PART-A
SHORT QUESTIONS WITH SOLUTIONS

Q1. What is virtualization?

Ans: Virtualization is a technique that allows applications to run in secured, customized and isolated environments. It provides an abstract environment and efficiently delivers Infrastructure-as-a-Service (IaaS) for cloud computing. It helps to build scalable systems to provide services with minimum costs. The techniques of virtualization provide virtual environments at various levels like operating system level, programming language level and application level. In addition to providing a virtual environment for execution of applications, it also provides virtual environment for storage, networking and memory.

Q2. What are the advantages of virtualization at OS-level? Model Paper-I, Q1(b)

Ans: The advantages of virtualization at OS level are as follows,

1. OS level virtualization is preferred because it provides the best performance and measurability.
2. This technique is easy to control and comparatively uncomplicated to manage as everything can be administered from the host system.
3. It has dynamic reallocation of resources.
4. It has the ability to create links back to the server host operating system which can perform lightening fast management operations.

Q3. List the advantages of programming level virtualization.

Ans: The advantages of programming level virtualization are as follows,

1. Programs compiled into byte code can be executed on any OS and platform.
2. No need of providing multiple versions of a single code.
3. It has an ability to provide uniform execution environment across different platforms.
4. Managed programming language provides the security by filtering the I/O operations with support of sandboxing.

Q4. Define storage virtualization.

Ans: Storage virtualization can be defined as the layer between physical storage and virtual storage. It maps the physical storage to virtual storage and vice-versa. In this, individual physical devices are abstracted to form one or more logical entities. The individual physical devices are no longer accessed directly by the operating system, instead they are accessed separately and independently. However, the virtual entities are only accessed directly by the operating systems.

Q5. Write short notes on KVM. Model Paper-II, Q1(b)

Ans: Kernel-based Virtual Machine (KVM) is an open source software, a virtualization solution for Linux on x86 hardware comprising virtualization extensions like Intel VT and/or AMD-V. This software comprises of two modules. A kernel module, KVM. KO, that provides the core virtualization infrastructure, and a processor-specific module, KVM-intel. KO that rely on the CPU manufacturer. The various operating systems that work with KVM comprises various versions of Linux, Solaris, React OS, BSD, Windows, Haiku and the AROS Research Operating System. The virtualized hardware includes disk, network card, graphics adapter and so on. However, the speed of the network and graphics is relatively slow. The performance of KVM is quite low when compared to the VM Ware or Virtual Box.

Q6. Write about VMware technology. Model Paper-III, Q1(b)

Ans: VMware technology is based on the full virtualization technique where the hardware is replicated and the guest operating system uses it without any modification. It uses Type II hypervisors for implementing full virtualization in desktop environment and Type I hpervisors for implementing in server environment. These implementations are done by using binary translation and direct execution methods thereby virtualizing *x*86 architecture.

VMware virtualizes *x*86 architecture which runs on the top of underlying hypervisors. In this architecture, the set of private instructions is not a subset of privileged instructions. Such type of instructions are not executed in Ring 0. Due to this the architecture functions differently. This issue is resolved by generating a trap. In dynamic binary translation, the trap will prompt the translation of miscreant instructions to function in the same way and generate result without any exceptions. The translated instructions are cached so that they can be used in future. This helps in improving the performance.

Q7. List the advantages of virtualization.

Ans: The various advantages for virtualization are,

1. Managed execution and isolation helps to control and construct secure computing of the virtualized execution environments. It reduce, the harmful operations without execution and it can be configured as a send box.
2. Portability for execution virtualization techniques, allows virtual machine instances to transport to a host physical system. The virtual machine instances are represented as a file and are execute only by virtual machine.
3. Portability reduces the maintenance cost since the number of hosts are lower than the number of virtual machine instances.
4. Virtualization reduce the cost by reducing the hardware and efficiently uses the resources. The coexistence of multiple systems allow the resources to be shared without any interference from others.

Q8. Write a brief note on memory migration. Model Paper-IV, Q1(b)

Ans: Memory migration refers to the moving of memory instances from one system to another. It can be accomplished in different ways. All these ways are based on sharing of a single implementation paradigm. Moreover, these methods are based on the capability of guest operating system to support the characteristics of workload. Size of memory instance to be migrated can range from megabytes to gigabytes.

A technique called Internet Suspend-Resume (ISR) makes use of temporal locality of the fact that memory instances can be in resumed and suspended states. The term temporal locality is nothing but the property of memory instance to differ from each other based on the amount of work done from its suspension to its initiation. Temporal locality in memory migration can be used by representing every file as a tree. This tree is copied into the virtual memory instances of both suspended and resumed states. Use of such an approach makes the system to forward only the files which are modified instead of sending all the files.

Q9. What are the challenges that arise in virtualization of multi-core processors?

Ans: The challenges that arise in such a virtualization process are,

1. Applications must fully utilize the overall cores involved in a multi-core processor in a parallelized format. For this, it is necessary to involve new models for programming, libraries and languages.
2. The cores must be allocated with the tasks explicitly by the software. For this, it is necessary to involve various policies for resource management and scheduling algorithms.

Apart from these two challenges, the technological improvement are also imposing certain challenges. This is because CPU cores are getting integrating with CPU cores which is called as dynamic heterogeneity.

Q10. List the steps to perform live migration of VM.

Ans: Live migration of the Virtual Machines (VMs) to be migrated from one server to another at runtime makes it possible to organize the VM to physical machine relationship for balancing the workload. This feature is supported by the ConVirt tool that involves the following steps for the proper VM migration.

1. Making the installation media to be accessible centrally.
2. Migration needs to be done within the same subnet.
3. It should provide a shared storage for all Guest OS disks (e.g., NFS, or ISCSI)
4. Preferable use of identical machines with the same version of virtualization platform.
5. Creating an identical mount point on all servers (hosts).
6. When using para-virtualized VMs the kernel and ram disk should also be shared. In case of using pygrub it is not required.

PART-B

ESSAY QUESTIONS WITH SOLUTIONS

2.1 IMPLEMENTATION LEVELS OF VIRTUALIZATION

11. What are the common virtualization layers? Explain them.

ns: Model Paper-III, Q3(a)

rtualization: Virtualization is a technology which multiplexes various virtual machines into a single hardware system. Virtual achines are used to increase the resource sharing capability and enhance the performance of the system. This technology enables e developers to create a secure, customized and isolated environment which runs applications without affecting the execution other applications.

rtualization Layers: The common virtualization layers are as follows,

1. Instruction Set Architecture (ISA) level
2. Hardware Abstraction Layer (HAL) level
3. Operating system level
4. Library support level
5. Application level.

Instruction Set Architecture (ISA) Level: In this level, an ISA is emulated by the ISA of host system. Emulation is usually ried out by performing code interpretation which uses an interpreter program for interpreting source instructions to target tructions. However, this process is slow since it translates one instruction after another. Hence, a dynamic binary translation thod has to be used which translates basic blocks of instructions together. This improves performance. Further efficiency can ncreased if program traces or super blocks are used instead of basic blocks.

Hardware Abstraction Layer (HAL) Level: In this level, the resources of computer like processors, memory and I/O ices are virtualized. This is done at the top of a base hardware. The goal of this level is to enhance the hardware utilization by enabling concurrent system usage among multiple users. It does this by creating a virtual hardware environment for a ual machine and managing the hardware through virtualization.

Operating System Level: The layer which is present between operating system and the applications is known as operating em layer. At this level, virtualization can be done using isolated containers which act as real servers and are created on only physical server. Moreover, OS instances are used in effectively utilizing software and hardware in data centers. Using such of virtualization, a virtual platform can be created to assign hardware resources to different users which do not trust each r. In some situations, it is used to integrate hardware associated with server into a single virtual machine. Hardware here can ituated on multiple hosts.

Library Support Level: Virtualization at library level can be done simply by managing the APIs associated with the ications and the system. An example of such type of implementation is WINE tool developed for accessing windows ication over UNIX systems.

Application Level: At this level user application is virtualized as a virtual machine. It is also called as process level alization because operating system considers each application as a process. In this type of virtualization, an application is e as a virtual machine and attached to the operating system as a layer which manages different virtual machines. Some of xamples of application level virtualization are sandboxing, streaming and application isolation.

. Write about the design requirements of VMM.

