Virtualization

UNIVERSITÀ CATTOLICA del Sacro Cuore

Definition

“

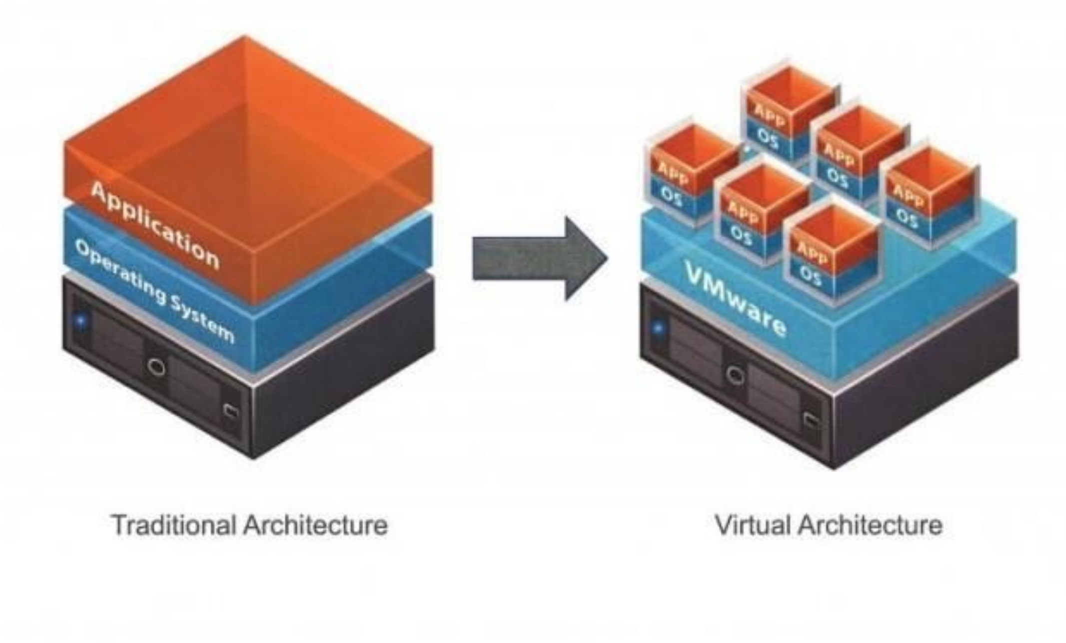
In computing, **virtualization** refers to the act of creating a virtual (rather than actual) version of something, including:

- virtual computer hardware platforms,
- storage devices, and
- computer network resources.

source: https://en.wikipedia.org/wiki/Virtualization

Virtualization and Cloud computing

Virtualizing resources is a central technique for the Cloud computing model



Different types of virtualization

Computing resources can be virtualized.

- **Virtual Machine (VM)**: is an emulation of a computer system. A piece of software “pretends” to be hardware
- OS-level virtualization (a.k.a. **Container**): is an isolated user-space instance within an OS
- **Sandbox**: is a security mechanism for separating running program

Benefits of virtualization (1)

Resource efficiency

Before virtualization, each application server required its own dedicated physical CPU—IT staff would purchase and configure a separate server for each application they wanted to run. (IT preferred one application and one operating system per computer for reliability reasons.) Invariably, each physical server would be underused. In contrast, server virtualization lets you run several applications—each on its own VM with its own OS—on a single physical computer (typically an x86 server) without sacrificing reliability. This enables maximum utilization of the physical hardware's computing capacity.

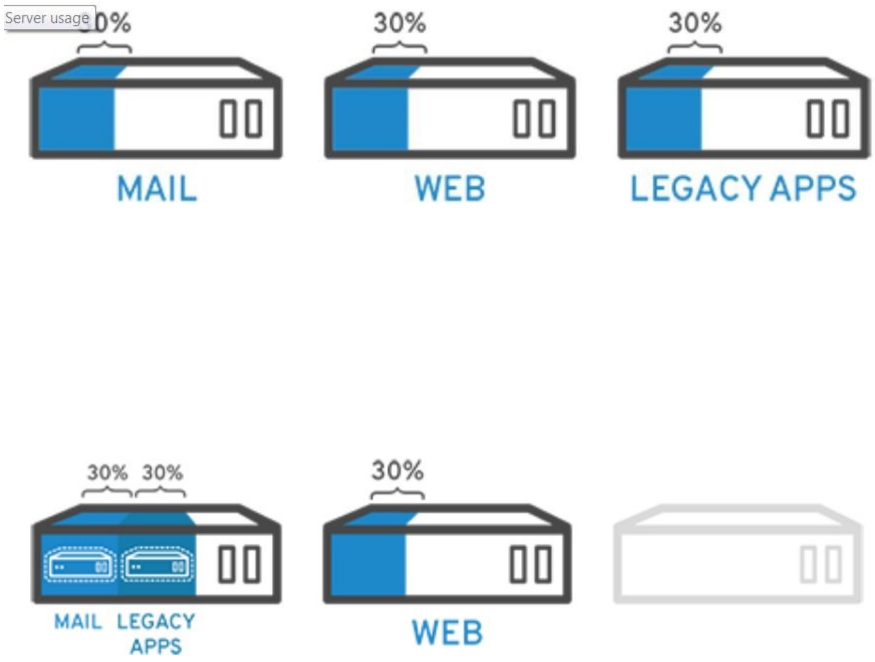
source: https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Server consolidation = resource efficiency

