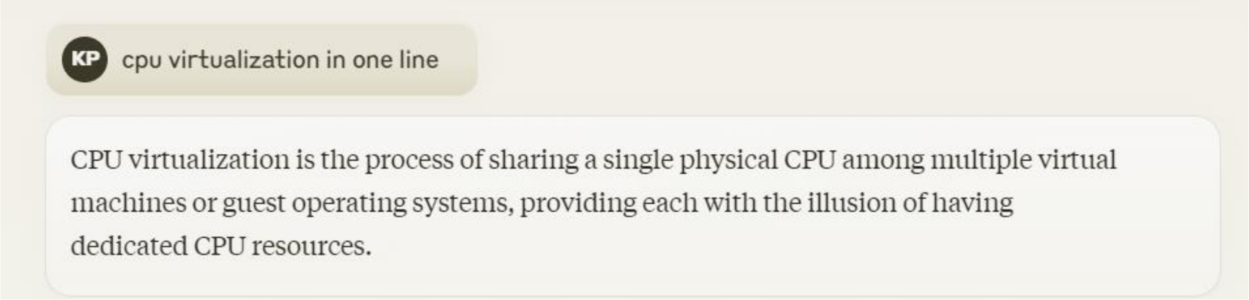
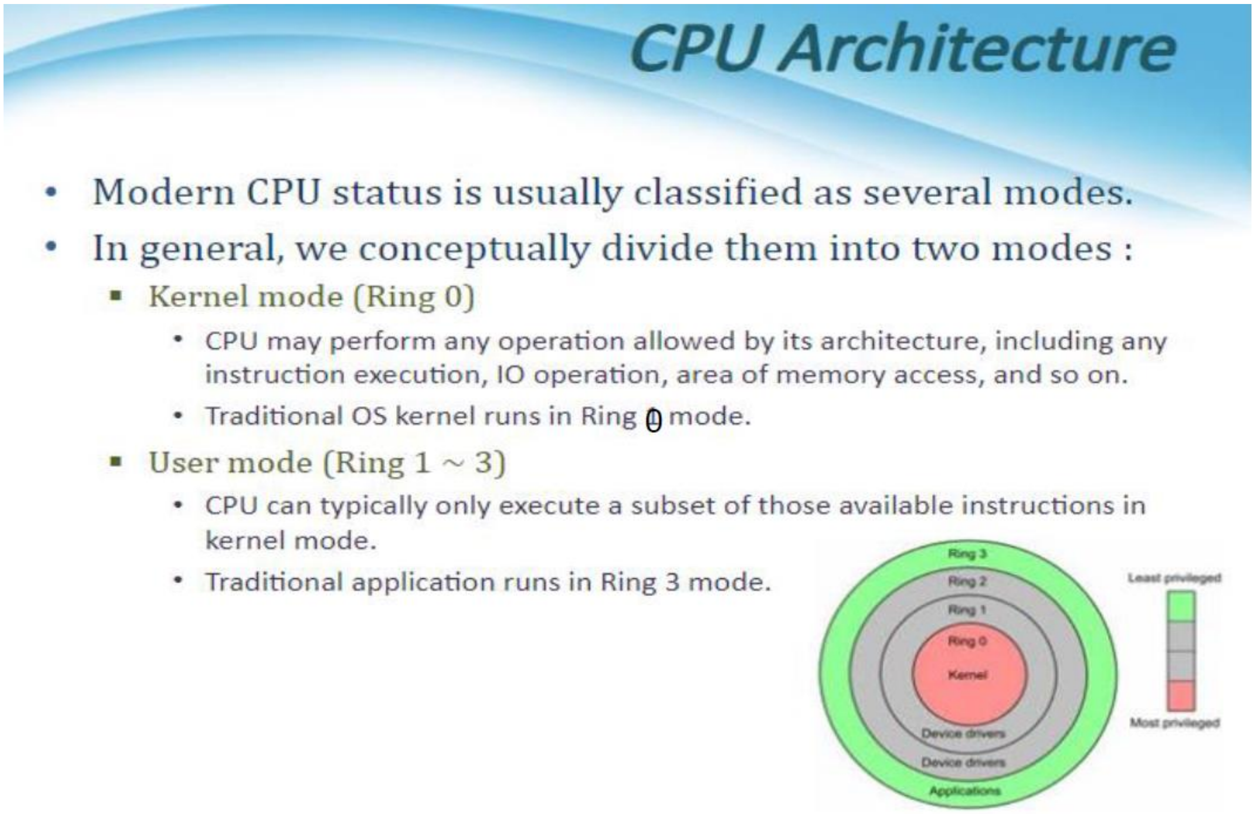
Mod-1



KP cpu virtualization in one line

CPU virtualization is the process of sharing a single physical CPU among multiple virtual machines or guest operating systems, providing each with the illusion of having dedicated CPU resources.

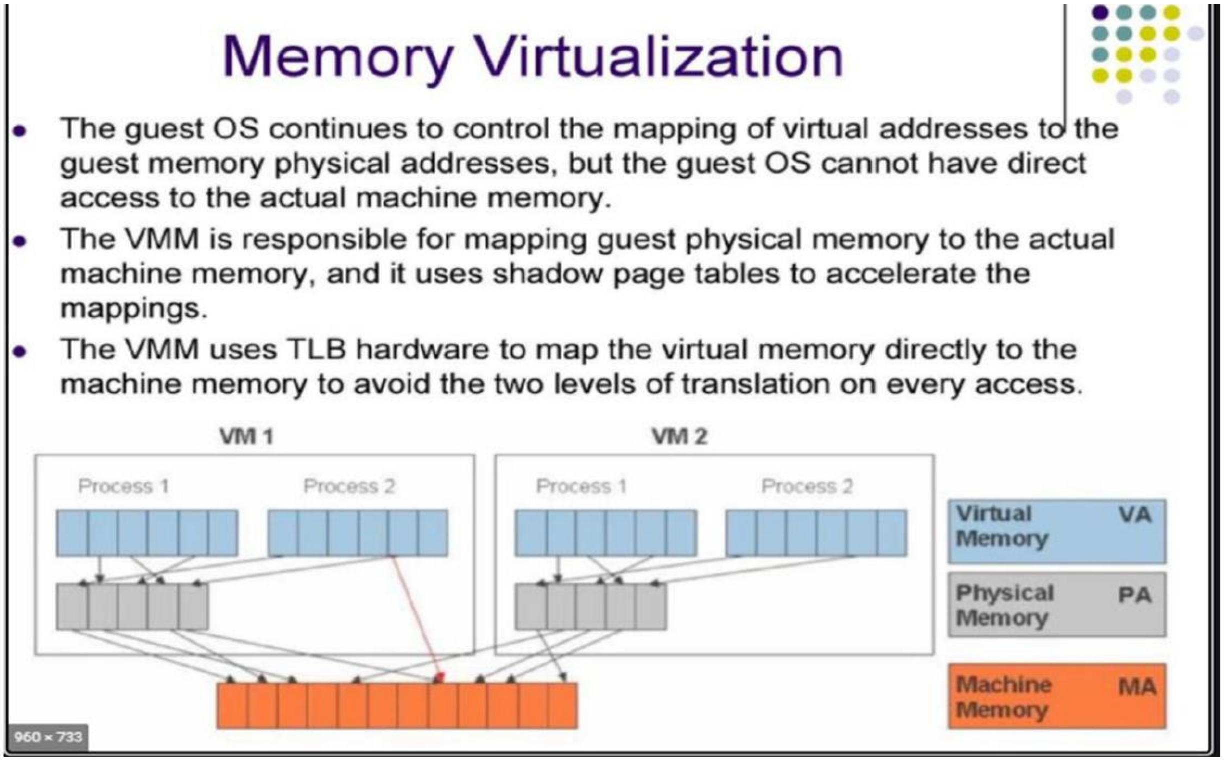


CPU Architecture

- Modern CPU status is usually classified as several modes.
- In general, we conceptually divide them into two modes :
  - Kernel mode (Ring 0)
    - CPU may perform any operation allowed by its architecture, including any instruction execution, IO operation, area of memory access, and so on.
    - Traditional OS kernel runs in Ring 0 mode.
  - User mode (Ring 1 ~ 3)
    - CPU can typically only execute a subset of those available instructions in kernel mode.
    - Traditional application runs in Ring 3 mode.

