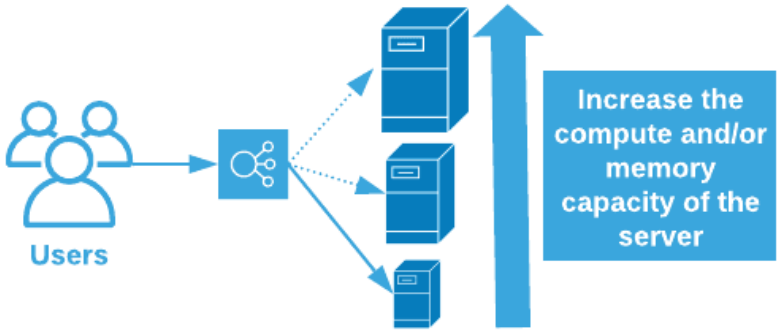
AZ-900 MS-Learn V1

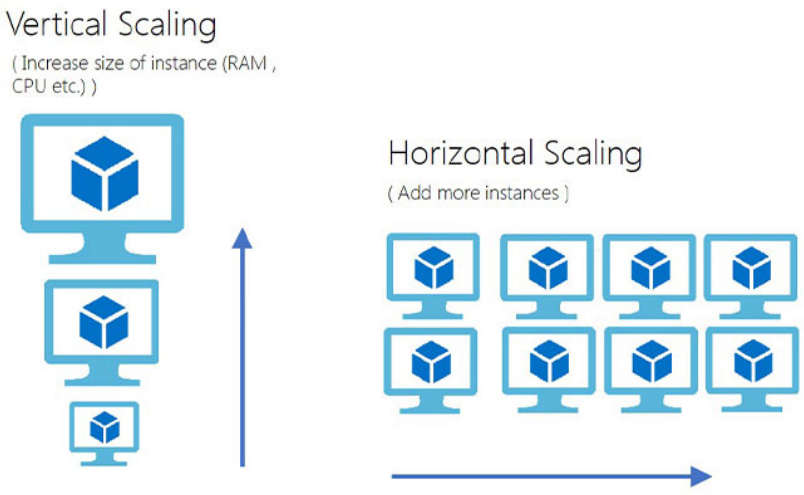
AZ-900 MS-Learn V1

- AZ-900 Sec 1.1
    - Describe the benefits of high-availability and scalability
        - High-availability
            - Available at all times
            - When architecting a solution, account for guarantees of uptime
            - Uptime is part of the SLA
                - SLA → Service License Agreement

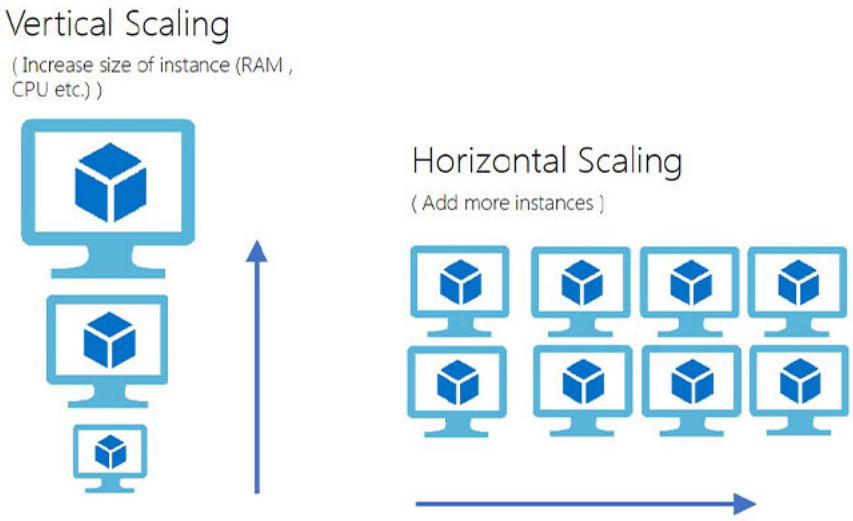
        - Scalability
            - One of the many benefits of cloud computing is scalability
                - Scalability → Ability to adjust resources on demand



- Vertical scaling
  - With vertical scaling, if you were developing an app and you needed more processing power, you could vertically scale up to add more CPUs or RAM to the virtual machine. Conversely, if you realized you had over-specified the needs, you could vertically scale down by lowering the CPU or RAM specifications.
    - Vertical Scaling → Increasing or decreasing the capabilities of existing resources



- Horizontal scaling
  - Horizontal scaling → Adding or subtracting the number of resources

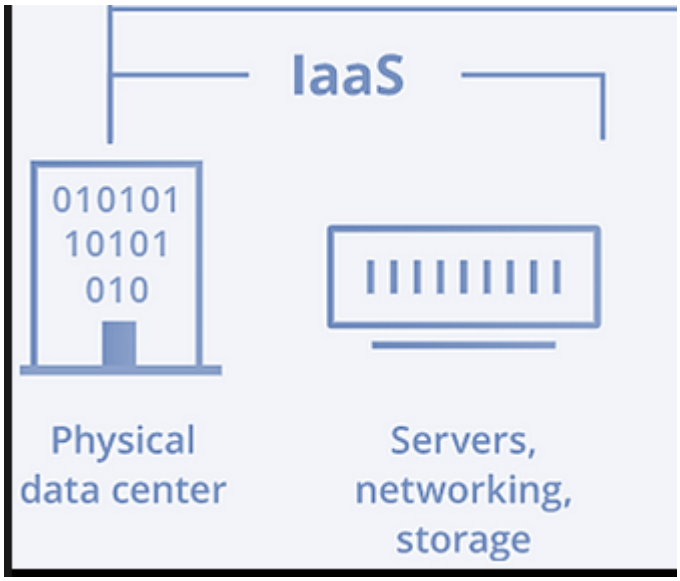


        - With horizontal scaling if you experience a steep jump in demand, you could add additional full virtual machines or containers

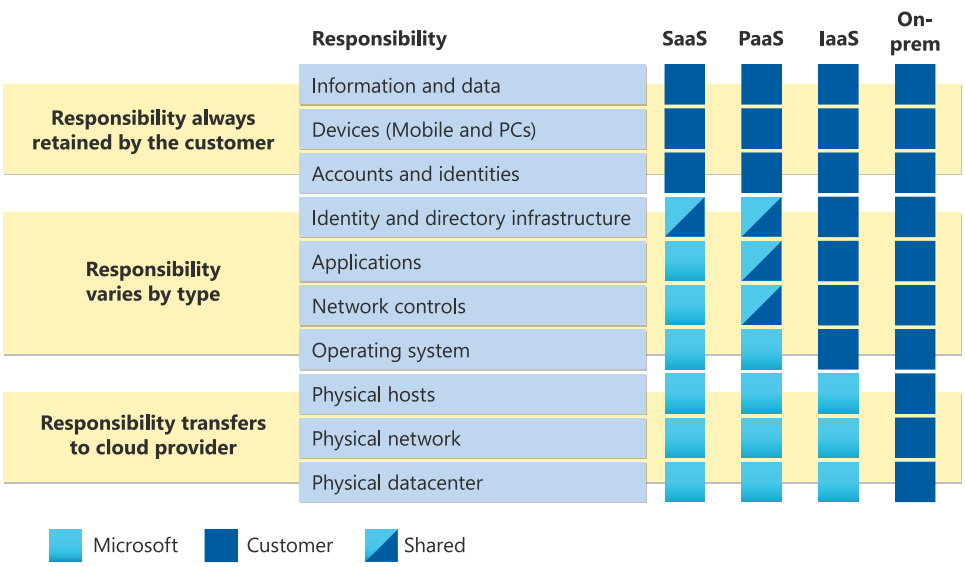
- AZ-900 Sec 1.2
    - Describe benefits of reliability and predictability
        - Predictability
            - Cost or performance predictability
        - Performance
            - Auto scaling
            - Load balancing
            - High availability
        - Reliability
            - Reliability → Ability to recover from failure and to continue to function
            - If a region globally has a failure, others will remain accessible
            - Can automatically shift with no action on your part
        - Cost
            - Prediction or forecasting of costs
            - Use cloud analytics tools and information to predict future costs and adjust as needed

