Quiz Solutions

QUIZ NO.2

1. Describe the benefits of AVD. What is the role of Multi-session windows in AVD.

- ★ Benefits of AVD:
  - Centralized Management: Manage desktops and applications from a single console, simplifying administration
  - Improved Security: Enhanced security posture with features like multi-factor authentication, conditional access, and application control
  - Cost Optimization: Reduce IT infrastructure costs by consolidating hardware and software
  - Enhanced Productivity: Provide employees with secure access to their work environments from anywhere
  - Improved Scalability: Easily scale resources up or down based on demand
- ★ Role of Multi-Session Windows in AVD:
  - Cost-Effectiveness: Allows multiple users to share a single Windows 10/11 virtual machine, reducing the number of VMs required.
  - Resource Optimization: Optimizes resource utilization by consolidating user sessions on fewer machines.
  - Simplified Management: Streamlines management by reducing the number of virtual machines to manage.

2. Briefly describe ACI. What container orchestration capabilities are provided by ACI?

- ★ ACI (Azure Container Instances): PaaS offering that runs a single container in Azure without VM management
- ★ Simplified Deployment: Easily deploy and run containers with minimal configuration.
- ★ Resource Isolation: Provides isolated environments for each container, enhancing security and stability.
- ★ Scalability: Automatically scales resources based on demand.
- ★ Integration with Azure Services: Seamlessly integrates with other Azure services like Azure Key Vault and Azure Monitor.

3. Compare VM vs Containers

Containers	**Virtual Machines**
Micro services	Diverse OS (windows and linux)
Rapid development/DevOps as it sits on top of host OS	Isolation
Resource Efficient, scalable, resilient	Legacy apps & lift-and-shift migration

4. What is the purpose of control plane and nodes in AKS?

- Control plane: core KS and orchestrate app. Workload
  - Kube-apiserver: exposes the kubernetes HTTP APi to enable requests from inside and outside the cluster
  - Etcd: key-value store for API data
  - Kube-scheduler: makes scheduling decisions (like master-slave in MapReduce)
  - Kube-controller-manager: implements API logic/behaviour

        - Cloud-controller-manager: embeds cloud-specific control logic to run controllers according to the cloud provider
    - Nodes: underlying VMs that run apps
        - Each AKS cluster has at least one node (which runs AKS node components)
        - Components:
            - Kubelet: ensures containers are running in a pod
            - Kube-proxy: network proxy that maintains network rules on nodes
            - Container runtime: manages execution and lifecycle of containers (software layer)

1. Briefly describe the benefits of App Services.
    - ★ Simplified Development and Deployment: App Services streamline the development and deployment process by abstracting away much of the underlying infrastructure management.
    - ★ High Availability and Scalability: Built-in features like automatic scaling and load balancing ensure high availability and the ability to handle fluctuating traffic demands.
    - ★ Enhanced Security: Robust security features, including built-in authentication, authorization, and security scanning, help protect your applications.
    - ★ Also cost, yada yada

3. Describe the benefits of AVD. How does it ensure that no data is left behind?
    - ★ AVD uses persistent disks to store user data, ensuring that it's not lost when the VM is rebooted or re-imaged

1. Describe container groups and their usage in ACI. What object in Kubernetes provides similar capabilities?
    - ★ Azure Container Instances (ACI) is a serverless container service that uses container groups to deploy and run containers without managing any underlying virtual machines. This makes it a lightweight and cost-effective solution for various workloads
        - A container group is a collection of containers that are deployed and managed together as a single unit
    - ★ Pods in kubernetes

2. Compare virtual machines and containers. Write down the orchestration capabilities provided by Kubernetes.
    - ★ Deployment: Automates the creation and updating of containerized applications.
    - ★ Service Discovery: Enables services to find and communicate with each other within the cluster.
    - ★ Scaling: Automatically scales applications up or down based on demand.
    - ★ Self-Healing: Restarts failed containers and replaces them with healthy ones.
    - ★ Storage Orchestration: Manages persistent storage for applications.
    - ★ Networking: Provides a virtual network for communication between containers and services.

3. Briefly describe Azure Functions. What is the purpose of serverless compute in Functions.
    - ★ A serverless compute service that allows you to run small pieces of code (functions) on-demand without managing any infrastructure
        - Developers can focus on writing business logic without worrying about infrastructure management
        - Only pay for the compute time used, making it cost-effective for event-driven or occasional workloads

4. What are the common types of application that can be hosted in App Services?
    - ★ Web Apps

- ★ API Apps
- ★ Mobile Apps
- ★ Logic Apps

QUIZ NO.3

1. Under what circumstances VPN is used in cloud environments? What are the key requirements to setting up VPN between two sites?

- ★ Connecting on-prem to Azure: extend your on-premises network into the cloud
- ★ Connecting Azure VNETs: secure and private connection between two or more Azure VNETs
    - connect resources in different virtual networks within the same Azure subscription or across subscriptions
- ★ Hybrid Connectivity

2. What is VNET peering? Explain the requirements to set up virtual network peering.

- ★ VNET peering enables secure and private communication between two or more Azure virtual networks
- ★ Allows resources in one virtual network to access resources in another virtual network as if they were within the same network

3. With a subnet mask of 27, how many bits are usable in an IP address? And what is the available range of IP Addresses?

- ★ 32 - 27 = 5
- ★ 2^5 host bits = 32 possible hosts
- ★ Subtract 2 for network and broadcast addresses: 32 - 2 = 30 usable IP addresses

4. You have mistakenly configured a newly created on a virtual network named VNET_TEST. You need to move it to VNET_PROD now. Explain how would you a VM to a new VNET?

