Azure

Cloud Computing :- It is a delivery of Computing Service.

- Over the Internet.
- Computing services include common IT infrastructures such as virtual machines, storage, databases and networking.

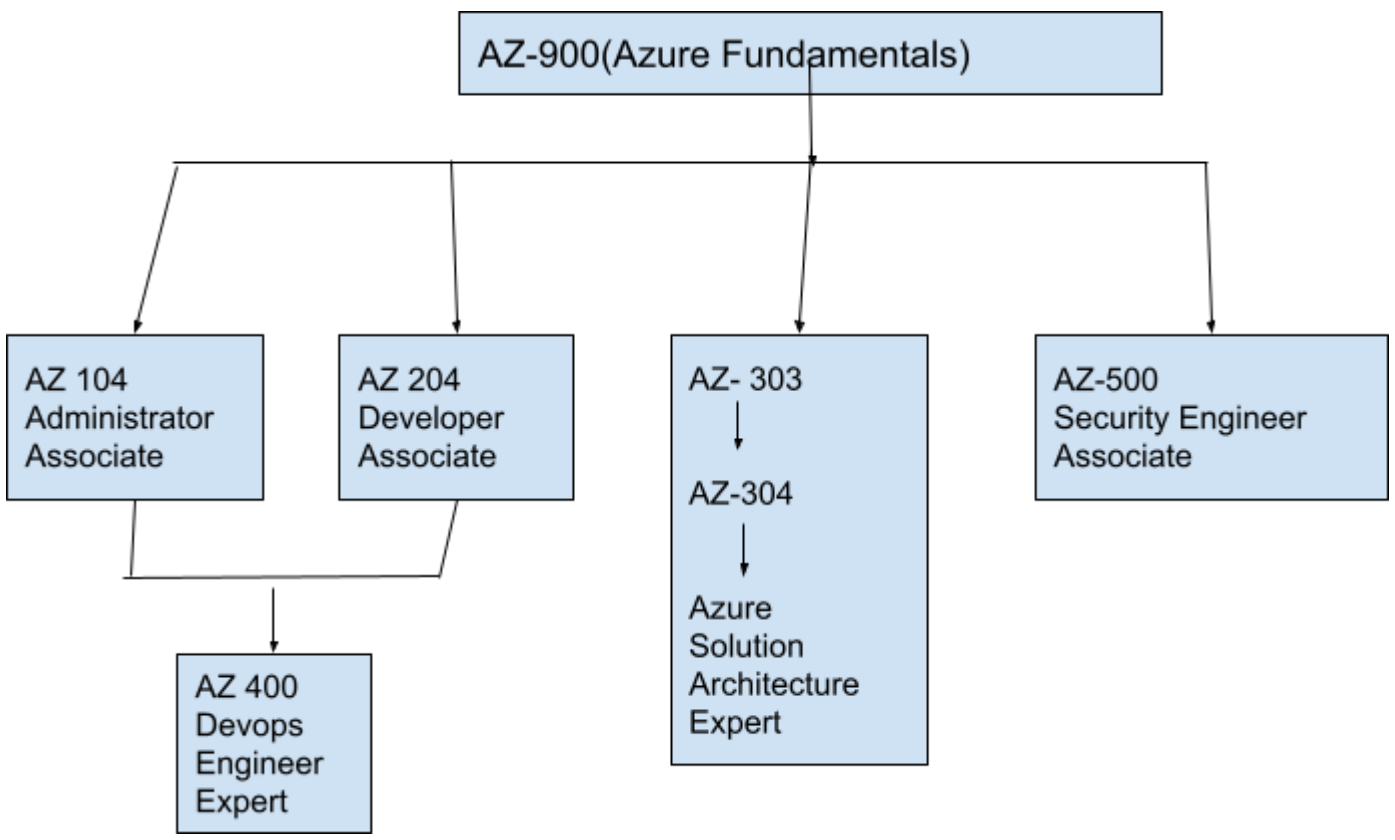
Resources Cloud Provide:-

1. Compute :- provide the computer power(memory & processor)
2. Networking:- Connecting of computer together to VM(Virtual Machine)
3. Storage:- Store of Data or information
4. Analytics:- How much memory required, kind of load etc.

