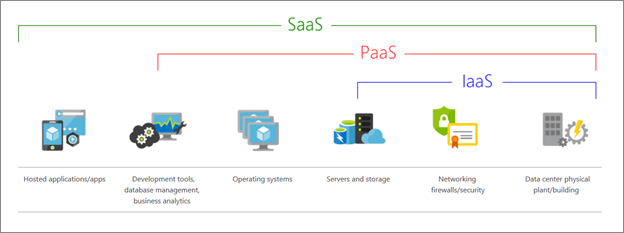
**PART 1**

**Learning Objectives: Cloud Concept**

* Describe cloud computing and the shared responsibility model.
* Define cloud models, including public, private, and hybrid.
* Identify appropriate use cases for each cloud model.
* Describe the consumption-based model.
* Compare cloud pricing models.

Cloud service model (Differences between categories of cloud services)



Shared Responsibilities for each cloud service model

A screen shot of a computer

Description automatically generated

Customer always responsible for – Information & Data, Devices, User accounts & Identities

Microsoft always responsible for – Physical hosts, Physical network & Physical datacenters

Shared depending on cloud model – Apps, Network control, OS, Identity & Directory infrastructure

In SaaS mostly Microsoft take care, but IaaS mostly customers responsible. In PaaS, only provision of OS is taken care of Microsoft, and the rest are shared.

Public, Private & Hybrid cloud (describe differences between types of cloud computing)

Timeline

Description automatically generated

A screenshot of a computer program

Description automatically generated

Multi-cloud: deal with two (or more) public cloud providers and manage resources and security in both environments.

**Azure Arc** - can help manage your cloud environment, whether it's a public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration, or even a multi-cloud environment running on multiple cloud providers at once.

**Learning Objectives: Describe the benefits of using cloud services**

* Describe the benefits of high availability and scalability in the cloud.
* Describe the benefits of reliability and predictability in the cloud.
* Describe the benefits of security and governance in the cloud.
* Describe the benefits of manageability in the cloud.

**High availability** - focuses on ensuring maximum availability, regardless of disruptions or events that may occur.

**Scalability** - refers to the ability to adjust resources to meet demand.

Vertical Scaling - to add more CPUs or RAM to the virtual machine

Horizontal Scaling - add additional virtual machines or containers, scaling out.

**Reliability** - the ability of a system to recover from failures and continue to function.

**Predictability** - can be focused on performance predictability or cost predictability

Performance predictability - focuses on predicting the resources needed to deliver a positive experience for your customers. Autoscaling, load balancing, and high availability are just some of the cloud concepts that support performance predictability.

Cost predictability - using cloud analytics and information, you can predict future costs and adjust your resources as needed.

Security and Governance in the cloud

Set templates help ensure that all your deployed resources meet corporate standards and government regulatory requirements. Cloud-based auditing helps flag any resource that’s out of compliance with your corporate standards and provides mitigation strategies.

For maximum control – go for IaaS, or for automatically applying patches, go for either PaaS or SaaS.

The Manageability in the cloud

Two concepts: Management of the cloud and Management in the cloud.

**Management of the cloud** – autoscaling, use of preconfigured template, monitoring health and automatically replace failing resources, real-time performance metrics

**Management in the cloud** – how cloud resources can be managed using APIs, web portal, CLI or PowerShell.

**Learning Objectives: Describe cloud service types**

* 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 (IaaS, PaaS, SaaS).

Infrastructure as a Service (IaaS) - the most flexible category of cloud services, as it provides you with the maximum amount of control for your cloud resources.

Scenarios to use IaaS:

1. Lift and shift migration – setting up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.
2. Testing and development – already established configurations for development and test environments that you need to rapidly replicate.

Platform as a Service (PaaS) - a middle ground between renting space in a datacenter (IaaS) and paying for a complete and deployed solution (SaaS). In a PaaS scenario, you don't have to worry about the *licensing or patching* for operating systems and databases.

Scenarios to use PaaS:

1. Development framework - PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
2. Analytics or BI - Tools provided as a service with PaaS allow organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.

Software as a Service (SaaS) - the most complete cloud service model from a product perspective. While the SaaS model may be the least flexible, it’s also the easiest to get up and running.

Scenarios to use SaaS:

1. Email and messaging.
2. Business productivity applications.
3. Finance and expense tracking.

**PART 2**

**Learning Objectives: Core architectural components of Azure**

* Describe Azure regions, region pairs, and sovereign regions.
* Describe Availability Zones.
* Describe Azure data centres.
* Describe Azure resources and Resource Groups.
* Describe subscriptions.
* Describe management groups.
* Describe the hierarchy of resource groups, subscriptions, and management groups.

