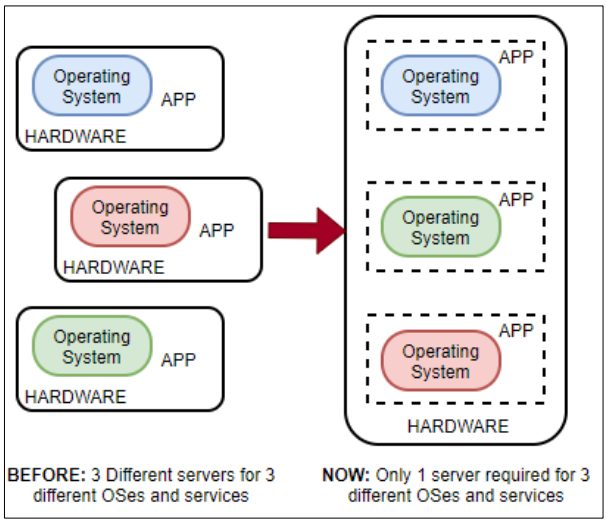
DHRUV GARG 16 BCE 1190

DIGITAL ASSIGNMENT 1

VIRTUALIZATION

QUESTION 1: *Compare and contrast the types of hypervisor with common features. In each type, two market available hypervisors to be considered and discussed.*

Virtualization: It refers to the abstraction of the physical hardware devices from applications running on that hardware. This gives an impression to the guest machines (virtual machines) as if they were operating alone, on the hardware. Using virtualization, we can create more logical IT resources, called virtual systems, within one physical system.

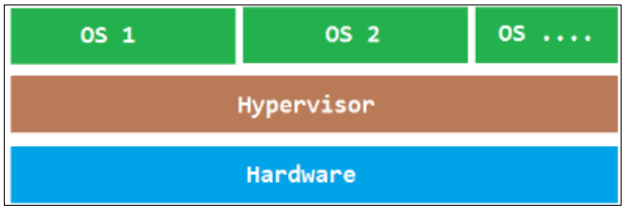


The functionality of virtualization (described above), is provided by a Hypervisor, traditionally called a Virtual Machine Monitor (VMM). The hypervisor virtualizes the hardware, manages and provisions the system's resources: processor, memory, storage and network resources. It enables the host system to work on more than one workload simultaneously, in a cost and energy efficient manner.

There are two types of hypervisors:

TYPE 1 Hypervisor (Bare metal/Embedded/Native): These run directly on the system hardware (bare metal) of the host and can monitor operating systems that run above the hypervisor. Since they do not have to load up on an underlying Operating System, they are completely independent of the OS. A major advantage of this hypervisor is that any problem on a VM or guest OS is isolated, i.e. it does not affect the other guest OSes running on the hypervisor.

Some advantages of Type 1 hypervisors are:



- Since these hypervisors have direct access to the underlying hardware and no intermediate software (Oses or drivers), their footprint is small, and are regarded as the most efficient performers.
- Their main task is limited to sharing and managing the hardware resources between different OSes.
- Hypervisors running directly on physical hardware are highly secure- Security flaws and vulnerabilities endemic to OSes are absent because the attacks from the underlying OS is eliminated. This ensures the logical isolation of every guest VM against malicious software and activity.

Two market available Type 1 hypervisors are:

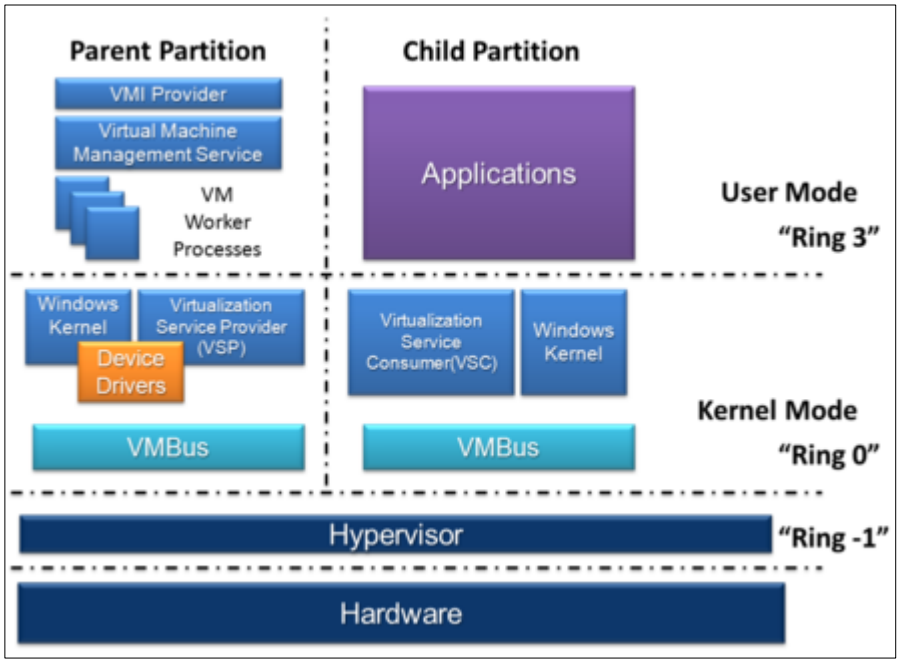
a. Microsoft Hyper-V

Hyper-V implements isolation of virtual machines in terms of a partition. A partition is a logical unit of isolation, supported by the hypervisor, in which each guest operating system executes. The virtualization software runs in the parent partition and has direct access to the hardware devices. The parent partition creates child partitions which host the guest OSs. A parent partition creates child partitions using the hypercall API, which is the application programming interface exposed by Hyper-V.

Requirements of Hyper-V:

- A 64-bit processor with second-level address translation (SLAT).
- VM Monitor Mode extensions
- Enough memory - plan for at least 4 GB of RAM. More memory is better.
- Virtualization support turned on in the BIOS or UEFI

Architecture of Hyper-V:



Features of Hyper-V:

1. **Nested Virtualization:** Nested Virtualization enables you to run a Hyper-V in a Virtual Machine. This Nested Hyper-V then work as a regular Hyper-V Host.
2. **Host Resources Protection:** Host Resources Protection is a feature to protect Hyper-V resources (like CPU, Ram, etc.) from being 100% taken by one VM. This feature protects Hyper-V resources from VMs using more resources than was allocated. When Hyper-V while monitoring its activity detects that a VM is using abnormal resources, automatically reduce allocated resources on that particularly VM so that not affect other VMs performance.
3. **Production VM checkpoints using VSS:** Using VSS admins have a more "Backup" data-consistent. In Linux VMs there is no VSS, so Checkpoints use a Linux File System Freeze to create a data-consistent backup.
4. **Shielded Virtual Machines:** Shield VM feature (Virtual Trusted Platform Module) was one of the features that Microsoft created to provide more VMs security using BitLocker technology and to protect against ransomware and other attacks. Including any inspection, theft, and tampering of company data from admins.

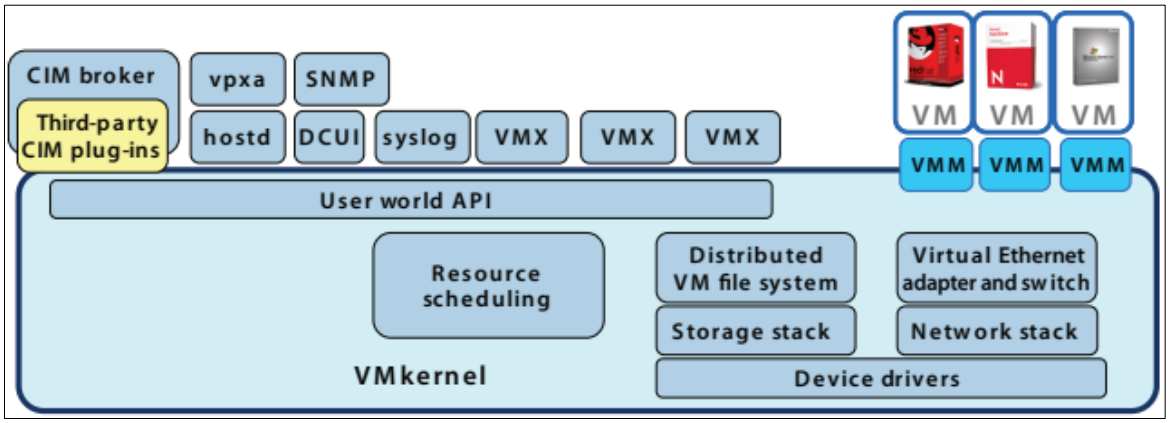
b. VMware ESXi Server

VMware ESXi is an operating system-independent hypervisor based on the VMkernel operating system that interfaces with agents that run on top of it. ESXi stands for Elastic Sky X Integrated. ESXi is targeted at enterprise organizations and its VMkernel interfaces directly with VMware agents and approved third-party modules. Admins can configure VMware ESXi using its console or a vSphere client.