        - Tools for estimation of spend
            - TCO → Total Cost of ownership
            - Azure Price Calculator → A tool to gain real-time cost estimates
- AZ-900 sec 1.3
    - Describe benefits of security and governance
        - Support of governance and Compliance
            - You manage OS an installed software, including patches and maintenance
            - Templates to meet corporate standards government regulatory requirements
            - Update to new standards as they change
        - Security
            - Maximum control provided by IaaS aka Physical resources
                - Well suited to hand DDOS and network attacks
- AZ-900 Sec 1.4
    - Describe the benefits of manageability in the cloud
        - Management of the cloud
            - Auto scale as needed
            - Deploy based on preconfigured templates, removing need for manual config
            - Monitor health of resources and automatically replace failing resources
            - Alerts for real time performance
        - Management in the cloud
            - Through a web portal for ease of management
            - Using a CLI → Command line interface
            - Using a API → Application Programming Interface
            - Using Powershell
- AZ-900 Sec 1.5

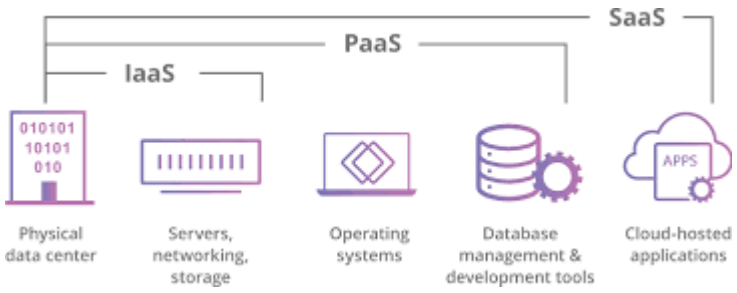
- Learning objectives
  - Describe infrastructure as a service - IaaS
    - Describe platform as a service - PaaS
    - Describe software as a service - SaaS
    - Identify appropriate use cases for each cloud service
  - Describe Infrastructure as a service
    - IaaS is the most flexible. Maximum control.
      - IaaS → Cloud computing where user is responsible for everything except the hardware



  - Shared responsibility model
    - Applies to all cloud types

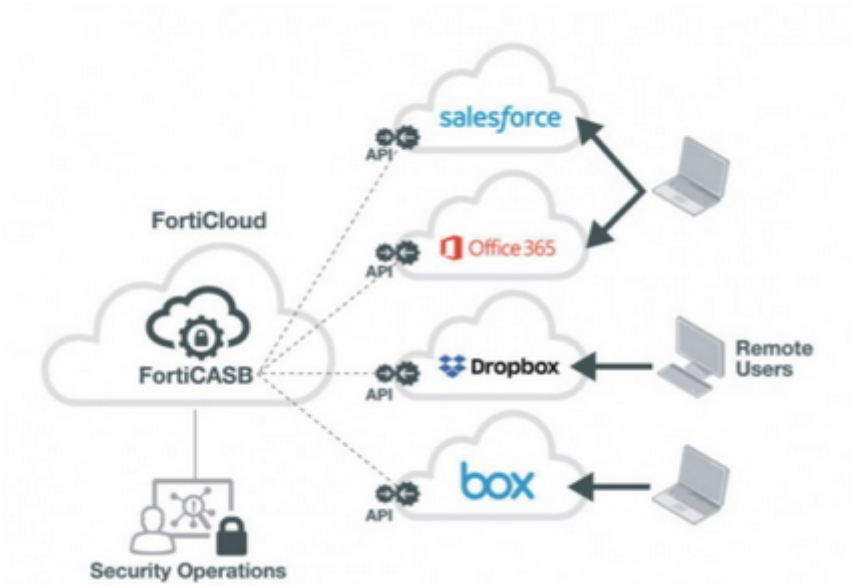


- Common IaaS scenarios
  - Lift and shift Migration → Copying on prem resources and moving to IaaS
  - Test and Development → Rapid replication of existing configurations and resources
- Describe Platform as a Service
  - Middle ground between (IaaS) and (SaaS)
  - PaaS → Cloud Provider maintains physical infrastructure, security and internet connection



    - Also maintains Operating System, Dev tools, Licensing and patches
  - Scenarios
    - Development framework

        - Scalability, high availability, multi-tenet, coding cost reduction
    - Analytics or business intelligence
        - Tools provided for analyzing, data mining, pattern prediction and investment returns
- Describe Software as a Service
    - Most complete service model
    - Renting / using fully developed
    - SaaS→Fully developed software/Infrastructure, maintained by cloud provider

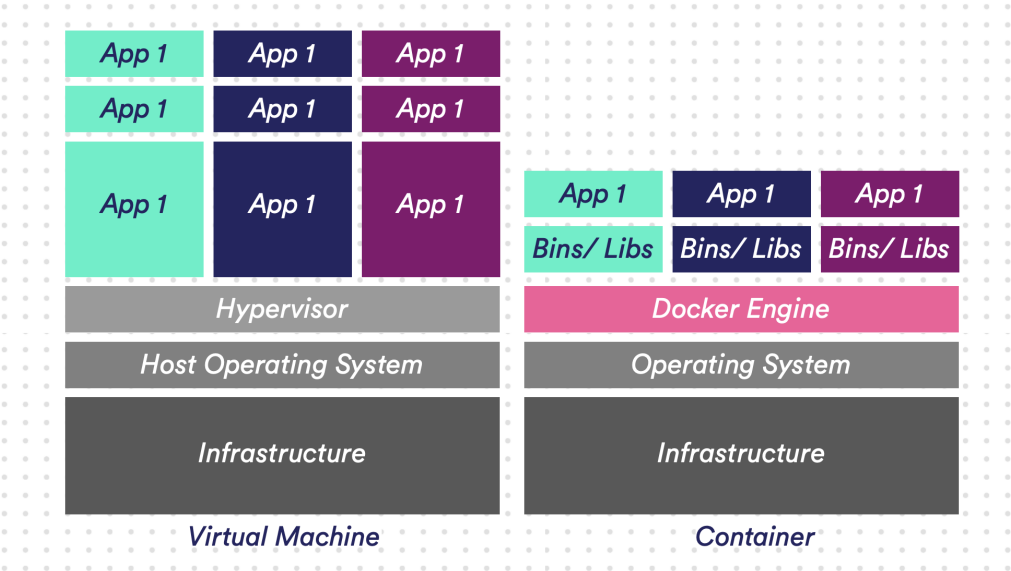


    - Examples : Dropbox, gmail, wordpress, office365, Salesforce
- Knowledge check
    - Which cloud service type is most suited to a lift and shift migration from an on-premises datacenter to a cloud deployment?
      →Infrastructure as a Service (IaaS)
    - A Finance and Expense tracking solution would typically be in?
      →Software as a Service (SaaS)

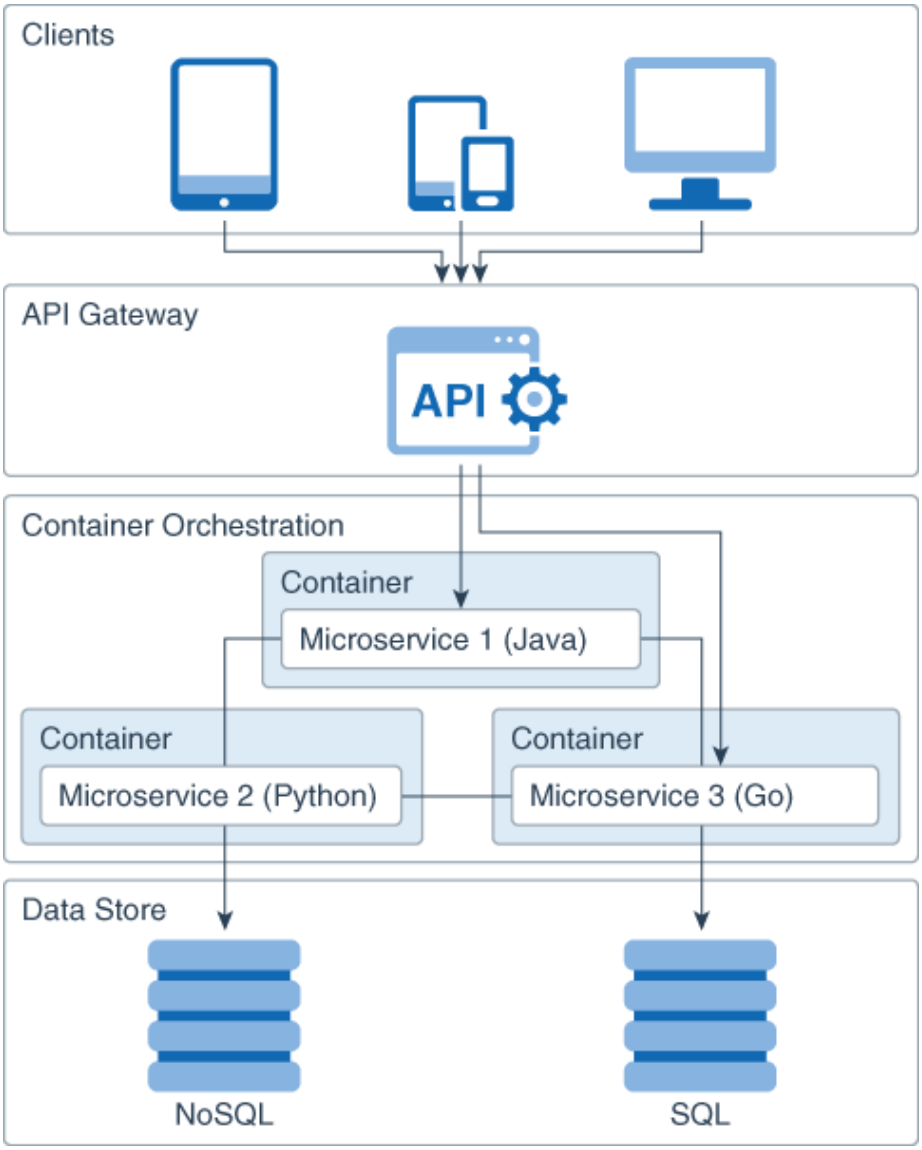
- AZ-900 Sec 1.6
    - Describe Azure compute and networking services

