Implementing Client Virtualization and Cloud Computing

Implementing Client Virtualization and Cloud Computing

- Configure Client-Side Virtualization
- Cloud Computing Concepts

Virtualization

Virtualization: Software allowing a host computer to run multiple guest operating systems known as virtual machines.

- Virtual platform requires:
  - Computer(s)
  - Hypervisor or Virtual Machine Monitor (VMM)
  - Guest operating system or Virtual Machines (VMs)

Hypervisors (Slide 1 of 4)

- Each VM runs in protected space
- View from inside the VM is a CPU and memory
- Hard disk is an image file
- Components such as network adapter are emulated
- Main functions of hypervisors
  - Emulation
  - Guest OS support
  - Assigning resources to each guest OS
  - Configuring networking
  - Configuring security

Hypervisors (Slide 2 of 4)

Hypervisors (Slide 3 of 4)

Type 2 hypervisor: A host-based hypervisor in which you install the host operating system first, then install the hypervisor.

- Examples:
  - VMware Workstation
  - Oracle Virtual Box
  - Parallels Workstation
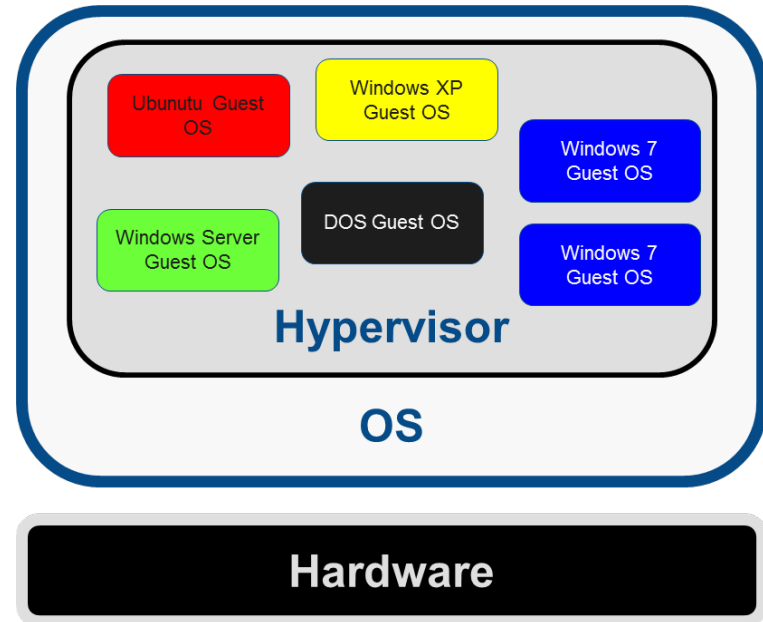
Hypervisors (Slide 4 of 4)

Type 1 hypervisor: A bare metal hypervisor in which you install directly on the server's hardware.

- Examples:
  - VMware ESX Server
  - Microsoft Hyper-V
  - Citrix XEN Server
  - Linux KVM
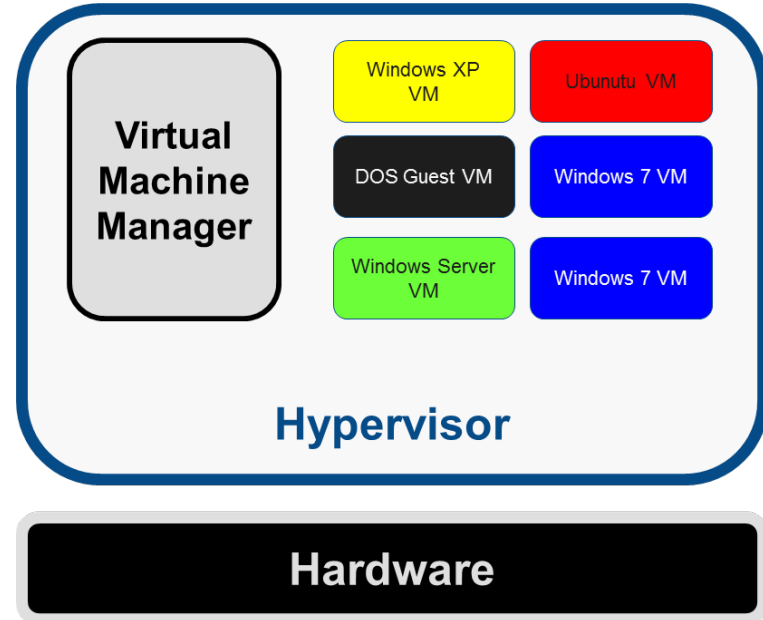
Processor Support and Resource Requirements (Slide 1 of 2)

