Cloud Computing -

Module 1

1. cloud reference model,

2. A closer look(practical application - 1.1.3),

3. Characteristics and benefits \* (1.1.5 includes main frame pg 16)

4. bird view of cloud computing(Subscription - Oriented Cloud Services)

Module 2

5. virtualization type 1 and 2 -

6. Machine reference model(diagram and explain)

7. virtualization technique (Hardware-assisted virtualization, Full virtualization, Paravirtualization Partial virtualization explain two)

8. Characteristics of virtualization environments(pg 71 - 74[guest, host layer])

Above is the question paper - Same order-

**5. Virtualization Type 1 and Type 2**

Virtualization is the process of creating virtual versions of physical hardware components such as servers, storage devices, or network resources. There are two main types of virtualization: **Type 1** (Bare Metal) and **Type 2** (Hosted) hypervisors.

**Type 1: Bare Metal Hypervisor**

* **Description:** A Type 1 hypervisor runs directly on the host’s hardware, without requiring a host operating system. It interacts directly with the hardware and manages guest operating systems.
* **Examples:** VMware ESXi, Microsoft Hyper-V, Xen.
* **Advantages:**
  + Direct access to hardware resources makes it more efficient.
  + High performance and better resource management.
  + More secure since there's no host OS to compromise.
* **Disadvantages:**
  + Requires specialized hardware and software expertise to manage.
  + Less user-friendly due to its complex setup process.

**Type 2: Hosted Hypervisor**

* **Description:** A Type 2 hypervisor runs on a conventional operating system (host OS) and relies on the host’s resources to manage the guest operating systems.
* **Examples:** VMware Workstation, Oracle VirtualBox, Parallels Desktop.
* **Advantages:**
  + Easier to set up and use, even on general-purpose hardware.
  + Ideal for development, testing, and personal use.
* **Disadvantages:**
  + Performance is lower compared to Type 1 hypervisors because it relies on the host OS.
  + More susceptible to security risks due to reliance on the host OS.

**6. Machine Reference Model (Diagram and Explanation)**

The **Machine Reference Model** is used in virtualization to separate the physical hardware from the virtual machines (VMs). Below is an explanation of the key components:

**Diagram (Generalized):**

lua

Copy code

------------------------------------------------

| Applications |

------------------------------------------------

| Guest Operating Systems |

------------------------------------------------

| Virtual Machines (VMs) |

------------------------------------------------

| Hypervisor Layer |

------------------------------------------------

| Physical Hardware |

------------------------------------------------

**Components:**

1. **Physical Hardware Layer**:
   * This includes the actual hardware components such as CPU, memory, storage, and networking devices.
2. **Hypervisor Layer**:
   * The hypervisor creates and manages virtual machines. It abstracts the physical hardware and makes it accessible to the virtual machines. There are two types of hypervisors (Type 1 and Type 2, as explained earlier).
3. **Virtual Machines (VMs)**:
   * VMs are the virtual instances of computers that run their own operating systems and applications. Each VM operates independently from the others.
4. **Guest Operating Systems**:
   * These are the OSs running within each virtual machine, such as Windows, Linux, or macOS.
5. **Applications**:
   * The applications that run inside the virtual machine environment.

The machine reference model essentially allows multiple OSs and applications to run on the same physical hardware while being isolated from one another.

**7. Virtualization Techniques**

**Hardware-Assisted Virtualization**

* **Description**:
  + Hardware-assisted virtualization uses the capabilities built into the CPU to help the hypervisor manage VMs more efficiently. Technologies like **Intel VT-x** and **AMD-V** are examples that allow better handling of privileged instructions by the hypervisor.
* **Advantages**:
  + Improved performance since the CPU handles critical tasks.
  + Reduced overhead for the hypervisor, leading to better scalability.
* **Use Case**:
  + It is commonly used in Type 1 hypervisors like VMware ESXi to enhance VM performance.

**Full Virtualization**

* **Description**:
  + Full virtualization involves completely simulating a real hardware environment, enabling an unmodified OS to run in a VM. The hypervisor controls the entire execution, translating guest OS instructions to hardware instructions.
* **Advantages**:
  + No modification needed for the guest OS.
  + Offers full isolation between VMs, enhancing security.
* **Disadvantages**:
  + Higher performance overhead due to complex instruction translation.
* **Use Case**:
  + Full virtualization is used in platforms like VMware and VirtualBox.

**Paravirtualization**

* **Description**:
  + Paravirtualization requires modifications to the guest OS so that it can communicate more efficiently with the hypervisor. Instead of simulating the hardware, the guest OS is aware it is running in a virtualized environment and makes system calls to the hypervisor.
* **Advantages**:
  + Better performance than full virtualization due to fewer instruction translations.
  + Lower overhead because the guest OS interacts directly with the hypervisor.
* **Disadvantages**:
  + The guest OS must be modified, which limits flexibility.
* **Use Case**:
  + Used in open-source platforms like Xen.

**Partial Virtualization**

* **Description**:
  + Partial virtualization emulates only parts of the hardware, meaning that the guest OS may still need direct access to some hardware components.
* **Advantages**:
  + More efficient than full virtualization as it only virtualizes select parts.
  + Simpler implementation than full virtualization.
* **Disadvantages**:
  + Guest OS needs to be aware of some hardware details.
* **Use Case**:
  + Often used in specialized environments where only part of the system needs to be virtualized.

**8. Characteristics of Virtualization Environments (Guest, Host Layers)**

Virtualization environments have several defining characteristics that make them suitable for modern IT infrastructure. Between **guest** and **host layers**, the following characteristics apply (from pg 71-74):

**1. Isolation:**

* **Host Layer**: The host layer provides a secure and isolated environment where multiple VMs (guests) run independently without affecting each other.
* **Guest Layer**: Each guest OS is completely isolated, ensuring that a failure or security breach in one guest does not impact others.

**2. Scalability:**

* **Host Layer**: Virtualization environments allow for easy scaling of hardware resources, enabling the creation of new VMs without the need for additional physical hardware.
* **Guest Layer**: Each guest VM can be scaled independently, either by increasing allocated memory, CPU resources, or disk space as required.

**3. Resource Pooling:**

* **Host Layer**: Hardware resources like CPU, memory, and storage are pooled and dynamically allocated to the VMs as needed. The host manages these resources efficiently to ensure optimal utilization.
* **Guest Layer**: From the guest OS's perspective, it has full access to its allocated resources, though they are virtualized.

**4. Abstraction:**

* **Host Layer**: The host provides a layer of abstraction between the physical hardware and the guest VMs. This abstraction allows multiple VMs to run on different hardware architectures without being dependent on specific hardware configurations.
* **Guest Layer**: The guest OS operates as though it is running on real hardware, even though it is operating on virtualized hardware resources.

**5. Performance:**

* **Host Layer**: With technologies like **hardware-assisted virtualization**, the host layer can offer near-native performance for guest VMs, especially in Type 1 hypervisors.
* **Guest Layer**: The guest can perform most tasks with minimal performance degradation, depending on the efficiency of the hypervisor and resource allocation.

**6. Security:**

* **Host Layer**: Virtualization environments enhance security by isolating the guest VMs from the host. Security tools can also be installed at the hypervisor level to monitor traffic between VMs.
* **Guest Layer**: Each guest is typically sandboxed, limiting the impact of any potential security threats within a single VM.

These characteristics make virtualization environments flexible, efficient, and secure, providing organizations with a powerful tool for optimizing their IT resources.