Requirements of ESXi:

As ESXi is lightweight, and requires a minimum amount of hardware resources. Specifically, ESXi version 6.7 requires a host machine with a minimum of 2 two CPU cores, a 64-bit x86 processor released before 2006, and 4 GB or preferably, 8 GB of RAM. ESXi is installed directly on a local hard disk in the host machine.

Architecture of ESXi:

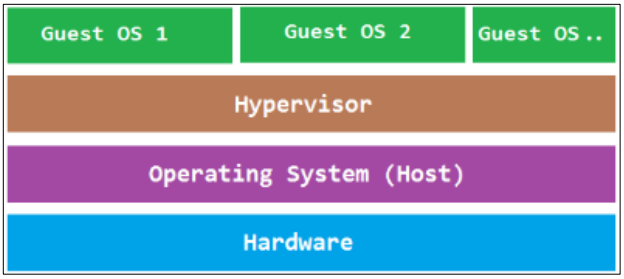


Features of ESXi

By consolidating multiple servers onto fewer physical devices, ESXi reduces space, power and IT administrative requirements while driving high-speed performance.

1. **Small Footprint:** With a footprint of just 150MB, ESXi allows users to do more with less, while minimizing security threats to your hypervisor.
2. **Reliable Performance:** Accommodates apps of any size- configures virtual machines up to 128 virtual CPUs, 6 TB of RAM and 120 devices to satisfy all application needs.
3. **Enhanced Security:** Protects sensitive virtual machine data with powerful encryption capabilities. Role-based access simplifies administration, and extensive logging and auditing ensure greater accountability and easier forensic analysis.
4. **Ecosystem Excellence:** Has support for a broad ecosystem of hardware OEM vendors, technology service partners, apps, and guest operating systems.
5. **User-Friendly Experience:** Manages day-to-day administrative operations with built-in modern UI based on HTML5 standards. For customers who need to automate their operations, VMware offers both- a vSphere Command Line Interface and developer-friendly REST-based APIs.

TYPE 2 Hypervisor (Hosted): Such hypervisors are installed on top of a Host OS, and it then supports other Guest OSes above it. Thus, it is heavily dependent on the Host OS for its operations. While the Host OS allows better specification policies, there are some issues with Type 2 hypervisors:



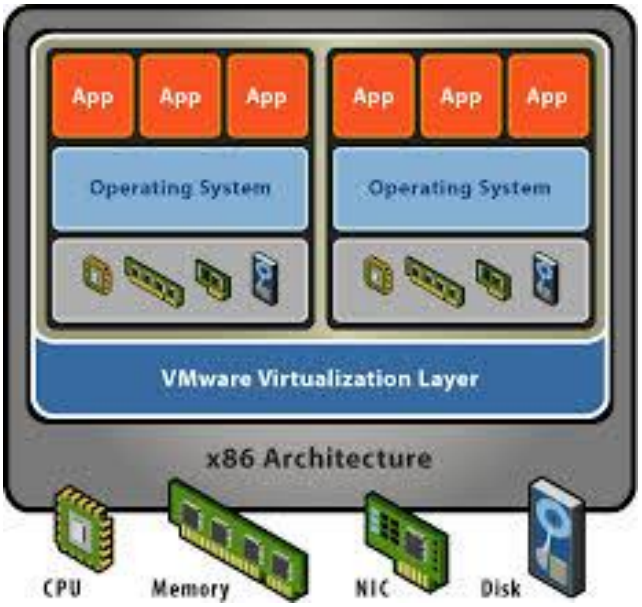
- Problems in the Host OS affects the entire system even if the hypervisor is running above the Host OS is secure. Any security flaws or vulnerabilities in the Host OS could compromise all of the VMs running above it.
- Although the purpose and goals of Type 1 and Type 2 hypervisors are identical, the presence of an underlying OS in Type 2 hypervisors introduced an unavoidable latency since all activities of the hypervisor would pass through the Host OS.

Eventually, Type 2 hypervisors are generally not used for data centre computing and are reserved for client or end-user systems – where performance and security are lesser concerns.

