




NEW YORK INSTITUTE OF TECHNOLOGY

INCS 775
Data Center Security

Virtualization and Security – Part 1



Dr. Zakaria Alomari
zalomari@nyit.edu

Objectives

- ❑ Definition of Virtualization
- ❑ Definition of a Hypervisor
- ❑ Type 1 vs, Type 2 Hypervisors
- ❑ Server Virtualization
- ❑ Pros and Cons of dedicated Server and virtual server

What is virtualization?

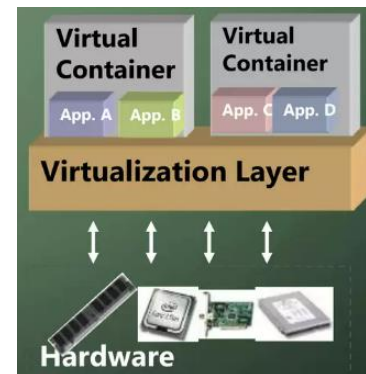
- **Virtualization** is a technology of creating a **virtual version**, **representation** of true underlying hardware or software, such as an operating system, computer program, servers, storage device, and networks.
- Therefore, **virtualization** improves **IT resource utilization** by dividing of physical resources into one or more execution environments, which means **users**, **applications**, and **devices** are **able to cooperate with the virtual resource** as if it were an actual single logical resource.

What is virtualization?

- Virtualization is a broad term(*virtual memory, storage, network, etc*)
 - Basically allows one computer to do the job of multiple computers, by sharing the resources of a single hardware across multiple environment.



Nonvirtualized system
A single OS controls all hardware platform resources



Virtualized system
It makes it possible to run multiple Virtual Containers on a single physical platform

Describing a Hypervisor

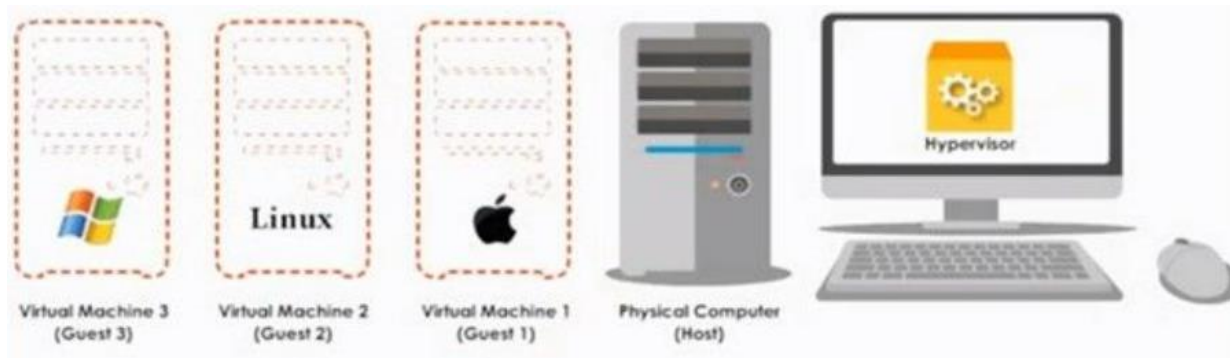


A physical machine is a computer, like this Windows. It has a **CPU**, **memory**, **hard-disk**, and **network connection**.



In the context of virtualization, the physical computer is called a “**host**”. Virtualization is the process of using special software on a physical machine – to create virtual machines.

