Describe Cloud Concepts

LP: https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/

Identify Cloud Computing benefits, use GASHED:

- **Geo-distribution**
- **Agility**
- **Scalability**
- **High Availability**
- **Elasticity**
- **Disaster Recovery**

Azure Portal

Definition: Web-based unified console that allows you to build, manage, and monitor everything in Azure.

Azure Marketplace

Definition: Connects users to partners and vendors that offer solutions/services for Azure

Accounts

Azure Account -> Many subscriptions -> Many Resource groups -> Resources

Types of Cloud

Type	Description	Expenditure
Public	Services over the internet. Owned by a third party	OpEx
Private	Exclusive by users from a company. Can be on-premise, datacenter, or hosted by a third-party service provider.	CapEx
Hybrid	Combination of Public and Private	

Expenses

Describe CapEx (Capital Expenditures) and OpEx (Operational Expenditures)

Type	Description
Capital Expenditure (CapEx)	Up-front spending on infrastructure. Value is reduced over time

Type	Description
Operational Expenditure (OpEx)	No up-front cost. Spending only on services and billed for what you use

Consumption-Based Model

Is the basis of OpEx:

- **No up-front costs**
- **Only pay for what you use/need**
- **Pay for additional resources when they are needed**
- **Stop paying for what you don't use**

Cloud Service models

Model	Description	Complexity/Ownership
IaaS	OS and Network owned by the user, including maintenance and configuration	High
PaaS	Apps are deployed into a managed OS. No ownership of hardware or software requirements	Medium
SaaS	User only provides data. Everything else is managed. E.g. MS Office	Low

Subscriptions, Management Groups, and Resources

Name	Definition
Management Groups	Manage access, policy, compliance for multiple subscriptions
Subscriptions	Groups accounts with resources. Can be used to manage costs+resources
Resource Groups	A logical grouping of services (resources)
Resources	Services that you create. E.g. a Virtual Machine

Azure Architecture and Services

Learning Path

Azure Regions

Definition: A geographical area with one or more datacenters nearby and networked together.

Special Regions: US DoD, US Gov: physically+logically isolated with additional compliance certifications. China is operated by 21Vianet.

Azure availability Zones

Definition: One or more physically separate datacenters within an Azure region. A.K.A. Isolation Boundary (HA/redundancy).

Availability Zones are interconnected with ultra high-speed, private, fiber network.

Not all regions have AZs.

Services that support AZs have these categories:

- **Zonal service**: Pins to a zone
- **Zone-redundant**: Auto-replication across zones
- **Non-regional**: HA in an Azure geography.

Azure Region Pairs

Definition: Each Azure region is **always paired** with another region within the same geography.

AZs have one or more datacenters, and a Region has at least 3 zones.

Helps protect against natural disasters or civil unrest. Separated at least 300 miles.

Replication resides always within the same Geography as the pair except for Brazil South.

Azure resources and Azure resource Manager

Resource: A manageable item within Azure. Like a database or a VM **Resource group**: A grouping of resources you want to manage as a group.

Azure Resource Groups

Can contain anything you create in Azure to form a logical grouping of services (resources). Helps provide organization.

- **Life cycle**: If you delete a resource group, all contained resources are deleted as well. Makes it easier to get rid of.
- **Authorization**: A resource group is a scope for applying RBAC

Azure Resource Manager

Definition: Deployment and management service for Azure. CRUD for Azure resources

- Manage infrastructure with templates
- Deploy, manage, and monitor
- Define dependencies between resources for correct ordering
- Apply RBAC and tags

Azure subscriptions

Definition: Provides you with authenticated and authorized access to products and services. Always linked back to an account.

An account can have one or many subscriptions.

Types of subscription boundaries:

- **Billing boundary**: Determines how an Azure account is billed. You can create multiple subscriptions for different billing requirements.
- **Access Control boundary**: Access-management policies happen at the subscription level. You can control access+resources for specific subscriptions.

Additional subscription helps with:

- **Environments**: Separate environments via subscriptions. E.g. development and testing
- **Org structure**: Marketing and IT, helping manage access and limit resources
- **Billing**: Make it easier to track billing better.

Azure management groups

Definition: Provides a level of scope above subscriptions. Helps organize subscriptions into groups.