(All service provide by internet)

Types of Clouds:-

PUBLIC CLOUD	PRIVATE CLOUD	HYBRID CLOUD
General public can host their service	Organization create a cloud environment in their data center	Now a days Organizations are adopting hybrid cloud, which is combination of public & private
Owned by cloud services or hosted provider	Organization is responsible for operating the services they provide.	Connecting existing datacenter to Azure datacenter via internet with the help of VPN Tunnel
Provide resources and services to multiple organization and user	Does not provide access to user outside organization	-
Example:- Azure	Disadvantage = cost	Application host on Azure datacenter and the database in client data center



Cloud Benefits

- High Availability
- Cost Savings
- Security
- Flexibility
- Mobility
- Insight
- Increased Collaboration
- Quality Control
- Disaster Recovery
- Loss Prevention
- Automatic Software Updates
- Competitive Edge
- Sustainability

Cloud- CAPEX & OPEX

CAPEX:- Capital Expenditure	OPEX:- Operational Expenditure
The upfront spending of money on physical infrastructure	Spend on products and services as needed, pay as you go
Costs from CAPEX have a value that reduce overtimes	Get billed immediately

Consumption-Based-Model:- Azure or any cloud service provider operates on a consumption-based model. Which means the end user pays for the resources that they use.

Whatever they use it, Is what they pay for

- Better cost prediction
- Price for individual resources and services are provided
- Billing is based on actual usage

CLOUD SERVICES (objective domain)

1. IaaS- Infrastructure-as-a-Service
2. PaaS- Platform-as-a-Service
3. SaaS- Software-as-a-Service

- Infrastructure-as-a-Service(IaaS):- In this model the host provides the user with cloud-hosted resources, such as storage space and virtualization.
  Examples: Amazon Web Services, DigitalOcean

- Platform-as-a-Service(PaaS):- In this model the host provides the user with a platform or a framework where they can develop, run and maintain their own applications, without having to build the whole infrastructure.
  Examples: Google App Engine, Red Hat OpenShift.

- Software-as-a-Service(SaaS):- In this model the host provides the user with a fully functional application hosted in a cloud and accessible through web browser or mobile application.
  Examples: Google Workspace, Dropbox.

Shared Responsibility Model:-

	Private	**Iaas**	**Pass**	**Saas**
Data & Access	**	**	**	**
Application	**	**	**	AZURE
Runtime	**	**	AZURE	AZURE
Operating System	**	**	AZURE	AZURE
Virtual machine	**	**	AZURE	AZURE
Compute	**	AZURE	AZURE	AZURE
Networking	**	AZURE	AZURE	AZURE
Storage	**	AZURE	AZURE	AZURE

**** :- Clinte are managing the responsibility**
AZURE :- Managed by Microsoft

Azure Function:- It is a code running your service and not the underlying platforms or infrasturcture. It creates infrastructure based on events.

Azure Logic: It is a cloud service that helps you to automate and orchastrate tasks, business processes and workforces, when you needed to integrate application, Data, Systems and Services.

AZURE SERVICES

Cloud Azure Services:- Azure services are divided into two parts

- Azure Architecture Components

    - Regions and Availability Zones
    - Subscription and Resource Group
- Azure Core- Resources
    - Compute
    - Network
    - Storage
    - Database

Azure Architecture Components:- Azure is an operating system, which manages a data center of microsoft. To manage below are the key architectural components:-

- Region’s & Region’s Pairs
- Availability Zone
- Azure Resource
- Resource Group
- Azure Resource Manager
- Subscription
- Azure Management Group