Describing a Hypervisor

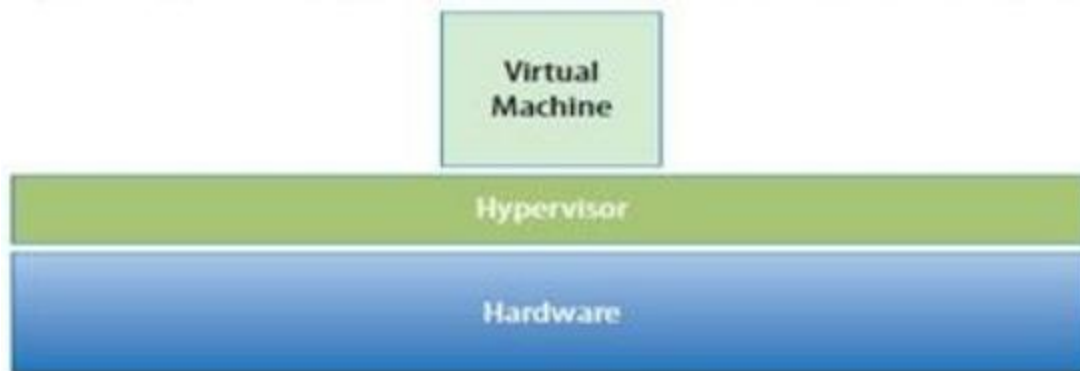


*This special software is called “**hypervisor**”.*
*A virtual machine (VM) is called a “**guest**”*

Describing a Hypervisor

The hypervisor

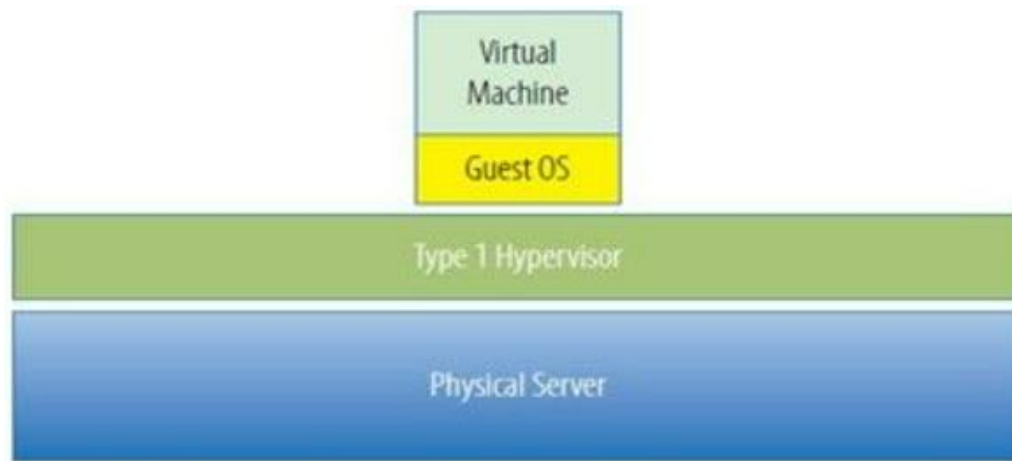
- Is the **key** to **enabling virtualization**,
- It's **software** installed on **top of computer hardware**,
- Creating the **virtualization layer**,
- Acting as a **platform** for the **VMs to be created on**,
- It **manages** the **sharing of physical resources** into **virtual**



Hypervisor is a layer of software that resides below the virtual machines and above the hardware

Two Types of Hypervisors

A **Type 1 hypervisor** runs directly on the **server hardware** without an **operating system** beneath it. Because there is no other **intervening layer of software** between the **hypervisor** and the **physical hardware**, this is also referred to as a **bare-metal implementation**. Without an intermediary.