Azure core architecture can be broken down into two components:

1. Physical Infrastructure
2. Management Infrastructure

Physical Infrastructure

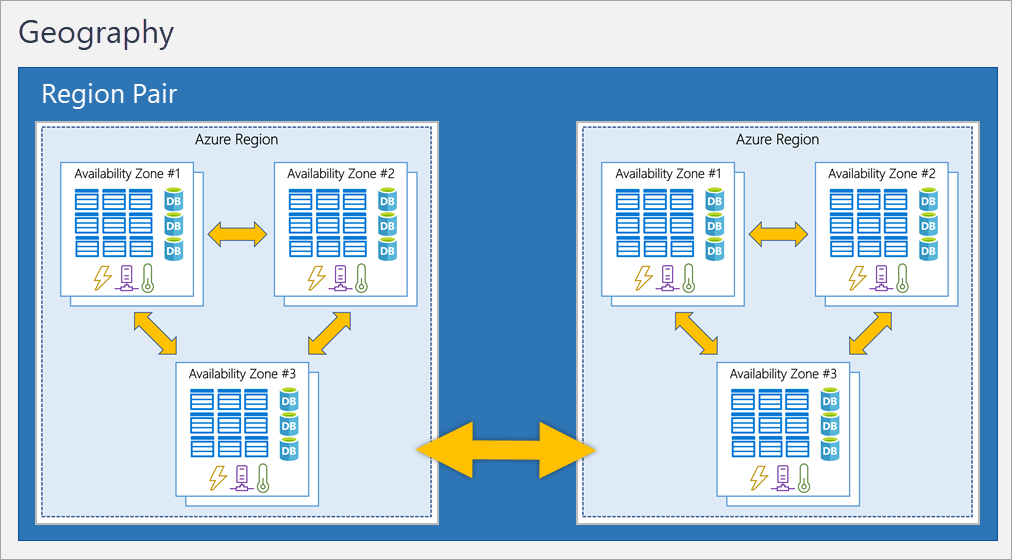
This includes Regions, Availability Zones, Region Pairs & Sovereign Regions.

Regions - a geographical area on the planet that contains at least one, but potentially multiple datacenters that are nearby and networked together with a low-latency network.

Availability Zones - physically separate datacenters within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support availability zones fall into three categories:

* Zonal services: You pin the resource to a specific zone (for example, VMs, managed disks, IP addresses).
* Zone-redundant services: The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).
* Non-regional services: Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

Region Pairs - regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away.



Advantages of Region Pairs

* If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly as possible for applications hosted in that region pair.
* Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
* Data continues to reside within the same geography as its pair (except for Brazil South) for tax- and law-enforcement jurisdiction purposes.

Sovereign Regions - instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes. E.g., US Government, Ch

Management Infrastructure

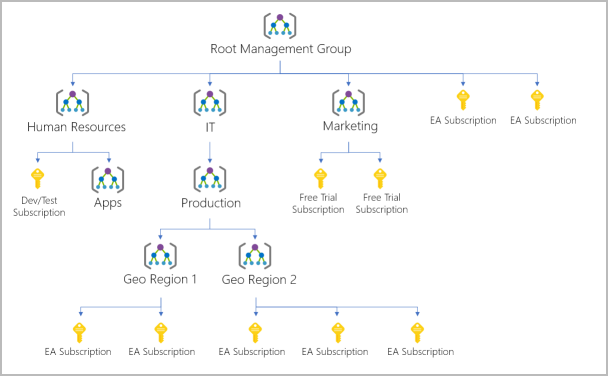
This includes Azure resources and resource groups, subscriptions, and accounts.

Resources - (VMs), virtual networks, databases, cognitive services, etc.

Resource Groups – resources are put into a resource group. A resource group can contain many resources, a single resource can only be in one resource group at a time.

Azure subscription - one Microsoft account can have multiple Azure subscriptions. If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. In a multi-subscription account, you can use the subscriptions to configure different billing models and apply different access-management policies.  Resources are gathered into resource groups, and resource groups are gathered into subscriptions.

Azure management groups - provide a governance scope above subscriptions. You organize subscriptions into management groups; the governance conditions you apply cascade by inheritance to all associated subscriptions.



Important facts about management groups:

* 10,000 management groups can be supported in a single directory.
* A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
* Each management group and subscription can support only one parent.

