NSM&V

Virtualization

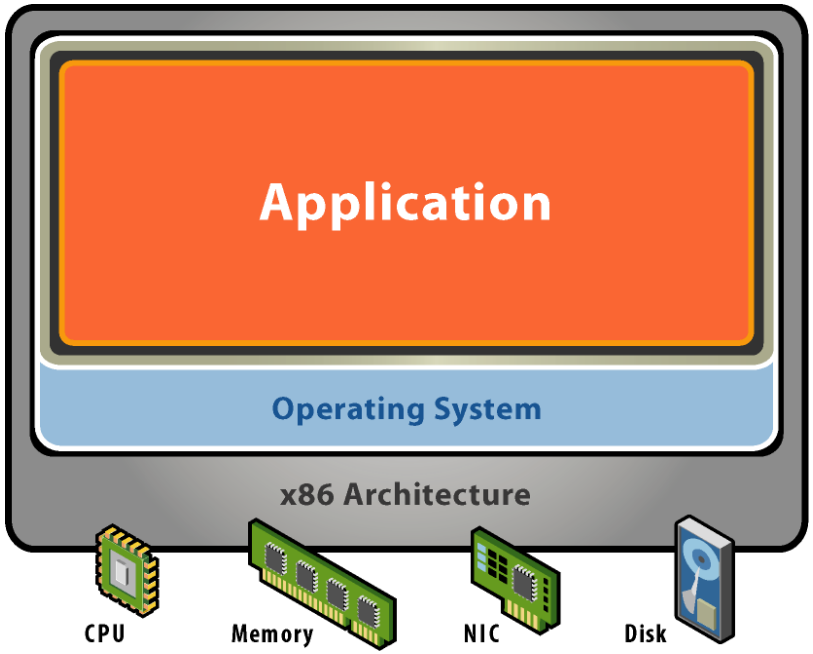
Starter Example Questions…10 mins

1. Why is Virtualization so popular with modern organisations?
2. What is a host OS?
3. What is a guest OS?
4. What is a type I and type II hypervisor?
5. What is the difference between "Bare Metal" and "Hosted" Virtual environments?
    a. Examples of products for each.

Traditional Computing

- In a traditional implementation, the operating system (Microsoft Windows, Suse Linux, MAC OS) is installed directly on a physical computer's hard drive and has exclusive access to any hardware on the physical machine, such as memory, network interface cards, and USB ports.
- Once installed, local operating system coordinates communication between itself, applications, and the hardware resources, which comprise the physical computer.
- **In terms of having managerial authority over all hardware, the local operating system calls the shots**

Starting Point: A Physical Machine



- Physical Hardware
  - Processors, memory, chipset, I/O devices, etc.
  - Resources often grossly underutilized
- Software
  - Tightly coupled to physical hardware
  - Single active OS instance
  - OS controls hardware

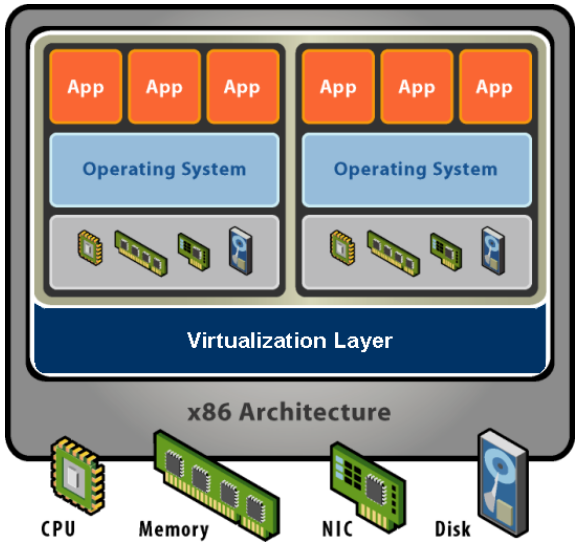
Introduction

- Virtualization is now an accepted solution for many organisations.
- Although they have been around for a long time, virtualization technologies are now available for a nominal cost.
- For some loading a few virtual servers on to hardware is enough.
- For others, a move to a complete Virtual infrastructure is required.

Virtualization

- By virtualizing different components of the IT infrastructure, one can:
  - Reduce the amount of physical space consumed by racks/cabinets
  - Reduce management overhead with centralized management,
  - Increase efficiency
  - Reduce downtime
  - The process of server deployment is simplified
  - The time involved is reduced with easier and faster deployment

What is a Virtual Machine?