- CPU with built-in instruction sets to facilitate virtualization
  - Intel: VT-x
  - AMD: AMD-v
- SLAT (second level address translation) to improve virtual memory performance by treating guest addresses like host addresses.
  - Intel: EPT
  - AMD: RVI
- Multiple CPU resources
  - SMP
  - Multiple physical processors
  - Multi-core
  - HyperThreading

Processor Support and Resource Requirements (Slide 2 of 2)

- Each guest OS requires memory above that required by the host.

- Each guest OS requires hard disk space for the VM image.

- Most hypervisors allow guest VMs to use host adapters and peripherals.

Virtual Networks (Slide 1 of 3)

- Multiple VMs can communicate with each other using standard networking protocols.

- Guest OS emulates standard network adapter hardware.
  - Can often have multiple adapters.
  - Configurable just like a physical adapter.

- Hypervisor implements network connectivity via virtual switches.
  - Function like Ethernet switches.
  - Implemented in software.
  - Connectivity between virtual adapters and virtual switches configured in hypervisor.

Virtual Networks (Slide 2 of 3)
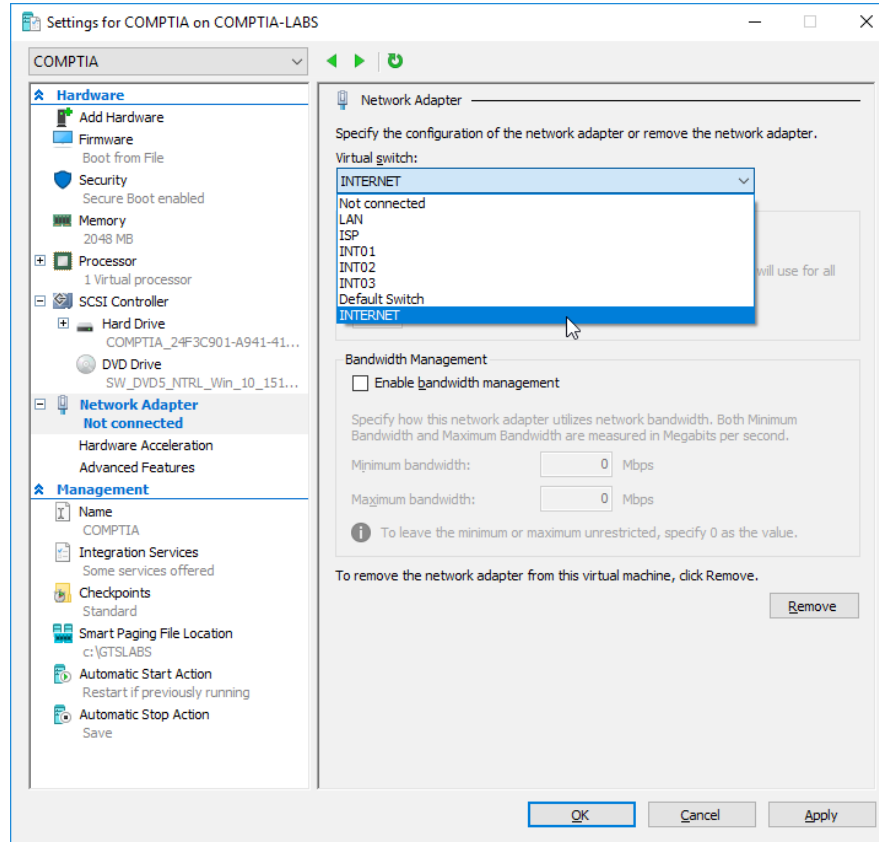
Virtual Networks (Slide 3 of 3)

