Virtualization Notes 🔥

By Garvit Singh, IT Undergraduate

What is Virtualization?

Virtualization is a technology that allows you to create multiple virtual instances of computer resources within a single physical machine.

It enables better resource utilization, improved scalability, and increased flexibility in managing and deploying applications and services.

There are different approaches to virtualization, including hypervisors, containerization, and virtual machines(VMs).

1. **Hypervisors**
   - A hypervisor, also known as a virtual machine monitor (VMM), is a software or hardware layer that creates and manages multiple virtual machines on a single physical server.
   - There are two main types of hypervisors:
     - **Type 1 Hypervisor**: This runs directly on the host hardware and doesn't require a host operating system. Ex - VMware vSphere/ESXi, Microsoft Hyper-V, and Xen.
     - **Type 2 Hypervisor**: This runs on top of a host operating system and is often used for development and testing. Ex - Oracle VirtualBox and VMware Workstation.
   - Hypervisors provide strong isolation between virtual machines, making them suitable for running different operating systems and applications on the same physical server.

- Each virtual machine (VM) created by a hypervisor has its own virtualized hardware and can run an independent operating system.

2. **Containerization**
    - Containerization is a lightweight form of virtualization that allows you to package an application and its dependencies into a single unit called a container.
    - Containers share the host operating system's kernel and use the same resources, making them highly efficient and fast to start and stop.
    - Docker is one of the most popular containerization platforms, and it uses container images to package applications and their dependencies. These images can be easily distributed and deployed across various environments.
    - Containers are typically used to isolate applications rather than entire operating systems, making them an excellent choice for microservices architectures and cloud-native applications.
3. **Virtual Machines (VMs)**
    - Virtual machines are complete emulations of physical computers, including a full operating system, running on a hypervisor.
    - Each VM runs its own guest operating system, which may be different from the host operating system. This allows for running multiple distinct operating systems on a single physical server.
    - VMs offer strong isolation between workloads, making them suitable for scenarios where security and complete separation are crucial.
    - VMs can be used for various purposes, from running legacy applications to creating test environments and disaster recovery solutions.

Characterstics Of Virtualized Environments

1. **Increased Security**

- Virtualization enhances security in several ways. By isolating workloads or applications in separate virtual machines (VMs) or containers, vulnerabilities in one component are less likely to impact others.
- Security policies and access controls can be applied at the virtualization layer to protect data and resources. Snapshots and backups in virtualized environments make disaster recovery and data protection more accessible.

2. **Managed Execution**

- Managed execution in virtualized environments involves various techniques for controlling and optimizing resource utilization.
  - a) **Sharing**
    - Virtualization allows for the sharing of physical resources among multiple VMs or containers.
    - This sharing maximizes resource utilization and cost-efficiency.
  - b) **Aggregation**
    - Virtualization platforms can aggregate the computational power of multiple physical servers, creating resource pools that can be allocated to VMs dynamically.
  - c) **Emulation**
    - Some virtualization approaches, such as full virtualization, use emulation to run guest operating systems on a different architecture.

        - This enables running legacy applications on modern hardware.
    - d) **Isolation**
        - Isolation ensures that VMs or containers run independently, with their own isolated file systems, processes, and network configurations.
        - Isolation helps prevent interference between workloads.

3. **Portability**

- Virtualization enhances application and workload portability.
- Virtual machines or containers encapsulate the application and its dependencies, allowing it to run consistently across different environments, from on-premises servers to public or private clouds.
- This portability simplifies deployment, migration, and scaling of applications.

Execution Virtualization

A technology that enables the creation of virtual environments or virtual machines (VMs) within a physical computing system.

These virtual environments mimic the behavior of actual physical hardware or software, allowing multiple isolated instances to run concurrently on the same physical machine.

1. **Machine Reference Model**

- This concept refers to the virtualization of an entire computing system, which replicates a reference model of a physical machine.
- It serves as a foundation for various virtualization techniques, allowing multiple virtual machines to operate independently on the same physical hardware.

2. **Hardware Level Virtualization**

- Hardware level virtualization, also known as system virtualization, involves creating multiple VMs that directly interact with the underlying hardware.
- Each VM has its own dedicated resources, such as CPU, memory, and storage. The virtualization software (hypervisor) manages and isolates these VMs from one another.

3. **Hardware Virtualization Techniques**

- a) **Hardware-assisted Virtualization**

    - This technique utilizes hardware features, like Intel VT-x and AMD-V, to improve the performance and security of virtualization.
    - It enables VMs to execute instructions directly on the physical CPU, reducing the need for complex emulation.
- b) **Full Virtualization**
    - In full virtualization, the VMs run unmodified guest operating systems, believing they are running on real hardware.
    - The hypervisor intercepts and emulates privileged instructions, making it appear as if the VMs have full control over the hardware.
- c) **Paravirtualization**
    - Paravirtualization involves modifying the guest operating systems to be aware of their virtualized environment.
    - This awareness allows for better performance and efficiency, as the guest OS can make direct calls to the hypervisor for certain operations.
- d) **Partial Virtualization**
    - Partial virtualization is a less common approach where only specific aspects of a system are virtualized, rather than the entire hardware stack. It may involve virtualizing specific devices or resources.