: VMM stands for Virtual Machine Monitor which is a layer existing between OS and hardware. It is responsible for handling ware and storing the processes that are using the hardware. The design requirements of VMM are as follows,

1. A VMM must be capable of creating a platform which act as original machine for all the programs it carry.
2. Working on such a platform should not decrease the speed of programs. However, minor decrease can be ignored.
3. The overall control over VMM needs to be handed over to system resources.
4. The functionality of programs running in VMM should be same as it is in original machine. However, two types of differences are allowed. First, the differences that arise while making the system resources available. These types of differences are generated in a situation where multiple virtual machines are running on a single machine. Second, the differences that arise due to the timing dependencies.

When each VM is compared with original machine, the requirements (such as memory) associated with hardware resources are reduced. However when all the VMs associated with a single machine are considered, these figures get multiplied resulting in a greater requirements than original machine. This is because all these virtual machines utilize the hardware concurrently.

A VMM is preferably adopted only when it provides description about efficient use of virtual machines. They can make use of simulators and emulators which uses macros or functions to emulate instruction but they become slower in case of real machines. The most effective way to ensure efficiency in this regard is to hand over the responsibility of instruction execution to processor itself which eliminates the dependency of VMM on software.

In order to gain complete control of resources, a VMM should posses the following aspects,

- Its role is to facilitate programs with hardware resources.
- Programs cannot access resources which are implicitly allocated to them.
- A VMM has the power of regaining control over allocated resources in certain situations.

Limitations of VMM

- It highly depends on the processor architecture.
- For certain processors such x86, be implementation of VMM carries many complexities.
- It cannot control certain privileged instructions.
- Hardware needs to be modified in case if the processor does not support virtualization.

Q13. Explain about the OS-level virtualization. List the advantages of OS extensions.

Ans: Model Paper-I, Q3(a)

OS-level Virtualization: At OS level virtualization creates various individual virtualization environments for different applications which are managed concurrently. Virtualization can be done within a single operating system which does not allow hypervisor and it can be done with OS kernel that allows multiple instance to be isolated within user space. It allows sharing of resources among various instances which typically limits the impact of these instances on each other. Such instances are considered as containers such as Virtual Engines (VE), Virtual Private Servers (VPS) etc.

Operating system needs to be general purpose for supporting virtualization. For example, a time-shared operating system provides a strong name space and resource isolation whereas unix systems uses a special mechanism called chroot to carryout virtualization. With respect to processes, a typical chroot operation transforms the root directory of file system and its children to a specific directory.

Virtualizing at the host operating system, parallels virtualization containers and provides a common virtualization layer that allocates system resources to all the virtual servers called as "containers". This results in the creation of a more efficient virtualization layer with an overhead of only 2%.

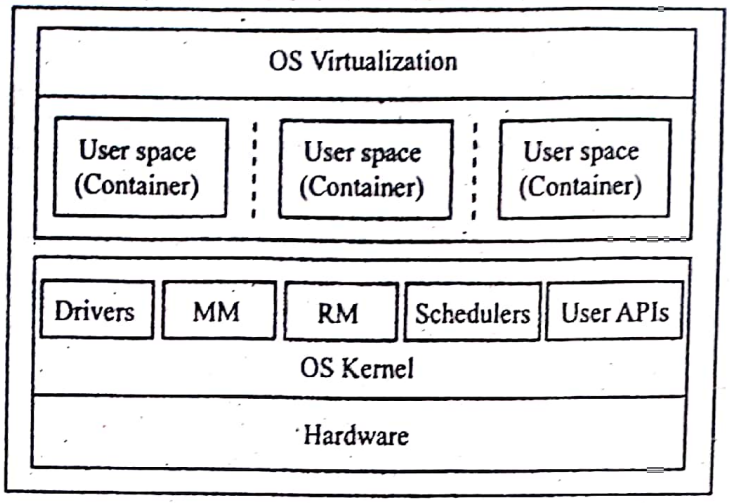


Figure: Operating System Level Virtualization

Operating system level virtualization is specially intended to grant the necessary security and separation mechanisms o run manifold applications and replicas of the same operating system present on a single server. Isolating, segregating and roviding a safe environment enables efficient execution and sharing of machines over numerous applications that are operating n a single server. This technique is used by linux-VServer, FreeBSD jails, OpenVZ, Solaris Zones and virtuozzo.

dvantages

- OS level virtualization is preferred because it provides the best performance and measurability.
- This technique is easy to control and comparatively uncomplicated to manage as everything can be administered from the host system.
- It has dynamic reallocation of resources.
- It has the ability to create links back to the server host operating system which can perform lightening fast management operations.

---

14. Give an overview of various library-level virtualization systems.

ns: Library-level virtualization is used to create a platform on which programs belonging to other systems can be executed ithout relying on the creation of a virtual machine. It explores the features of API call interception and remapping. This type virtualization is also referred to as API (Application Programming Interface) or ABI (Application Binary Interface).

Various library-level virtualization systems include,

1. WABI
2. Lxrun
3. WINE
4. Visual MainWin
5. vCUDA.

WABI: WABI is an acronym of Windows Application Binary Interface. It provides a middleware that is capable of nsforming system calls of windows into system calls of Solaris. The former ones run on x86 computers whereas the latter es run on SPARC workstations.

Lxrun: Lxrun is an acronym of Linux Run which acts as a system call emulator for running programs or applications eloped using Linux for x86 on the systems carrying UNIX operating system.

WINE: WINE is an acronym of Wine Is Not an Emulator. It provides a middleware that is capable of executing applications rograms of windows operating system on UNIX hosts. It enables virtualization of x86 processors.

4. **Visual MainWin:** Visual MainWin provides a compiler support system with which applications or programs developed for windows can be executed on various platforms including FreeBSD, Linux and Solaris.

5. **vCUDA:** vCUDA provides virtualization support for general purpose GPUs with which applications which are data intensive can be executed under special guest operating system. One major limitation of vCUDA is that running of these applications on virtual machines direc ory carries many difficulties.

2.2 VIRTUALIZATION STRUCTURES/TOOLS AND MECHANISMS

Q15. Write short notes on Xen architecture. . Model Paper-II, Q3(b)

Ans: Xen is the most popular implementation of paravirtualization. It supports full virtualization using hardware level virtualization and allows high performance execution of guest operations performed on OS by eliminating the performance loss at the time of instruction execution guest OS can be modified accordingly.