Use management groups if you need to:

1. Create a hierarchy that applies a policy - policy will inherit onto all the subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions.
2. **Provide user access to multiple subscriptions** - One assignment on the management group can enable users to have access to everything under that management group

**Learning Objectives: Compute and Networking Services**

* Compare compute types, including containers, virtual machines, and functions
* Describe virtual machine options, including Azure virtual machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop
* Describe the resources required for virtual machines
* Describe application hosting options, including web apps, containers, and virtual machines
* Describe virtual networking, including the purpose of Azure virtual networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and ExpressRoute
* Define public and private endpoints

**Virtual Machine** - Single OS running as emulated computer. Virtualize the hardware. Run single VMs for testing, development, or minor tasks. Or group VMs together to provide high availability, scalability, and redundancy. Azure can also manage the grouping of VMs for you with features such as scale sets and availability sets.

**Virtual machine scale sets** - The number of VM instances can automatically increase or decrease in response to demand, or you can set it to scale based on a defined schedule. Virtual machine scale sets also automatically deploy a load balancer to make sure that your resources are being used efficiently.

**Virtual machine availability sets** - to help you build a more resilient, highly available environment. there’s no additional cost for configuring an availability set. You only pay for the VM instances you create. It staggers updates across VMs based on their update domain and fault domain.

**Azure Virtual Desktop** – a desktop and application virtualization service that runs on the cloud. It enables you to use a cloud-hosted version of Windows from any location. Let you use Windows 10 or Windows 11 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM.

**Container** – lightweight virtual environment and can run multiple containers on a single physical or virtual host. Unlike virtual machines, you don't manage the operating system for a container.

**Azure Container Instance** - offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services. Azure Container Instances are a platform as a service (PaaS) offering. Azure Container Instances allow you to upload your containers and then the service will run the containers for you.

**Azure Container Apps** - similar in many ways to a container instance. They allow you to get up and running right away, they remove the container management piece, and they're a PaaS offering. Container Apps have extra benefits such as the ability to incorporate load balancing and scaling.

**Azure Kubernetes Service (AKS)** - a container orchestration service. An orchestration service manages the lifecycle of containers. When you're deploying a fleet of containers, AKS can make fleet management simpler and more efficient.

**Azure Functions** - an event-driven, serverless compute option that doesn’t require maintaining virtual machines or containers. Azure Functions runs your code when it's triggered and automatically deallocates resources when the function is finished.

**Azure App Service** -  to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability. Following are types of Azure App Service:

* 1. Web App - includes full support for hosting web apps by using programming languages and can select to host either Window or Linux OS
  2. API App - much like hosting a website, you can build REST-based web APIs by using your choice of language and framework
  3. WebJobs - to run a program (.exe, Java, PHP, Python, or Node.js) or script (.cmd, .bat, PowerShell, or Bash) in the same context as a web app, API app, or mobile app. They can be scheduled or run by a trigger. WebJobs are often used to run background tasks as part of your application logic.
  4. Mobile App - to quickly build a back end for iOS and Android apps. Store data on cloud SQL database, authenticate using social logins, push notification and execute custom back-end login using C# or NodeJS

App Service handles most of the infrastructure decisions you deal with in hosting web-accessible apps:

* Deployment and management are integrated into the platform.
* Endpoints can be secured.
* Sites can be scaled quickly to handle high traffic loads.
* The built-in load balancing and traffic manager provide high availability.

**Azure Virtual Networking**

Azure virtual networks and virtual subnets enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises client computers. Provide following key networking capabilities:

Isolation & Segmentation - allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges. The IP range only exists within the virtual network and isn't internet routable. You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.

Internet Communication - enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer

Communicate between Azure resources – enable Azure resources to communicate securely with each other. You can do that in one of two ways:

* 1. Virtual networks can connect not only VMs but other Azure resources.
  2. Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

Communicate with on-premises resources - enable you to link resources together in your on-premises environment and within your Azure subscription. Three mechanisms to achieve this:

1. Point-to-site virtual private network connections are from a computer outside your organization back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect to the Azure virtual network (instead of corporate network).
2. Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
3. Azure ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

Route Network Traffic - By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

1. Route tables allow you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
2. Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or Azure ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

Filter Network Traffic - Azure virtual networks enable you to filter traffic between subnets by using the following approaches:

1. Network security groups are Azure resources that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
2. Network virtual appliances are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

Connect Virtual Networks - can link virtual networks together by using virtual network peering. Peering allows two virtual networks to connect directly to each other. Network traffic between peered networks is private, and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

Diagram

Description automatically generated

User-defined routes (UDR) allow you to control the routing tables between subnets within a virtual network or between virtual networks. This allows for greater control over network traffic flow.