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.



Memory Virtualization

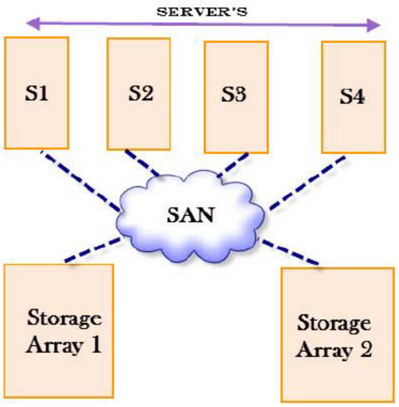
- The guest OS continues to control the mapping of virtual addresses to the guest memory physical addresses, but the guest OS cannot have direct access to the actual machine memory.
- The VMM is responsible for mapping guest physical memory to the actual machine memory, and it uses shadow page tables to accelerate the mappings.
- The VMM uses TLB hardware to map the virtual memory directly to the machine memory to avoid the two levels of translation on every access.

Server Virtualization

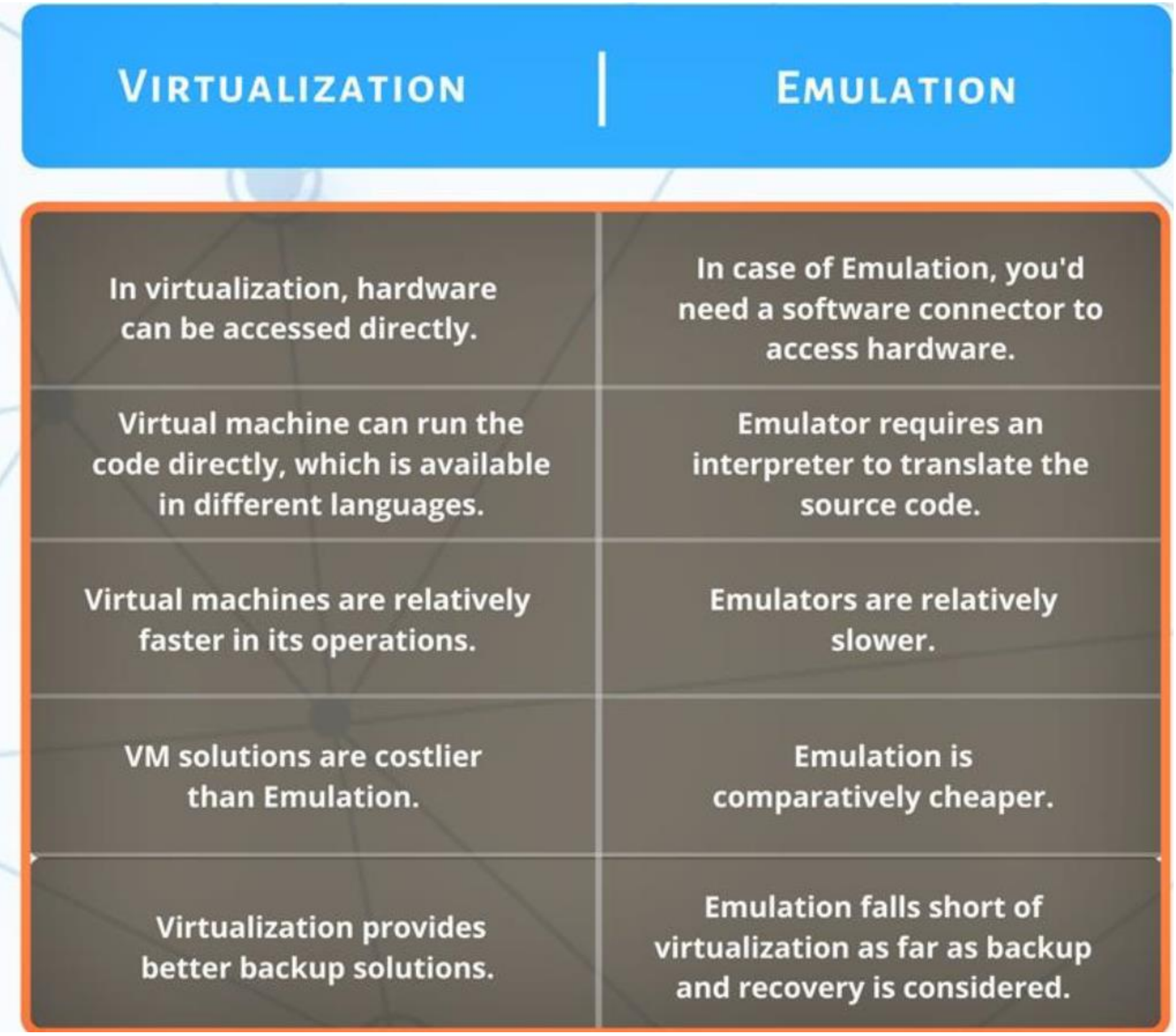
- Pros
  - Resource pooling
  - Highly available
  - Rapidly deploy new servers
  - Easy to deploy
  - Reconfigurable while services are running
  - Optimizes physical resources by doing more with less
- Cons
  - Slightly harder to conceptualize
  - Slightly more costly (must buy hardware, OS, Apps, and now the abstraction layer)

SAN

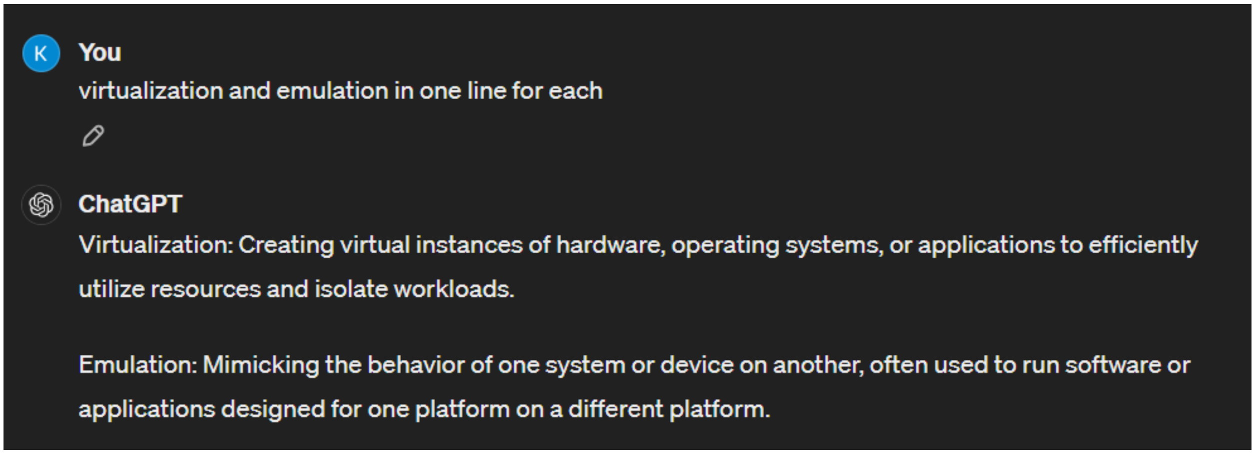
- Network of storage devices, Fibre Channel
- Internet Small Computer Systems Interface (iSCSI) are examples of SAN protocols.
- Administrator will group a set of disks (or a portion of a set of disks) into a LUN (logical unit), which then behaves like a single disk drive to outside computers.
- The LUN is the fundamental unit used to manage SAN storage.
- Block level data storage



Storage Area Network (SAN) Implementation



Virtualization	Emulation
In virtualization, hardware can be accessed directly.	In case of Emulation, you'd need a software connector to access hardware.
Virtual machine can run the code directly, which is available in different languages.	Emulator requires an interpreter to translate the source code.
Virtual machines are relatively faster in its operations.	Emulators are relatively slower.
VM solutions are costlier than Emulation.	Emulation is comparatively cheaper.
Virtualization provides better backup solutions.	Emulation falls short of virtualization as far as backup and recovery is considered.