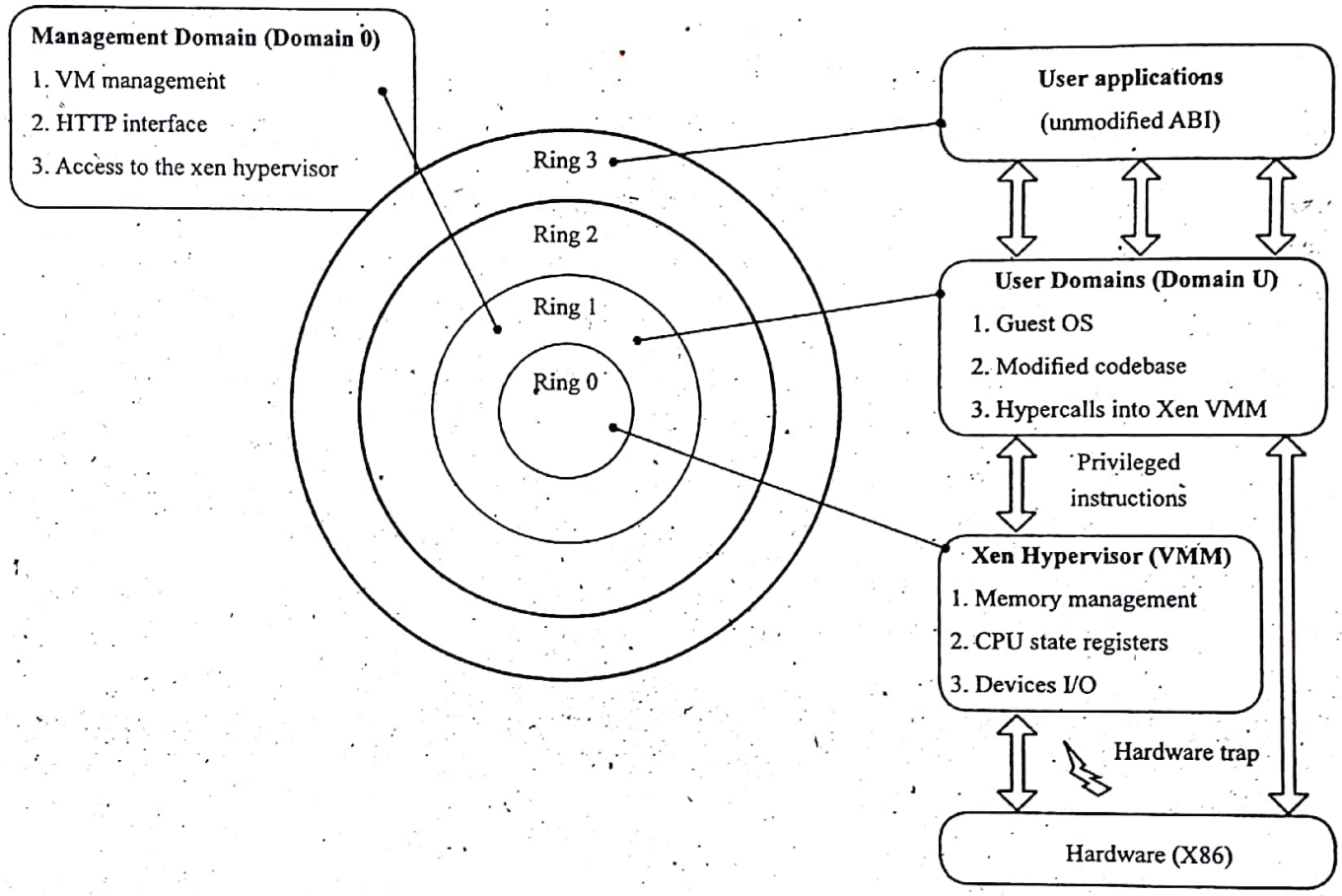


Figure: Xen Architecture and Guest OS Management

Xen-based system is typically handled by Xenhypervisor with which it can be executed in a highest privileged mode where it is controlled at the hadrware level of a guest operating system. Guest OS denotes the virtual machine instances and executed in domains. In domain 0, the specific control software has privileged access to the host and controls the other guest OS.

In X86 implementation, ring 0 denotes the level with highest privileges and ring 3 denotes the level with the lowest privileges. Every OS uses ring 0 a kernel mode and Ring 3 as user application and non-privileged OS code.

In Ring 0, Xen Hypervisor (VMM) is implemented. Domain 0 can execute every guest OS which is referred as domain U in Ring 1 however user applications can run in Ring 3. Sometimes, the execution of a code can be executed from Ring 3 to Ring 0 by the using X86 instruction set. At hardware level these operations are performed in the virtualized environment which generate results like a taps or silent faults and they do not allow the operations to be performed on guest OS.

Paravirtualization requires the OS to modify only the code base but not the overall OS used in guest system in a Xen-based environment. It is not possible for a hardware assisted virtualization to be executed at Ring 1 and guest OS at Ring 0.

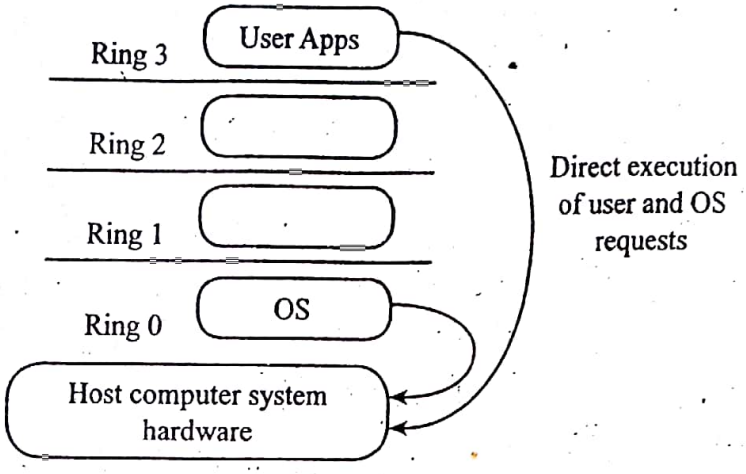


Figure: X86 Privillege Level Architecture without Virtualization

Q16. Classify the hardware virtualization.

Ans: Hardware-level virtualization provides an abstract execution environment in terms of computer hardware can be executed on the top level of a guest operating system figure below shows the hardware virtualization reference model. The virtual machine manager uses hypervisor as a software and hardware combination that can accepts the underlying physical hardware.

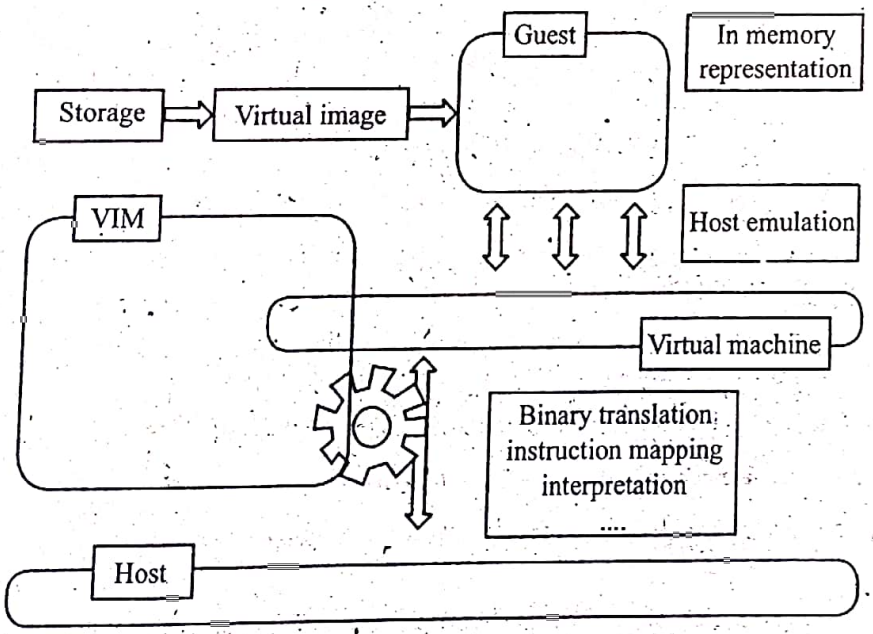


Figure: Hardware Virtualization Reference Model

The hardware virtualization is nothing but the system virtualization that provides ISA to virtual machines and denotes the ardware interface of a system.

lypervisors: Hypervisor is the fundamental element to the hardware virtualization which is also known as the Virtual Machine lanager (VMM). The guest operating systems can be installed and recreated within the hardware environment. These hypervisors re of two types,

ype 1: It runs directly on top of the hardware, so OS directly interact with the ISA interface. As it runs natively on the hardware, is also known as "native virtual machine".

ype 2: It is providing the virtualization services with the help of OS by interacting through the ABI and emulate the ISA of rtual hardware for guest operating systems. It is hosted within an operating system and therefore is also known as "host virtual achine".

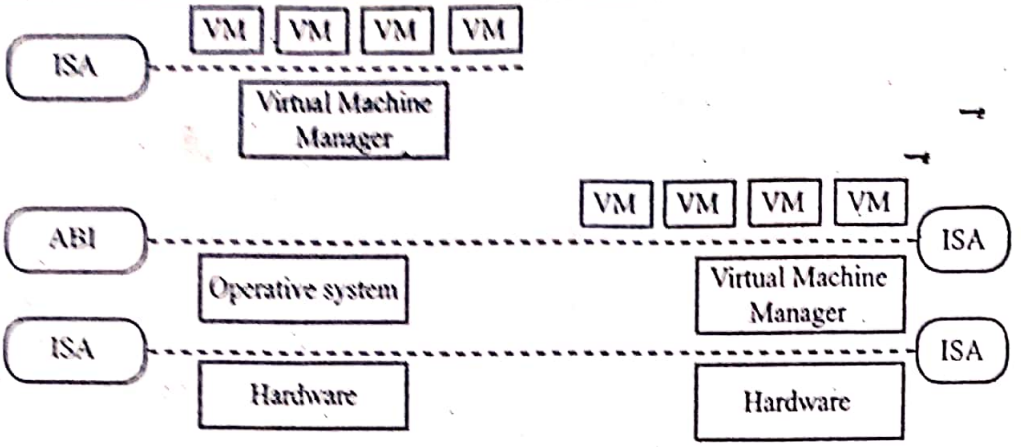


Figure: Hosted (Left) and Native (Right) Virtual Machine

A virtual machine manager is internally organized is shown in below figure.