- ★ Deallocate the VM in the source VNET.
- ★ Detach any disks attached to the VM.
- ★ Create a new VM in the destination VNET.
- ★ Attach the moved disks to the new VM.
- ★ Reinstall and configure.

5. How can an organization connect its AWS and Azure networks? What are the key requirements to setup such a connection?

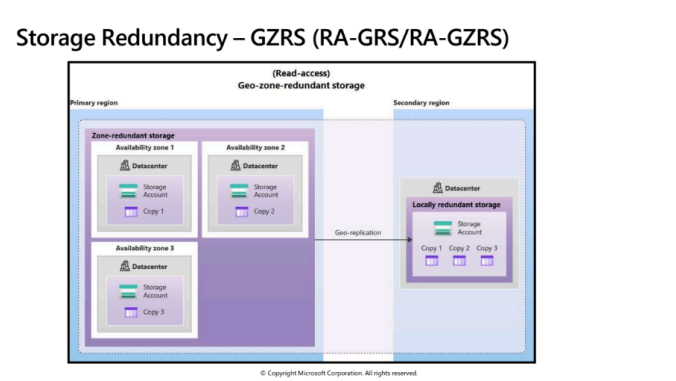
- ★ VPN
- ★ Steps to VPN:
    - Encryption algorithm/hashing - both parties need to know the keys
    - Tunnel to be used
    - IP address range acceptable by both parties

6. You have a VNET with an address space of 10.10.0.0/24. Divide the whole address space into 3 subnets.

- ★ Subnet 1: 10.10.0.0/25 (128 usable IP addresses)
- ★ Subnet 2: 10.10.0.128/25 (128 usable IP addresses)
- ★ Subnet 3: 10.10.1.0/24 (254 usable IP addresses)

QUIZ NO.4

1. Draw a figure to show storage account configured as RA-GRS



2. What is required in DNS to create a custom domain for a storage account?
   - ★ CNAME

3. Name the four services provided by azure on top of storage.
   - ★ Blob
   - ★ File
   - ★ Queue
   - ★ Table

4. What is the purpose of blob lifecycle management rules?
   - ★ Automate the management of the data lifecycle for your blobs, optimizing costs and ensuring compliance
     - Tiering manages costs and retention

5. Briefly provide the purpose of azcopy and azure file sync.
   - ★ Azcopy is primarily designed for efficient data transfer between various Azure storage types (e.g., Blob storage, File storage) and on-premises locations
     - Unidirectional
   - ★ Azure File Sync focuses on synchronizing files between Azure File shares and on-premises servers
     - Centralized

AzCopy	Azure Storage Explorer	Azure File Sync
• Command line utility (copy blobs/files) • To and from storage accounts • Can work with other cloud providers (uni-directional)	• GUI for files/blobs management • AzCopy on the backend	• Centralized file sharing/content delivery network • Bi-directional sync • Cache, all protocols, replace failed local servers, configure cloud tiering for frequent access

6. Briefly describe the usage of blob access tiers
   - ★ Blob access tiers are used to optimize storage costs and performance in Azure Blob Storage by storing data in the most appropriate tier based on access frequency

7. Why azure requires globally unique names for storage accounts?

- ★ ensure that each storage account has a distinct identity and can be accessed and managed without confusion
    - URLS

9. What protocol is used by azure files?
    - ★ Server message block (SMB) or NFS

10. List and briefly describe azure storage access tiers.
    - ★ Access tiers: generated, accessed, processed or modified in (temperature changed based on demand)
        - Hot: frequently
        - Cool: 30 days
        - Cold: 90 days
        - Archive: 180 days
            - Offline storage
            - Cheapest storage, but most expensive rehydration

11. What is the purpose of disk storage in azure storage services?
    - ★ provide high-performance, durable, and scalable storage for virtual machines (VMs) and other Azure services. 1
        - Meet needs of different workloads
        - Durability and availability

QUIZ NO.5

1. Briefly state the following:

a. What is the relationship between Azure App Service and App Service Plan (ASP)?
    - ★ App Service Plan provides the underlying compute resources for App Service
    - ★ App Service is a platform as a service (PaaS) offering that lets you build, deploy, and scale web, mobile, and API apps without managing the underlying infrastructure
    - ★ App Service Plan is a collection of compute resources that provides the environment for your App Service apps to run
        - Defines power, memory, resources

b. What is the minimal ASP which allows you to have deployment slots?
    - ★ Standard

2. Briefly describe the functionality and usage of deployment slots
    - ★ Separate environments within your App Service app that allow you to deploy and test new versions of your application before making them live to your users

3. In app service plan, what is the difference between dedicated compute and isolated compute?
    - ★ Isolated: each app runs on its own dedicated VM within a dedicated virtual network
        - Applications with high security requirements, specific hardware needs, or those that need to be completely isolated from other apps
    - ★ Dedicated: share the same physical or virtual machines (VMs)
        - Most applications that don't require strict isolation or have specific hardware/network needs

4. Explain persistent volume claim and persistent volume in AKS. When would you attach managed disk vs azure files to containers?