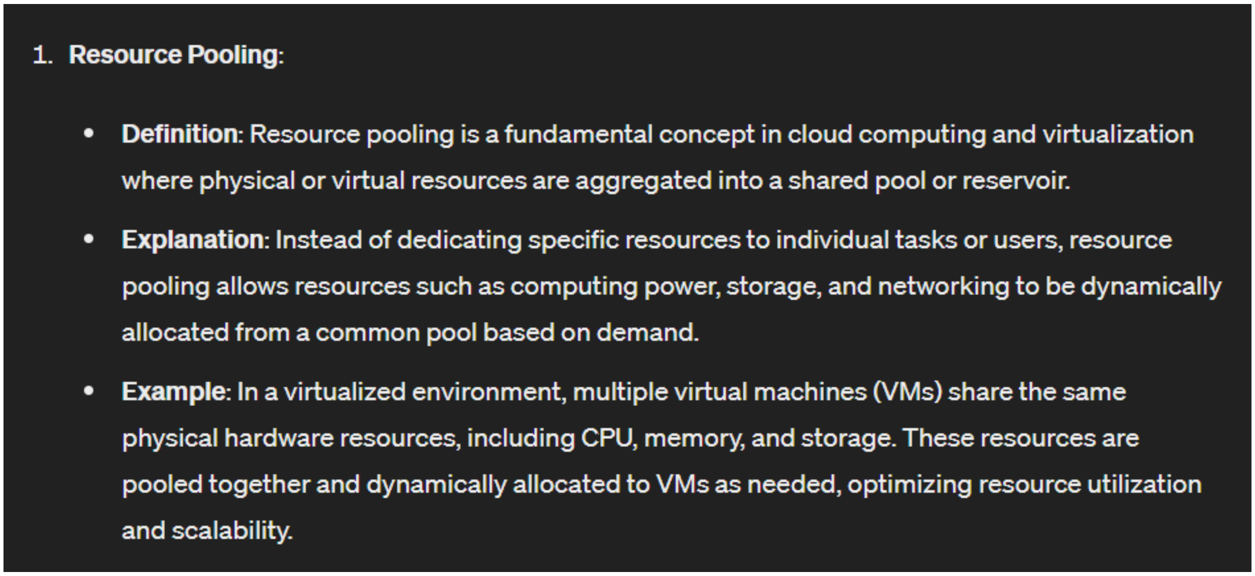
You

virtualization and emulation in one line for each

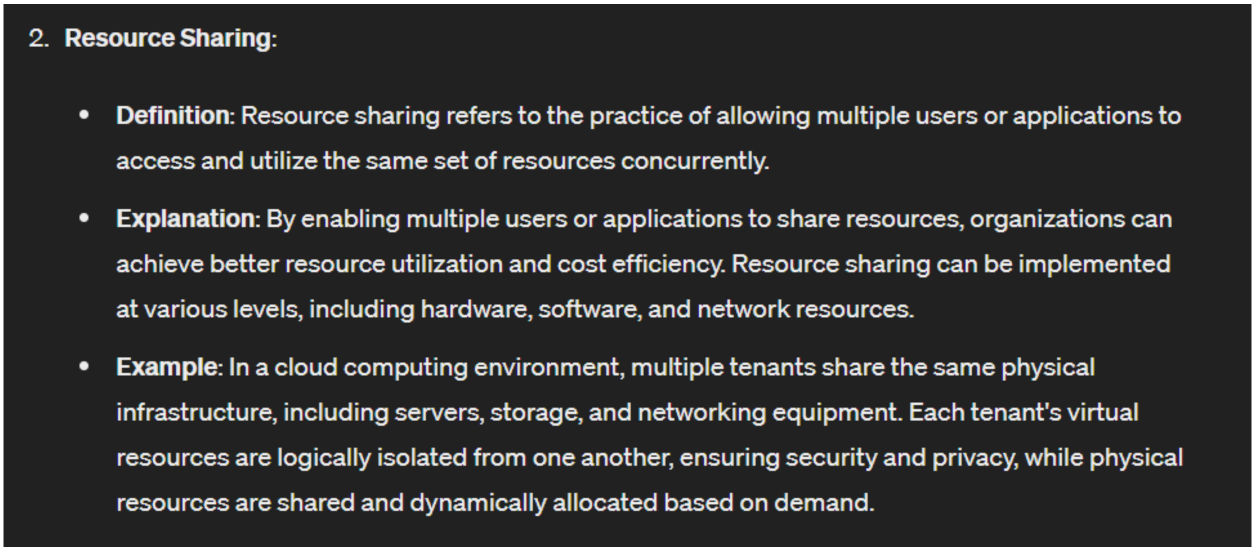
ChatGPT

Virtualization: Creating virtual instances of hardware, operating systems, or applications to efficiently utilize resources and isolate workloads.

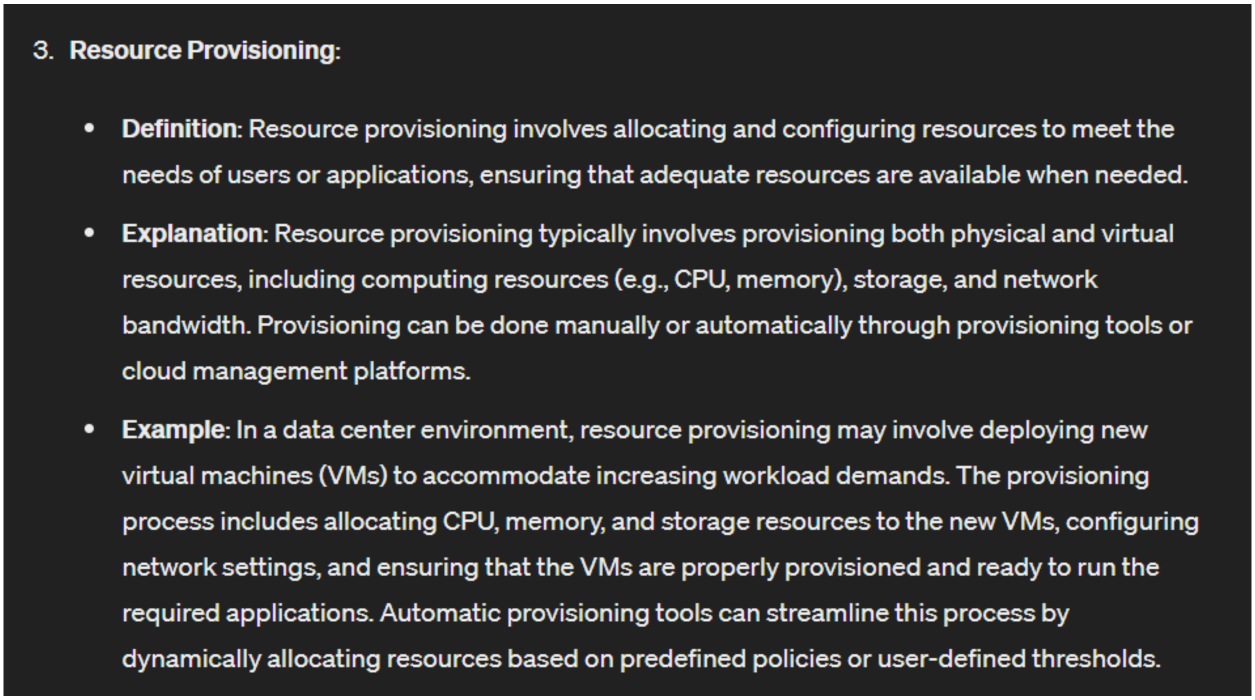
Emulation: Mimicking the behavior of one system or device on another, often used to run software or applications designed for one platform on a different platform.