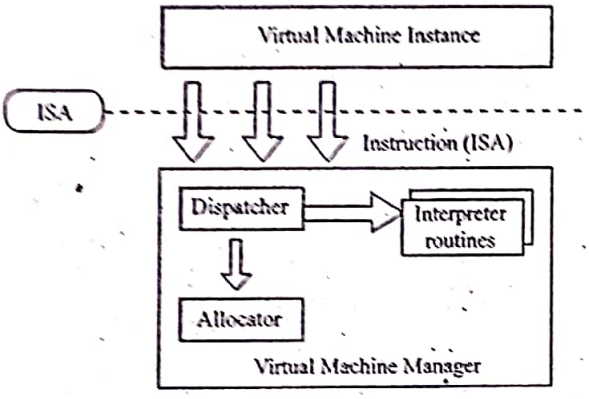


Figure: Hypervisor Reference Architecture

It uses three modules to provide coordination among underlying hardware components. They are,

1. **Dispatcher:** It monitors the instructions and reroutes them to the allocator and interpreter routines. The instructions are issued to the dispatcher by the virtual machine instance.
2. **Allocator:** It decides which system resources are to be provided to the virtual machine that usually tries to change the machine resources and makes the execution instructions to interact with the VM.
3. **Interpreter:** It executes the routines when a machine executes a privileged instruction.

With respect to virtual machine manager, hardware virtualization posses three properties. They are,

(i) **Equivalence:** Virtual machine manager controls the active guest that shows the common behaviour if it is directly executed on a physical host.

(ii) **Resource Control:** Virtual machine manager can be under the control of virtualized resources in certain situations.

(iii) **Efficiency:** Dominant fraction can be done in a statistical way on the instructions of machine that should execute without any intervetion from the virtual machine manager.

Popek and Goldberg proposed three theorems that defines properties and provides certain instructions based on hardware which can perfectly support the virtualization. They are,

Theorem 1: For any conventional third-generation comput , VMM may be constructed if the set of sensitive instructions for that computer is a subset of the set of the privileged instructions.

This theorem establishes that every instruction is used to change system resources configuration that can be taken from the user mode and virtual machine manager has controlled the execution process. It accepts the hypervisors for controlling the instructions perfectly that shows about an abstraction layer, and can be executed without any loss of performance. If hypervisor is in privileged mode (Ring 0) then it will be in resource control property. Non-privileged instructions are executed normally without any involvement of the hypervisor. The property of equivalence is considered as efficient since the code output is identical in both cases because it cannot be changed.

heorem 2: A conventional third-generation computer is recursively virtualizable if, it satisfies the following two conditions,

It is virtualizable

A VMM without any timing dependencies can be constructed for it.

Recursive virtualization has an ability to run the virtual machine manager at the top of another virtual machine manager. accepts the nesting supervisors whose the capacity is big enough to accommodate it to the underlying resources. virtualizable rdware already exist for the recursive virtualization.

heorem 3: A hybrid VMM may be constructed for any conventional third generation machine in which the set of user sensitive structions are a subset of the set of privileged instructions.

Hybrid Virtual Machine (HVM) is another term, whose efficiency is lower than the virtual machine system. More number instructions in the HVM can be interpreted instead of directly executing. But the instructions can be interpreted in virtual pervisor mode only. An attempt is made to execute the behaviour sensitive or the control sensitive instructions using HVM to ntrol the direct execution or else it can be controlled through a trap. To stimulate every sensitive instruction it can be monitored th use of HVM.

17. List and explain the various hardware virtualization techniques. Explain them briefly.

ıs: Model Paper-I, Q3(b)

The various hardware virtualization techniques are as follows,

1. Hardware-assisted virtualization
2. Full virtualization
3. Paravirtualization
4. Partial virtualization.

Hardware-assisted Virtualization: This type of virtualization provides architectural support to build a virtual machine manager that can run a guest operating system in isolation. Extensions to *x*86 - 64 bit architecture in Intel VT and AMD V are the examples of hardware - assisted virtualization. These extensions minimize the performance penalties and obtains better performance. This is possible by emulating *x*86 hardware with hypervisors.

Full Virtualization: This type of virtualization runs a program/operating system on the top of virtual machine without modifying the program. This operation is performed successfully when the virtual machine managers provide emulation of the complete hardware. This method provides isolated and secured virtualization allowing different systems to exist on the same platform. The key to build a secured and efficient implementation is to combine the hardware and software and present the execution of harmful instructions directly on the host.

Paravirtualization: This type of virtualization opens up a software interface for the virtual machine which is modified from the host. This modification will require the guest to be modified. Paravirtualization performs direct execution of performance critical operations without any performance loss. It does this by transferring the complex operations of virtual machine manager directly onto the host.

Partial Virtualization: This type of virtualization partially emulates the hardware without executing the guest operating system in a complete isolated environment. It allows the applications to run in a transparent way. However, it is not able to provide all the features of operating system to it (i.e transparently run applications). Address space virtualization in time-sharing systems is an example of this type of virtualization. It allows multiple applications and users to run concurrently in separate memory space. These applications share the same hardware resources.

. Write about programming language level virtualization.

: This type of virtualization implements virtual machines that can easily be deployed, managed and ported. The virtual ine executes byte code of a program. It is basically a simplified implementation of its hardware instruction set. It provides level instructions that are in accordance to some feature of languages that are compiled for them. Compilers implemented this technology develop a binary format that represents a machine code for an abstract architecture.

Java and CLI are stack-based virtual machines. The abstract architecture of the reference model is developed on the basis of an tion stack that performs all the operations. The byte code for this architecture contains instructions that load operands onto the and perform operations onto it. Then the result is put onto the stack. It also includes instructions for invoking methods, managing s and classed. This type of virtual machines are easy to interpret and are executed by lexical analysis. They are portable.

ntages

Provides uniform execution environment

Simple development and deployment

Managed execution provides the security by filtering the I/O operations to support the sand boxing of applications.

No requirement of various versions of same code.

2.3 VIRTUALIZATION OF CPU, MEMORY AND I/O DEVICES

Q19. Write about CPU and memory virtualizations.

Ans: Model Paper-III, Q3(a)

CPU Virtualizations: In a virtual machine environment, higher efficiency is achieved by running unprivileged instructions on host systems. In order to carryout CPU virtualization, both privileged and unprivileged instructions need to be supported by CPU. These instructions should be executed in the user mode and the virtual machine manager needs to be in the supervisors mode. Once privileged instructions get executed, VMM captures these instructions and allocates hardware resources to various virtual machines. This allocation ensures accuracy and stability of the system.

One major fact related to CPU virtualization is that some CPUs such as RISC are naturally virtualized whereas some CPUs such as x86 cannot be virtualized. The reason behind the naturally virtualized architecture of RISC CPU is that behavior sensitive and control instructions are considered as privileged instructions. The reason behind the unsupportive nature of x86 CPU architecture is that many sensitive instructions are not considered as privileged instructions. Therefore, VMM fails to capture such instructions during their execution.

Unlike UNIX based systems where control is handed over to the kernel using a system call which generates an interrupt of 80h, systems that are based paravirtualization, control is handed over to hypervisor using a system call of guest operating system which generates an interrupt of 80h. After successful completion of a task, the control is returned to the kernel of guest OS. A major advantage of CPUs that are based on paravirtualization is that they allow execution of unmodified applications on virtual machine. However a small degradation of performance occurs.

The process of virtualization in para and full virtualization is complex and to eliminate such complexities, hardware assisted CPU virtualization is used.

Hardware Assisted CPU Virtualization: To eliminate the complications, AMD and Intel x86 CPUs make use of a special mode called privilege mode level or ring-1. Creation of such a layer assists the system in running the OS at ring 0 and at ring-1, hyper visor can carryout its functionality. Instructions automatically gets captured in the hypervisor thereby eliminating the need of performing binary translation of full virtualization.

Memory Virtualization: Virtualization of virtual memory is identical to the process of paging or page table where OS is responsible for carrying mappings of virtual memory to machine memory.