- Software Abstraction
  - Behaves like hardware
  - Encapsulates all OS and application state
- Virtualization Layer
  - Extra level of indirection
  - Decouples hardware, OS
  - Enforces isolation
  - Multiplexes physical hardware across VMs

Virtualization is the addition of a software layer (the virtual machine monitor) between the hardware and the existing software that exports an interface at the same level as the underlying hardware.

Virtualization Properties

- Isolation
  - Fault isolation
  - Performance isolation
- Encapsulation
  - Cleanly capture all VM state
  - Enables VM snapshots, clones
- Portability
  - Independent of physical hardware
  - Enables migration of live, running VMs
- Interposition
  - Transformations on instructions, memory, I/O
  - Enables transparent resource overcommitment, encryption, compression, replication …

Notes (1)

- Virtualization has three main properties that give rise to all its applications.
- **Isolation**
- First, virtualization provides isolation. Isolation is key for many applications and comes in several flavors.

- Fault Isolation. If one virtual machine contains a buggy operating system, that OS can start scribbling all over physical memory. These wild rights must be contained within the VM boundaries.
- Performance Isolation. Ideally VMs performance would be independent of the activity going-on on the hardware. This must be accomplished by smart scheduling and resource allocation policies in the monitor.
- Software Isolation. Most of the issues with computers today are complex software configurations. DLL hell on PCs, operating system and library versions, viruses, and other security threats. VMs are naturally isolated for each other by running in separate software environments.

Notes (2)

- Virtualization has three main properties that give rise to all its applications.

Encapsulation

Encapsulation is the property that all VM state can be described and recorded simply. The VM state is basically the dynamic memory, static memory, and the register state of the CPU and devices. These items typically have a simple layout and are easy to describe. We can checkpoint a VM by writing out these items to a few files. The VM can be moved and copied by moving these files around. You can think about this as similar to doing a backup at the block level vs. doing a backup by recording all the packages, configuration and data files that encompass a file system.

Interposition

At some level all access to the hardware passes through the monitor first. This gives the monitor and chance to operate on these accesses. The best example of this is encrypting all data written to a disk. The advantage of this is that it does it without the knowledge of the OS.

What is a Virtual Machine Monitor?

- Classic Definition (Popek and Goldberg '74)

> A virtual machine is taken to be an *efficient, isolated duplicate* of the real machine. We explain these notions through the idea of a *virtual machine monitor* (VMM). See Figure 1. As a piece of software a VMM has three essential characteristics. First, the VMM provides an environment for programs which is essentially identical with the original machine; second, programs run in this environment show at worst only minor decreases in speed; and last, the VMM is in complete control of system resources.

- VMM Properties
  - Fidelity
  - Performance
  - Safety and Isolation

Benefits

- This brings many economic advantages.
- It allows an organization to run multiple operating systems, called virtual machines (VMs), simultaneously on a single physical machine.
- The ability to consolidate multiple machines allows the IT department to reduce its hardware and software costs as well as significantly reducing its operational costs.
  - Reduced number of servers
  - Less power consumption
  - Less maintenance overhead
  - More resource utilization
  - More efficient Hardware upgrades
  - More efficient Patch Management
  - More efficient Disaster Recovery Planning

Virtualized Infrastructure

- Virtualization isn't limited to simply creating virtual machines.
- Other infrastructure components, such as networking and storage can also be virtualized, hiding the complexities of the underlying networking and storage components from the virtual machines.
- Once virtualized, the physical resources such as processor power, network switches, and Storage Area Network resources can be aggregated and combined together for use by virtual machines
- This leads to better utilisation of physical resources, load balancing, and fault tolerance/redundancy

Virtualization Model

- Virtualization creates an environment by **presenting physical hardware components in a virtual form to a software based computer's guest operating system.**
- This provides a means of aggregating physical resources to one or more virtual machines running on a physical server.
- The physical hardware is hidden from the VM, and virtual hardware is presented in its place.
- This allows for an environment where several operating systems can run simultaneously on a single physical computer.
- This separation and aggregation of physical hardware is provided by a hypervisor.