- Regions:- Azure offers more global regions that any other cloud provider with 60+ Regions representing 140+ Countries.
    - Regions are made up of one or more data center
    - Provide Flexibility and scale to reduce customer latency
    - Preserve data residency with a comprehensive compliance offer

    - **1 Region -> might be a collection of Zones**

    - Region Pairs:- For Availability , In the worst case scenario a complete region might be outage(might be due to nature problem or some disaster happen, Flood, Power outage). To avoid this problem statement a region-pairs is done where microsoft create a pair-zone to present data during such a disaster.
        - Both region should be in a same geographic location
        - At least 300 miles of separation between region pairs
        - Automatic replicate for some services
        - Prioritized region recovery in the outage

    - **Pairing are fixed, defined by Microsoft only**

- AVAILABILITY ZONES:-
  You want to ensure your services and data are redundant so you can protect your information in case of failure.
  When you are hosting your infrastructure, this requires creating duplicate hardware environments. Azure can help make your app highly available through Availability Zones.
    - Availability zones are physically separate data centers within an Azure region

AZURE CLOUD SHELL:-

Azure Cloud Shell is a browser-based command-line experience for managing and developing Azure resources.
Think of Cloud Shell as an interactive console that you run in the cloud.
Cloud Shell provides two experiences to choose from: Bash and PowerShell. Both include access to the Azure CLI, the command-line interface for Azure.
You can use any Azure management interface, including the Azure portal, Azure CLI, and Azure PowerShell, to manage any kind of VM

VIRTUAL MACHINE:-

A virtual machine, or VM, is a software emulation of a physical computer. A snapshot of a running VM is called an image. Azure provides images for Windows and several flavors of Linux. You can also create your own preconfigured images to make deployments go faster.
A virtual machine is defined by a number of factors, including its size and location. Before you bring up your VM, let’s briefly cover what’s involved.

More Control - With Azure VMs, Developers have more control over the development environment which is very helpful in case of building a highly secured architecture for a complex solution. Developers can choose an operating system, Networking, Storage connections etc. to build a sandbox solution.

Easy Diagnostics - Azure VMs provide the facility to troubleshoot issues with options like remote debugging, event logs, IIS logs, application logs etc.

Alerts - We can trigger actions and alerts based on metrics of computing resources consumed by VM.

Pricing - We can shut down and stop the VMs if not in use. A stopped VM will not incur any charge. Restarting the VM will maintain its state based on persistent disks.

Scaling - We can scale up/down and out/In the Virtual machines. Auto scale feature is also there to support based on some metrics. For example, scale out to 5 instances when CPU utilization is greater than 70% for more than 5 minutes.

Scale Sets - Virtual Machine Scale Sets are a group of VMs with identical configuration and will be managed by a load balancer.

Virtual Machine Prices:-
Azure VM has two kinds of pricing models - Pay as you Go and Reserved Virtual machine Instance.

Pay as you Go – This modal charge only for the time compute resource like Azure VM is used. It does not have any long-term commitment or any fixed monthly charges. We can scale out or even stop the VM in order to utilize efficiently and reduce bills.This kind of plan works for short term projects with unpredictable business requirements. Developers try out the stability of applications in this plan.

Reserved Instances – This plan brings an advanced purchase option for a reserved VM instance for a period of 1 or 3 years. With this, users get up to 72 % price savings than pay as you go plan. Reserved Virtual machines can easily be replaced with another one in case of any downgrade in performance. This plan suits with stable traffic on applications deployed on Azure VM. Software development with the fixed budget can prefer having a reserved Azure VM.

Virtual Networks:-

- You can create a virtual network in the cloud dedicated to your Azure account. It is the fundamental building block where you can launch Azure resources.
- Azure VNet is the networking layer of Azure VMs.
- A VNet spans all the Availability Zones in the region. After creating a VNet, you can add one or more subnets in each Availability Zone.

