SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY

Department Of Computer Science & Engineering
&
Department Of Information Technology

COURSE MATERIAL

Subject Name : Cloud Computing **Subject Code : SIT1304**

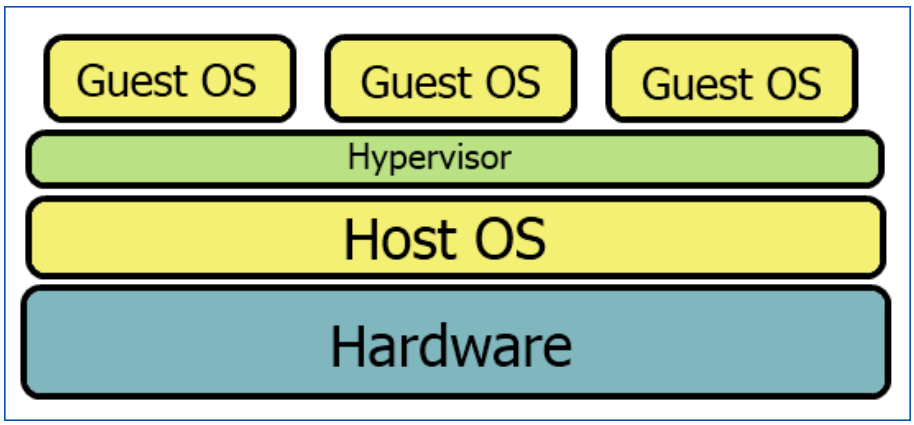
Unit – III – Cloud Deployment Models

1. Hypervisor

a. Introduction

- A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines.
- A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.
- The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems.
- Multiple instances of a variety of operating systems may share the virtualized hardware resources.
- Example - Linux, Windows, and macOS instances can all run on a single physical x86 machine.
-

b. Architecture



c. Types of Hypervisor

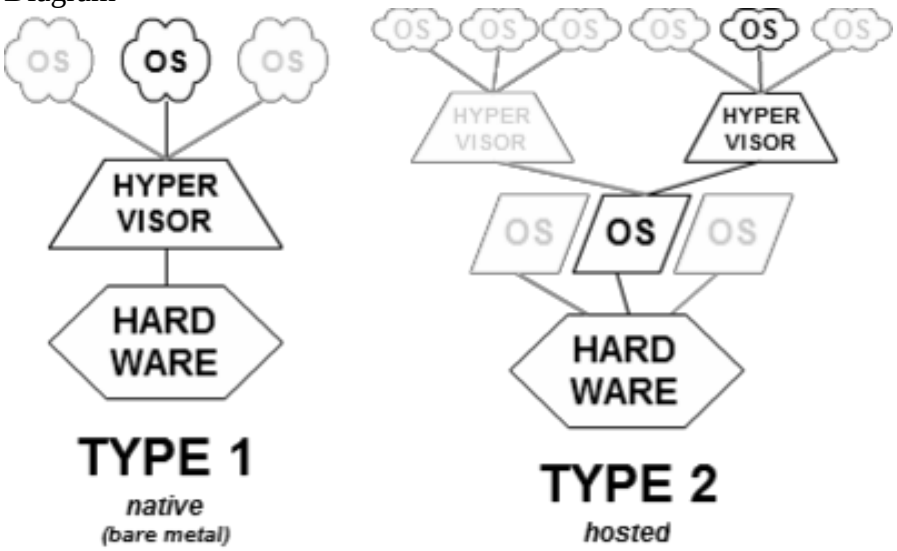
- Type-1, native or bare-metal hypervisors

1. These hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems.
2. The first hypervisors, which IBM developed in the 1960s, were native hypervisors.
3. Example - Xen, Oracle VM Server for SPARC, Oracle VM Server for x86, Microsoft Hyper-V and VMware ESX/ESXi.

- Type-2 or hosted hypervisors

1. These hypervisors run on a conventional operating system (OS) just as other computer programs do. A guest operating system runs as a process on the host.
2. Example - VMware Workstation, VMware Player, VirtualBox, Parallels Desktop for Mac and QEMU

- Diagram

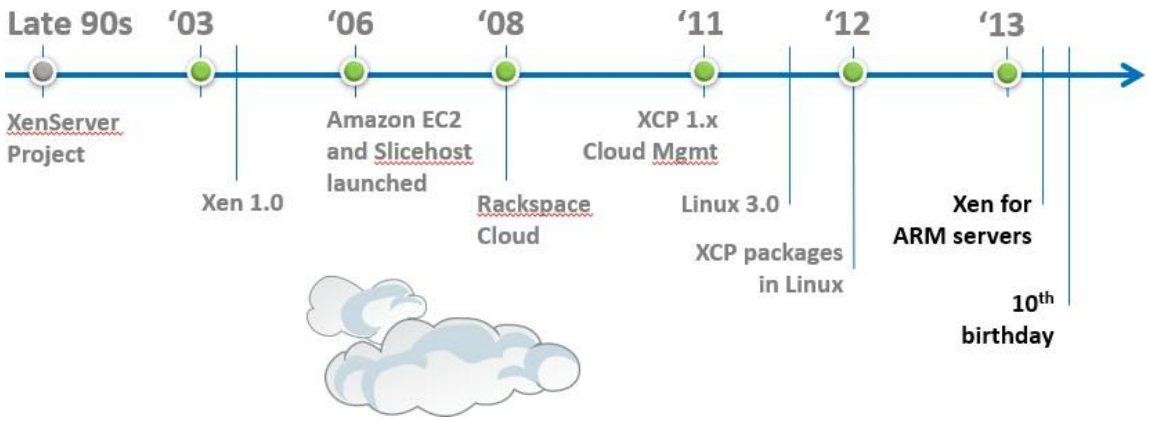


2. Xen

a. Introduction

- The Xen Project hypervisor runs directly on the hardware and is responsible for handling CPU, Memory, and Interrupts.
- It is the first program running after exiting the bootloader.
- On top of the hypervisor run a number of virtual machines.
- A running instance of a virtual machine is called a domain or guest.

b. A Brief History of Xen in the Cloud



c. Xen.org

- Guardian of Xen Hypervisor and related OSS Projects
- Xen Governance similar to Linux Kernel

