AZURE Notes

1 ....20-25%.....................

Cloud Computing intro

Benefits of cloud --availability,scalability,elasticity,agility,disaster recovery

diff bw cap ex n opex

consumption based model

Categories of cloud

shared responsibility

iaas,paas,saas serverless computing

Types of cloud computing

public,private,hybrid

2 ....15-20%...................

core az services

1.architectural components

- **region n region pairs**
- **availability zones**
- **resource groups**
- **subscriptions**
- **management groups**
- **az resource manager**
- **az resources**

2.core resources

- **Virtual Machines, Azure App Services, Azure**
- **Container Instances (ACI), Azure Kubernetes Service (AKS), and Windows Virtual Desktop**
- **Virtual Networks, VPN Gateway, Virtual Networkpeering, and ExpressRoute**
- **Container (Blob) Storage, Disk Storage, File Storage,and storage tiers**
- **Cosmos DB, AZ SQL Database, AZ Database forMySQL, AZ Database for PostgreSQL, SQL Managed Instance**
- **Azure Marketplace**

3......................(10-15%).....................

Management tools

3.core solutions

- **Internet of Things (IoT) Hub, IoT Central, and Azure Sphere**
- **Azure Synapse Analytics, HDInsight, and AzureDatabricks**
- **Azure Machine Learning, Cognitive Services andAzure Bot Service**
- **serverless computing solutions that include AzureFunctions and Logic Apps**
- **Azure DevOps, GitHub, GitHub Actions, and AzureDevTest Labs**

4.Azure management tools

- **Azure Portal, Azure PowerShell, Azure CLI,Cloud Shell, and Azure Mobile App**
- **Azure Advisor Azure Resource Manager (ARM) templates, Azure Monitor, Azure Service Health**

4................................10-15%...................................

Describe general security and network security features (10-15%)

Describe Azure security features

- **AZ Security Center, including policy compliance, security alerts, secure score, and resource hygiene**
- **Key Vault**
- **Azure Sentinel**
- **Azure Dedicated Hosts**

Describe Azure network security

- **defense in depth**
- **Network Security Groups (NSG)**
- **Azure Firewall**
- **Azure DDoS protection**

5...........................20-25%)...

Describe identity, governance, privacy, and compliance features (20-25%)

core Azure identity services

- **authentication and authorization**
- **Azure Active Directory**
- **Conditional Access, Multi-Factor Authentication(MFA), and Single Sign-On (SSO)**

Describe Azure governance features

- **Role-Based Access Control (RBAC)**
- **resource locks**
- **tags**
- **Azure Policy**
- **Azure Blueprints**
- **Cloud Adoption Framework for Azure**

Describe privacy and compliance resources

- **Microsoft core tenets of Security, Privacy, and Compliance**
- **Microsoft Privacy Statement, Online Services Terms (OST)Product Terms site, and Data Protection AmendmentAddendum (DPA)**
- **Trust Center**
- **Azure compliance documentation**
- **purpose of Azure Sovereign Regions (Azure Government cloud services and Azure China cloud services)**

6............................10-15%.......................................

Azure cost management and Service Level Agreements

Describe methods for planning and managing costs

- **factors that can affect costs (resource types, services, locations, ingress and egress traffic)**
- **factors that can reduce costs (reserved instances, reserved capacity, hybrid use benefit, spot pricing)**
- **the Pricing calculator and the Total Cost ofOwnership (TCO) calculator**
- **Azure Cost Management**

Azure Service Level Agreements (SLAs) and service lifecycles

- **Azure Service Level Agreements (SLAs)**
- **actions that can impact an SLA (i.e. Availability Zones)**
- **service lifecycle in Azure (Public Preview and General Availability)**

...

Benefits of cloud

- availability,
- Scalability -vertical –ram,cpu

  -horizontal-new instance of resources

- elasticity, --add resources

- agility, --adapt to include new changes
- disaster recovery
- Cloud categories

Cloud types

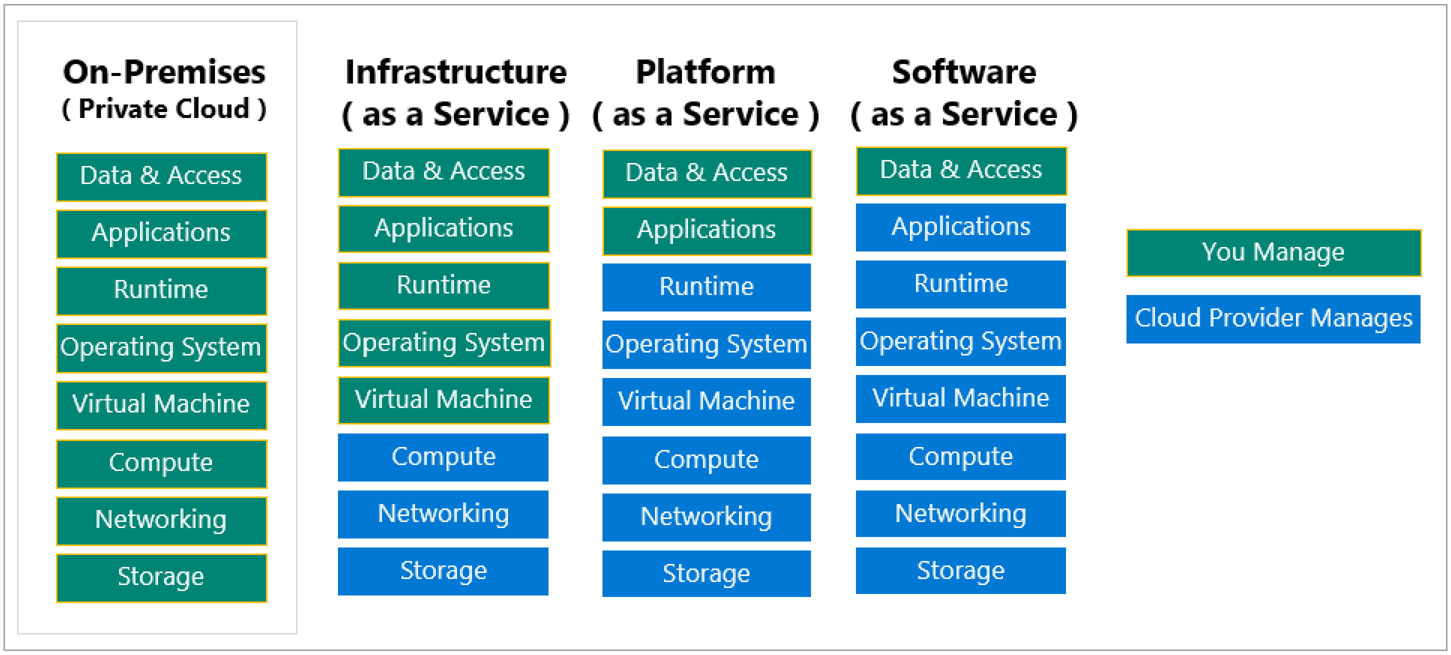
- Public- services are available over internet,
  - anyone can purchase
  - Services Owned by third party
- Private- available for users of organization
- Hybrid –combo of public and private

Categories of cloud

IAAS – hardware managed by Cloud provider, rest all we should manage, eg-virtual machine,network

PAAS-infrastructure and OS,network all managed by cloud, we have to deploy eg app services

SAAS—predeployed softwares can be used as licence or account subscription,eg office 365



On-Premises (Private Cloud)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟩 Data & Access	🟩 Data & Access	🟩 Data & Access	🟩 Data & Access
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtual Machine	🟩 Virtual Machine	🟦 Virtual Machine	🟦 Virtual Machine
🟩 Compute	🟦 Compute	🟦 Compute	🟦 Compute
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage

🟩 You Manage

🟦 Cloud Provider Manages

Types of Expenses

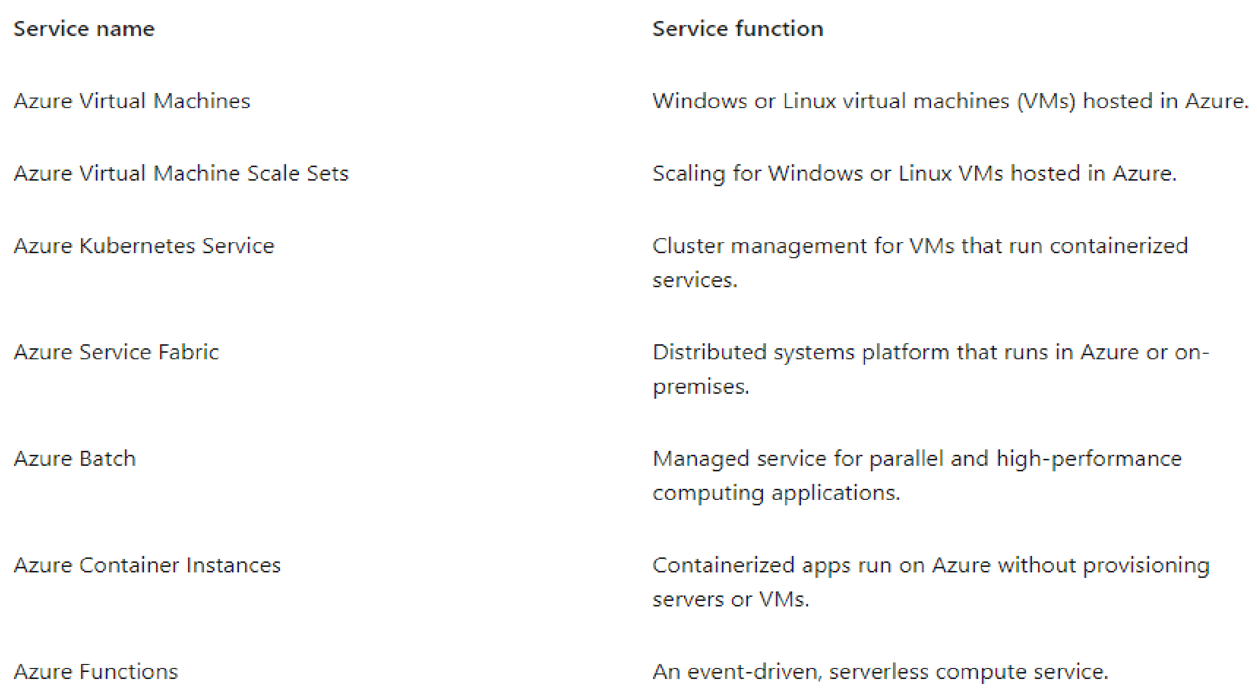
- **Capital Expenditure (CapEx)** investments on building infrastructure,hardware etc.value reduces over time as hardware life reduces
- **Operational Expenditure (OpEx)** pay per use model,no investments, pay for consumptions used

……

10 major services in AZURE

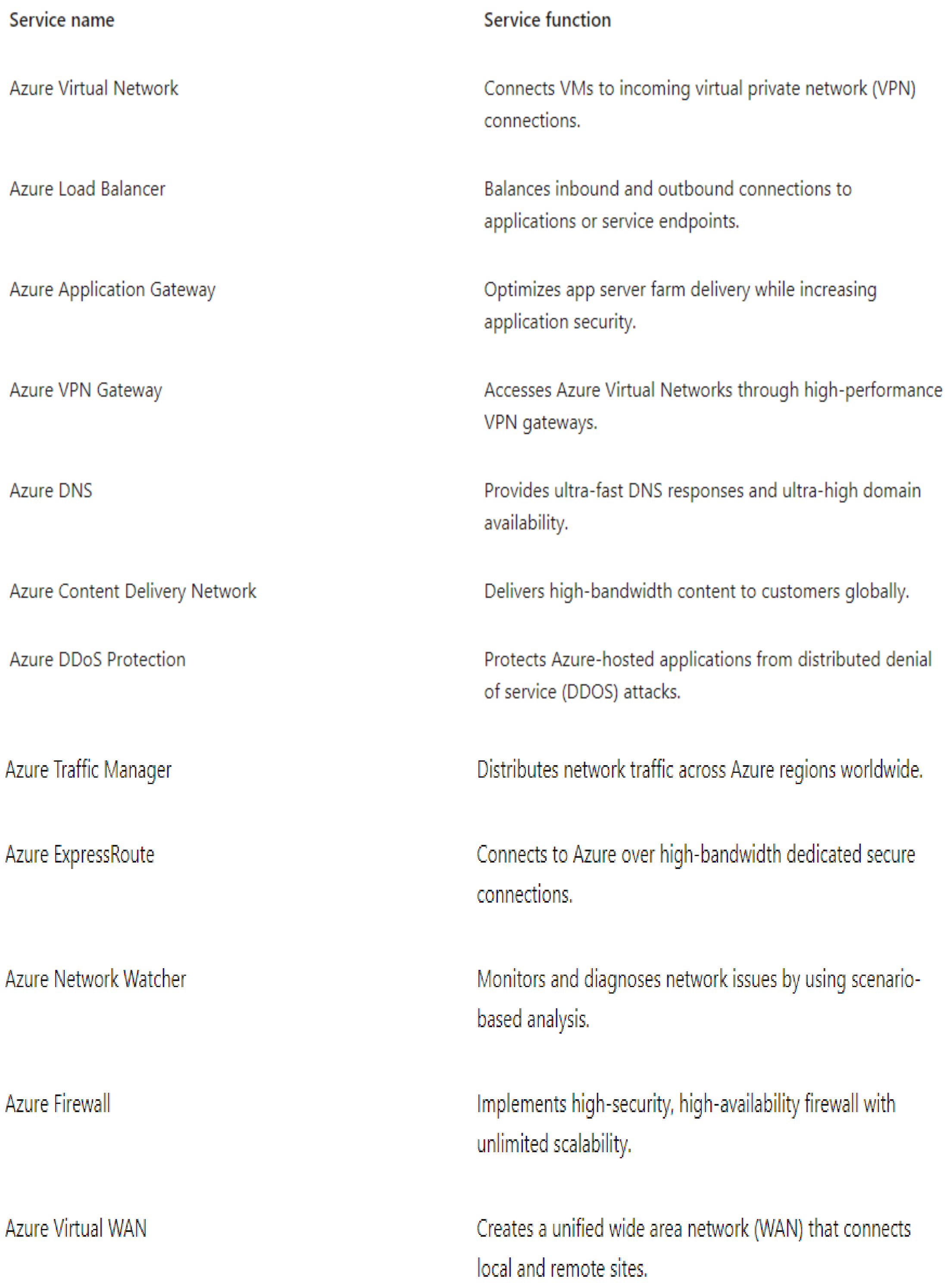
- Compute --scale computing capability on demand, eg VM pay per use
- Networking --connect cloud and on premise infrastructure(outside world to azure services),eg vnp, load balancer
- Storage --disk,file,blob,archival storage
- Mobile --build n deploy crossplatform native app,send notification,use xamarin,cognitive services to make app smarter
- database --sl,cosmos db,mysql etc
- web --build deploy manage, scale web applications,public api,azuremaps to provide geospacial
- IOT --connect n manage iot assets,analyse data from sensors,take actions
- Bigdata --large volume of data ,help to run analysis
- AI --use existing data to forcast future behaviour,machine learning
- dev-ops --brings people ,process and technology and CICI, create release piplelines.

