**Microsoft Azure Fundamentals: Cloud Computing**

**Cloud Computing Characteristics:**

* Resource pooling
* Broad access
* Rapid elasticity
* On-demand self-service
* Metered usage

**Resource pooling:**

Cloud service provider (CSP) equipment available for cloud tenants (hypervisor hosts, storage arrays, network equipment).

Compute, network, and storage resources appear infinite to cloud customers.

**Broad Access:**

Cloud service accessibility over a private or public network

Support for any client device type

**Rapid Elasticity**

Add/remove storage

Add/remove virtual machines manually or through autoscaling

Resize virtual machines (vertical scaling)

**On-demand Self-service**

Cloud user deploys and manages resources

CSP technicians not involved with normal cloud service deployment and management

Provides more cloud resource coryfor cloud tenants

**Metered Usage**

Resource usage is tracked by the CSP

Monthly charges are based on cloud service usage and storage

**Virtualization and the Cloud**

. Operating system virtualization requires a hypervisor

. Type 1 hypervisor - dedicated to virtualization

. Type 2 hypervisor - runs as an app within a multipurpose OS

· Application virtualization (app streaming)

· Application containers

· Virtual desktop infrastructure (VDI); Azure Virtual Desktop

· Software-defined networking (SDN)

**Type 1 Hypervisor**

. Is the operating system

. Runs directly on "bare metal" hardware

. Streamlined to support virtualization hosting

. VMware ESXi, Microsoft Hyper-V

**Dedicated Virtual Machine Hosting**

. Physical host in a data center

. Used by a single cloud tenant

. More expensive than shared hosting for virtual machines

· Legal/regulatory compliance

**VM Sprawl**

Pro: Quick and easy provisioning of virtual machines

Cons: Easy to forget about unused virtual machines, increased attack surface

**Cloud Deployment Models**

**Public Clouds**

* Available to anybody over the Internet
* An account must be created, trial subscription allows resource deployment and management
* Cloud provider owns the IT infrastructure

. Physical data center security

. Network link speed

. CSP security accreditations

* Shared responsibility (depends on cloud service)
* Data sovereignty
* Larger target for malicious users
* Cloud service offerings may vary between geographical regions

**Private Clouds**

* Owned and used by a single organization
* Full configuration control, full responsibility
* Uses virtualization
* Metered usage for departmental or project chargeback

**Hybrid Cloud**

* Combines private and public clouds
* Full configuration control (private)
* Uses virtualization
* Confidential processes and data might have to remain under singular organization control

**Community Clouds**

* Adheres to all cloud computing characteristics
* Specialized cloud with services tailored for specific needs
* E.g., Azure US Government cloud, Azure Germany

**Infrastruture as a Service (IaaS)**

**Azure Data Centers**

* Locations not disclosed publicly for security reasons
* One or more per availability zone (AZ)
* Redundancy (power, network, equipment)
* Physical facility security

**Infrastructure as a Service (laaS)**

· Service-level agreement (SLA) for each laaS service

· Underlying infrastructure that supports IT services, such as:

· Storage

· Network addressing and routing

· Network security

· Compute services (VMs, containers)

Shared responsibility

CSP: Hypervisor, network equipment, physical storage arrays

Tenant: VM deployment and management, virtual networks (VNets), storage provisioning

**Azure IaaS Examples**

* Storage account
* Virtual machine
* Virtual network
* Azure Firewall

**IaaS Benefits**

* Less provisioning time than on-premises
* Accessible from anywhere
* Shared responsibility

**Azure laaS**

· Graphical user interface (GUI) management (Azure portal)

· Azure command-line interface (CLI)

· Azure PowerShell

. Programmatic application programming interface (API) calls

. Templates

**Platform as a Service (PaaS)**

* Underlying infrastructure required to support IT services is automatically provisioned
* Provisioning done by the CSP
* Managed service/"serverless"
* Configured by IT sys admins, software
* SLA