1. Plus project lifecycle and Project Management Committee (PMC)

- Projects

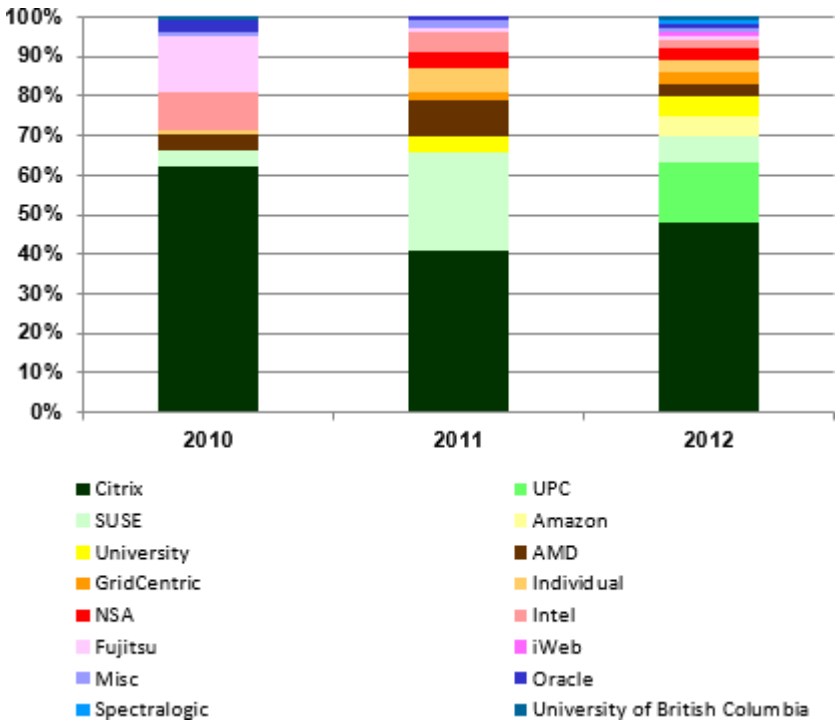
1. Xen Hypervisor (led by 5 committers, 2 from Citrix, 1 from Suse, 2 Independent)
2. Xen Cloud Platform aka XCP (led by Citrix)

3. Xen ARM : Xen for mobile devices (led by Samsung)

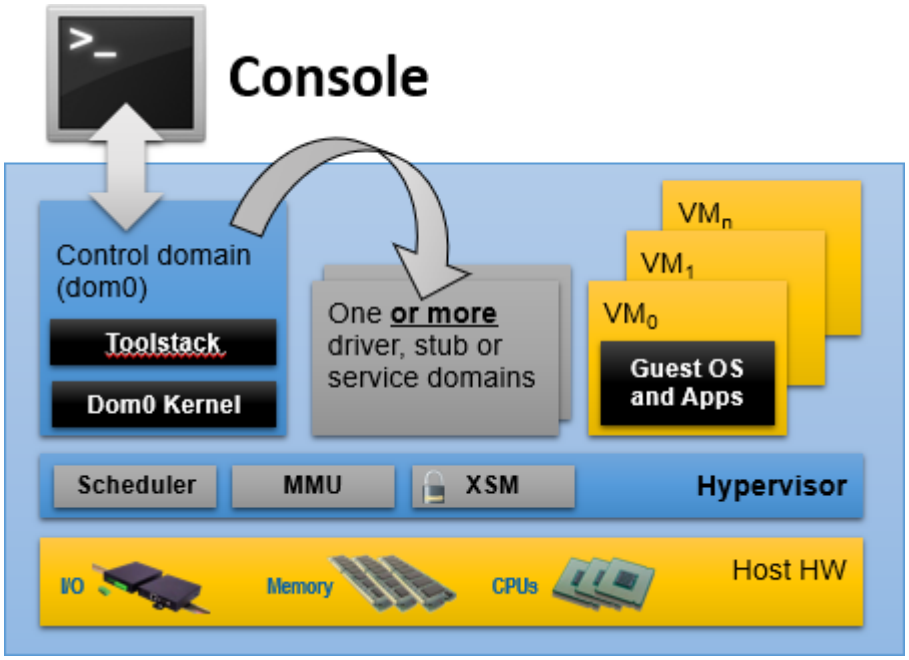
d. Xen contributor community is diversifying

- The number of "significant" active vendors is increasing

- New feature development driving new participation
- Diagram



e. Architecture



- Console
  1. Interface to the outside world
- Control Domain aka Dom0
  1. Dom0 kernel with drivers
  2. Xen Management Toolstack
- Guest Domains
  1. Your apps

- Driver/Stub/Service Domain(s)
    1. A “driver, device model or control service in a box”
    2. De-privileged and isolated
    3. Lifetime: start, stop, kill
- Xen Hypervisor is not in the Linux kernel
- BUT: everything Xen and Xen Guests need to run is!
- Xen packages are in all Linux distros (except RHEL6)
    1. Install Dom0 Linux distro
    2. Install Xen package(s) or meta package
    3. Reboot
    4. Config stuff: set up disks, peripherals, etc.

3. VMware

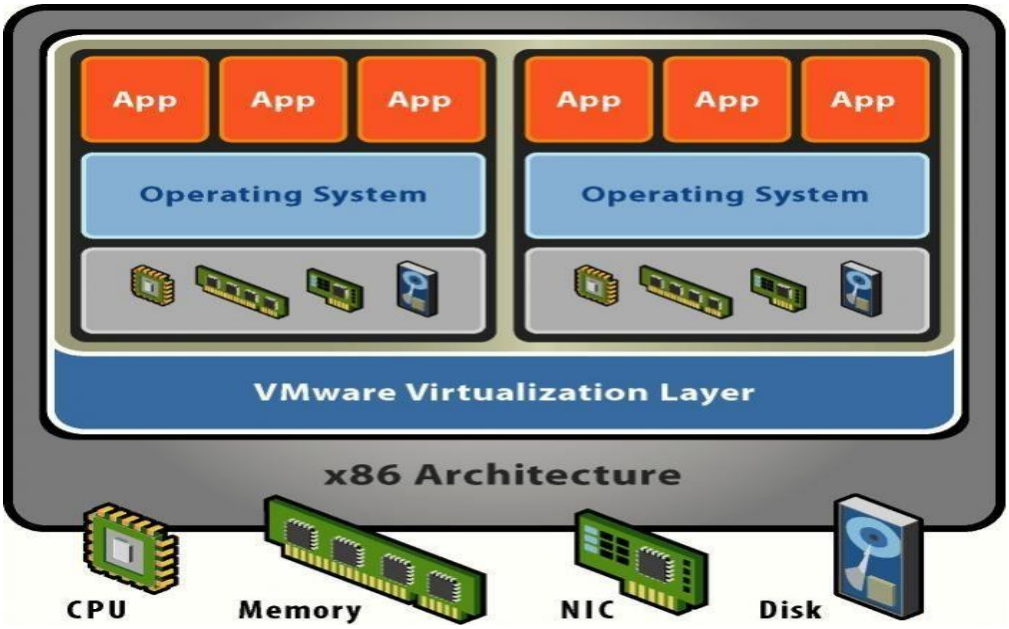
a. Introduction

- VMware is a virtualization and cloud computing software provider based in Palo Alto, California.
- Founded in 1998, VMware is a subsidiary of Dell Technologies.
- EMC Corporation originally acquired VMware in 2004; EMC was later acquired by Dell Technologies in 2016.
- VMware bases its virtualization technologies on its bare-metal hypervisor ESX/ESXi in x86 architecture.
- With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server.
- Each VM can run its own operating system (OS), which means multiple OSes can run on one physical server.
- All of the VMs on the same physical server share resources, such as networking and RAM.
- VMware is a company that was established in 1998 and provides different software and applications for virtualization.
- It has become one of the key providers of virtualization software in the industry.
- VMware’s products can be categorized in two levels:
    1. desktop applications
    2. server applications
- VMware was founded in 1998 by five different IT experts.
- The company officially launched its first product, VMware Workstation, in 1999, which was followed by the VMware GSX Server in 2001. The company has launched many additional products since that time.
- VMware's desktop software is compatible with all major OSs, including Linux, Microsoft Windows, and Mac OS X.
- VMware provides three different types of desktop software:
    1. VMware Workstation: This application is used to install and run multiple copies or instances of the same operating systems or different operating systems on a single physical computer machine.