4. **Operating System Level Virtualization**

- Also known as containerization, this virtualization method creates isolated environments at the operating system level.

- Containers share the host OS kernel but have their own user spaces, allowing for efficient resource utilization and fast startup times.
- Docker and Kubernetes are popular tools for managing containers.

5. **Programming Language Level Virtualization**

- This is often referred to as language-level virtualization.
- It involves creating isolated runtime environments for a specific programming language.
- Examples include the Java Virtual Machine (JVM) for Java and the Common Language Runtime (CLR) for .NET languages.
- These runtime environments provide a level of abstraction that allows applications to run independently of the host platform.

6. **Application Level Virtualization**

- Application-level virtualization focuses on virtualizing specific applications rather than entire operating systems or hardware.
- This approach encapsulates an application and its dependencies into a self-contained package, making it portable and isolated from the host environment.
- Examples include application virtualization solutions like VMware ThinApp and Microsoft App-V.

Other Types Of Virtualization

1. **Storage Virtualization**

- Storage virtualization abstracts and pools physical storage resources from various storage devices into a single virtual storage unit.
- This abstraction allows for centralized management and improved utilization of storage capacity.
- It can be implemented at different levels, such as file-level, block-level, or object-level virtualization, and is often used in storage area networks (SANs) and network-attached storage (NAS) environments.

2. **Network Virtualization**

- Network virtualization is the creation of multiple virtual networks on a single physical network infrastructure.
- It abstracts network resources, such as switches, routers, and even IP addresses, allowing multiple virtual networks to coexist independently.
- This technology is particularly valuable in cloud computing, data centers, and Software-Defined Networking (SDN) environments.
- Network virtualization can improve network flexibility, security, and scalability.

3. **Desktop Virtualization**

- Desktop virtualization, often known as Virtual Desktop Infrastructure (VDI), separates a user's desktop environment from the physical device, such as a PC or thin client.

- It allows users to access their desktops from various devices and locations, while the actual computing takes place on a server in a data center.
- This enhances security, centralizes management, and simplifies application deployment and updates.

4. **Application-Server Virtualization**

- Application-server virtualization, also known as application virtualization or server virtualization, focuses on running multiple instances of applications or application servers on a single physical server.
- This is accomplished by abstracting the underlying server hardware and operating system, allowing applications to operate in isolated environments.
- This approach simplifies application deployment, improves resource utilization, and enhances application availability and scalability.

Advantages & Disadvantages Of Virtualization

Advantages

1. **Resource Consolidation**

- Virtualization allows multiple virtual machines (VMs) to run on a single physical server, which optimizes resource utilization.
- This results in cost savings as fewer physical servers are needed.

2. **Isolation**

- VMs are isolated from each other, which means problems in one VM are less likely to affect others.
- This isolation enhances security and stability.

3. **Flexibility and Scalability**

- Virtualized environments can easily scale up or down, making it simpler to adapt to changing workload requirements.

4. **Disaster Recovery**

- Virtualization makes backup and disaster recovery processes more efficient.
- VM snapshots and replication can quickly restore VMs in case of failures.

5. **Efficient Testing and Development**

- Virtualization allows for the creation of isolated development and test environments, reducing the risk of interfering with production systems.

6. **Hardware Independence**

- VMs are not tied to specific hardware, making them more portable and easier to migrate between physical hosts.

7. **Energy Efficiency**

- By consolidating workloads onto fewer physical servers, virtualization can lead to energy savings and a reduced carbon footprint.

8. **Easy Software Deployment**

- Virtual appliances and images make it simple to deploy and manage software across different environments.

Disadvantages

1. **Overhead**

- There is a performance overhead associated with virtualization, as the hypervisor adds some latency and resource consumption.
- This can affect the performance of resource-intensive applications.

2. **Licensing Costs**

- Virtualization software and management tools can be expensive.

- Licensing models can also be complex, making cost management challenging.

3. **Resource Contention**

- If not managed properly, resource contention among VMs on the same host can lead to performance degradation.
- This requires careful resource allocation and monitoring.

4. **Complexity**

- Managing virtualized environments can be complex, especially in large deployments.
- Proper planning and expertise are needed to ensure optimal performance and security.

5. **Security Risks**

- While virtualization provides isolation, vulnerabilities in the hypervisor or misconfigurations can lead to security risks.
- Attackers could potentially compromise the entire virtualized environment.

6. **Vendor Lock-In**

- Some virtualization platforms have proprietary features and formats, making it challenging to migrate VMs to other platforms or cloud services.

7. **Backup and Recovery Complexity**

- While virtualization can enhance disaster recovery, managing backups and recovery processes for a large number of VMs can be complicated.

8. **Limited Hardware Support**

- Virtualization may not support certain types of hardware or require specific hardware features for optimal performance, limiting hardware choices.

Thanks For Reading! 💙

By GARVIT SINGH

Information Technology