Server consolidation is a top reason to use VMs.

Most operating system and application deployments only use a small amount of the physical resources available when deployed to bare metal.

By virtualizing your servers, you can place many virtual servers onto each physical server to improve hardware utilization.



Benefits of virtualization (2)

Easier management

Replacing physical computers with software-defined VMs makes it easier to use and manage policies written in software. This allows you to create automated IT service management workflows.

For example, automated deployment and configuration tools enable administrators to define collections of virtual machines and applications as services, in software templates. This means that they can install those services repeatedly and consistently without cumbersome, time-consuming. and error-prone manual setup.

Admins can use virtualization security policies to mandate certain security configurations based on the role of the virtual machine. Policies can even increase resource efficiency by retiring unused virtual machines to save on space and computing power.

source: https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Benefits of virtualization (3)

Minimal downtime

OS and application crashes can cause downtime and disrupt user productivity. Admins can run multiple redundant virtual machines alongside each other and failover between them when problems arise. Running multiple redundant physical servers is more expensive.

source: https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Benefits of virtualization (4)

Faster provisioning

Buying, installing, and configuring hardware for each application is time-consuming. Provided that the hardware is already in place, provisioning virtual machines to run all your applications is significantly faster. You can even automate it using management software and build it into existing workflows.

source: https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Virtual Machines (VMs)

A virtual machine is a virtual representation, or emulation, of a physical computer. They are often referred to as a **guest** while the physical machine they run on is referred to as the **host**.

Virtualization makes it possible to create multiple virtual machines, each with their own operating system (OS) and applications, on a single physical machine. A VM cannot interact directly with a physical computer. Instead, it needs a lightweight software layer called a hypervisor to coordinate between it and the underlying physical hardware. The hypervisor allocates physical computing resources—such as processors, memory, and storage—to each VM. It keeps each VM separate from others so they don't interfere with each other.

VMs characteristics

- **Partitioning**
  - Run multiple operating systems on one physical machine.
  - Divide system resources between virtual machines.
- **Isolation**
  - Provide fault and security isolation at the hardware level.
  - Preserve performance with advanced resource controls.
- **Encapsulation**
  - Save the entire state of a virtual machine to files.
  - Move and copy virtual machines as easily as moving and copying files.
- **Hardware Independence**
  - Provision or migrate any virtual machine to any physical server.

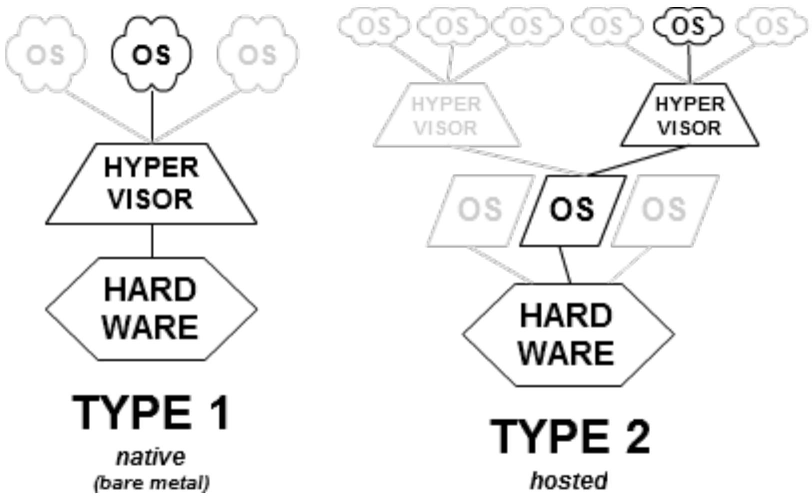
Cloud computing wouldn’t be possible without **virtualization**.

Virtualization wouldn’t be possible without the **hypervisor**.