Compute



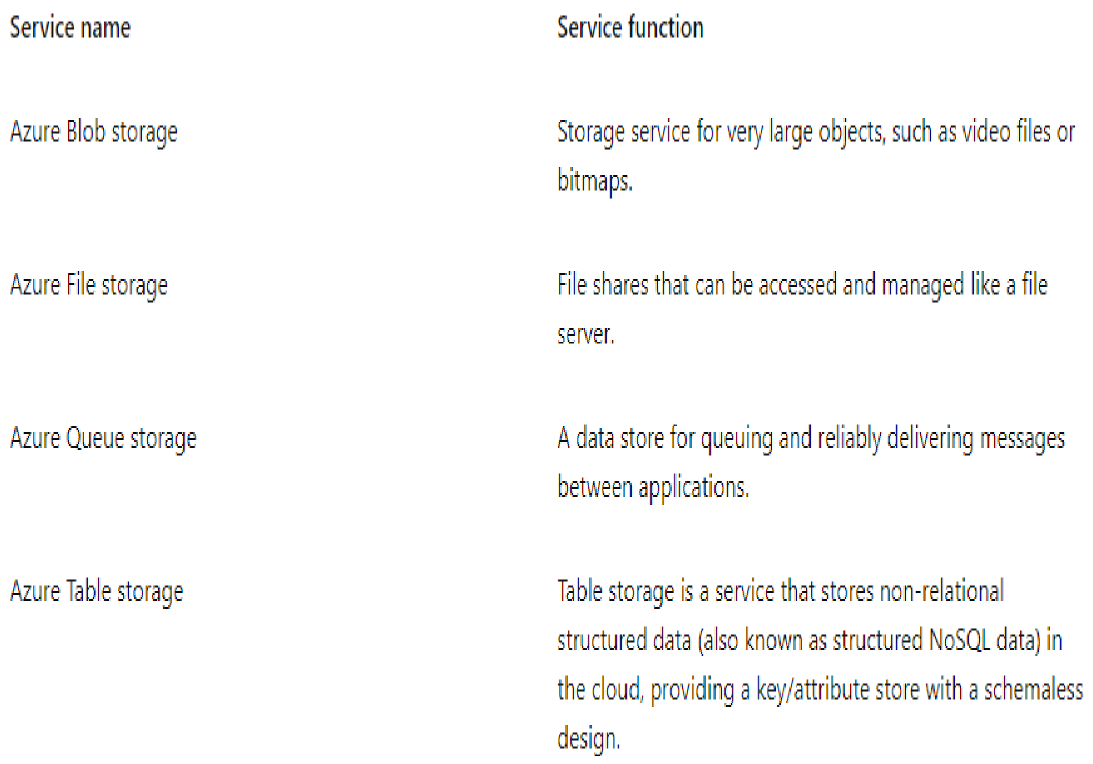
Service name	Service function
Azure Virtual Machines	Windows or Linux virtual machines (VMs) hosted in Azure.
Azure Virtual Machine Scale Sets	Scaling for Windows or Linux VMs hosted in Azure.
Azure Kubernetes Service	Cluster management for VMs that run containerized services.
Azure Service Fabric	Distributed systems platform that runs in Azure or on-premises.
Azure Batch	Managed service for parallel and high-performance computing applications.
Azure Container Instances	Containerized apps run on Azure without provisioning servers or VMs.
Azure Functions	An event-driven, serverless compute service.

Networking



Service name	Service function
Azure Virtual Network	Connects VMs to incoming virtual private network (VPN) connections.
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints.
Azure Application Gateway	Optimizes app server farm delivery while increasing application security.
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways.
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability.
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally.
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks.
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide.
Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections.
Azure Network Watcher	Monitors and diagnoses network issues by using scenario-based analysis.
Azure Firewall	Implements high-security, high-availability firewall with unlimited scalability.
Azure Virtual WAN	Creates a unified wide area network (WAN) that connects local and remote sites.

Storage



Service name	Service function
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps.
Azure File storage	File shares that can be accessed and managed like a file server.
Azure Queue storage	A data store for queuing and reliably delivering messages between applications.
Azure Table storage	Table storage is a service that stores non-relational structured data (also known as structured NoSQL data) in the cloud, providing a key/attribute store with a schemaless design.

- **Durable** and highly available with redundancy and replication.
- **Secure** through automatic encryption and role-based access control.
- **Scalable** with virtually unlimited storage.
- **Managed**, handling maintenance and any critical problems for you.
- **Accessible** from anywhere in the world over HTTP or HTTPS.

Mobile

With Azure, developers can create mobile back-end services for iOS, Android, and Windows apps quickly and easily.

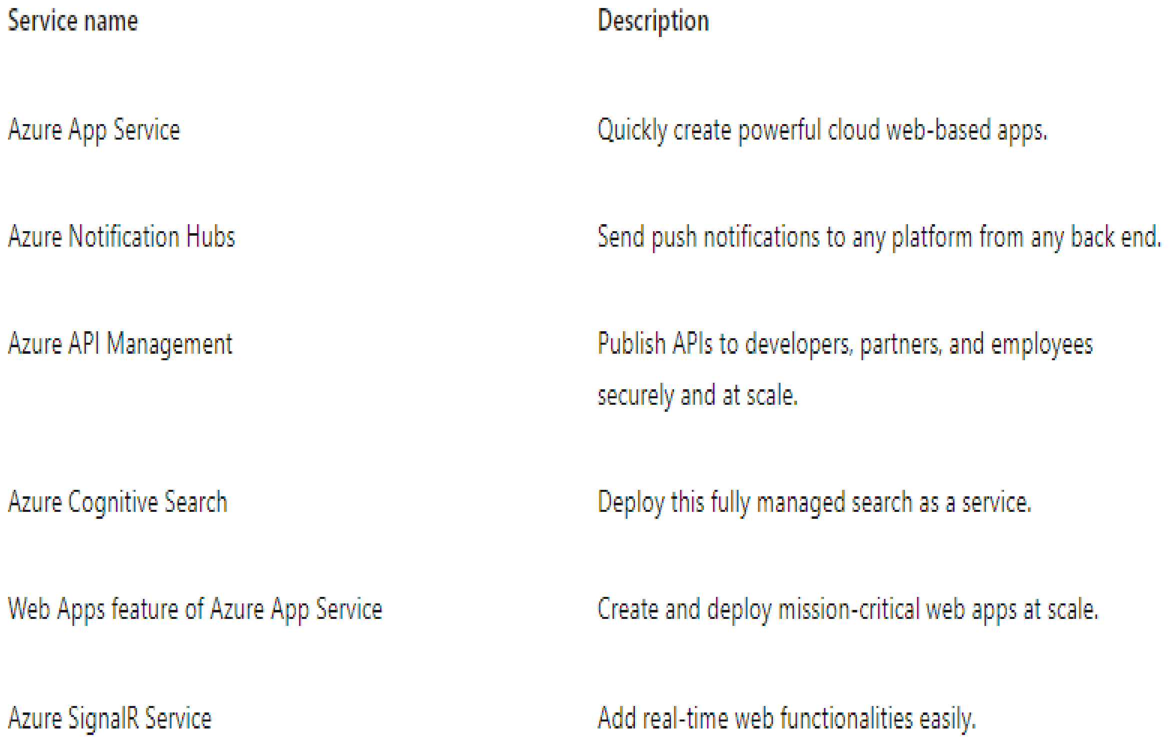
Other features of this service include:

- Offline data synchronization.
- Connectivity to on-premises data.
- Broadcasting push notifications.
- Autoscaling to match business needs.

