Chapter Objectives

- Explore virtualization concepts
- Become familiar with cloud concepts

**Cloud and Virtualization**

Virtualization and cloud services are becoming common enterprise tools to manage
- costs
- capacity
- resources
- complexity
- risk

**Hypervisor**

- Virtualization technology enables a computer to have more than one OS and operating at the same time
- It is an abstraction of the OS layer
- To enable virtualization, a hypervisor is employed
- A hypervisors are low-level programs that allow multiple operating systems to run on a single host computer
- They use a thin layer of code to allocate resources in real time - they control I/Os and memory management: separation of software and hardware
- Host machine and host OS - guest machine and guest OS
- Type I and Type II hypervisors
**Type I**

- Type I hypervisors run directly on the system hardware
- Native, bare-metal, or embedded hypervisors
- They are designed for speed and efficiency – no additional OS layer
- KVM (Kernel-based Virtual Machine, a Linux implementation),
  - Xen (Citrix Linux implementation),
  - Microsoft Windows Server Hyper-V (Windows OS core)
- VMware’s vSphere/ESXi platforms
- They come with management tools

**Type II**

- Type II hypervisors run on top of a host operating system
- Oracle’s VirtualBox and VMware’s VMware Player
- These are designed for limited numbers of VMs, typically running in a desktop or small server environment

**Application Cells/Containers**

- A hypervisor enables multiple OS instances to coexist
- The concept of application cells/containers is similar
- Container holds the portions of an OS that it needs
- But have separate memory, CPU, and storage threads so they will not interact with each other
- Multiple instances of an application or different applications share a host OS with virtually no overhead
- It is the evolution of the VM concept to the application space
- This eliminates the differences between a development, test, or production environment

**VM Sprawl Avoidance**

- You can lose track of a VM
- VMs basically are files that contain a copy of a working machine’s disk and memory structures
- Creating a new VM is a simple process
- As the number of VMs grows over time, sprawl can set in
- Can be avoided through naming conventions and proper storage architectures
- VMware can manage, locate and use resources when required
VM Escape Protection

- One concern is VM escape, where escapes from one VM to the underlying OS
- VMs use the same RAM, the same processors, and so forth
- Large-scale VM environments have specific modules designed to detect escape and provide VM escape protection to other modules

Cloud Storage

- Cloud storage: computer storage provided over a network
- One of the characteristics is transparency to the end user
- This improves usability, performance, scalability, flexibility, security, and reliability
- Security is a particular challenge: how to allow data to be stored outside your enterprise and yet remain in control
- The common answer is encryption
- Apple iCloud, Microsoft OneDrive, and Dropbox

Cloud Deployment Models

- Cloud deployment models: internal and external
- Big scale from Google and Amazon
- The promise of cloud computing is improved utility
- Platform as a Service, Software as a Service, and Infrastructure as a Service

SaaS

- Software as a Service (SaaS) is the offering of software to end users from within the cloud
- SaaS acts as software on demand, and runs from the cloud
- Advantages: updates can be seamless to end users, and integration between components can be enhanced
- Microsoft Office 365 and Adobe Creative Suite
**PaaS**

- **Platform as a Service (PaaS)**: computing platform in the cloud
- Multiple sets of software can be delivered
- PaaS offerings generally focus on security and scalability

**IaaS**

- **Infrastructure as a Service (IaaS)**: a virtual solution for computing
- Rather than building data centers, IaaS allows firms to contract for utility computing as needed
- IaaS is specifically on a pay-per-use basis, scalable directly with need
- You can even rent supercomputers

**Private**

- **Private clouds** are essentially reserved resources used only for the organization—your own little cloud within the cloud.
- This service will be more expensive, but it should also carry less exposure
- Better defined security, processing, handling of data

**Public**

- **Public cloud**: is rendered over a system that is open for public use
- There is little operational difference between public and private cloud architectures
- Security ramifications can be substantial
- Services separate users with security restrictions, the depth and level of these restrictions, will be significantly less in a public cloud
Community

- A community cloud system for several organizations with a common interest
- They share a cloud environment for the specific purpose
- Community initiatives
- Cost-sharing mechanism for specific data-sharing initiatives

Hybrid

- A hybrid cloud: elements are combined from private, public, and community cloud structures
- They can be used together:
  - sensitive information can be stored in the private cloud
  - issue-related information can be stored in the community cloud

On-Premise vs. Hosted vs. Cloud

- On-premises: the system resides locally
  - VM, storage, or even services
  - locally hosted and maintained
  - advantage: organization has total control, high connectivity
  - disadvantage: requires local resources, not as easy to scale
- Hosted services: the services hosted somewhere else
  - provides a set cost based on the amount you use
  - advantage: costs, especially when scale is included

VDI/VDE

- Virtual desktop infrastructure (VDI) and virtual desktop environment (VDE): hosting of a desktop environment on a central server.
- VDI: all the components needed to set up the environment
- VDE: what the user sees, the actual user environment
- User "machine" and all of its data are persisted in the server environment
- Users can use a wide range of machines, even mobile phones, to access their desktop and perform their work
- Tremendous security advantages because all data resides on servers inside the enterprise, in the data center
Cloud Access Security Broker

- Cloud access security brokers (CASBs): security policy enforcement between cloud service providers and their customers to maintain and enforce security policies
- CASBs belong to the broader category of managed security service providers (MSSPs)
- CASB vendors provide a range of security services designed to protect cloud infrastructure and data

Security as a Service

- Security as a Service: outsourcing security functions
- Advantages: scale, costs, and speed
- Security is a complex, wide-ranging cornucopia of technical specialties, all working together to provide appropriate risk reductions
- Technically savvy security pros, experienced management, specialized hardware and software, fairly complex operations – any or all of this can be outsourced
- Specializations in network security, web application security, e-mail security, incident response services, infrastructure updates

Stay Alert!

There is no 100 percent secure system, and there is nothing that is foolproof!