Helps provide user access to multiple subscriptions with a single RBAC that gets inherited

Azure Compute Services

LM: https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/

Virtual Machines (VMs)

Definition: Emulate physical machines. These provide IaaS.

Virtual machine scale sets

Definition: Deploy and manage set of identical VMs. Supports autoscale

Containers and K8s

Definition: Azure compute resources that you can use to deploy+manage containers. Quickly create, scale, and stop dynamically.

Azure App Service

Definition: a Paas that allows to build, deploy, and scale web/mobile/API apps on any platform.

Types:

- Web apps
- API apps
- Webjobs (for background tasks)
- Mobile apps

Service handles:

- Deployment and management
- Can secure endpoints
- Scaling of sites
- Built-in load balancing and traffic manager

Azure Functions

Definition: Serverless code that does not require managing the underlying platform.

Similar to Azure Logic Apps. Both are serverless.

Use them for:

- Running on a timer
- Trigger over HTTP
- With queues.

Key difference with Azure Logic Apps: Functions requires code and is not an orchestration service

When to use VMs

- Total control of the OS
- To use custom Software
- Custom hosting configurations

Example scenarios:

- In testing/development
- When extending your datacenter to the cloud
- For disaster recovery (quickly provisioning VMs)

Azure Batch

Definition: Allows large-scale parallel and high-performance computing (HPC) batch jobs. Can scale to thousands of VMs

Batch can:

- Start a pool of compute
- Install apps + stage data
- Run jobs
- Identify failures
- Reque work
- Scale down

Azure Logic Apps

Definition: It executes workflows, designed to automate (orchestrate) business scenario from predefined logic blocks

Similar to Functions. Both can get triggered with logic based on event.

Workflows are persisted in JSON.

Declarative and stateful. Runs only in the cloud.

Key difference with Azure Functions: Logic Apps don't require code, and it is an orchestration service

Azure Virtual Desktop

Definition: A Windows desktop virtualization service in the cloud.

Works across devices like Windows, Mac, iOS, Android, and Linux. Including most browsers

Use it because:

- Provides flexibility (supported across devices)
- Enhanced security. Data+apps are separate from the local hardware
- **Simplified management**: with Azure AD + RBAC
- **Performance management**: Can load balance on VM host pools
- **Multi-session**: Allows concurrent users on Windows 10

Reduce costs by bringing your own licenses. Available with no extra costs for existing MSFT 365 license. Save on compute by buying 1 or 3 year Azure reserved virtual machine instances.

Azure Networking

LM https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/

Azure Virtual Network fundamentals

- Isolate
- Communicate over the internet
- Communicate between Azure resources
- Communicate with on-premise
- Route+filter traffic
- Connect virtual networks

Internet communications: VMs can connect to the internet *by default*

Communicate between Azure resources: with Virtual networks, or service endpoints (from an Azure resource)

Communicate with on-premise:

- via Point-to-site (typical VPN)
- Site-to-site (everything appears on the same network)
- Azure ExpressRoute: dedicated private connection to Azure (not over the internet)

Route Network traffic

- Route tables: defines rules for directing network traffic
- Border Gateway Protocol: (BGP) Propagate on-premises BGP to Azure virtual networks

Connect virtual networks: With network peering. Peering allows connecting virtual networks together.

Azure VPN gateway fundamentals

VPN Gateway

Definition: A type of virtual network gateway.

They enable:

- Connecting on-premise datacenter to virtual networks (site-to-site)
- Connecting individual devices to virtual networks (point-to-site)
- Connect virtual networks to other virtual networks (network-to-network)

Only 1 VPN gateway per virtual network

Supports two types:

Policy-based

- IKEv1 only

- Static-routing: Combinations of address prefixes control traffic. Source+destination are declared in policy (**not** in routing tables)
- Mainly used for compatibility with legacy VPN

Route-based Use it for:

- point-to-site, connections between virtual networks, multisite, coexistence with Azure ExpressRoute
- IKEv2 support
- Wildcard (any-to-any) traffic selectors
- Dynamic routing protocols. Source/Destination networks don't need to be statically defined. Supports Border Gateway Protocol (BGP)