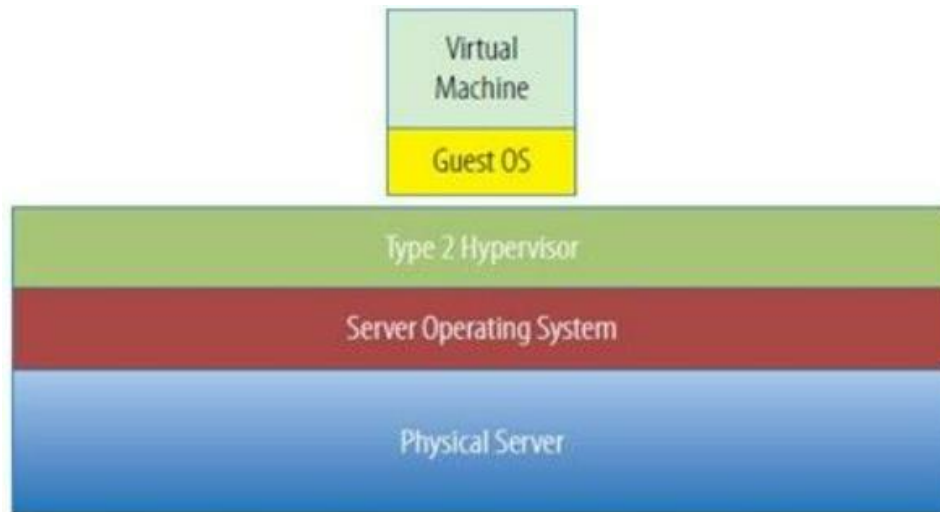


A Type 1 hypervisor

*Example of Type 1 hypervisor include **VMware ESX**, **Microsoft Hyper-V**, and the many Xen variants.*

Two Types of Hypervisors

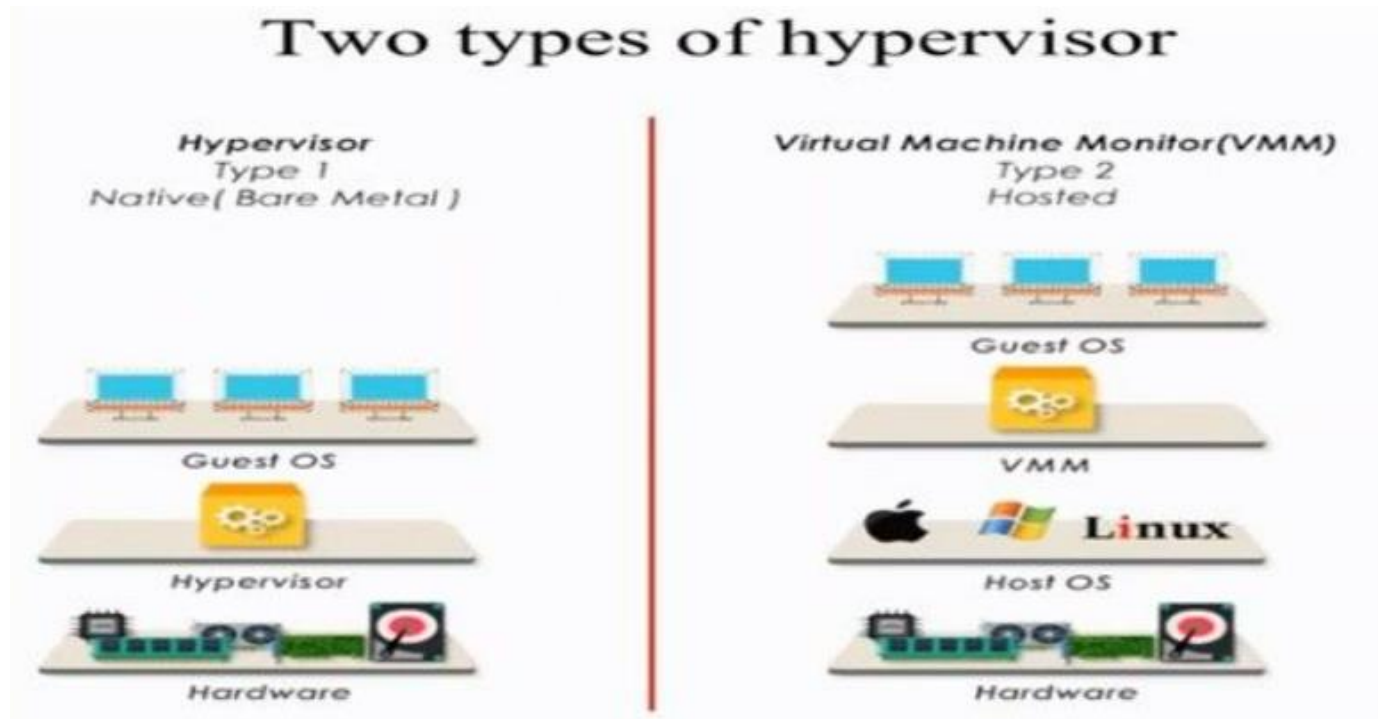
A **Type 2 hypervisor** itself is an application that runs a top of traditional operating system, this is also referred to as a hosted.