- ★ Persistent Volume Claim (PVC): A request for storage by a pod.
    - Specifies the required storage size and access modes (e.g., ReadWriteOnce, ReadOnlyMany, ReadWriteMany).
    - Decouples the pod from the underlying storage implementation.
- ★ Persistent Volume (PV): A piece of storage that has been provisioned for use with Kubernetes pods.
    - Can be dynamically or statically provisioned.
    - Bound to a PVC when matched.
- ★ Managed disks: application primarily deals with large datasets that are accessed infrequently
    - If your application demands high input/output operations per second (IOPS) and low latency
    - When a single pod or a small group of tightly coupled pods needs exclusive access to the storage
- ★ Azure files: when multiple pods or applications need to access the same data concurrently
    - Applications that primarily work with files, such as web servers, media streaming, or file sharing platforms
    - Azure Files can be accessed by various operating systems and platforms, making it suitable for hybrid or multi-cloud environments

5. Briefly state how containers isolation differs from VM isolation? how fault tolerance is managed in containers vs virtual machines.

- ★ VMs: Provide complete isolation, each running its own operating system. This offers strong security, as a compromise in one VM doesn't affect others. However, VMs are resource-intensive, requiring a full OS for each instance.
    - Fault domains, update domains, availability zones
- ★ Containers: Share the host OS's kernel, making them lightweight and efficient. They isolate applications and dependencies within user space. While generally secure, a compromised kernel could affect all containers.
    - Orchestration, replication, self-healing

6. In AKS, what is the role of a) horizontal pod scaler b) cluster auto-scaler.

- ★ Horizontal pod scaler: adjusts the number of pods based on resource demand/utilization
- ★ Cluster auto scaler: Adjusts the number of VMS based on pod scheduling needs

7. For the auto-scale functionality, which is the minimal app service plan that can be used?

- ★ Basic

8. What is the purpose of mountPath attribute in AKS manifest file?

- ★ Allows containers to access data from external storage sources like persistent volumes
- ★ Enables applications to store and retrieve data beyond the container's lifecycle

9. When creating a custom domain for the web app, which DNS record is needed and why?

- ★ CNAME Record: This is the primary record that maps your custom domain to the Azure App Service endpoint
    - Directs traffic from your custom domain to the specific IP addresses or load balancers associated with your Azure web app

QUIZ NO.6

1. Briefly explain the concept of zero trust.

- ★ Zero Trust: assumes the worst case scenario and protects resources with that expectation

        - Verify explicitly
        - Use least privilege access
        - Assume breach
    - Protect assets with central policies

2. Active Directory Domain Services are used to store which kind of objects? Which container in ADDS is used to store these objects?

User Objects	Computer Objects	Group Objects
Username, account, password, group memberships	Security principles (account sign-in creds, they authenticate with domain, can belong to groups and access resources)	Security groups, distribution groups (local, domain, global, universal groups)

The container in AD DS that is used to store these objects is the domain. A domain is a logical grouping of objects that share a common security boundary.

3. Which services are used to synchronize information between ADDS and Entra ID? Which objects are synchronized?
- ★ MS Entra Connect. Users, groups and devices are synced

4. Explain options for password hash sync between ADDS and Entra ID.
- ★ Password Hash Synchronization is a straightforward method for enabling single sign-on between AD DS and Entra ID
- ★ One-way synchronization: Updates are pushed from on-premises AD to Microsoft Entra ID, but not the other way around
- ★ Two-way synchronization: Updates are made in both directions between on-premises AD and Microsoft Entra ID

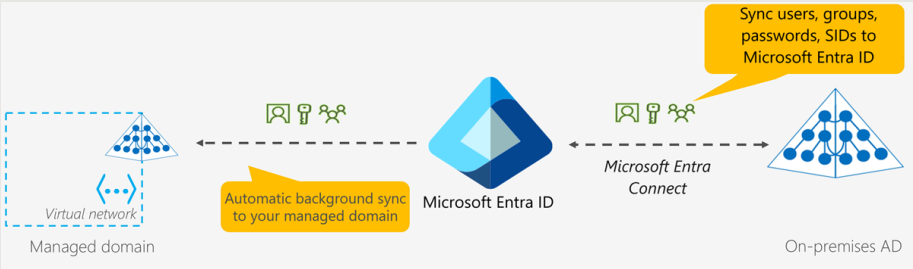
5. Which service allows an administrator to block user access if he is outside his country of residence?
- ★ Conditional access (geographical policy)

6. How would you configure Entra ID to allow only admins to login with MFA but not the regular users?
- ★ Conditional access administrator role

7. How and why secure score is calculated by defender for cloud?
- ★ A percentage that functions as an indicator for how aligned you are with Microsoft's recommendations for security. By comparing the security settings of a subscription's resources to the recommended optimal security settings

8. Briefly describe functionality and usage of Microsoft Entra ID service.
- ★ Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps

9. Draw & briefly explain the process of synchronization of AD objects to Entra Domain Services.
- ★ Use Microsoft Entra Connect to synchronize objects from an on-premises AD DS domain to Microsoft Entra ID.
- ★ Domain Services will automatically synchronize objects and credentials from Microsoft Entra ID to the managed domain.