        - Learning objectives
            - Compare compute types, including container instances, virtual machines, and functions
            - Describe virtual machine (VM) options, including VMs, virtual machine scale sets, availability sets, Azure Virtual Desktop
            - Describe resources required for virtual machines
            - Describe application hosting options, including Azure Web Apps, containers, and virtual machines
            - Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, VPN Gateway, and ExpressRoute
            - Define public and private endpoints
    - Describe Azure Virtual Machines
        - Azure Virtual Machines = Creating VM's in the cloud
        - VM image→template that includes OS, software, and dev tools
        - Scale VMs in Azure
            - Can run single VM's for testing and dev or can group together for scaling, availability and redundancy
        - Virtual machine scale sets
            - VM Scale Set→Group of identical, load-balanced VM's
            - Can automatically scale up or down in response to demand
            - VM Scale sets can automatically deploy load balancing
        - Virtual machine availability sets
            - Designed to stagger updates to Vm's that have varied power and network connectivity, preventing lose of all VM's.
                - Update Domain→Can be rebooted at the same time
                - Fault Domain→Groups by common power source and network switch
            - No addition cost
        - Examples of when to use VMs

            - During testing and development
            - When running applications in the cloud
            - When extending on prem data center to cloud
            - During disaster recovery
                - Run critical apps in the cloud to keep business going, then shutdown when done
        - Move to the cloud with VMs
            - VM Resources
                - Size - cpu cores, ram
                - Storage
                - Networking
        - Exercise - Create an Azure Virtual Machine
            - Nginx → Linux based Web-server
    - Describe Azure Virtual Desktop
        - AVD → Azure Virtual Desktop - a cloud hosted full windows desktop environment
        - RBAC → Role based access controls
    - Describe Azure Containers
        - Containers → Standard unit of software that bundles code and its dependencies to a application runs from one computing environment to another



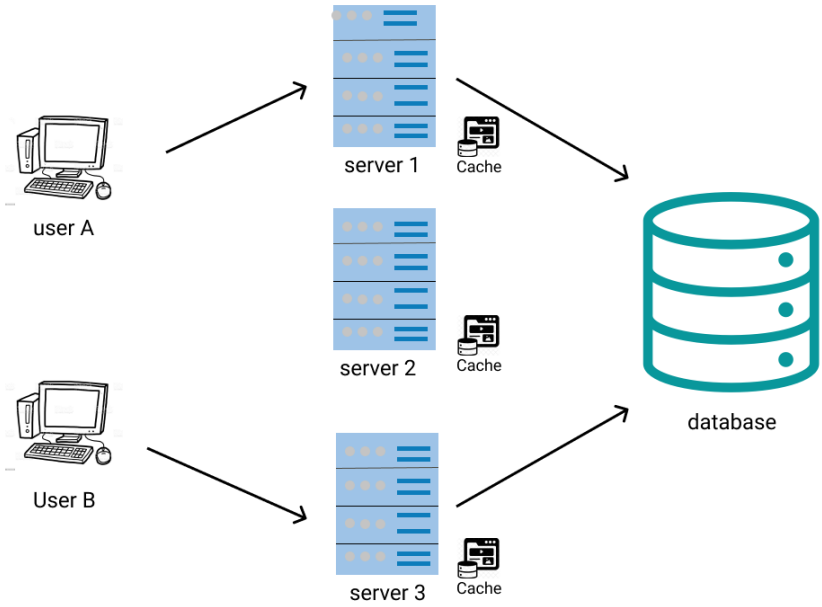
- Azure containers are a PaaS
- Use containers in your solutions
  - Often used to create solution by using microservice architecture
    - Microservice architecture → Application architecture where the application is developed as a collection of services



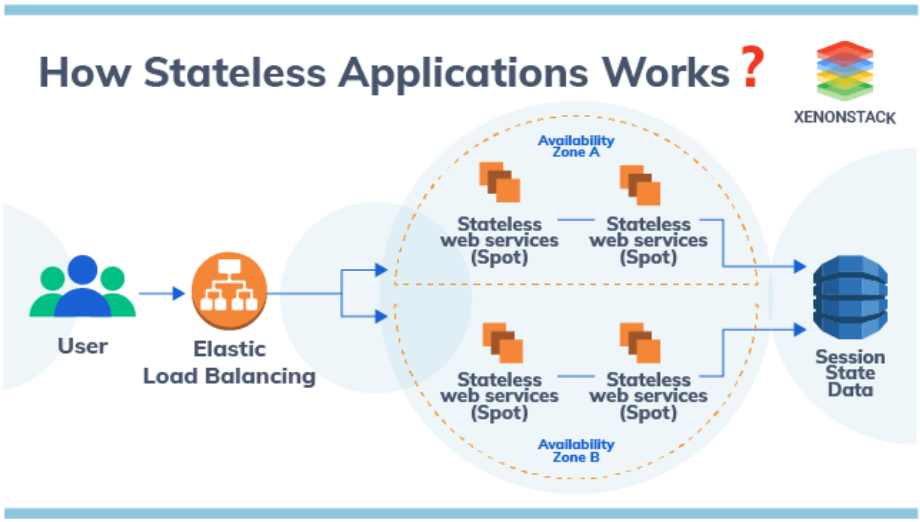
        - Breaking solutions into smaller, independent pieces
    - Separate app into sections that can be scaled, maintained or updated independently
    - If web front end is ok, but back end is overloaded, the back end can be scaled independently with out disruption or added cost in relation to the front end
    - Modular scaling
    -
- Describe Azure Functions
    - Event driven, serverless compute. No maintenance of VM or Containers

- Serverless → Allows developers to build and run applications without having to manage servers
- Payment model for only what you use

- Benefits of Azure Functions
  - Ideal when only concerned about the code running, not the underlying platform and infrastructure
  - Azure Functions scale automatically bases on demand
  - Azure Functions can be either stateless **or** stateful (Stateless is default)
    - Stateful → Application program that keep track of the state of interaction



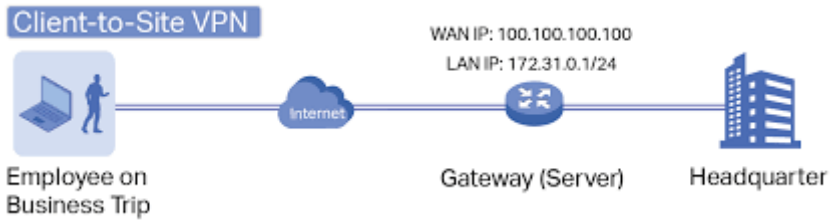
    - Stateless → A application program that does not save client data