**Azure VPN Gateway**

Deployed in Azure virtual network, enable following capabilities:

1. Connect on-premises data center to virtual network through site-to-site connection
2. Connect individual devices to virtual network through point-to-site connection
3. Connect virtual network to other virtual network through network-to-network connection

Can only deploy one VPN gateway in each virtual network but can connect to other virtual networks in different locations. Two types of VPN gateway: 1) Policy-based 2) Route-based. These types define how data is encrypted over the network. Both use pre-shared key as the only method for authentication.

1. Policy-based uses static routing, useful to connect legacy system.
2. Route-based is preferred way. It uses dynamic routing (also support static routing) via route tables. More resilient to topology changes such as the creation of new subnets

Table

Description automatically generated

Diagram

Description automatically generated

**High-availability Configuration**

There are a few ways to maximize the resiliency of your VPN gateway.

1. Active/standby – By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure. Standby becomes active within 90s when the active connection go down during service disruption.
2. Active/active – Can also configure both instances as active but need to assign a unique public IP address to each instance. Then create separate tunnels from the on-premises device to each IP address. Extend availability by deploying an additional VPN device on-premises.
3. ExpressRoute failover – uses the Border Gateway Protocol or BGP writing protocol. BGP is used to exchange routes between on premises networks on resources running in azure. This protocol enables dynamic routing between your on-premises network and services running in the Microsoft Cloud. Use ExpressRoute Circuit and traffic will travel over Microsoft networks. With an outage of an ExpressRoute circuit, you can also provision a VPN gateway that uses the internet as an alternative method of connectivity
4. Zone-redundant gateways – In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration. This configuration brings resiliency, scalability, and higher availability to virtual network gateways by protecting your on-premises network connectivity to Azure from zone-level failures.

Diagram

Description automatically generatedDiagram

Description automatically generated

Diagram

Description automatically generated

Features and benefits of ExpressRoute

* Connectivity to Microsoft cloud services across all regions in the geopolitical region.
* Global connectivity to Microsoft services across all regions with the ExpressRoute Global Reach.
* Dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP).
* Built-in redundancy in every peering location for higher reliability. Can configure multiple circuits to complement this feature.

ExpressRoute Connectivity Models - ExpressRoute supports four models:

1. CloudExchange colocation
2. Point-to-point Ethernet connection
3. Any-to-any connection
4. Directly from ExpressRoute sites

Graphical user interface, diagram, application, Teams

Description automatically generated

ExpressRoute Security Considerations – private connection that does not go over public network, so it's not exposed to the potential risks associated with internet communications. However, DNS queries, certificate revocation list checking, and Azure Content Delivery Network requests are still sent over the public internet.

Azure DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. The benefits of using Azure DNS:

* Reliability and performance - DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain
* Security - Azure DNS is based on Azure Resource Manager, which provides features such as Azure role-based access control (Azure RBAC), activity logs to monitor how a user in your organization modified a resource and resource locking
* Ease of Use – because it is running on Azure, applications that require automated DNS management can integrate with the service by using the REST API and SDKs
* Customizable virtual networks - this feature allows you to use your own custom domain names in your private virtual networks, rather than being stuck with the Azure-provided names
* Alias records - if the IP address of the underlying resource changes, the alias record set seamlessly updates itself during DNS resolution

**Learning Objectives: Azure Storage Services**

* Compare Azure Storage services
* Describe storage tiers
* Describe redundancy options
* Describe storage account options and storage types
* Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync
* Describe migration options, including Azure Migrate and Azure Data Box

**Azure Storage Account**

Start by picking the storage account type. The type of account determines the storage services and redundancy options and has an impact on the use cases.

* Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only and must be unique
* Your storage account name must be unique within Azure. No two storage accounts can have the same name. This supports the ability to have a unique, accessible namespace in Azure.
* The combination of the account name and the Azure Storage service endpoint forms the endpoints for your storage account. (e.g., https://<storage-accountname>.blob.core.windows.net)

Consider the tradeoffs between lower costs and higher availability, a few factors include:

1. How data is replicated in the Primary region
2. Data replicated in second region is geographically distant to protect against regional disasters
3. Require read access to the replicated data in the second region if primary region unavailable

Redundancy in Primary Region

Always replicated three times in primary region. Offers two options for that - LRS and ZRS.

Locally Redundant Storage - replicates your data three times within a single data center in the primary region. If a disaster such as fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable. Durability with 11 nines %.