2. VMware Fusion: This product was designed for Mac users and provides extra compatibility with all other VMware products and applications.
3. VMware Player: This product was launched as freeware by VMware for users who do not have licensed VMWare products. This product is intended only for personel use.

- VMware's software hypervisors intended for servers are bare-metal embedded hypervisors that can run directly on the server hardware without the need of an extra primary OS.
- VMware's line of server software includes:
  1. VMware ESX Server: This is an enterprise-level solution, which is built to provide better functionality in comparison to the freeware VMware Server resulting from a lesser system overhead. VMware ESX is integrated with VMware vCenter that provides additional solutions to improve the manageability and consistency of the server implementation.
  2. VMware ESXi Server: This server is similar to the ESX Server except that the service console is replaced with BusyBox installation and it requires very low disk space to operate.
  3. VMware Server: Freeware software that can be used over existing operating systems like Linux or Microsoft Windows.

b. Vmware Architecture



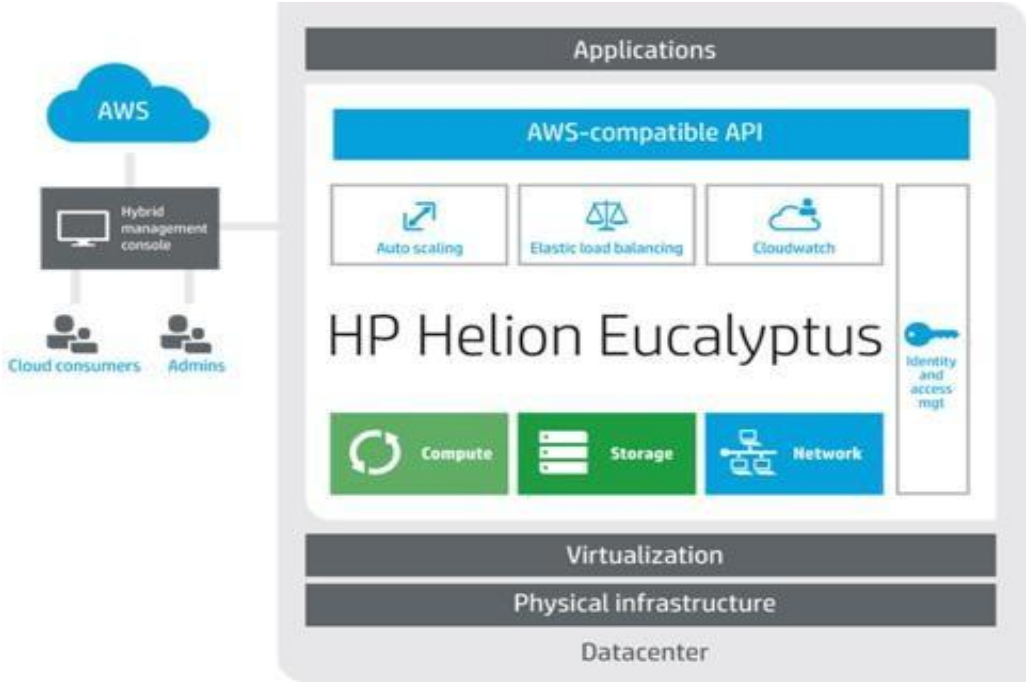
4. Eucalyptus

a. Introduction

- Eucalyptus is a paid and open-source computer software for building Amazon Web Services (AWS)-compatible private and hybrid cloud computing environments, originally developed by the company Eucalyptus Systems.
- Eucalyptus is an acronym for Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems.

- Eucalyptus enables pooling compute, storage, and network resources that can be dynamically scaled up or down as application workloads change.
- Marten Mickos was the CEO of Eucalyptus.
- In September 2014, Eucalyptus was acquired by Hewlett-Packard and then maintained by DXC Technology.
- On-premise IaaS software
    1. Runs on top of Linux on your own hardware
    2. Numerous control components work together with nodes (virtual hosts) to create a cloud
    3. Commodity hardware focus; abstracts away physical infrastructure into a service-orientated platform
- Open Source
    1. Freely available
    2. downloads.eucalyptus.com
- Subscription-based business model
    1. Support tiers with global coverage
    2. Subscription-only add-ons
- First software release in 2008
- Incorporated in 2009
-

b. Architecture

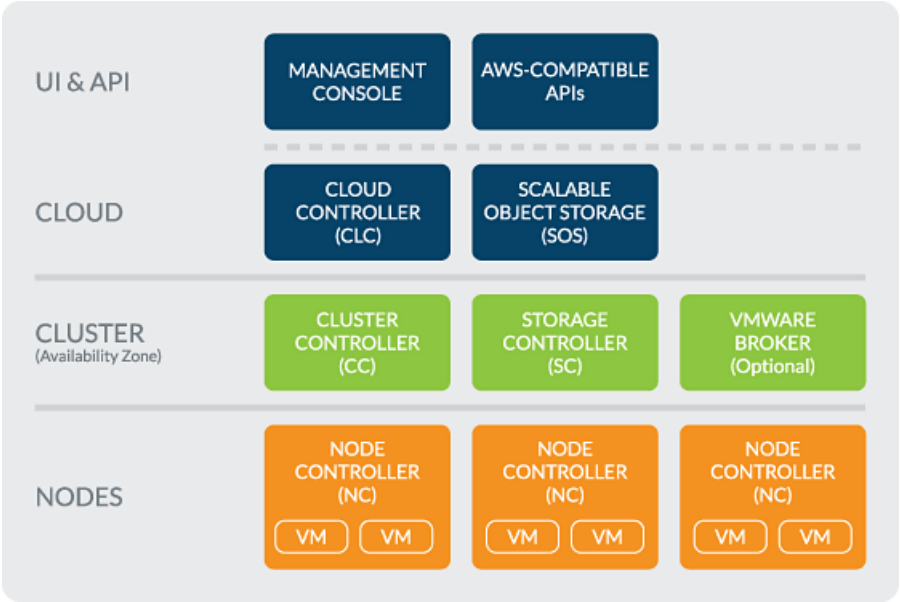


- Images – An image is a fixed collection of software modules, system software, application software, and configuration information.
- When bundled and uploaded to the Eucalyptus cloud, this becomes a Eucalyptus machine image (EMI).
- Instances – When an image is put to use, it is called an instance. The configuration is executed at runtime, and the Cloud Controller decides where the image will run, and storage and networking is attached to meet resource needs

- IP addressing – Eucalyptus instances can have public and private IP addresses. An IP address is assigned to an instance when the instance is created from an image.
- Security – TCP/IP security groups share a common set of firewall rules. This is a mechanism to firewall off an instance using IP address and port block/allow functionality.
- Networking – There are three networking modes. In Managed Mode Eucalyptus manages a local network of instances, including security groups and IP addresses.
- Access Control – A user of Eucalyptus is assigned an identity, and identities can be grouped together for access control.
- Autoscaling – Allows application developers to scale Eucalyptus cloud resources up or down in order to maintain performance and meet SLAs. With auto-scaling, developers can add instances and virtual machines as traffic demands increase.
- Elastic Load Balancing – A service that distributes incoming application traffic and service calls across multiple Eucalyptus workload instances, providing greater application fault tolerance.
- CloudWatch – A monitoring tool similar to Amazon CloudWatch that monitors resources and applications on Eucalyptus clouds. It enables cloud users to view, collect and analyze metrics of their could resources.
- CloudWatch Alarm - currently helps cloud users to take decisions on the resources (e.g instances, EBS volumes, Auto Scaling instances, ELBs) automatically based on the rules defined by the users based on the metrics. Eucalyptus CloudWatch alarm currently works with Auto Scaling policies.
-

c. The Components

- Diagram



- The Cloud Controller (CLC) is a Java program that offers EC2-compatible interfaces, as well as a web interface to the outside world.