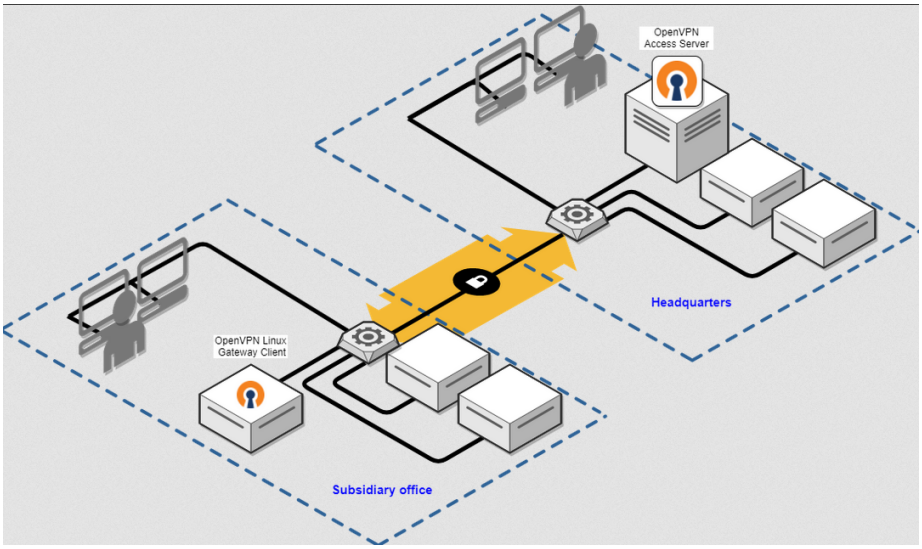
- Runs when triggered, de-allocates when function is finished

- Describe application hosting options
  - VM - Virtual machines
  - Containers
  - Azure App Service
    - Build and host in the language of your choice with out managing infrastructure
    - Automatic scaling
    - Windows and linux
    - Enables automated deployments from any Git repo supporting continuous deployment models : Gibuth/Azure DevOps/Etc
    - Focus on your app, not the environment and infrastructure
    - Supports multiple coding languages
      - .net, .net core, java, node.js, php, python. Windows and Linux
  - Types of app services
    - Web apps→Application stored on a remote server and delivered via internet
    - API apps→
    - WebJobs→Run a program or script in same instance as web app/api app or mobile app

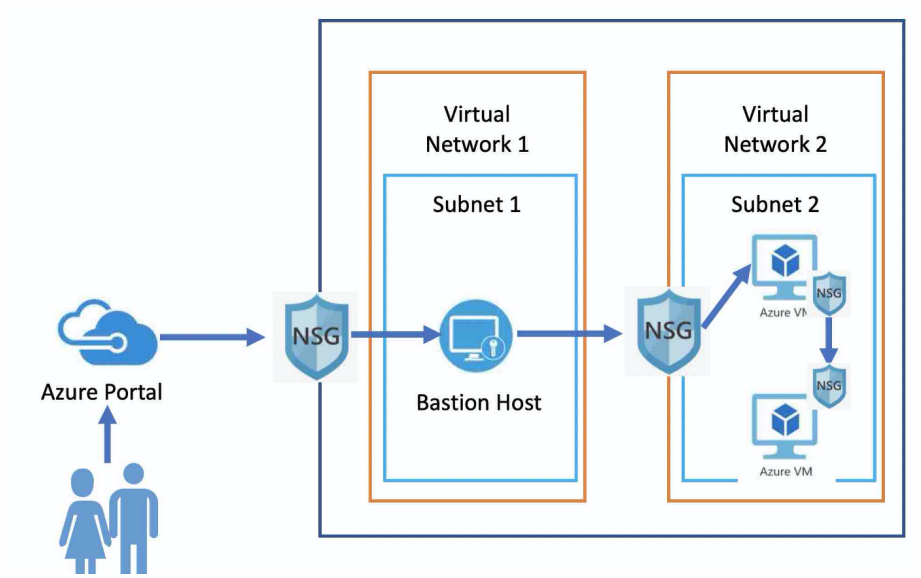
        - Mobile apps
    - Describe Azure Virtual Networking
        - Supports both public and private endpoints
        - Endpoint → **Remote computing device that communicates back and forth with a network to which it is connected**
        - Isolation and segmentation
            - Azure virtual network allows multiple Vlans
            - Built in DNS
            - Can also use external or internal name services
        - Communicate with on prem resources
            - Link cloud and on prem
            - Create a network that spans cloud and on prem
            - VPN's
                - Point to Point VPN → Typically 1 client connection to a central enterprise network



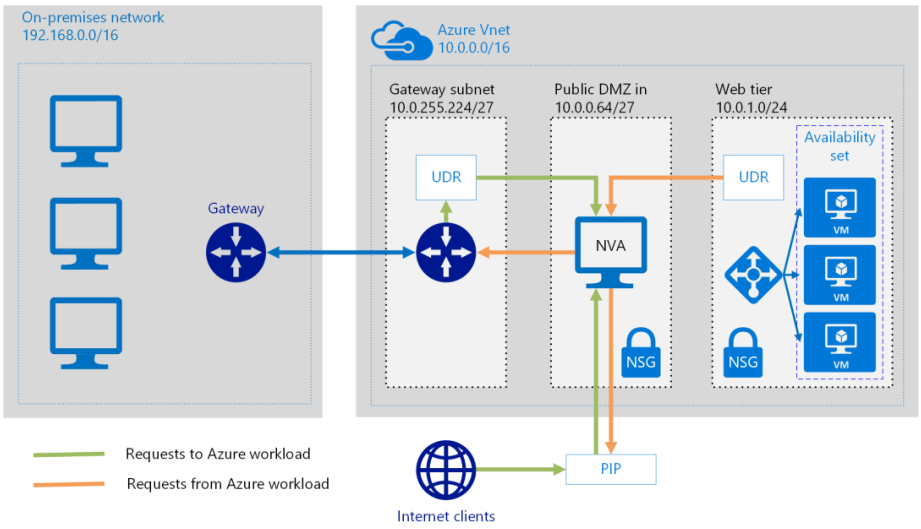
                - Site to site VPN → Encrypted always on private network



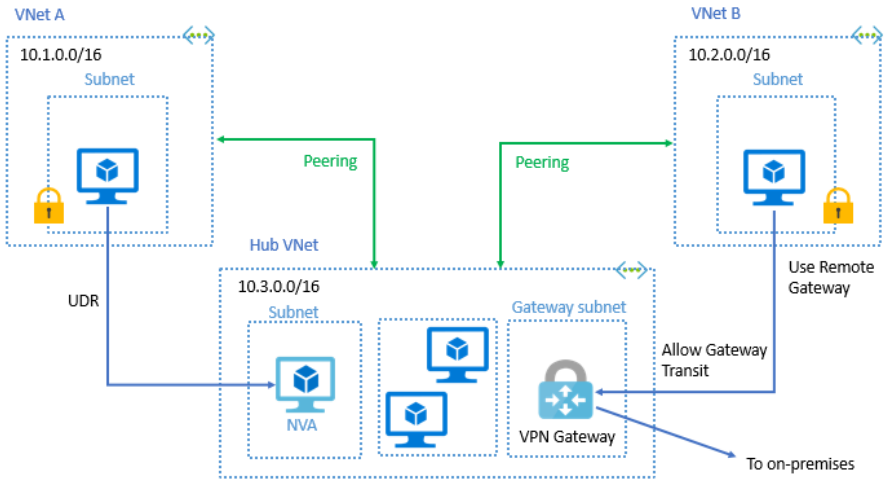
- Filter Network Traffic
  - Network security groups → Contains inbound and outbound rules to block or allow traffic



  - Network virtual appliances → Such as a virtual firewall



- Connect virtual networks
  - Virtual networking peering → Connecting 2 or more Azure virtual networks