- Can configure connectivity between host physical NIC and virtual switches.
  - Provides a bridge between host platform and physical network switches.
  - Allows frames to pass between:
    - Physical and virtual machines.
    - Virtual machines and the host.
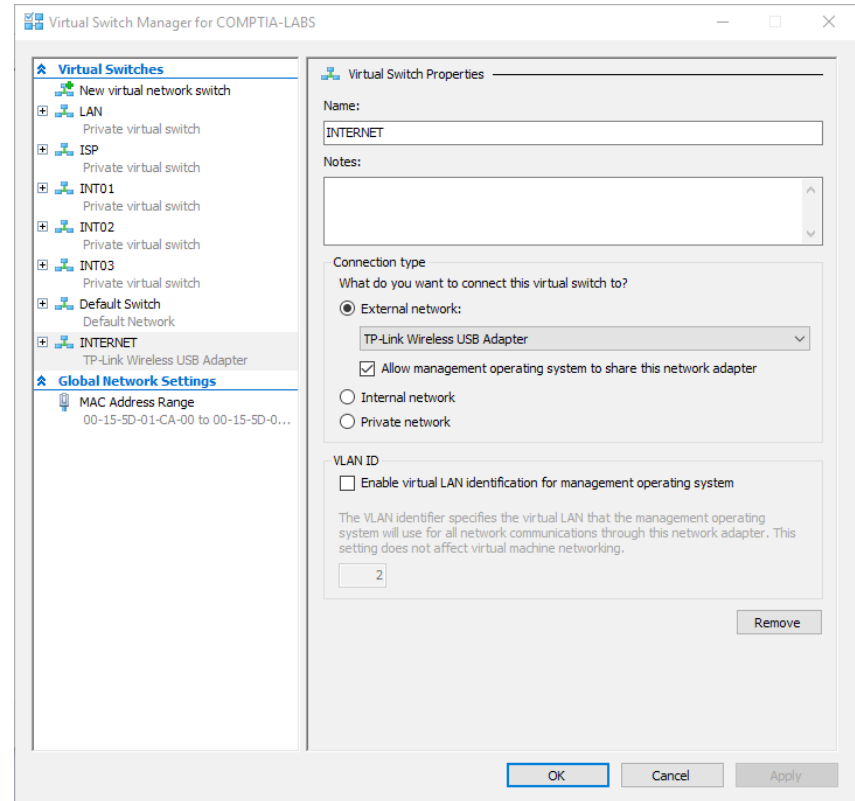
Virtual Machines (Slide 1 of 3)

- Client and Server OSs can be virtualized
- Some hypervisors have limited support for certain OSs
- Many purposes for deploying a virtual platform
- Client-side virtualization
  - Deployed to desktop-type machines
- Server-side virtualization

Virtual Machines (Slide 2 of 3)

Client-side virtualization: Any solution designed to run on desktops or workstations in which the user interacts with the virtualization host directly.

- Virtual labs
- Support legacy software applications
- Development environment
- Training

Virtual Machines (Slide 3 of 3)

Server-side virtualization: A solution in which one or more virtual servers are created on a physical server in which each virtual server acts like it was a separate computer.

Server consolidation: Using virtual servers, make more efficient use of system resources and hardware since most servers' capacity is not fully utilized.

- Better hardware utilization:
  - Typical server hardware resource utilization of 10%.
  - Implies 8-9 additional server instances could obtain the same performance.

Security Requirements (Slide 1 of 3)

Rogue VM: A virtual machine that has been installed without authorization.