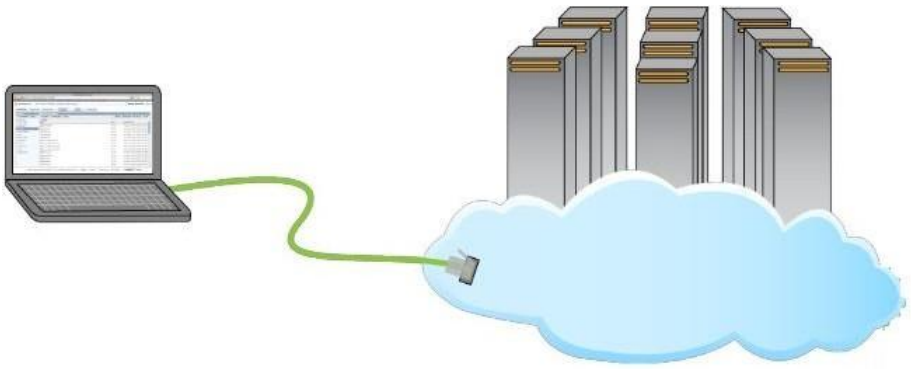
- Only one CLC can exist per cloud and it handles authentication, accounting, reporting, and quota management.
- The Cluster Controller (CC) is written in C and acts as the front end for a cluster within a Eucalyptus cloud and communicates with the Storage Controller and Node Controller. It manages instance (i.e., virtual machines) execution and Service Level Agreements (SLAs) per cluster.
- The Storage Controller (SC) is written in Java and is the Eucalyptus equivalent to AWS EBS. It communicates with the Cluster Controller and Node Controller and manages Eucalyptus block volumes and snapshots to the instances within its specific cluster.
- The VMware Broker is an optional component that provides an AWS-compatible interface for VMware environments and physically runs on the Cluster Controller.
- The Node Controller (NC) is written in C and hosts the virtual machine instances and manages the virtual network endpoints.

d. Features
   - Compute
     1. Virtual Machine (instance) provisioning
     2. AutoScaling of instance groups
     3. Metric collection of VMs
     4. Image/template ingress
   - Storage
     1. Network-attached block storage for instances
     2. General purpose scalable object storage
   - Network
     1. Dynamic and flexible IP addresses allocation
     2. Flexible network topologies
     3. Instance network isolation
     4. Load Balancing for instances
   - Resource Management
     1. Accounts, user and group management
     2. AD/LDAP sync
     3. Quotas and resource access
   - Interface
     1. GUI Management Console
     2. AWS compatible API and services
     3. AWS ecosystem tools
   - Administration
     1. Easy to install
     2. Reporting
     3. Detailed component logging

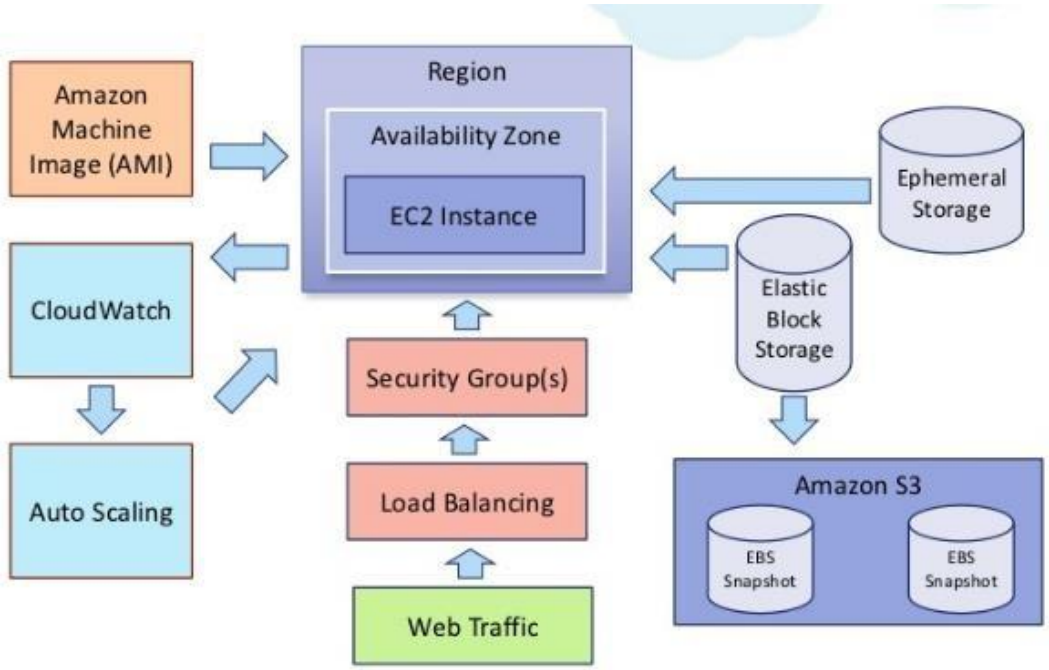
5. Amazon EC2

a. Introduction

- Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.
- It is designed to make web-scale cloud computing easier for developers.
- EC2 allow users to use virtual machines of different configurations as per their requirement.
- Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction.
- Amazon Web Services is a cloud computing platform that provides flexible, scalable, and cost-effective technology infrastructure for businesses of all sizes around the world.
- Diagram



b. Amazon EC2 Architecture



- Load Balancing
  1. It means to hardware or software load over web servers, that improver's the efficiency of the server as well as the application.
- Elastic Load Balancing

1. It can dynamically grow and shrink the load-balancing capacity to adjust to traffic demands and also support sticky sessions to address more advanced routing needs.

- Auto Scaling
    1. It is particularly effective for those applications that fluctuate on hourly, daily, or weekly usage.
    2. Auto Scaling is enabled by Amazon CloudWatch and is available at no extra cost.
    3. AWS CloudWatch can be used to measure CPU utilization, network traffic, etc.
- Web traffic
    1. Web traffic is the amount of data sent and received by visitors to a website.
- AMI (Amazon Machine Image)
    1. An Amazon Machine Image (AMI) is a special type of virtual appliance that is used to create a virtual machine within the Amazon Elastic Compute Cloud ("EC2").
    2. It serves as the basic unit of deployment for services delivered using EC2.
- Amazon S3 (Simple Storage Service)
    1. It has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web.
    2. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites.
- Amazon CloudWatch
    1. It is a monitoring service for AWS cloud resources and the applications you run on AWS.
    2. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

c. EC2 Components

- Operating System Support
    1. Amazon EC2 supports multiple OS in which we need to pay additional licensing fees like: Red Hat Enterprise, SUSE Enterprise and Oracle Enterprise Linux, UNIX, Windows Server, etc.
    2. These OS needs to be implemented in conjunction with Amazon Virtual Private Cloud (VPC).
- Security
    1. Users have complete control over the visibility of their AWS account.
    2. The security systems allow create groups and place running instances into it as per the requirement.