A Type 2 hypervisor

VMware Player, VMware Workstation, and Microsoft Virtual Sever are examples of Type 2 hypervisors.

Hypervisor Type 1 VS. Type 2

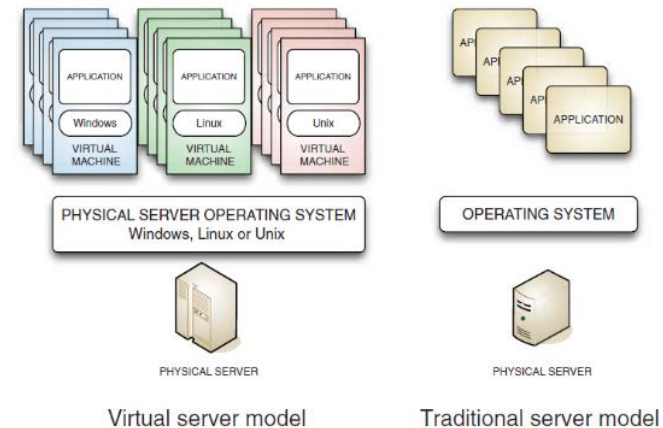


Example of Hypervisors

- Type 1 Hypervisor (*Loaded directly on the hardware*)
 - VMware ESX/ESXi
 - Hyper-v
 - XenServer
- Type 2 Hypervisor (*Loaded in an OS running on the hardware*)
 - VMware Fusion
 - Oracle Virtualbox
 - VMware Workstation

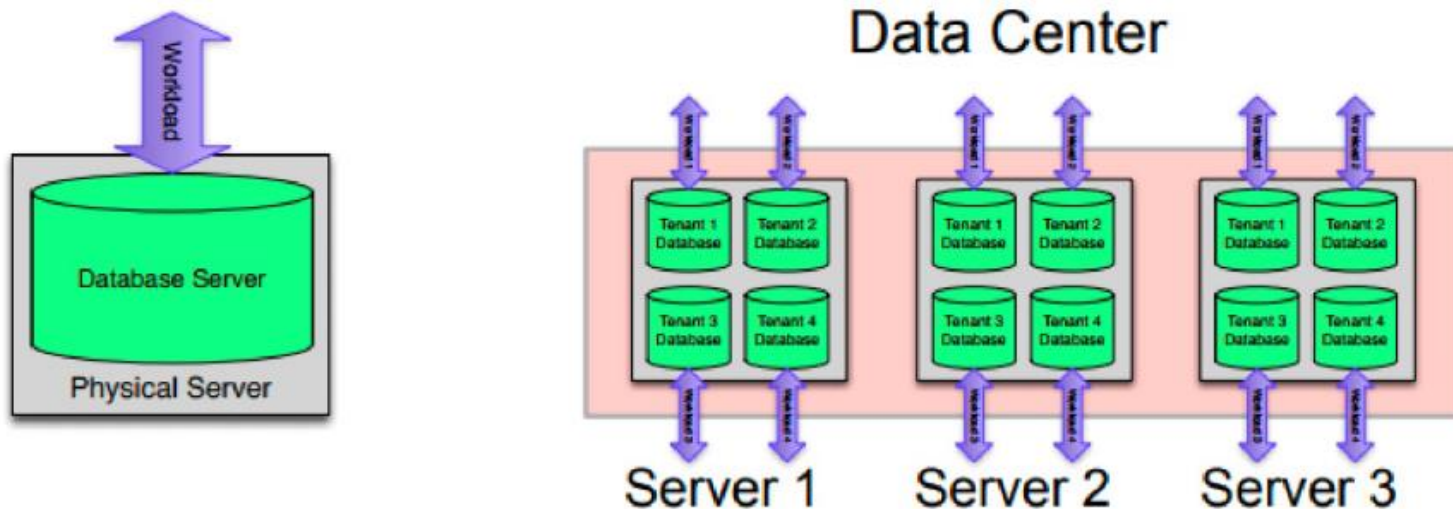
Server Virtualization

- Allows a **server** to be “sliced” into **Virtual Machines (VMs)**
- VM has own **OS/applications**
- Rapidly **adjust resource allocation**
- Each **virtual machine acts like it owned the whole physical machine**, including a **virtual CPU, virtual memory, virtual storage and so on.**
- Each virtual machine has an **operating system** also called "**guest operating system**", those operating systems communicate with hardware by **Virtual Machine Manager (VMM)**.
- Each **guest operating system** handles its own **applications as it normally does in a non-virtual environment**, exclude that it has been isolated in the physical machine by the **VMM**.