Zone-redundant Storage – replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. Durability with 12 nines %. ZRS is also recommended for restricting replication of data within a country or region to meet data governance requirements.

Redundancy in Secondary Region

Copying data in storage account from primary to secondary region which usually hundreds of miles away. Allow to select the primary region but the paired secondary region is based on Azure Region Pairs and can't be changed. Offer two options (both provide at least 16 nines % of durability) for copying data from primary to secondary region:

1. Geo-redundant storage (GRS) - is similar to running LRS in two regions. GRS copies your data synchronously three times within a single physical location in the primary region using LRS.
2. Geo-zone-redundant storage (GZRS) - is similar to running ZRS in the primary region and LRS in the secondary region. Tecommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery

Note: GRS/GZRS is to protect against regional outages. Data is available to be read only if failover is initiated. If you need to read access to be available to secondary region, you need to enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

**Azure Storage Services**

Azure Storage platform includes the following data services:

**Azure Blobs**: A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2. It is unstructured and there are no restrictions on the kinds of data it can hold. Data is uploaded as blobs, and Azure takes care of the physical storage needs. Offer below tiers to manage cost effectively.

Hot access tier – for frequently access data (website images)

Cool access tier – for infrequently access and stored for at least 30 days (e.g., customer invoice)

Cold access tier - for infrequently access and stored for at least 90 days

Archive access tier – for data that is rarely accessed and stored for at least 180 days (e.g., long-term). Store data offline for the lowest storage cost but also the highest costs to rehydrate and access data.

**Azure Files**: fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols. Azure Files file shares can be mounted concurrently by cloud or on-premises deployments.

**Azure Queues**: storage is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS.

**Azure Disks** (or **Azure managed disks**): block-level storage volumes managed by Azure for use with Azure VMs. Virtualized alternative for physical disk offering greater resiliency and availability.

**Azure Tables**: stores large amounts of structured data. Azure tables are a NoSQL datastore that accepts authenticated calls from inside and outside the Azure cloud. For storing structured, non-relational data.

**Azure Data Migration Options**

**Azure Migrate** is a service that helps you migrate from an on-premises environment to the cloud. In the Azure Migrate hub, a range of tools (including third parties) to assess and migrate on-premises infrastructure to Azure.

**Azure Data Box** is a physical migration service that helps transfer large amounts of data (maximum usable storage capacity of 80 terabytes) in a quick, inexpensive, and reliable way. Order the box from Microsoft and return it (data will be automatically uploaded once received it).

**Azure File Management Options**

**AzCopy** is a command-line utility that you can use to upload/download/copy/synchronize blobs or files to or from your storage account. Synchronize is one directional, from source to destination defined by user.

Azure Storage Explorer is a GUI (standalone app) similar to Windows Explorer to manage files/blobs in storage accounts. Works on Win, Mac & Linux and uses AzCopy on the backend to perform all operations.

**Azure File Sync** is a tool that allows to sync Azure and on-premises in a bi-directional manner.

**Learning Objectives: Azure Identity, Access and Security**

* Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services.
* Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and passwordless.
* Describe external identities and guest access in Azure.
* Describe Microsoft Entra Conditional Access.
* Describe Azure Role Based Access Control (RBAC).
* Describe the concept of Zero Trust.
* Describe the purpose of the defense in depth model.
* Describe the purpose of Microsoft Defender for Cloud.

**Azure Directory Service**

**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. Microsoft Entra ID can also help you maintain your on-premises Active Directory deployment.

Who uses Microsoft Entra ID – IT administrator (to control access), App developers (adding functionality to the app they build), Users (self-service such as password reset) and Online service subscribers (such as M365, Dynamic, Azure users).