Hypervisors

- A hypervisor, also called **virtual machine manager (VMM),** is one of many hardware virtualization techniques allowing multiple operating systems, termed **guests**, to run concurrently on a **host** computer.
- There are two types of Hypervisor:
  - Type 1 – Bare Metal Hypervisor
  - Type 2 – Hosted Hypervisor

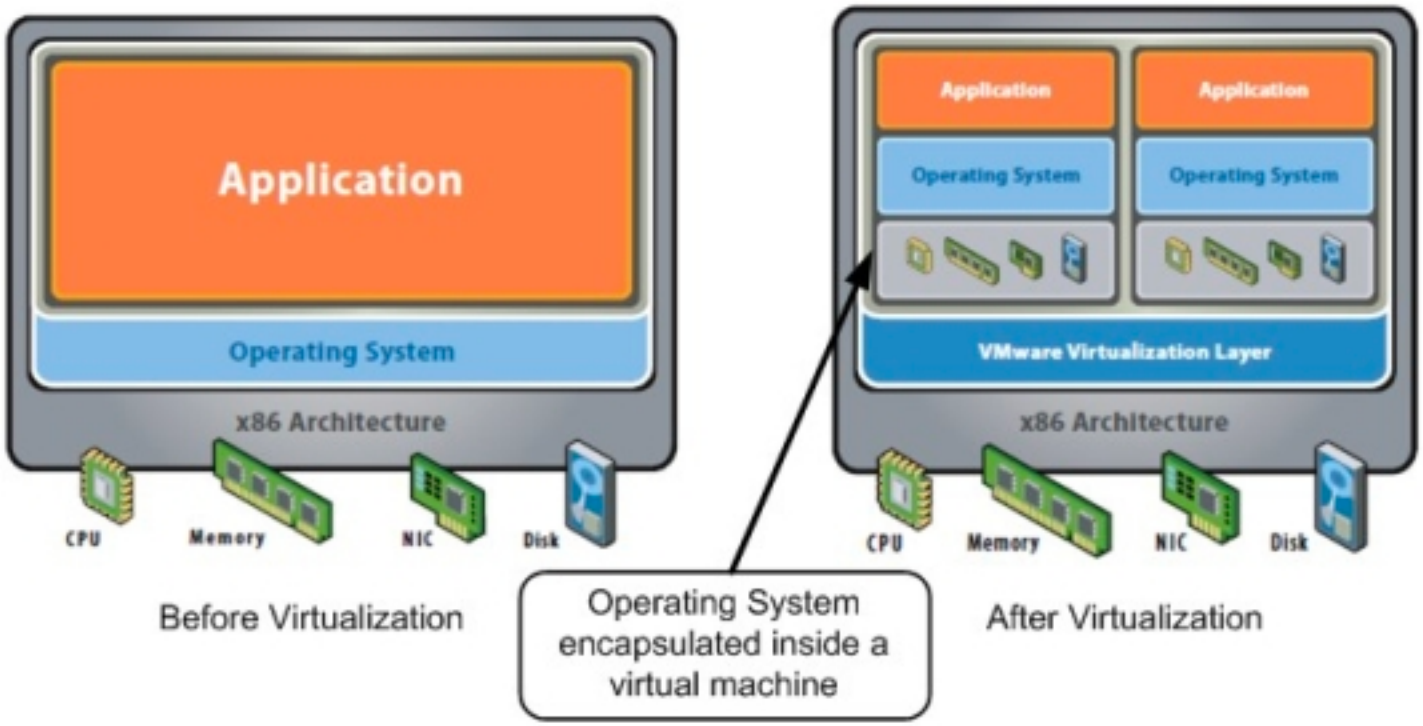
Hypervisors – Type 1

- A hypervisor is a virtualization technique, which provides a virtual operating platform for one or more simultaneous instances of an operating system.
- **A Type 1 hypervisor, also known as a bare metal hypervisor, is software installed directly onto a physical computer.**
- Once installed and configured, the **hypervisor will act as a mediator of sorts between the virtual machines, their guest operating systems, and the physical hardware now being controlled by the hypervisor.**
- The guest OS of a VM passes data to the virtual hardware presented to it, and it is then passed to the hypervisor, which handles the actual processing by physical hardware.
- E.G VMware use a hypervisor called ESXi

