virtualization**

* There is hardware that gets assistance to support CPU Virtualization from certain processors.
* Here, the guest user uses a different version of code and mode of execution known as a guest mode.
* The guest code mainly runs on guest mode.
* The best part in hardware-assisted CPU Virtualization is that there is no requirement for translation while using it for hardware assistance.
* For this, the system calls runs faster than expected.

Benefits of CPU VIRTUALIZATION:

* Overall performance and efficiency are improved
* Security: The VM machines are also kept separate from each other and because of that any cyber-attack or software glitch unable to create damage to the system, as a single machine cannot affect another machine.
* Cost is very less
* It provides the best backup of computing resources since the data is stored and shared from a single system.
* It also offers great and fast deployment procedure

Storage virtualization:

* A grouping is done of physical storage which is from multiple networked storage devices.
* This is done so it looks like a single storage device.
* It is a sharing of the physical storage from multiple storage devices.

Direct attached storage (DAS):

* Simplest storage model
* laptops, phones, and desktop computers
* Physically impossible to remove the storage from the compute
* But even in the case of servers, where it is theoretically possible to pull disk drives, once a drive is separated from the server, it is generally wiped before reuse.
* Small Computer System Interface (SCSI) is examples of DAS protocols.
* Cloud IaaS compute have attached memory (storage) with processor and separated secondary

Storage area network (SAN):

* Rather than attaching disks to each individual computer, we placed all the disks on a single cluster of servers and accessed the disk over the network.
* Shared storage, since multiple computers will use a single pool of storage.
* client and server over the network using the same (or very similar) **block protocols** that were used to communicate with locally attached disk drives.
* SAN technologies present the storage as block level storage (like Fibre Channel). SAN technologies receive the operating instructions only when if the storage was a locally attached device.

Network Attached storage (NAS):

* Communicate with the storage using file system protocols, which closely resemble the file systems run on local computers.
* The file system abstraction allows multiple servers to access the same data at the same time.
* Multiple servers can read the same file at the same time, and multiple servers can place new files into the file system at the same time.
* Thus, NAS is a very convenient model for shared user or application data.
* Server Message Block (SMB) and Network File system (NFS ) are examples of NAS protocols.

Advantages of Storage Virtualization

1. Data is stored in the more convenient locations away from the specific host. In the case of a host failure, the data is not compromised necessarily.
2. The storage devices can perform advanced functions like replication, reduplication, and disaster recovery functionality.
3. By doing abstraction of the storage level, IT operations become more flexible in how storage is provided, partitioned, and protected.

Server virtualization:

* Server virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application. Each virtual server can run its own operating systems independently.
* Software directly installs on the server system and use for a single physical server can divide into many servers on the demand basis and balance the load.
* With the help of software, the server administrator divides one physical server into multiple servers.
* Virtual servers seek to encapsulate the server software away from the hardware
* This includes the OS, the applications, and the storage for that server.
* A virtual server can be serviced by one or more hosts
* One host may house more than one virtual server
* Virtual servers can be scaled out easily.
* If the administrators find that the resources supporting a virtual server are being taxed too much, they can adjust the amount of resources allocated to that virtual server
* Virtual servers themselves can be migrated from host to host

### **Advantages of Server Virtualization:**

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

### **Disadvantages of Server Virtualization:**

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

MEMORY VIRTUALIZATION:

Memory virtualization is a technique that abstracts, manages, and optimizes physical memory (RAM) used in computer systems. It creates a layer of abstraction between the RAM and the software running on your computer. This layer enables efficient memory allocation to different processes, programs, and virtual machines. Memory Virtualization plays a critical role in cloud computing for several reasons. It contributes to cloud services’ efficiency, scalability, effective resource utilization, and cost-effectiveness.