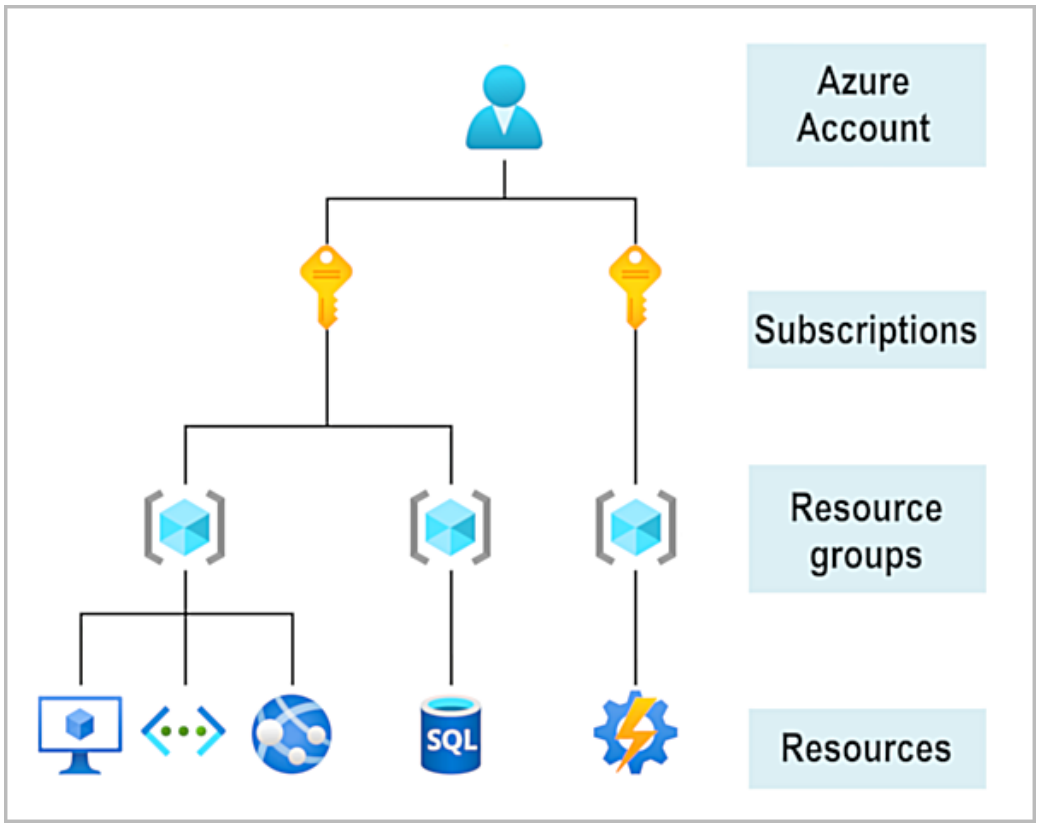


- UDR → User defined routes
  - Over riding the default azure routing to configure a custom networking path

- AZ-900 Sec 1.7
  - Sec 1.7 A - What is Azure ?
    - IaaS

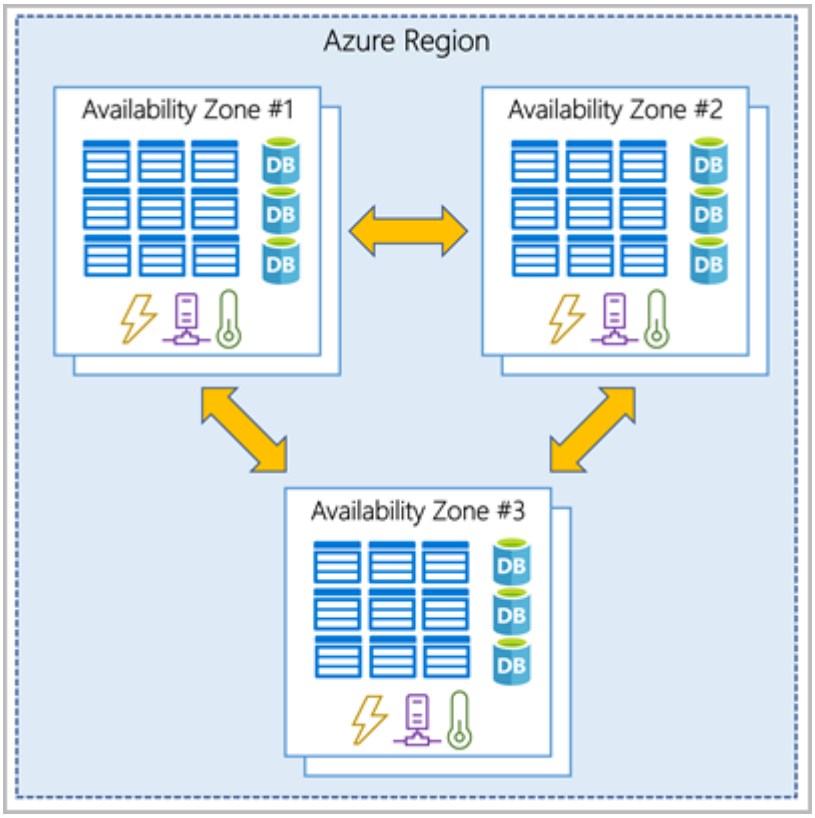
- PaaS
- SaaS
    - VM's in the cloud
    - Website and database hosting
    - AI
    - IoT
    - Machine Learning
    - Cloud based storage

- Sec 1.7 B - Get started with Azure accounts
    - Subscription based account model

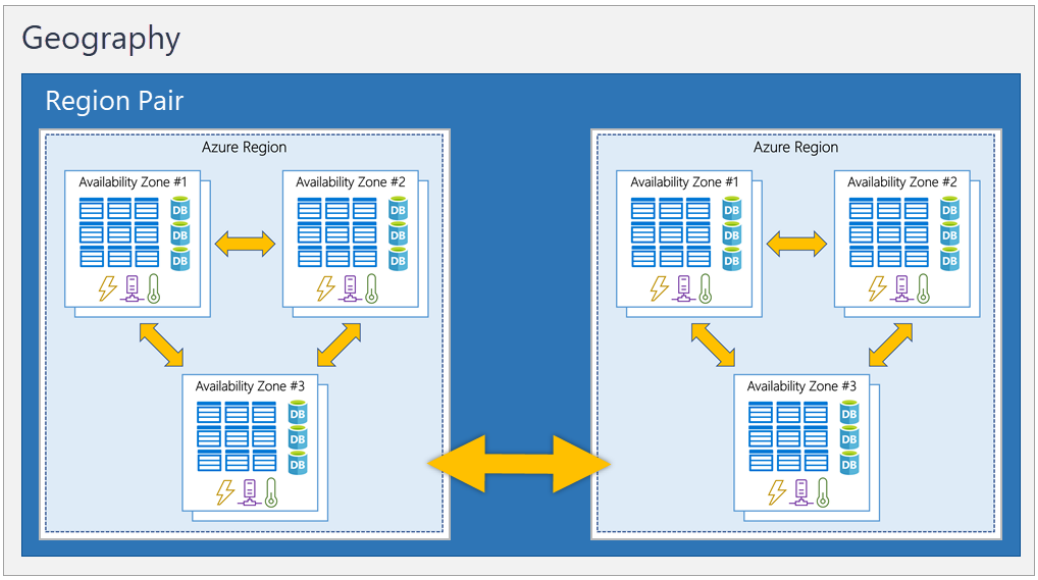


    -
    - Describe Azure physical
        - Azure global infrastructure experience
            - Virtual tour of the infrastructure

-
- Regions
  - Geographical location
  - Some features are only available in some regions
    - Azure active directory
    - Azure Traffic Manager and Azure DNS
- Availability Zones
  - Mainly for VM, managed disks, load balancers and SQL databases
  - Physically separate data centers with in a azure region



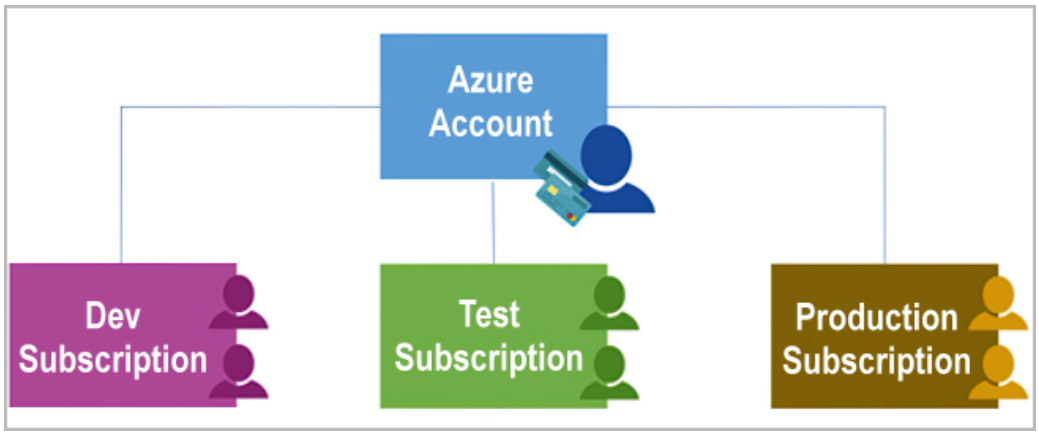
    - Independent power, cooling and networking
    - Minimum of 3 availability zones in a region, where supported
  -
- Use availability zone in your apps
  - Redundancy