Key Concepts:-

- A virtual network (VNet) allows you to specify an IP address range for the VNet, add subnets, associate network security groups, and configure route tables.
- A subnet is a range of IP addresses in your VNet. You can launch Azure resources into a specified subnet. Use a public subnet for resources that need to connect to the Internet and a private subnet for resources that won't be connected to the Internet.
- To protect the Azure resources in each subnet, use network security groups.

VNet Use Case
- VNet with a single public subnet.
- VNet with public and private subnets (NAT).

Subnets
- When you create a VNet, you must specify a range of IPv4 addresses for the VNet in the form of a CIDR block (example: 10.0.0.0/16).
- A CIDR block must not overlap with any existing CIDR block that's associated with your VNet.
- You can add multiple subnets in each Availability Zone of your VNet's region.
- Types of subnets:
    - Public subnet
    - Private subnet
    - Gateway subnet

- The CIDR block size of an IPv4 address is between a /16 netmask (65,536 IP addresses) and /29 netmask (8 IP addresses).
- The 5 reserved addresses in each CIDR block are not available for you to use, and cannot be assigned to any virtual machines.
- You can delegate a subnet to be used by a dedicated service.

VNet Components
- NAT Gateway
    - Allows your virtual network resources to have an outbound-only connection.
    - A NAT gateway resource can use up to 16 static IP addresses.
    - You can use multiple subnets in a NAT gateway.
- Route tables are used to determine where network traffic is directed.
    - A subnet can only be associated with one route table.
    - If multiple routes contain the same address prefix, the selection will be based on the following priority: User-defined route, BGP route, and System route.
- You can connect VNets to each other using VNet peering.
- If you need to connect privately to a service, you can use Azure Private Endpoint powered by Azure Private Link.

VNet Peering

- Allows you to connect two virtual networks seamlessly. You can:
    - Connect virtual networks in the same Azure region known as virtual network peering.
    - Connect virtual networks across different Azure regions known as global virtual network peering.
- Ensure that your VNet address ranges do not overlap with one another. Plan accordingly before initiating the peer.

Azure Virtual Network Pricing

- You are charged for the public IP address and reserved IP address inside your VNet.
- You are charged for the ingress and egress data of VNet Peering.
- You are charged for the NAT gateway resource hours and data processed (per GB).

Azure Storage:-

Azure Storage is the cloud storage solution for modern applications that rely on durability, availability, and scalability to meet the need of their customers.

- The very first thing you need to use storage in azure is a storage account.
- To use any storage type in Azure, you first have to create an account in Azure. After creating an account, you can transfer data to or from services in your storage account. Create a storage account to store up to 500 TB of data in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed.

A storage account can be of two types:

1. General Purpose
2. Blob Storage

General Purpose

A general purpose storage account provides a space where it gives you access to blobs, queues, files and tables, all of these services in a unified account. A general-purpose storage account can be used to store object data, can be used as a NoSQL data store, can be used to define and use queues for message processing, and set up file shares in the cloud. You can get a better understanding with the Azure Course.

As mentioned, primarily there are 4 types of storage types in azure:

- Tables
- Blobs
- Queues
- File Storage

Tables - The Azure Table storage service stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data.

Blobs - Blob storage is a service that stores unstructured data in the cloud as objects/blobs. Blob storage can store any type of text or binary data, such as a document, media file, or application installer. Blob storage is also referred to as object storage.

Queue - Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world via authenticated calls using HTTP or HTTPS. A single queue message can be up to 64 KB in size, and a queue can contain millions of messages, up to the total capacity limit of a storage account.

File Storage - A File Storage share is an SMB file share in Azure. All directories and files must be created in a parent share. An account can contain an unlimited number of shares, and a share can store an unlimited number of files, up to the 5 TB total capacity of the file share.

Blob Storage

Blob storage accounts are specialized in storing blob data and can also be used to choose an access tier, which allows you to specify how frequently data in the account is accessed. You can choose an access tier suitable for your storage and which suits your expenses. You can learn more from the Microsoft cloud engineer certification.