VM sprawl: The uncontrolled development of more and more virtual machines.

Guest OS Security

- Each guest OS must be patched and protected against malware.
- Running security software on each guest OS can cause performance issues.
- Rogue VMs and VM sprawl are major security concerns.
  - System management software can detect rogue VMs.
  - VMs should conform to an application template.
  - Rogue developers often install backdoors and logic bombs.

Security Requirements (Slide 2 of 3)

MTBF: The rating on a device or component that predicts the expected time between failures.

Denial of Service (DoS): A network attack that aims to disrupt a service, usually by overloading it.

Host Security

- If host is compromised, so are guest Oss.
- Host hardware failures are a single point of failure.
- High resource utilization can decrease MTBF of components.
- DOS attack on host or hypervisor causes more damage than to a single server.
  - Most hypervisors support disk snapshots to revert to saved image.
  - Snapshots can be misused to perform DoS attacks.

Security Requirements (Slide 3 of 3)

VM escaping: Malware running on a guest OS jumping to another guest or to the host.

Hypervisor Security

- Hypervisor provides another attack surface
- Few attacks have been detected so far
- Keep hypervisor up-to-date with patches to help prevent VM escapes

Activity

Discussing Client-Side Virtualization

30bird 4.1.4, Installing a VM using VirtualBox:
https://www.youtube.com/watch?v=S26CKNo4Tgs

CompTIA.

Cloud Computing (Slide 1 of 2)

Cloud: Any sort of IT infrastructure provided to the end user where the end user is not aware of or responsible for any details of the procurement, implementation, or management of the infrastructure.

- NIST definition for cloud computing:

    Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

    (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, section 2.)

Cloud Computing (Slide 2 of 2)

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Benefits of Cloud Computing

Rapid elasticity: The ability to scale cloud computing resources quickly to meet peak demand and just as quickly remove resources if they are not currently needed.

Measured service: A provider's ability to control and bill a customer's use of resources such as CPU, memory, disk, and network bandwidth through metering.

- Rapid elasticity
- On-demand and pay-per-use
- Measured service
- Resource pooling
- Flexibility

Common Cloud Models

- Public or multi-tenant
- Hosted private
- Private
- Community
- Hybrid

CompTIA

Internal and External Shared Resources

- All networks share pool of resources
- File servers provide disk storage resources to clients
  - Shared folders
- Servers use shared disk storage
  - SANs
- Mix of virtualization and hybrid cloud solutions
  - Allows shared resources to be provisioned using:
    - Internally owned assets
    - Externally provisioned assets

CompTIA.

Cloud Service Options (Slide 1 of 2)

IaaS: A cloud computing service that enables a consumer to outsource computing equipment purchases and running their own data center.

SaaS: A cloud computing service that enables a service provider to make applications available over the Internet.

PaaS: A cloud computing service that enables consumers to rent fully configured systems that are set up for specific purposes.

Cloud Service Options (Slide 2 of 2)

Operating Systems and Software

Operating Systems

Amazon Machine Images (AMIs) are preconfigured with an ever-growing list of operating systems. We work with our partners and community to provide you with the most choice possible. You are also empowered to use our bundling tools to upload your own operating systems. The operating systems currently available to use with your Amazon EC2 instances include:

Operating Systems		
Red Hat Enterprise Linux	Windows Server	Oracle Enterprise Linux
OpenSolaris	Amazon Linux AMI	Ubuntu Linux
Fedora	Gentoo Linux	Debian
	SUSE Linux Enterprise	

Software

Amazon EC2 enables our partners and customers to build and customize Amazon Machine Images (AMIs) with software based on your needs. We have hundreds of free and paid AMIs available for you to use. A small sampling of the software available for use today within Amazon EC2 includes:

Databases	Batch Processing	Web Hosting
IBM DB2	Hadoop	Apache HTTP
IBM Informix Dynamic Server	Condor	IIS/Asp.Net
Microsoft SQL Server Standard	Open MPI	IBM Lotus Web Content Management
MySQL Enterprise		IBM WebSphere Portal Server
Oracle Database 11g		