        - Scalability
        -
    - Geography
    - 

    - Additional advantages of region pairs
        - Back up in case of outage
        - Updates rolled out to regions in case of failure, issues are isolated
        - Data is region specific for taxes and law enforcement
    - Sovereign Regions
        - Isolated from main azure instance
            - Used for compliance or legal reasons
        -
- AZ-900 Sec 1.8
    - Describe Azure management infrastructure
    - Azure resources and resource groups
        - Anything you create, provision, deploy

- Resources can only be in one group at a time
- Simply put, grouping of resources
- Cant be nested
- Resources can be moved between groups, just not in more then one

- Azure subscriptions



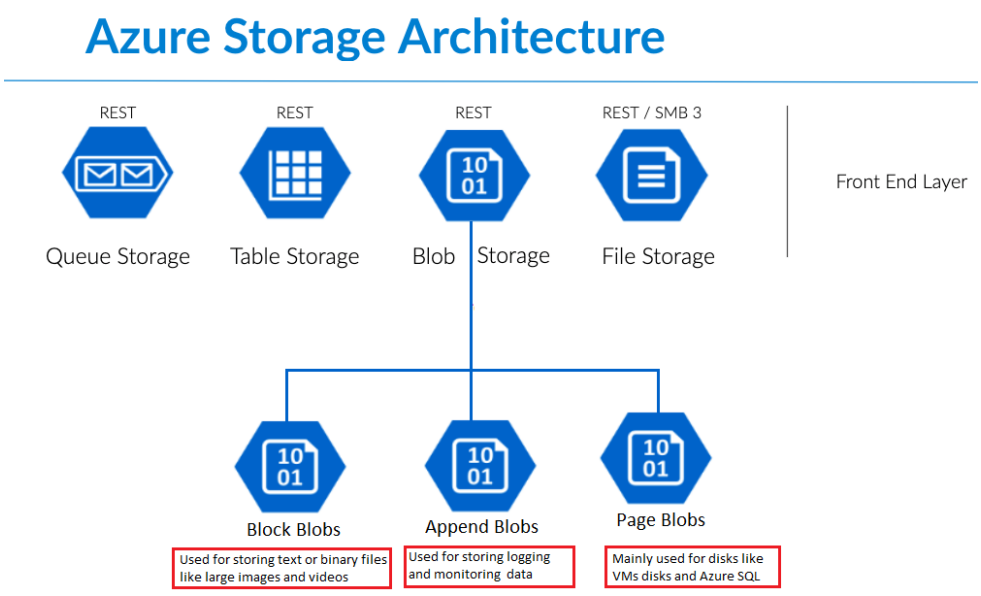
  - A unit of management, billing and scale
  - organize resource groups for easy billing
- Billing boundary
  - How the account is billed
- Access control boundary
  - Access policy defined subscription

- Create additional Azure subscriptions

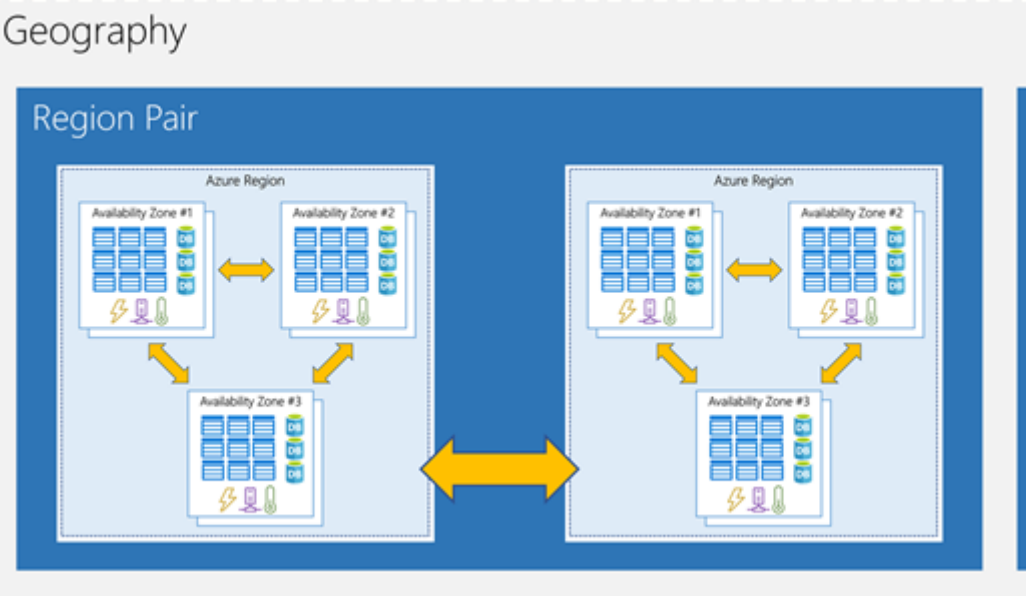
        - **Environments**
            - Development and testing, security, or to isolate data for compliance reasons.
        - **Organizational structures**
            - Reflect different organizational structures. For example, limit one team to lower-cost resources, while allowing the IT department a full range.
        - **Billing**
            - One subscription for production workloads, another for development and testing
    - Azure management groups
        - Example: Multiple applications, multiple development teams, in multiple geographies.
        - Organize subscriptions into containers called management groups and apply governance conditions
    - Management group, subscriptions, and resource group hierarchy
        - Example of a hierarchy for governance
    - Knowledge check
        - How many resource groups can a resource be in at the same time?↓
            - One : A resource can only be in one group at a time.
        - What happens to the resources within a resource group when an action or setting at the Resource Group level is applied?↓
            - The setting is applied to current and future resources.
        - What Azure feature replicates resources across regions that are at least 300 miles away from each other?→Region pairs : Most Azure regions are paired with another region at least 300 miles away.
    -
- AZ-900 Sec 1.9
    - Describe Azure storage accounts
        - Redundancy options

- **Locally redundant storage → (LRS)**
  - Replicates your storage account three times within a single data center in the primary region
- **Geo-redundant storage → (GRS)**
  - Copies your data synchronously three times within a single physical location in the primary region using LRS
- **Read-access geo-redundant storage → (RA-GRS)**
  - Allows data to be read from both Azure regions. Object Replication for Block Blob Storage
- **Zone-redundant storage → (ZRS)**
  - Synchronous replication of data across the zones in a region
- **Geo-zone-redundant storage → (GZRS)**
  - Copies your data synchronously across three Azure availability zones in the primary region using ZRS
- **Read-access geo-zone-redundant storage → (RA-GZRS)**
  - Copies your data synchronously across three Azure availability zones in the primary region using ZRS

- Storage account endpoints



- **Azure Region Pairs** → Azure Regions within the same geographic region for recovery purposes



- RPO → Recovery Point Object
  - Interval between the most recent writes to the primary region and the last write to the secondary region. The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes

◦ Describe Azure storage services

- Storage platform Definitions
  - **Azure Blobs** → A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
  - **Azure Files** → Managed file shares for cloud or on-premises deployments.
  - **Azure Queues** → A messaging store for reliable messaging between application components.
  - **Azure Disks** → Block-level storage volumes for Azure VMs.
- Blob storage tiers
  - **Hot access tier** → Optimized for storing data that is accessed frequently (for example, images for your website).