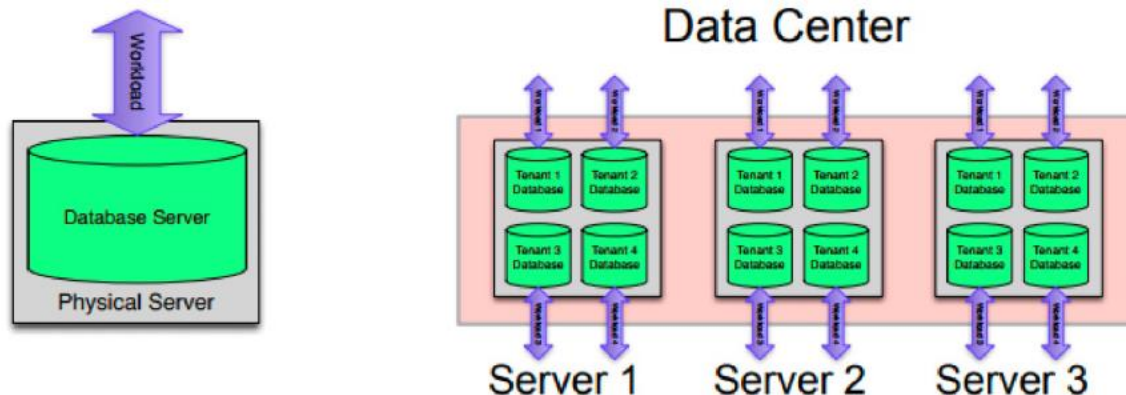
Example: Virtualized DB Servers

- **Conventional**: one physical server, one database sever
- **Data Center**: multiple physical servers, multiple database servers per (virtualized) physical server.



Example: Virtualized DB Servers

- Virtualized database servers refer to database servers that are hosted on virtual machines (VMs) rather than on physical servers.
- This approach leverages virtualization technology to create multiple virtual instances of servers on a single physical machine, thereby optimizing resource utilization and providing flexibility in managing database environments.



Pros and Cons of Server Virtualization

- Pros
 - Cost
 - Less physical servers
 - Less server space (consolidation of servers)
 - Less energy costs
 - Less maintenance
 - Efficient Administration
 - Easier management, management through one machine
 - Smaller IT staff

Pros and Cons of Server Virtualization

- Pros

- Growth and Scalability

- Upgrading one server upgrade them all
 - Easy growth

- Security

- Single server security maintenance
 - Hypervisor software often provides security benefits

Pros and Cons of Server Virtualization

- Cons

- Slow Performance

- High stress on single machine
 - Longer processing times
 - More network bottlenecking

- Single point of Failure

- Many servers on one host machine
 - Hardware or software failures can be critical
 - Backup servers will need to be setup

Pros and Cons of Server Virtualization

- Cons
 - Cost
 - High initial investment
 - Software licensing costs
 - Security
 - All servers through one machine
 - Learning curve
 - Many different types of software
 - Different architecture

Pros and Cons of Dedicated Servers

- Pros
 - High Performance
 - All resources on server are dedicated
 - Can handle high stress scenarios
 - Multiple Points of failure
 - Easier to identify problems
 - Only one server will fail at a time