Gateway sizes

- Basic (does not support Border Gateway Protocol)
- VpnGw1
- VpnGw2
- VpnGw3

Required Azure resources

- Virtual Network
- Gateway subnet
- Public IP
- Local network gateway
- Virtual network gateway
- Connection resource

HA for VPN gateways

- **Active/Standby**: By default VPN gateways are deployed as two instances. Automatic failover. Connections can be interrupted
- **Active/Active**: Use with Border Gateway Protocol, create each VPN with unique IPs but separate tunnels from on-premise device.
- **ExpressRoute Failover**: If an ExpressRoute connection fails, connectivity can fail over to traffic over the internet with the VPN
- **Zone-redundant gateways** For regions that support AZs, VPNs can be deployed with zone-redundancy. Requires a Standard public IP (not a **basic** IP)

Azure ExpressRoute Fundamentals

LM https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/express-route-fundamentals

Definition: Extends/connects your on-premise network into Azure over a private connection (**not** over the internet)

Connection types:

- Point-to-Point (between nodes) (L2)
- Any-to-Any (VPN) (L3)

Features:

- Fast (over private fiber optic)
- Low latency
- Higher security
- Global connectivity with ExpressRoute premium
- Reduntant + Dynamic Routing
- Uptime SLA

Redundancy

Only for Layer 3 connections. Redundancy uses multiple devices for HA

Connectiviy to cloud services

Direct connection to:

- Compute services like: VMs
- Cloud services like Cosmos DB or Storage

Dynamic Routing

Uses Border Gateway Protocol (BGP) routing protocol, allowing dymaic routing between on-premise and Azure services

Connectivity Models

- **Cloud Exchange**: From an ISP/Datacenter to Azure
- **Point-to-Point**: From on-premise to Azure
- **Any-to-Any**: WAN with Azure with L3 connectivity. Access Azure like any private service in a WAN

Azure Storage Services

LM https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/

Disk Storage

Definition: Provides (virtual) disks for Azure VMs. Similar like on-premise server with disks.

Types:

- SSDs
- HDDs
- Premium SSDs
- Ultra Disks

ZERO% annualized failure rate.

Blob storage

Definition: Unstructured object storage for massive amounts of data.

Features:

- Can be readched anywhere from http
- Does not require space/disk management

Use it for:

- Serve assets over to a browser
- Store files for distributed access
- Video+Audio streaming
- Disaster recovery backups
- Analyzis for on-premise Azure-hosted services
- Storing up to 8TB of data for VMs

Blobs are stored in containers which are owned by an account:

Account -> Many containers (e.g. movies/pictures) -> many blobs (files)

Azure files

Definition: Is a file share service in the cloud available via SMB (Server Message Block) and NFS (preview) (Network File System).

File shares can be mounted on Windows, Linux and OSX at the same time.

Features:

- Data encrypted at rest.
- Access files from anywhere in the world via a URL

- Provide temporary access with a SAS (Shared Access Signature)

Use it for:

- Seamless support for apps that use SMB that need to be migrated to the cloud
- Store, retrieve, and share configuration files that can be accessed by multiple VMs
- Write metrics, crash dumps, or diagnostic logs, so that they can be analyzed later

Blob Access Tiers

Definition: Allows organizing data depending on access frequency and retention period.

- **Hot access tier**: Frequently accessed data like website assets
- **Cool access tier**: Infrequent access stored for at least 30 days
- **Archive access tier**: Almost never accessed and stored for at least 180 days, like backups

Service attributes:

- Hot + Cool tiers are set at the account level. Acrhive isn't available at the account level.
- All tiers can be set before or after uploading at the blob level.
- Archive has the lowest cost, but it is more expensive to rehydrate and access data.

Tier cost

Tier	SLA	Access Cost	Storage Cost
Hot	High	Low	High
Cold	Medium	High	Low
Archive	-	Highest	Lowest

Azure Database and analytics

LM https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/

Azure Cosmos DB

Definition: A globally distributed, multi-model database service.

Although usually meant for Key/Value store, it abstracts out several APIs providing support for:

- SQL
- MongoDB
- Cassandra

- Tables
- Gremlin

Azure SQL Database

Definition: Relational DB based on the latest stable version of Microsoft SQL Server database.

