Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the actual hardware. Most commonly, it refers to running multiple operating systems on a computer system simultaneously. To the applications running on top of the virtualized machine, it can appear as if they are on their own dedicated machine, where the operating system, libraries, and other programs are unique to the guest virtualized system and unconnected to the host operating system which sits below it.

There are many reasons why people utilize virtualization in computing. To desktop users, the most common use is to be able to run applications meant for a different operating system without having to switch computers or reboot into a different system. For administrators of servers, virtualization also offers the ability to run different operating systems, but perhaps, more importantly, it offers a way to segment a large system into many smaller parts, allowing the server to be used more efficiently by several different users or applications with different needs. It also allows for isolation, keeping programs running inside of a virtual machine safe from the processes taking place in another virtual machine on the same host.

Some terminologies associated with Virtualization

* Hypervisor: It is an operating system, performing on the actual hardware, the virtual counterpart is a subpart of this operating system in the form of a running process. Hypervisors are observed as Domain 0 or Dom0.
* Virtual Machine (VM): It is a virtual computer, executing underneath a hypervisor.
* Container: Some light weighted VMs that are subpart of the same operating system instance as its hypervisor are known as containers. They are a group of processes that runs along with their corresponding namespace for process identifiers.
* Virtualization Software: Either be a piece of a software application package or an operating system or a specific version of that operating system, this is the software that assists in deploying the virtualization on any computer device.
* Virtual Network: It is a logically separated network inside the servers that could be expanded across multiple servers.

Characteristics of Virtualization

1. Resource Distribution: Either be a single computer or a network of connected servers, virtualization allows users to make a unique computer environment from one host machine that lets users to restrict the participants as active users, scale down power consumption and easy control.
2. Isolation: Virtualization software involves self-contained virtual machines, these VMs give guest users (not an individual but several instances as applications, operating systems, and devices) an isolated online, virtual environment. This online environment not only defends sensitive knowledge but also allows guest users to remain-connected.
3. Availability: Virtualization software provides various number of features that users won’t obtain at physical servers, these features are beneficial in increasing uptime, availability, fault tolerance, and many more. These features help users to avoid downtime that subverts the users’ efficiencies and productivities and generates security threats and safety hazards.
4. Aggregation: Since virtualization allows several devices to split resources from a single machine, so it can be deployed to join multiple devices into a single potent host. In addition to that, aggregation also demands for cluster management software to connect a homogeneous group of computers or servers collectively for making a unified resource centre.
5. Authenticity and security: At ease, virtualization platforms assure the continuous uptime by balancing load automatically that runs an excessive number of servers across multiple host machines to prevent interruption services.

* Full virtualization

Full virtualization is a common and cost-effective type of virtualization, which is basically a method by which computer service requests are separated from the physical hardware that facilitates them. With full virtualization, operating systems and their hosted software are run on top of virtual hardware. It differs from other forms of virtualization (like paravirtualization and hardware-assisted virtualization) in its total isolation of guest operating systems from their hosts.

Full Virtualization provides a complete simulation of the underlying hardware allowing execution of unmodified operating systems in the virtual machines. It requires that every salient feature of the hardware be reflected into every one of several virtual machines. In Full Virtualization machine language code of the guest OS is converted into the machine language code of the host through a binary translation process.

Diagram

Description automatically generated

* Paravirtualization

Paravirtualization (PV) is an enhancement of virtualization technology in which a guest operating system (guest OS) is modified prior to installation inside a virtual machine (VM) to allow all guest OS within the system to share resources and successfully collaborate, rather than attempt to emulate an entire hardware environment.

The main limitation of PV is the fact that the guest OS must be tailored specifically to run on top of the virtual machine monitor (VMM), the host program that allows a single computer to support multiple, identical execution environments. However, paravirtualization eliminates the need for the virtual machine to trap privileged instructions. Trapping, a means of handling unexpected or unallowable conditions, can be time-consuming and can adversely impact performance in systems that employ full virtualization.

In PV, the guest kernel is modified to run with the hypervisor. This frequently involves removing operations that only run-in ring 0 of the processor with calls to the hypervisor, or hypercalls.

Paravirtualization offers various performance advantages as well as efficiencies that offer improved scaling. It is useful in a variety of technical fields, including:

* disaster recovery.
* capacity management.
* separating test systems and development environments; and
* transferring data from one system to another.
* Partial virtualization

In Partial virtualization multiple instances of an underlying hardware environment are simulated. It is not mandatory that in para virtualization, it simulates hardware. It may provide an API, which can be exceptionally used by altering the guest operating systems. Including this, it has provided various dexterous virtual machines that are compatible to several important applications. In simpler terms, it connotes that the entire operating system cannot run on the Virtual Machine as in case of full virtualization in which many applications can run.