There are two types of access tier:

Hot: This access tier grants us the lowest latency possible. Hence, it should be used with data which is frequently accessed. Naturally, since it offers low latency it is more expensive.

Cold: This access tier is less in performance than the “Hot” access tier i.e offers higher latency than the former access tier. That being said, it comes with a lesser price tag and hence can be used for data which is less frequently accessed.

Azure Networking & Content Delivery

Azure Application Gateway

- A web traffic load balancer.
- It allows you to distribute incoming traffic based on HTTP request properties such as URL and host headers.
- Application gateway has four tiers: Standard, Standard V2, WAF, and WAF v2
- You can use the same application gateway for up to 100+ websites with multi-site hosting.

- Set the minimum and maximum scale units based on your needs.
- Azure Application Gateway vs Azure Load Balancer
    - An application gateway operates at layer 7.
    - A load balancer functions at layer 4.
- You can use both public and private IP on the frontend.

Azure Content Delivery Network

- A distributed network of servers that delivers web content closer to users.
- CDNs store cache content on edge servers to minimize end-user latency.

Azure DNS

- Enables you to host your DNS zone and manage your DNS records.
- DNS zone allows you to configure a private and public DNS zone.
- Alias recordsets:
    - A – maps the host to IPv4.
    - AAAA – maps the host to IPv6.
    - CNAME – create a record to point to another domain.
- A limit of 20 alias record sets per resource.
- Uses Anycast networking to route users to the closest name servers.
- You can monitor your DNS zone metrics using Azure Monitor.
    - QueryVolume – query traffic received.
    - RecordSetCount – the number of recordsets in your DNS.
    - RecordSetCapacityUtilization – percentage of utilization of your recordset capacity.
- Azure Private DNS allows you to use your custom domain name in your private VNet.
- Alias record allows you to point your naked domain or apex to a traffic manager or CDN endpoint

Azure ExpressRoute

- Enables you to establish a private connection between your on-premises data center or corporate network to your Azure cloud infrastructure.
- More secure, reliable, and faster than conventional VPN connections.
- Supports dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP). The connection is redundant in every peering location for higher reliability.

Azure Front Door

- A service that uses Microsoft's global network to improve the availability and performance of your applications to your local and global users.
- It works at the HTTP/HTTPS layer and uses a split TCP-based anycast protocol to ensure your users connect to the nearest Front Door point of presence.
- Supports a range of traffic-routing methods and backend health monitoring options for various application needs and automatic failover models.
- With URL-based routing, it routes the traffic to backend pools based on URL paths of the request.
- You can configure more than one website on the same Front Door with multiple-site hosting.
- Use cookie-based session affinity to redirect the user session to the same application backend.
- Redirect traffic based on protocol, hostname, path, and query string with URL redirect.
- URL rewrite allows you to configure a Custom Forwarding Path that will copy any part of the incoming path that matches a wildcard path to the forwarded path.
- Front Door supports end-to-end IPv6 connectivity and HTTP/2 protocol.

Azure Load Balancer

- Distributes incoming network traffic across multiple targets.
- Allows you to route traffic based on source IP address and port to a destination IP address and port.

Azure Traffic Manager

- A DNS-based traffic load balancer.
- Improves the responsiveness of your applications by sending the request to the closest endpoint.
- It offers a range of traffic-routing methods and endpoint monitoring options.

Azure VPN Gateway

- A secured hybrid cloud architecture.
- It is composed of gateway subnet, tunnel, and on-premises gateway.
- Protocols: Internet Protocol Security (IPsec) and Internet Key Exchange (IKE)
- VPN gateway connections: VNet-to-VNet, Site-to-Site, and Point-to-Site
    - Create a secure connection from your on-premises network to an Azure virtual network with a site-to-site VPN.
    - VNet-to-VNet connection automatically routes to the updated address space, if you updated the address space on the other VNet.
    - If you need to establish a connection to your virtual network from a remote location, you can use a point-to-site (P2S) VPN.
- You can also have one VPN gateway with more than one on-premises network using a Multi-Site connection

Azure Database Services

Azure Cosmos DB

- Globally distributed database that supports NoSQL.
- A fully-managed database service with turnkey global distribution and transparent multi-master replication

Azure Database Migration Service

- Accelerates the migration of your data to Azure.
- Enables seamless migrations from multiple database sources.
- To perform an online migration, you need to create an instance based on the premium pricing tier.