3. You can specify the groups with which other groups may communicate, as well as the groups with which IP subnets on the Internet may talk.

- Pricing
    1. AWS offers a variety of pricing options, depending on the type of resources, types of applications and database.
    2. It allows the users to configure their resources and compute the charges accordingly.
- Migration
    1. This service allows the users to move existing applications into EC2.
    2. It costs $80.00 per storage device and $2.49 per hour for data loading.
    3. This service suits those users having large amount of data to move.
- Fault tolerance
    1. Amazon EC2 allows the users to access its resources to design fault-tolerant applications.
    2. EC2 also comprises geographic regions and isolated locations known as availability zones for fault tolerance and stability.
    3. It doesn't share the exact locations of regional data centers for security reasons.
    4. When the users launch an instance, they must select an AMI (Amazon Machine Image) that's in the same region where the instance will run.
    5. Instances are distributed across multiple availability zones to provide continuous services in failures, and Elastic IP (EIPs) addresses are used to quickly map failed instance addresses to concurrent running instances in other zones to avoid delay in services.
    6.

d. Features of EC2

- Reliable
    1. Amazon EC2 offers a highly reliable environment where replacement of instances is rapidly possible.
    2. Service Level Agreement commitment is 99.9% availability for each Amazon EC2 region.
- Designed for Amazon Web Services
    1. Amazon EC2 works fine with Amazon services like Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon SQS.
    2. It provides a complete solution for computing, query processing, and storage across a wide range of applications.
- Secure
    1. Amazon EC2 works in Amazon Virtual Private Cloud to provide a secure and robust network to resources.
- Flexible Tools

1. Amazon EC2 provides the tools for developers and system administrators to build failure applications and isolate themselves from common failure situations.

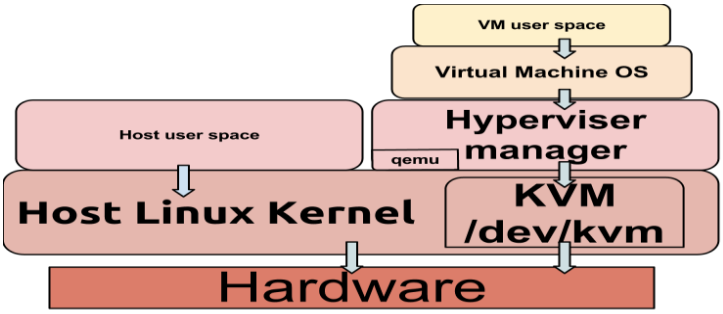
- Inexpensive
  1. Amazon EC2 wants us to pay only for the resources that we use.
  2. It includes multiple purchase plans such as On-Demand Instances, Reserved Instances, Spot Instances, etc. which we can choose as per our requirement.

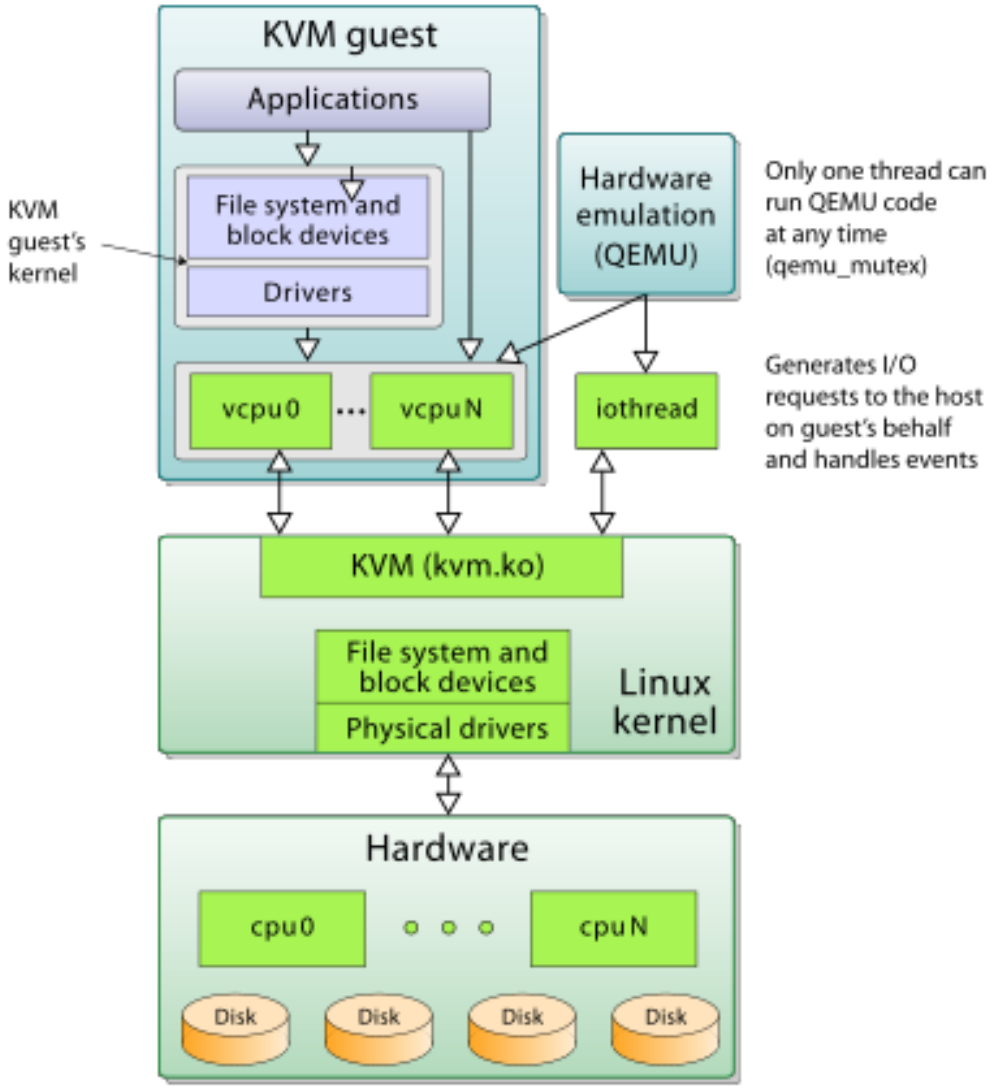
e. Benefits
- Scale capacity on demand
- Enhanced or improved sales because of highly available servers
- Keep data fresh in variety of data stores
- Focus on product
- Cost Effective
- Grow with AWS
-

7. KVM (Kernel-based Virtual Machine)

a. Introduction
- Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns it into a hypervisor.
- It was merged into the Linux kernel mainline in kernel version 2.6.20, which was released on February 5, 2007.
- KVM requires a processor with hardware virtualization extensions.
- KVM originally supported x86 processors.
- It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.
- A wide variety of guest operating systems work with KVM, including many flavours and versions of Linux, BSD, Solaris, Windows, Haiku, ReactOS, Plan 9, AROS Research Operating System and OS X. In addition, Android 2.2, GNU/Hurd (Debian K16), Minix 3.1.2a, Solaris 10 U3 and Darwin 8.0.1.
- Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- KVM is open source software.

b. Architecture





c. KVM Features

- Over-committing : Which means allocating more virtualized CPUs or memory than the available resources on the system.
- Thin provisioning : Which allows the allocation of flexible storage and optimizes the available space for every guest virtual machine.
- Disk I/O throttling : Provides the ability to set a limit on disk I/O requests sent from virtual machines to the host machine.
- Automatic NUMA balancing : Improves the performance of applications running on NUMA hardware systems.
- Virtual CPU hot add capability : Provides the ability to increase processing power as needed on running virtual machines, without downtime.

