5. Virtualization Fundamentals

What is Virtualization?

Virtualization is the creation of a virtual representation of physical and logical resources through software. This includes servers, storage, networks, operating systems, and applications. This practice allows for better utilization of available resources, greater flexibility, and scalability in IT environments.

What is a Hypervisor?

A hypervisor is the core of virtualization; it acts as an intermediary between virtual machines and physical servers, enabling proper resource allocation. There are two types of hypervisors:

Type 1 or Bare-Metal Hypervisor

This type installs directly on physical hardware without needing a host operating system, making it more efficient. It is commonly used in enterprise environments. Examples include VMware ESXi, Microsoft Hyper-V, Xen, and KVM.

Type 2 or Hosted Hypervisor

This type runs on an existing operating system as a standard application, making it easier to install but less efficient. Examples include VMware Workstation, VirtualBox, and QEMU.

Virtualized Environments

Virtualization helps organizations reduce the number of physical machines needed in their IT infrastructure. Different elements can make up a virtualized system:

Virtual Machines (VM)

These are fully virtualized operating systems running on a hypervisor. It is essential to keep them updated and protected, as they share hardware and run with elevated privileges. If a VM is compromised, the host machine could also be at risk.

Containers

Containers are lightweight environments that include an application and its dependencies, sharing the host operating system's kernel. Docker is one of the most widely used platforms for this type of virtualization. While they are more efficient, a compromised container with elevated privileges could affect the underlying operating system.

Virtual Desktop Infrastructure (VDI)

User desktop environments can be stored remotely on a server using thin clients or virtual desktops. This approach makes it much easier to create, delete, copy, archive, or quickly deploy configurations over the network. VDI requires high availability and storage capacity.

Types of Virtualization

Server Virtualization

This type of virtualization aims to create multiple virtual servers from a single physical server, enabling the simultaneous and independent execution of multiple operating systems. It consists of the following elements: server, hypervisor, and virtualized machines.

Desktop Virtualization

Allows users to work on a machine with all its processes and applications without needing the physical device.

Hardware Resource Virtualization

This involves the logical simulation of hardware resources, including RAM, storage units, and network interfaces.

Network Virtualization

Separates a physical network into multiple virtual networks or merges several physical networks into a single virtual network. It can also implement technologies like Software Defined Networking (SDN) for programmable network management.

Application Virtualization

Enables applications to run from a remote server without being installed directly on the user's physical machine.

Types of Networks in Hypervisors

NAT (Network Address Translation)

Shares the host system's network connection, allowing access to the internet and local network devices. Virtual machines receive private IP addresses, making them inaccessible from external networks. This setup is ideal for testing and lab environments.

Bridged Adapter

Connects the virtual machine directly to the physical network, assigning it its own public IP address and making it visible to external networks. This configuration is useful for production environment simulations.

Internal Network

Allows communication only between virtual machines within the same internal network created by the hypervisor. It has no connection to the host system or the external physical network, making it suitable for isolated labs and testing environments.

Virtual Machine Protection

Like physical computers, virtual machines require patches, updates, and antimalware measures to protect against external threats. Depending on the specific tools available on a cloud platform, additional security options for virtual machines include:

Subnet Placement

Carefully assigning subnets for each instance to ensure it only has the necessary access to external networks.

Disabling Unneeded Ports and Services

Enabling only essential services and ports to minimize unnecessary exposure to external threats.

Account Management and Policies

Disabling default user accounts and creating user accounts with recommended management policies, such as strong password requirements and least privilege access.

Installing Antivirus/Antimalware Software

Installing protection software is crucial, and some cloud platforms offer these services as part of their infrastructure.

Implementing Host-Based Firewalls/IPS/IDS

Configuring host-based firewalls and using intrusion prevention and detection services to monitor and protect virtual machines from external threats. Some cloud platforms offer these as managed services.

Disadvantages of Virtualization

Despite its many benefits, virtualization also has some drawbacks:

- **Virtual Machine Sprawl**: Occurs when too many underutilized virtual servers consume more resources and space than needed for their workloads.
- **Virtual Machine Escape**: Happens when a compromised virtual machine interacts with and affects the host operating system.