Hypervisor

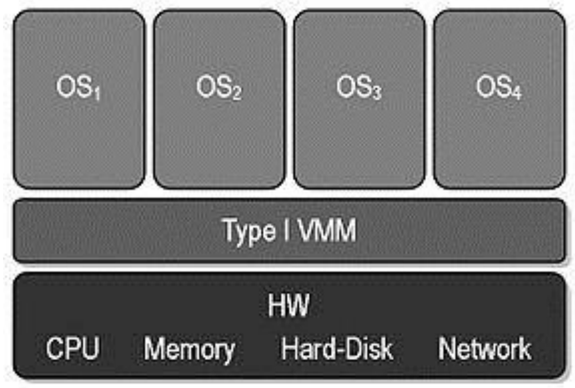
- A hypervisor is software **that creates and runs virtual machines** (VMs). A hypervisor, sometimes called a *virtual machine monitor* (VMM), isolates the host operating system and resources from the virtual machines and enables the creation and management of those VMs.
- The physical hardware, when used as a hypervisor, is called the **host**, while the many VMs that use its resources are **guests**.
- The hypervisor treats resources—like CPU, memory, and storage—as a **pool** that can be easily **reallocated** between existing guests or to new virtual machines.
- All hypervisors need some **operating system-level components**—such as a memory manager, process scheduler, input/output (I/O) stack, device drivers, security manager, a network stack, and more—to run VMs.

Hypervisors: Type-1 and Type-2



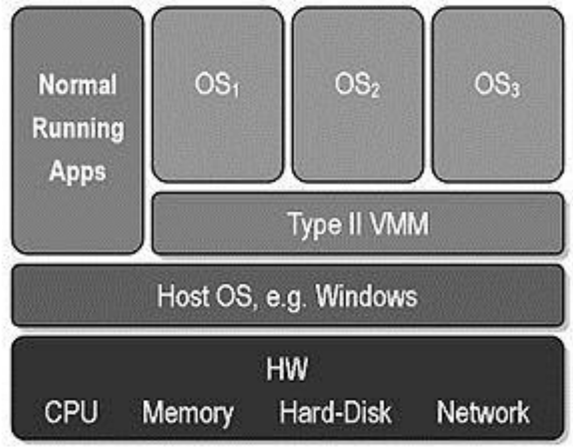
Type 1 hypervisor

- A type 1 hypervisor, also referred to as a native or bare metal hypervisor, runs directly on the host's hardware to manage guest operating systems. It takes the place of a host operating system and VM resources are scheduled directly to the hardware by the hypervisor.
- This type of hypervisor is most common in an enterprise data center or other server-based environments.
- Examples: KVM, Microsoft Hyper-V, and VMware vSphere



Type 2 hypervisor

- A type 2 hypervisor is also known as a hosted hypervisor and is run on a conventional operating system as a software layer or application.
- It works by abstracting guest operating systems from the host operating system. VM resources are scheduled against a host operating system, which is then executed against the hardware.
- A type 2 hypervisor is better for individual users who want to run multiple operating systems on a personal computer.
- Examples: VMware Workstation and Oracle VirtualBox



Hypervisors: pros and cons

Type 1

- **Pros:** Type 1 hypervisors are highly efficient because they have direct access to physical hardware. This also increases their security, because there is nothing in between them and the CPU that an attacker could compromise.
- **Cons:** A Type 1 hypervisor often needs a separate management machine to administer different VMs and control the host hardware.

Type 2

- **Pros:** A Type 2 hypervisor enables quick and easy access to an alternative guest OS alongside the primary one running on the host system. This makes it great for end-user productivity. A consumer might use it to access their favorite Linux-based development tools while using a speech dictation system only found in Windows, for example.
- **Cons:** A Type 2 hypervisor must access computing, memory, and network resources via the host OS, which has primary access to the physical machine. This introduces latency issues, affecting performance. It also introduces potential security risks if an attacker compromises the host OS because they could then manipulate any guest OS running in the Type 2 hypervisor.

Types of virtualization

Many other IT infrastructure elements can be virtualized to deliver significant advantages to IT managers (in particular) and the enterprise as a whole.

- Server virtualization (the one we talked about)
- Desktop virtualization
- Network virtualization
- Storage virtualization
- Data virtualization
- Application virtualization
- Data center virtualization
- CPU virtualization
- GPU virtualization
- …

