AZ-900: Microsoft Azure Fundamentals

August 1, 2023 Umangkumar Patel

Exam

Cost	$99 USD
Official Link	https://learn.microsoft.com/en-us/certifications/exams/az-900/
Passing Score	700/1000
Free Practice Assessments	https://learn.microsoft.com/certifications/exams/az-900/practice/assessment?assessment-type=practice&assessmentId=23

Cloud Concepts

- **Cloud Computing -** renting resources such as servers, storage, memory on cloud provider's computers (AWS, Microsoft, Google)
  - Pay-as-you go pricing model
  - Transfer the cost model from CapEx(capital expenditure) to OpEx (operational expenditure)
  - CapEx - upfront investment for physical infrastructure
  - OpEx - paying for a service as you use it (ongoing/operational)
- public vs private vs hybrid cloud
- IaaS, PaaS, SaaS
- Shared Responsibility

Azure Architecture

- Regions - set of data-centers (one or more data-center) in a latency defined perimeter connected using dedicated low latency network (fiber)
    - Choose region closer to customers
    - Feature - certain features may not be available in every regions
- Availability Zones - unique physical location **within** a region
    - Each zone has has independent power, cooling and networking
    - Each region has **minimum** of **three** zones
- Resource groups - container that has related resources for Azure solution
    - Resource can only belong to one RG
- **Azure Resource Manager**
    - Deployment and management service for Azure (handles request)

Compute

Virtual Machines (VM)

- Infrastructure-as-a-Service(IaaS)
    - Manage everything except the hardware (including network components)
- Configure (RAM, CPU, Operating System etc.)
- Pricing
    - Hourly (pay per use)
- Choose only when
    - Need control of the environment
    - Need to install/run specific applications or databases
    - Migrating existing resources

Scale Sets

- Manage identical copies of an existing virtual machine
    - Used for spinning up VM quickly when in need
- Benefits
    - Easier to manage multiple VM's
    - High Availability - spin another instance if one fails
    - Auto Scaling - respond to the demand
- Limit of 1000 VMs per scale set

App Services

- Azure managed platform (Platform-as-a-Service) for deployment of:
    - Web apps
        - Choose Windows/Linux
        - Support of popular programming languages
    - Container applications
        - Self containing application with its dependencies

    - API Apps
        - Exposing / Connecting data back-end
        - Support of various programming languages

Azure Container Instances (ACI)

- Fixes the *"It works on my machine"* problem
- A container has all the necessary components required for a software such as
    - operating system, frameworks, dependencies, other software etc.
- Benefits
    - Easy to manage application dependencies
    - Less overhead
    - Portability
    - Efficient
    - Consistency
- Used for running container workloads
- On demand

Azure Kubernetes Services (AKS)

- Kubernetes is an open-source container orchestration system for automating application deployment, scaling, and management
- Features
    - Allows to replicate container architectures
    - Azure Managed Service (no need to worry about infrastructure and hardware)
    - Extend to on-premise

Azure Container Registry (ACR)

- Manages container images (artifacts)
    - Versioning
    - Feeding container images to ACI and AKS
    - Security controls

Azure Virtual Desktop

- Run Windows 10 instance on 100% virtually on Azure Cloud
- Benefits
    - Reuse windows licenses
    - Concurrency - Multiple users can use the instance at the same time

Azure Functions

- Function-as-a-Service(FaaS)
- Server-less compute service
- Smallest compute service available on Azure
- Runs on invocation (via other services or URL)
- Executes only once → stops (one unit of compute)
- Benefits

    - Only runs when in need
    - Saves money
    - Provides high availability, scalability, and resiliency

Networking

Virtual Network (VNet)