**PaaS Responsibility**

Tenant: Configuration of the solution, data

CSP: Underlying infrastructure, virtual machines, software, patching

**Azure Active Directory (Azure AD) - Microsoft Entra ID**

· Centralized cloud authentication

. Users, groups, devices, applications

. No network configuration to deploy or manage

. No servers to deploy or manage

· No organizational units (OUs)

. No Group Policy

. For full AD control, deploy AD in an laaS VM

**Azure SQL Database**

· No network configuration to deploy or manage

. No servers to deploy or manage

. No database software to install

. Full SQL database control - deploy manually as laaS

**Azure Virtual Desktop (AVD)**

* No network configuration to deploy or manage
* No client-based virtual machines to deploy or manage
* Select a bundle (hardware and software configuration)
* Customized bundles

**Azure PaaS**

· GUI management (Azure portal)

· Azure CLI

. Azure PowerShell

· Programmatic API calls

· Templates

**Software as a Service (SaaS)**

. Managed cloud service

. End-user applications

. Software is managed by the CSP

. Service-level agreement for each SaaS

· Limited configuration options

. Isolated from other cloud tenants

**Azure SaaS**

. Shared responsibility

. CSP: Supporting infrastructure, software maintenance/patching, tenant isolation

. Tenant: Available configuration options, usage data privacy

* Cloud tenant user and group provisioning
* Multi-factor authentication (MFA)
* User and group permissions
* Single sign-on (SSO)

**SaaS Benefits**

Accessible from anywhere using any platform

Normally no software deployment (apps on devices vs. browser-based)

User familiarity with cloud-based applications

Pay only for what you use

App accessibility using a web browser

**Azure SaaS Examples**

. Microsoft 365

. Customized line-of-business apps

. Web application

**Azure Data Centers**

* Public cloud – CSP data centers
* Private cloud - owned and used by a single organization
* Configuration flexibility
* Data privacy
* Regulatory compliance

**On-premises IT Hardware Responsibilities**

· Acquisition, payment, and shipping times

· Configuration

· Ongoing management

· Firmware updates

· Decommissioning

**On-premises IT Software Responsibilities**

· Acquisition, licensing

· Configuration

· Ongoing management

· Software updates

· Decommissioning

**On-premises vs. Public Cloud**

* CapEX vs. OpEX
* Total cost of ownership (TCO)

**On-premises vs. Public Cloud**

* CSP security accreditations
* CSP economies of scale

**Natural and Person-made Disasters**

* The cloud can serve as an alternate site
* IT system duplication in the cloud for resiliency
* Data replication to the cloud for resiliency

**Azure Regions**

* Geographical locations where Microsoft has a cloud presence
* More than 60 worldwide; this changes over time
* Service availability can vary by region

1. Some configurations require resources to be in the same region
2. E.g., Key Vault and storage account using customer-managed keys

**Azure Availability Zones**

. Contained within an Azure region

. Each Azure region has at least one availability zone

· An availability zone is a separate location (a data center)

. High-speed networks link availability zones together

· Some Azure services can be replicated across availability zones

**Azure Sovereign Regions**

* A type of community cloud
* Isolated from the standard public Azure cloud
* Dedicated to specific entities: Azure German cloud, Azure Government, Azure China

**Azure Arc**

Manage IT resources across platforms, clouds, anddata centers as if they were running in Azure usingfamiliar Azure management tools

* Centralized compliance (Azure Policy)
* Centralized server configuration management

**Azure Arc Centralized Management and Governance**

* On-premises IT services
* Multi-cloud IT services
* Edge IT services

**Azure Arc - Unified Management**

* Azure portal
* Azure CLI
* Azure PowerShell
* Azure REST API

**Azure Arc – External Services Management**

* Physical/virtual servers for Linux and Windows
* Kubernetes clusters
* Microsoft SQL Server

**Azure Arc-enabled Servers**

· Azure Connected Machine agent must be installed

. Server is assigned a resource ID, becomes a part of a resource group, and is assigned a managed identity

· Server is then treated as a standard Azure resource and can have tags applied and use Azure Policy

. Servers can be monitored using a Log Analytics workspace