Chapter 6

Migrating to the Cloud

Episode 6.01

Migration Types

Physical to Virtual (P2V)

- Most common type
- Converting physical servers to virtual servers
  - For the cloud or for conversion to virtualization
- Involves several actions
  - Migrating OS
  - Migrating applications
  - Migrating data

Physical to Virtual (P2V)

- Process may be manual or automated
  - Manual
    - Generalize OS
    - Shut down, reboot off media, make image
    - Load image and drivers into VM
  - Semi-automated
    - Run script to generalize OS
    - Load image and drivers
  - Fully automated
    - Script or app does everything

Virtual to Virtual (V2V)

- Converting virtual server from one virtualization platform to another
- Or moving it from one location to another
- Platform-to-alternate-platform requires the same process as P2V
- Platform-to-same-platform requires only a move of the VM

Virtual to Physical (V2P)

- Converting a virtual machine to a physical machine
- May be used to move from the cloud to on-premises
- May be used in some cloud providers to dedicate a physical machine to your process
- Machine should be generalized before the move

Physical to Physical (P2P)

- Migrating the software from one physical server to another
- Often performed with imaging/cloning software
- Requires generalization before the move when moving to different hardware
- May require generalization to move between like models

Storage Migrations

- Simpler than machine migrations
- Pointers to the data must be redefined
- User data is often mapped to drive letters
- Scripts may be used to remap drives

Online vs. Offline Migrations

- Online migrations allow users to continue accessing the system
  - Most easily allowed when the data is stored external to the system
  - System can be migrated
  - Data migrated later

Online vs. Offline Migrations

- Offline migrations disable access to the system
  - May be required for data consistency
  - Most useful when data is integral to the system

Quick Review

- P2V and V2V both result in virtual instances in the cloud
- V2P and P2P both result in physical instances
- When migrating storage it is important to plan for the reconfiguration of all pointers to the data throughout your applications and operating systems

Episode 6.02

Workload Management

Workload Migrations

- Standard operating procedures (SOPs) should be defined
  - How do you migrate P2V, V2V, V2P, and P2P?
  - How is data migrated?
  - What operating systems are supported?
  - What database systems are supported?
- As you implement cloud-based virtualization, procedures should be updated based on experience

Workload Format

- Virtualization format
  - Cloud providers may have their own formats and systems
  - Private clouds are usually VMware, Hyper-V, or open source virtualization formats
  - The format of the virtual hard disks and configuration files must be considered

Workload Format

- Application and data portability
  - Can the application(s) be moved without breaking configurations?
    - Will a reinstallation be required?
  - Is the data accessed explicitly or through pointers?

Quick Review

- Standard operating procedures (SOP) should be defined that optimize the migration of workloads
- As you work with a cloud solution, SOPs will be updated based on experience
- Some applications will require reinstallation if configuration parameters cannot be modified post-installation

Episode 6.03

Visualizing Physical Systems

Shared vs. Dedicated

- Will the physical systems be virtualized on shared systems or dedicated systems?
  - Processor demands
  - Memory demands
  - Physical hardware access requirements

OS Selection

- OS installation options may change when virtualizing
  - Windows Core instead of GUI
  - Linux without GUI
- Services may be moved to a better OS for virtualization
  - DNS
  - DHCP
  - NTP

Management Methods

- Remote shell (SSH)
  - Command-line interface
  - Required in-depth command line/shell skills
- Remote desktop (RDP/VNC)
  - GUI interface
  - Uses same skills as local administration

Quick Review

- In a cloud environment, dedicated systems are used only by one customer or may be used as one server
- Some operating systems offer a minimized installation that is frequently used in virtualized servers
- Management methods should be selected based on the functionality required and the security they offer

Episode 6.04

Migrating Security

Cloud Security

- Security of cloud management
  - Who can access the cloud administration tools?
  - How can they access the tools?
  - When can they access the tools?

Cloud Security

- Security of deployed systems
  - Who can access the databases?
  - Who can access the servers?
  - Who can access the managed services?