**Key Elements Involved in Memory Virtualization:**

* Abstraction of Physical Memory: Memory virtualization abstracts the physical memory of various VMs to create a pool of resources that can be allocated as needed. This is achieved using a Virtual Machine Monitor (VMM) that manages VM memory in cloud computing, allowing VMs to request and consume memory without limitations, enabling users to scale memory resources as required [**2**](https://en.wikipedia.org/wiki/Memory_virtualization)[**3**](https://medium.com/geekculture/virtualization-in-cloud-computing-processor-memory-virtualization-part-1-8d1342720e51).
* Resource Pooling: Memory virtualization pools memory resources from the data center to form a shared resource pool, which can be allocated to VMs and cloud users according to their dynamic needs and workloads [**2**](https://en.wikipedia.org/wiki/Memory_virtualization)[**3**](https://medium.com/geekculture/virtualization-in-cloud-computing-processor-memory-virtualization-part-1-8d1342720e51).
* Dynamic Allocation: Memory virtualization allows for instant allocation and reallocation of virtual memory to VMs and cloud users on demand, based on workload fluctuations. This dynamic nature of memory allocation helps to effectively utilize available resources [**2**](https://en.wikipedia.org/wiki/Memory_virtualization)[**3**](https://medium.com/geekculture/virtualization-in-cloud-computing-processor-memory-virtualization-part-1-8d1342720e51).
* Isolation and Data Security: The virtual memory allocated to each cloud user or VM is isolated, ensuring that one user cannot access another's data or memory. This isolation is critical for data security and is a reason why some companies opt for private cloud services to prevent unauthorized access [**2**](https://en.wikipedia.org/wiki/Memory_virtualization)[**3**](https://medium.com/geekculture/virtualization-in-cloud-computing-processor-memory-virtualization-part-1-8d1342720e51)

**Here are some of the key points that show the importance of memory virtualization in cloud computing:**

1. Memory virtualization allows cloud providers to use physical memory resources in the most efficient way. Overcommitting of memory allows the optimization of memory resources and hardware.

2. This virtualization enables the dynamic allocation of cloud memory to cloud user instances. This elasticity is crucial in cloud computing to manage varying workloads. It allows cloud users to scale up and down memory resources as needed and promotes flexibility and cost savings.

3. Allocating separate cloud memory for every single user prevents unauthorized access and is a must for data security.

4. Memory virtualization is vital for handling a large number of users and workloads. It ensures that scaling up or down memory can be done without manual intervention whenever a VM is required.

5. Migration and live migration are important for load balancing, hardware maintenance, and disaster recovery in cloud computing. Transferring VM memory from one host to another is only possible by live migration and feasible when memory is virtualized.

6. By optimizing virtual memory usage, memory virtualization maximizes physical memory utilization and helps reduce the overall operational cost of the cloud.

OS VIRTUALIZATION:

* Operating system-based virtualization involves creating isolated user-space instances using the kernel of an existing operating system, known as the host OS [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Virtualization software is installed on the host OS, allowing users to run and manage virtual machines, with the software providing access to these machines [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* The host OS can cause hardware compatibility issues, even if drivers aren't allocated to the virtualization software [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Virtualization software can convert hardware resources into virtual ones, making use of the host OS's full capabilities [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Hardware capabilities and connected peripherals can be accessed via the host OS, which also manages read-write data operations [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/)[**4**](https://www.tutorialspoint.com/operating-system-based-virtualization).
* Containers in OS-based virtualization offer scalability, security, reduced overhead, and ease of management [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Performance overhead can occur due to the host OS using hardware resources and the necessity of navigating through layers for hardware-related calls [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Security risks exist due to shared host OS, potential lack of complete isolation, complexity in setup, and dependency issues [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Limited hardware access can also be a challenge, restricting the performance of certain tasks or applications [**1**](https://www.geeksforgeeks.org/operating-system-based-virtualization/).
* Resource isolation, lightweight containers, better performance, scalability, and portability are among the benefits of OS-based virtualization [**4**](https://www.tutorialspoint.com/operating-system-based-virtualization).
* Compatibility issues, reliance on host OS security, and complexity are challenges faced by OS-based virtualization [**4**](https://www.tutorialspoint.com/operating-system-based-virtualization).

Some major operating system-based services are mentioned below:

1. Backup and Recovery.
2. Security Management.
3. Integration to Directory Services.

Various major operations of Operating System Based Virtualization are described below:

1. Hardware capabilities can be employed, such as the network connection and CPU.
2. Connected peripherals with which it can interact, such as a webcam, printer, keyboard, or Scanners.
3. Data that can be read or written, such as files, folders, and network shares.