1. **Resource Pooling**:
    - **Definition**: Resource pooling is a fundamental concept in cloud computing and virtualization where physical or virtual resources are aggregated into a shared pool or reservoir.
    - **Explanation**: Instead of dedicating specific resources to individual tasks or users, resource pooling allows resources such as computing power, storage, and networking to be dynamically allocated from a common pool based on demand.
    - **Example**: In a virtualized environment, multiple virtual machines (VMs) share the same physical hardware resources, including CPU, memory, and storage. These resources are pooled together and dynamically allocated to VMs as needed, optimizing resource utilization and scalability.

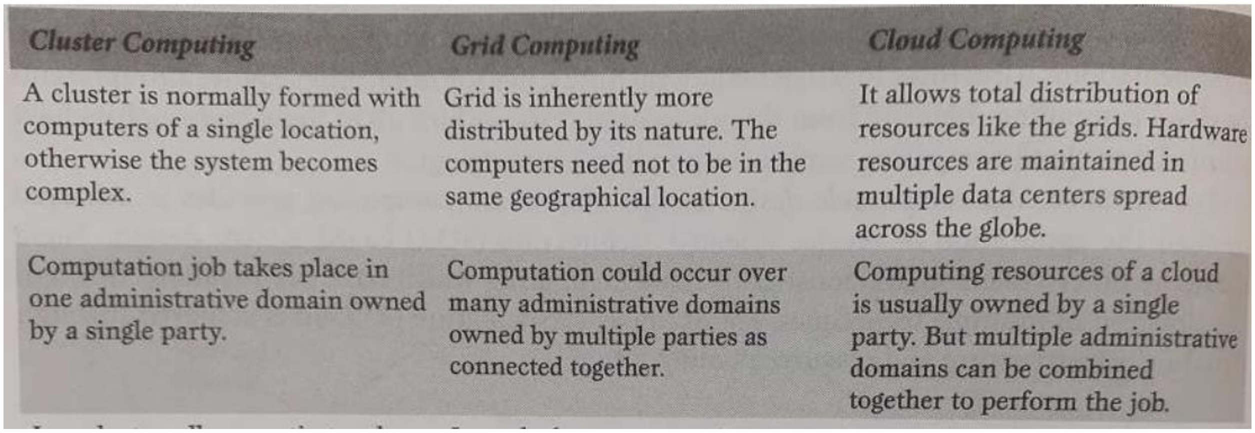


2. **Resource Sharing**:
    - **Definition**: Resource sharing refers to the practice of allowing multiple users or applications to access and utilize the same set of resources concurrently.
    - **Explanation**: By enabling multiple users or applications to share resources, organizations can achieve better resource utilization and cost efficiency. Resource sharing can be implemented at various levels, including hardware, software, and network resources.
    - **Example**: In a cloud computing environment, multiple tenants share the same physical infrastructure, including servers, storage, and networking equipment. Each tenant's virtual resources are logically isolated from one another, ensuring security and privacy, while physical resources are shared and dynamically allocated based on demand.

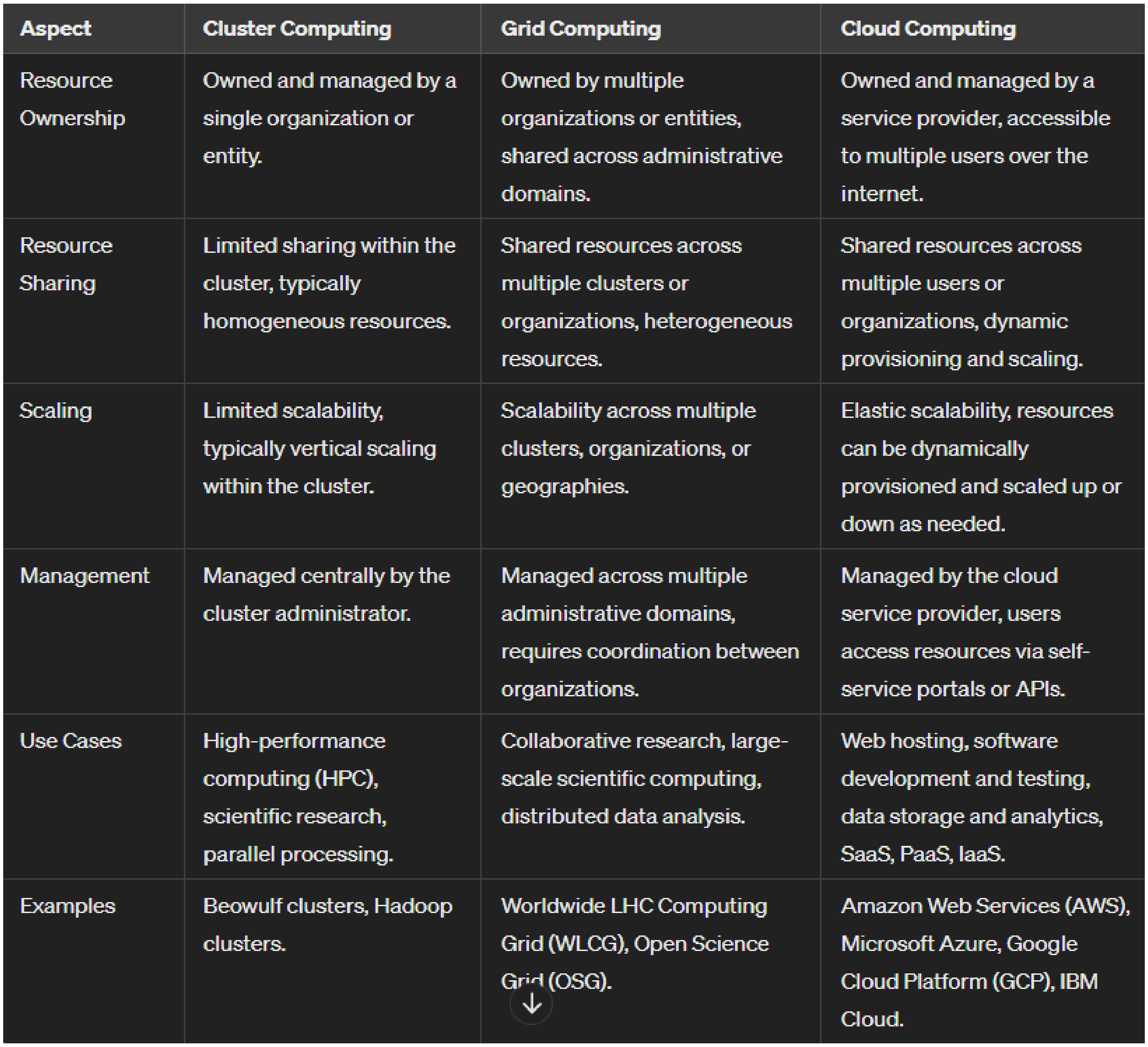


3. **Resource Provisioning**:
   - **Definition**: Resource provisioning involves allocating and configuring resources to meet the needs of users or applications, ensuring that adequate resources are available when needed.
   - **Explanation**: Resource provisioning typically involves provisioning both physical and virtual resources, including computing resources (e.g., CPU, memory), storage, and network bandwidth. Provisioning can be done manually or automatically through provisioning tools or cloud management platforms.
   - **Example**: In a data center environment, resource provisioning may involve deploying new virtual machines (VMs) to accommodate increasing workload demands. The provisioning process includes allocating CPU, memory, and storage resources to the new VMs, configuring network settings, and ensuring that the VMs are properly provisioned and ready to run the required applications. Automatic provisioning tools can streamline this process by dynamically allocating resources based on predefined policies or user-defined thresholds.

Mod-2



Cluster Computing	*Grid Computing*	*Cloud Computing*
A cluster is normally formed with computers of a single location, otherwise the system becomes complex.	Grid is inherently more distributed by its nature. The computers need not to be in the same geographical location.	It allows total distribution of resources like the grids. Hardware resources are maintained in multiple data centers spread across the globe.
Computation job takes place in one administrative domain owned by a single party.	Computation could occur over many administrative domains owned by multiple parties as connected together.	Computing resources of a cloud is usually owned by a single party. But multiple administrative domains can be combined together to perform the job.