Security Considerations

- Identity
  - How will identities be managed?
- Authentication
  - What authentication methods will be supported?
- Authorization
  - How will access be granted/denied?
  - Who will approve access and how?
  - Do you have defined access policies?

Federation

- Separation of authentication/ authorization from the service being accessed
- Accomplished through trust
    - One domain trusts another domain to authenticate/ authorize users
    - Users are required only to authenticate to a single domain

Quick Review

- Security of the cloud is managed by the provider and security in the cloud is managed by the subscriber
- Planning for user management within cloud providers is important as they all differ in the specifics of implementation
- Federated security may be used so that an external authenticator can validate identity

Episode 6.05

Protocols and Services

Data Transfer Methodologies

- Data can be transferred using common file transfer protocols
  - HTTP/HTTPS
  - FTP/SFTP/FTPS
- Network connections required
  - Internet connectivity
  - VPN protocols
- Direct connection
- Out-of-channel
  - Ex: AWS Snowball

Migrating Protocols to the Cloud

- DNS
  - Cloud providers usually offer this as a service
- DHCP
  - Cloud is DHCP server
  - Set up VM as DHCP server

Migrating Protocols to the Cloud

- Certificate services
  - Deploying PKI can be expensive
  - Cloud deployment just needs 3 VM instances
- All protocols should be selected based on requirements
  - Never run a protocol you don't need

Other Services and the Cloud

- Local agents
- Load balancing
- Antivirus/anti-malware
- Firewalls
- IDS/IPS
- Multifactor authentication

Quick Review

- Out-of-channel data transfers usually involve copying data to an external storage system and shipping that system to the cloud provider
- Organizations may choose to run DNS for both cloud and local systems in the cloud
- Cloud providers typically offer robust load balancing solutions that are simpler to implement than traditional on network load balancing systems

Episode 6.06

Environmental Constrains

Bandwidth

- Calculate
  - Bandwidth required per application per user (App_req)
  - Number of users per application (Num_users)
  - App_req X Num_users = Bandwidth Per Application
  - Sum all of the applications for total bandwidth

Time Constraints

- Downtime impact
- Working hours restrictions
- Follow-the-sun constraints/time zones
- Peak timeframes

Legal Constraints

- Cloud service providers must be able to comply with regulations
  - Most major providers can
- Ensure implementations are in compliance

Quick Review

- Internet connection speeds can significantly reduce the ability to work with the cloud
- The times within which systems must be available can impact how the solutions are implemented in the cloud
- Legal constraints often related to security and data retention

Episode 6.07

Virtual Desktop Interface (VDI)

VDI Defined

- A technology that allows for the virtualization of entire desktop computing environments
- Desktops are hosted on centralized servers or in the cloud
- Services are provided by AWS, Azure, GCP and others

VDI Benefits

- Reduced cost
  - Hardware costs
  - Maintenance costs
- Enhanced scalability
- Enhanced security
- Flexibility and mobility
- Simplified management

VDI Components

- Virtualization layer
- Cloud infrastructure
- Connection broker
- Desktop images
- User data and profiles

VDI Implementation

- Assess requirements and objectives
- Choose a cloud provider and VDI platform
- Design the architecture
- Configure the cloud insfrastructure
- Install and configure VDI software components
- Create and optimize desktop images
- Test, deploy, monitor and manage

Episode 6.08

High Availability in the Cloud

High Availability & Migration

- Redundancy and distribution
- Load balancing and traffic management
- Auto-scaling and elasticity
- Fault tolerance and self-healing
- Backup and disaster recover
- Monitoring and alerting
- Application architectures
- Data replication and consistency
- Security and compliance

Chaos Engineering

- Chaos engineering and resilience testing
  - Identify weaknesses
  - Test fault tolerance and redundancy
  - Validate disaster recover and backup strategies
  - Improve observability and monitoring
- Chaos engineering steps
  - Define the systems steady state
  - Hypothesize potential failures
  - Design and run chaos experiments
  - Analyze the results
  - Share findings and iterate