Virtualization in Cloud Computing

Comprehend theoretical, technical, and commercial aspects of cloud computing

- Virtualization concepts
- Types of virtualization (Hypervisor, Containerization)
- Virtualization in cloud infrastructure

Virtualization concepts

Virtualization is a process that allows a computer to share its hardware resources with multiple digitally separated environments. Each virtualized environment runs within its allocated resources, such as memory, processing power, and storage. With virtualization, organizations can switch between different operating systems on the same server without rebooting.

Virtualization is a technology that allows you to create multiple virtual instances of physical hardware, such as servers, storage devices, or networking resources. These virtual instances, often referred to as virtual machines (VMs), can run multiple operating systems and applications independently on the same physical hardware. Virtualization offers several benefits, including improved resource utilization, isolation, flexibility, and scalability. Here are some key concepts and types of virtualization:

- Virtual Machine (VM): A virtual machine is a software emulation of a physical computer. It runs an operating system and applications just like a physical computer but is hosted on a physical server or a hypervisor.
- Hypervisor: A hypervisor, also known as a virtual machine monitor (VMM), is a software or hardware layer that manages multiple VMs on a physical host. There are two types of hypervisors:
    1. Type 1 Hypervisor: This runs directly on the physical hardware and doesn't require a host operating system. Examples include VMware vSphere/ESXi, Microsoft Hyper-V, and Xen.
    2. Type 2 Hypervisor: This runs on top of a host operating system. Examples include VMware Workstation, Oracle VirtualBox, and Parallels.
- Virtualization Layer: The virtualization layer is the software or hardware component that abstracts physical resources, such as CPU, memory, storage, and networking, to create virtual resources that can be allocated to VMs.
- Guest OS: Each VM typically runs its own guest operating system, which can be different from the host operating system. Common guest OS choices include Windows, Linux, and various server operating systems.
- Resource Pooling: Virtualization allows for the pooling of physical resources across multiple VMs. This means that resources like CPU, memory, and storage can be dynamically allocated to VMs as needed, optimizing resource utilization.

- Isolation: VMs are isolated from each other, so if one VM experiences issues or crashes, it does not affect other VMs running on the same host. This isolation enhances security and stability.
- Snapshot: A snapshot is a point-in-time copy of a VM's state. It allows you to capture the VM's configuration and data at a specific moment, making it easier to back up and recover VMs.
- Cloning: Cloning is the process of creating a duplicate copy of a VM. This is useful for quickly deploying multiple VMs with the same configuration.
- Live Migration: Live migration, also known as vMotion (in the case of VMware), enables the movement of a running VM from one physical host to another without downtime. This is useful for load balancing, maintenance, and fault tolerance.
- Application Virtualization: In addition to server virtualization, there's application virtualization. This technology allows you to run applications in isolated containers, making it easier to manage and deploy software across different environments.
- Network Virtualization: Network virtualization involves creating virtual networks within a physical network infrastructure. It allows for improved network segmentation, isolation, and management.
- Storage Virtualization: Storage virtualization abstracts physical storage resources and presents them as virtual storage pools. It can improve storage utilization and provide features like data replication and snapshots.
- Desktop Virtualization: Desktop virtualization allows multiple virtual desktops to run on a single physical machine. It's commonly used in organizations to centralize desktop management and provide remote access to desktop environments.

Virtualization has become a fundamental technology in data centers and IT infrastructure, enabling greater flexibility, efficiency, and cost savings in managing computing resources.

Types of virtualization (Hypervisor, Containerization)

Virtualization technology encompasses various approaches to abstracting and isolating computing resources. Two of the most prominent types of virtualization are hypervisor-based virtualization and containerization. Here's an overview of each:

Hypervisor-Based Virtualization

Hypervisor-based virtualization involves the use of a hypervisor, which is a software or hardware layer that creates and manages virtual machines (VMs) on a physical host. Each VM runs its own full-fledged operating system, and multiple VMs can coexist on the same physical hardware. Hypervisor-based virtualization is typically used in scenarios where strong isolation between VMs is required, and different operating systems need to run concurrently. There are two main types of hypervisors:

- Type 1 Hypervisor (Bare-Metal Hypervisor): Type 1 hypervisors run directly on the physical hardware without the need for a host operating system. They are well-suited

for enterprise data centers and cloud environments. Examples include VMware vSphere/ESXi, Microsoft Hyper-V, and Xen.
- Type 2 Hypervisor (Hosted Hypervisor): Type 2 hypervisors run on top of a host operating system. They are typically used for development, testing, and desktop virtualization. Examples include VMware Workstation, Oracle VirtualBox, and Parallels Desktop.