- Data-center on the cloud (similar to traditional network which you would operate on-prem)
- Address Space
    - Range of IP address that can be assigned to resources attached to the virtual network
    - Every service / resource will be assigned a unique IP
- Subnets
    - Allows for multiple networks
    - Group resources
    - Efficiently allocate address
    - Secure network by separating subnets
- VNet maps to a single regions
    - Resources contained within must be in the same region as VNet
- Many-to-1 relationship with subscription
- Scalability, Availability
- VNet Peering
    - Connect 2 or more virtual networks with azure- (on azure backbone network without crossing public internet)
    - Provides low-latency, high bandwidth connection
    - Communicate with resources in a separate network
    - Transfer data between subscriptions and deployment models

Load Balancer

- Evenly distribute inbound traffic to back-end services, based upon rules and health checks
- Access point of all traffic
- Ensures traffic is sent to a healthy back-end instance
- Uses IP address / port to route requests
- Log traffic

Virtual Private Network (VPN) Gateway

1. Virtual Private Network
    a. Can be used to create a secure hybrid cloud architecture
2. Main components
    a. Site-to-Site connection
        i. VPN Gateway on Azure Cloud
        ii. Tunnel (secure connection with encryption mechanisms in place)
        iii. On-prem network with complementary gateway to accept encrypted data
    b. Multi-site connection

        i. One VPN gateway with many sites

Application Gateway

- Route Layer 7 (HTTP/Path based) requests
- Benefits
    - Scalability
    - Encryption
    - Zone Redundancy
    - Multi-site hosting

Content Delivery Network

- Distributed network of servers to deliver content closer to users (minimizes latency)
- Benefits
    - Performance - user experience and application performance
    - Scaling - protects from high spikes of traffic
- Cache - collects temp copies of assets in CDN server (must specify TTL for this content)
- Origin Server - original location of the content, which contains master copy

ExpressRoute

- Superfast connection between on-premises and Azure
- Dedicated connection which is private (secure), reliable, low-latency and high-bandwidth
- On-premises → ExpressRoute → Azure

Storage

Storage Account

- Unique Azure Namespace (globally unique across Azure)
- Every object has its own web address
- Example
    - AnyCompany is the **storage account name**
    - anycompany.<storage-type>.core.windows.net

Blob

- Binary Large Object (almost everything made from bits-bytes)
- Store images, all file types, stream audio/video, log files, data store (backup)
- Types
    - Block - text & binary data at max 4.7TB
    - Append - Log files where data is constantly appended
    - Page - Store files upto 8TB (virtual hard drive etc.)
- Pricing
    - Hot - Frequently accessed; Low access times = Higher costs
    - Cool - Low storage costs = Higher access times (min storage of 30 days)
    - Archive - Lowest storage costs = Highest access times

Disks

- Managed disks for virtual machines
- Types
    - HDD - low cost old school hard drive (backups)
    - SSD - standard for production (low latency, high reliability and scalability)
    - Premium SSD - better than standard SSD = super fast and high perforce (critical workloads)
    - Ultra Disk - data intensive workloads (upto 64TB), sub-millisecond

File

- Managed file system
- Benefits
    - Sharing - across multiple VM's & on-prem
    - Managed - no need to worry about maintenance
    - Resilient
- Easily upgrade file storage
- Can be Hybrid or Lift and Shift

Archive

- Lowest price
- Durable, encrypted and stable (suitable for infrequent access)

Data Redundancy

- Ensuring multiple copies are readily available
- Azure Storage have **minimum of 3** copies at all the times
- Can be Single zone, multiple-zones, or cross-regions
- Single Region
    - Locally Redundant Storage (LRS)
        - Lowest cost
        - Three copies in single datacenter/zone
    - Zone Redundant Storage (ZRS)
        - One copy per zone (3 zones = 3 copies)
        - Protects against zone outage
- Multiple Region
    - Geo-Redundant Storage (GRS)
        - Three copies in 2 different region (6 total copies) w. LRS
        - Protects against regional failure
        - Option to enable read-access
    - Geo-Zone-Redundant Storage (GZRS)
        - Three copies (ZRS) in *primary* region
        - Three copies in *secondary* region
        - Protect against regional w. primary zone failure

        - Option to enable read access
        - Highest cost

Moving Data

- **AzCopy**
    - Command line utility
    - Transfer blobs and azure files
- **Azure Storage Explorer**
    - GUI - drag and drop
    - All storage format transfer capability
- **Azure File Sync**
    - Synchronize azure files with on-prem file servers
    - Used for backups (local file server), disaster recovery etc.