Paging is a non-contiguous allocation scheme. It divides the physical memory into fixed-sized blocks called frames and logical memory into pages. The blocks and pages are of the same size as a result one logical page fits perfectly in 1 physical block.

Memory Management Unit (MMU) handles this paging mechanism. It uses a page table in which information of frames and pages are stored. It generates a page fault when the requested data is not found in memory.

Moreover, MMU even handles demand paging which is a sort of swapping where in pages of data are not copied until needed from disk. MMU uses a Translation Look aside Buffer (TLB) for paging. TLB is a small piece of associative memory within a processor. It catches part of translations from virtual to physical address.

Address Translation in Paging: Translation from logical address containing page number and offset into a physical address containing frame number and offset is done in order to read a word from memory. The page table is of variable length, due to this it cannot be held in registers and must be in main memory. The following figure show the address translation is a paging system.

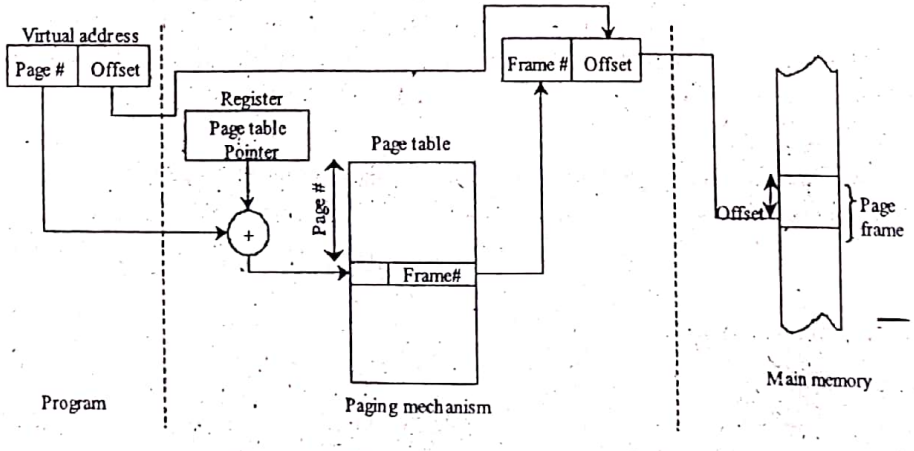


Figure: Address Translation in a Paging System

When a particular process is being executed, a register holds the starting address of page table for that process. Page number of a virtual address indexes the table and looks up the corresponding frame number. This is added to the offset portion of virtual address inorder to derive the desired real address.

However, the disadvantage of this virtualisation is that the amount of memory used up by the page tables alone can be high. To overcome this, virtual memory schemes store page tables in virtual memory than in real memory and so the page tables are also subjected to paging. When a process is being executed a part of the page table along with the page table entry of the currently executing page must be in main memory. Some processors employ a two level scheme to organize large page tables. This scheme requires a page directory in which each entry points to a page table. So, if length of page directory is 'x' and if maximum length of it is 'y', a process will consist upto xy pages. Usually, length of page table is restricted to one page.

Q20. Describe I/O virtualization.

Ans: Serving requests related to input and output with use of virtual devices and original hardware is referred to as I/O virtualization. It can be implemented in three ways namely, full device emulation, paravirtualization and direct I/O.

1. **Full Device Emulation:** Using full device emulation, physical devices can be emulated. It uses software to replicate functionalities performed by various devices. This software is included in the VMM itself in the form of a virtual device. The requests generated by the guest operating system which are related to I/O are captured by VMM which inturns communicate with the associated hardware.

2. **Paravirtualization:** In a virtual machine environment, multiple virtual machines can utilize a single device and use of software makes this execution slower. For this reason, architectures such as Xen uses paravirtualization method for serving I/O requests. This method carries front end and back end drivers and hence it is called as split driver model. The front end and back end drivers belongs to domain U and O respectively and communicate through a shared memory block. The functionalities of both of these drivers are handling I/O requests and handling I/O devices respectively. Use of this method eliminates the drawback involved in full device emulation but involves CPU overhead.

3. **Direct I/O:** This method provides a platform with which devices can be assessed directly by virtual machines. It is capable of achieving the performance close-to-native without involving additional costs but most of such implementations are getting used in networking of mainframes.

One alternative of these approaches is the use of SV-IO (Self Virtualized I/O). Its major focus is to utilise the resources associated with multi-core processor. It carries all the activities involved in making the I/O devices virtualized. Here, virtual machines are provided with access to API and virtual devices whereas the control of API is allocated to VMM. It also provides a special interface called as virtual interface to each of the virtual device associated with the I/O. The communication between these interfaces and the OS is carried out using device drivers of these virtual interfaces. These interfaces carry two types of message queues for incoming and outgoing of messages along with a unique ID.

Q21. Discuss about the virtualization in multi-core processors.

Ans: As multi-core processors involve multiple cores of processors within a single chip, the process of virutalization is much more complex. The challenges that arise in such a virtualization process are,

1. Applications must fully utilize the overall cores involved in a multi-core processor in a parallelized format. For this, it is necessary to involve new models for programming, libraries and languages.
2. The cores must be allocated with the tasks explicitly by the software. For this, it is necessary to involve various policies for resource management and scheduling algorithms.

Apart from these two challenges, the technological improvement are also imposing certain challenges. This is because CPU cores are getting integrating with CPU cores which is called as dynamic heterogeneity.

Certain virtualization methods are developed for virtualizing such processor cores which are as follows,

1. **Well's Method:** Using this method, hardware designers can capture the description of processor cores. This minimizes the overhead and inefficiencies involved in controlling hardware resources with respect to the software. The abstraction provided by this method is stored in ISA and cannot be modified by OS or VMM. In this method, a software visible VCPU is used which migrates from one core to another. It is responsible for suspending the active VCPU in case of absence of appropriate cores.

2. **Virtual Hierarchy:** This method was proposed by Marty and Hill which is dedicated for the workload optimization of space sharing. Using this method, the cores which are present in larger quantity are used in a space sharing environment to allocate a group of cores with multiple jobs to be carried out simultaneously. The time intervals for these jobs are longer enough. Using virtual hierarchy. The space sharing can be designed accordingly which is not possible in case of fixed physical hierarchy.

The physical hierarchy in modern many-core CMPs two or more than two levels of cache. These levels in case of virtual hierarchy performs the following actions.

Level-1: At this level, the following actions are performed,

- ❖ Allocation of blocks to the cores which are closer to each other.
- ❖ Establishment of shared-cache domain.
- ❖ Establishment of point of coherence.

In case that a tile of block gets missed, an attempt is made to locate it in the level-1 itself. In case if it cannot be allocated, then it is accessed in level-2..

The three types of workloads i.e., database workload, webserver workload and middle-ware workload are assigned to three clusters of virtual cores. They are VMO-VM3, VM1-VM2 and VM4-VM7 respectively. Using such cores, the workloads are executed on their responsible virtual machines.

2.4 VIRTUAL CLUSTERS AND RESOURCE MANAGEMENT

Q22. List the features of virtual clusters.

Ans: Virtual clusters make use of virtual machines that are employed as physical clusters on a distributed server. These virtual machines communicates with each other using a virtual network. They provide some attracting features in a virtualization environment which include the following,

(i) The nodes associated with virtual clusters can be implemented as VMS and physical machines and they can employ multiple operating systems on a single node.

(ii) Even with the inclusion of virtual clusters, virtual machines can be replicated among available servers which assist in making the system fault tolerant, recoverable and parallel.

(iii) A virtual cluster can be extended and compressed with respect to its size at any point of the distributed systems.

(iv) A typical physical cluster is distributed may cause failure of virtual machine if a failure occurs in one of its nodes whereas a failure of virtual cluster will not effect the functionality of virtual machines.

(v) OS on virtual machines and host machines can be different but can be implement in common.

(vi) Use of virtual clusters improves server utilization and provides flexibility in handling various applications.

Q23. Explain in detail about VM migration on services.

Ans: Model Paper-IV, Q3(b)

Virtual Machine Migration Services: In case of virtual machine the term migration service can be defined as the mechanism in which it involves a Virtual Machine (VM) is moved from one host server(or) storage location to another server. In this mechanism the components of all basic machines are completely virtualized. The Virtual Machine(VM) migration services are supported by lot of VM migration techniques such as hot/life migration cold/regular migration and live storage migration of a VM.