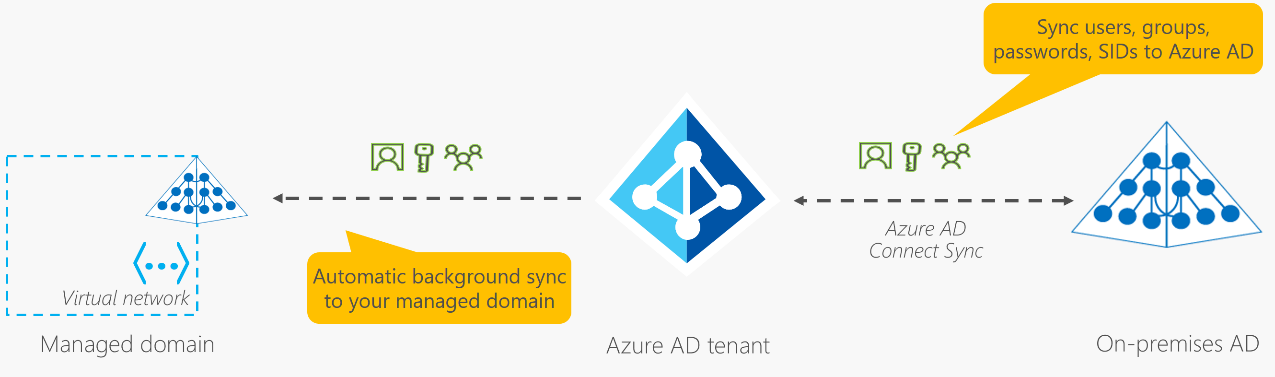
What does Microsoft Entra ID do – Authentication, Single sign-on (SSO), Application Management and Device Management (allows for device-based Conditional Access policies to restrict access attempts)

Can I connect my on-premises AD with Microsoft Entra ID – Need to maintain two identity sets but can connect using Microsoft Entra Connect. Microsoft Entra Connect synchronizes user identities between on-premises Active Directory and Microsoft Entra ID.

What is Microsoft Entra Domain Services - is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud. Let you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

How does Microsoft Entra Domain Services work - When you create a Microsoft Entra Domain Services managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set. You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

Is information synchronized -A managed domain is configured to perform a one-way synchronization from Microsoft Entra ID to Microsoft Entra Domain Services. You can create resources directly in the managed domain, but they aren't synchronized back to Microsoft Entra ID. In a hybrid environment with an on-premises AD DS environment, Microsoft Entra Connect synchronizes identity information with Microsoft Entra ID, which is then synchronized to the managed domain.



Applications, services, and VMs in Azure that connect to the managed domain can then use common Microsoft Entra Domain Services features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.

Microsoft Entra multifactor authentication – enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification

Password-less Authentication - needs to be set up on a device before it can work (device registration)

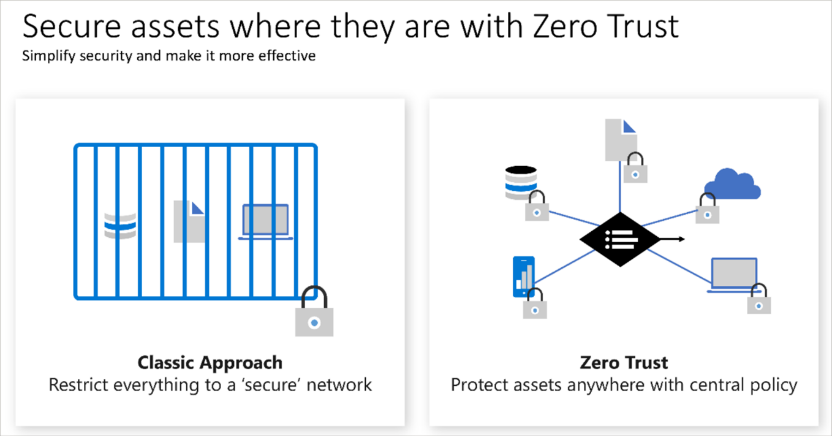
E.g., Window Hello for Business (PIN), Microsoft Authenticator app, FIDO2 (Hardware token device)

Microsoft Entra External ID - refers to all the ways you can securely interact with users outside of your organization (collaborations with vendors, partners, etc.)

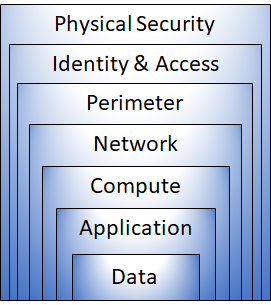
Azure Conditional Access - Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from. Useful when we need to 1) require certain role to use MFA 2) blocking access from unknown device/location 3) allow certain apps to connect to our service

Azure RBAC – it is access rule for cloud resources. Enforced on any action that's initiated against an Azure resource that passes through *Azure Resource Manager*. Resource Manager is a management service that provides a way to organize and secure your cloud resources.

Zero Trust – a security model that assumes the worst-case scenario and protects resources with that expectation. It requires everyone to authenticate even though they are all within the corporate network.



Defense-in-depth – a strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data. All the layers functioning to protect the central data layer.



Physical security - securing access to buildings and controlling access to computing hardware

Identity & Access - identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged

Perimeter – protects from network-based attacks (DDoS). Use perimeter firewalls to identify and alert on attacks against the network

Network – Limit network connectivity across resources. Deny all by default.