Pros and Cons of Dedicated Servers

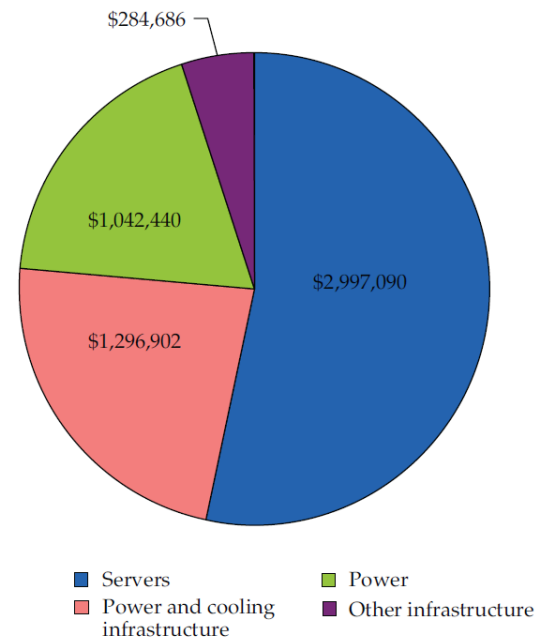
- Pros
 - Price
 - Old servers already exist
 - No long term investments
 - If it's not broke, don't fix it
 - Small Learning Curve
 - Dedicated servers have been around for a long time
 - IT staff will not need to learn any new systems if dedicated servers already exist.

Pros and Cons of Dedicated Servers

- Cons
 - Price
 - Long term costs of dedicated servers can add up
 - More applications and services = more servers
 - Servers not being utilized
 - Servers may not be efficient
 - Even at peak, some servers may not need all resources

Data Center Costs

- Running a data center is **expensive**
- As can be seen from this figure, **energy related costs including three parts: direct power consumption, power infrastructure, and cooling infrastructure** amount to **41.62%** of the total.
- In other words, **the largest investment to build data centers for cloud computing** is not only to purchase thousands of server equipment, but also to **buy the distribution and cooling infrastructure and to pay the bill for energy consumption of all these facilities.**



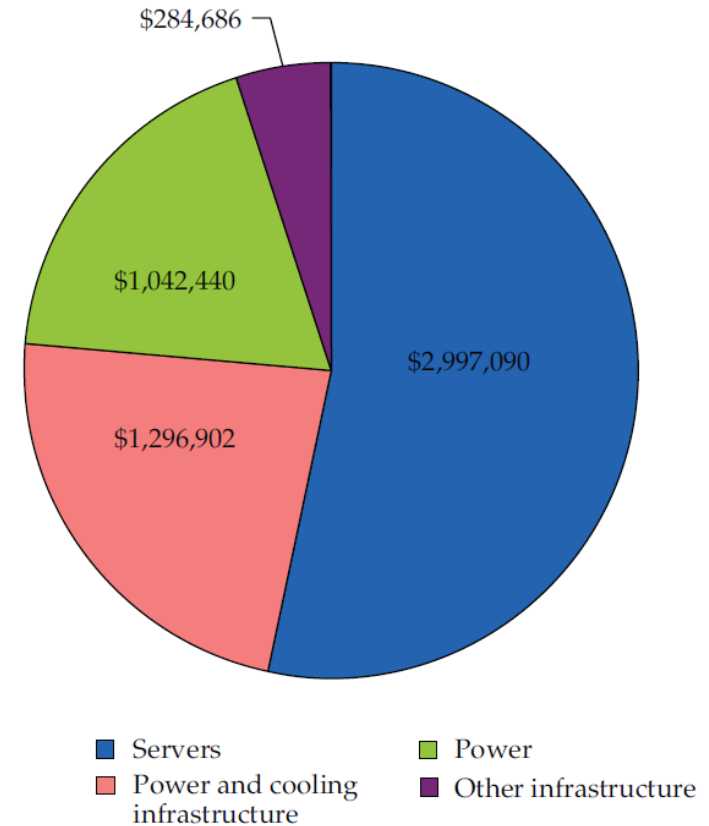
Data Center Costs

- Running a data center is expensive

Amortized Cost	Component	Sub-Components
~45%	Servers	CPU, memory, storage systems
~25%	Infrastructure	Power distribution and cooling
~15%	Power draw	Electrical utility costs
~15%	Network	Links, transit, equipment