Hypervisors – Type 2

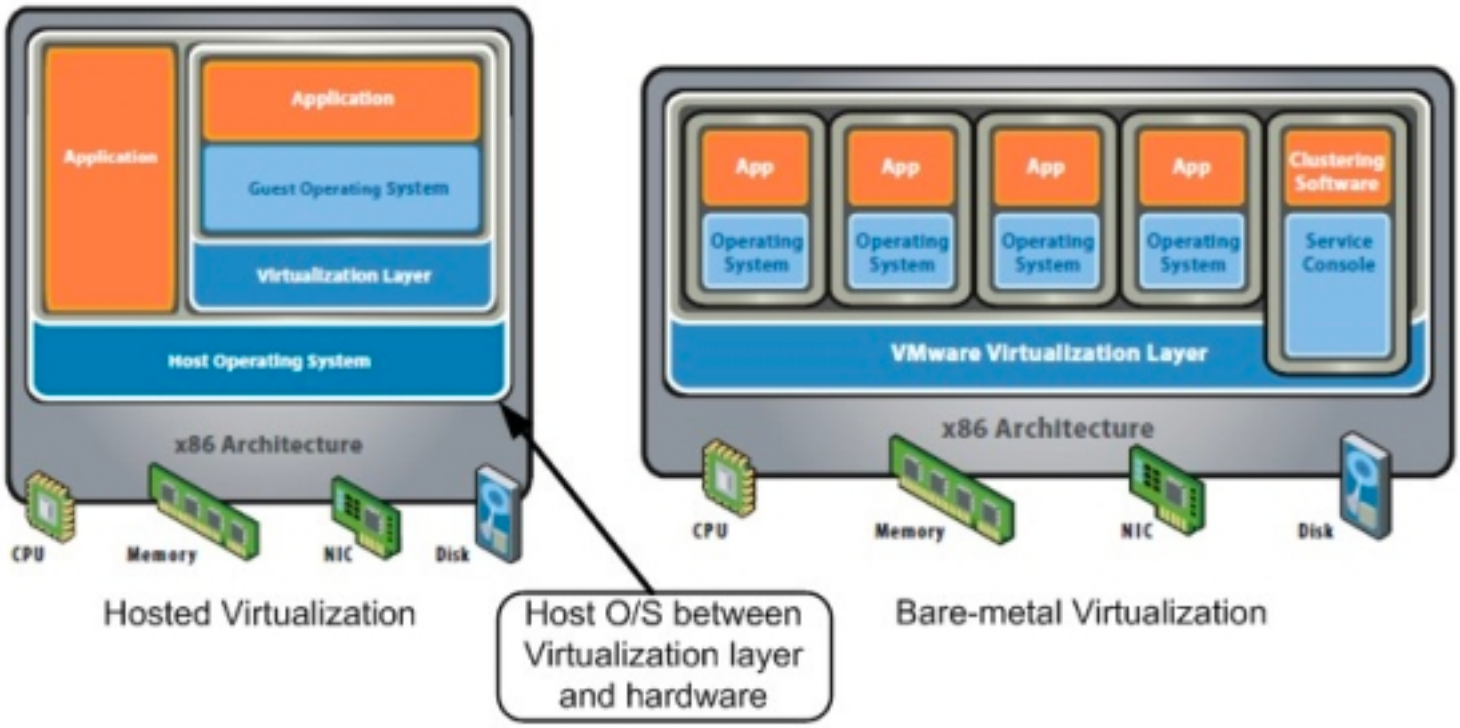
- A Type 2 hypervisor provides hypervisor functionality above, or on top of an already installed operating system.
- In short, the hypervisor is installed as an application, providing the platform for VMs.
- An example would be Oracle Virtualbox running on Windows 10 PC.

Before and after Virtualization



Ref: http://itknowledgeexchange.techtarget.com/virtualization-pro/what-is-virtualization/

Hosted Virtualization and Bare-metal Virtualization



Ref: http://itknowledgeexchange.techtarget.com/virtualization-pro/what-is-virtualization/

Hosted v bare-metal hypervisors

- Hosted hypervisors:
  - Requires a host operating system (Windows/Linux/Mac), installs like an application.
  - Creates virtual machine environments and coordinates calls for CPU, memory, disk, network, and other resources **through the host OS.**
  - Virtual machines can use all the hardware resources that the host can see.
  - Maximum hardware compatibility as the operating system supplies all the hardware device drivers.
  - Overhead of a full general-purpose operating system between the virtual machines and the physical hardware results in performance 70-90% of native.
- Bare-metal hypervisors:
  - Installs right on the bare metal and therefore offers higher performance and scalability but runs on a narrower range of hardware.
  - Many advanced features for resource management, high availability and security.
  - Supports more VMs per physical CPU then hosted products.
  - Because there is no overhead from a full host operating system performance is 83-98% of native. There is a small bit of overhead from the virtualization layer of the hypervisor

Ref: http://itknowledgeexchange.techtarget.com/virtualization-pro/what-is-virtualization/

Hosted v bare-metal hypervisors

- Type 1 hypervisors are generally preferred because they can :
  - Achieve higher virtualization efficiency by dealing directly with the hardware.
  - They provide higher performance efficiency, availability, and security than type 2 hypervisors.