Databases

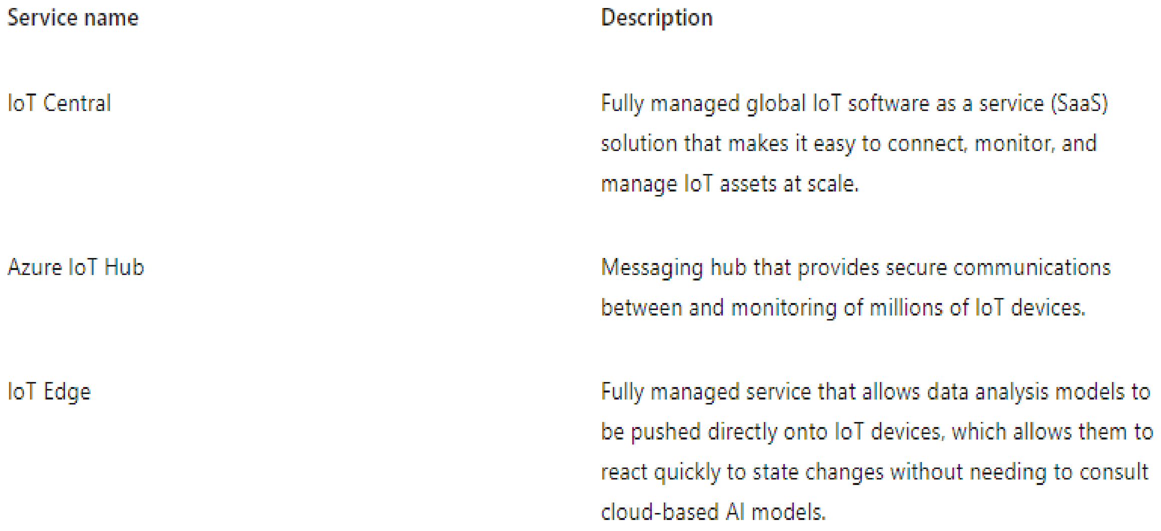
Service name	Service function
Azure Cosmos DB	Globally distributed database that supports NoSQL options.
Azure SQL Database	Fully managed relational database with auto-scale, integral intelligence, and robust security.
Azure Database for MySQL	Fully managed and scalable MySQL relational database with high availability and security.
Azure Database for PostgreSQL	Fully managed and scalable PostgreSQL relational database with high availability and security.
SQL Server on Azure Virtual Machines	Service that hosts enterprise SQL Server apps in the cloud.
Azure Synapse Analytics	Fully managed data warehouse with integral security at every level of scale at no extra cost.
Azure Database Migration Service	Service that migrates databases to the cloud with no application code changes.
Azure Cache for Redis	Fully managed service caches frequently used and static data to reduce data and application latency.
Azure Database for MariaDB	Fully managed and scalable MariaDB relational database with high availability and security.

Web



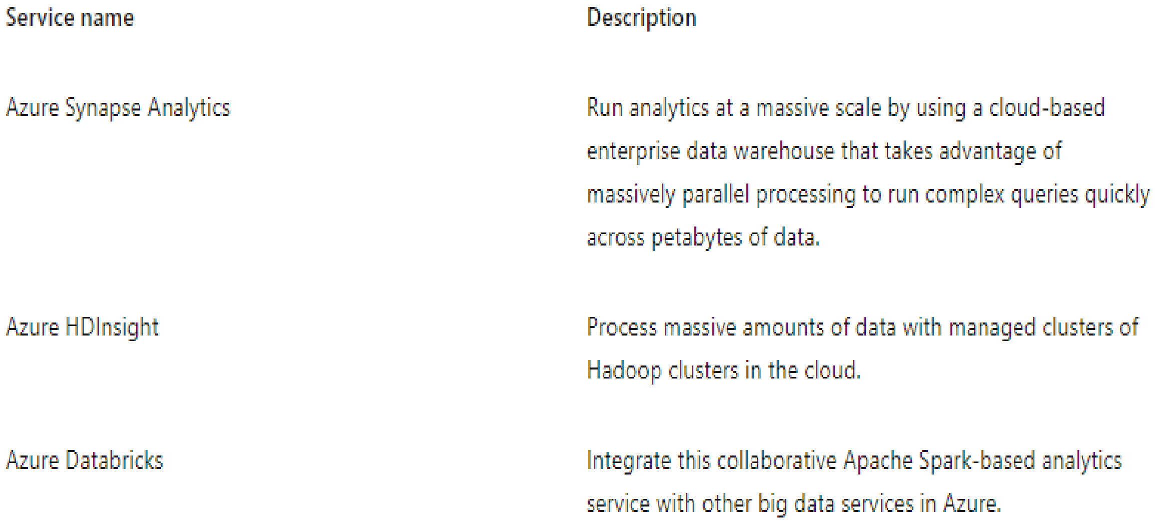
Service name	Description
Azure App Service	Quickly create powerful cloud web-based apps.
Azure Notification Hubs	Send push notifications to any platform from any back end.
Azure API Management	Publish APIs to developers, partners, and employees securely and at scale.
Azure Cognitive Search	Deploy this fully managed search as a service.
Web Apps feature of Azure App Service	Create and deploy mission-critical web apps at scale.
Azure SignalR Service	Add real-time web functionalities easily.

IoT



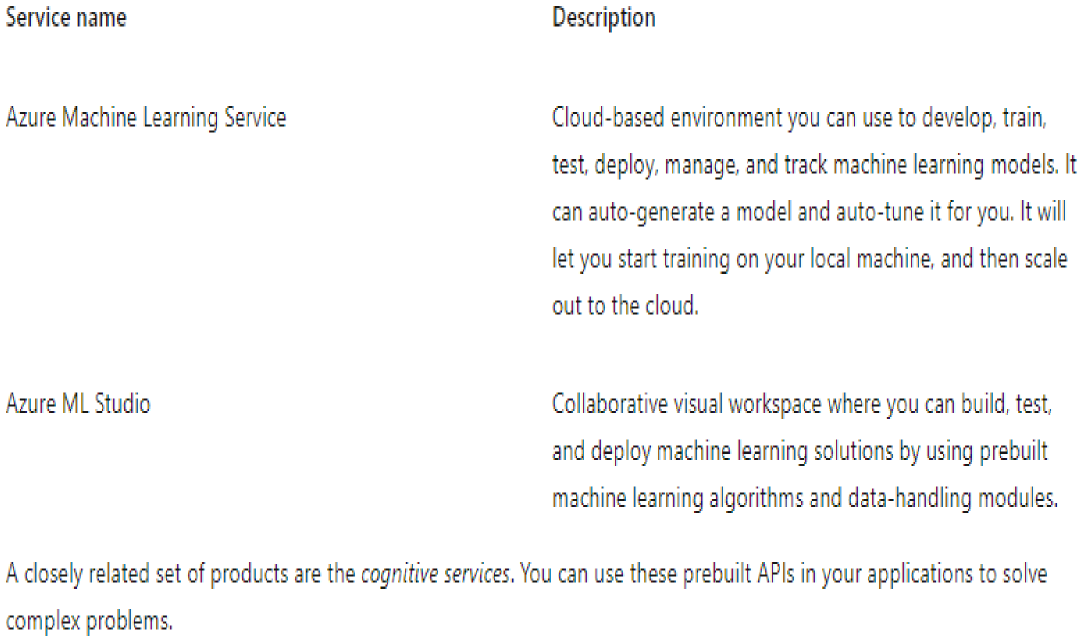
Service name	Description
IoT Central	Fully managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage IoT assets at scale.
Azure IoT Hub	Messaging hub that provides secure communications between and monitoring of millions of IoT devices.
IoT Edge	Fully managed service that allows data analysis models to be pushed directly onto IoT devices, which allows them to react quickly to state changes without needing to consult cloud-based AI models.