Two market available Type 2 hypervisors are:

a. VMware Workstation Pro

VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems. It enables users to set up virtual machines (VMs) on a single physical machine, and use them simultaneously along with the actual machine. Each virtual machine can execute its own operating system, including versions of Microsoft Windows, Linux, BSD, and MS-DOS.



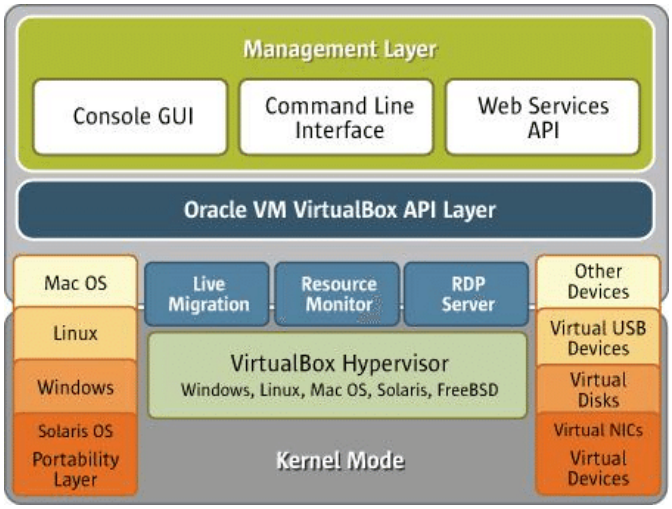
Requirements of VMware Workstation

- Systems using Processors (CPUs) launched in 2011 or later are supported
- 1.3GHz or faster core speed
- 2GB RAM minimum/ 4GB RAM or more recommended
- Host Operating Systems (64-bit): Ubuntu 15.04+, Red Hat Enterprise Linux 6+, CentOS 7.0+, Oracle Linux 7.0+, openSUSE Leap 42.2+, SUSE Linux 13+, Windows 7+ and Windows Server 2008+.
- Guest Operating Systems: Windows XP/7/ 8.X/10, Ubuntu, Red Hat, SUSE, Fedora, Mint, CentOS and many more.

Features of VM Workstation Pro

1. **vSphere Integration:** A shared hypervisor ensures that apps can easily move between desktop, data centre and cloud. Workstation brings insight into remote clusters, data centres and virtual machines, as well as allow users to quickly deploy ESXi as VMs in a local lab on a single PC.
2. **REST API for VM Automation:** The REST API provides over 20 controls for operations such as Host and Guest Virtual Networking, VM Power, and shared folder management for programmatic mounting of source code directories from the host.
3. **Powerful Virtual Networking:** Allows complex IPv4 or IPv6 virtual networks for VMs, or integration with third-party software to design full data centre topologies using real-world routing software and tools.
4. **Helpful Snapshots:** Creates a rollback point to revert to on the fly, which is perfect for testing unknown software or creating customer demos. Multiple snapshots make it easy to test a variety of different scenarios without the need to install multiple operating systems.
5. **Restricted Access to Virtual Machines:** Protects corporate content by restricting access to Workstation VM settings like drag-and-drop, copy-and-paste and connections to USB devices. Virtual machines can be encrypted and password-protected to ensure only authorized users have access.
6. **Monster Virtual Machines:** Creates massive VMs with up to 16 vCPUs, 8 TB virtual disks, and 64 GB of memory to run the most demanding desktop and server applications in a virtualized environment. Give graphics-intensive apps an additional boost by allocating up to 3GB of available host video memory to a VM.

b. Oracle VirtualBox



Oracle VM VirtualBox is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation. Users of VirtualBox can load multiple guest OSes under a single host operating-system (host OS). Each guest can be started, paused and stopped independently within its own virtual machine (VM).

Requirements of Oracle VirtualBox

- Processor: Any recent Intel or AMD processor should do.
- Memory: Depending on what guest operating systems you want to run, you will need at least 512 MB of RAM.
- Hard disk space: IDE, SATA, and SCSI hard drives are supported.
- Supported guest operating system: Many OSes are supported, such as: Windows XP, Windows 7, Windows 8, Windows Server 2008, FreeBSD, Debian, etc.