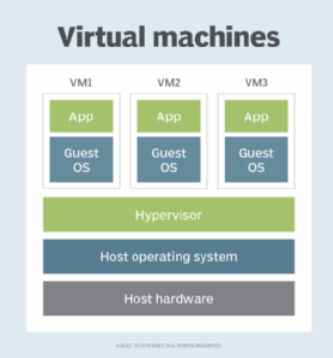
QUIZ NO.7

- ★ Data Warehouses vs OLTP Databases: Data warehouses in Azure Synapse are designed for analytical processing with denormalized schemas, while OLTP databases like Azure SQL focus on transaction processing with normalized schemas for high-speed operations.
- ★ DDL Commands: DDL commands (e.g., CREATE, ALTER, DROP) are used in SQL to define and manage the structure of Azure SQL databases.
- ★ SQL Server on Azure VMs: Use when custom configurations, full control over OS/SQL Server, or compatibility with existing SQL workloads are required. Benefits include scalability, hybrid capabilities, and cost-efficiency.
- ★ Drivers for IaaS Migration: Drivers include cost optimization, scalability, disaster recovery, compliance needs, and reducing on-premises infrastructure dependencies.
- ★ Automatic Index Management: Azure Cosmos DB offers automatic index creation and tuning, reducing the need for manual intervention and improving query performance.
- ★ NoSQL Database Types: Cosmos DB supports key-value, document, column-family, and graph database models.
- ★ Lift-and-Shift for MongoDB: Cosmos DB provides API compatibility with MongoDB, allowing seamless migration without major code changes.

Deck # 3 - Azure Compute

VIRTUAL MACHINES (VMs)

- ★ IaaS in the form of a virtualized server
  - Total control of the OS
  - Run custom softwares
  - Custom host configurations
- ★ Emulations of physical computers (virtual processors, memory, storage, networking)
  - Development & test: custom configurations for testing (eg: run apps on linux nad/or windows)
  - Apps to cloud: efficient resource usage and extended data centers
  - Isolated: each machine is independent
- ★ Image templates: pre configured codes/information



VIRTUAL MACHINE SCALE SETS (VMSS)

- ★ Manage identical, load-balanced VMs
- ★ Vertical scaling (scale up and scale down): increasing or decreasing power to a single instance of a workload
  - Usually manual
- ★ Horizontal scaling (scale out and scale in): increasing or decreasing the number of instances of a workload
  - Frequently automated
- ★ Identical configurations, routing & scaling is automated (horizontal scaling)
  - Centrally manage, configure, and update large number of VMs
  - Auto deploy load balancers (efficient resource utilization)
    - 0 - 1000

VIRTUAL MACHINE AVAILABILITY SETS

- ★ VMs stagger updates, provide varied power and connectivity, ensure not losing data upon network/power failure
  - Update domains: groups of VMs rebooted at the same time (max 20, default 5)
    - Update one group (all VMs at once) while other groups run services
    - 30 mins recovery time
  - Fault domains: common power source & network switch (max 3, default 2)
    - VMs in an availability set are placed in at least two fault domains

VIRTUAL MACHINE SIZING

Name	Core Ratio
General Purpose	1:4
Compute Optimized	1:2
Memory Optimized	1:8
Storage Optimized	Disk throughput
GPU	Graphics & Rendering

STEPS OF CREATING A VIRTUAL MACHINE

1. Start with the network
2. Understand pricing models
3. Name your VM
4. Consider storage
5. Decide location
6. Select Operating System
7. Determine VM size

AZURE VIRTUAL DESKTOP (AVD)

- ★ Cloud-based hosted version of windows
- ★ Create a full desktop environment without having to run additional gateway servers
    - Enables security: EntraID + RBAC + MFA
    - Multi-session: multiple concurrent users on single session/VM
        - Reduce resources being left behind
- ★ Use Azure Portal, Azure CLI, PowerShell, REST API
- ★ Host pods: VMs registered as session hosts
    - Load balancing, scaling, updates, sessions, etc
    - Validation environment: monitor updates before the updates happen (control availability)
    - Application groups: logical grouping of apps
        - Desktop: users access the full Windows desktop from a session host
            - Available with pooled or personal host pools
        - RemoteApp: users access individual applications you select and publish to the application group
            - Available with pooled host pools only

CONTAINERS

- ★ Virtualization environments
    - Lightweight + do not require OS management
- ★ Docker compose vs docker engine vs docker container