Big data



Service name	Description
Azure Synapse Analytics	Run analytics at a massive scale by using a cloud-based enterprise data warehouse that takes advantage of massively parallel processing to run complex queries quickly across petabytes of data.
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud.
Azure Databricks	Integrate this collaborative Apache Spark-based analytics service with other big data services in Azure.

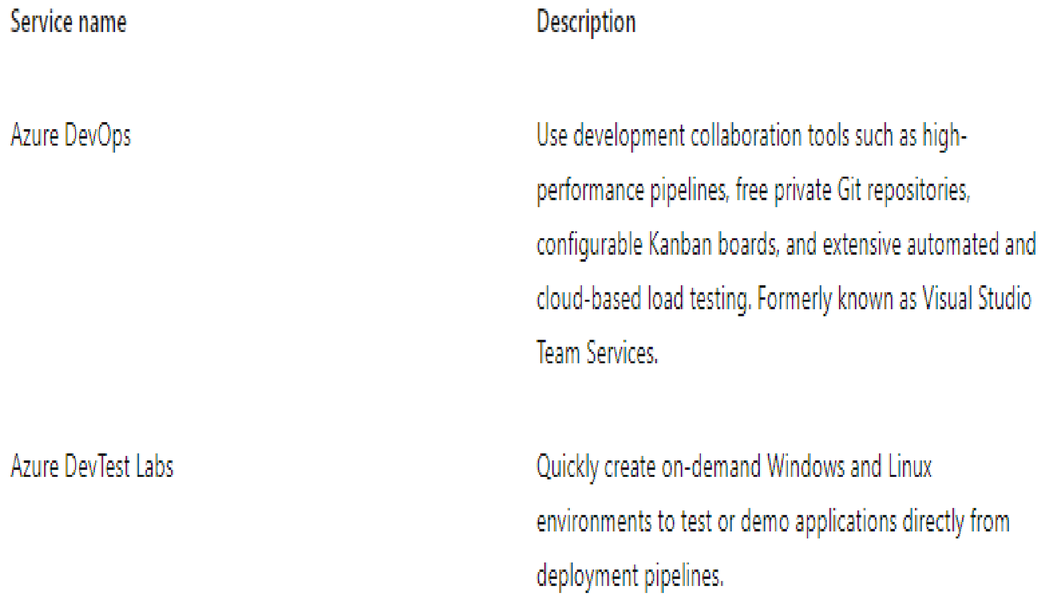
AI



Service name	Description
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud.
Azure ML Studio	Collaborative visual workspace where you can build, test, and deploy machine learning solutions by using prebuilt machine learning algorithms and data-handling modules.

A closely related set of products are the *cognitive services*. You can use these prebuilt APIs in your applications to solve complex problems.

DevOps



Service name	Description
Azure DevOps	Use development collaboration tools such as high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. Formerly known as Visual Studio Team Services.
Azure DevTest Labs	Quickly create on-demand Windows and Linux environments to test or demo applications directly from deployment pipelines.

- management groups -- manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
- Subscriptions -- groups together user accounts and the resources
- resource groups –Logical container of resources
- Resources -- Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

Some services or VM features are only available in certain regions, such as specific VM sizes or storage types. There are also some global Azure services that don't require you to select a particular region, such as Azure Active Directory, Azure Traffic Manager, and Azure DNS.

Availability zones

physically separate datacenters within an Azure region.

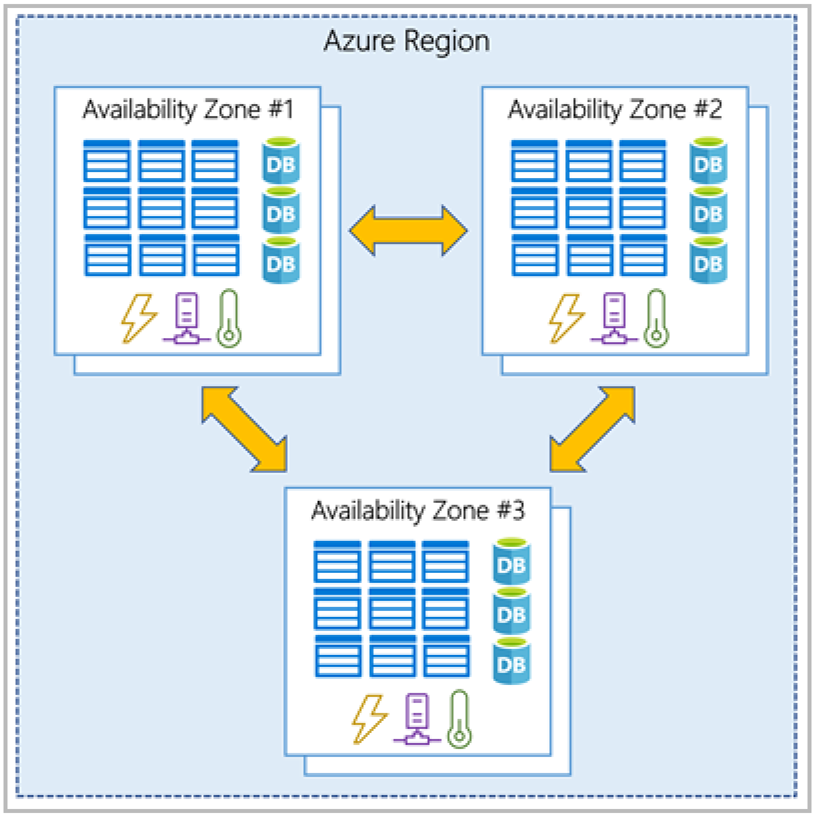
Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

An availability zone is set up to be an *isolation boundary*. If one zone goes down, the other continues working

Not every region has support for availability zones.

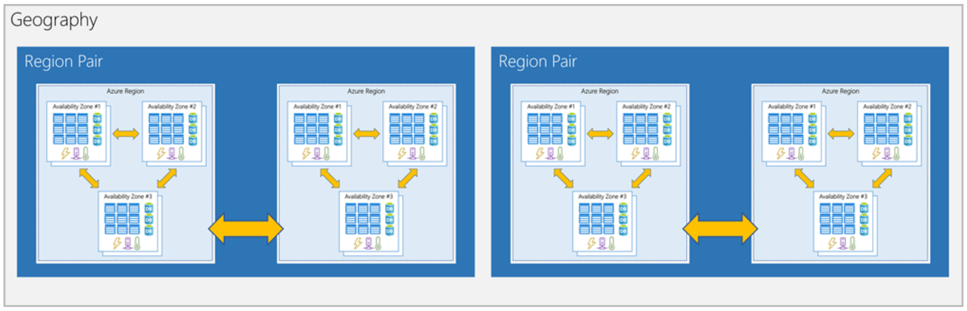
Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases.

There's a minimum of three zones within a single region.