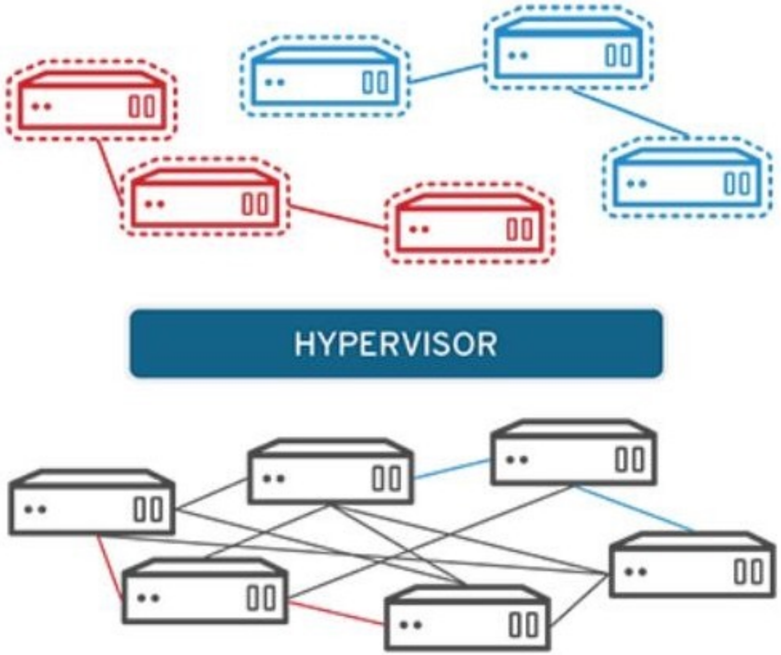
Desktop virtualization

Desktop virtualization lets you run multiple desktop operating systems, each in its own VM on the same computer.

There are two types of desktop virtualization:

- **Virtual desktop infrastructure (VDI)** runs multiple desktops in VMs on a central server and streams them to users who log in on thin client devices. In this way, VDI lets an organization provide its users access to variety of OS's from any device, without installing OS's on any device.
- **Local desktop virtualization** runs a hypervisor on a local computer, enabling the user to run one or more additional OSs on that computer and switch from one OS to another as needed without changing anything about the primary OS.

Network virtualization



Network virtualization uses software to create a "view" of the network that an administrator can use to manage the network from a single console. It abstracts hardware elements and functions (e.g., connections, switches, routers, etc.) and abstracts them into software running on a hypervisor. The network administrator can modify and control these elements without touching the underlying physical components, which dramatically simplifies network management.

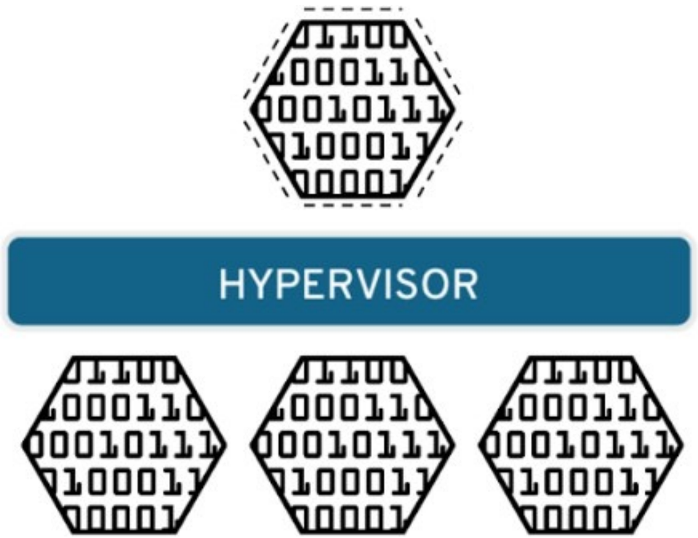
Types of network virtualization include **software-defined networking (SDN)**, which virtualizes hardware that controls network traffic routing (called the "control plane"), and **network function virtualization (NFV)**, which virtualizes one or more hardware appliances that provide a specific network function (e.g., a firewall, load balancer, or traffic analyzer), making those appliances easier to configure, provision, and manage.

Storage virtualization

- Storage virtualization enables all the storage devices on the network— whether they’re installed on individual servers or standalone storage units—to be accessed and managed as a single storage device. Specifically, storage virtualization masses all blocks of storage into a single shared pool from which they can be assigned to any VM on the network as needed. Storage virtualization makes it easier to provision storage for VMs and makes maximum use of all available storage on the network.

Data virtualization

- Modern enterprises store data from multiple applications, using multiple file formats, in multiple locations, ranging from the cloud to on-premise hardware and software systems. Data virtualization lets any application access all of that data—irrespective of source, format, or location.
- Data virtualization tools create a software layer between the applications accessing the data and the systems storing it. The layer translates an application's data request or query as needed and returns results that can span multiple systems. Data virtualization can help break down data silos when other types of integration aren't feasible, desirable, or affordable.



Resources

- https://www.vmware.com/solutions/virtualization.html
- https://www.redhat.com/en/topics/virtualization/what-is-virtualization
- https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Questions, comments?