Features of Oracle VirtualBox

1. It supports both software-based virtualization and hardware-based virtualization
2. 64-bit guests (hardware virtualization support is required)
3. Snapshots
4. Seamless mode — the ability to run virtualized applications side by side with normal desktop applications
5. Shared clipboard
6. Shared folders
7. Command line interaction (in addition to the GUI)
8. Public API (Java, Python, SOAP, XPCOM) to control VM configuration and execution
9. Nested paging for AMD-V and Intel VT (only for processors supporting SLAT and with SLAT enabled)
10. Teleportation (aka Live Migration)
11. SATA disk hot plugging
12. Pass-through mode for solid-state drives
13. Pass-through mode for CD/DVD/BD drives — allows users to play audio CDs, burn optical disks, and play encrypted DVD discs
14. Can disable host OS I/O cache
15. Allows limitation of IO bandwidth
16. Raw hard disk access — allows physical hard disk partitions on the host system to appear in the guest system

QUESTION 2: *Discuss the key points to be considered in the choice of hypervisor for virtualization in Cloud provider's datacentre.*

Most hypervisors have the same basic features, but the devil lies in the details. There are many factors that help to determine which hypervisor to for virtualization in a Cloud provider's datacentre. There are two decisions to be made: (i) choice between type 1 and type 2 hypervisor, and (ii) choosing a hypervisor in the type chosen in (i), from those available in the market. Matching this data to your organization's requirements will be at the core of the decision you make.

DECISION 1: Choosing between Type 1 and Type 2

1. **Performance:**
    a. For high performance, a bare-metal virtualization hypervisor is the go-to option. It offers minimal resource overhead.

   b. Hosted hypervisors typically have no or limited resource controls, so VMs have to fight each other for resources.
   c. Unlike bare-metal virtualization, hosted hypervisors often have steep resource-overhead penalties.
2. **Ease of use:**
   a. Hosted virtualization hypervisors are easy to install, use and maintain. Most hosted hypervisors install like an application and are fairly intuitive.
   b. Bare-metal virtualization hypervisors are easy to but they can be complicated to configure.
3. **High availability:**
   a. Bare-metal virtualization hypervisors offer high-availability features
   b. Hosted virtualization hypervisors typically lack high-availability features, so if a host fails, VMs are down until you resolve the problem.
4. **Reliability:**
   a. For reliability, bare-metal hypervisors definitely have an edge. This type of virtualization hypervisor typically goes through more quality-assurance testing than hosted products, because they're aimed at data centres.
   b. Hosted hypervisors use regular drivers that go through no special testing for virtualization.
5. **Virtualization hypervisor management:**
   a. Bare-metal hypervisors have more options for management and automation. They have centralized consoles that allow for managing large numbers of hosts and VMs.
   b. Hosted hypervisors, on the other hand, tend to be islands that admins have to manage individually, which can be very tedious and time consuming in large infrastructures.
6. **Cost:**
   a. Hosted virtualization hypervisors have a big edge over bare-metal hypervisors.
   b. Bare-metal hypervisors can be very costly, especially when you want to scale and use advanced features.
7. **Scalability:**
   a. Bare-metal hypervisor can scale very high. You can easily run hundreds of VMs on a single host if you have enough hardware resources.
   b. In contrast, hosted hypervisors have very limited scalability, both in the size of the VMs and the number of VMs that can run on a single host.

DECISION 2: Choosing a market available hypervisor

1. **Comparing hypervisors' performance metrics:**
   a. Most hardware virtualization hypervisors include similar basic features. One of the best ways to determine which hypervisor meets your needs is to compare their performance metrics.
   b. These include CPU overhead, amount of maximum host and guest memory and support for virtual processors.
2. **Comparing OSes supported by the different hypervisors:**
   a. One must also verify the guest operating systems that each hypervisor supports. The hypervisor should have support for the operating systems you currently run.
3. **The cost of a hypervisor:**
   a. For many buyers, it is about striking the right balance between cost and functionality. Licensing frameworks also vary, so it's important to be aware of exactly what you're getting for your money.
   b. It is also worth thinking about whether or not you should stick to one vendor or use several. Consider a tiered approach that matches price point to workload.
4. **Ecosystem:**
   a. Ecosystem is the availability of documentation, support, training, third-party developers and consultancies.
   b. It is almost always preferable to go for the hypervisor with the healthier user community.
5. **The availability of management tool:**
   a. Preference is given to solutions that have better management tools and utilities than others, both in terms of out-of-the-box software and optional add-ons from third-party developers.