

AZ - 900

IYAN S.

Q1 2022



- USE paired regions for backups
- mgmt groups > subscriptions > resource groups > resources
can be nested Billing unit
- ARM - Azure resource Mgr, API handles all resources
- Compute resources:
 - virtual machine (VM) - IaaS
 - App Services (web app) - PaaS
 - Azure Container Services (ACI)
 - Azure Kubernetes services (AKS)
 - Windows Virtual Desktop
- Network Services (Covered)
 - Virtual Networks - VPC
 - VPN Gateway
 - VPN Peering
 - Express Route
 - DDos protection
 - Azure Firewall
 - Network Watcher
 - NSG
 - Traffic Mgr
 - Private Link
 - Load balancer - LB
 - Application Gateway - AGB, LB
 - CDN - ELB
 - Azure Front door service
 - expressroute monitor
 - Azure monitor
- Storage services
 - container (blob) storage
 - file storage
 - gpv2
 - Data Lake Gen2
 - disk storage
 - Hot, cool, archive
 - storage tiers
- DB services
 - dynamoDB
 - cosmos DB
 - Azure SQL DB - Aurora
 - Azure DB for MySQL
 - Azure DB for PostgreSQL
 - SQL managed instance

Azure Core Solutions

IoT

- IoT Hub
- IoT Central } comms for devices to cloud
- Azure Sphere - chip, protocol, security

Big Data

- Azure Synapse Analytics - SQL data warehouse
- HD Insight - Apache products
- Azure Databricks - Delta analytics & AI/ML

AI

- Azure ML - Applied AI
- Cognitive Services - predictive
- Azure Bot Service - front end chat bot service

Azure Functions

- Azure Functions - Lambda
- Logic Apps - workflows, orchestration
- Event Grid

DevOps Solutions

- Azure DevOps - provides dev services
- GitHub
- GitHub Actions - automate workflows
- Azure DevTest Labs

AZURE MGMT TOOLS

- Azure Advisor - trusted ADV
- ARM Templates - Azure Resource Mgr
- Azure Monitor - CloudWatch, CloudTrail
- Azure Service Health - issues across all AZURE

AZURE SECURITY

- Azure security center - security hub
- Azure Key Vault - KMS & Secrets Mgr & ACM
- Azure Sentinel - Guard Duty
- Azure Dedicated Hosts - single tenancy

AZURE NETWORK SECURITY

- NSG - NACLs
- Azure Firewall - WAF
- DDoS Protection - shield (Basic = free, Standard = paid)

AZURE IDENTITY SERVICES

- Azure AD - diff from on-prem AD, providers IAM
 - preferred solution for identity MGMT
 - individual access: signal > decision > enforcement

AZURE GOVERNANCE FEATURES

- RBAC - reader, contributor, owner
- Resource Locks - WORM
- Azure Policy - create rules against all resources, custom user JSON
- Azure Blueprints - subscription templates w/ policies & roles defined
- Cloud App Framework (CAF) - adoption guidance & tools

AZURE POLICY & COMPLIANCE

- Azure Trusted Cloud - well trusted framework, security pillar
- Online services terms (OST) & privacy statement
- Trust Center
- Azure Sovereign Regions

MANAGING Azure Costs

- * Azure pricing :
 - pay for consumption (metered)
 - pay for time
 - inbound data is free
- * SAVING money
 - Azure Advisor cost tab
 - auto shutdown resources
 - . cool/archive storage where possible
 - . Reserved Instances
 - . set billing Alerts

Azure Pricing Calculator

- TCO calculator - on-prem vs cloud costs

Azure Cost Mgmt - see account cost analysis

Azure SLAs

- * Preview feature , Not for Prod
 - private requires registration } Service
- * General availability : most services } Lifecycle

- * Mgmt Groups : enables orgs to manage the access, policies, & compliance of resources across multiple subscriptions

- * Site-to-site VPN to connect on-prem to Azure via IPSEC/IKE VPN

- * BLOB : object store * Azure Disks : Block-level storage volumes

- * Azure Table : structured NoSQL data in clouds

- * Azure Files : shared access, uses SMB protocol

- * use multiple VNETS to segment / subnet

- * DDoS Standard : mitigate volumetric attacks, protocol, & resource/tpp AIPS
 - can do 5-min increment report } AIPS

- * You can attach NSGs to subnet & network interface

- * Microsoft Defender for Cloud : security posture mgmt & threat protection
 - evaluate compliance, regulatory DASH
 - improve compliance through recommendations

- Application Security Groups: group VM's & define network security policies
- Azure Dedicated Hosts = single tenancy
- Microsoft Sentinel: SIEM & SOAR
- Azure Sphere: built-in comp & security for internet-connected devices
- Defender for Cloud: unified infra security mgmt system
- Azure Firewall: managed, stateful, firewall as a service, HA, scales
- Availability set: logical groupings of VMs, auto distributed in fault domains
 - Fault domains: group of VM's share common power source & switch
 - VMs with 2+ instances deployed in availability set 99.5% avail
- Resource Group: container that holds related resources for Azure solution
 - store metadata, free but resources inside will have costs
- Azure monitor: telemetry & alerts for cloud & on-prem environments
- Azure Cost Mgmt & Billing: optimize cost & efficiency for workloads
 - VMs are billed by the second; disks NOT deleted w/o VM; Disks will incur costs after VM deleted
- Microsoft Defender for Cloud to use just-in-time VM Access (JIT)
- Azure Sphere: MCU, secure environment for IoT
 - Azure IoT Edge: analyze data locally
 - Azure Digital Twins: create digital representation of connected environments
 - Azure SQL Edge: analyze IoT data using MySQL SQL engine
- Azure Synapse Analytics: enterprise data warehousing + data Analytics
 - integrated with Power BI
- Compliance Manager: track & manage to standards & Regs
- Trust Center: ensure Azure env adheres to regional compliance reqs
- Azure AD Connect Health: robust monitoring of on-prem; reliable conn to O365 & Microsoft online services
- Resource Groups: CAN add or remove resources at any time
 - CAN connect to other resources in other RG's
 - regional in scope, CAN span to multiple regions
- Private Load Balancer: provide HA & scale across VM's in VNET
- Microsoft Def for Identity: monitor DC traffic, detect security threats using sensor

- Azure Resource Mgr (ARM) Templates: automate deployment & config of resources across regions
- Data transfer between AZ & regions are NOT free
- Public Load Balance: distribute Internet traffic to VMs
- Point-to-site VPN: for few clients to secure connect to VNET
- NSG can connect to subnets & Network Interface
- Azure Stream Analytics: real-time analytics & event-processing engine
- Azure AD has SLA: 99.9%, same for basic & premium
- Azure Traffic Mgr: DNS based traffic load balancer
- Delete resource group will delete resources inside it
- Data in Azure Storage is replicated 3x in the primary region
- Microsoft Defender for Cloud: evaluate regulatory compliance as well as improve compliance posture