Migration Techniques: The various migration techniques are discussed below,

1. **Live Migration and High Availability:** Live migration or real-time migration is the process of moving a running VM or application between physical machines without disconnecting the client or application while being powered on. The proper execution of this process takes place without any noticeable effect from the perspective of the end user's. The proactive nature of live migration supports a system failures by providing the solution for potential problem before the disruption of service occurs. Thus, indirectly providing a system with high availability with failure recovery as well as with load balancing by sharing the workload among the various machines with the optimized utilization of available CPU resources.

2. **Live Migration Anotomy, Xen Hypervisor Algorithm:** The anotomy of live migration involves the practical analyzation about live migration's mechanism and how memory and VM states are being transferred via network, from one host say A, to another host say B, this can be achieved by using Xen hypervisor mechanism. The following figure shows the logical steps that are executed while OS migration is executed where it can be viewed where it can be viewed as a transactional interaction between the two hosts.

The timeline process of live migration involves the following steps which passes through various stages,

Stage 0(Pre-Migration): Within this stage pre-migration of an active VM will be started that exist on the physical host A.

Stage 1(Reservation): Here a resource that can migrate an OS from host A to host B is requested. But this is possible only if the required resources exists on host B and on a VM container of that size.

Stage 2(Iterative Pre-Copy): It is a shadow paging enabled iterative process that involves the subsequent iterations to copy dirty pages in successive rounds or the pages that are transferred from A to B in the previous transfer phase, of the first iteration.

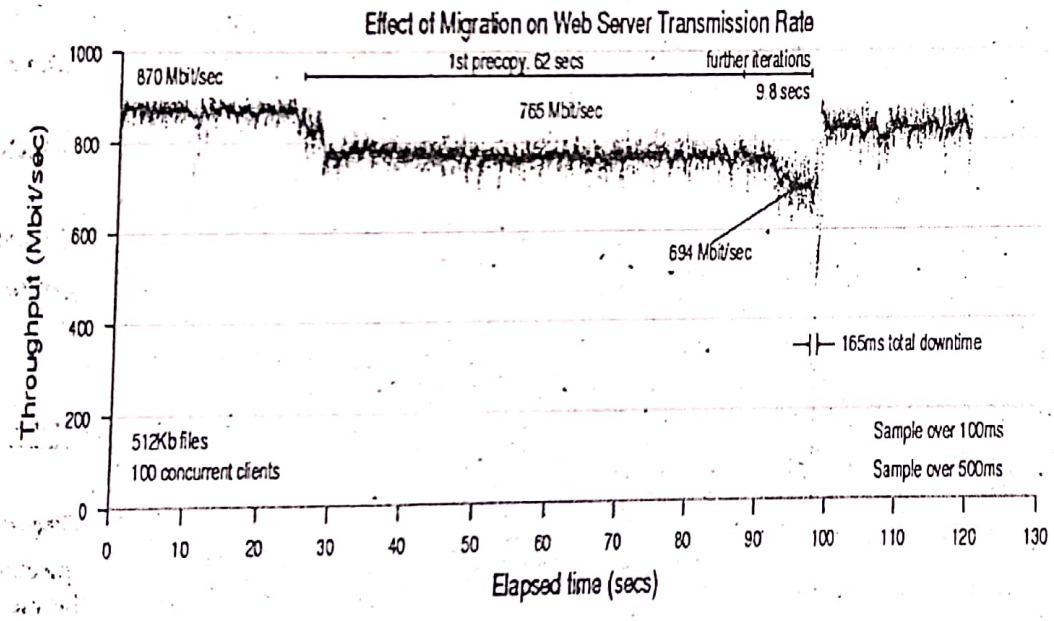
Stage 3(Stop-and-Copy): It occurs at the time of system downtime/that is when the running OS instance at A is suspended, then its network traffic is redirected to B. Thus, any variable memory pages and CPU state are then transferred. There is a constant suspended copy of the VM at both A and B at the end of this stage. The copy present at A is assumed as predominant and it is resumed when a failure is occurred.

Stage 4(Commitment): Host A give a commitment of the migration transaction by acknowledgement the OS image that have been received from the host B. Then the host A rejects the original VM and host B is considered as the primary host.

Stage 5(Activation): Here the activation of migrated VM is done on host B. Also, reattachment of the device drivers to the new machine is done by running the post-migration code which inturn can advertise moved IP addresses. Thus, the VM will run normally on Host B.

This approach provides assurity that the failure management with at least one host has a constant VM image at all times while performing migration.

3. **Live Migration Effect on a Running Web Server:** The effect of live migration was demonstrated on a running web server Apache 1.3 which served static content at a high rate as shown in the figure below,



Here a high through put is achieved when a set of one hundred concurrent clients are continuously served by a single 512 KB file. The storage capacity of web server VM is 800 MB. 870 M bit/sec is the approximate consistent throughput which is achieved by the server at the time when the trace 100 Mbit/sec starts is the limited rate at which initially the migration starts 27sec into the trace, that results in server's throughput falls upto 765 Mbit/sec. This starting ow-rate pass forwards 776 MB and remains for 62 sec. At this instance, the migration algorithm can increase it's rate for many iterations and finally suspends the VM after a further 9.8 sec. After 165-msec downtime the web server resumes at full rate and the final stop and copy phase transfers the remaining pages.

4. **Live Migration Vendor Implementation Examples:** There are several managing and provisioning tools of VM that helps in live migration of VM. Among all Vmware vmotion and citrix Xenserver "Xenmotion" are the best examples for the migration vendor implementations.

(i) **VMware Vmotion:** This tool has two beneficial features,

(a) It can perform automatic optimization as well as allocation of entire pool of resource for maximum hardware utilization flexibility and availability.

(b) It carries hardware maintenance even in the absence of scheduled downtime. In addition to this it also allow VM to move away from the collapsed server.

(ii) **Citrix XenServer XenMotion:** It is an advantageous feature of the product Citrix XenServer that is acquired from the xen live migrate utility. That facilitate an IT administrator to transport a running VM from one XenServer to another comfortably in the same pool without causing any interruption of services and making it a highly available service. So that, it can enhance the system available by sharing workloads.

5. **Regular/Cold Migration:** Cold migration refers to the migration of turned-off or suspended virtual machines. With this migration technique, the associated disks can be transported from one data store to another. It doesn't require the VMs to be on a shared storage. However the VMs are required to be turned off or available suspended before migrating. Migrating a suspended VM is considered as a cold migration because even if the VM is turned on it is not running. The process for implementing cold migration involves the following steps.

(i) Select the options move to a different database inorder to transfers the configuration files along with the other files such as, the Non-volatile Random Access Memory(NVRAM) file (BIOS settings), log files and suspended file from the source host to the storage area of the destination host.

(ii) Register the virtual machine with the new host.

(iii) On the completion of VM migration, the old version of the VM gets deleted from the source host.

6. **Live Storage Migration of Virtual Machine(VM):** Transporting the virtual disks or configuration file of a running VM to a new data store conveniently, with no interruption in the availability of the VM's service is known as live storage migration of VM.

Migration Virtual Macine SLA and On-Demand Computing: Migration is an important concept in data centers because it can easily adjust the priorities of resource to match the demanding conditions of the resource. With this concept the SLAs can be achieved. If a VM is found to be using resources beyond its assigned limit of fair share on the tariff of other VMs residing on the same host, then it is suitable either to move this machine to another host(Which is in use) or to assign additional resources to it(only if host machine has resources). This is done inorder to prevent violation of the SLA and to achieve the needs of on-demand computing resources. However, all such goals can be achieved only if ther exists an integration between the management tools of virtualization and SLA.

Migration of Virtual Machines to Alternate Platforms: The achievement of the most advantageous ability of data center's technologies is to migrate VM from one platform to another that depends on the source and target virualization's platforms and on the vendors tools who manges this facility.

Example: The migration between ESX hosts such as VMware server and the VMware workstation are handled by the VMware convertor.

Q24. State the advantages and disadvantages of virtualization.