Guide to where costs go in the data center

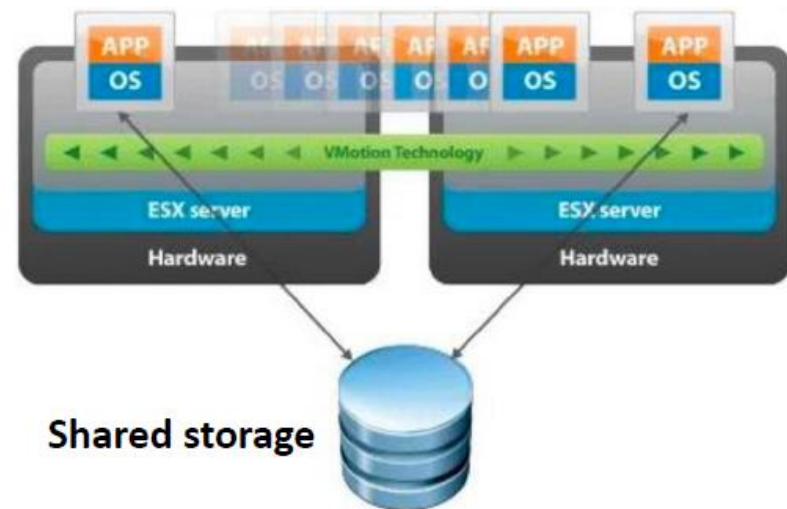
https://www.researchgate.net/figure/Monthly-costs-of-the-data-center_fig3_258385511



Monthly costs of the data center.

VM Live Migration

- **VM live migration** is a feature provided by **virtualization platforms** that allows a **running virtual machine (VM)** to be moved from **one physical host** to **another** without any **noticeable downtime** or **disruption** to the **VM's operation**.

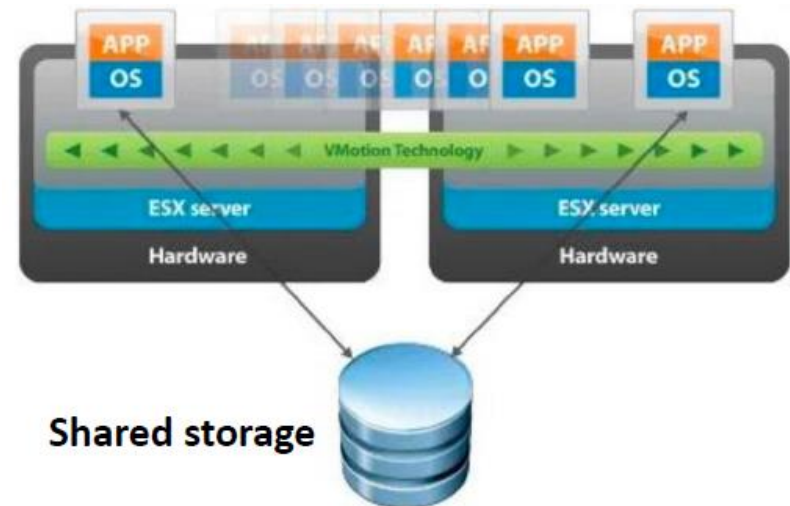


VM Live Migration

- Live migration of running virtual machines from one physical server to another are useful for:
 - Hardware maintenance
 - Performance and optimizes resource usage
 - Load balancing across physical
 - Disaster recovery

*VMotion on ESX server handles the VM Migration among servers **with shared storage**.*

*• SVMotion on ESX server handles the VM Migration among servers **without shared storage**.*



VM Live Migration

❑ vMotion:

- **Purpose:** vMotion is used to migrate a running virtual machine (VM) from one physical host to another within the same cluster or datacenter without downtime.
- **Process:** During a vMotion migration, the VM's memory state, CPU state, and network connections are transferred from the source host to the destination host. The storage remains unchanged, meaning the VM continues to use the same datastore.
- **Use Case:** This is useful for load balancing, hardware maintenance, and minimizing downtime during host upgrades or failures.

VM Live Migration

❑ Storage vMotion (SVMotion):

- **Purpose:** Storage vMotion is used to migrate a running VM's disk files from one datastore to another without downtime.
- **Process:** During a Storage vMotion migration, the VM's disk files are moved to a different datastore while the VM continues to run. This migration is transparent to the users and does not affect the VM's operations.
- **Use Case:** This is useful for storage maintenance, performance optimization, and freeing up space on a datastore.