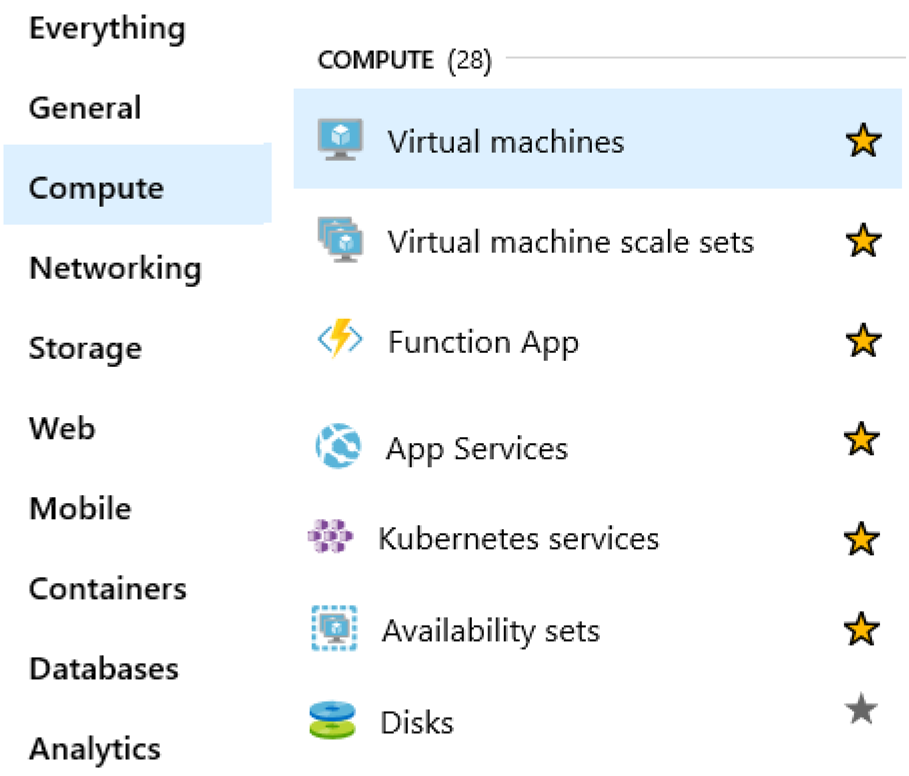


Azure region pairs

Each Azure region is always paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away.



COMPUTE SERVICES



1.VMs in Azure

Virtual machines are software emulations of physical computers

2.virtual machine scale sets

- Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs
- Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes to provide highly available applications.
- The number of VM instances can automatically increase or decrease in response to demand or a defined schedule

3.Azure Container Instances and Container Instance

Container Instances and Azure Kubernetes Service are Azure compute resources that you can use to deploy and manage containers. Containers are lightweight, virtualized application environments offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services. It's a platform as a service (PaaS) offering that allows you to upload your containers, which it runs for you.

Container instance-upload and run a container instance

Kubernetes services -- The task of automating, managing, and interacting with a large number of containers is known as orchestration. Azure Kubernetes Service is a complete orchestration service for containers with distributed architectures and large volumes of containers.

4.Azure app services

With App Service, you can host most common app service styles like:

- Web apps
- API apps
- 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.
- Mobile apps

5.Azure functions

Functions are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure

Azure has two implementations of serverless compute:

- **Azure Functions**: Functions can execute code in almost any modern language.pay for only code running time,stateless by defaulr
- **Azure Logic Apps**: Logic apps are designed in a web-based designer and can execute logic workflow triggered by Azure services without writing any code.workflow is json file known workflow schema.

NETWORKING

Azure Virtual Network fundamentals learn more

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

Azure virtual networks 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. You can think of an Azure network as a set of resources that links other Azure resources.

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Bound to single region,if need to connect to other region use vpn gateway or VN peering

Note

Azure VMs use Azure Disk Storage to store virtual disks. However, you can't use Azure Disk Storage to store a disk outside of a virtual machine.

Azure VN gateway

VPNs use an encrypted tunnel within another network. They're typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

All transferred data is encrypted in a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network

When you deploy a VPN gateway, you specify the VPN type: either *policy-based* or *route-based*. The main difference between these two types of VPNs is how traffic to be encrypted is specified. In Azure, both types of VPN gateways use a pre-shared key as the only method of authentication

Azure Express route

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

ExpressRoute connections don't go over the public Internet.

AZ load balancer

Public --pu

Private –internal traffic

Application gateway—only wor web based req, based on url

CDN –globaly distributed servers, deliver static files, user get contents faster.

STORAGE

Azure Storage account fundamentals
Need to create storage account

A storage account provides a unique namespace for your Azure Storage data, that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable.

Type of data

Structured, -has schema, eg db

Unsctuctured—pdf,word ,jpeg,

Semi structured – csv,xml,json

Type of storage

Blob,disk,file ,archive

Disk storage –disk of vm, SSD or HDD,ultra disk

- You can use standard SSD and HDD disks for less critical workloads,
- premium SSD disks for mission-critical production applications, and
- ultra disks for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads

Azure Blob storage—unstructured data

It can store massive amounts of data, such as text or binary data. Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.
- Storing up to 8 TB of data for virtual machines.

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).

- Only the hot and cool access tiers can be set at the account level. The archive access tier isn't available at the account level.
- Hot, cool, and archive tiers can be set at the blob level, during upload or after upload.
- Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.

- Archive storage stores data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.

Azure Files

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block and Network File System (preview) protocols.

Accessed using SMB(server message block)

Archive storage--

Store data that Used frequently,eg long term backuo

Stored offline, low storage cost

To pull data, high cost.

180 days

Azure Database services-paas

- Azure Cosmos DB

Azure Cosmos DB provides comprehensive service level agreements for throughput, latency, availability, and consistency guarantees.

<10 milli seconds responsive , 99.99 availability

Azure Cosmos DB supports schema-less data, which lets you build highly responsive and "Always On" applications to support constantly changing data.

Azure Cosmos DB stores data in atom-record-sequence (ARS) format. The data is then abstracted and projected as an API

- Azure SQL Database

Azure SQL Database is a relational database

- Azure SQL Managed Instance
- Azure Database for MySQL
- Azure Database for PostgreSQL

BIG DATA AND ANALYTICS SERVICES

- Azure Synapse Analytics formerly Azure SQL Data Warehouse

is a limitless analytics service that brings together enterprise data warehousing and big data analytics

- Azure HDInsight

is a fully managed, open-source analytics service for enterprises. It's a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data,apache spark, apache hadoop

- Azure Databricks

helps you unlock insights from all your data and build artificial intelligence solutions. You can set up your Apache Spark environment in minutes, and then autoscale and collaborate on shared projects in an interactive workspace

- Azure Data Lake Analytics

is an on-demand analytics job service that simplifies big data. Instead of deploying, configuring, and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by setting the dial for how much power you need. You only pay for your job when it's running, making it more cost-effective.

IOT SERVICE

- IOT hub – act as central hub for birectional communication,send and receive msg, no need further reporting features ,
- IOT central – on top of IOT hub add, customized dashboard, analysis, control,monitor and monitor,setup alert,templates for different industries,

- AZure sphere – end to end iot solution from hardware and os of system, ,connectivity and security,when security is more important

AI SERVICES

Azure Machine Learning is a platform for making predictions. It consists of tools and services that allow you to connect to data to train and test models to find one that will most accurately predict a future result. After you've run experiments to test the model, you can deploy and use it in real time via a web API endpoint.

Choose Azure Machine Learning when your data scientists need complete control over the design and training of an algorithm using your own data

Azure Cognitive Services provides prebuilt machine learning models that enable applications to see, hear, speak, understand, and even begin to reason. Use Azure Cognitive Services to solve general problems, such as analyzing text for emotional sentiment or analyzing images to recognize objects or faces. You don't need special machine learning or data science knowledge to use these services. Developers access Azure Cognitive Services via APIs and can easily include these features in just a few lines of code.

- **Language** services: Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.
- **Speech** services: Convert speech into text and text into natural-sounding speech. Translate from one language to another and enable speaker verification and recognition.
- **Vision** services: Add recognition and identification capabilities when you're analyzing pictures, videos, and other visual content.
- **Decision** services: Add personalized recommendations for each user that automatically improve each time they're used, moderate content to monitor and remove offensive or risky content, and detect abnormalities in your time series data.

Azure Bot Service and Bot Framework are platforms for creating virtual agents that understand and reply to questions just like a human.

Behind the scenes, the bot you build uses other Azure services, such as Azure Cognitive Services, to understand what their human counterparts are asking for.