Address space virtualization is one of the forms of partial virtualization, wherein each virtual machine comprises of a dedicated address space. This technology is often considered as an important milestone in the path of full virtualization. Partial virtualization technique was applied on the IBM M44/44X experimental paging system, first-generation time-sharing system CTSS, and systems like MVS and the Commodore 64. It very well confabulates that any OS with specific address spaces for individual users or processes, does not fall in the category of virtual machine systems.

The obligations and user experience with Partial virtualization has led to the development of the first full virtualization system. When compared on ease to impellent, Partial virtualization comes before full virtualization.

For sharing computer resources among multiple users, this technique has provided successful results. When the partial virtualization is compared with full virtualization, its demerit is that in certain situations it requires portability and backward compatibility.

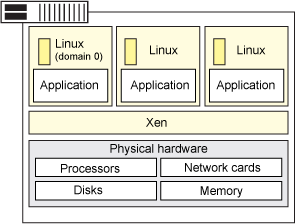
The role of partial virtualization in cloud computing is crucial. First, it is only due to virtualization that a technology like the cloud exists. Second, virtualization also allows segregation of users based on their websites. Means, clouds allow clients to work as if they had their own private server. This is achievable because virtualization treats different VM instances differently.

For example, if there are ten users hosted on a single server, they will continue to enjoy the hosting environ like dedicated server. The idea is to have several virtual servers on a shared platform.



Xen is a type 1 hypervisor that creates logical pools of system resources so that many virtual machines can share the same physical resources.

Xen is a hypervisor that runs directly on the system hardware. Xen inserts a virtualization layer between the system hardware and the virtual machines, turning the system hardware into a pool of logical computing resources that Xen can dynamically allocate to any guest operating system. The operating systems running in virtual machines interact with the virtual resources as if they were physical resources.



Xen is primarily a bare-metal, type-1 hypervisor that can be directly installed on computer hardware without the need for a host operating system. Because it's a type-1 hypervisor, Xen controls, monitors, and manages the hardware, peripheral and I/O resources directly. Guest virtual machines request Xen to provision any resource and must install Xen virtual device drivers to access hardware components. Xen supports multiple instances of the same or different operating systems with native support for most operating systems, including Windows and Linux. Moreover, Xen can be used on x86, IA-32 and ARM processor architecture.

## **Features**

### Full virtualization

Most hypervisors are based on full virtualization which means that they completely emulate all hardware devices to the virtual machines. Guest operating systems do not require any modification and behave as if they each have exclusive access to the entire system.

Full virtualization often includes performance drawbacks because complete emulation usually demands more processing resources (and more overhead) from the hypervisor. Xen is based on paravirtualization; it requires that the guest operating systems be modified to support the Xen operating environment. However, the user space applications and libraries do not require modification.

Operating system modifications are necessary for reasons like:

* So that Xen can replace the operating system as the most privileged software.
* So that Xen can use more efficient interfaces (such as virtual block devices and virtual network interfaces) to emulate devices — this increases performance.

### Xen can run multiple guest OS each in its on VM

Xen can run several guest operating systems each running in its own virtual machine or domain. When Xen is first installed, it automatically creates the first domain, Domain 0 (or dom0).

Domain 0 is the management domain and is responsible for managing the system. It performs tasks like building additional domains (or virtual machines), managing the virtual devices for each virtual machine, suspending virtual machines, resuming virtual machines, and migrating virtual machines. Domain 0 runs a guest operating system and is responsible for the hardware devices.

### Instead of a driver, lots of great stuff happens in the Xen daemon

The Xen daemon, xend, is a Python program that runs in dom0. It is the central point of control for managing virtual resources across all the virtual machines running on the Xen hypervisor. Most of the command parsing, validation, and sequencing happens in user space in xend and not in a driver.

## **Choosing Xen**

On the pro side:

* The Xen server is built on the open source Xen hypervisor and uses a combination of paravirtualization and hardware-assisted virtualization. This collaboration between the OS and the virtualization platform enables the development of a simpler hypervisor that delivers highly optimized performance.
* Xen provides sophisticated workload balancing that captures CPU, memory, disk I/O, and network I/O data; it offers two optimization modes: one for performance and another for density.
* The Xen server takes advantage of a unique storage integration feature called the Citrix Storage Link. With it, the sysadmin can directly leverage features of arrays from such companies as HP, Dell Equal Logic, NetApp, EMC, and others.
* The Xen server includes multicore processor support, live migration, physical-server-to-virtual-machine conversion (P2V) and virtual-to-virtual conversion (V2V) tools, centralized multiserver management, real-time performance monitoring, and speedy performance for Windows and Linux.

On the con side:

* Xen has a relatively large footprint and relies on Linux in dom0.
* Xen relies on third-party solutions for hardware device drivers, storage, backup and recovery, and fault tolerance.
* Xen gets bogged down with anything with a high I/O rate or anything that sucks up resources and starves other VMs.
* Xen’s integration can be problematic; it could become a burden on your Linux kernel over time.