7.13.3 Virtualization Facts

Virtualization is the ability to install and run multiple operating systems concurrently on a single physical machine. Virtualization typically includes the following components:

Component	Description
Physical Machine	A *physical machine* (also known as the host operating system) has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, and motherboard.
Virtual Machine	A *virtual machine* (also known as the guest operating system) is a software implementation of a computer that executes programs like a physical machine. The virtual machine appears to be a self-contained and autonomous system.
Virtual Hard Disk (VHD)	A *virtual hard disk* (VHD) is a file that is created within the host operating system and simulates a hard disk for the virtual machine.

Hypervisor	A *hypervisor* is a thin layer of software that resides between the guest operating system and the hardware. A hypervisor allows virtual machines to interact with the hardware without going through the host operating system. There are two types of hypervisors.
	▪ A Type I hypervisor is often called a native hypervisor or bare-metal hypervisor. A hypervisor in a dedicated appliance is called an embedded hypervisor. A Type I hypervisor is like a thin operating system that directly interfaces with the computer hardware. Examples of Type I hypervisors are:
	  ▪ VMware ESX and ESXi
	  ▪ Microsoft Windows Server Hyper-V
	  ▪ Citrix XenServer
	▪ A Type 2 hypervisor is known as a hosted hypervisor. It runs as an application on a conventional operating system. While there may be used in a production environment, they are most often used by as a development sandbox. Examples of Type II hypervisors are:
	  ▪ VMware Workstation and VMware Player
	  ▪ Oracle Virtual Box
	  ▪ Parallels Desktop for Mac

The following table explains advantages of virtualization:

Advantage	Description
Flexibility	Virtual machines can be given network access, and other network devices will consider them to be real physical machines. ▪ Virtual machines should have the latest service packs and patches, just like physical machines. ▪ Virtual machines should be hardened, just like physical machines. ▪ Virtual machines can be connected to the production network by creating a bridged (external) virtual switch. Because they are self-contained, virtual machines can be easily moved between hypervisor hosts as needed.
Security	To better protect other systems, virtual machines can be used to create honeypots and honeynets to attract attackers and analyze how they are attacking the system.
Testing	Virtual machines can be configured in a lab environment that mirrors your production network for testing purposes. This lab environment can be used to: ▪ Test applications before installing them on production systems. ▪ Test updates and patches before rolling them out into the production environment. ▪ Test security controls to verify that they are working as designed.
Server Consolidation	Server consolidation allows you to move multiple physical servers onto just a few physical servers with many virtual machines. *Physical-to-virtual migration* (P2V) is the process of moving an older operating system off aging hardware and into a virtual machine. Consolidating servers: ▪ Requires fewer physical computers ▪ Reduces power consumption ▪ Increases physical server utilization of resources ▪ Increases administrative efficiency ▪ Aids with incompatibility issues
Isolation	A virtual machine can be isolated from the physical network to allow testing to be performed without impacting the production environment. This is called sandboxing.

	▪ Sandboxed virtual machines offer an environment where malware can be executed with minimal risk to equipment and software. ▪ Virtual machines that are isolated in this fashion are isolated from many kinds of security threats. ▪ To allow the virtual machines to communicate with each other while isolating them from the production network, create a new virtual switch configured for host-only (internal) networking and connect the virtual network interfaces in the virtual machines to the virtual switch.
Application Virtualization	Applications can be virtualized. ▪ A virtual application appears to be local, but is really running on a different system. ▪ Virtualized browsers can protect the underlying physical operating system from malware installation. Any malware installed from the virtual browser affects only the browser, not the rest of the system. Malware can also use virtualization techniques that make it difficult to detect.

Disadvantages of virtualization include:

- An attack on the host machine could compromise all guest machines operating on that host.
- A bottleneck or failure of any hardware component that is shared between multiple guests, such as a failure in a disk subsystem, could affect multiple virtual machines.
- While administration is centralized, virtualization is a newer technology and requires new skills, and managing virtual servers could add complexity.
- Your configuration is susceptible to server sprawl, which is when many virtual machines are created and patch and security update management falls behind.

Security considerations for a virtual machine should be the same as for physical machines. For both the host and all guest machines, be sure to:

- Reduce the number of services running
- Apply patches and updates regularly
- Install antivirus and other security software
- Implement backups, operating system snapshots, or other solutions for data protection

In addition, you should protect against virtual machine escape, which is an exploit where the attacker runs malware that allows the operating system within a virtual machine to break out and interact directly with the hypervisor. There are actions you can take to minimize this vulnerability.

- Apply patches and updates regularly.
- Install only the resources-sharing features that are necessary.
- Install only the software applications that are necessary.

Load Balancing is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time. The primary goal of load balancing is to improve performance and create high availability by configuring multiple devices to respond as one. Load balancing can also provide fault tolerance. If the load balancing mechanism is able to detect when a specific farm member is unavailable, new requests will automatically be distributed to the available members. Load balancing methods with virtualization include the following:

- Resource pooling creates shared logical pools of CPU and memory resources from many physical machines within the hypervisor to guarantee a level of resources for specific virtual machines.
- Workload balancing distributes a workload (the total requests made by users and applications of a system) across multiple computers or a computer cluster to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload.