Key characteristics of hypervisor-based virtualization include strong VM isolation, the ability to run different OS types simultaneously, and support for live migration and snapshots.

Containerization Virtualization

Containerization is a lightweight form of virtualization that allows you to package an application and its dependencies into a single container image. Containers share the host operating system's kernel, making them more resource-efficient compared to VMs. Containerization is commonly used for deploying and scaling applications in cloud-native environments. Key containerization technologies include:

- Docker: Docker is a popular platform for creating, distributing, and running containerized applications. Docker containers package an application, its libraries, and runtime environment into a single image. Docker Compose is used to define and manage multi-container applications.
- Kubernetes: Kubernetes is an orchestration platform for containerized applications. It provides tools for deploying, scaling, and managing container workloads across clusters of machines. Kubernetes can be used with various container runtimes, including Docker and containerd.

Key characteristics of containerization include fast application deployment, efficient resource utilization, portability, and the ability to scale applications easily.

Comparison

- Hypervisor-based virtualization offers stronger isolation since each VM runs its own OS, making it suitable for scenarios where security and isolation are critical.
- Containerization is more lightweight and resource-efficient, making it ideal for microservices and cloud-native applications. Containers start faster and consume fewer resources than VMs.
- Hypervisors allow running different operating systems on the same host, while containers share the host OS kernel.
- Hypervisors are suitable for scenarios requiring diverse OS environments, while containers are focused on packaging and running applications and services.

In practice, organizations often use a combination of hypervisor-based virtualization and containerization to meet various workload and infrastructure requirements within their IT ecosystems.

Hypervisor-based virtualization is typically used for running full-fledged virtual machines with different operating systems, while containerization is used for lightweight, portable, and efficient application deployment. Both approaches offer benefits in terms of resource utilization, isolation, and scalability, but they are suited to different use cases and workloads. Application virtualization, on the other hand, focuses specifically on isolating and managing individual applications.

Other Types of Virtualizations

Server virtualization: Server virtualization is a process that partitions a physical server into multiple virtual servers. It is an efficient and cost-effective way to use server resources and deploy IT services in an organization. Without server virtualization, physical servers use only a small amount of their processing capacities, which leave devices idle.

Storage virtualization: Storage virtualization combines the functions of physical storage devices such as network attached storage (NAS) and storage area network (SAN). You can pool the storage hardware in your data center, even if it is from different vendors or of different types. Storage virtualization uses all your physical data storage and creates a large unit of virtual storage that you can assign and control by using management software. IT administrators can streamline storage activities, such as archiving, backup, and recovery, because they can combine multiple network storage devices virtually into a single storage device.

Network virtualization: Any computer network has hardware elements such as switches, routers, and firewalls. An organization with offices in multiple geographic locations can have several different network technologies working together to create its enterprise network. Network virtualization is a process that combines all of these network resources to centralize administrative tasks. Administrators can adjust and control these elements virtually without touching the physical components, which greatly simplifies network management.

The following are two approaches to network virtualization.

- Software-defined networking: Software-defined networking (SDN) controls traffic routing by taking over routing management from data routing in the physical environment. For example, you can program your system to prioritize your video call traffic over application traffic to ensure consistent call quality in all online meetings.
- Network function virtualization: Network function virtualization technology combines the functions of network appliances, such as firewalls, load balancers, and traffic analyzers that work together, to improve network performance.

Data virtualization: Modern organizations collect data from several sources and store it in different formats. They might also store data in different places, such as in a cloud infrastructure and an on-premises data center. Data virtualization creates a software layer between this data and the applications that need it. Data virtualization tools process an application’s data request and return results in a suitable format. Thus, organizations use data virtualization solutions to increase flexibility for data integration and support cross-functional data analysis.

Application virtualization: Application virtualization pulls out the functions of applications to run on operating systems other than the operating systems for which they were designed. For example, users can run a Microsoft Windows application on a Linux machine without changing the machine configuration. To achieve application virtualization, follow these practices:

- Application streaming – Users stream the application from a remote server, so it runs only on the end user's device when needed.
- Server-based application virtualization – Users can access the remote application from their browser or client interface without installing it.
- Local application virtualization – The application code is shipped with its own environment to run on all operating systems without changes.

Application virtualization focuses on encapsulating individual applications and their dependencies in isolated environments, separate from the host operating system. It allows multiple versions of an application to coexist on the same system without conflicts.

Key characteristics of application virtualization

- Isolation: Applications are isolated from the host OS and other applications, reducing conflicts and compatibility issues.
- Compatibility: Legacy applications can be run on modern operating systems through application virtualization.
- Portability: Virtualized applications can be moved between systems with ease.
- Sandboxing: Applications are run in controlled environments, enhancing security.

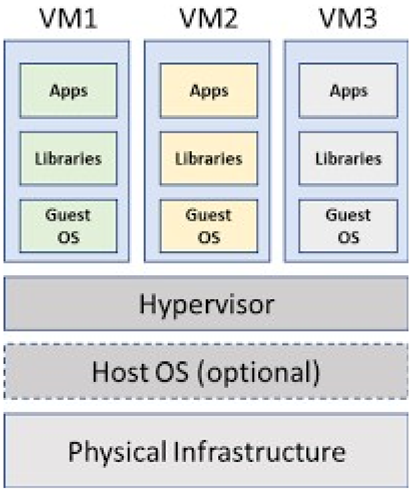
Desktop virtualization: Most organizations have nontechnical staff that use desktop operating systems to run common business applications. For instance, you might have the following staff:

A customer service team that requires a desktop computer with Windows 10 and customer-relationship management software

A marketing team that requires Windows Vista for sales applications

You can use desktop virtualization to run these different desktop operating systems on virtual machines, which your teams can access remotely. This type of virtualization makes desktop management efficient and secure, saving money on desktop hardware. The following are types of desktop virtualization.

Virtualization in cloud infrastructure



Virtual infrastructure components

By separating physical hardware from operating systems, virtualization can provision compute, memory, storage and networking resources across multiple virtual machines (VMs) for greater application performance, increased cost savings and easier management. Despite variances in design and functionality, a virtual infrastructure typically consists of these key components:

- ***Virtualized compute:*** This component offers the same capabilities as physical servers, but with the ability to be more efficient. Through virtualization, many operating systems and applications can run on a single physical server, whereas in traditional infrastructure servers were often underutilized. Virtual compute also makes newer technologies like cloud computing and containers possible.
- ***Virtualized storage:*** This component frees organizations from the constraints and limitations of hardware by combining pools of physical storage capacity into a single, more manageable repository. By connecting storage arrays to multiple servers using storage area networks, organizations can bolster their storage resources and gain more flexibility in provisioning them to virtual machines. Widely used storage solutions include fiber channel SAN arrays, iSCSI SAN arrays, and NAS arrays.
- ***Virtualized networking and security:*** This component decouples networking services from the underlying hardware and allows users to access network resources from a centralized management system. Key security features ensure a protected environment for virtual machines, including restricted access, virtual machine isolation and user provisioning measures.
- ***Management solution:*** This component provides a user-friendly console for configuring, managing and provisioning virtualized IT infrastructure, as well automating processes. A management solution allows IT teams to migrate virtual machines from one physical server to another without delays or downtime, while enabling high availability for applications running in virtual machines, disaster recovery and back-up administration.

Virtual infrastructure architecture

A virtual infrastructure architecture can help organizations transform and manage their IT system infrastructure through virtualization. But it requires the right building blocks to deliver results. These include:

1. **Host:** A virtualization layer that manages resources and other services for virtual machines. Virtual machines run on these individual hosts, which continuously perform monitoring and management activities in the background. Multiple hosts can be grouped together to work on the same network and storage subsystems, culminating in combined computing and memory resources to form a cluster. Machines can be dynamically added or removed from a cluster.
2. **Hypervisor:** A software layer that enables one host computer to simultaneously support multiple virtual operating systems, also known as virtual machines. By sharing the same physical computing resources, such as memory, processing and storage, the hypervisor stretches available resources and improves IT flexibility.
3. **Virtual machine:** These software-defined computers encompass operating systems, software programs and documents. Managed by a virtual infrastructure, each virtual machine has its own operating system called a guest operating system. The key advantage of virtual machines is that IT teams can provision them faster and more easily than physical machines without the need for hardware procurement. Better yet, IT teams can easily deploy and suspend a virtual machine, and control access privileges, for greater security. These privileges are based on policies set by a system administrator.
4. ***User interface:*** This front-end element means administrator can view and manage virtual infrastructure components by connecting directly to the server host or through a browser-based interface.