    - Features
        - Migrates your database and server objects with minimal downtime.
        - Supports Microsoft SQL Server, MySQL, PostgreSQL, MongoDB, and Oracle migration to Azure from on-premises and other cloud providers.
        - You can use DMS for both operational database and data warehouse migrations.
        - Automate the migration of data with Azure PowerShell.
        - Use Azure Migrate to discover your on-premises data estate and assess migration readiness.
        - You can create up to 2 DMS services per subscription.

Azure Database for MySQL and PostgreSQL

- PaaS relational database services
- Mitigate database downtime with high availability, redundancy, and resiliency capabilities.
- Enables you to scale vertically when needed.
- Receive alerts based on the metrics of your servers.
- Protect sensitive data at rest and in transit.
- Automated backups, up to 35 days.
- PostgreSQL deployment options: Single Server and Hyperscale (Citus)
- Single server pricing tiers: Basic, General Purpose, and Memory Optimized.
- Basic – light compute and I/O performance workloads.
- General Purpose – a balanced compute and memory with scalable I/O throughput workloads.
- Memory Optimized – for high performance database workloads requiring in-memory performance.

    - PostgreSQL – Hyperscale (Citus)
        - Sharding – scales horizontally across multiple machines.
        - Supports query parallelization for faster responses on large datasets.
        - Primarily used for multi-tenant applications, real-time operational analytics, and high throughput transactional workloads.

Azure SQL

- A fully managed database built upon the SQL Server engine.
- SLA durability up to 99.995%.
- SQL Databases Resource type:
    - Single Database – offers serverless and hyperscale storage (up to 100TB).
    - Elastic Pool – a collection of databases with a shared set of resources.
    - Database Server – manage groups of single databases and elastic pools.

- SQL Managed Instances are for migrations “lift-and-shift” to the cloud.
    - The features of both SQL Server database engine and Azure SQL are available in SQL Managed Instance.
        - PaaS benefits – Azure will handle all infrastructure management.
        - Business continuity – the data are protected with automated backups.
        - Security and compliance – supports native VNet implementation and it is exposed only through a private IP address.
        - Management operations – automatically deploy new instances, update instance properties, and delete instances that are no longer needed.
    - Automate the migration of existing SQL Server instance to SQL Managed Instance with Azure Data Migration Service
    - Azure Hybrid Benefit for SQL Server allows you to exchange existing licenses to get discounted rates on SQL Managed Instance.

- SQL Virtual Machines are used for applications requiring OS-level access.
- Endpoint: <server_name>.database.windows.net
- vCore-based service tiers:
    - General Purpose is for common workloads.
    - Hyperscale is appropriate for online transaction processing (OLTP) and hybrid transactional analytical workloads (HTAP).
    - Business Critical is best for OLTP applications with high transaction rates and low IO latency.
- Azure Hybrid Benefit for SQL Server enables you to use your SQL Server licenses to pay a reduced rate on Azure SQL.
- Azure Data Studio is a modern cross-platform database tool with customizable code snippets, lightning-fast, useful peek definitions, and an integrated terminal to run other SQL tools.

Azure Security Services

Advanced Threat Protection (ATP)

- Enables you to identify, detect, and investigate advanced threats in your organization.
- Allows you to monitor user activities and information.
    - Identify and investigate advanced threats throughout the entire cyber-attack kill chain:
    - Reconnaissance – identify attempts by attackers to gain information.
    - Compromised credentials – any attempts that compromise user credentials shall be detected.
    - Lateral movements – attacks to gain access to sensitive accounts.
    - Domain dominance – the attacker has the credentials to access your domain controller.
    - Exfiltration – unauthorized data transfer.

