6.1.3 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*, or *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*, or *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(s) and the hardware. A hypervisor allows virtual machines to interact with the hardware without going through the host operating system.

Advantages of virtualization are:

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.
Testing Functions	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 moving an older operating system off of aging hardware and into a virtual machine. Consolidating servers: ▪ Require fewer physical computers ▪ Reduce power consumption ▪ Increase physical server resource utilization ▪ Increase administrative efficiency ▪ Aid resolving 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, perform the following:
	  ▪ Create a new virtual switch configured for host-only (internal) networking.
	  ▪ Connect the virtual network interfaces in the virtual machines to the virtual switch.

Disadvantages of virtualization include the following:

- 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.

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 or other data protection solutions.