Ans: Virtualization has become widely popular in cloud clouding. It eliminates the technology barriers like performance and delivers IT infrastructure and services. It has the following advantages and disadvantages,

Advantages

The various advantages for virtualization are,

1. Managed execution and isolation helps to control and construct secure computing of the virtualized execution environments. It reduce, the harmful operations without execution and it can be configured as a send box.
2. Portability for execution virtualization techniques, allows virtual machine instances to transport to a host physical system. The virtual machine instances are represented as a file and are executel only by virtual machine.
3. Portability reduces the maintenance cost since the number of hosts are lower than the number of virtual machine instances.
4. Virtualization reduce the cost by reducing the hardware and efficiently uses the resources. The coexistence of multiple systems allow the resources to be shared without any interference from others.

Disadvantages

1. Performance degradation in virtualization occurs when both the execution and scheduling of virtual machine manager is done together with other applications. This allows the resources of the host to be shared with each other.
2. Increased latencies and delays happen because of the placement of an abstraction layer between the guest and host.
3. Inefficient use of host and inaccesibility of host occurs when the abstraction layer does not expose all the features of host.
4. Malicious programs extract private information from the guest when the host is emulated transparently.

Q25. Describe the migration of memory, file system and network resources.

Ans:

Memory Migration: Memory migration refers to the moving of memory instances from one system to another. It can be accomplished in different ways. All these ways are based on sharing of a single implementation paradigm. Moreover, these methods are based on the capability of guest operating system to support the characteristics of workload. Size of memory instances to be migrated can range from megabytes to gigabytes.

A technique called Internet Suspend-Resume (ISR) makes use of temporal locality of the fact that memory instances can be in resumed and suspended states. The term temporal locality is nothing but the property of memory instances to differ from each other based on the amount of work done from its suspension to its initiation. Temporal locality in memory migration can be used by representing every file as a tree. This tree is copied into the virtual memory instances of both suspended and resumed states. Use of such an approach makes the system to forward only the files which are modified instead of sending all the files.

File System Migration: For an efficient migration of virtual machine, it is necessary that a clear view of filesystem associated with all hosts needs to be provided. To do this, a virtual disk is included with every virtual machine. The contents carried by these virtual disks are forwarded to the filesystem along with the other states. This approach is not feasible because modern disks are capable of storing large amount of data. An alternative method is to use a global file system with respect to all the systems. Thus the migration of contents from one system to another can be eliminated.

In ISR, a distributed file system is used which acts as a transport of suspended virtual memory to resume. A VMM uses its local filesystem to suspend or resume. A suspend operation is performed by moving the files of VM out of the file system while a resume operation is performed by inserting the VM files back into the filesystem. Use of such an approach eliminates the burden of creating distributed file system calls for various systems in a distributed environment.

In situations where users move around some specific areas such as home, office etc., smart copying can be used which is based on the concept of spatial locality. Here, the difference between two file systems is transmitted by considering the suspension and resume locations.

Network Migration: A virtual machine that is to be migrated must be capable of controlling all the network connections irrespective of forwarding, mobility and redirection mechanisms. Every virtual machine is provided with a virtual internet protocol address with which it can communicate with remote and local virtual machines. They can also be assigned with unique MAC addresses. These virtual addresses along with their respective virtual machine are stored in VMM.

When a migration is done within a LAN connection, a reply is generated using address resolution protocol indicating the change in address of a VM has occurred. When this indication is generated, all the packets that are to be forwarded to the old address are forwarded to the new address. However, the packet transmission that is in progress will be dropped.

2.5 VIRTUALIZATION FOR DATA CENTER AUTOMATION

Q26. What is meant by data center automation? Write short notes in data center virtualizaton.

Ans: Model Paper-III, Q3(b)

Data-Center Automation: The process of allocating large number of hardware, software and database resources to large number of users over the internet is referred to as data center automation. The process of allocation for all the users is carried out simultaneously in a cost effective way while providing quality of service.

Virtualization of Data Centers: Data center virtualization is a new era in computing field which enables virtualization of infrastructure. This virtualization allows multiple customers to share the same infrastructure simultaneously. Moreover, using the concept of infrastructure virtualization, the providers focus on providing managed services on remote basis as well as in cost effective manner. These managed services such as Saas, Paas, Mass are evolving and are considered as a core of computing service. Among these services, Saas is one of the services that is growing continually and is becoming a major part of cloud computing.

Basically, cloud computing is a set of Internet protocol services which enables the user to use certain functionalities on a "pay-for-use" basis.

The primary advantage of using cloud computing from enterprise customer point of view is that it is one of the substitutes for the expensive outsourced data centers. Apart from this, cloud computing even frees the customer from the overhead of having the information regarding the physical storage of data and service. This is because the customer of cloud computing pays for only those services that have been used.

Q27. Discuss in brief about storage virtualization and server virtualization.

Ans:

Storage Virtualization: Storage virtualization can be defined as the layer between physical storage and virtual storage. It maps the physical storage to virtual storage and vice-versa. In this, individual physical devices are abstracted to form one or more logical entities. The individual physical devices are no longer accessed directly by the operating system, instead they are accessed separately and independently. However, the virtual entities are only accessed directly by the operating systems.

Example: The volume manager of a server integrates the physical entities of disk stack and forms a large logical entity. Thus, forming a storage virtualization layer between the two entities. The storage virtualization is shown in the following figure.

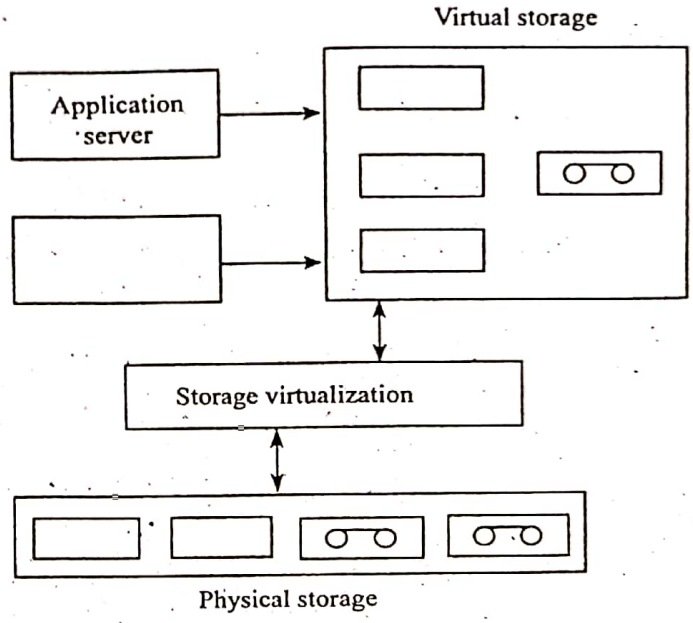


Figure: Virtualization/Storage Virtualization

Implementation of Virtualization: The storage virtualization can be implemented on three different levels of storage networks. They are,

- Server
- Storage devices
- Network.

Server Virtualization: Virtualization is a mechanism in which multiple independent virtual operating systems are made to run on a single physical computer. It is useful for maintaining of return on investment for the computers.

The term virtualization was coined during the year 1960s with content to a virtual machine which sometimes referred to as a pseudo-machine. The virtual machines were used to be created and managed, this process is oftenly referred to as 'platform virtualization'.

A software called control program is used to perform the platform virtualization. This program generates a simulated environment called virtual computer which makes the device to utilize the hosted software of a particular virtual environment which is sometime known as guest software.

The guest software is oftenly behave as a complete operating system and run as if it has been installed on a stand-alone computer.

Oftenly, multiple virtual machine can be simulated on one physical computer. The number of virtual machine to be used depends on the physical hardware resources of the host device. Because the guest software can perform its function by accessing to particular peripheral devices. And therefore, the virtualized platform is used to support this access i.e., it support guest interfaces to those devices. Example of this devices may include, disk drive, DVD, CD-ROM and network interface card.

The technology of virtualization is an approach that can be used to reduce the maximum of hardware acquisition, thus used for costs maintenance.

Q28. Illustrate VM-based intrusion detection system. Model Paper-IV, Q3(a)

Ans: An intrusion detection system is a defensive tool used for detecting malicious attacks that can affect the security features of a system. These systems are employed not only for early detection of attacks but also for preventing the attacks. They can be of two types i.e., host based IDS and network-based IDS.