Compute – secure access to VMs, end-point protection on devices, keeping system patched and current.

Application – make security a design requirement for app development and store sensitive application secrets in a secure storage medium. Make sure app free of vulnerabilities.

Data – store and control access to data are responsible for integrity, availability and is properly secured.

MS Defender for Cloud – monitoring tools for security and threat protection. Natively integrated to Azure. Defender plans are extended to non-Azure machines (those resources on AWS or GCP) with the help of Azure Arc. Limit exposure to brute force attacks (by reducing access to VM ports, set secure access policies on selected ports). Three important points 1) Assess 2) Secure 3) Defend.

Graphical user interface

Description automatically generated with medium confidence

**PART 3**

**Learning Objectives: Cost Management in Azure**

* Describe factors that can affect costs in Azure.
* Compare the Pricing calculator and Total Cost of Ownership (TCO) calculator.
* Describe the Microsoft Cost Management Tool.
* Describe the purpose of tags.

Following are the factors that can affect (OpEx) costs in Azure.

1. Resource type – settings for the resource and region impact the cost. Azure creates metered instances for resource. The meters track the resource’s usage and generate a usage record that is used to calculate your bill
2. Consumption – pay-as-you-go. It is one of the biggest drivers of costs. Commit to a level of resource usage and get the discount for reserved resources. (up to 72%)
3. Maintenance – monitor resource usage and adjust resources based on demand to control cost.
4. Geography – same resource can cost differently depending on the geographic area
5. Network traffic – resource is impacted by billing zones (geographical grouping of Azure regions for billing purposes). Some inbound data transfers (if same AZ) are free, but outbound is not free.
6. Subscription type – type and configuration of the subscription can impact cost
7. Azure marketplace – using third-party solutions from vendors listed on Azure marketplace

Pricing calculator - can estimate the cost of any provisioned resources, including compute, storage, and associated network costs. You can even account for different storage options like storage type, access tier, and redundancy

Total Cost of Ownership (TCO) calculator - designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure.

What is 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.

What is the purpose of tags – similar to resource group to manage resources, we can use tags to group resources. Tags provide metadata and logically organize resources into taxonomy. It made up of name-value pair and useful for rolling up billing information (cost/workload optimization).

**Learning Objectives: Governance and Compliance**

* Describe the purpose of Microsoft Purview.
* Describe the purpose of Azure Policy.
* Describe the purpose of resource locks.
* Describe the purpose of the Service Trust portal.

**Microsoft Purview**

Microsoft Purview is a family of data governance, risk, and compliance solutions that helps you get a single, unified view into your data. Microsoft Purview brings insights about your on-premises, multicloud, and software-as-a-service data together.  
Two main solution areas comprise Microsoft Purview: risk and compliance and unified data governance.

**Risk & Compliance –** Microsoft 365 features as a core component here. Ensurethe organization’s data in protected across clouds, apps and devices. Identify risks and manage regulatory compliance requirements.

**Unified Data Governance -** robust data governance capabilities enable you to manage your data stored in Azure, SQL and Hive databases, locally, and even in other clouds like Amazon S3.

**Azure Policy**

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules across your resource configurations so that those configurations stay compliant with corporate standards.

Can define both individual policies and group policies (known as initiatives). Noncompliance resources are highlighted or prevented from creating. Can create at each level, i.e., resources, resource group, subscription, etc. Azure Policies are inherited from top to bottom. It comes with built-in policy and can also add exception to exclude certain resources from the policy.

**Azure Policy Initiatives**

An Azure Policy initiative is a way of grouping related policies together. The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal. For example, Azure Policy includes an initiative named Enable Monitoring in Azure Security Center. Its goal is to monitor all available security recommendations for all Azure resource types in Azure Security Center.

Purpose of resource locks – to prevents resources from being accidentally deleted or changed. Even with Azure role-based access control (Azure RBAC) policies in place, there's still a risk that people with the right level of access could delete critical cloud resources. Can create at each level, i.e., resources, resource group, subscription, etc. Azure Policies are inherited from top to bottom.

Types of resource locks – two types, one that prevents users from deleting and one that prevents users from changing or deleting a resource. Delete allows to update but changing allow read-only. Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity.

Purpose of Service Trust Portal - provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

**Learning Objectives**

* Describe the Azure portal.
* Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell.
* Describe the purpose of Azure Arc.
* Describe Azure Resource Manager (ARM), ARM templates, and Bicep.