Features:

- HA: 99.99%
- PaaS: Update, patching, backups, and monitoring are all managed
- Fully managed: No need to manage infrastructure or the OS
- Can process relational and non-relational data like graphs, JSON, and XML

Key differences from SQL Managed Database:

- Offers *less* options that are available in Azure SQL Managed Database

See: https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison

Azure SQL Managed Instance

Definition: Similar to SQL Database. Relational DB based on the latest stable version of Microsoft SQL Server database.

Features:

- HA: 99.99%
- PaaS: Update, patching, backups, and monitoring are all managed
- Fully managed: No need to manage infrastructure or the OS
- Can process relational and non-relational data like graphs, JSON, and XML
- Can use the Azure Database Migration Service (DMS) or native backup/restore

Key differences from SQL Database:

- Offers *more* options that aren't available in Azure SQL Database
- Can manually initiate backups
- Has access to all built-in functions
- Collation choices at instance creation
- Cross-database name queries and transactions
- Database Mail

See: https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison

Azure Database for MySQL

Definition: Relational DB based on MySQL community edition

Features:

- HA at no additional cost
- Automatic backups + up to 35 days for a point-in-time restore
- Scale as needed within seconds
- Fully managed
- Several tiers offered

Azure Database for PostgreSQL

Definition: Relational DB based on PostgreSQL database engine

Features:

- HA at no additional cost
- Automatic backups + up to 35 days for a point-in-time restore
- Scale as needed within seconds
- Fully managed
- SSL encryption between client and server communications

Available in two deployment options:

Single Server

- 3 tiers: Basic, General, and Memory Optimized
- Dynamic scaling

Hyperscale (Citus)

- Horizontally scalling using sharding
- Query parallelization across server for fast responses on large datasets
- Made for applications that need greater scale+performance for 100GB of data or more
- Supports multi-tenant, real-time analytics, high (transactional) throughput
- Standard connection + minimal changes

Azure Synapse Analytics

Definition: Limitless analytics service for big data analytics.

Features:

- Serverless queries or provisioned resources at scale
- Unified experience to ingest+prepare+manage+serve data
- Data warehousing
- Big data analytics

Azure HDInsight

Definition: Fully managed analytics service

Features:

- Works with Apache Spark, Apache Hadoop, Apache Kafka, Apache HBase, Apache Storm
- Supports Machine Learning Services
- ETL support
- Data Warehousing

Azure Delta Lake Analytics

Definition: Simplified on-demand analytics job service for big-data

Features:

- Handle jobs of any scale
- Configure analytics power instantly
- Pay for when the job is running (cost effective)

Azure Databricks

Definition: Apache Spark environment to build AI solutions and insights from data.

Features:

- Support for Python, Scala, Java, and SQL
- Support for data science frameworks like TensorFlow, PyTorch, and Scikit-Learn

Azure identity, access, and security

LM: https://learn.microsoft.com/en-us/training/modules/describe-azure-identity-access-security/

Azure Active Directory (AAD)

Definition: Cloud-based identity and access management service

Active Directory	Azure Active Directory
Managed by your own org	Managed by Azure

Active Directory	Azure Active Directory
On-premise identity control	Global identity control service

Note: Can connect AAD with Active Directory for sign-in attempts

Features:

- Control access to applications and resources
- SSO functionality within apps, integration with existing creds
- Self-service password reset for users
- MSFT 365, Azure, and other services already use AAD

Services:

- Authentication
- Single Sign-On (SSO)
- Application management
- Device management (device registration)

Secure:

- Both internal and external resources
- Internal resources like on-premise (behind firewall) apps and resources

Connect AD with AAD

- Azure AD Connect syncs user identities between on-premise and cloud (AAD).
- SSO, password resets, multi-factor auth within both systems

Azure Active Directory Domain Services

Definition: Azure AD DS provides managed domain services like domain join, group policy, LDAP (Lightweight Directory Access Protocol), and Kerberos

- Create an Azure AD DS managed domain with a unique namespace
- Namespace becomes the domain name
- 2 Windows Server domain controllers are deployed into selected Azure region A.K.A replica sets.