Migration Solutions

- **Azure Data Box**
    - Transfer vast amount of data
    - Offline data transfer to/from Azure
    - Copy data to physical data storage device (Azure Data Box) that is rugged & encrypted
    - Ship data to/from Azure (storage account)
- **Azure Migrate**
    - Migrate non-Azure resources to Azure (Servers, Databases and Applications)
    - Discover dependent resources
    - Migrate to managed services(databases)
    - Migrate bulk data transfers(data box)

Premium Performance

- **Standard**
    - default options
- **Premium**
    - Premium Block Blobs
        - Ideal for low-latency storage workloads
        - Redundancy (LRS/ZRS only)
    - Premium Page Blobs
        - Unmanaged virtual disk
        - LRS only (single zone)
    - Premium File Shares
        - Azure Files
        - Mainly for high-performance enterprise applications
        - Support for Server Message Block (SMB) and Network File System (NFS) file shares
        - LRS/ZRS only

Database

Cosmos DB

- Globally distributed database
- Synchronization
- 0-9 milliseconds latency
- Scalability and Infinite performance
- Can be costly
- Connect via SDK, API
- Support many programming languages
- Integrate with SQL, MongoDB and Cassandra

Azure SQL

- Database-as-a-Service (DaaS)
- Relational database made by Microsoft
- Ability to migrate on-premise to Azure SQL
- Built in ML optimization and warnings
- Scalability and Reliability
- Azure SQL Database vs Azure SQL Managed Database
- Offers SQL and PostgreSQL

Database Migration

- Azure Database Migration Service

Authentication and Authorization

Identity Services

- Authentication
    - Confirming the identity of the user
- Authorization
    - Comes after authentication

Azure Active Directory (AAD)

- It is **different** than Active Directory
- Accounts are created within AAD service (including the root user upon account creation)
- Tenant
    - represents an organization
    - Dedicated AAD
    - One user = One tenant (can be guests of other tenants)
- Subscription
    - Billing Entities that receives invoices for each resources every month
    - Cost separation (multiple subscriptions per tenant for separating costs)
    - Resources subscribed will terminate if subscription isn't paid
- Can help managing users for hybrid cloud architecture

Microsoft Entra (new Microsft Product family)

- Azure AD + Permission Management + Verified ID + Identity and Access capabilities

Zero Trust Concepts

- Trusted Perimeter
    - Trust boundary for secure access (corporate network)
    - Devices outside corporate network aren't trusted and vice versa
- *All users are assumed untrustworthy unless proven otherwise*
    - Principle of Least Privilege
    - Trusted by **identity**

Multi-Factor Authentication

- "Something you have" → DUO, Google Auth etc. factor in addition with "Something you know" → Password
- More secure but Less convenient

Conditional Access

- If/then policy for granting access
- Often paired with MFA
- Assigns *signals* (conditions) and Access *decisions (*grant/block/MFA)

Password-less Authentication

- High Security + Convenient
- Microsoft Authenticator Mobile App (for official MFA)
- Windows Hello
- FIDO2 Key (YubiKey)
- Steps: Enter Username → Check Microsoft Authenticator App → Bio-metrics/Pin confirmation → Confirm number challenge

Guess Access

- Business to Business Collaboration
    - Add Guest User
        - Invite account types (Microsoft, Google, Facebook)
        - Assign Permissions (keep PLOP in mind)
        - Assign users to applications
        - Apply policies
    - Invite External
        - Configure identity provider
        - Invite
        - Invitation acceptance