#### Advantages of Operating System-Based Virtualization:

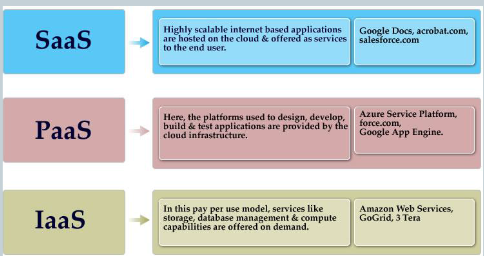
* **Resource Efficiency:**Operating system-based virtualization allows for greater resource efficiency as containers do not need to emulate a complete hardware environment, which reduces resource overhead.
* **High Scalability:** Containers can be quickly and easily scaled up or down depending on the demand, which makes it easy to respond to changes in the workload.**Easy Management:** Containers are easy to manage as they can be managed through simple commands, which makes it easy to deploy and maintain large numbers of containers.  
  **Reduced Costs:** Operating system-based virtualization can significantly reduce costs, as it requires fewer resources and infrastructure than traditional virtual machines.
* **Faster Deployment:** Containers can be deployed quickly, reducing the time required to launch new applications or update existing ones.
* **Portability:**Containers are highly portable, making it easy to move them from one environment to another without requiring changes to the underlying application.

#### Disadvantages of Operating System-Based Virtualization:

* **Security:** Operating system-based virtualization may pose security risks as containers share the same host operating system, which means that a security breach in one container could potentially affect all other containers running on the same system.
* **Limited Isolation:**Containers may not provide complete isolation between applications, which can lead to performance degradation or resource contention.
* **Complexity:** Operating system-based virtualization can be complex to set up and manage, requiring specialized skills and knowledge.
* **Dependency Issues:**Containers may have dependency issues with other containers or the host operating system, which can lead to compatibility issues and hinder deployment.
* **Limited Hardware Access:** Containers may have limited access to hardware resources, which can limit their ability to perform certain tasks or applications that require direct hardware access.

Abstraction:

* Abstraction in cloud computing refers to the process of reducing complex systems to a simplified, more manageable form [**1**](https://www.freecodecamp.org/news/cloud-computing-abstractions-explained/).
* The four primary service models in cloud computing are IaaS (Infrastructure as a Service), PaaS (Platform as a Service), FaaS (Function as a Service), and SaaS (Software as a Service) [**1**](https://www.freecodecamp.org/news/cloud-computing-abstractions-explained/).
* Users choose a cloud abstraction layer based on their business requirements, considering factors like the level of control needed and the available resources and services [**2**](https://www.techtarget.com/searchcloudcomputing/tip/Understand-cloud-abstraction-for-your-IT-needs).
* Containers represent an abstraction that democratized access to software dependencies and enabled running separated applications with different software dependencies [**4**](https://aws.amazon.com/blogs/architecture/compute-abstractions-on-aws-a-visual-story/).
* With containers, there is a control plane for defining, deploying, and managing containers, and a data plane for providing capacity so containers can run and connect to a network [**4**](https://aws.amazon.com/blogs/architecture/compute-abstractions-on-aws-a-visual-story/).
* Service Models are the reference models on which the Cloud Computing is based. These can be categorized into  three basic service models as listed below:
* Software as a Service (SaaS):
  + In this model, a complete application is offered to the customer, as a service on demand.
  + A single instance of the service runs on the cloud & multiple end users are serviced.
  + On the customer’s side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained.
  + Today SaaS is offered by companies such as Google, Salesforce, Zoho, etc.
* Platform as a Service (PaaS):
  + A layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built.
  + The customer has the freedom to build his own applications, which run on the provider’s infrastructure.
  + To meet manageability and scalability requirements of the applications, PaaS  providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE,Ruby etc.
  + Google’s App Engine, Force.com, etc. are some of the popular PaaS examples.
* Infrastructure as a Service (IaaS):
  + Physically, the pool of hardware resource is pulled from a multitude of servers and networks usually distributed across numerous data centers, all of which the cloud provider is responsible for maintaining.
  + IaaS provides a layer of virtualized hardware that delivers the computing power and data centers required for applications to run.
  + Amazon Elastic Cloud Compute (Amazon EC2), Rackspace Cloud Servers, GoGrid, Joyent, and AppNexus