DC stands for Domain Controllers

Features:

- No need to manage/configure DCs

- One-way synchronization from Azure AD to Azure AD DS (not backwards!)

Single Sign-On

Definition: Allows to sign-in one time and use that credential for multiple applications and resources. Applications must trust the initial authenticator

Multifactor Authentication

Definition: Prompts a user for an extra form (factor) of identification.

Feature: Prevents problems with compromised passwords

Uses two or more of:

- Something the user knows (a challenge question)
- Something the user has (phone)
- Something the user is (fingerprint)

Azure AD Multi-factor authentication

Definition: Provides multifactor authentication capabilities on Azure Active Directory

Passwordless Authentication

Definition: A way to authenticate without the need of passwords or extra security layers.

Example: A computer that is enrolled (registered) and Azure knows that it is associated with you.

Integrations:

- Windows Hello for Businness
- Microsoft Authenticator App
- FIDO2 security keys

Windows Hello For Business

Definition: Uses biometric and PIN crednetials directly tied to the user's PC (only work on Windows PC) to access resources on-premises and in the cloud.

Microsoft Authenticator App

Definition: A cellphone application that allows getting a notification that can enable a user to allow reousrces after using biometric information or PIN to confirm access.

FIDO2 (Fast IDentity Online) Security Keys

Definition: It is an open standard for passwordless authentication alloing users to sign-in by using an external security key or platform key built into a device.

Azure AD External Identities

Definition: A way to collaborate with partners (B2B) outside of your organization. External providers manage identity while AAD External Identities manages access.

Note: Sounds similar to SSO (Single Sign-On).

Features:

- B2B Collaboration: Let users choose their preferred identity to sing-in for your resources. B2B users are represented as guest users in your directory
- B2B Direct Connect: Two way trust with another Azure AD organization that enables external users.
- Azure AD Business to Customer (B2C): Publish applications (excluding Microsoft Apps) to consumers/costumers using B2C for identity and access management

Azure Conditional Access

Definition: An Azure AD tool to allow/deny access to resources based on signals. Signals include who, where, and what device the user is requesting access from.

Use it when:

- Requiring Multifactor Authentication
- Requiring access to services through client applications
- Requiring access only through managed devices
- Blocking access from specific locations or devices

Azure Role Based Access Control (RBAC)

Definition: A way to provide access based on role rules that apply to a group instead of per-user privileges. RBAC is applied to a scope which is one or more resource that the access applies to.

-	Reader	Resource-specific	Custom	Contributor	Owner				
Management Group	Observers		Users managing resources			Admins			
Subscription	Observers		Users managing resources			Admins			
Resource Group	Observers		Users managing resources			Admins			
Resource		Automated Processes							

Azure RBAC uses an **allow model**. Roles providing permissions are *additive* for resource and resource groups.

Note: Is enforced on any action that goes through Azure Resource Manager (Portal, Cloud Shell, Power Shell, and Azure CLI). It does *not enforce access permissions* at the application or data level.

Zero Trust Model

Definition: A security model that assumes *the worst case scenario*. Verifies each request as it came from an uncontrolled network.

Principles:

- **Verify explicitly**: Always authenticate/authorize based on all data points
- **Least Privilege Access**: Limit access with Just-In-Time and Just-Enough-Access.
- **Assume Breach**: Access segmentation, end-to-end encryption, analytics for visibility.

Classic Approach: System-wide access behind "secure" network Zero Trust: All assets and resources are protected with central policy

Defense In Depth

Definition: Protect information and prevent unauthorized access using mechanisms to slow down an attack.

Based on usage of layers of access. Each layer protects access further even if one layer is breached. These are:

- Physical (e.g. Hardware and datacenters)
- Identity: Use SSO, audit events, controlled access.
- Perimeter (e.g. DDoS): Firewalls and DDoS protection
- Network: Limit communication between resources. Deny everything by default.
- Compute: Secure access with patched systems (Malware, Viruses, Unpatched vulnerabilities)
- Application: Prevent and patch vulnerabilities. Secure design by default
- Data: Control access for confidentiality, integrity, and availability

Microsoft Defender for Cloud

_ Assess, Secure, and Defend_ Definition: Monitors security and threat protection for cloud, on-premises, hybrid, and multicloud environments to provide guidance and notifiactions.