Azure AD Domain Services

- For legacy application that cannot work with modern authentication methods
- Solutions
    - Use on-premise AD (using Azure AD / Connect)

    - Use AD server on Azure VM
    - Use AADDS (this service) that is managed by Azure
        - Create unique domain name
        - One-way sync from Azure AD to Azure AD DS / can be bi-directional as well

Single Sign On

Azure Solutions

Internet of Things

- System of inter-related computing devices that collects and sends data without any human intervention
- **IoT Hub (PaaS)**
    - System that receives and manage the data for millions of devices
- **IoT Central**
    - Appliation PaaS
    - Simplifies and speeds up implementing IoT Solution without coding
- **Azure Sphere**
    - All in one solution for IoT devices on Azure

Big Data

- Benefits
    - Cost savings
    - Speed
    - New products and services
- **Azure Data Analytics**
    - Process large amounts of data without managing servers or hardware
- **Azure HDInsights**
    - Similar to Azure Data Analytics but Open Source
    - Works with Hadoop, Spark, and Kafka
- **Azure Databricks**
    - Based in Apache Spark - distributed cluster-compute framework
    - Integrates with other azure storage services
- **Azure Synapse Analytics**
    - Data warehouse service
    - Can be used for reporting and data analysis

Machine Learning

- **Azure Bot Service**
    - PaaS to build bots for Q&A, Virtual Assistants and more
    - Can be made code or visually + branding + integrate with other services

- **Azure Cognitive Services**
  - Vision - use vision services for recognize pictures and videos (for captioning)
  - Decision - detecting anomalies, offensive language etc.
  - Speech - transcription, identification, and verification
- **Azure Machine Learning Studio**
  - visual tool for machine learning services
- **Azure Machine Learning Service**
  - End to End machine learning services
  - Create model based on usage and interaction with Azure services

Server-less

- **Azure Functions**
  - Function as a Service
  - Only runs once for each invocation
- **Logic Apps**
  - Connect system in and out of Azure platform
  - Schedule and automate tasks and processes
  - No-coding
- **Event Grid**
  - Server-less service
  - Sends and receives events between applications

DevOps

- Work between development and production (mix of development and operation)
- **Azure DevOps (has the following five tools)**
  - **Azure Boards**
    - keeps tracks work tracks, timelines and more.
  - **Azure Pipelines**
    - Produce and test software automatically
  - **Azure Repos**
    - Store source code for application securely
  - **Azure Test Plans**
    - Design test of application and implement automatically
  - **Azure Artifacts**
    - Share application and code libraries with other teams in and out of organization
- **Azure DevTest Labs**
  - Focus on creating environments for test and developments
  - Create templates for reuse
  - Cost managements

Security

- 7 layers of security
    - Physical
    - Identity and Access
    - Perimeter
    - Network
    - Compute
    - Gateways and Firewalls
    - Data
- Firewall - rules that allow or deny traffic before a service
- **Azure DDoS Protection Service**
- **Azure Network Security Group (NSG) -** personal firewalls for resources
- Application Security Groups - protects application infrastructure
- Public vs Private endpoints
- **Microsoft Defender for Cloud**
    - threat alerts
    - work with hybrid -cloud
    - policy and compliance metrics
- **Azure Key Vault**
    - Secure place to store secret passwords (including rotations)
    - Secure hardware + Application isolation + scalable
- **Azure Information Protection**
    - secure documents, emails and data outside of the company network
    - classify data + log activities + share data + more
- **Microsoft Defender for Identity**
    - Monitor users and behavior
    - Baseline behavior + suggest changes
- **Azure Sentinel**
    - Security information and event management tool (SIEM)
    - step 1 - collection of data
    - step 2 - aggregate data
    - step 3 - analysis + threat detection
    - step 4 - magic happens
    - step 5 - take action
    - use case - behavioral analytics, aws integrations, cloud scale etc.
- **Azure Dedicated Hosts**
    - Physical server under control
    - Meet compliance requirements

Monitoring and Management

- **Azure Policy**

    - Used to create policy
    - A set of rules to ensure resources are compliant
- **Role-based access control (RBAC)**
    - Define user access
    - Follow POLP
    - *Security Principal* - entity that can access the resource
    - *Role Definition* - collection of permissions (read, write, delete)
    - *Scope* - resources access applies to
- **Locks**
    - Simple and efficient to manage changes and removal of resources
    - can be assigned to subscription,resource group or resource
- **Azure Blueprints -** templates for creating Azure resources (package of resources templates, RBAC, policies)
- **Cloud Adoption Framework -** collection of docs to guide through cloud adoption process + guidance + governance
- **Azure Advisor for Security Assistance**
- **Azure Monitor -** telemetry (information about how services are performing)
    - Fully managed + query + machine learning capabilities
    - Maximize performance and prevention
- **Log Analytics**
    - analyze logs and telemetry data
    - query and store data for insights
- **Application Insights**
    - performance insights for web applications
    - answers questions like, "*How are users using our application?"*
- **Azure Monitor Alerts**
    - Notification when things break (unexpected events)
    - Alert Rule
        - trigger (monitored resource)
        - telemetry (metric i.e. memory utilization)
        - condition (i.e. < 5%)
        - severity (2 - warning)
    - Action group - action taken when rule is triggered
- **Azure Service Health**
    - notifies about planned and unplanned incidents on the platform
    - real-time tracking (free service) + notifies if any resources is affected as a result
- **Compliance**
    - GDPR, ISO, NIST - regulations and standard for compliance
    - **Azure Compliance Manager -** recommendation for ensuring compliance, task assignment, compliance score, secure store of docs, reports of compliance
    - **Azure Government Cloud -** dedicated cloud regions mainly for government body / contracts
    - **China Region -**data-center in China. data stays in China. Cannot be global if this region is selected
- **Privacy**

    - **Azure Privacy -** AIP, PA, Guides, CM
- **Trust**
    - **Azure Trust Center -** hub for security and privacy implementation for services
    - **Service Trust Portal -** review independent reports and audits performed on MS products and services
- **Azure Arc**
    - ability to manage both Azure and Non-Azure resources
    - extends azure control to non-azure environments

Pricing

- Subscription
    - All resources belong to a subscription
    - Multiple subscriptions - can have multiple subscriptions
    - Billing Admin - pays for subscriptions
    - Billing Cycle - 30/60 days
- Management groups
    - access policies and compliance in bulk
    - maintain billing associated with the budgets
    - manage multiple subscriptions
- **Azure Cost Management**
    - portal to visualize cost with a detailed view of current and future projected costs
    - reports and recommendations
    - optimization (multi-cloud)
- **Spot VMs**
    - deep discounts for compute (save upto 90%)
    - used for non-production loads (can be interrupted)
- Ingree (data in) is *FREE,* egrees (data out) is *NOT FREE*
- Data transfer within same zone is *FREE*
- **Pricing Calculator**
- Spending Limit
- Quotas - can be increase (charges can incurr)
- Tags
- **Reserved Instances -** 1 or 3 years commitment
- **Azure Hybrid Benefit -** use existing licences
- **Advisor -** best practices for Azure resource (including cost optimization)

Support

- Five support plans
    - Included in all plans
        - 24/7 billing support
        - Self help online + forums

        - Azure Advisor
        - Service Health
    - Basic - all above
    - Developer
    - Standard
    - Professional Direct - arch guidance, webinar training, on-boarding reviews, < 1 - 8 hrs based in sev
    - Premier - on demand training, < 15 min support, tech account manager
- Tickets - support inquiry
- Channels - Azure documentation, forums, social media
- SLA - contract between a service provider and a client