VM Live Migration

Key Differences:

❑ Target of Migration:

- **vMotion:** Migrates the VM's compute resources (memory and CPU) to a different host.
- **Storage vMotion:** Migrates the VM's storage (disk files) to a different datastore.

❑ Component Moved:

- **vMotion:** Moves the in-memory state and CPU state.
- **Storage vMotion:** Moves the virtual disks and configuration files.

VM Live Migration

❑ Network Impact:

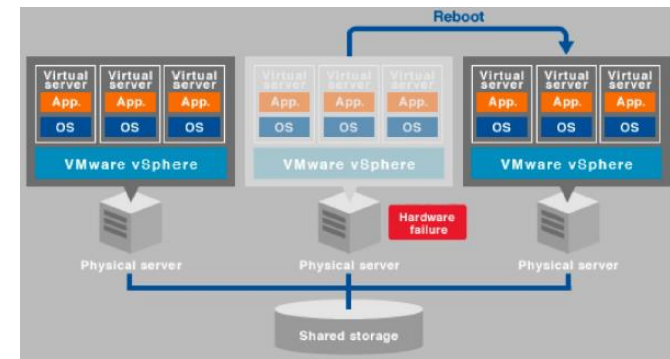
- **vMotion:** Requires a high-speed network connection between the source and destination hosts.
- **Storage vMotion:** Requires high-speed connectivity between datastores but does not impact the VM's network connections.

❑ Typical Use Cases:

- **vMotion:** Load balancing, hardware maintenance, minimizing downtime for host upgrades.
- **Storage vMotion:** Storage maintenance, performance tuning, managing datastore space.

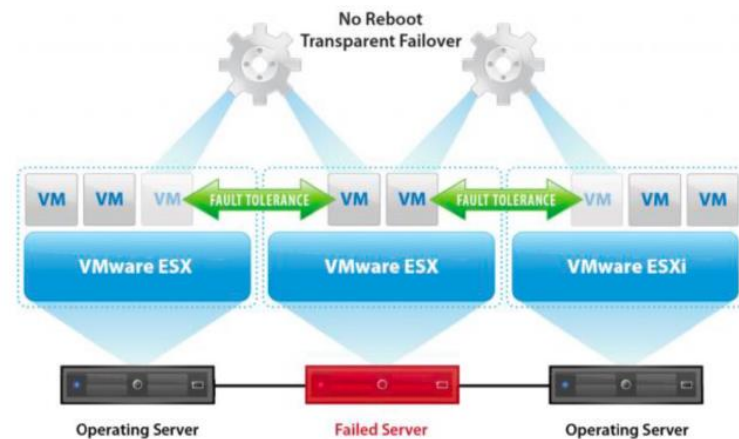
High availability

- High availability (HA) in a data center refers to the ability of an IT infrastructure to maintain continuous operation and ensure uninterrupted access to critical services and applications, even in the event of hardware failures, network outages, or other disruptions.
- If a 15-second period elapses without the receipt of heartbeats from host, and the host cannot be pinged, it is declared as a failed.
- In the event of a host failure, the virtual machines running on the host are failed over, that is restarted on alternate hosts



Fault Tolerance

- **Fault Tolerance** provides a higher level of business continuity than VMware HA (High Availability).
- When a Secondary VMs is called upon replace its Primary VM counterpart, the Secondary VM immediately takes over the primary VM's role with the entire of the virtual machine preserved.



High availability VS Fault Tolerance

- ❑ **High Availability (HA)** aims to **minimize downtime** by using **redundant components** and **failover mechanisms**, allowing for brief interruptions when switching to backup systems.
- ❑ **Fault Tolerance (FT)** **aims for zero downtime** by providing **complete redundancy and real-time synchronization**, ensuring continuous operation without any interruptions even when components fail.
- ❑ HA is generally less expensive and less complex than FT, which requires more resources and sophisticated systems to achieve uninterrupted service.

Different Types of Virtualization

- Desktop Virtualization
- Application Virtualization
- Storage Virtualization
- Network Virtualization
- I/O Virtualization
- CPU Virtualization
- Memory Virtualization