Azure Native

- **Azure PaaS**: Detects threats against services like App Service, SQL, and Storage Account.
- **Azure data services**: Helps classify data in SQL and get assesments across storage devices.
- **Networks**: Limit exposure to brute force attacks.

Hybrid resources Customized threat intelligence for specific (custom) environments

Multi-Cloud Includes protection on other clous like AWS and GCP, as well as:

- Assets and inventory

- Containers on EKS Linux Clusters
- Windows and Linux EC2 (AWS) Virtual Machines

Three vital needs:

1. Continously Assess: Identify and automatically track vulnerabilities for VMs, Container Registies, and SQL Servers.
2. Secure (harden resources): Provides constant monitoring and recommendations to reduce attacks with secure configuration standards across resources.
3. Defend (detect and resolve threats): Security alerts and advanced threat protection features.

Security alerts generate:

- Description of the affected resources
- Suggests remediation steps
- Optionally a logic app trigger in reponse

Azure Management and Governance

Learning Path

Cost management

Learning Module

Service	Definition
Azure Cost management + Billing	A Free service that helps you grasp your Azure bill, manage subscription, monitor, optimize and control spending.
Azure Reservations	Offers discounted pricing on certain Azure services for reserving and paying in advance for services
Azure Pricing Calculator	A calculator that estimates cost based on all preceding factors according to specific requirements
Azure Advisor	Identifies unused/underutilized resources and makes recommendations.
TCO Calculator	Helps estimate the cost savings of operating your solution on Azure over time vs. on-premise datacenter

Azure Pricing Calculator

Definition: A calculator that estimates cost based on all preceding factors according to specific requirements

Azure Advisor

Definition: Identifies unused/underutilized resources and makes recommendations.

Spending limits

Prevent accidental overrun by setting limits.

Azure Reservations

Definition: offers discounted pricing on certain Azure services for reserving and paying in advance for services

Azure Cost Management + Billing

Definition: A Free service that helps you grasp your Azure bill, manage subscription, monitor, optimize and control spending.

Features and tools for Governance and Compliance

Learning Module

Azure Policy

Definition: Enables you to create, assign, and manage policies that control resources. Highlights non-compliant resources and prevents noncompliant resources from being created.

Can automatically remediate noncompliant resources+configurations

Works with Azure DevOps for CI and Pipeline for app pre and post deployment phases.

Initiative: Individual or group of related policies.

Built-in initiatives for:

- Storage
- Network
- Compute
- Security Center
- Monitoring

Enable it by:

1. Create a definition
2. Assign definition to resources
3. Review results

Enforce:

- VM SKUs
- Allowed geographical locations
- Multifactor authentication with specific permissions
- CORS. Only required domains can interact with certain apps
- Install system updates on machines

Policy assignment:

- To resources
- Takes place within a scope (management group, single subscription, or resource group)
- Automatically inherited for all child resources within a resource group (can be excluded)

Review:

- Each resource is marked as compliant or noncompliant
- Evaluation happens every hour

Initiatives

Definition: groups related policies. Helps track for a larger objective

Initiatives are assigned to a scope of a mangement group, subscription, or resource group.

Azure Blueprints

Definition: Orchestrate/automate deployment of resource templates and artifacts like Roles, Policies, ARM templates, and Resource groups

Action	Description
Define/Create	Describes what should be deployed
Assign	An actual deployed resource
Track	Capture changes via versioning

Artifacts: a component in a Blueprint definition. Can contain zero or more parameters to configure

Resource Locks

Definition: Prevents resources from being accidentally deleted or changed

Level	Permissions
CanNotDelete	Authorized users can still read and modify but can't delete
ReadOnly	Authorized users can read but cannot change. Like Reader role in RBAC

Changes to locked resource: Must remove the lock first. Regardless of RBAC permissions.

Combine: Use locks with Azure Blueprints to prevent accidental lock removal. Blueprints can automatically replace the resource lock if removed.

Service Trust Portal

Definition: Centralized location for content, tooling, and resources for compliance and privacy for Azure.

Example: Applying GDPR constraints or enabling tooling to comply with GDPR in Azure.