Business benefits of virtualization:

* Virtualization leads to cost savings by reducing the need for physical servers, allowing more virtual servers to be hosted on one physical server, thus saving on power, cooling, and office space [**1**](https://www.mattnj.com/news-events/benefits-of-virtualization-for-business).
* It provides a testing environment for new software and upgrades, which can lead to safer deployments and improved uptime [**1**](https://www.mattnj.com/news-events/benefits-of-virtualization-for-business).
* Business continuity is enhanced because hardware failures decrease, and downtime from such events is reduced, with data and applications easily migrated to virtual servers [**1**](https://www.mattnj.com/news-events/benefits-of-virtualization-for-business).
* Disaster recovery becomes quicker and more reliable due to faster restoration of virtual servers compared to repairing physical environments [**1**](https://www.mattnj.com/news-events/benefits-of-virtualization-for-business).
* Security is heightened as web activities can be contained within virtual servers, preventing malware from spreading across the network, and remote workers can securely access their virtual desktops [**1**](https://www.mattnj.com/news-events/benefits-of-virtualization-for-business).
* Virtualization reduces upfront hardware costs and ongoing operational expenses, resulting in a lower total cost of ownership [**2**](https://www.cdw.com/content/cdw/en/articles/datacenter/what-is-virtualization.html).
* It minimizes or eliminates downtime, increases IT productivity, and simplifies data center management [**2**](https://www.cdw.com/content/cdw/en/articles/datacenter/what-is-virtualization.html).
* It allows for faster provisioning of applications and resources, which is beneficial for business agility [**2**](https://www.cdw.com/content/cdw/en/articles/datacenter/what-is-virtualization.html).
* Virtualization can lead to better return on investment (ROI) and enhanced system security [**3**](https://itmagic.pro/blog/10-benefits-of-virtualization-guide-to-advance-your-business).
* Overall, virtualization contributes to a more sustainable IT environment by reducing energy consumption and helping companies become eco-friendly

HYPERVISERS:

* Virtualization requires the use of a [hypervisor](https://searchservervirtualization.techtarget.com/definition/hypervisor), which was originally called a virtual machine monitor or VMM.
* [A hypervisor abstracts operating systems](https://searchservervirtualization.techtarget.com/tip/Understanding-hosted-and-bare-metal-virtualization-hypervisor-types) and applications from their underlying hardware.
* The physical hardware that a hypervisor runs on is typically referred to as a host machine, whereas the VMs the hypervisor creates and supports are collectively called guest machines.
* A hypervisor enables the host hardware to operate multiple VMs independent of each other and share abstracted resources among those VMs.
* Virtualization with a hypervisor increases a data center's efficiency compared to physical workload hosting.

TYPE 1 HYPERVISERS:

* Type 1 Hypervisors: Also known as bare-metal or native hypervisors, Type 1 hypervisors run directly on the host machine's physical hardware without requiring an underlying operating system [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors)[**5**](https://history-computer.com/type-1-vs-type-2-hypervisors/).
* They offer high performance, stability, and security due to direct access to hardware and no intermediate software layers [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors)[**5**](https://history-computer.com/type-1-vs-type-2-hypervisors/).
* These hypervisors are suitable for production-level workloads requiring high uptime, advanced failover mechanisms, and support for complex workloads [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors).
* They are particularly favored in enterprise settings for their scalability, reliability, and efficiency [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors).
* Type 1 hypervisors are highly secure because each virtual machine (VM) has its own OS, preventing the spread of malware and attacks [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors).
* They often come with support for software-defined storage and networking, adding to security and mobility of virtualized workloads [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors).
* Due to their efficiency and security, Type 1 hypervisors are considered the best-performing hypervisors for enterprise computing [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors).
* They typically require dedicated hardware and may necessitate specialized management tools or interfaces like Microsoft System Center Virtual Machine Manager or VMware vCenter for full functionality [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors)[**4**](https://www.ibm.com/topics/hypervisors).
* Despite their advantages, Type 1 hypervisors may have a higher initial cost and more stringent support contract requirements [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors).