- ★ Container groups: collection of containers that get scheduled on the same host machine
    - Share lifecycle, resources, LAN, storage volumes
    - Similar to pods in AKS
        - Single DNS name label, one exposed port that listens
        - YAML file/resource management template
            - Export configurations for later use, using Azure CLI
        - Resource requests
            - Minimum 1GB memory and 1 CPU
        - External facing IP on one or more ports and a FQDN
    - Azure File Share, cloud Git repo allowed for storage
    - Run web apps, logging containers, monitoring containers, front-end/back-end containers
- ★ ACI (Azure Container Instances): PaaS offering that runs a single container in Azure without VM management
- ★ AKS (Azure Kubernetes Service): orchestration service for containers with distributed architecture and large volumes of containers
    - Automating deployment, scaling, management of containerized apps
    - Control plane: core KS and orchestrate app. Workload
        - Kube-apiserver: exposes the kubernetes HTTP APi to enable requests from inside and outside the cluster
        - Etcd: key-value store for API data
        - Kube-scheduler: makes scheduling decisions (like master-slave in MapReduce)
        - Kube-controller-manager: implements API logic/behaviour
        - Cloud-controller-manager: embeds cloud-specific control logic to run controllers according to the cloud provider
    - Nodes: underlying VMs that run apps
        - Each AKS cluster has at least one node (which runs AKS node components)
        - Components:
            - Kubelet: ensures containers are running in a pod
            - Kube-proxy: network proxy that maintains network rules on nodes
            - Container runtime: manages execution and lifecycle of containers (software layer)
- ★ ACA (Azure Container Apps): ACI but with load balancing & scaling (elasticity)

Containers	Virtual Machines
Micro services	Diverse OS (windows and linux)
Rapid development/DevOps as it sits on top of host OS	Isolation
Resource Efficient, scalable, resilient	Legacy apps & lift-and-shift migration

AZURE FUNCTIONS

- ★ Event driven, serverless (don't worry about infrastructure) compute
    - No VMs or Containers required
- ★ REST requests

    - Timers or message events
    - Auto-scale based on demand
        - Auto allocate/deallocate
- ★ ML/AI, scheduled tasks, alerts

AZURE APP SERVICES

- ★ Event driven, serverless (don't worry about infrastructure) compute

Deck # 4 - Azure Networking

VIRTUAL NETWORKS (VNETs)

- ★ Enable Azure resources to communicate with each other, users on internet, and with on-prem client computers
  - Isolation & segmentation: define public/private address spaces that exist within a VNET & not routable to the internet
  - Internet communications: public IP or public load balancer
  - Communication between Azure resources and on-prem resources
  - Route & filter network traffic: route tables (traffic redirection), BGP, security rules
  - Connect VNETs
- ★ Name resolution using DNS configuration (build-in Azure)
- ★ Public vs private communication endpoints
  - Public IP
  - Private IP from the VNET address space
- ★ Azure VNET resource communications
  - Connect with resources such as app service environment, AKS, VMSS
  - Service endpoints connect to other resource types (AzSQL, storage accounts)
    - Improve security
    - Optimal routing
- ★ On-prem connections
  - Point-to-site: outside the organization to inside (encrypted VPN) network
  - Site-to-site: link on-site VPN to AzureVPN
    - Appear as a part of local network
  - Azure Express Route: dedicated private connectivity to avoid public exposure using greater bandwidth on (connectivity provider)
- ★ Peering: two VNETs connect to each other directly
  - Network traffic in private (MS backbone network)
  - VNETs can be in separate regions (global interconnected networks)
  - User defined routes: custom routing tables

VIRTUAL PRIVATE NETWORKS (VPNs)

- ★ VPN uses encrypted tunnel within another network (default authentication is the preshared key)
  - Two or more trusted networks over an untrusted channel
- ★ VPN gateway: instances are deployed in dedicated subnet of VNETs
  - On-prem data centers to VNETs
  - Individual devices to VNETs
  - VNETs to VNETs or coexistence with Express Route Gateway
- ★ Only one VPN gateway per VNET
  - Multiple locations
- ★ Types of VPN:
  - Policy based: static IP specification using tunneling tables
  - Route based: network interfaces, flexible to topology changes

        - Preferred for on-prem

AZURE VPNs

- ★ VPN must be highly scalable and fault tolerant
    - Active/standby: 2 instances, even if we only see one gateway
        - Standby auto assumes responsibility during updates
        - Maximum 90 seconds to restore in case of unexpected failures
    - Active/active: used in BGP
        - Unique public IP in each instance
        - Separate tunnel for on-prem to each IP address
        - Additional VPN device on-prem in case of high availability
    - Express Route Failover: configure VPN as failover paths for Express Route (built-in resilience)
        - Not immune to physical problems to the cables
        - Ensures always on
    - Zone redundant gateway: resilience, scalability, higher availability
        - Physical and logical separation
- ★ Express Route
    - Express route circuit establishes connections to MS cloud service
        - Offices, data centers, etc
        - Each location has its own express route
    - Do not go over public internet
        - Reliable, fast, consistent, secure
    - Features: geopolitical connectivity, dynamic routing using BGP, built-in redundancy in every peering location
- ★ Azure DNS: hosting service that provides name resolution using MS Azure infrastructure
    - Manage DNS records using same credentials, APIs and billing as other Azure Services
    - Benefits: reliability (resilient and highly available), performance, security (RBAC, logs, subscriptions), ease of use(CLI, REST API), custom VNETs (domain names), alias records (refer to an Azure resource, auto updates upon IP address changes)

Deck # 5 - Azure Storage Services

AZURE PHYSICAL INFRASTRUCTURE (RECAP)