**Tools for interacting with Azure**

**Azure Portal** - a web-based, unified console that provides an alternative to command-line tools.

**Azure Cloud Shell** - a browser-based shell tool (no local installation or configuration required) that allows you to create, configure, and manage Azure resources using a shell. Azure Cloud Shell support both Azure PowerShell and the Azure Command Line Interface (CLI), which is a Bash shell.

**Azure PowerShell** - Azure PowerShell is a shell with which developers, DevOps, and IT professionals can run commands called command-lets (cmdlets). These commands call the Azure REST API to perform management tasks in Azure. Cmdlets can be run independently to handle one-off changes, or they may be combined to help orchestrate complex action.

**Azure CLI** - The Azure CLI is functionally equivalent to Azure PowerShell, with the primary difference being the syntax of commands. While Azure PowerShell uses PowerShell commands, the Azure CLI uses Bash commands.

**Purpose of Azure Arc** - In utilizing Azure Resource Manager (ARM), Arc lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform. Even with resources hosted outside of Azure, Azure Arc can help to manage servers, Kubernetes clusters, Azure data services, SQL server and VM.

**Azure Resource Manager (ARM)** - provides a management layer that enables you to create, update, and delete resources in your Azure account. Anytime you do anything with your Azure resources, ARM is involved. When a user sends a request from any of the Azure tools, APIs, or SDKs, ARM receives the request. ARM authenticates and authorizes the request. Then, ARM sends the request to the Azure service, which takes the requested action. All requests are handled through the same API (consistency).

**Infrastructure as code** - a concept where you manage your infrastructure as lines of code. At an introductory level, it's things like using Azure Cloud Shell, Azure PowerShell, or the Azure CLI to manage and configure your resources. As you get more comfortable in the cloud, you can use the infrastructure as code concept to manage entire deployments using repeatable templates and configurations. ARM templates and Bicep are two examples of using infrastructure as code with the Azure Resource Manager to maintain your environment.

**ARM templates** - describe the resources you want to use in a declarative JSON format. With an ARM template, the deployment code is verified before any code is run. needs only to define the desired state and configuration of each resource in the ARM template, and the template does the rest. Templates can even execute PowerShell and Bash scripts before or after the resource has been set up.

**Bicep** - a language that uses declarative syntax to deploy Azure resources. A Bicep file defines the infrastructure and configuration. Then, ARM deploys that environment based on your Bicep file. While like an ARM template, which is written in JSON, Bicep files tend to use a simpler, more concise style.

**Learning Objectives**

* Describe the purpose of Azure Advisor.
* Describe Azure Service Health.
* Describe Azure Monitor, including Azure Log Analytics, Azure Monitor Alerts, and Application Insights.

**Azure Advisor** - evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Azure Advisor is designed to help you save time on cloud optimization.

Azure Service Health - helps you keep track of Azure resource, both your specifically deployed resources and the overall status by combining three different Azure services: Azure Status, Service Health & Resource Health. Gives you a complete view of your Azure environment-all the way from the global status of Azure services and regions down to specific resources. Azure Service Health provides links to support.

Azure Monitor - a platform for collecting data on your resources, analyzing that data, visualizing the information, and even acting on the results. Azure Monitor can monitor Azure resources, on-premises resources, and even multi-cloud resources like virtual machines hosted with a different cloud provider.

Azure Log Analytics - is the tool in the Azure portal where you’ll write and run log queries on the data gathered by Azure Monitor. Log Analytics is a robust tool that supports both simple, complex queries, and data analysis. You can write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze the records.

Azure Monitor Alert - an automated way to stay informed when Azure Monitor detects a threshold being crossed. You set the alert conditions, the notification actions, and then Azure Monitor Alerts notifies when an alert is triggered. Depending on your configuration, Azure Monitor Alerts can also attempt corrective action. You could set a metric-based alert up to notify you when the CPU usage on a virtual machine exceeded 80%. Alert rules based on metrics provide near real time alerts based on numeric values. Rules based on logs allow for complex logic across data from multiple sources. Azure Monitor, Service Health, and Azure Advisor all use actions groups to notify you when an alert has been triggered.

Application Insights - an Azure Monitor feature, monitors your web applications. Application Insights is capable of monitoring applications that are running in Azure, on-premises, or in a different cloud environment. There are two ways to configure Application Insights to help monitor your application. You can either install an SDK in your application, or you can use the Application Insights agent. The Application Insights agent is supported in C#.NET, VB.NET, Java, JavaScript, Node.js, and Python.