TYPE 2 HYPERVISERS:

* Type 2 hypervisors, also known as hosted hypervisors, run on top of an existing operating system (OS) on the host machine. They rely on the host OS to manage physical resources like CPU, memory, storage, and networks [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors#:~:text=They%20are%20ideal%20for%20personal,more%20layers%20to%20go%20through.)[**2**](https://www.parallels.com/blogs/ras/types-of-hypervisor-in-cloud-computing/).
* They are typically easier to set up and use, making them popular among end users and for personal or small-scale virtualization [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors#:~:text=They%20are%20ideal%20for%20personal,more%20layers%20to%20go%20through.)[**2**](https://www.parallels.com/blogs/ras/types-of-hypervisor-in-cloud-computing/).
* While they are less costly than Type 1 hypervisors, they introduce latency due to the host OS and are less secure because vulnerabilities in the host OS could affect all VMs running on it [**1**](https://www.linkedin.com/advice/0/how-do-you-choose-between-type-1-2-hypervisors#:~:text=They%20are%20ideal%20for%20personal,more%20layers%20to%20go%20through.)[**2**](https://www.parallels.com/blogs/ras/types-of-hypervisor-in-cloud-computing/).
* Due to these reasons, Type 2 hypervisors are less commonly used for data centers and are instead suited for client systems or virtual desktop environments. They are also a good choice for testing platforms and can support complex nested environments

High level language virtual machine:

* HLL VM stands for High Level Language Virtual Machine, and it is a type of virtual machine that is used in cloud computing to run high-level programming languages, such as Java, Python, and Ruby, among others.
* HLL VMs, such as the Java Virtual Machine (JVM), are designed to run high-level programming languages that are compiled into bytecode.
* The HLL VM translates the bytecode into machine language that can be executed by the underlying hardware.
* This provides a layer of abstraction between the high-level programming language and the hardware, which makes it easier to write and deploy applications.
* One of the benefits of using HLL VMs in cloud computing is that they provide a consistent and reliable environment for running applications, regardless of the underlying hardware.
* HLL VMs are also portable, which means that applications can be moved between different cloud providers without the need for significant code changes.
* In summary, HLL VMs are an important technology in cloud computing that enable the running of high-level programming languages in a virtualized environment, providing a layer of abstraction between the application and the underlying hardware, and allowing for portability and scalability of applications.

Emulation

• Emulation is a concept of creating an environment that imitates the properties of one system onto another.

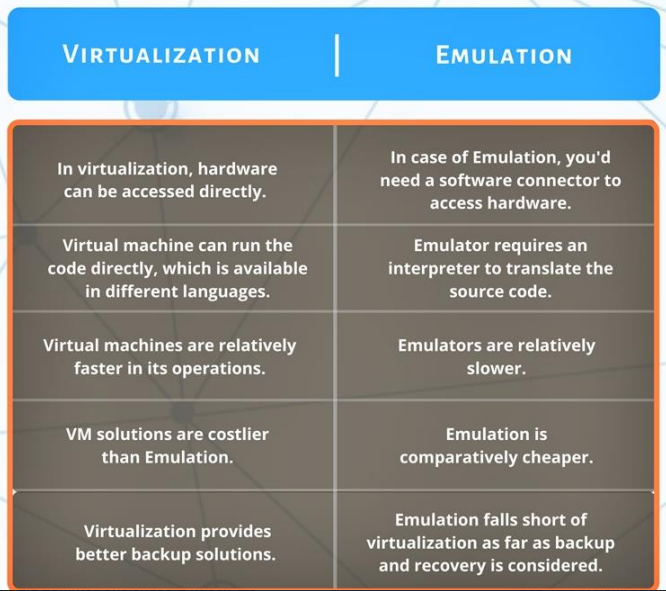
• An Emulator mimics the qualities and logic of one processor to run in another platform efficiently.

• Emulation is an excellent way to run an OS or software in any other system. Guest Operators need a translation.

An emulator converts the needed architecture CPU instructions and successfully runs it on another architecture.

• Anyone can access the emulation platforms remotely and is easier to use. It is an excellent ability to have for embedded/OS development, without affecting the underlying OS.