Aspect	Cluster Computing	Grid Computing	Cloud Computing
Resource Ownership	Owned and managed by a single organization or entity.	Owned by multiple organizations or entities, shared across administrative domains.	Owned and managed by a service provider, accessible to multiple users over the internet.
Resource Sharing	Limited sharing within the cluster, typically homogeneous resources.	Shared resources across multiple clusters or organizations, heterogeneous resources.	Shared resources across multiple users or organizations, dynamic provisioning and scaling.
Scaling	Limited scalability, typically vertical scaling within the cluster.	Scalability across multiple clusters, organizations, or geographies.	Elastic scalability, resources can be dynamically provisioned and scaled up or down as needed.
Management	Managed centrally by the cluster administrator.	Managed across multiple administrative domains, requires coordination between organizations.	Managed by the cloud service provider, users access resources via self-service portals or APIs.
Use Cases	High-performance computing (HPC), scientific research, parallel processing.	Collaborative research, large-scale scientific computing, distributed data analysis.	Web hosting, software development and testing, data storage and analytics, SaaS, PaaS, IaaS.
Examples	Beowulf clusters, Hadoop clusters.	Worldwide LHC Computing Grid (WLCG), Open Science Grid (OSG).	Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud.

Limited Portability Between Cloud Providers

Due to a lack of established industry standards within the cloud computing industry, public clouds are commonly proprietary to various extents. For cloud consumers that have custom-built solutions with dependencies on these proprietary environments, it can be challenging to move from one cloud provider to another.

Portability is a measure used to determine the impact of moving cloud consumer IT resources and data between clouds (Figure 1).

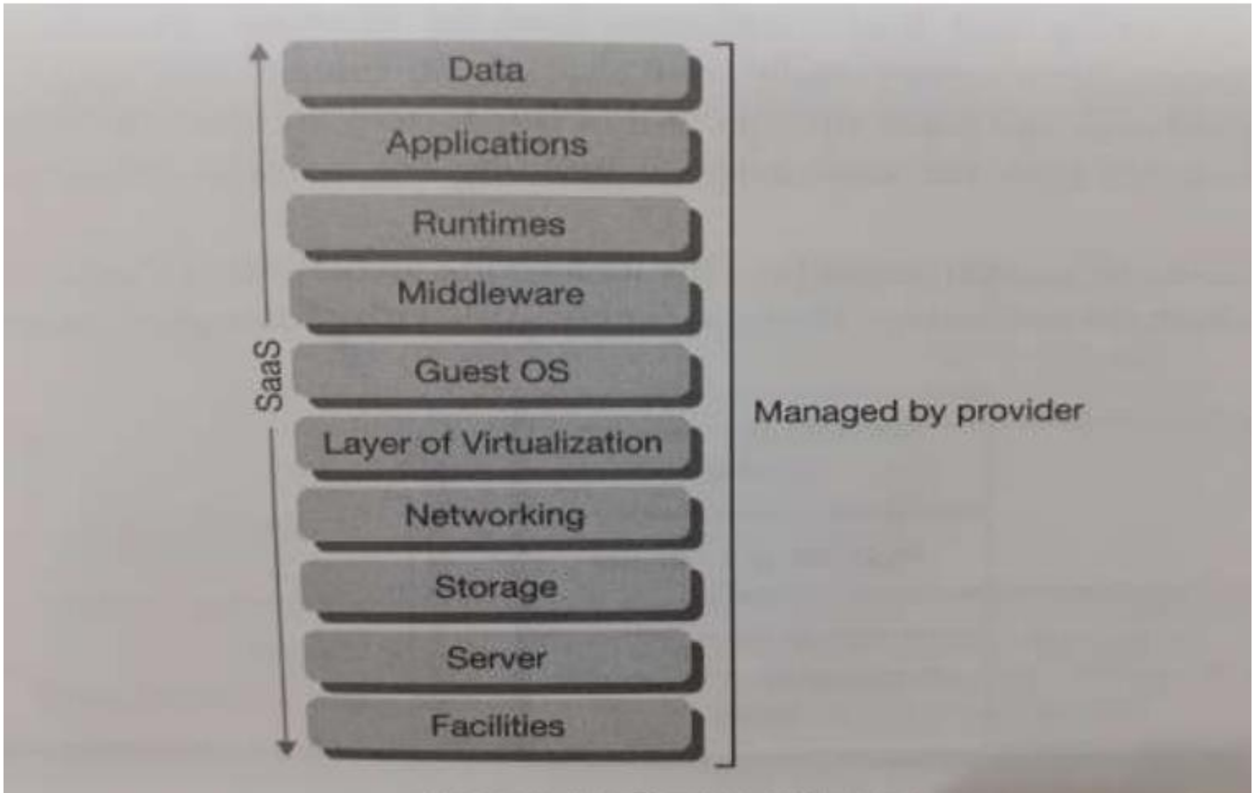
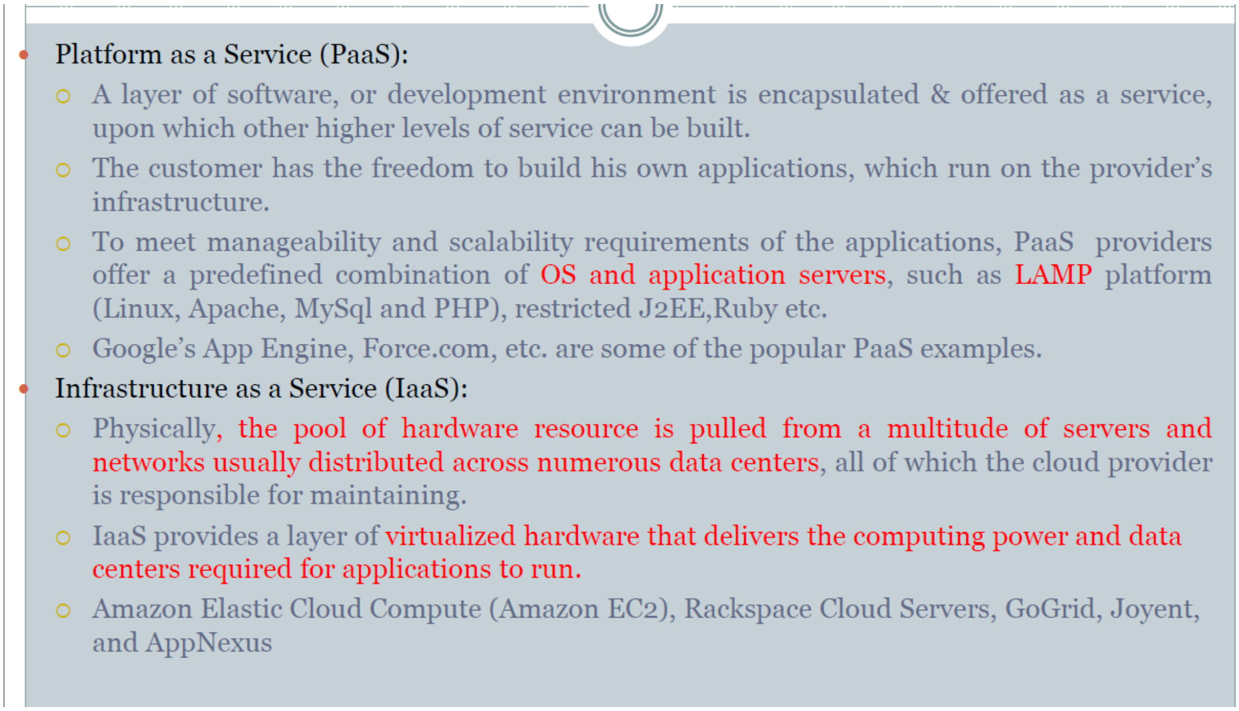