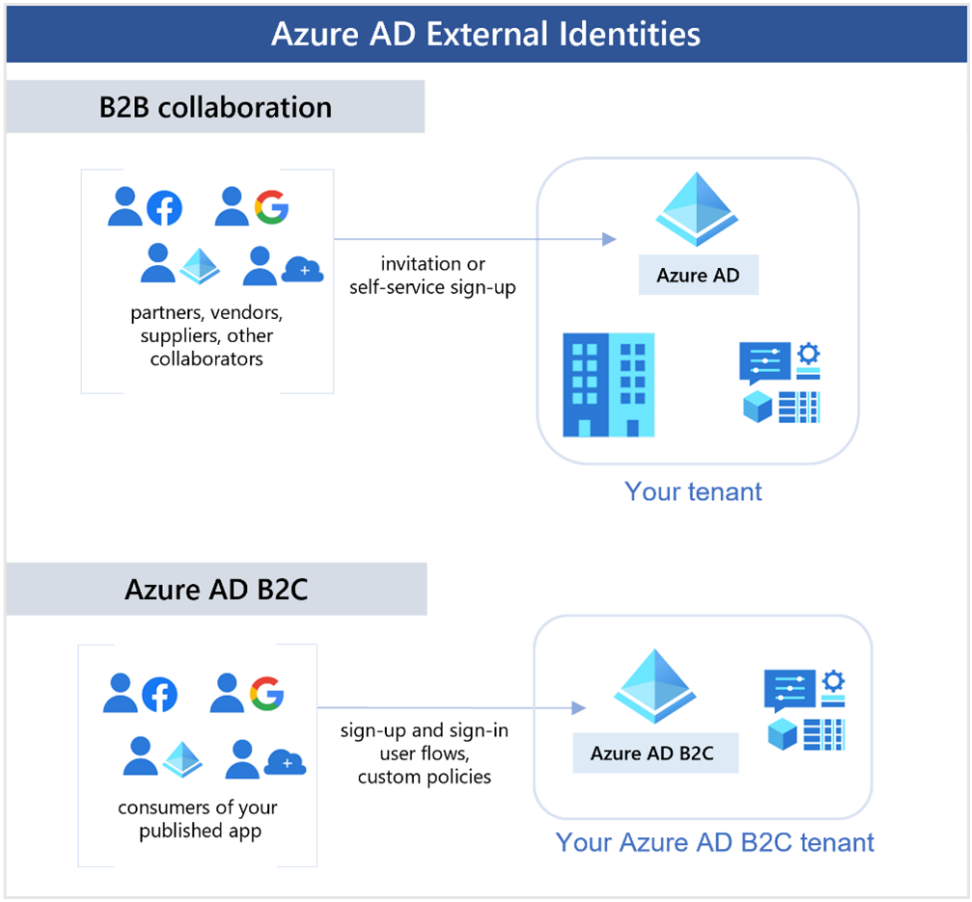
        - **Cool access tier** → Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
        - **Archive access tier** → Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).
    - Azure Files
        - Accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols
    - Queue storage
        - Azure Queue Storage → Commonly used to create a backlog of work to process asynchronously
    - Disk Storage
        - Azure managed disks → Block-level storage volumes managed by Azure for use with Azure VMs
- Identify Azure data migration options
    - **Azure Migrate** → A service that helps you migrate from an on-premises environment to the cloud
        - **Azure Migrate : Discovery and assessment** → Discover and assess on-premises servers running on VMware, Hyper-V, and physical servers in preparation for migration to Azure.
        - **Azure Migrate: Server Migration** → Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
        - **Data Migration Assistant** → Data Migration Assistant is a stand-alone tool to assess SQL Servers. It helps pinpoint potential problems blocking migration. It identifies unsupported features, new features that can benefit you after migration, and the right path for database migration.
        - **Azure Database Migration Service** → Migrate on-premises databases to Azure
        - **Web app migration assistant** → Azure App Service Migration Assistant is a standalone tool to assess on-premises websites for

migration to Azure App Service. Use Migration Assistant to migrate .NET and PHP web apps to Azure.

- **Azure Data Box** → Use Azure Data Box products to move large amounts of offline data to Azure.

- Identify Azure file movement options
  - AzCopy → A command-line utility that you can use to copy blobs or files to or from your storage account
  - Azure Storage Explorer → a standalone app that provides a graphical interface to manage files and blobs
  - Azure File Sync → a tool that lets you centralize your file shares in Azure Files

- AZ-900 Sec 2.0
  - New terms
    - FIDO (Fast IDentity Online) → the latest standard that incorporates the web authentication (WebAuthn)
    - WebAuthn → an API built into browsers that communicates authentication information from an authenticator to a web application.
  - Describe Azure external identities
    - External identity → person, device, service, etc. that is outside your organization

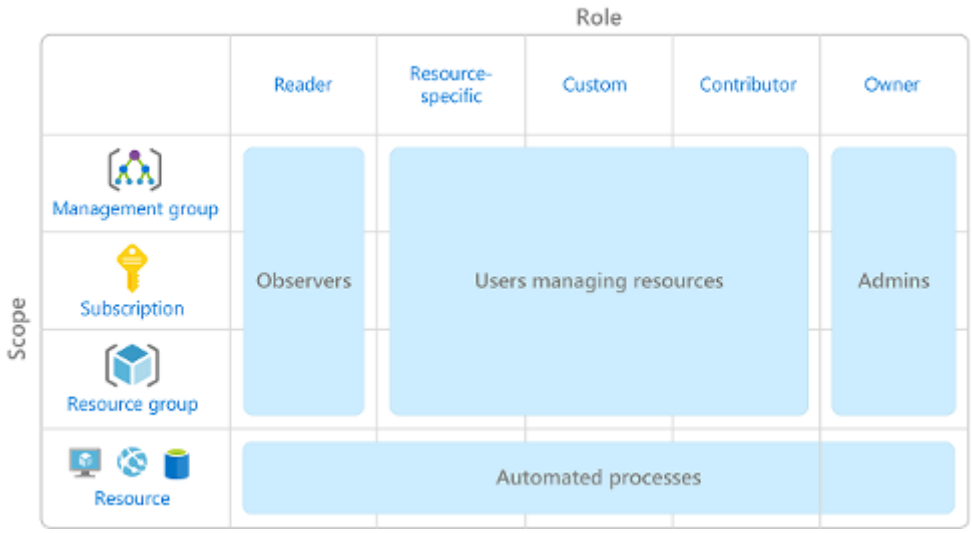
- 

  - **Business to business (B2B) collaboration** → Collaboration with external users by letting them use their preferred identity to sign-in. represented typically as guest users.
  - **B2B direct connect** → two-way trust with another Azure AD organization. Example : Teams Shared Channels
  - **Azure AD business to customer (B2C)** → Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.
  -
  -
  - Describe Azure conditional access
    - Conditional Access
      - Empower users to be productive where ever they are, when ever they want
      - Protect the organizations assets

- More Granular MFA
- Secondary authentication challenges, based on log in request.
  - If location is unknown, device is unknown, etc, secondary challenges may be employed

- When is conditional access useful ?
  - MFA to access an application based in role, location or network
  - Require access to services through approved client applications
  - Require users to access application from a managed device
  - Block access from untrusted sources

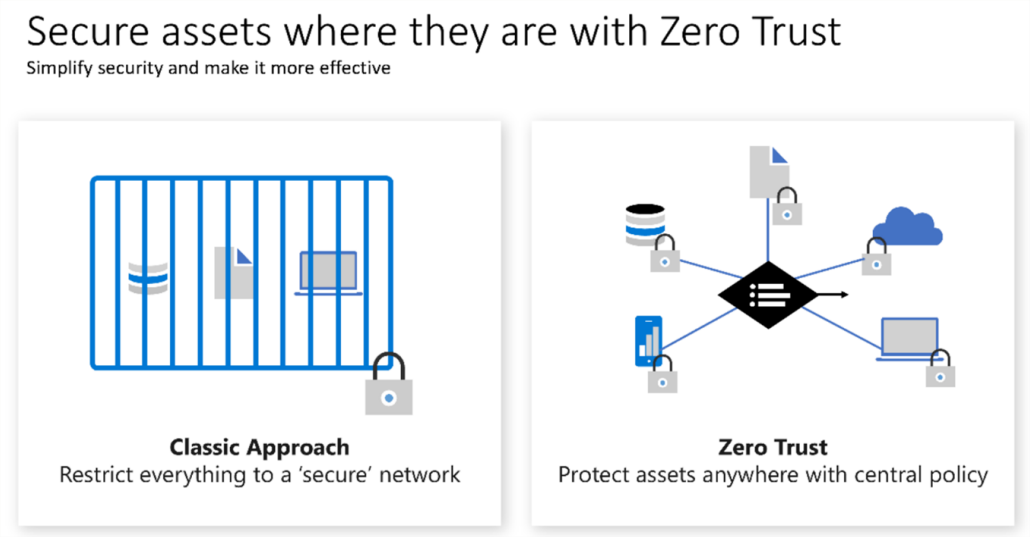
- Describe Azure role-based access control
  - Built in roles as well as the ability to create custom roles



  - Scopes
    - A management group (a collection of multiple subscriptions).

- A single subscription.
- A resource group.
- A single resource.

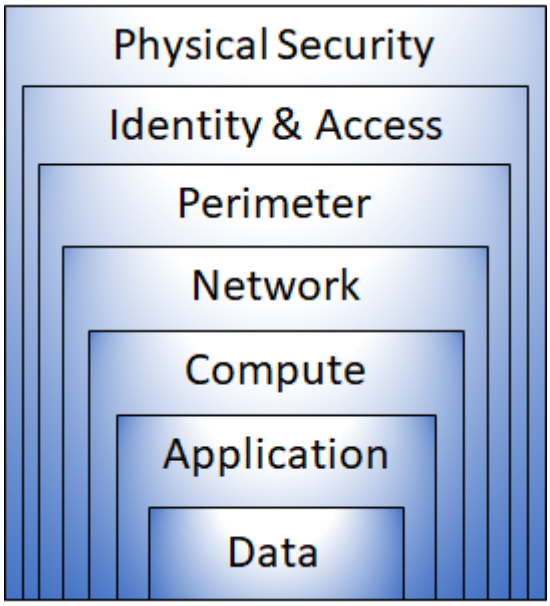
- Definitions
  - **Principle of least privilege** →a subject should be given only those privileges needed for it to complete its task
  - Blob→binary large object - stores any kind of binary data in random-access chunks
  - Azure RBAC→Azure role-based access control

- Describe zero trust model
  - **Verify explicitly** - Always authenticate and authorize based on all available data points.
  - **Use least privilege access** - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
  - **Assume breach** - Minimize blast radius and segment access. Verify end-to-end encryption. Use analytics to get visibility, drive threat detection, and improve defenses.
  - 

  - Definitions

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

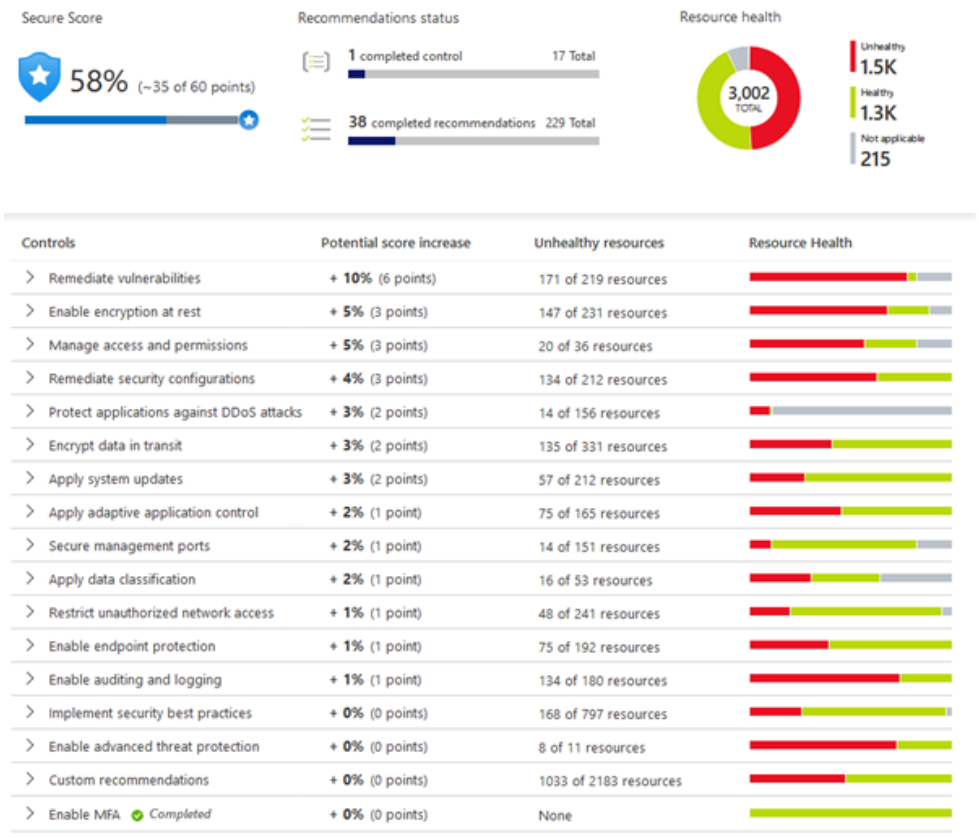
    - Describe defense-in-depth
        - Defense-in-depth → Strategy that leverages multiple security measures to protect an organization's assets
        - Layers of defense - in-depth



        - Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure
        - Overview of the role of each layer
            - The physical security layer is the first line of defense to protect computing hardware in the datacenter.
            - The identity and access layer controls access to infrastructure and change control.
            - The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
            - The network layer limits communication between resources through segmentation and access controls.
            - The compute layer secures access to virtual machines.

        - The application layer helps ensure that applications are secure and free of security vulnerabilities.
        - The data layer controls access to business and customer data that you need to protect.
    - Describe Microsoft Defender for Cloud
        - Defender for Cloud → a monitoring tool for security posture management and threat protection
        - Monitors cloud, hybrid, on-prem and multi cloud
        - Can defend other cloud resources like AWS
    - Assess, Secure, and Defend
        - Continuously assess – Know your security posture. Identify and track vulnerabilities.
        - Secure – Harden resources and services with Azure Security Benchmark.
        - Defend – Detect and resolve threats to resources, workloads, and services.
        - 

        - Azure Security Benchmark > Microsofts cloud version of Nessus essentially



- Knowledge check
  - Which Azure Active Directory tool can vary the credentials needed to log in based on signals, such as where the user is located?
    - Conditional Access
    - Passwordless
    - Guest access
  - Which security model assumes the worst-case security scenario, and protects resources accordingly?
    - Zero trust
    - Defense-in-depth
    - Role-based access control
  - A user is simultaneously assigned multiple roles that use role-based access control. What are their actual permissions? The role permissions are: Role 1 - read || Role 2 - write || Role 3 - read and write.
    - Read only

        - Read and write
        - Write only
- AZ-900 Sec 2.1
    -
    - Describe Azure management and governance
        - Simplify, automate, and optimize the management and compliance of your cloud resources
    - Describe factors that can affect costs in Azure
        - Resource type
            - When you provision an Azure resource, Azure creates metered instances for that resource. The meters track the resources' usage and generate a usage record that is used to calculate your bill.
        - Consumption
            - If you use more compute this cycle, you pay more
        - Maintenance
            - By keeping an eye on your resources and making sure you’re not keeping around resources that are no longer needed, you can help control cloud costs.
        - Geography
            - cost of power, labor, taxes, and fees vary depending on the location
        - Network Traffic
        - Subscription type
    - Compare the Pricing and Total Cost of Ownership calculators
        - Pricing calculator
        - TCO calculator
    - Describe the Azure Cost Management tool
        - Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

        - Cost alerts
            - Budget alerts
            - Cost analysis is a subset of Cost Management
            - Department spending quota alerts.
        - Credit alerts
            - notify you when your Azure credit monetary commitments are consumed
        - Budget Alerts
            - Notify you when spending, based on usage or cost, reaches or exceeds the amount defined
        - Department spending quota alerts
            - notify you when department spending reaches a fixed threshold of the quota
        - Budgets
- Describe the purpose of tags
    - Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources.
    - **Resource management**
    - **Cost management and optimization**
    - **Operations management**
    - **Security**
    - **Workload optimization and automation**
- Describe features and tools in Azure for governance and compliance
    - Learning objectives
        - Describe the purpose of Azure Blueprints
            - Lets you standardize the cloud subscription/Environment
            - Artifacts→Components in the Azure Blueprint
                - Role assignments
                - Policy assignments

        - Azure Resource Manager templates
        - Resource groups
    - Describe the purpose of Azure Policy
        - enables you to create, assign, and manage policies that control or audit your resources
    - Describe the purpose of resource locks
        - prevents resources from being accidentally deleted or changed
    - Describe the purpose of the Service Trust portal
    - How many parameters does a azure blueprint artifact need to be valid ? →0
    - How can you prevent none-compliant resources from being created without having to manually evaluate each resource as its created ? →Azure Policy
    - Review
        - Azure Blueprints→a package or container of standards, patterns
        - Azure Policy→**Enforce and control the properties of a resource**
- Describe features and tools for managing and deploying Azure resources
    - Learning objectives
        - Describe Azure portal
        - Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell
        - Describe the purpose of Azure Arc
        - Describe Azure Resource Manager (ARM) and Azure ARM templates
- Describe the purpose of Azure Arc
    - ARM→Azure Resource Manager
        - Used to interact with azure- cli, portal, etc
    - Arc→Extends Azure control plane to other services.
    -

- Knowledge Checks