- ★ Individual data centers are not directly accessible
  - Regions and zones
- ★ Regions: geographical area with at least one data center
  - Nearby
  - Low-latency network
  - Intelligent load balancing
- ★ Zones: separate data centers within a region (one or more data centers)
  - Independent power, cooling, networking
  - Isolation boundary
  - Reliable & resilient
    - Private fiber optic networks

STORAGE ACCOUNTS

- ★ Unique, globally accessible namespace (http/https)
  - Data is secure, highly available, durable, massively scalable

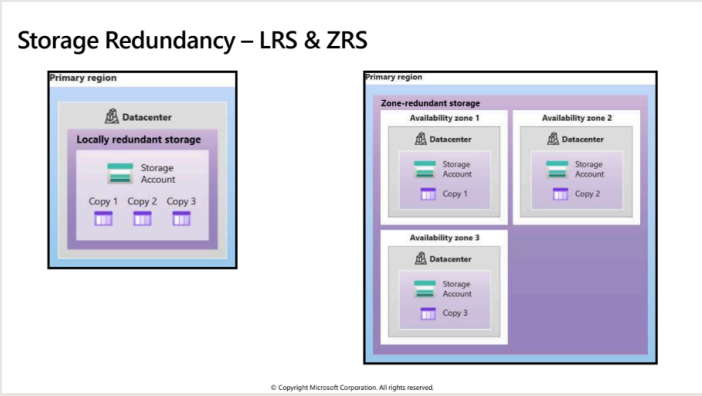
Type	Services	Redundancy	Usage
Standard	Blob, queue, table, Azure files	All	Anything without NFS Azure files
Premium blobs	Blob (block)	LRS, ZRS	Low latency, small transactions, high frequency access
Premium file share	Azure files	LRS, ZRS	SMB & NFS - high performance at enterprise levels
Premium page blobs	Blob (page)	LRS	Page blobs

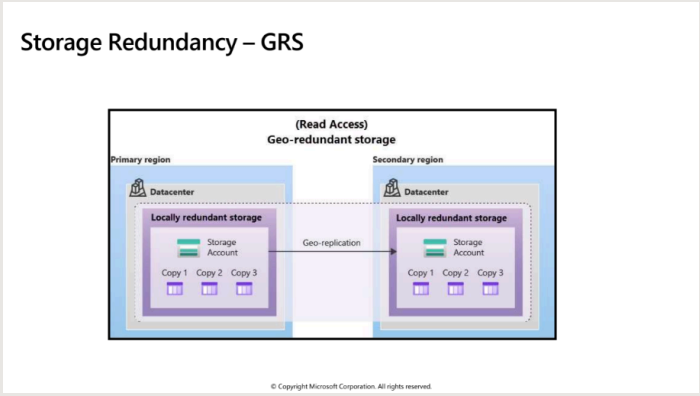
- ★ Naming storage accounts (unique)
  - 3-24 characters (lowercase only, numbers ok!)
  - Eg: https://<accountname1>.dfs.core.windows.net
    - dfs/file/blob/queue

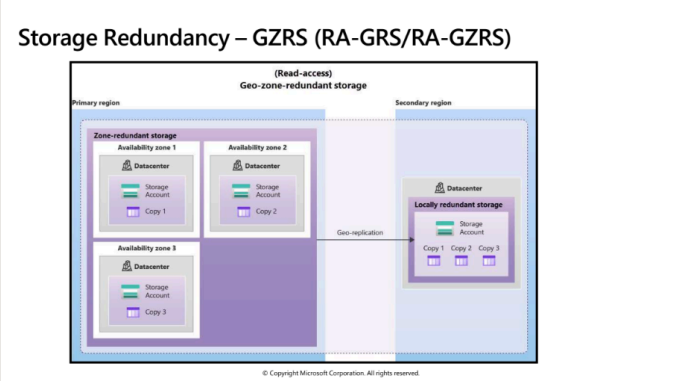
STORAGE REDUNDANCY

- ★ Ensures availability and durability by maintaining copies of data
- ★ Cost - availability trade off
- ★ Primary region redundancy
  - LRS

        - Cannot withstand physical disconnection
    - ZRS
        - Can read/write even if zone fails (fault tolerance)
        - No remounting is required (of clients)
- ★ Secondary region redundancy
    - Cannot be accessed until failure
    - High durability + 300 miles
    - Based on region pairs
    - Async copy
    - RA: Data is available to read from secondary region







- ★ Durable and highly available
    - Redundancy and replication
- ★ Secure: encrypted by service + fine-grained access control
- ★ Scalable
- ★ Managed: Azure automatically updates and maintains
- ★ Accessible: anywhere in the world + REST API + variety of programming languages
    - PowerShell & CLI

AZURE BLOBS

- ★ Text + binary objects storage solution
- ★ High volume of uploads, video data, log files
- ★ Accessible globally through internet
- ★ No need to think about managed disks (integrated availability sets & zones, disk backup, granular access control)
    - Block level storage volumes used by Azure VMs
    - Physical disks on-prem but virtualized

    - Specify disk size, fragments, type
- ★ URLS/REST APIs/CLI/Storage Client Library
- ★ Access tiers: generated, accessed, processed or modified in (temperature changed based on demand)
    - Hot: frequently
    - Cool: 30 days
    - Cold: 90 days
    - Archive: 180 days
        - Offline storage
        - Cheapest storage, but most expensive rehydration