Application Development Environments	Application Servers	Video Encoding & Streaming
IBM sMash	IBM WebSphere Application Server	Wowza Media Server Pro
JBoss Enterprise Application Platform	Java Application Server	Windows Media Server
Ruby on Rails	Oracle WebLogic Server	

Virtual Desktops (Slide 1 of 2)

VDI: Using a VM as a means of provisioning corporate desktops.
VDE: The virtual desktop environment or workspace.

- Desktop computers are replaced by low-spec, low-power thin client computers.
- The thin client boots a minimal OS, allowing the user to log on to a VM stored on the company server infrastructure.
- All application processing and data storage in the VDE or workspace is performed by the server.
- All data is stored on the server so it is easier to back up, and the desktop VMs are easier to support and troubleshoot.

Virtual Desktops (Slide 2 of 2)

- VDIs are better locked against unsecure user practices.
- The main disadvantage is that in the event of a failure in the server or network infrastructure, users have no local processing ability.
- Virtual NIC

Cloud-Based Applications

Application virtualization: Rather than run the whole client desktop as a virtual platform, the client either accesses a particular application hosted on a server or streams the application from the server to the client for local processing.

Virtual application streaming: Just enough of an application is installed on the end user device for the system to recognize that the application is available to the user, and when the user accesses the application, additional portions of the code are downloaded to the device.
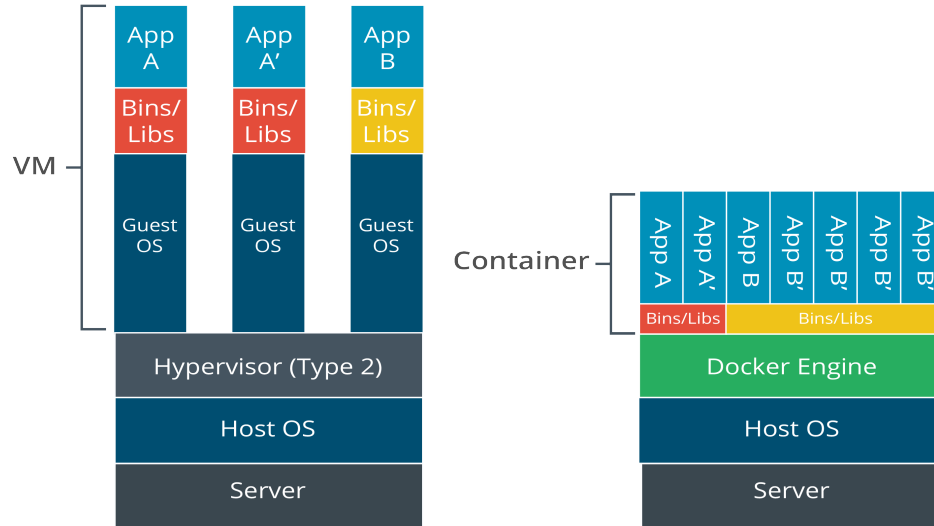
- Off-site email applications
- Cloud file storage
- Virtual application streaming
- Client platforms

Container Virtualization

Container virtualization: Enforces resource separation at the operating system level with each user having a separate instance to run in.

Container vs. VMs

Cloud-Based Network Controllers

- When using mix of local and cloud-based resources:
  - Can be difficult to see the entire network from a single management and monitoring interface.
- Cloud-based network controller:
  - Allows you to register and monitor all of the organization's networks.
  - Depends on Software Defined Networking (SDN).
- SDN can be used to configure network access devices through software programs and scripts.

Activity

Discussing Cloud Computing Concepts

PBQ Lesson 7

Reflective Questions

1. What types of client-side virtualization technologies does your organization use?

2. What type of cloud computing does your organization use? What other services might you recommend be implemented?