Azure Active Directory

- An identity and access management service that helps you access internal and external resources.
- Azure AD licenses: Free, Premium P1, Premium P2 and Pay as you go
    - Free – user and group management in your on-premises directory
    - Premium P1 – allows access to both on-premises and cloud resources.
    - Premium P2 – provides an additional feature called Azure AD Identity Protection.
    - Pay as you go – offers a feature called Azure AD B2C.

Azure DDoS Protection

- Allows you to protect your Azure resources from denial of service (DoS) attacks.
- DDoS protection (layers 3 and 4) offers two service tiers: Basic and Standard.

Azure Firewall

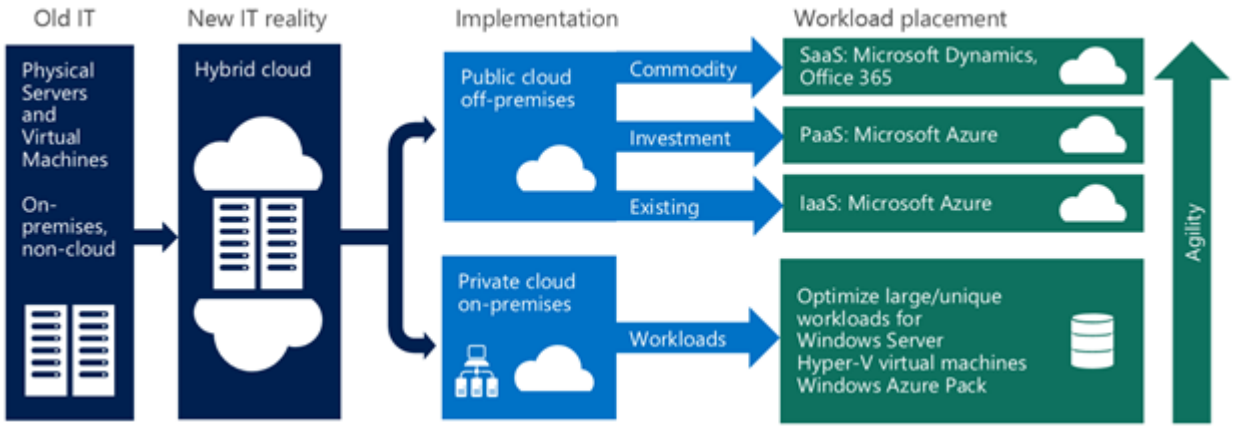
- A service that uses a static public IP address to protect your VNet resources.
- Azure Firewall is PCI, SOC, ISO, ICSA Labs, and HITRUST compliant.

Azure Key Vault

- A service that allows you to store tokens, passwords, certificates, and other secrets.
- You can also create and manage the keys used to encrypt your data.

Useful Diagrams:-

	IaaS	PaaS	SaaS
Costs	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay a subscription, typically on a monthly or annual basis.
User Responsibility	Purchase, installation, configuration, and management of their own software, operating systems, middleware, and applications.	Custom development of their own applications. Allows the user to focus on the application or workload they want to run. Not responsible for managing the underlying server or infrastructure.	Users just use the application software Not responsible for any maintenance or management of the underlying software.
Cloud Provider Responsibility	Ensures that the underlying cloud infrastructure *(such as virtual machines, virtualization, storage, and networking)* is available for the user.	Operating system management, network, and service configuration. Typically responsible for everything apart from the application that a user wants to run. Provide the user a complete managed platform on which to run the application.	Provision, management, and maintenance of the application software.
Examples	Azure Virtual Machines	Azure Storage Azure SQL Databases Azure App Service	Office 365, Skype, and Dynamics CRM Online



	IaaS	PaaS	SaaS
Examples	Azure Virtual Machines	Azure Storage Azure SQL Databases Azure App Service	Office 365 Dynamics CRM Online Skype