AZURE FILES

- ★ Fully managed file shares accessed through SMD/NFS (containerisation, replace on-prem, lift & shift, simplify cloud development)
    - Bidirectional mounting (on-prem/cloud)
    - Cached using Azure File Sync for frequent access
- ★ Key benefits
    - Shared access (compatible with anything)
        - Ways: direct mount (SMB) and cache using Azure File Sync
    - Fully managed (no need to manage hardware/OS)
    - Scripting/tooling (CLI used to create, mount, etc + Azure Storage Explorer)
    - Built-in resilience and compatible with existing codes
- ★ Secure storage endpoints: restrict access from specific subnet/IP addresses
    - Subnets/VNETs must exist in the same Azure region/region pairs as storage accounts
    - Serverless file share (cloud endpoints) for Azure File Sync

AZURE QUEUES

- ★ Storing large number of messages
    - Access using http/https authentication calls
    - Each message is maximum 64KB
- ★ Commonly used to maintain backlog of work to process asynchronously
- ★ Can be paired with Azure functions events (trigger once customer performs a certain action)

AZURE TABLES

- ★ NoSQL, always-on

AzCopy	Azure Storage Explorer	Azure File Sync
• Command line utility (copy blobs/files) • To and from storage accounts • Can work with other cloud providers (uni-directional)	• GUI for files/blobs management • AzCopy on the backend	• Centralized file sharing/content delivery network • Bi-directional sync • Cache, all protocols, replace failed local servers, configure cloud tiering for frequent access

Deck # 7 - Identity, Access & Security

ACTIVE DOMAIN

- ★ EntraID allows sign-in and access to MS cloud apps and resources
  - Used by admins, developers, users, and subscribers of SaaS services
- ★ For on-prem environments, Active Domain provides identity and access management
  - EntraID controls the accounts
- ★ On-prem AD secure (doesn't monitor) but if configured with EntraID (MS monitors)

ENTRAID - DOES WHAT?

- ★ Authentication
- ★ Single Sign-On
- ★ App management
- ★ Device Management

CONNECT HOW?

- ★ 2 identity sets (on-pre o AD and MS EntraID deployment)
  - If connect AD with EntraID, you can create a consistent link between
- ★ MS EntraConnect: syncs user IDs

ENTRA DOMAIN SERVICE

- ★ Managed domain services that provide domain join, group policy, LDAP (Lightweight Directory Access Protocol), kerberos authentication
- ★ Just like EntraId allows usage of directory services without worrying about the infrastructure, Entra Domain Service lets DS usage without deploying, maintaining, controlling DCs (domain controllers)
  - Run legacy apps/lift-and-shift
  - Use existing credentials to access services/apps on connected domain
- ★ Steps:
  - Define unique namespace (EntraDS)
  - 2 DCs are deployed in Azure region (replica set)
- ★ One-way sync (EntraID to Entra Domain Service)

ADDS

- ★ Services that form the foundation for enterprise networks that run on windows OS
  - ADDS database central store of all domain objects (user accounts, computer accounts, groups)
- ★ Searchable, hierarchical directory for configuration and security settings
- ★ ADDS forest: An AD DS forest is a collection of one or more AD DS trees that contain one or more AD DS domains
  - Share a common root, schema, global catalog
    - A domain tree is a collection of one or more domains that share a contiguous namespace
    - The forest root domain is the first domain that you create in the forest
    - The forest root domain contains objects that don't exist in other domains in the forest

- Security (no users from outside the forest can access any resources inside the forest + trust other domains within forest) and replication boundary (organizations that want to deploy applications with incompatible schemas must deploy additional forests)
- Top-level container
- Provides access to resources in a complex ADDS environment
- Root domain objects:
  - Schema master role
  - Domain naming master role
  - Enterprise admins group
  - Schema admins group
- Other domain objects (also root domains):
  - RID master role
  - PDC emulator master role
  - Infrastructure master role
  - Domain admins group

★ ADDS domain: logical container that manages objects
- Forest: A collection of one or more trees that share a common global catalog, schema, and configuration
- Tree: A hierarchical grouping of domains with a contiguous namespace
- Domain: A logical grouping of computers, users, and other objects
- Trust: A relationship between two or more domains that allows users in one domain to access resources in another domain

★ Relationships:
- Forest Root Domain: The first domain created in a forest
  - foundation for the entire forest
- Child Domain: A domain that is subordinate to the forest root domain or another child domain within the same tree
- Another Tree: A separate tree within the same forest or a tree in a different forest

★ Trust Types:
- Transitive Trust: A trust relationship that extends to other domains within the same forest or tree.
- Non-transitive Trust: A trust relationship that does not extend to other domains.
- Two-way Trust: A trust relationship that allows authentication in both directions.
- One-way Trust: A trust relationship that allows authentication in only one direction.
- Types of trust
  - Parent and child
  - Tree-root
  - External
  - Realm
  - Forest
  - Shortcut

★ Azure AD DS is a managed service that provides on-premises Active Directory Domain Services capabilities in the cloud
- It can be used to extend an on-premises Active Directory environment to the cloud or to create a new, cloud-based Active Directory environment.