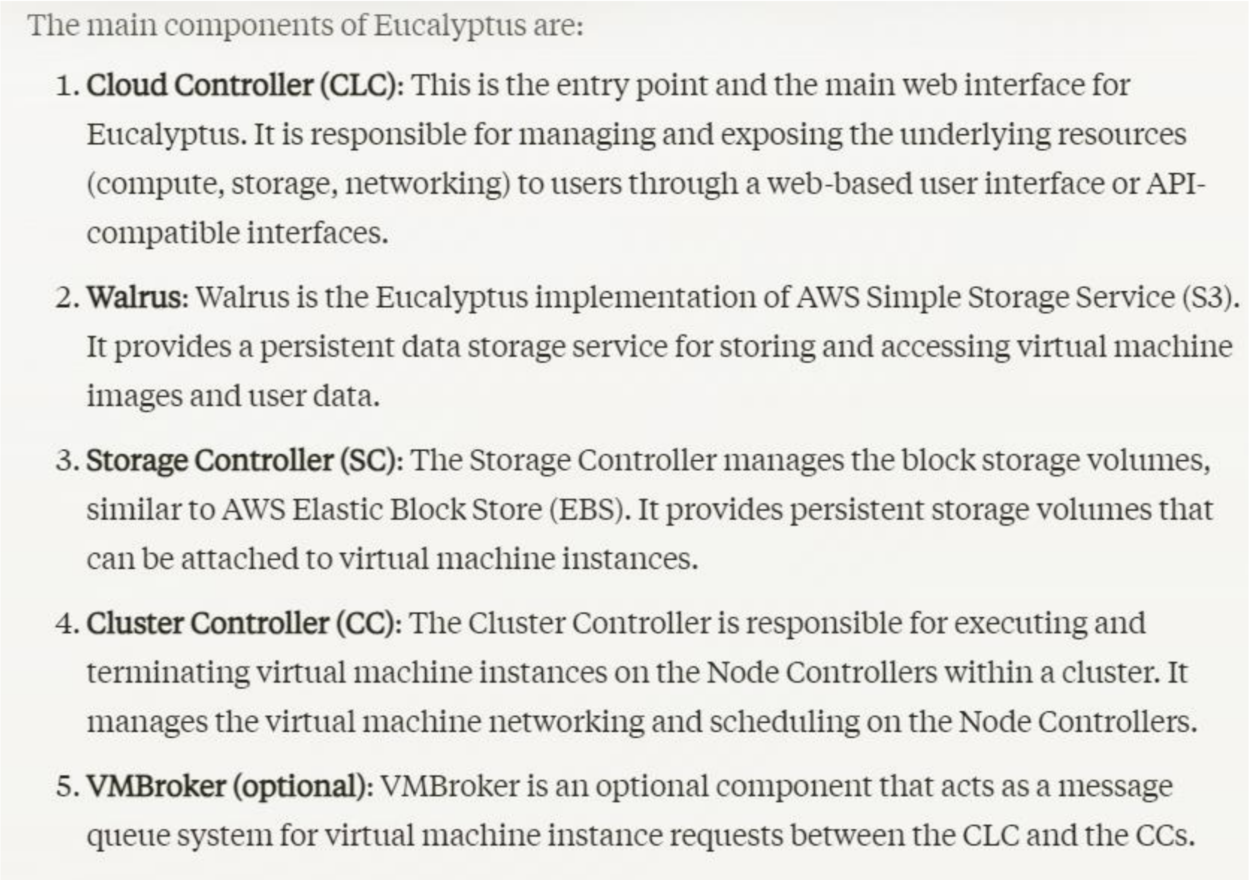
FIG 5.5: SaaS component stack

- 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.



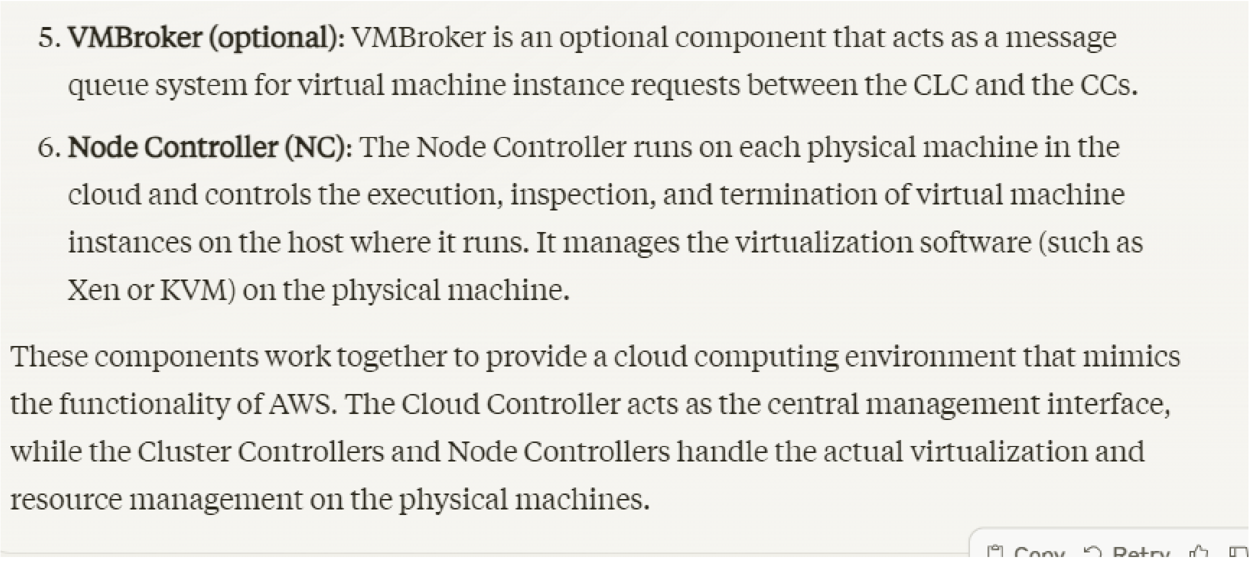
- Platform as a Service (PaaS):
  - A layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built.
  - The customer has the freedom to build his own applications, which run on the provider's infrastructure.
  - To meet manageability 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

Mod-3



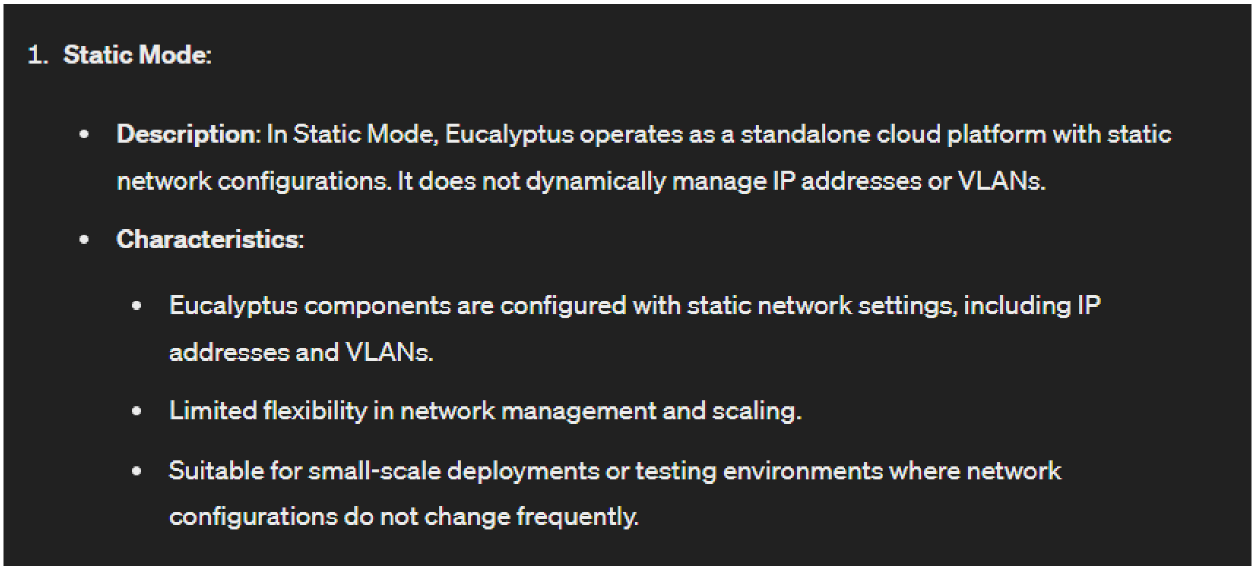
The main components of Eucalyptus are:

1. **Cloud Controller (CLC):** This is the entry point and the main web interface for Eucalyptus. It is responsible for managing and exposing the underlying resources (compute, storage, networking) to users through a web-based user interface or API-compatible interfaces.
2. **Walrus:** Walrus is the Eucalyptus implementation of AWS Simple Storage Service (S3). It provides a persistent data storage service for storing and accessing virtual machine images and user data.
3. **Storage Controller (SC):** The Storage Controller manages the block storage volumes, similar to AWS Elastic Block Store (EBS). It provides persistent storage volumes that can be attached to virtual machine instances.
4. **Cluster Controller (CC):** The Cluster Controller is responsible for executing and terminating virtual machine instances on the Node Controllers within a cluster. It manages the virtual machine networking and scheduling on the Node Controllers.
5. **VMBroker (optional):** VMBroker is an optional component that acts as a message queue system for virtual machine instance requests between the CLC and the CCs.

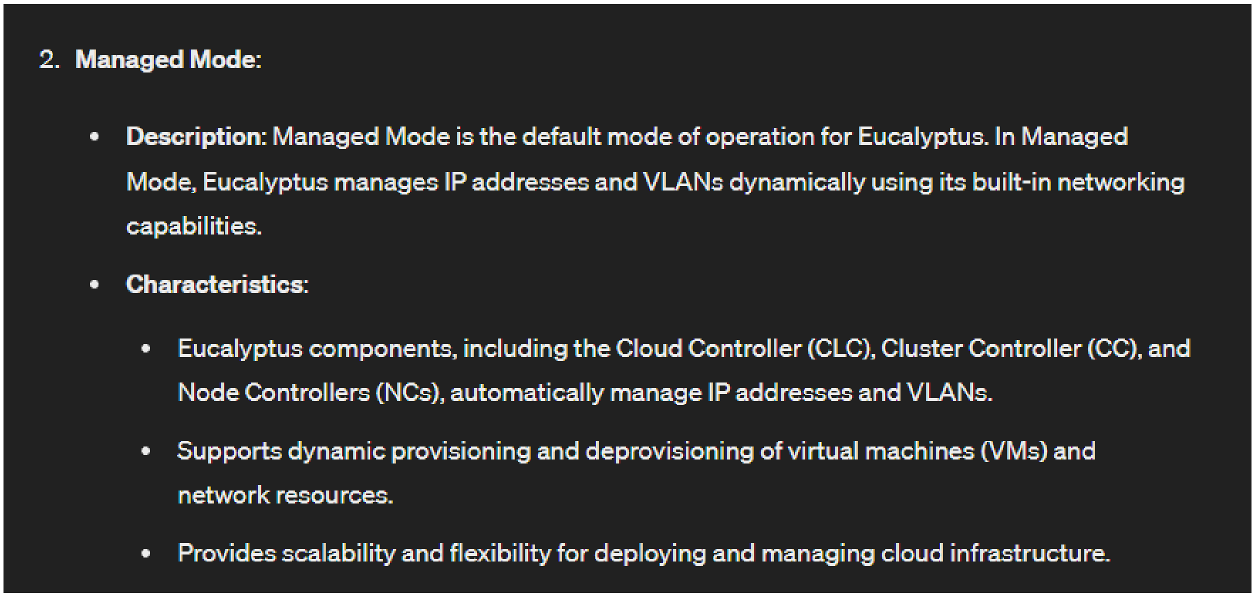


5. **VMBroker (optional):** VMBroker is an optional component that acts as a message queue system for virtual machine instance requests between the CLC and the CCs.
6. **Node Controller (NC):** The Node Controller runs on each physical machine in the cloud and controls the execution, inspection, and termination of virtual machine instances on the host where it runs. It manages the virtualization software (such as Xen or KVM) on the physical machine.

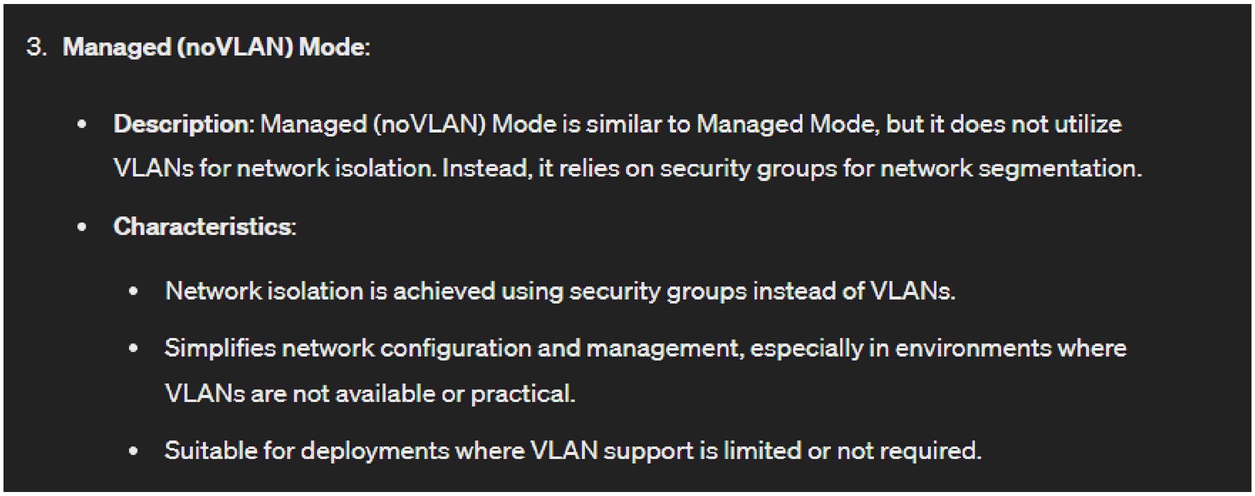
These components work together to provide a cloud computing environment that mimics the functionality of AWS. The Cloud Controller acts as the central management interface, while the Cluster Controllers and Node Controllers handle the actual virtualization and resource management on the physical machines.



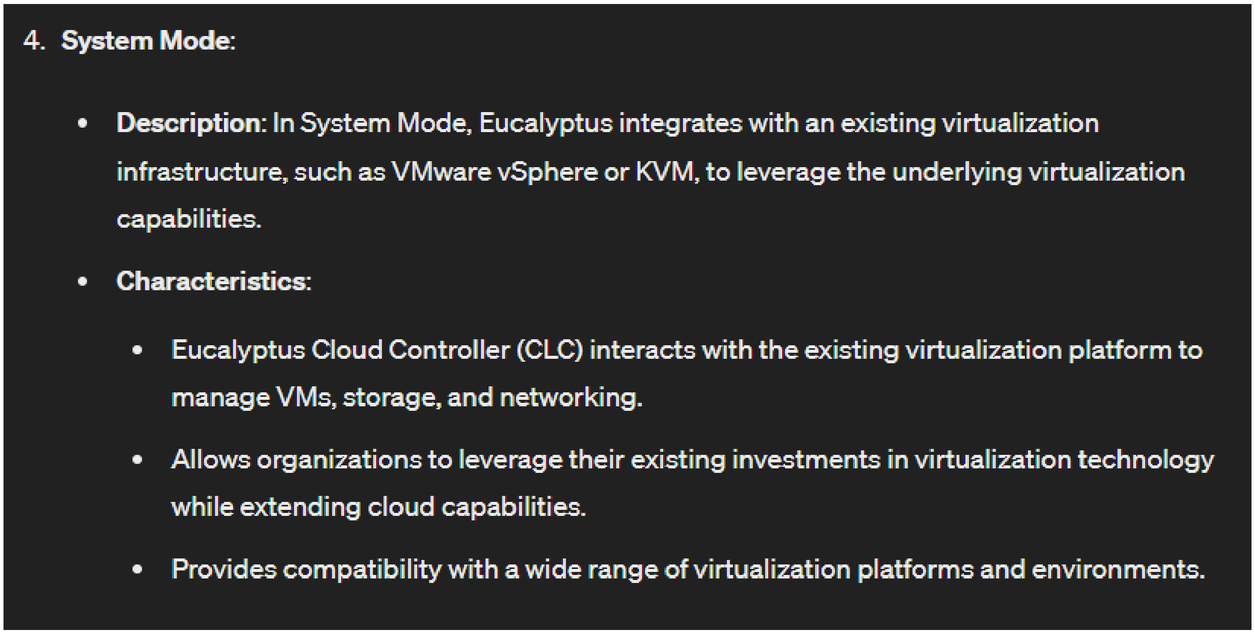
1. **Static Mode:**
   - **Description:** In Static Mode, Eucalyptus operates as a standalone cloud platform with static network configurations. It does not dynamically manage IP addresses or VLANs.
   - **Characteristics:**
     - Eucalyptus components are configured with static network settings, including IP addresses and VLANs.
     - Limited flexibility in network management and scaling.
     - Suitable for small-scale deployments or testing environments where network configurations do not change frequently.