- Type 2 hypervisors are used mainly on client systems where efficiency is less critical.
  - They are also used mainly on systems where support for a broad range of I/O devices is important and can be provided by the host operating system.
  - Examples of Type 2 hypervisors: Oracle Virtual Box, VMware Workstation, Microsoft Virtual PC

Computer Virtualization

- Because each VM is presented with its own unique virtual hardware, they are unaware of each other and of the fact that they are not communicating directly with physical hardware.
- **Failure of a VM does not affect the operational state of another VM.**

- The *use of virtual hardware also means that the guest OS of a VM is not dependent on the physical hardware, allowing VMs with different guest OSs to run simultaneously*

Resource Sharing

- A key component of virtualization is resource sharing.
- Virtual machines share access to CPUs (scheduled by the hypervisor)
- VMs also share access to the Physical network and disk components
- They are also assigned their own memory
  - The virtualization layer creates an address space the same size as what is allocated, this allows multiple VMs to work simultaneously and to protect each VM's memory from the other.

Server Consolidation

- A foundational component of virtualization is the concept of server consolidation, which is an application of or form of computer virtualization.
- **It is not uncommon for many staple servers, such as DNS or DHCP servers to be underutilized.**
- This is even more emphasized if these services happen to be hosted on different servers.
- Whether 20% utilized or 90% utilized, a server that is powered on is still running up an electrical bill.
- Among other things, converting several physical servers into virtual machines running on an ESXi host reduces the amount of physical space they occupy, reduces the electrical costs associated with powering and cooling, and increases security

Business Continuity

- The availability of critical business applications is something that must be ensured.
- Virtualization strategies such as server consolidation present the potential problem of a single point of failure.
- **Putting all of one's virtual eggs into a virtual basket may seem risky.**
- **A server failure on the physical host would of course cause any virtual machines running on the host to fail as well.**
- Virtualization can significantly reduce disaster recovery processes.

Business Continuity

- **A virtual machine running on one physical host can quickly and seamlessly be moved to another.**
- **The consolidated servers become portable, allowing an administrator to quickly relocate them.**
- When physical hosts are clustered, solutions such as High Availability can reduce downtime, and features such as Fault Tolerance can eliminate it.
- Consider that in a traditional environment, disaster recovery is typically a relatively daunting task, involving several manual steps

Cloud Computing

- Utility computing provides the resources in which one is interested (computation power, storage, application services) on an as needed basis.
- It allows for a shift in thinking of computing as a consumable service as opposed to a product which needs to be purchased, implemented, and maintained.
- Virtualization allows for a very scalable delivery model, which allows administrators to adjust for changing needs of resources.

Virtualization Vendors

Vendor	Product
Microsoft	Hyper-v
Citrix	Xen
Oracle	Oracle VM
VMware	vSphere /ESX

Management of Applications

- From a management and security perspective, **virtualization** provides a method for **standardising and automating the way in which IT processes are implemented and serviced.**
- They provide a management framework for securing virtualized resources from the host level all the way to the desktop.
- Workflow automation engines can dynamically create and remove resources as required.

Datacenter Components

- The virtual datacenter is a virtualization of the physical datacenter, including host servers, virtual machines, storage, and networks.
- Hosts represent the physical host, which aggregates the physical resources of the server, making them available to virtual machines.
- Just as the physical resources of a single host are aggregated and presented to VMs, multiple hosts can be clustered, which aggregates the resources of multiple hosts.
- Further aggregation and distribution of resources can be fine-tuned through the use of resource pools.

Virtual Networks

- Virtual networking provides a means for creating virtual networks,
- VMs use these to communicate with each other or with the physical network.
- This is accomplished by binding the virtual networks addressing information to the physical NIC located on the host (called an uplink).

High Availability

- (HA) provides a means to restart a VM on a different host in case of a server failure.
- There is downtime associated with the restart of the VM on a new functioning server.
- Fault tolerance expands on the idea of HA, but without the associated downtime.
  - Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components.
- A shadow VM is required which continually updates and can immediately step in should the primary VM fail.

Why is Virtualization so popular with modern organisations?

- Server Consolidation
  - Ability to "do more with less" saves money (equipment, space, power)
- Extremely versatile technology–Convert underutilized servers to VMs
- Simplified Management
- Datacenter provisioning and monitoring, Dynamic load balancing
- Improved Availability–Automatic restart
- Fault tolerance
- Disaster recovery
- Test and Development -snapshots

Summary

- The goal of virtualization is usually one of the following:
  - higher levels of performance,
  - scalability,
  - reliability/availability,
  - agility
  - or to create a unified security and management domain.