HIDS has a different functionality from that of a NIDS. A NIDS is located on a computer network to detect the actions across the entire network whereas a HIDS is located on a specified computer server to detect the actions performed by only that server. HIDS is also known as a host or a system integrity verifier. It detects the position of a configured file when an attacker creates, changes or deletes those files. Hence, Host-based Intrusion Detection Systems (HIDSs) are designed to create, detect or examine the actions performed on a particular network host.

A HIDS not only stores information about the configured files but also about the configurable databases such as windows records. They check the configured files to determine whether an attack has occurred or not. HIDSs install software programs and stores data about various available storage locations to keep the user's information on a specific host. A HIDS permit an organization to detect attackers who are responsible for performing malicious activities.

HIDSs are used mainly when an attacker attempts to access files or operations located on a single computer. The operating system is fragmented into different hosts by the intruders. This allows an IDS to develop individual entities for placing IDS as a centralized IDS. The problems such as inheriting security features can be prevented by a centralized IDS. When HIDSs are installed on a particular host, there are no individual intrusion entities as in NIDSs because of which there is a drastic reduction in cost in host-based intrusion detection systems. As a result, centralized IDSs are cheaper than distributed IDSs. Figure below represents a centralized IDS.

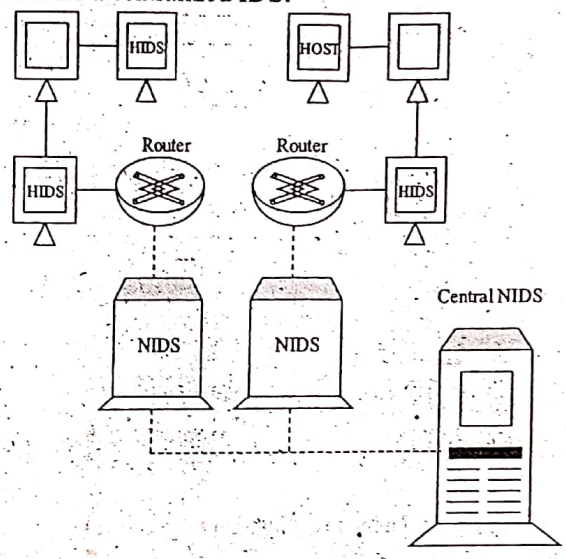


Figure: Centralized IDS

VM-based IDS works similar to NIDS as the virtual machines which are intruded do not affect the functionality of others. To avoid unauthorized actions, VMM always verifies access request to carryout the functionality of HIDS.

VM-based IDS is typically implemented using two methods. First, it can be implemented as a process which is independent and is included in every virtual machine. Second, it can be included in VMM with higher privilege over hardware. In some systems, policy framework is employed to trace all the activities involved in the virtual machine of guest OS. When an intrusion is detected, a detailed analysis is performed. Some other techniques such as honeypots and honeynets are also used in detecting the intruders in a VM.

Q29. What is Eucalyptus? Explain the architecture of Eucalyptus.

Ans:

Eucalyptus: Eucalyptus is a free and open-source computer software or infrastructure which is used to implement cloud computing on computer clusters. That is used for building Amazon Web Services(AWS) compatible with private and hybrid cloud computing environments marketed by the company Eucalyptus system. The Word EUCALYPTUS is an abbreviation of Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems. Allows pooling compute, storage and network resources that can dynamically scaled up or down as application workload change. Following are the features offered by Eucalyptus.

1. Cloud based systems and user accounts are managed by cloud administrator's tool.
2. It provides the EC2, S3 interface compatibility.
3. Eucalyptus software installation and deployment is easy.
4. Multiple clusters configuration with private internal network addresses into a single cloud.
5. Platform support for most linux distributions.
6. SOAP with WS security enables secure internal communication.
7. Xen hypervisor of KVM platform support for running VMs.

Eucalyptus Architecture: The architecture of Eucalyptus is a high-level architecture, that is comprised of high level system's component as a stand-alone web service as shown in the following figure,

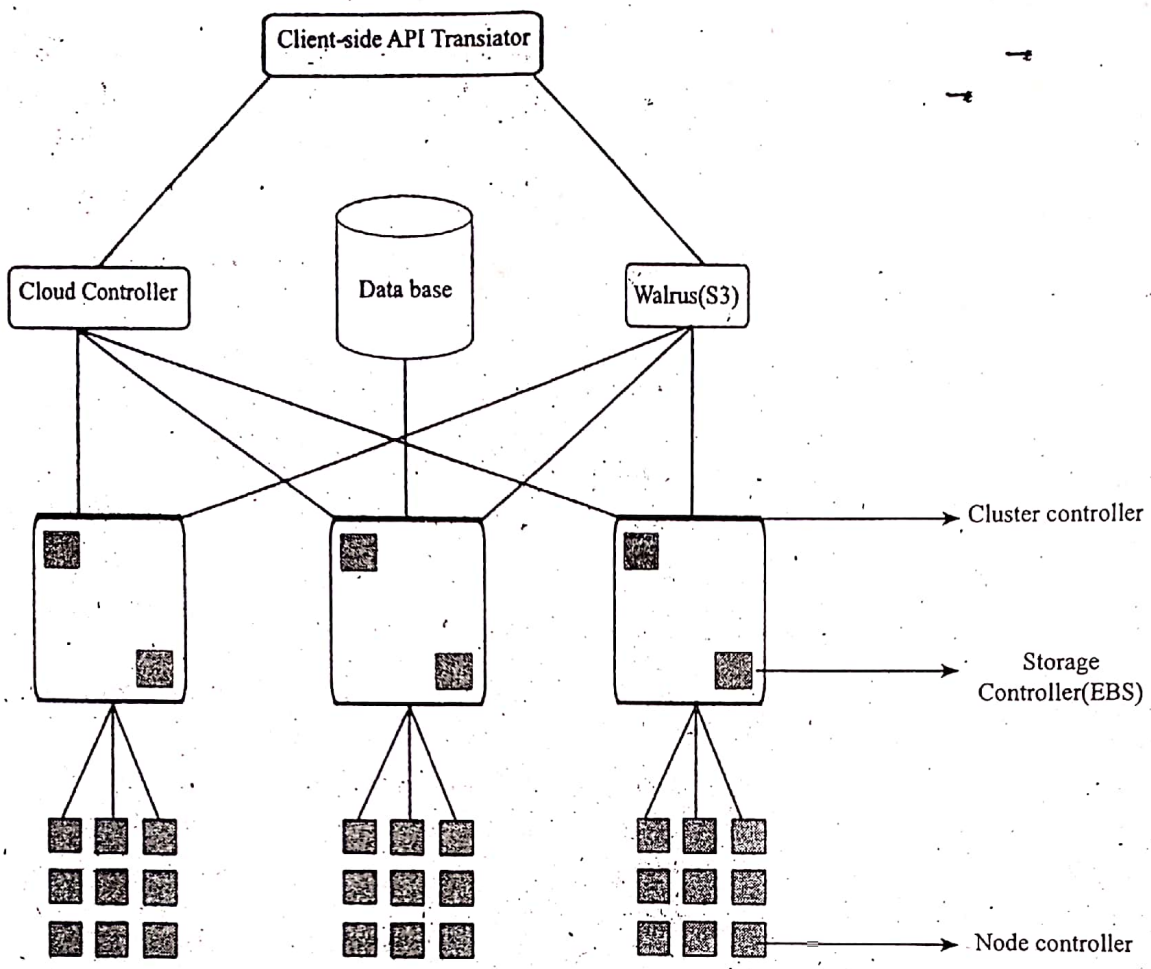


Figure: Eucalyptus High-Level Architecture

1. **Node Controller(NC):** NC is responsible for controlling the VM instances-execution, inspection and termination that run on the host.
2. **Cluster Controller(CC):** CC is responsible for collecting VMs information and scheduling its execution on particular node controllers. In addition to this it also manages virtual instance network.
3. **Storage Controller(SC):** SC allows the user to store and access VM images and user data by authorizing as put/get storage services through the implementation of Amazon's S3 interface
4. **Cloud Controller(CC):** CLC controls the users by acting as an entry point for both the clients and the administrators. Beside, this it makes request to cluster controllers by making the high-level scheduling decisions which are taken by querying the mangers for information about resources availability.
5. **Walrus(W):** With in the Eucalyptus software tool walrus is the controller component that controls the access to the storage service. This controls the input requests for the resource allocation through the SOAP communication interface.