2. **Managed Mode:**
   - **Description:** Managed Mode is the default mode of operation for Eucalyptus. In Managed Mode, Eucalyptus manages IP addresses and VLANs dynamically using its built-in networking capabilities.
   - **Characteristics:**
     - Eucalyptus components, including the Cloud Controller (CLC), Cluster Controller (CC), and Node Controllers (NCs), automatically manage IP addresses and VLANs.
     - Supports dynamic provisioning and deprovisioning of virtual machines (VMs) and network resources.
     - Provides scalability and flexibility for deploying and managing cloud infrastructure.



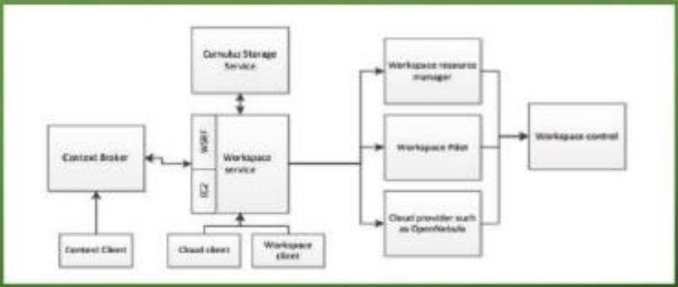
3. **Managed (noVLAN) Mode:**
   - **Description**: Managed (noVLAN) Mode is similar to Managed Mode, but it does not utilize VLANs for network isolation. Instead, it relies on security groups for network segmentation.
   - **Characteristics**:
     - Network isolation is achieved using security groups instead of VLANs.
     - Simplifies network configuration and management, especially in environments where VLANs are not available or practical.
     - Suitable for deployments where VLAN support is limited or not required.



4. **System Mode**:
   - **Description**: In System Mode, Eucalyptus integrates with an existing virtualization infrastructure, such as VMware vSphere or KVM, to leverage the underlying virtualization capabilities.
   - **Characteristics**:
     - Eucalyptus Cloud Controller (CLC) interacts with the existing virtualization platform to manage VMs, storage, and networking.
     - Allows organizations to leverage their existing investments in virtualization technology while extending cloud capabilities.
     - Provides compatibility with a wide range of virtualization platforms and environments.

System Architecture And Design

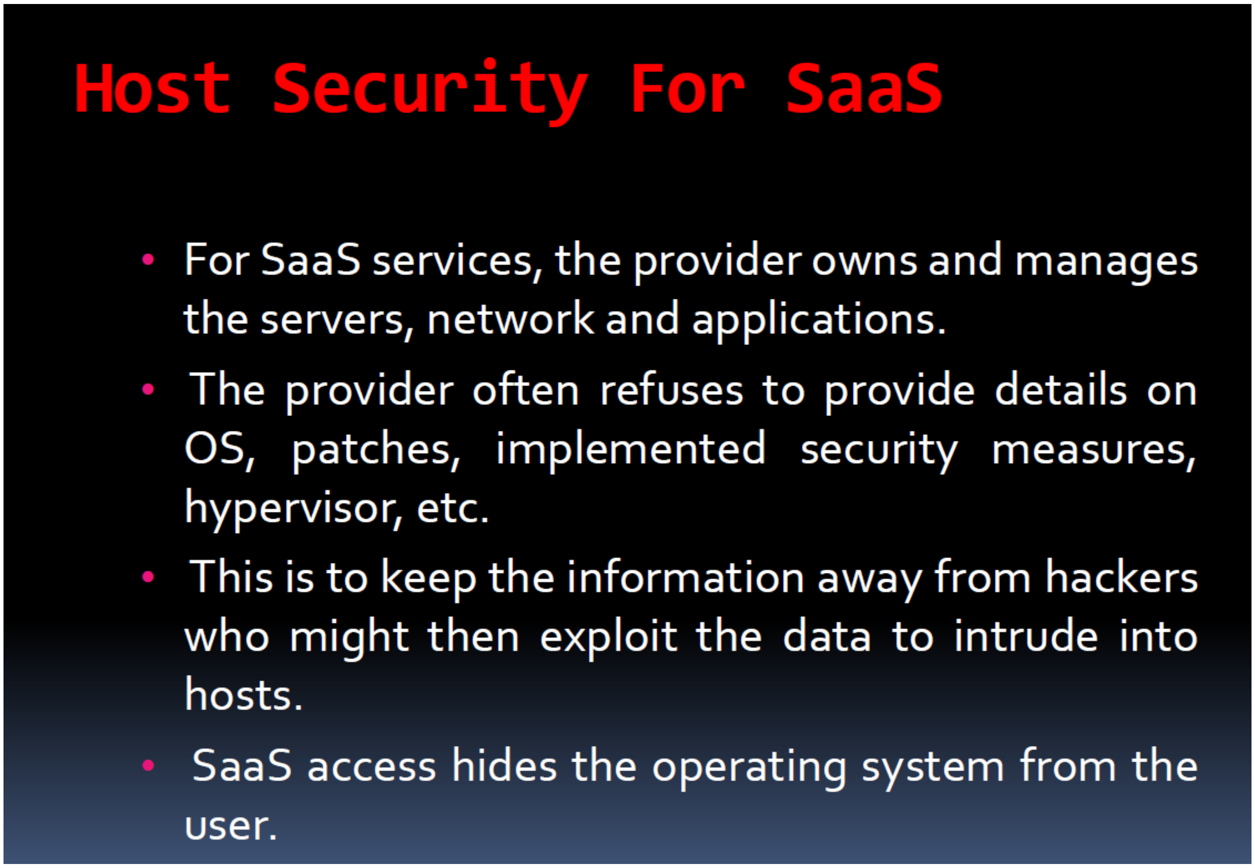
- The design of Nimbus which consists of a number of components based on the web service technology:



1. Workspace Service
   - Allows clients to manage and administer VMs by providing to two interfaces;
     1. One interface is based on the web service resource framework (WSRF)
     2. The other is based on EC2 WSDL.

2. Workspace Resource Manager
   - Implements VM instance creation on a site and management.
3. Workspace Pilot
   - Provides virtualization with significant changes to the site configurations.
4. Workspace Control
   - Implements VM instance management such as start, stop and pause VM. It also provides image management and sets up networks and provides IP assignment.
5. Context Broker
   - Allows clients coordinate large virtual cluster launches automatically and repeatedly.
6. Workspace Client
   - A complex client that provides full access to the workspace service functionality.
7. Cloud Client
   - A simpler client providing access to selected functionalities in the workspace service.
8. Storage Service
   - Cumulus is a web service providing users with storage capabilities to store images and works in conjunction with GridFTP.

Mod-4



Host Security For SaaS

- For SaaS services, the provider owns and manages the servers, network and applications.
- The provider often refuses to provide details on OS, patches, implemented security measures, hypervisor, etc.
- This is to keep the information away from hackers who might then exploit the data to intrude into hosts.
- SaaS access hides the operating system from the user.