★ Azure AD DS and Trust Relationships:

- Azure AD DS can be configured to trust an on-premises Active Directory domain
    - Allows users and devices in the on-premises environment to access resources in the Azure AD DS environment
- Azure AD DS can also be configured to trust other Azure AD DS environments
    - Allows users and devices in one Azure AD DS environment to access resources in another Azure AD DS environment

★ ADDS can:

- Install, configure, update apps
- Manage security infrastructure
- Enable remote access service and direct access
- Issue and manage digital certificates

User Objects	Computer Objects	Group Objects
Username, account, password, group memberships	Security principles (account sign-in creds, they authenticate with domain, can belong to groups and access resources)	Security groups, distribution groups (local, domain, global, universal groups)

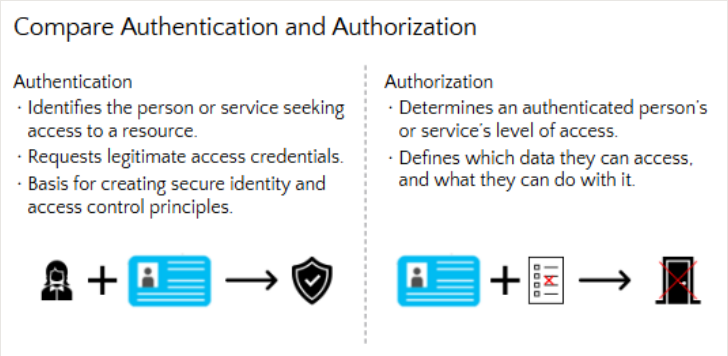
★ What are computer objects?

- Computers, like users, are security principals, in that:
    - They have an account with a sign-in name and password that Windows changes automatically on a periodic basis.
    - They authenticate with the domain.
    - They can belong to groups and have access to resources, and you can configure them by using Group Policy.
- A computer account begins its lifecycle when you create the computer object and join it to your domain. After you join the computer account to your domain, day-to-day administrative tasks include:
    - Configuring computer properties.
    - Moving the computer between OUs.
    - Managing the computer itself.
    - Renaming, resetting, disabling, enabling, and eventually deleting the computer object.
- Before you create a computer object in AD DS, you must have a place to put it. The Computers container is a built-in container in an AD DS domain. This container is the default location for the computer accounts when a computer joins the domain.
    - Container is not an OU, but an object of computer class
    - Cannot create an OU within a container, cannot subdivide the computer container
    - Cannot link a group policy object to container
- OUs are recommended

ENTRA ID

★ Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop.

- ★ For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization.
- ★ Microsoft Entra ID is Microsoft's cloud-based identity and access management service. With Microsoft Entra ID, you control the identity accounts, but Microsoft ensures that the service is available globally.
- ★ Entra ID connect:
    - Provides password hash sync
    - Users and groups sync
- ★ Users can use a single identity to access on-prem apps and cloud services



- ★ MFA can include something you know, something you are, or something you possess
- ★ External identities
    - (B2B) collaboration:
        - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.)
            - B2B collaboration users are represented in your directory, typically as guest users
    - B2C collaboration:
        - Business-to-Consumer collaboration, refers to strategic partnerships between businesses that aim to directly reach and serve individual consumers
- ★ Conditional access: bring signals together, to make decisions, and enforce organizational policies (if-then statements)
    - User or group membership
    - IP location
    - Device
    - Application
    - Risk detection
- ★ When to use conditional access?
    - Require multi factor authentication (MFA) to access an application depending on the requester's role, location, or network. For example, you could require MFA for administrators but not regular users or for people connecting from outside your corporate network.
    - Require access to services only through approved client applications. For example, you could limit which email applications are able to connect to your email service.
    - Require users to access your application only from managed devices. A managed device is a device that meets your standards for security and compliance.
    - Block access from untrusted sources, such as access from unknown or unexpected locations.
- ★ Zero Trust: assumes the worst case scenario and protects resources with that expectation
        - Verify explicitly
        - Use least privilege access

        - Assume breach
    - Protect assets with central policies
- ★ Microsoft Defender for Cloud: unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises
    - Strengthen security posture: Defender for Cloud assesses your environment and enables you to understand the status of your resources, and whether they are secure.
    - Protect against threats: Defender for Cloud assesses your workloads and raises threat prevention recommendations and security alerts.
    - Get secure faster: In Defender for Cloud, everything is done in cloud speed. Because it is natively integrated, deployment is easy, providing you with auto-provisioning and protection with Azure services.
    - Policy compliance Defender for Cloud is built on top of Azure Policy controls so you can set and monitor your policies to run on management groups, across subscriptions, and even for a whole tenant.
    - Security alerts Defender for Cloud automatically collects, analyzes, and integrates log data from your Azure resources like firewall and endpoint protection to detect real threats. Then list of prioritized security alerts is shown in Microsoft Defender for Cloud along with the information you need to quickly investigate and remediate an attack.
    - Secure score Defender for Cloud continually assesses your resources for security issues; then aggregates all the findings into a single score so that you can tell your current security situation.

Deck # 8 - Azure Data Services

CORE DATA CONCEPTS

- ★ EntraID allows sign-in and access to MS cloud apps and resources

Lazy bas