• Emulation can generally handle the size of the design under test (DUT), without considering the host’s capabilities.



SECURITY THREATS:

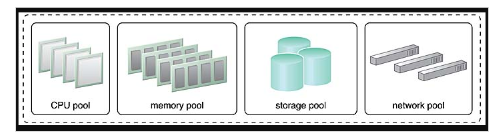
* VM sprawl occurs when an uncontrolled number of VMs are created for specific purposes and then left unmanaged or abandoned, potentially leading to security risks and resource waste [**1**](https://www.solarwinds.com/virtualization-manager/use-cases/vm-sprawl-control)[**3**](https://www.techtarget.com/whatis/definition/virtualization-sprawl-virtual-server-sprawl)[**4**](https://www.nakivo.com/blog/how-to-prevent-vm-sprawl/)[**5**](https://www.redswitches.com/blog/vm-sprawl/).
* Virtual machines are susceptible to malware and ransomware attacks, which can spread across the virtual infrastructure if not properly isolated and secured [**1**](https://www.solarwinds.com/virtualization-manager/use-cases/vm-sprawl-control)[**3**](https://www.techtarget.com/whatis/definition/virtualization-sprawl-virtual-server-sprawl)[**4**](https://www.nakivo.com/blog/how-to-prevent-vm-sprawl/).
* Poor network configuration choices can expose the virtual infrastructure to security risks, and if physical servers are not kept up-to-date, they can become a security threat [**1**](https://www.solarwinds.com/virtualization-manager/use-cases/vm-sprawl-control)[**3**](https://www.techtarget.com/whatis/definition/virtualization-sprawl-virtual-server-sprawl)[**4**](https://www.nakivo.com/blog/how-to-prevent-vm-sprawl/).
* Access controls are crucial to protect against unauthorized access to the virtual infrastructure, and any breach can cause significant damage.
* The hypervisor, which is the foundation for VMs, can be a single point of failure for the entire virtual infrastructure if not secured
* Mismanagement of VMs with differing trust levels can create security risks by placing low-trust servers on the same physical hardware as high-trust servers.

Resource Pooling:

* A resource pool is a group of resources that can be assigned to users. Resources of any kind, including computation, network, and storage, can be pooled.
* It adds an abstraction layer that enables uniform resource use and presentation. In cloud data centers, a sizable pool of physical resources is maintained and made available to consumers as virtual services.
* Any resource from this pool may be given to one user or application only, or it may even be shared by several users or apps.
* Additionally, resources are dynamically provided according to need rather than being permanently allocated to users. As load or demand fluctuates over time, this results in efficient resource usage.

## Resource Pooling Architecture

Developing rich pool of  processor, memory, storage and network



### CPU Pools

These are a collection of processing units that are prepared to be assigned to virtual servers and are often divided into separate processing cores.

* Physical server pools can be used to vertically scale physical servers or to provision new physical servers.
* Each sort of resource can have a specific pool built for it, and smaller pools can be made up of larger ones, in which case each one becomes a sub-pool.
* Multiple pools may be formed for different cloud users or apps, which might lead to extremely complicated resource pools.

### Virtual Server Pools

It is a networked collection of virtual servers that have operating systems and other required software installed and are ready for use right away. Typically, they are set up using one of the many accessible templates that the cloud consumer has selected during provisioning. for instance, a cloud user may create a pool of low-tier Ubuntu servers with 2 GB of RAM or a pool of mid-tier Windows servers with 4 GB of RAM.

### Storage Device Pools

It is a collection of block- or file-based storage structures that house both empty and/or populated cloud storage devices. One of the crucial elements required for enhancing performance, data management, and protection is storage resources. Storage pools, which are accessible to users in virtualized mode, are made up of file-based, block-based, or object-based storage made up of storage devices like discs or tapes.

### Network Pools (Interconnect Pools)

It is a collection of several preset network connectivity devices, such as a virtual firewall device pool or physical network switches, that can be used for load balancing, redundancy connectivity, etc. Through network infrastructure, resources in pools can be linked to one another or to resources in other pools. Switches, routers, gateways, and other networking hardware make up network pools. These physical networking devices are then used to build virtual networks that are provided to clients. These virtual networks can be used by customers to further develop their own networks.