Features and tools for managing and deploying Azure resources

Learning Module

Azure Portal

Definition: Build, manage, and organize custom view using the web UI in one centralized place

Azure CLI

Definition: A CLI tool to execute commands in Bash that call the Azure REST API for resource/service management.

It is almost **the same** as Azure PowerShell

Key difference: The syntax used. If you are proficient in Bash, then use the Azure CLI.

Features:

- Execute independently or combined to orchestrate setup, teardown, or maintenance or 1 or more resources
- Deploy an entire infrastructure wich might contain hundreds of resources
- Use imperative code
- Create repeatable+automatable processes by using code
- Windows, Linux, OSX, and browser availability via Azure Cloud Shell

Azure Cloud Shell

Definition: Cloud service that integrates fully with the Azure CLI and the PowerShell

Azure PowerShell

Definition: A shell where you can execute commands called *cmdlets* (command-lets) that call into the Azure REST API for resource/service management.

Features:

- Execute independently or combined to orchestrate setup, teardown, or maintenance or 1 or more resources
- Deploy an entire infrastructure wich might contain hundreds of resources
- Use imperative code
- Create repeatable+automatable processes by using code
- Windows, Linux, OSX, and browser availability via Azure Cloud Shell

Azure Arc

Definition: Allows you to manage both Azure and non-azure resources with ARM (Azure Resource Manager)

Works for servers, K8s, Azure Data services, SQL Server, and VMs (preview)

Azure Resource Manager and ARM Templates

Definition: Deployment and management service for Azure. Abstracts management for CRUD operations in services and infrastructure.

Benefits:

- Manage infrastructure through templates instead of scripts (ARM templates)
- Deploy and re-deploy solutions to a consistent state
- Define or update dependencies in a specific order
- Apply tags for logical organization of resources
- Native RBAC integration

Templates allow you to:

- Create declarative syntax (defining what you want, not the programming logic)
- Repeatable results
- Orchestration (ordering of operations)
- Modular files (smaller reusable files)
- Extensible via PowerShell or Bash

ARM Template features:

- ARM templates are verified before execution

- Orchestration of resources in parallel
- Define only the desired state and configuration of each resource
- Templates can use PowerSHell or the Azure CLI for before/after actions

Monitoring tools in Azure

Learning Module

Azure Advisor

Definition: Evaluates and then provides recommendations for five categories: reliability, security, performance, operational excellence, and reduce costs.

Uses a dashboard with the 5 categories to visualize its recommendations.

Features:

- Get alerts on new recommendations that you can use, dismiss, or postpone
- Personalized recommendations for *all your subscriptions*
- Available in the Azure Portal and the REST API

5 categories:

- **Reliability**: Improve availability of applications
- **Security**: Detect threats and vulnerabilities
- **Performance**: Improve speed of applications
- **Cost**: Optimize/reduce Azure spending
- **Operational Excellence**: Deployment best-practices, efficiency workflow, resource management

Azure Service Health

Definition: Tracks the status of **both** the Azure overall status as well as your individual resources

Type	Description
Azure Status	Overall Azure status, globally. Includes service outages.
Service Health	Narrower view of Azre services and regions
Resource Health	Custom view of *your* individual resources with historical data

status.azure.com does **not** provide the full picture. as its main informational dashabord

Features:

- Both major and smaller health displays, localized to issues that affect you
- Peronalizable to services and regions that are interesting to you
- Set up alerts to help triage outages
- Provides official incident reports and Root Cause Analyses (RCAs)
- Advertises **Planned Maintenance** that can affect availability
- Publishes **Health Advisories** that include service retirements (sunsetting) or breaking changes.

Key difference with status.azure.com: The status dashboard is **not** personalized and not granular to issues that might affect you directly.

Azure Monitor

Definition: Platform to collect, analyze, visualize, and take action based on data from your entire Azure **and on-premise environment**

Features:

- Monitor applications, integrating them with PagerDuty, Jira, or Azure DevOps
- Monitor and optimize your infrastructure, including VMs, K8s, and Storage
- Monitor and diagnose your network, trigger packet capture or analyze routing issues
- Supports an extensive query language to analyze and get insights from operational data
- Visualize, analyze, gain insights, and set alerts based on monitoring data

Application Insights uses Azure Monitor under the hood