Bots can be used to shift simple, repetitive tasks, such as taking a dinner reservation or gathering profile information, on to automated systems that might no longer require direct human intervention

Use Azure Cognitive Services when it comes to general purpose tasks, such as performing speech to text, integrating with search, or identifying the objects in an image

For data analysis

Choose Azure Machine Learning when you need to analyze data to predict future outcomes

Decission making

SERVERLESS COMPUTING

Azure Functions— developed using progrmaing in mind

With the Azure Functions service, you can host a single method or function by using a popular programming language in the cloud that runs in response to an event. An example of an event might be an HTTP request, a new message on a queue, or a message on a timer.

Azure Functions scales automatically, and charges accrue only when a function is triggered.

An Azure function is a stateless environment. A function behaves as if it's restarted every time it responds to an event. This feature is ideal for processing incoming data. And if state is required, the function can be connected to an Azure storage account.

Azure Logic Apps. --developed using Workflow in mind

Logic Apps is a low-code/no-code development platform hosted as a cloud service. The service helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations

Azure Logic Apps is designed in a web-based designer and can execute logic that's triggered by Azure services without writing any code. You build an app by linking triggers to actions with connectors. A trigger is an event (such as a timer) that causes an app to execute,

To build enterprise integration solutions with Azure Logic Apps, you can choose from a growing gallery of over 200 connectors. The gallery includes services such as Salesforce, SAP, Oracle DB, and file shares.

Logic Apps pricing is based on the number of executions and the type of connectors that it utilizes.

AZURE DEVOPS SERVICES

Azure Devops

- **Azure Repos** is a centralized source-code repository where software development, DevOps engineering, and documentation professionals can publish their code for review and collaboration.
- **Azure Boards** is an agile project management suite that includes Kanban boards, reporting, and tracking ideas and work from high-level epics to work items and issues.
- **Azure Pipelines** is a CI/CD pipeline automation tool.
- **Azure Artifacts** is a repository for hosting artifacts, such as compiled source code, which can be fed into testing or deployment pipeline steps.
- **Azure Test Plans** is an automated test tool that can be used in a CI/CD pipeline to ensure quality before a software release.

Git n GIThub actions

Azure DevTest Labs

AZURE MANGEMENT TOOLS OPTIONS

The Azure portal
The Azure portal provides a friendly, graphical UI to view all the services you're using, create new services, configure your services, and view reports

The Azure mobile app

Azure PowerShell—cross platform,need storage accc,browser based

The Azure CLI –cross platform

ARM templates
By using Azure Resource Manager templates (ARM templates), you can describe the resources you want to use in a declarative JSON format.

Azure PowerShell and the Azure CLI are Azure management tools that allow you to quickly obtain the IP address of a virtual machine (VM) you've deployed, reboot a VM, or scale an app

Keep in mind that ARM templates can include both PowerShell and/or Azure CLI scripts

However, if you're in a cloud management or administrative role, it's less efficient to rely solely on visual scanning and clicking. To quickly find the settings and information you want to work with, the Azure CLI or PowerShell will give you the most flexibility for repeatable tasks.

ARM templates define your application's infrastructure requirements for a repeatable deployment that is done in a consistent manner. A validation step ensures that all resources can be created in the proper order based on dependencies, in parallel, and idempotent.

By contrast, it's entirely possible to use either PowerShell or the Azure CLI to set up all the resources for a deployment. However, there's no validation step in these tools. If a script encounters an error, the dependency resources can't be rolled back easily, deployments happen serially, and only some operations are idempotent.

If you or your cloud administrators come from a Windows administration background, it's likely you'll prefer PowerShell. If you or your cloud administrators come from a Linux administration background, it's likely you'll prefer the Azure CLI.

managing Azure from the portal takes too much time and is not repeatable.

We're looking for a technology to automate the deployment of an entire infrastructure, as needed.
Using ARM templates

Bash –azure cli

Infrastructure as a code-ARM

MONITORING TOOLS OF CLOUD

Azure Advisor

evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs

- **Reliability**: Used to ensure and improve the continuity of your business-critical applications.
- **Security**: Used to detect threats and vulnerabilities that might lead to security breaches.
- **Performance**: Used to improve the speed of your applications.
- **Cost**: Used to optimize and reduce your overall Azure spending.
- **Operational Excellence**: Used to help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Azure Monitor

Azure Monitor is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.

Azure Service Health

Azure Service Health provides a personalized view of the health of the Azure services, regions, and resources you rely on. The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full picture

You can set up alerts that help you triage outages and planned maintenance. After an outage, Service Health provides official incident reports, called root cause analyses (RCAs), which you can share with stakeholders.

Service Health helps you keep an eye on several event types:

- **Service issues** are problems in Azure, such as outages, that affect you right now. You can drill down to the affected services, regions, updates from your engineering teams, and find ways to share and track the latest information.
- **Planned maintenance** events can affect your availability. You can drill down to the affected services, regions, and details to show how an event will affect you and what you need to do. Most of these events occur without any impact to you and aren't shown here. In the rare case that a reboot is required, Service Health allows you to choose when to perform the maintenance to minimize the downtime.
- **Health advisories** are issues that require you to act to avoid service interruption, including service retirements and breaking changes. Health advisories are announced far in advance to allow you to plan.

Azure security tools

Azure Security Center is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premise

Secure score is a measurement of an organization's security posture.

Azure Sentinel is Microsoft's cloud-based SIEM system. It uses intelligent security analytics and threat analysis.

Azure Sentinel enables you to:

- **Collect cloud data at scale**
- Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
- **Detect previously undetected threats**
- Minimize false positives by using Microsoft's comprehensive analytics and threat intelligence.
- **Investigate threats with artificial intelligence**
- Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.
- **Respond to incidents rapidly**
- Use built-in orchestration and automation of common tasks.

Azure Sentinel supports a number of data sources, which it can analyze for security events

- **Connect Microsoft solutions**
- Connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, and Windows Defender Firewall.
- **Connect other services and solutions**
- Connectors are available for common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud, and Okta SSO.
- **Connect industry-standard data sources**

- Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

  Azure Monitor Playbooks to automate responses to threats. For example, it can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps:

  Azure Key Vault is a centralized cloud service for storing an application's secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.

- **Manage secrets**
- You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- **Manage encryption keys**
- You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
- **Manage SSL/TLS certificates**
- Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.
- **Store secrets backed by hardware security modules (HSMs)**
- These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

  ```
  az keyvault secret show \ --name MyPassword \ --vault-name <my-keyvault-NNN> \ --query value \ --output tsv
  ```

Azure Dedicated Host:

- Gives you visibility into, and control over, the server infrastructure that's running your Azure VMs.
- Helps address compliance requirements by deploying your workloads on an isolated server.

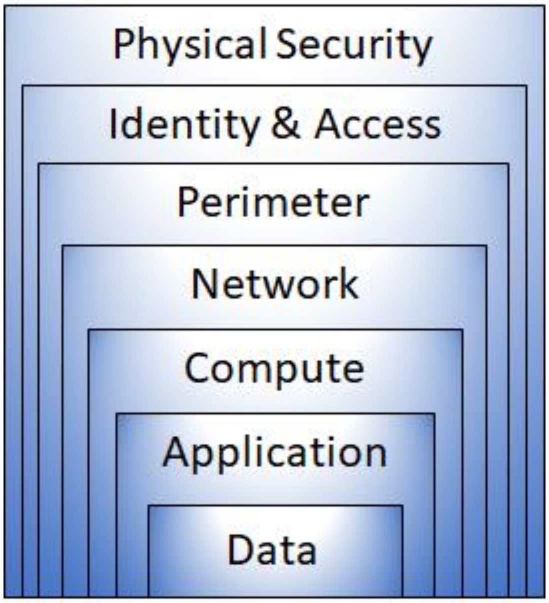
- Lets you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Azure Sentinel is Microsoft's cloud-based SIEM. A SIEM aggregates security data from many different sources to provide additional capabilities for threat detection and responding to threats.