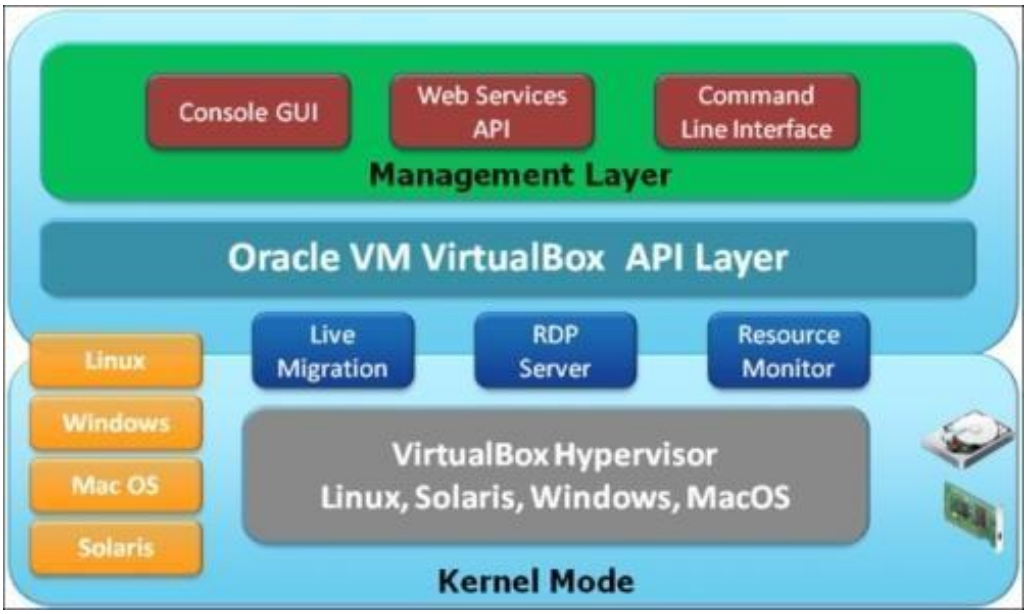
8. Oracle Virtual Box

a. Introduction

- Oracle VM VirtualBox (formerly Sun VirtualBox, Sun xVM VirtualBox and Innotek VirtualBox) is a free and open-source hypervisor for x86 computers currently being developed by Oracle Corporation.

- Developed initially by Innotek GmbH, it was acquired by Sun Microsystems in 2008 which was in turn acquired by Oracle in 2010.
- VirtualBox may be installed on a number of host operating systems, including: Linux, MacOS, Windows, Solaris, and OpenSolaris.
- For some guest operating systems, a "Guest Additions" package of device drivers and system applications is available which typically improves performance, especially of graphics.
- Oracle VirtualBox is a Type2 hypervisor that can run on Linux, Windows, Macintosh and Solaris hosts.
- It is portable as it can run on a large number of 32-bit and 64-bit host operating systems.
- It is called a hosted hypervisor as it requires an existing operating system to be installed.
- One good feature of VirtualBox is that virtual machines can be easily imported and exported using OVF (Open Virtualization Format).
- It is even possible to import OVFs that are created by different virtualisation software.
- VirtualBox is a cross-platform virtualization application.
- VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.
- It can run everywhere from small embedded systems or desktop class machines all the way up to datacenter deployments and even Cloud environments.
-

b. Architecture



c. Features

- Portability
- No hardware virtualization required
- Guest Additions: shared folders, seamless windows, 3D virtualization

- Great hardware support
    1. Guest multiprocessing (SMP).
    2. USB device support.
    3. Hardware compatibility
    4. Full ACPI (Advanced Configuration and Power Interface) support
    5. Multiscreen resolutions
    6. Built-in iSCSI support
    7. PXE (Preboot Execution Environment) Network boot
- Multigeneration branched snapshots
- VM groups
- Clean architecture; unprecedented modularity
- Remote machine display.

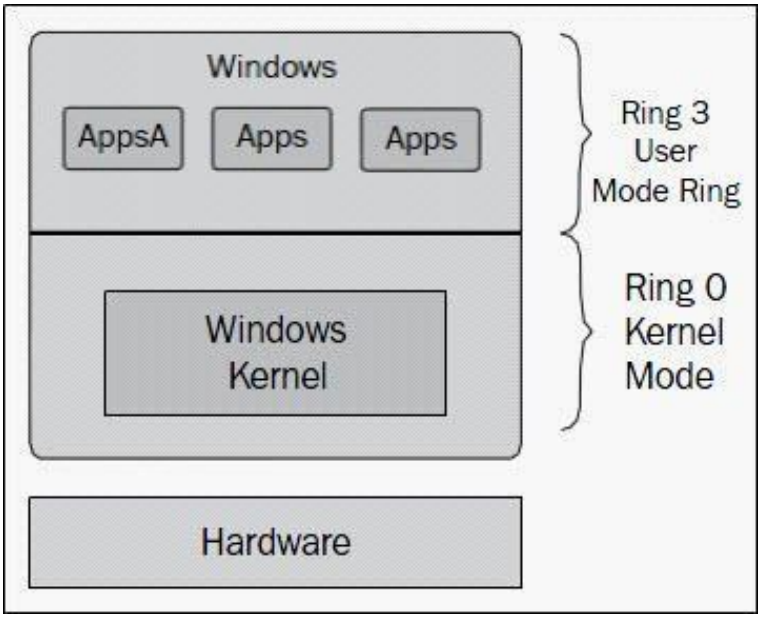
d. Advantages
- Seamless mode - the ability to run virtualized applications side by side with normal desktop applications
- Shared folders
- Special drivers and utilities to facilitate switching between systems
- Command line interaction (in addition to the GUI)
- Public API (Java, Python, SOAP, XPCOM) to control VM configuration and execution

e. Limitations
- VirtualBox has a very low transfer rate from and to USB2 devices
- It is not supported by older guest OS like Windows Vista and Windows XP due to the lack of drivers.
- Video RAM is limited to 128 MB due to technical difficulties

8. Hyper-V

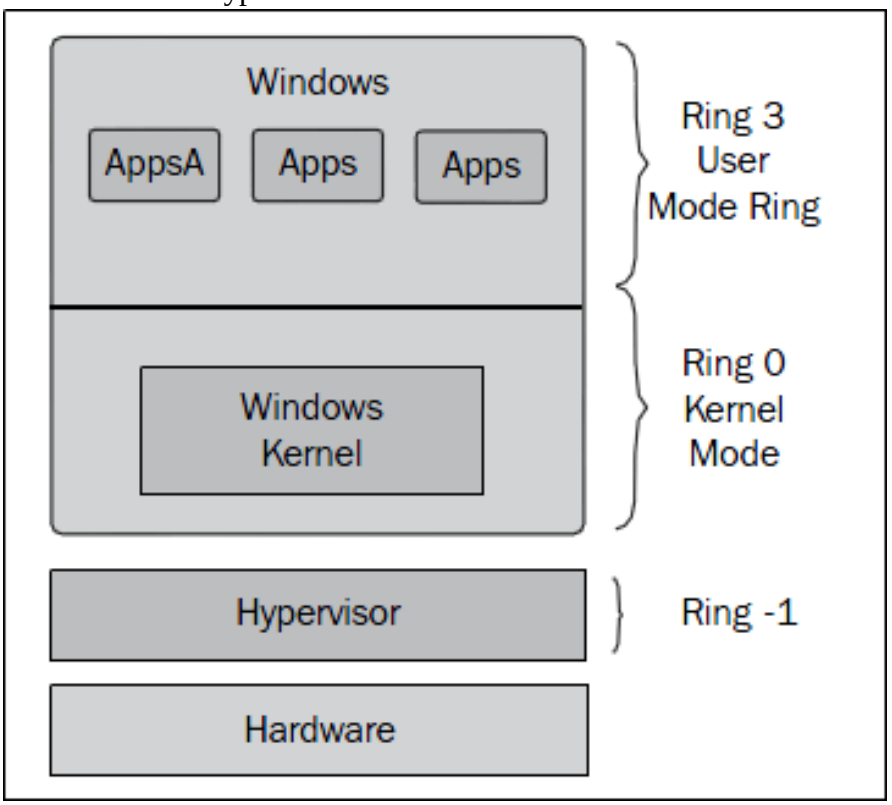
a. Introduction
- Hypervisor technology is software on which multiple virtual machines can run, with the hypervisor layer controlling the hardware and allocating resources to each VM operating system.
- Hyper-V is the virtualization platform that is included in Windows Server 2008.
- As server virtualization becomes more important to businesses as a cost-saving and security solution, and as Hyper-V becomes a major player in the virtualization space.
- With Hyper-V Server 2012 R2, the hypervisor license is free. Even so, you are still required to license the virtual machines that you will be running on top of the hypervisor.

b. Windows before Hyper-V



- The instructions access is divided by four privileged levels in the processor called Rings
- The most privileged level is Ring 0, with direct access to the hardware and where the Windows Kernel sits.
- Ring 3 is responsible for hosting the user level, where most common applications run and with the least privileged access.

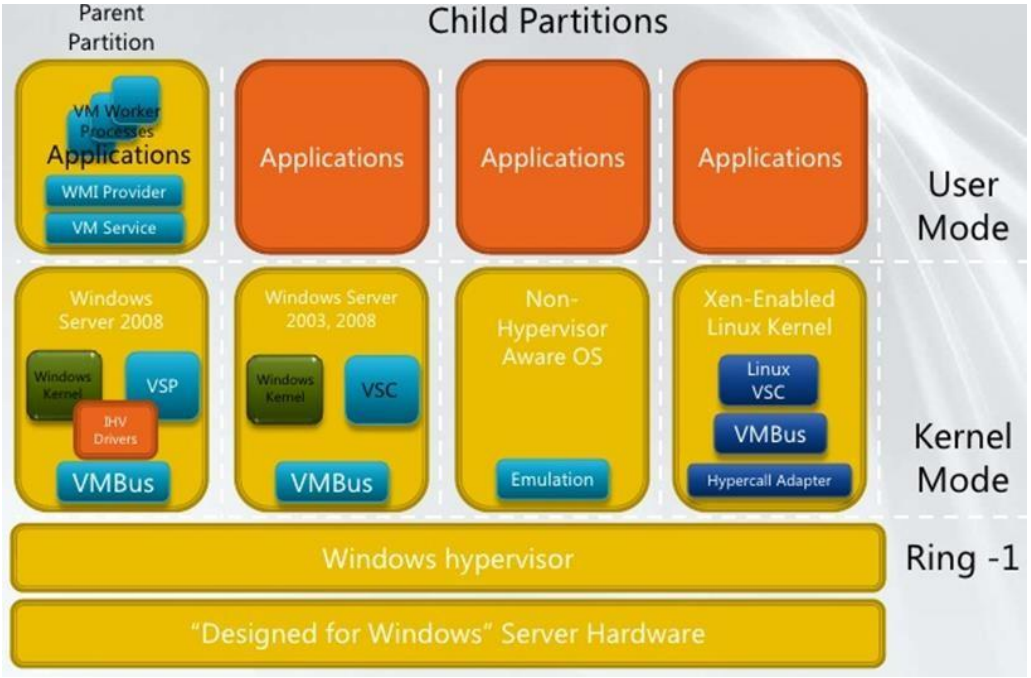
c. Windows after Hyper-V



- When Hyper-V is installed, it needs a higher privilege than Ring 0. Also, it must have dedicated access to the hardware.

- This is possible due to the capabilities of the new processor created by Intel and AMD, called Intel-VT and AMD-V respectively, that allows the creation of a fifth ring called Ring -1.
- Hyper-V uses this ring to add its Hypervisor, having a higher privilege and running under Ring 0, controlling all the access to the physical components, as shown in figure.

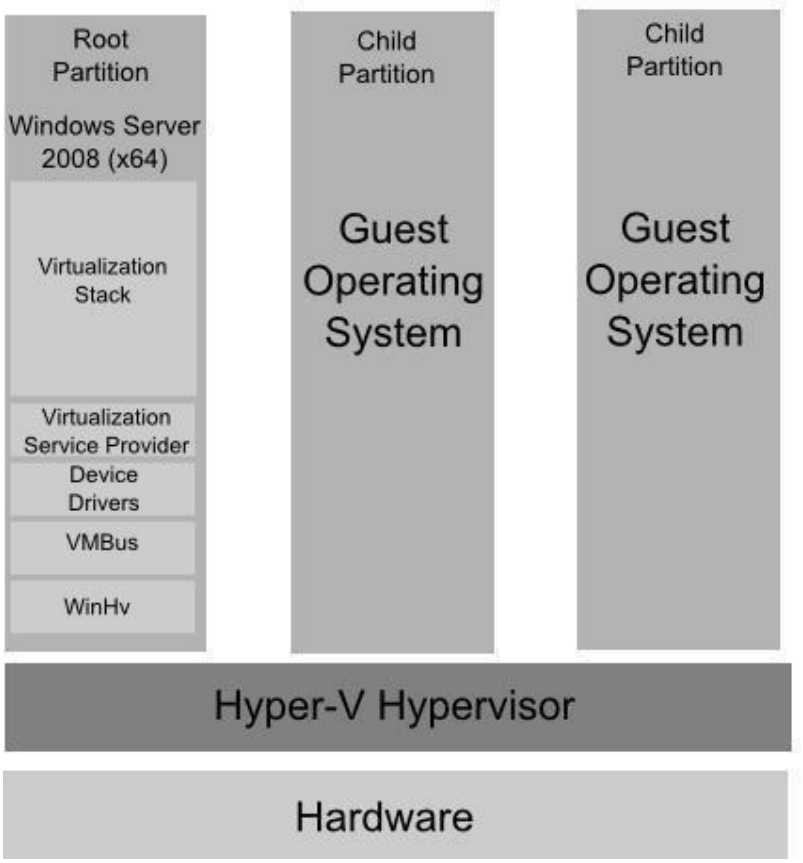
d. Architecture



- The hypervisor is the processor-specific virtualization platform that can host multiple virtual machines (VMs) that are isolated from each other but share the underlying hardware resources by virtualizing the processors, memory, and I/O devices.
- The necessary virtual server client (VSC) drivers and services are installed on the guest operating system.
- Hyper-V Integration services that provide VSC drivers are also available for other client operating systems.
- Hyper-V supports isolation in terms of a partition.
- A partition is a logical unit of isolation, supported by the hypervisor, in which operating systems execute.
- The Microsoft hypervisor must have at least one parent, or root, partition, running Windows Server.
- The virtualization stack runs in the parent partition and has direct access to the hardware devices.
- The root partition then creates the child partitions which host the guest operating systems.
- A root partition creates child partitions using the hypercall application programming interface (API).
- The hypervisor handles the interrupts to the processor, and redirects them to the respective partition.

- Hyper-V can also hardware accelerate the address translation between various guest virtual address spaces by using an Input Output Memory Management Unit (IOMMU) which operates independent of the memory management hardware used by the CPU.
- An IOMMU is used to remap physical memory addresses to the addresses that are used by the child partitions.
- Child partitions make a requests to the virtual devices are redirected either via the VMBus or the hypervisor to the devices in the parent partition, which handles the requests.
- The VMBus is a logical inter-partition communication channel.
- The parent partition hosts Virtualization Service Providers (VSPs) which communicate over the VMBus to handle device access requests from child partitions.
- Child partitions host Virtualization Service Consumers (VSCs) which redirect device requests to VSPs in the parent partition via the VMBus.
- This entire process is transparent to the guest operating system.

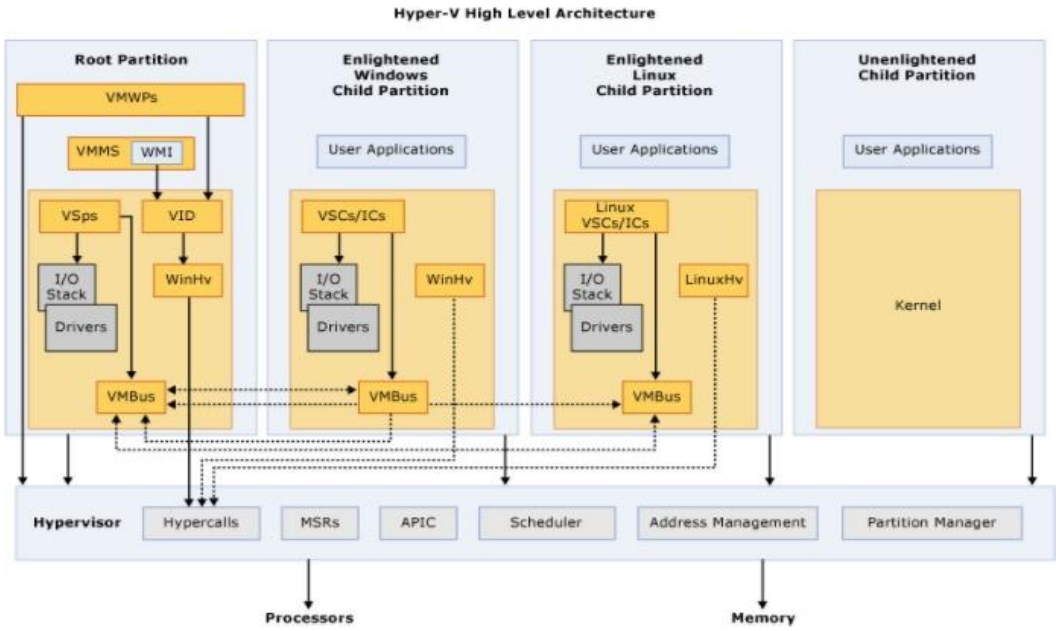
e. Simplified architecture



- Virtual Machine Worker Processes are started by the VMM Service when virtual machines are started.
- The duties of the Virtual Machine Worker Process include creating, configuring, running, pausing, resuming, saving, restoring and snapshotting the associated virtual machine.

- Virtual Infrastructure Driver - Operates in kernel mode (i.e. in the privileged CPU ring) and provides partition, memory and processor management for the virtual machines running in the child partitions.
- VMM Service - Manages the state of virtual machines running in the child partitions (active, offline, stopped etc).
- Virtual Devices are managed by the Virtual Motherboard (VMB). Virtual Motherboards are contained within the Virtual Machine Worker Processes, of which there is one for each virtual machine.

f. Detailed architecture



- APIC – Advanced Programmable Interrupt Controller. A device which allows priority levels to be assigned to its interrupt outputs.
- Child Partition – Partition that hosts a guest operating system. All access to physical memory and devices by a child partition is provided via the Virtual Machine Bus (VMBus) or the hypervisor.
- Hypercall – Interface for communication with the hypervisor. The hypercall interface accommodates access to the optimizations provided by the hypervisor.
- Hypervisor – A layer of software that sits between the hardware and one or more operating systems. Its primary job is to provide isolated execution environments called partitions. The hypervisor controls and arbitrates access to the underlying hardware.
- IC – Integration component. Component that allows child partitions to communication with other partitions and the hypervisor.
- I/O stack – Input/output stack.
- MSR – Memory Service Routine.
- Root Partition – Manages machine-level functions such as device drivers, power management, and device hot addition/removal. The root (or parent) partition is the only partition that has direct access to physical memory and devices.

- VID – Virtualization Infrastructure Driver. Provides partition management services, virtual processor management services, and memory management services for partitions.
- VMBus – Channel-based communication mechanism used for inter-partition communication and device enumeration on systems with multiple active virtualized partitions. The VMBus is installed with Hyper-V Integration Services.
- VMMS – Virtual Machine Management Service. Responsible for managing the state of all virtual machines in child partitions.
- VMWP – Virtual Machine Worker Process. A user mode component of the virtualization stack. The worker process provides virtual machine management services from the Windows Server instance in the parent partition to the guest operating systems in the child partitions.
- VSC – Virtualization Service Clients are synthetic device instances that reside in child partitions. They communicate with the VSPs in the parent partition over the VMBus to fulfill the child partition's device access requests.
- VSP – Virtualization Service Provider. Resides in the root partition and provide synthetic device support to child partitions over the VMBus.
- WinHv – Windows Hypervisor Interface Library. WinHv is essentially a bridge between a partitioned operating system's drivers and the hypervisor which allows drivers to call the hypervisor using standard Windows calling conventions
- WMI – The Virtual Machine Management Service exposes a set of Windows Management Instrumentation (WMI)-based APIs for managing and controlling virtual machines.

g. Advantages
- Consolidation of hardware resources
- Ease of administration
- Significant cost savings
- Fault tolerance support through Hyper-V clustering
- Ease of deployment and management
- Key Hyper-V performance characteristics
    1. Improved hardware sharing architecture
    2. Processor hardware-assisted virtualization support
    3. Multi-core (SMP) guest operating system support
    4. Both 32-bit and 64-bit guest operating system support
- Comprehensive product support
- Scalability

h. Disadvantages
- Hardware requirements
- Software requirements