Resource Sharing

* To increase the Utilization rate resources run on pools of resources
* Avg. utilization can be increased by sharing them among applications, users and servers
* All application do not use their peak demand
* Implementation need Architectural support
* Resources are shared among several VMs

Here are some key aspects of resource sharing in cloud computing:

* On-Demand Self-Service: Users can provision computing resources as needed without requiring human interaction with each service request.
* Broad Network Access: Resources are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
* Resource Pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
* Rapid Elasticity (offered by some providers): Capabilities like automatic scaling, allowing elasticity and availability optimization.
* Measured Service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service components.

Resource Provisioning:

Resource provisioning in cloud computing refers to the process of allocating and configuring computing resources such as virtual machines (VMs), storage, and networking infrastructure to meet the demands of applications or services running in the cloud environment. The goal of resource provisioning is to ensure that the necessary resources are available to support the workload efficiently, while also optimizing resource utilization and minimizing costs.

Autonomic resource provisioning:

Autonomic resource provisioning is a self-managing approach in cloud computing where the system dynamically adjusts resource allocation based on changing workload demands, without requiring manual intervention thereby improving agility, scalability, reliability, and cost-effectiveness. By automating resource management tasks, organizations can focus on higher-level objectives such as innovation, business growth, and delivering value to customers, rather than routine maintenance and administration.

Static approach:

A static approach in resource provisioning involves allocating a fixed set of resources to applications or services based on predetermined requirements and assumptions. Unlike dynamic provisioning, which adjusts resource allocation in response to changing workload demands, the static approach does not modify resource allocations once they are provisioned, regardless of variations in workload or system conditions.

Dynamic approach:

A dynamic approach to resource provisioning in cloud computing involves the allocation and management of resources based on real-time demand and workload characteristics. Unlike static provisioning, where resources are allocated based on predetermined requirements and remain fixed, dynamic provisioning adjusts resource allocation dynamically in response to changes in workload, performance metrics, and other factors.The dynamic approach to resource provisioning offers greater agility, scalability, efficiency, and cost-effectiveness compared to static provisioning methods.

Hybrid approach:

The hybrid approach to resource provisioning offers a flexible and adaptive solution that combines the predictability of static provisioning with the agility of dynamic scaling. By leveraging a mix of static and dynamic allocation methods, along with predictive analytics and policy-based management, organizations can achieve optimal resource utilization, performance, and cost efficiency in heterogeneous cloud environments.

1. **Underprovisioning**:

Underprovisioning occurs when the allocated resources (such as CPU, memory, storage, or network bandwidth) are insufficient to meet the demands of the workload or application. This can lead to various performance issues, including slow response times, degraded user experience, and service disruptions. Underprovisioning can occur due to inaccurate capacity planning, underestimation of workload demands, or unexpected spikes in usage.

**Effects of Underprovisioning**:

* + Decreased performance: Insufficient resources can lead to performance bottlenecks and slower response times for applications.
  + Service disruptions: Underprovisioning may result in service outages or downtime, affecting availability and reliability.
  + Poor user experience: Sluggish performance and frequent errors can degrade the user experience and impact customer satisfaction.
  + Increased operational costs: Addressing performance issues and mitigating service disruptions may require additional resources and incur extra costs.

1. **Overprovisioning**:

Overprovisioning occurs when more resources are allocated than actually needed to support the workload. While overprovisioning ensures ample capacity to handle peak loads and unexpected spikes in demand, it can lead to inefficient resource utilization and unnecessary costs. Overprovisioning often results from overly conservative capacity planning, fear of performance degradation, or lack of visibility into workload patterns.

**Effects of Overprovisioning**:

* + Wasted resources: Excessively provisioned resources remain idle during periods of low demand, leading to wasted capacity and increased costs.
  + Higher expenses: Overprovisioning results in higher infrastructure costs due to the unnecessary allocation of resources.
  + Reduced ROI: Inefficient resource utilization reduces the return on investment (ROI) from cloud infrastructure and can hinder cost optimization efforts.
  + Environmental impact: Overprovisioning contributes to higher energy consumption and carbon footprint, impacting sustainability goals.