With Azure Security Center, you can define a list of allowed applications to ensure that only applications you allow can run. Azure Security Center can also detect and block malware from being installed on your VM

DEFENCE IN DEPTH



- 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.

Azure Firewall is a managed, cloud-based network security service that helps protect resources in your Azure virtual network

Azure DDoS Protection (Standard) helps protect your Azure resources from DDoS attacks.

Basic and standard options

A network security group enables you to filter network traffic to and from Azure resources within an Azure virtual network. You can think of NSGs like an internal firewall. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

A network security group rule enables you to filter traffic to and from resources by source and destination IP address, port, and protocol.

Azure Firewall enables you to limit outbound HTTP/S traffic to a specified list of fully qualified domain names (FQDNs).

AZURE IDENTITY SERVICES

Azure Active Directory (Azure AD),

single sign-on (SSO),

multifactor authentication, and

Conditional Access

Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally.

Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

A *tenant* is a representation of an organization. A tenant is typically separated from other tenants and has its own identity.

Azure AD is for:

- **IT administrators**
- Administrators can use Azure AD to control access to applications and resources based on their business requirements.

- **App developers**
- Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **Users**
- Users can manage their identities. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
- **Online service subscribers**
- Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD.

Azure AD provides services such as:

- **Authentication**
- This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on**
- SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management**
- You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the *access panel*), and single sign-on provide a better user experience.
- **Device management**
- Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for

device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD.

The Azure Active Directory free edition enables Azure AD Multi-Factor Authentication for administrators with the *global admin* level of access, via the Microsoft Authenticator app, phone call, or SMS code. You can also enforce Azure AD Multi-Factor Authentication for all users via the Microsoft Authenticator app only, by enabling *security defaults* in your Azure AD tenant.

Conditional Access is a tool that Azure Active Directory 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.

Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access feature

Conditional Access enables you to require users to access your applications only from approved, or managed, devices.

Authenticating through multifactor authentication can include something the user knows, something the user has, and something the user is.

CLOUD GOVERNANCE

Azure RBAC

AZURE Locks

A resource lock prevents resources from being accidentally deleted or changed.

You can apply locks to a subscription, a resource group, or an individual resource. You can set the lock level to **CanNotDelete** or **ReadOnly**.

To modify a locked resource, you must first remove the lock

Resource *tags* are another way to organize resources. Tags provide extra information, or metadata, about your resources. This metadata is useful for:

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources.

Eg:create vm only in specific region

Azure Policy enables you to define both individual policies and groups of related policies, known as ***initiative***

Implementing a policy in Azure Policy involves these three steps:

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

Policy assignments are inherited by all child resources within that scope. If a policy is applied to a resource group, that policy is applied to all resources within that resource group

Policy evaluation happens about once per hour. If you make changes to your policy definition and create a policy assignment, that policy is evaluated over your resources within the hour.

Azure Blueprints

Instead of having to configure features like Azure Policy for each new subscription, with Azure Blueprints you can define a repeatable set of governance tools and standard Azure resources that your organization requires.

Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Implementing a blueprint in Azure Blueprints involves these three steps:

4. Create an Azure blueprint.
5. Assign the blueprint.
6. Track the blueprint assignments.

Tags provide extra information, or metadata, about your resources. The team might create a tag that's named BillingDept whose value would be the name of the billing department. You can use Azure Policy to ensure that the proper tags are assigned when resources are provisioned.

After you enable this policy, that policy is applied when you create new virtual machines or resize existing ones. Azure Policy also evaluates any current virtual machines in your environment.

Azure RBAC enables you to create roles that define access permissions. You might create one role that limits access only to virtual machines and a second role that provides administrators with access to everything.

compliance offerings that are available on Azure.

The Microsoft Privacy Statement explains what personal data Microsoft collects, how Microsoft uses it, and for what purposes.

The Online Services Terms (OST) is a legal agreement between Microsoft and the customer. The OST details the obligations by both parties with respect to the processing and security of customer data and personal data. The OST applies specifically to Microsoft's online services that you license through a subscription, including Azure, Dynamics 365, Office 365, and Bing Maps.

The Trust Center is a great resource for people in your organization who might play a role in security, privacy, and compliance.

The compliance documentation provides reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription.

Plan and Manage Azure cost

The TCO Calculator helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.

These costs include electricity, network maintenance, and IT labor.

You don't need an Azure subscription to work with the TCO Calculator.

Step 1: Define your workloads

- **Servers**
- This category includes operating systems, virtualization methods, CPU cores, and memory (RAM).
- **Databases**
- This category includes database types, server hardware, and the Azure service you want to use, which includes the expected maximum concurrent user sign-ins.
- **Storage**
- This category includes storage type and capacity, which includes any backup or archive storage.
- **Networking**

Step 2: Adjust assumptions
key operating cost assumptions across several different area

- Electricity price per kilowatt hour (KWh).
- Hourly pay rate for IT administration.

- Network maintenance cost as a percentage of network hardware and software costs.

Step 3: View the report
Choose a time frame between one and five years. the TCO Calculator generates a report that's based on the information you've entered. Here's an example:

types of Azure subscriptions
Free trial

Pay-as-you-go

Member offers

purchase Azure services
Through an Enterprise Agreement—annual billing,customized pricing

Directly from the web—monthly billing

Through a Cloud Solution Provider-- A Cloud Solution Provider (CSP) is a Microsoft Partner who helps you build solutions on top of Azure.

factors affect cost

Resource type -- They depend on the type of resource or how you customize it.

For example, with a storage account you specify a type (such as block blob storage or table storage), a performance tier (standard or premium), and an access tier (hot, cool, or archive). These selections present different costs.

Usage meters

Resource usage-eg, vm if deallocated, disks are billed

Azure subscription types—free tiral

Azure Marketplace—purchase third party services

Location

Zones for billing of network traffic

Bandwidth refers to data moving in and out of Azure datacenters. Some inbound data transfers (data going into Azure datacenters) are free. For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on *zones*.

Mimimise cost ways

Use Azure Advisor to monitor your usage

Ideally, you want your provisioned resources to match your actual usage.

Azure Advisor identifies unused or underutilized resources and recommends unused resources that you can remove. This information helps you configure your resources to match your actual workload.

Use spending limits to restrict your spending

Use Azure Reservations to prepay

Azure Reservations offers discounted prices on certain Azure services. Azure Reservations can save you up to 72 percent as compared to pay-as-you-go prices. To receive a discount, you reserve services and resources by paying in advance.

For example, you can prepay for one year or three years of use of VMs, database compute capacity, database throughput, and other Azure resources.

Choose low-cost locations and regions

Research available cost-saving offers

Keep up to date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

Use Azure Cost Management + Billing to control spending

Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use.

Apply tags to identify cost owners
Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure resources to organize billing data.

Resize underutilized virtual machines
A common recommendation that you'll find from Azure Cost Management + Billing and Azure Advisor is to resize or shut down VMs that are underutilized or idle.

Deallocate virtual machines during off hours

Delete unused resources

Migrate from IaaS to PaaS services

Save on licensing costs

a *service-level agreement* (SLA) is a formal agreement between a service company and the customer.

You can access SLAs from Service Level Agreements.

Note

You don't need an Azure subscription to review service SLAs.

A *service credit* is the percentage of the fees you paid that are credited back to you according to the claim approval process.

Free products typically don't have an SLA.

Azure status provides a global view of the health of Azure services and regions. If you suspect there's an outage, this is often a good place to start your investigation.

An *application SLA* defines the SLA requirements for a specific application. This term typically refers to an application that *you* build on Azure.

The Azure updates page provides information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements.