WHIZLABS

Microsoft Azure: AZ-900 Certification

Whizcard

Quick Bytes for you before the exam!

The information provided in WhizCards is for educational purposes only; created in our efforts to help aspirants prepare for the Microsoft Azure Exam AZ-900 certification. Though references have been taken from Azure documentation, it's not intended as a substitute for the official docs. The document can be reused, reproduced, and printed in any form; ensure that appropriate sources are credited and required permissions are received.

Index

Fundamentals of Cloud Computing..... 2

- What is Cloud Computing?..... 2
- On-premises vs. Cloud..... 2
- Why Cloud?..... 2
- Advantages of Cloud Computing... 3
- Cloud Computing Services..... 4
- Cloud Computing Models..... 6
- Shared responsibility Model..... 6
- Consumption-based Model..... 7
- Cloud Pricing Models 8

Azure Core Architectural Components 9

- What is Azure?..... 9
- Azure regions, Region pairs, and Sovereign regions 9
- Azure Availability Zones and Datacentres.... 10
- Azure Resource and Resource groups..... 11
- Azure Subscriptions and Management groups .. 11

Azure Compute and Networking Services.... 13

1. Azure Virtual Machines..... 13

- Azure Compute Types..14
- Azure Availability Sets and Azure Virtual Machine Scale Sets.... 14
- Azure Virtual Desktop.... 15
- Application Hosting Options in Azure..... 15

2. Azure Virtual Networks..... 16

- Azure DNS..... 16
- Azure VPN Gateway and ExpressRoute.. 17
- Azure Public and Private Endpoints ... 18

Azure Storage Services..... 19

- Comparison Table for Azure Storage..... 20
- Azure storage tiers and Redundancy options 20
- Identify Azure File Movement Options... 22
- Azure Data Migration Options... 22

Azure identity, access, and security..... 23

- Microsoft Entra..... 23
- Azure Active Directory (Azure AD) ... 23
- Azure Authentication Methods.... 24
- External Identities and Guest access in Azure ... 25
- Azure AD Conditional Access..... 26
- Azure Role-Based Access Control (RBAC)... 27
- Microsoft Defender for Cloud..... 27
- Zero Trust & Defense in Depth model ... 28

Azure Cost Management..... 29

- Factors affecting costs in Azure.... 29
- Azure Cost Management and Billing tool... 29
- Azure Pricing, Budgets and Tags ... 30
- Azure Pricing and TCO Calculator... 30

Monitoring Tools in Azure...31

- Azure Advisor & Service Health..... 31
- Azure Monitor & Monitor alerts.. 31
- Log Analytics & Application Insights..... 33

Features and Tools for managing and deploying Azure resources.... 34

- Azure Portal 34
- Azure PowerShell, CLI and CloudShell 34
- Azure Arc.... 35
- Azure Resource Manager and Resource Manager Templates.... 35

Governance and Compliance in Azure... 37

- Azure Locks and Policies.... 37
- Azure Blueprints.... 37
- Microsoft Service Trust Portal..... 38

Extra Learning..... 39

- Azure Core Solutions 39
- Security features in Azure 40
- Azure Service Level Agreement 42

Fundamentals of Cloud Computing

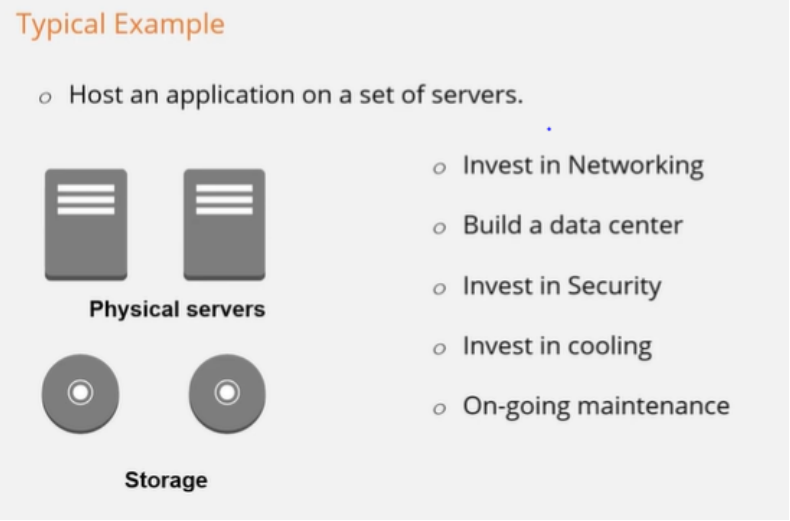
What is Cloud Computing?

Cloud computing transmits computer services via the Internet (the cloud) to enable faster innovation, more flexible resources, and scale economies. You typically only pay for the cloud services you use, which allows you to save money, better manage your infrastructure, and expand as your company develops.

On-premises vs. Cloud

If you wish to be on-premises, you must make significant upfront investments in servers, storage, security, and a place for a data center, among other things.

This is known as **Capital Expenditure(CapEx)**, which many businesses cannot afford in the first place. There are many additional drawbacks for on-premises, such as no scalability, no disaster recovery, and so on, which we will explore more.



Reference: Whizlabs AZ-900 OC #4

Why Cloud?

The supply of computer services via the internet utilizing a pay-as-you-go pricing mechanism is known as cloud computing. You usually just pay for the cloud services you utilize, which allows you to do things like

- Reduce your operational expenses.
- Improve the efficiency of your infrastructure.
- Scale up or down as your company's requirements vary.

To put it another way, cloud computing uses someone else's data center to rent computing power and storage.

You may handle cloud resources the same way you would your local data center's resources. You return them after you've finished using them. You are only charged for what you use. This is called **Operational Expenditure(OpEx).**

You rent CPUs and storage when you need them rather than keeping them in your data center. The cloud provider maintains the underlying infrastructure for you. You may utilize the cloud to rapidly solve your most difficult business problems and provide cutting-edge solutions to your users.

Advantages of Cloud Computing

High Availability

High availability is the quality of a computing infrastructure that allows it to continue functioning even if some of its components fail. It is the ability to keep resources available for longer periods of time. Azure provides high availability for most of its resources.

(Reference: Microsoft Docs)

Scalability

Scalability refers to the ability to adjust resources according to demand. If you suddenly experience peak traffic and your systems are overwhelmed, you can add more resources to handle the increased demand.

Manageability

It is the major benefit of cloud computing. There are two types of manageability for the cloud:

Management of the cloud means managing your cloud resources.

- Automatically scaling resource deployment based on need.
- Deploy resources based on a preconfigured template,
- Monitor the health of the resources and automatically replace failing resources.
- Receive automatic alerts based on configured metrics

Management in the cloud means how you're able to manage your cloud environment and resources. You can manage the resources through a portal, using a **command line interface (CLI), APIs, and PowerShell.**

Elasticity

It is also known as the automatic scaling of resources. It has the ability to dynamically scale resources(like recovering from failures and continuing to function)

Predictability

Predictability in the cloud lets you move forward with confidence. It is focused on performance predictability or cost predictability.

Both performance and cost predictability is heavily influenced by the Microsoft Azure Well-Architected Framework.

Security and Governance

- Security governance connects your business priorities with technology implementation such as architecture standards and policy.
- Governance teams provide oversight and monitoring features to maintain and improve security posture over time. These teams also report compliance needed by regulatory bodies.
- Depending on your operating model, software patches and updates may also be automatically applied, which helps with both governance and security.

Cloud Computing Services

Software as a service (SaaS):

- With this service, you don't need to download or install any software on your PC.
- As with many cloud services, it can be accessed through the internet via a web browser.
- The cloud vendor manages everything. You simply need to concentrate on how you can get the most out of it.
- Examples of SaaS: *Office 365, Google docs, Google sheets, DropBox, etc.*
- Users*: End Customers*

Platform as a service (PaaS):

- It's a service that lets clients maintain and develop applications without worrying about the underlying infrastructure.
- In this service, the cloud vendor manages infrastructure, operating system, middleware, etc.
- Example of PaaS: *Heroku, Google App Engine, Azure Web Apps, OpenShift*
- Users - *Developers*

Infrastructure as a Service(IaaS):

- It's a service that provides key computation, storage, and networking resources on demand but in a virtual environment.
- The cloud vendor manages the infrastructure in this service, but the User itself manages the operating system, middleware, runtime, etc.
- Examples: DigitalOcean, AWS, Microsoft Azure, Azure VMs, Google Cloud Platform
- Users: *System administrators*

Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)

IaaS vs. PaaS vs. SaaS

	IaaS	PaaS	SaaS
Who uses it	System administrators	Developers	End users
What users get	Virtual data center to store information &create platforms for services and app development, testing, and deployment	Virtual platform and tools to create, test and deploy apps and services	Web software and apps to complete business tasks
Provider controls	Servers Storage Networking Virtualization	Servers Storage Networking Virtualization os Middleware Runtime	Servers Storage Networking Virtualization os Middleware Runtime Applications Data
User controls	OS Middleware Runtime Applications Data	Applications Data	- - - -

Cloud Computing Models

Public Cloud:

- In this kind of cloud, the whole infrastructure is situated at the cloud vendor aka the business that sells its services to the general public.
- In the case of the public cloud, we just need to go to the website of the relevant cloud provider and build or administer the resources.
- Others can use the resources that we previously utilized once we destroy them.

  Examples:- Microsoft Azure, Amazon Web Services,

Private Cloud:

- This type of cloud is similar to a public cloud, but the difference is that the infrastructure and requirements are reserved for just a single organization only.
- The resources are isolated and can't be used by other organizations.
- The cloud can be located on-premise as well.

  Examples:- Azure stack, Amazon private cloud

Hybrid Cloud:

This is a combination of public cloud and private cloud. This is much more complex than public or private clouds. In this type of cloud

- The public cloud is used for non-critical tasks.
- The private cloud is used to carry out critical tasks.

Shared Responsibility Model

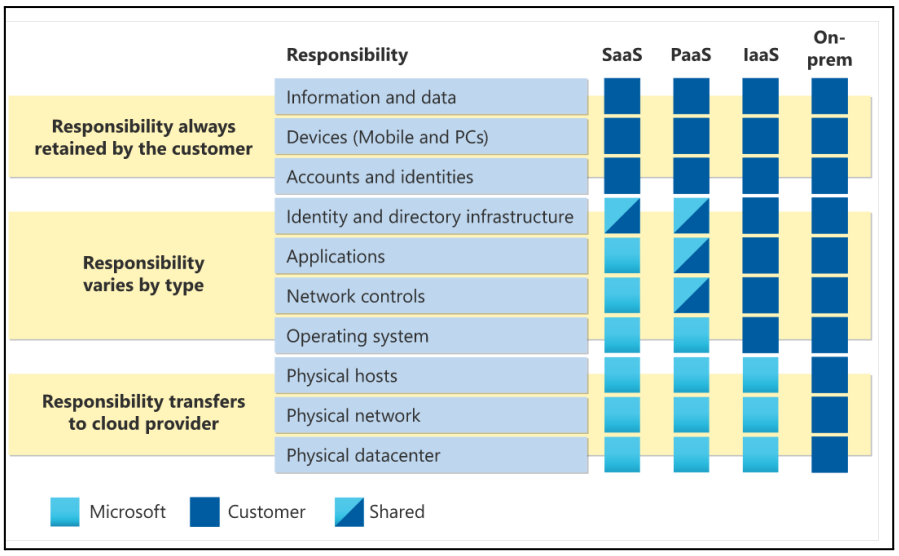
In the traditional infrastructure,

- Company is responsible for maintaining the physical space, security, and maintaining servers and infrastructure, and replacing servers.
- The IT department is responsible for maintaining all the infrastructure and software required to keep the datacentre up and running and keeping all systems patched to the correct version.

With Shared Responsibility Model, the responsibilities like Physical Infrastructure, Security, and Softwares updates get shared between the cloud provider and the consumer.

Cloud Provider is responsible for - Physical Infrastructure (security, power, cooling, and network)

Consumer is responsible for - Data and information stored in cloud & managing security access.



(Reference: Microsoft Docs)

Consumption-based Model

When comparing IT infrastructure models, there are two types of expenses to consider.

Capital Expenditure (**CapEx**) and Operational Expenditure **(OpEx).**

- **CapEx** is defined as funds used by **organizations to obtain, upgrade, and maintain physical assets such as data centers**. Ex: Building a datacentre, buying a company vehicle & repaving the parking lot.
- **OpEx** is defined as funds **used by organizations for their day-to-day operations.**
  Ex: Renting a building, leasing a company vehicle, or signing up for cloud services**.**

CapEx vs OpEx

Objective	Capital Expenditure(CapEx)	Operational Expenditure(OpEx)
Purpose	Assets intended to benefit the organization for more than one year	Ongoing expenses to run the day-to-day business
The way of purchasing	One-time purchase	Pay-as-you-go approach
Accounting treatment	Can't be fully deducted in the accounting period. They are depreciated or amortized over time.	Fully deducted in the accounting period.
Examples	Purchasing office buildings, equipment, vehicles, intellectual property assets	Consumables, wages, rent, maintenance, and repair of machinery

Note: Cloud computing falls under **OpEx** because it operates on a **Consumption-based model.**

--Back to Index--

Benefits of the consumption-based model:

- There's no need for upfront costs.
- Users don't have to buy & maintain the expensive infrastructure that isn't used to its full potential.
- Ability to pay for more resources when needed.
- Ability to stop paying for resources no longer needed.

Cloud Pricing Models

Microsoft offers three main pricing models for Azure-cloud resources:

Pay-as-you-go pricing model: You only pay for the cloud services you use most often and it helps

- Plan and manage your operating costs.
- Run your infrastructure more efficiently.
- Scale as your business needs change.

Instead of maintaining CPUs and storage in your data center, you can rent CPUs, storage, and more as and when you need them. The cloud provider takes care of managing the underlying infrastructure for you.

Azure Reservations:

- Azure Reservations help you save money by committing to one-year or three-year plans for multiple products. Azure Reservation is a long-term contract for a variety of Azure services.
- You pay the money monthly or in full upfront, but you can make almost 72% profit compared to pay-as-you-go pricing.
- This is good for businesses that have similar usage patterns most of the time.

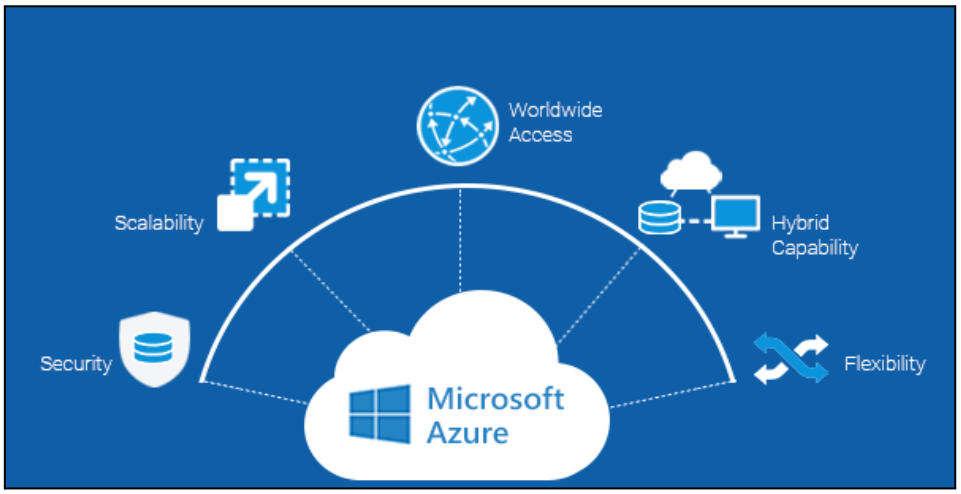
Azure Spot Instances:

- These make use of Microsoft's leftover Compute Capacity.
- You can save almost 90% compared to pay-as-you-go pricing, but you should use Spot Instances for mostly stateless periodic workloads.
- This suggests that they should only be used when stopping in the middle of work is not a problem.
- Azure Spot instances - not suitable for a production-based environment.

Azure Core Architectural components

What is Azure?

- Azure is one of the largest cloud service providers in the world.
- It offers you the flexibility to use your preferred tools and frameworks to *create, manage, and deploy apps on a large global network.*
- Azure's ever-expanding nature makes it one of the finest on the market, and it is also provided by one of the biggest and most famous MNCs in Microsoft.
- Azure provides a wide range of services, *including computing resources, networking resources, serverless computing, and many more.*



Reference:- Microsoft Docs

Azure regions, Region pairs, and Sovereign regions

Azure Regions:

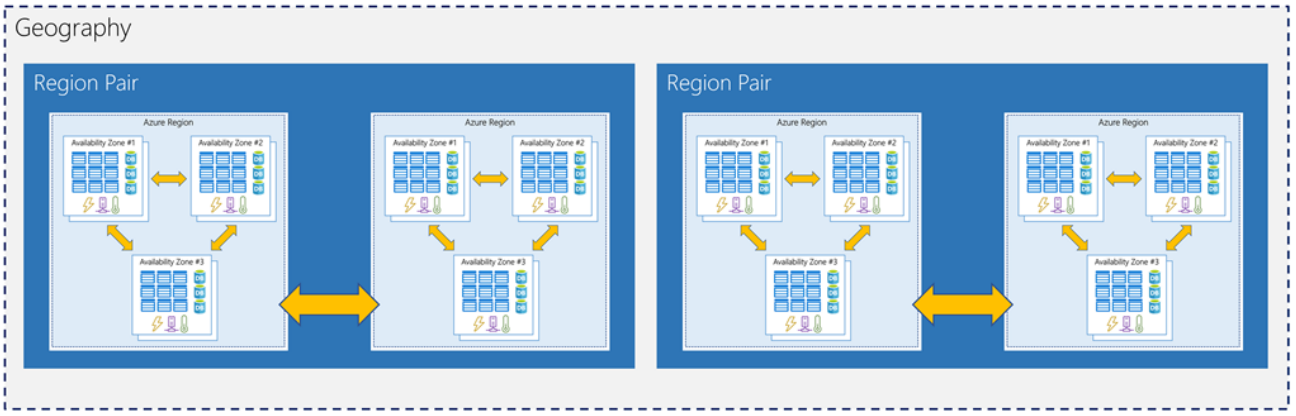
- A region is a geographical location on the globe with at least one, but possibly many, data centers close by and connected by a low-latency network.
- When you create a resource in Azure, you must define the location/region to which it should belong. There are a few exceptions, such as Azure DNS, but generally, all resources must be created with a location specified.
- Azure makes it simple to select the data center and regions appropriate for you and your clients, with more announced regions than any other cloud provider (60+).

Azure Region Pairs:

Azure Region Pair is a relationship between two Azure Regions within the same geographic location for disaster recovery purposes.

- Azure regions are paired with other regions in the same geography at least 300 miles away.
- This approach allows for the replication of resources across geography to help mitigate disruptions due to events such as natural disasters, civil unrest, power outages, or physical network outages affecting the entire region.

Ex: if a region in a pair was affected by a natural disaster, services would automatically failover to the other region(2nd Region) in its region pair.



(Reference: Microsoft Docs)

Sovereign Regions:

- Azure Sovereign regions are dedicated to specific sovereign entities.
- These cloud regions are isolated in-country platforms with independent authentication, storage, and compliance requirements.
- They are not necessarily managed by Microsoft and may be restricted to certain types of customers.
  Examples: Azure China 21Vianet, Azure Germany, Azure Government - the US, Australia

Azure Availability Zones and Datacentres

Azure Availability Zones

- Within an Azure region, availability zones are physically distinct data centers.
- Each availability zone comprises one or more data centers that are self-contained in terms of power, cooling, and networking.
- Availability zones are connected through high-speed, private fiber-optic networks.
- The goal of having more than one availability zone in a region is to allow data to be redundantly stored in more than one availability zone, ensuring that even if a data center fails, it does not affect our resources.

Azure Datacentres

- Datacentres are unique physical buildings like a group of networked computer servers.
- It contains a number of physical servers with their own power, cooling, & networking infra.
- Individual datacentres aren't directly accessible.
- Azure Datacentres are grouped into Azure Regions/Availability Zones that are designed to help you achieve resiliency and reliability for your business-critical workloads.

Azure Resources and Resource groups

Azure Resources:

- A resource is something that is used to manage services in azure.
- At any one moment, a resource can only be in one resource group.
- The final component in the Azure architectural hierarchy is the resource.
- A resource group and a resource can be in two different locations; there is no restriction.

Azure Resource Group:

- A resource group is the next level in the hierarchy of Azure Architecture. A resource group is the logical mapping of the resources.
- For Creating Any Resource, you need a resource group.
- An Azure Management group is optional. However, azure resource groups and subscriptions are required. Resource groups can't be nested.

Azure Subscriptions and Management Groups

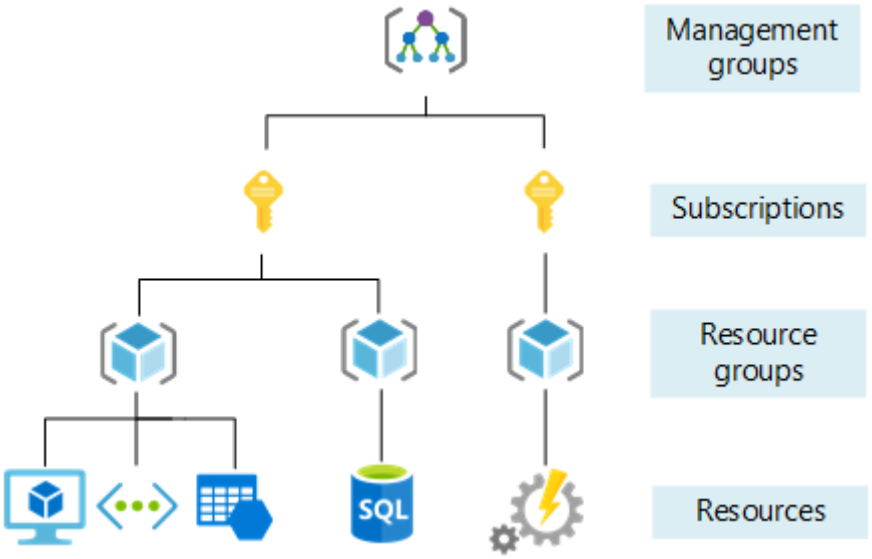
Azure Subscriptions

- As the name implies, a subscription is a logical entity that grants access to deploy and consume Azure resources.
- A resource may be anything from a virtual machine to a storage account or something that's related to networking.
- Almost anything in Azure can be utilized as a resource.
- A subscription is something that can be purchased and used for a certain amount of time. The same is true for Azure subscriptions.

Azure Management Groups

- A company may use Azure management groups to govern and *manage access, compliance, and rules* for their subscription inside their tenancy.
- An azure management group comes above the azure subscription in the hierarchy of management of resources in Azure.
- A subscription can only have one management group.

Hierarchy of Management Groups, Subscriptions, Resource Groups, and Resources



(Reference: Microsoft Docs)

Azure Compute and Networking services

Azure Virtual Machines

Virtualization

- In general, virtualization refers to the process of simulating something.
- The technique of operating a virtual instance of a computer system in a layer separate from the real hardware is known as virtualization.
- It most often refers to the use of several operating systems on a computer system at the same time.
- So, if you have a Windows computer, you may run a Linux-based operating system in a Windows virtual machine by using technologies like VMware, which supports Virtualization.

Azure Virtual Machines (Infrastructure as a Service)

1. Azure Virtual Machines are an IAAS offering
2. Azure Virtual Machine:
    a. *Are cost-effective*
    b. *Multiple resources are created along with VM when created*
    c. *Users can choose from a variety of available configurations and OS as per their requirements.*

With regular use of a Linux operating system through virtualization, one must download software such as VMware and certain files linked to the Linux OS itself, but this is not the case for Azure Virtual Machines, which can be run in the cloud itself.

We don't need to download any hefty software since we can connect to the VM directly in many ways. Two of those ways are:-

- Using Remote Desktop Connection (RDP)
- Using Azure Bastion Service

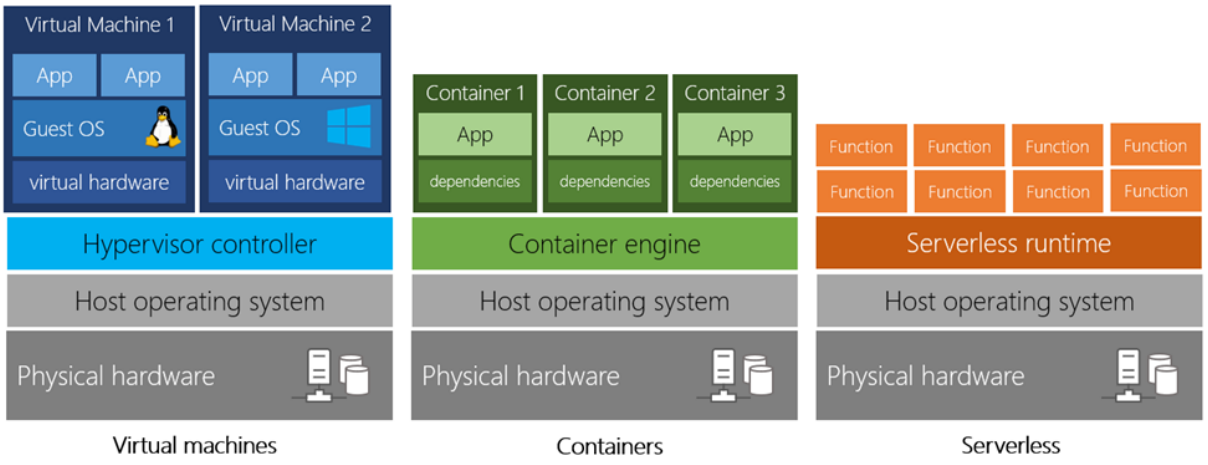
A public IP address is assigned to the virtual machine for it to communicate with the internet.

It's important to know how virtual machines are created in azure. For that, please refer to the link given below.

Quickstart - Create a Windows VM in the Azure portal - Azure Virtual Machines | Microsoft Docs

Azure Compute Types

Containers vs. Virtual machines vs. Functions



Containers provide an easy way to run batch jobs without having to manage the Infrastructure (environment and dependencies.)

Virtual machines are used to host applications when the customer requires more control over the computing environment

Functions is a serverless solution that allows you to write less code, manage less infrastructure and save costs.

Azure Availability Sets and Azure Virtual Machine Scale Sets

Virtual Machine Availability Sets (VM AS)

Availability set is a way of providing high availability within a datacentre. To protect your resources from rack/server failures you can place your VMs in an availability set.

By placing your VMs in an AV set, they will be distributed across multiple racks and servers to avoid hardware-level issues impacting your VMs.

Fault Domains - Rack level protection.

It helps to protect against physical power or network-related failures.

Update Domains - Server-level protection.

It helps protect against the few general updates, and patches for servers.

- You need to pay for VM that you create, not for the Availability Set.
- Availability Set has 99.95% Azure SLA.

Virtual machine scale sets (VMSS)

- Azure Virtual machine scale sets means - you can create and manage a group of identical and load-balanced virtual machines.
- It can increase the number of virtual machine instances across availability zones based on demand.
- Easy to create and manage multiple VMs.
- Optimize costs by reducing the number of redundant VM instances running your application when demand is low.

Azure Virtual Desktop (AVD)

Azure Virtual Desktop is a desktop virtualization and application virtualization service that runs on the cloud and enables users to use a cloud-hosted version of Windows (Windows 10 and 11 desktop versions) from anywhere in the world.

- It works on Windows, Mac, Android, and Linux devices.
- It works with apps that we can use to access remote desktops and most modern browsers.
- No additional license costs for Azure Virtual Desktop are required, it can be used with the existing Microsoft 365 or Windows per-user license.

Resources required for the Virtual Machines(VMs):

- Size (purpose, number of processor cores, and amount of RAM)
- Storage disks (hard disk drives, solid state drives, etc.)
- Networking (virtual network, public IP address, and port configuration)

Application hosting options in Azure:

Azure offers multiple ways to host applications depending on the needs.

Virtual machines: gives you maximum control over the Hosting environment and allows you to configure it the way you want.

Containers: They are strong and compelling options, separating and individually managing the different aspects of a hosting solution.

Azure App Service: It's an HTTP-based service for hosting web applications.

It offers high availability & automatic scaling and supports Windows, and Linux operating systems.

It also supports multiple languages —> .NET, .NET Core, Java, Ruby, Node.js, PHP, and Python.

Azure Virtual Networks

Azure Virtual Machines are hosted in an Azure Virtual Network. In Azure, you create your virtual network. If necessary, you may build several virtual networks in Azure. Each virtual network in azure needs to be assigned to an address space.

Example of an address space 15.0.0.0/16

Subnets

Subnets are the small networks used to divide the Virtual network into multiple small networks(sub networks) for the organization. It is a range of IP addresses in the VNet. Each Network Interface Card (NIC) in a virtual machine is connected to one subnet in one VNet. After this, we can deploy our resources into a specific subnet in the virtual network.

Virtual Network Peering (VNet Peering)

We can connect two virtual networks within Azure through a private network, which means we can connect over the private IP address space.

This allows you to have seamless connectivity between two or more virtual networks in Azure.

There's no need for a public IP address in VNet Peering.

VNet peering: It connects virtual networks within the same Azure region.

Global VNet peering: It connects virtual networks across Azure regions.

Azure DNS

DNS means - Domain Name System: It is responsible for translating service names to IP addresses.

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

Benefits: Reliability and performance, Security, Ease of Use, Customizable VNets, and Alias records.

Azure Virtual Private Network (VPN):

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over the public internet.

Azure VPN Gateway and ExpressRoute

Azure VPN Gateway:

A VPN gateway is a type of virtual network gateway. All data transfer is encrypted inside a private tunnel as it crosses the internet. When you deploy a VPN gateway, you specify the VPN type: either policy-based or route-based.

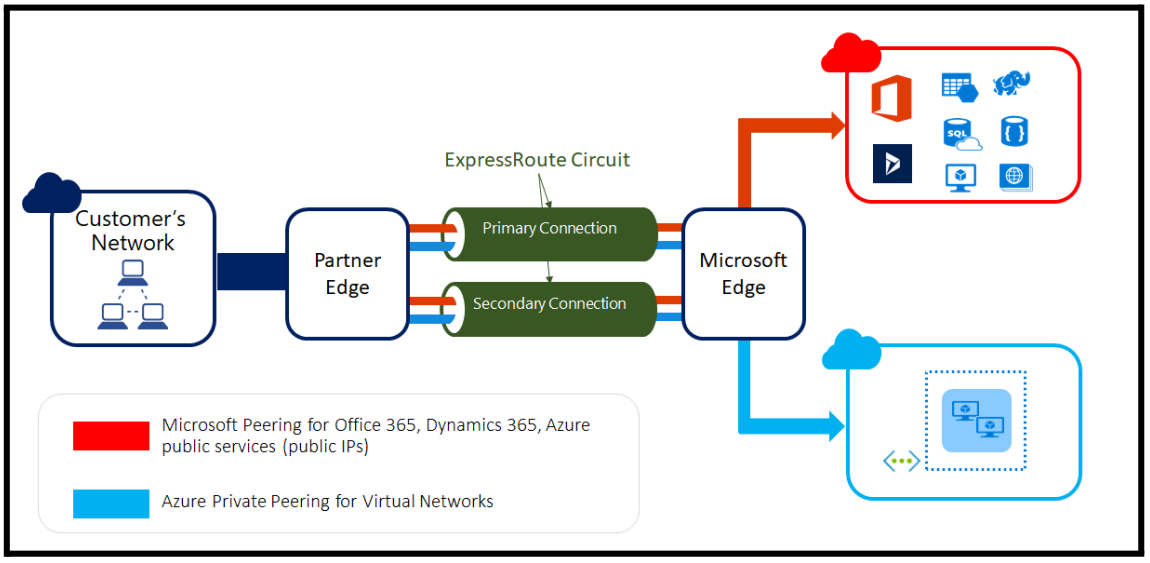
Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network and enable the following connectivities:

- Connect on-premises datacentres to virtual networks through a site-to-site connection.
- Connect individual devices to virtual networks through a point-to-site connection.
- Connect virtual networks to other virtual networks through a network-to-network connection.

Azure ExpressRoute:

Azure ExpressRoute allows you to extend your on-premises networks into the Microsoft cloud through a private connection with the help of a connectivity provider.

- ExpressRoute connections don't go over the public Internet.
- To set up a fast private connection to Microsoft Cloud services from your on-premises infrastructure, you need to create a VNet Gateway to connect to the virtual networks in Azure with ExpressRoute.
- You can establish connections to Microsoft cloud services(Microsoft Azure and Microsoft 365)



(Reference: Microsoft Docs)

Features and benefits:-

- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with ExpressRoute premium add-on.

- Dynamic routing between your network and Microsoft via Border Gateway Protocol
- Built-in redundancy in every peering location for higher reliability.
- Connection uptime SLA and Quality of Service(QoS) support for Skype for Business.

Azure Public and Private Endpoints

Public Endpoint means - for a managed instance it allows data access to your managed instance from outside the virtual network. You can access the managed instance from multi-tenant Azure services like –> Power BI, Azure App Service, or on-premises network.

By using a public endpoint in a managed context, you don't need to use a VPN, which helps avoid VPN throughput issues.

Private endpoint means - It's a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to the service provided by Azure Private Link.

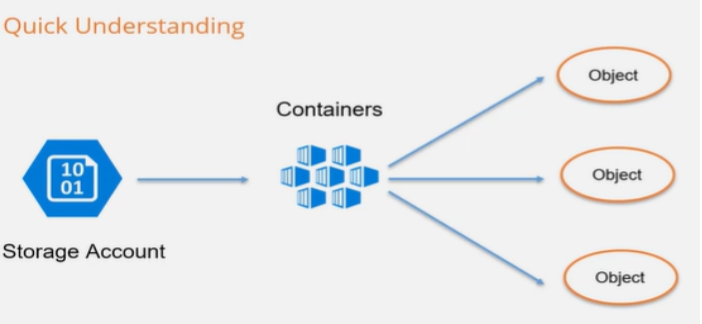
By enabling a private endpoint, you are bringing the service into your virtual network.

Azure Storage Services

Azure Storage includes massively scalable object storage for data objects, a cloud file system, a messaging store for secure communications, and a NoSQL store. Azure Storage accounts are extremely durable and available.

Blob Storage:

Blob Storage is useful for storing videos, images, large files, log files, etc. Blob storage stores things in the form of objects.



Reference: Whizlabs AZ-900 OC #27

Table Storage:

It is a low-cost method of storing table-like data for applications. This type of storage is key-attribute storage and is most significantly utilized for NoSQL data.

File Storage:

File Storage uses the Server Message Block Protocol to retrieve files. It can be used to mount file shares on Windows, Linux, and Mac machines.

Queue Storage:

It is a messaging service offered by Azure. It is used to retrieve and save messages. A queue may hold millions of messages.

Comparison Table for Azure Storage types:

Storage Type	Example Usage
Table	No SQL Data
Queue	Retrieve and Save Messages
Blob	Images, Pdfs, etc
FIle	Mounting file shares on Various Operating Systems

Comparing Azure Storage types and services

Type	Supported services	Redundancy Options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs	Blob Storage (including Data Lake Storage)	LRS, ZRS	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency.
Premium file shares	Azure Files	LRS, ZRS	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	LRS	Premium storage account type for page blobs only.

(Reference: Microsoft Docs)

Azure Storage Tiers and Redundancy options

Azure Storage Tiers:

- **Hot tier** is used to optimize for storing frequently accessed or modified data. It has the highest storage costs and lowest access costs.
- **Cool tier** is used to optimize for storing infrequently accessed or modified data. Data is stored for at least 30 days. It has high access costs and low storage costs.
- **Archive tier** is used to optimize for storing rarely accessed data, and it has flexible latency requirements on the order of hours. Data is stored for at least 180 days.

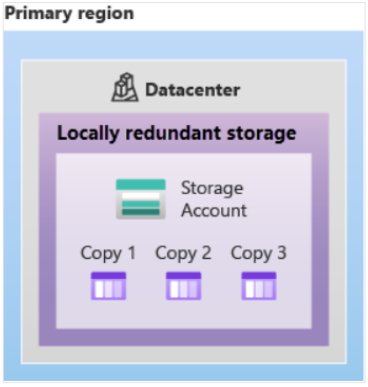
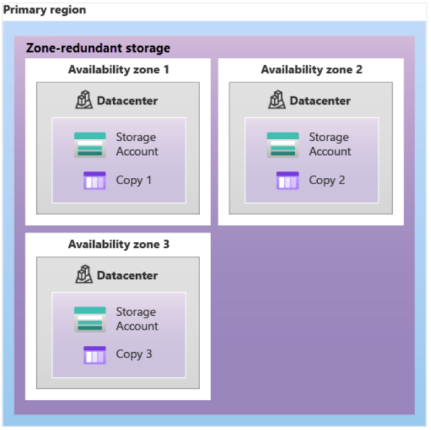
Azure Redundancy options:

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters. Redundancy ensures - your storage account meets its availability and durability goals even in failures.

Redundancy in the primary region:-

- **Locally redundant storage (LRS)** copies data synchronously and replicates your storage account three times within a single data center in the primary region**.**

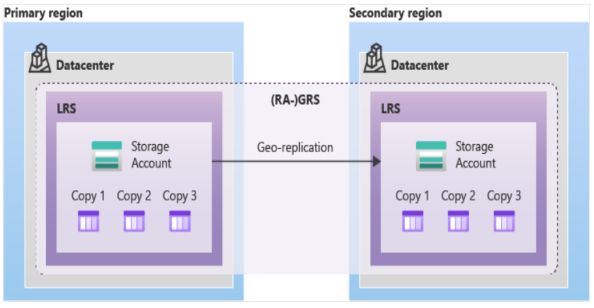
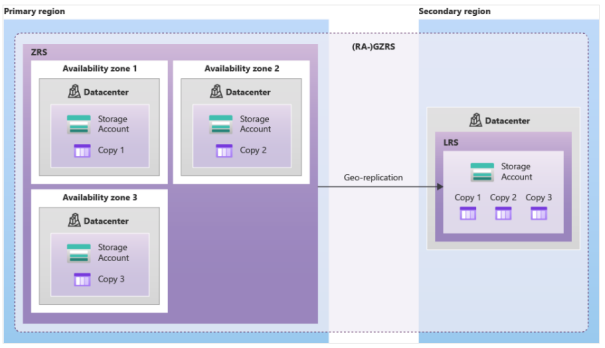
- **Zone-redundant storage (ZRS)** copies data synchronously and replicates your storage account across three Availability Zones in the primary region.

LRS	ZRS
	

Redundancy in the secondary region:-

- **Geo-redundant storage (GRS)** copies your data the same as LRS in the primary region and then asynchronously copies your data to a single physical location in a secondary region that is hundreds of miles away from the primary region.

- **Geo-zone-redundant storage (GZRS)** copies your data the same as ZRS in the primary region and then asynchronously copies your data to a single physical location in the secondary region.

GRS	GZRS
	

(Reference: Microsoft Docs)

Identify Azure File Movement Options

Azure also has tools designed to help you move or interact with individual files or small file groups. Among those tools are AzCopy, Azure Storage Explorer, and Azure File Sync.

AzCopy is a command-line interface that you can use to copy blobs or files to or from a storage account. You can upload, download copies and synchronize files between storage accounts. AzCopy can also be configured to work with other cloud providers to help move files back and forth between clouds.

Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your storage account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. You can upload to Azure, download from Azure, or switch between storage accounts.

Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on the Windows Server to access data locally, including SMB, NFS, and FTPS. It is used to centralize an organization's file shares in Azure Files while keeping the flexibility, performance, and compatibility of an on-premises file server.

Azure Data Migration options

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud. It provides a simplified migration, modernization, and optimization service. Azure Migrate serves as a hub to help you manage the assessment and migration of your on-premises datacentre to Azure.

- Unified migration platform single portal to start, run and track your migration to Azure.
- Range of tools for assessment and migration.
- Assessment and migration: In the Azure Migrate hub, you can assess and migrate your on-premises infrastructure to Azure.

Azure Data Box is a physical migration service that helps transfer large amounts of data quickly, inexpensively, and reliably. It's suited for transferring data sizes larger than 40 TB in situations with limited network connectivity.

- One Time Migration – when large amounts of on-premises data are migrated/moved to Azure.
- Moving/Migrating a media library from offline tapes into Azure to create an online media library.
- We can migrate - VM farm, SQL server, and applications to Azure.
- We can move historical data to Azure for in-depth analysis and reporting using HDInsight.
- Initial bulk transfer - when an initial bulk transfer is done by using Azure Data Box
- Periodic uploads - When large amounts of data are generated periodically and moved to Azure.

Azure Identity, Access, and Security

Microsoft Entra

It is a new product in the Microsoft family that includes all of Microsoft's identity and access capabilities. It includes three product categories:

(Reference: Microsoft Entra - Secure Identities and Access | Microsoft Security)

1. **Azure Active Directory (Azure AD) —> Known Product**
2. **Microsoft Entra Permissions and Management(Cloud Infrastructure Entitlement Management (CIEM)) —> New Product**
3. **Microsoft Entra Verified ID(decentralized identity) —> New Product**

Azure Active Directory

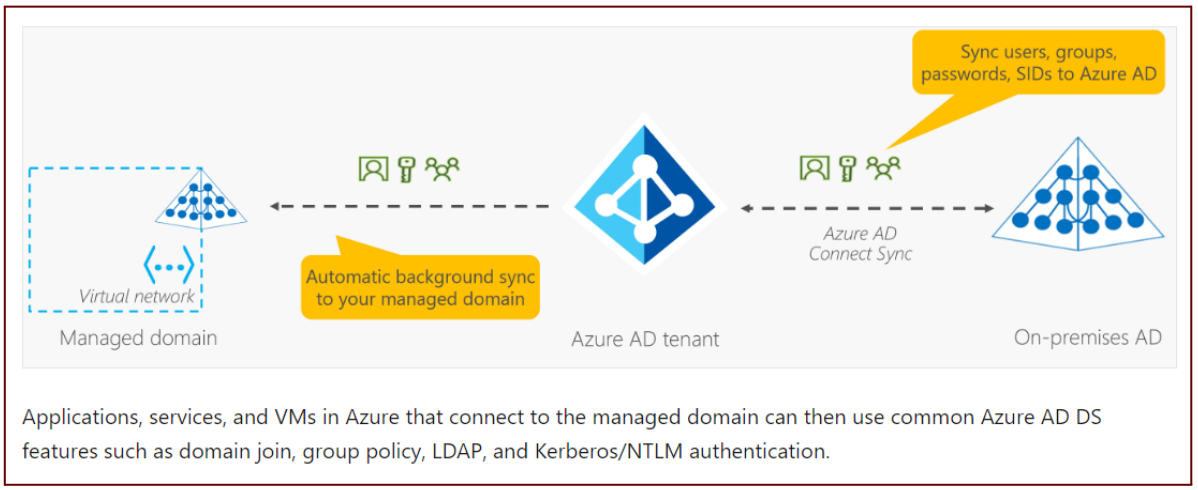
(Azure AD) is now part of Microsoft Entra, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to protect against 99.9 percent of cybersecurity attacks.

- Azure AD is a cloud-based Tenant Identity Management Service by Microsoft that is extremely scalable and distributed globally through the Azure Cloud.
- Essentially, it's a multi-tenant cloud service, which means it resides in the cloud and has tenants as part of it.
- In the universe of Azure AD, each tenant is a separate entity.
- Azure AD is unique in that it provides a single Identity Solution for all Microsoft Cloud services, including *Office365, Intune,* and others.
- When compared to any other Active Directory, Azure utilizes a completely different kind of authentication called OAuth.

Azure Active Directory Domain Services

It is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication.

You get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud with Azure AD DS.



(Reference: Microsoft Docs)

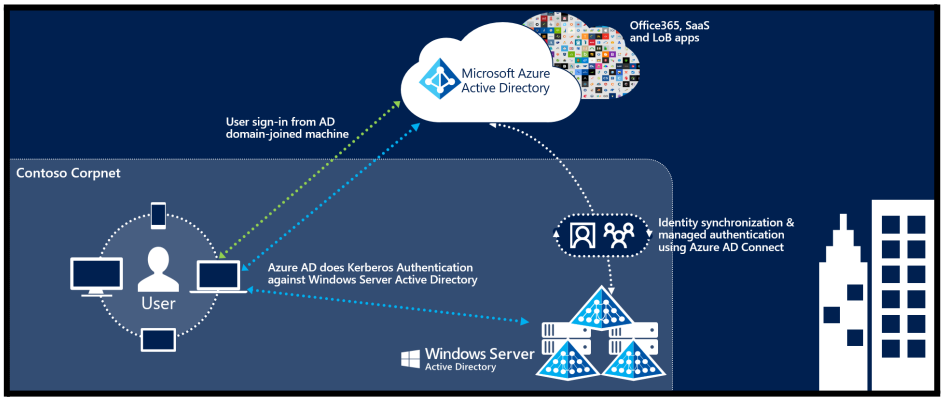
Azure Authentication Methods

Azure supports multiple authentication methods, including standard passwords, Single Sign-On (SSO), Multifactor authentication (MFA), and Passwordless.

Single Sign-On Authentication:

Single sign-on (SSO) allows a user to sign in at once and use those credentials to access multiple resources and applications from different providers.

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network.



(Reference: Microsoft Docs)

--Back to Index--

Multi-Factor Authentication(MFA):

Multi-Factor Authentication employs two or more factors to provide access to the accounts you are attempting to access.

MFA employs two, and in some cases three, components. They're

- *Something you are aware of*
- *Something you possess*
- *Something You are*

To make any modifications to the MFA of the users in Azure, you must be a Global Administrator. A global Administrator is regarded as having the greatest level of privilege. A global administrator can enable the MFA in the security blade of the Azure Active Directory.

Passwordless Authentication:

Passwordless authentication methods are more convenient because the password is removed and replaced with something you have or something you know.

For example, your computer is something you have. Once it's been registered/enrolled then Azure knows that it's associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.

Azure Managed Identity

System Assigned Managed Identity:

It provides a mechanism for the service to have an identity instead of an end-user in the Azure Active Directory. In this case, the identity is tightly coupled to the azure resource.

This kind of Identity has two main Advantages.

- Automatic Credential Rotation
- Identity lifecycle Management

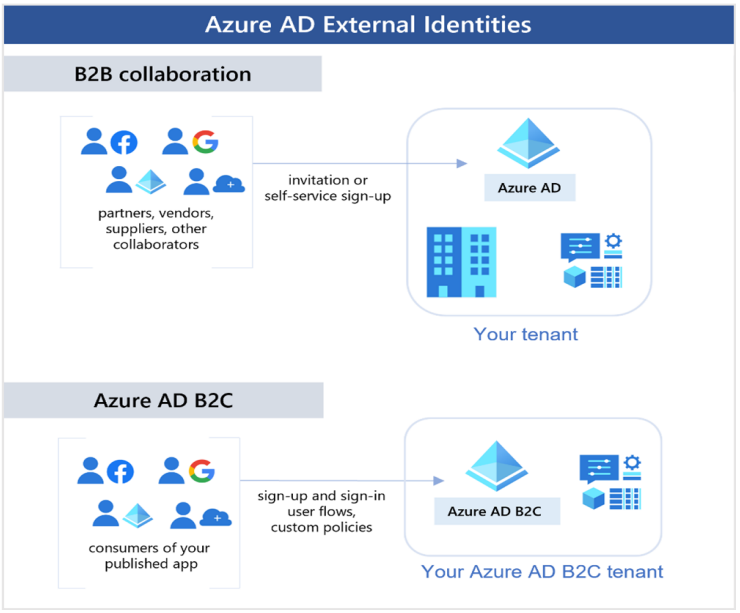
User Assigned Managed Identity:

We utilize this kind of Identity when we have numerous resources that all share the same target resource. In this instance, it generates an identity independent of the Azure resource's lifetime and when new Azure resources are set up for the application.

External Identities and Guest access in Azure

Azure External Identities:

Azure AD external identities represent the ways you interact securely with the users outside your organization. External identities may sound similar to single sign-on. With these Identities, external users can "bring their own identities."



(Reference: Microsoft Docs)

Capabilities make up External Identities:

1. **Business-to-business (B2B) collaboration** -Collaborate with external users by letting them use their preferred identity to sign in to your Microsoft applications or other enterprise applications
2. **B2B direct connect** - Establish a mutual, two-way trust with another Azure AD organization for seamless collaboration. B2B Direct Connect currently supports team-sharing channels, enabling external users to access your resources from within their own teams.
3. **Azure AD Business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps to users and customers, while using Azure AD B2C for identity and access management.

Guest Access:

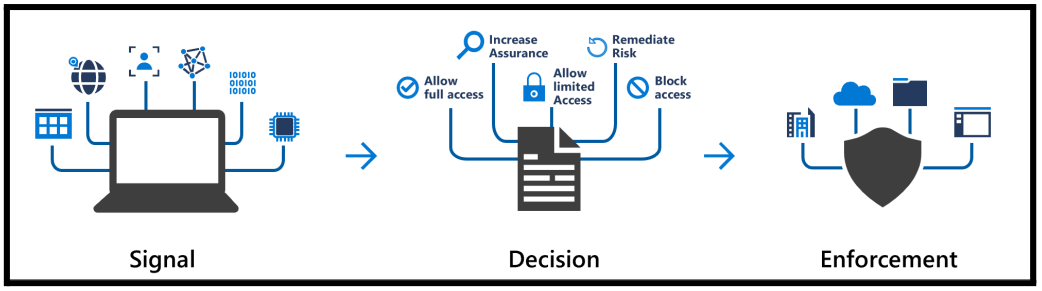
With Azure AD B2B collaboration, you can invite anyone to collaborate with your organization using their own work, school, or social account. with the given link (Quickstart), you'll learn how to add a new guest user to your Azure AD by using the Azure portal.

you can also add guest users by using PowerShell, or the bulk invite.

Quickstart: Add a guest user and send an invitation - Azure AD - Microsoft Entra | Microsoft Learn

Azure AD Conditional Access

It is a tool that Azure AD uses to allow or deny access to resources based on identity signals. These signals include who the user is, where the user is, and from which device the user is requesting access.



(Reference: Microsoft Docs)

Conditional Access helps IT administrators;

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.
- This provides users with a more granular multifactor authentication experience.

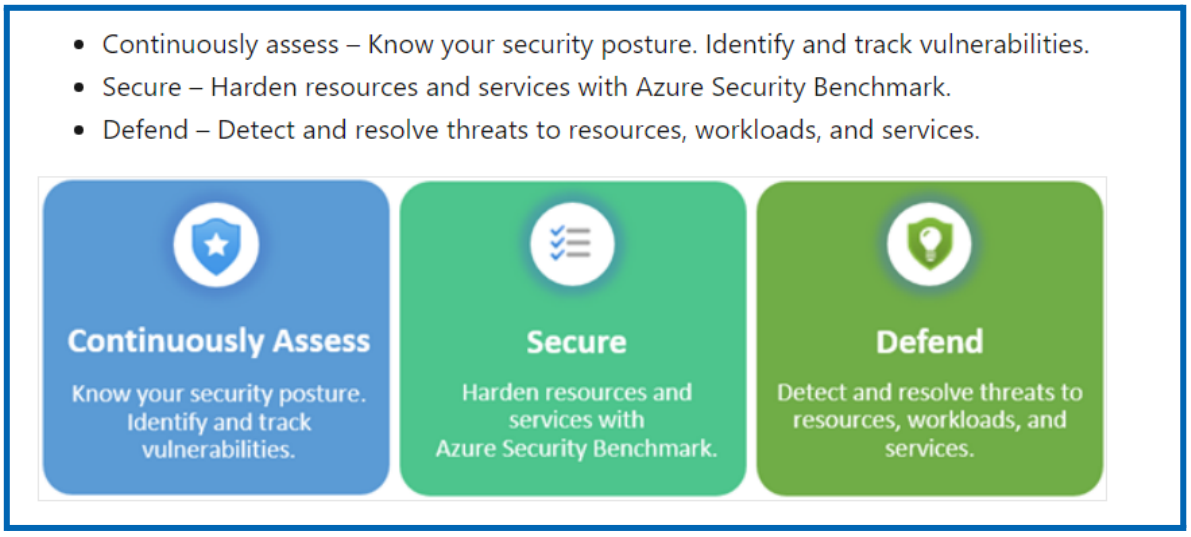
Azure Role-Based Access Control (RBAC)

- Azure Role-based Access Control is a mechanism to provide access to resources.
- You can provide access at different scope levels like a resource group or a subscription level.
- There are many built-in roles available to provide a certain type of access to the user.
- The different types of Inbuilt roles that are available Owner, Contributor, Reader, etc
- Different roles have different kinds of abilities on the specific scope given to them.

For further details, please refer —> [Azure built-in roles - Azure RBAC | Microsoft Docs]

Microsoft Defender for Cloud

- It is a monitoring tool for security posture management and threat protection.
- It monitors cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications to strengthen your security posture.



Reference: Microsoft Docs

--Back to Index--

Zero trust and Defense in Depth models in Azure

Zero trust concept in Azure:

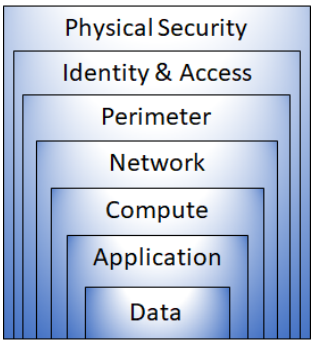
Zero trust is a security model that assumes the worst-case scenario and protects resources against that assumption. Zero Trust assumes breach at the outset and then verifies each request as though it originated from an uncontrolled network.
To address this new world of computing, Microsoft highly recommends the Zero Trust model.

- **Verify explicitly -** Always authenticate and authorize based on all available data points.
- **Use least privilege access -** Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach -** It's verify end-to-end encryption. Use analytics to gain visibility, drive threat detection, and improve defenses.

Defense-in-depth in Azure:

The goal of Defense-in-Depth is to protect information and prevent it from being stolen by those who are not authorized to access it.

Layers of defense-in-depth:



(Reference: Microsoft Docs)

Each layer provides protection so that if one layer is breached, the next layer is already in place to prevent further exposure. This approach eliminates reliance on any protective layer.

It slows down an attack and provides alerting information that security teams can take action on automatically or manually.

Azure Cost Management

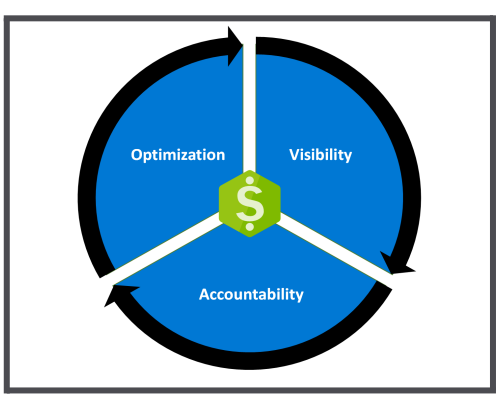
Factors affecting costs in Azure

The way you use resources, your subscription type, and pricing from third-party vendors.

- Azure uses these meters to create a usage record that can be used to help calculate your bill.
- In Azure, you're always charged based on what you use.
- Azure free trial subscription provides access to a number of Azure products (free for 12 months)
- You can also purchase Azure-based services from vendors through Azure Marketplace.

Azure Cost Management and Billing tool

Cost Management and Billing tool are provided by Microsoft which help you to analyze, manage, and optimize the costs of your workloads.



Cost Management + Billing features to:

- Conduct billing administrative tasks such as paying your bill
- Manage billing access to costs
- Download cost and usage data that was used to generate your monthly invoice
- Proactively apply data analysis to your costs
- Set spending thresholds
- Identify opportunities for workload changes that can optimize your spending

(Ref: Microsoft Docs)

Azure Billing is the process of invoicing customers for goods or services and managing the commercial relationship. You may have access to multiple billing accounts and you can use a billing account to manage your invoices and payments and track the expenses.

Cost Management shows organizational cost and consumption patterns with advanced analytics.

This gives us the ability to quickly check Azure resource costs.

Azure Pricing, Budgets, and Tags

Azure Pricing:

- Businesses that subscribe to Azure may pick and choose which services and capabilities to employ on an a la carte basis.
- Each service has its pricing structure, and many are charged according to the service tier required and used.
- There are many ways to save costs in Azure, such as using Azure Reservations, Budgets, etc.

- If your resource is intended for long-term use, Azure Reservations will save you approximately 70% of what you would spend for a pay-as-you-go subscription.

Azure Budgets:

- Azure Budgets is a tool that enables you to establish spending limits in Azure.
- We may configure it to several scopes, such as Subscription level, Resource Group level, etc.
- Once we have established the threshold, budgets will notify you when your expenditure is nearing the limit, allowing you to take appropriate action.
- Budgets have the potential to automate in reaction to you reaching certain criteria. For example, if you exceed a certain threshold number, you may implement a policy that shuts down these virtual machines.

Purpose of Azure Tags:

- Tags are used to organize your Azure resources.
- Tags are metadata elements that you apply to your Azure resources.
- They are key-value pairs that help you identify resources based on your organization's settings.
- Tags are applied to your Azure resources, resource groups, and subscriptions.

To apply the Tags - Azure PowerShell offers two commands: New-AzTag and Update-AzTag.
To apply the Tags - Azure CLI offers two commands: az tag create and az tag update.

Azure Pricing and TCO Calculator

Azure Pricing Calculator:

- An azure price calculator is a tool that can be used to assist us in understanding the costs of Azure services and features. It simply calculates the cost of Azure Services.
- You choose the resources to utilize in Azure Pricing Calculator. You modify the service settings, and, finally, you examine the expenses.

Please refer to Pricing Calculator | Microsoft Azure - to know more about Azure PCO.

Azure TCO Calculator:

- The Azure TCO calculator calculates the cost reductions that could be obtained by moving your workloads to Azure.
- It produces a comprehensive PDF report on the savings by moving to Azure.
- It is your responsibility to change all of the factors in it, such as the number of virtual machines you use, the price tier you choose for the web apps, and so on.

Azure Monitoring Tools

Azure Advisor and Service Health

Azure Advisor:

Azure Advisor is a recommendation tool that provides suggestions by using some algorithms on four key aspects for resources hosted in Azure, namely: high availability, security, performance, and cost.

It's better to follow these recommendations as it is very beneficial to maintain the health of the resources and the cost deduction.

Azure Service Health:

Azure offers a suite of experiences to inform you about the health of cloud resources about the current and upcoming issues such as events affecting the Service, planned maintenance, and other changes that affect service availability.

Azure Service Health helps you to track both, your specifically deployed resources and the overall status of Azure. It is a combination of three separate smaller services.

- **Azure status** informs about the service outages in a global view of the health of all Azure services across all Azure regions.
- **Service health** provides you with a personalized view of the health of Azure services and regions.
- **Resource health** provides information about the health of individual cloud resources.

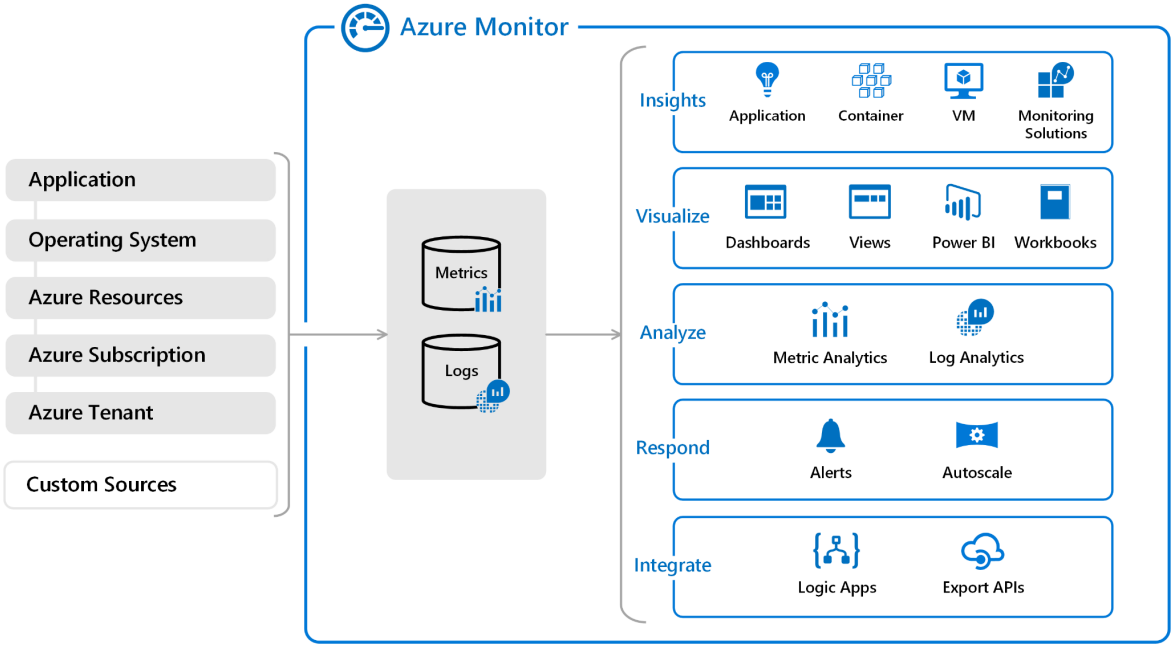
Azure Monitor and Monitoring alerts

Azure Monitor:

Azure Monitor is a tool that helps you improve the performance and availability of your apps and services. It provides a complete solution for *obtaining, evaluating,* and responding on telemetry from your cloud as well as on-premise platforms.

- Metrics and Logs are the two main diagnostic data that can be seen with the assistance of Azure Monitor.
- You can identify your issues with the help of these diagnostic data
- One can create alerts as well in azure based on the metrics and logs
- A blade called service health allows you to monitor the health of deployed resources and generate alerts based on the health.

Here's a visual representation of how an Azure monitor works.

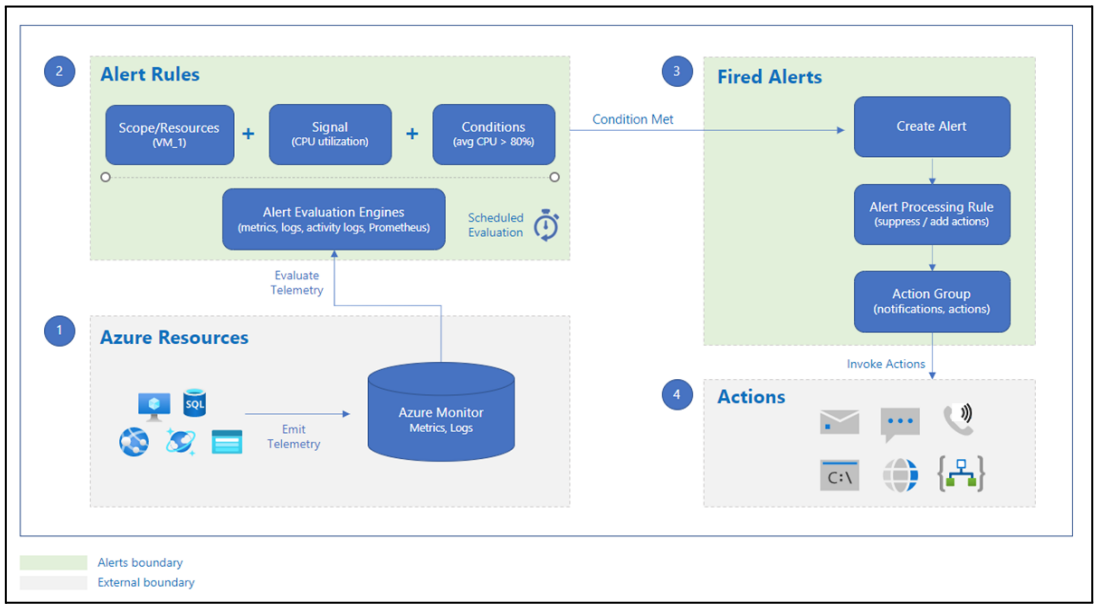


Reference:- Microsoft Docs

Azure Monitor Alerts:

It proactively notifies you when significant conditions are detected in your monitoring data. Alerts help you to identify and fix the problems before the customer notices them.

We can alert on any log/metric data source in the Azure Monitor.



Reference: Microsoft Docs

Log Analytics and Application Insights in Azure

Log Analytics Workspace in Azure:

Log Analytics workspace is a centralized, unique environment for logging data from Azure Monitor and other Azure services like - Microsoft Sentinel and Microsoft Defender for Cloud, etc.

It is the tool to write and run log queries on the monitor data in the Azure portal.

Log Analytics is a robust tool that supports both simple and complex queries and data analysis.

You can create multiple workspaces based on the following requirements:

- Data Geographic location.
- Access rights define which users can access the data.
- Configuration settings such as pricing tiers and data retention.

Application Insights in Azure:

- Application Insights is a feature in Azure Monitor, used for monitoring your web applications mainly for the in-depth analysis of the web applications.
- Application Insights has the ability to monitor applications running in Azure, on-premises, or in another cloud environment. It provides extensible application performance management (APM) and monitoring for live web apps.
- You can configure Application Insights in two ways to help monitor the application.
- You can install the SDK in your application or use the Application Insights agent.

Features and Tools for managing & deploying Azure resources

Azure Portal

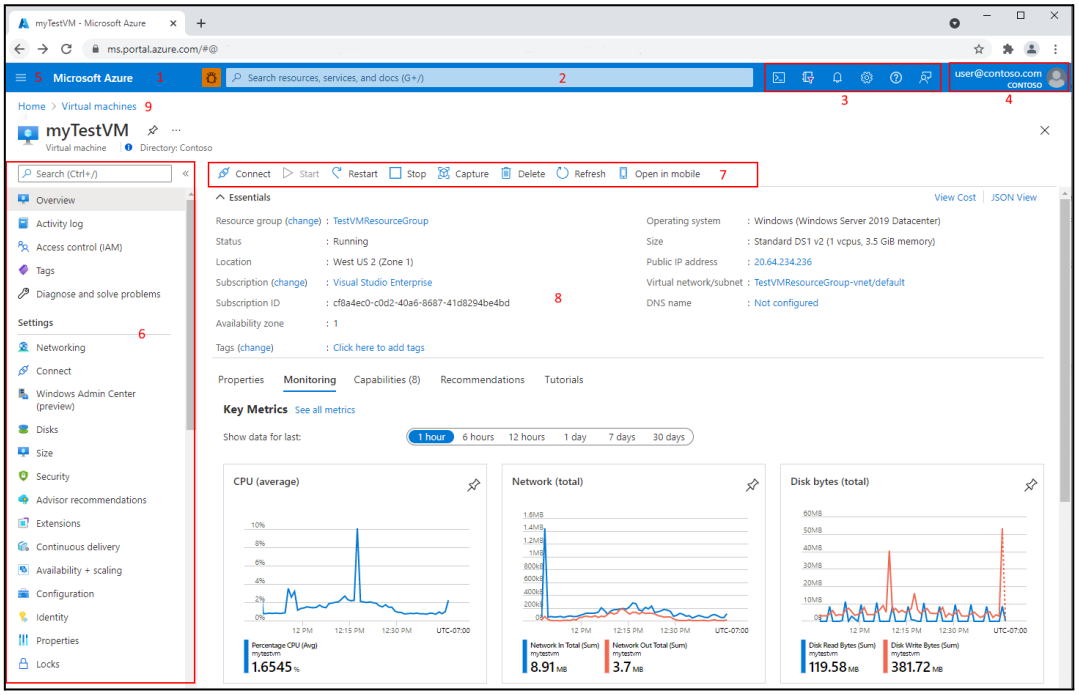
The Azure portal is a web-based and unified console for creating and managing Azure Resources.

Azure Portal is designed for resiliency and continuous availability.

It has a presence in every Azure datacenter. This configuration makes Azure Portal resilient to individual datacenter failures and avoids network slow downs by being closer to users.

Azure portal is constantly updated and does not require any downtime for maintenance activities.

- By using the graphical user interface, you can manage Azure subscription.
- Build, manage, & monitor everything from simple web apps to complex cloud deployments



(Reference: Microsoft Docs)

Azure PowerShell, CLI, and CloudShell:

They are command-line tools for creating, configuring, and managing Azure resources using PowerShell.**Azure PowerShell is** a set of commands to manage Azure resources using commands.

Azure CLI is another **command-line interface designed** to manage Azure Resources. It is created based on python. Azure PowerShell uses PowerShell commands, and Azure CLI uses Bash commands.

Another command-line interface is the **Azure Cloud Shell. It**'s a browser-based shell tool. It is accessible straight from the Azure portal.

Note: Azure Cloud Shell (similar to Bash shell) supports both Azure PowerShell and Azure CLI.

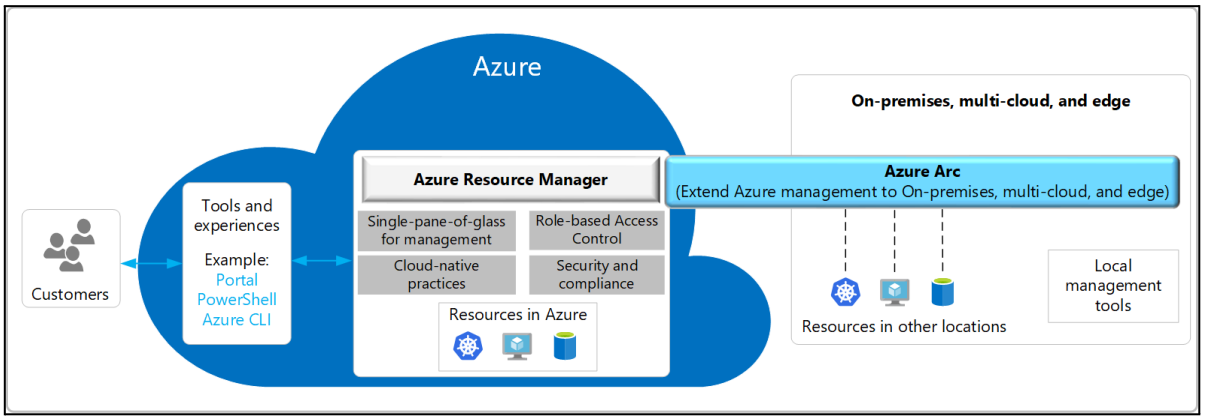
--Back to Index--

Azure Arc Overview and Purpose

Azure Arc simplify this governance and management by delivering a consistent multi-cloud and on-premises management platform.

Azure Arc provides a centralized, unified way to;

- Manage your entire environment together by projecting your existing non-Azure and/or on-premises resources into Azure Resource Manager.
- Manage virtual machines, Kubernetes clusters, and databases as if they were running on Azure.
- Use familiar Azure services and management capabilities regardless of where they live.
- You can continue by using the traditional Information Technologies Operations (ITOps) while introducing DevOps practices to support new cloud-native models in your environment.
- You can configure custom locations as an abstraction layer on top of Azure Arc-enabled Kubernetes clusters and cluster extensions.



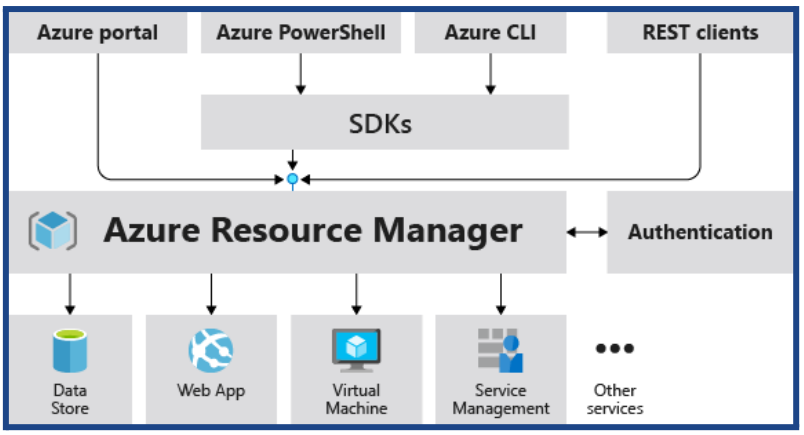
(Reference: Microsoft Docs)

Azure Arc allows to manage the below resources hosted outside of Azure:
Servers, Kubernetes clusters, Azure data services, SQL Server, and Virtual machines (preview)
To know about the Azure Arc, please refer —> [Azure Arc overview - Azure Arc | Microsoft Learn]

Azure Resource Manager and Resource Manager templates

Azure Resource Manager: It is a deployment and management service for Azure.
Benefits:

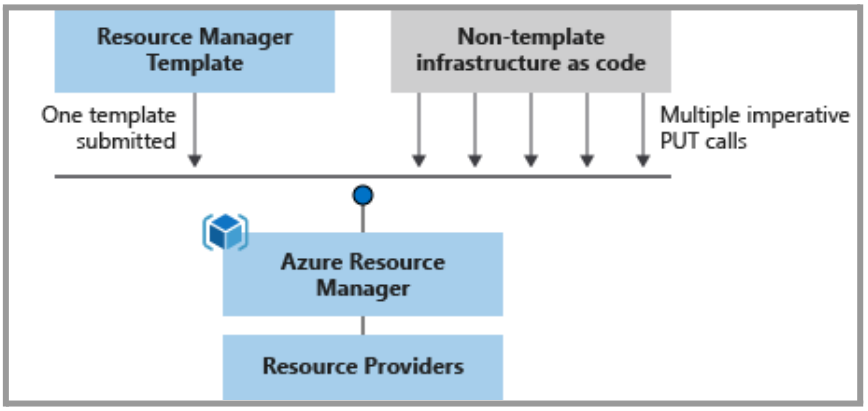
- You can manage your infrastructure through declarative templates rather than scripts.
- You can deploy, manage, and monitor all the resources in your subscription.
- You can apply access control to all services.
- You can apply tags to resources to organize all resources in your subscription.



(Reference: Microsoft Docs)

Azure Resource Manager (ARM) Templates:

- ARM templates are used to implement infrastructure as code (IaC) for the Azure infrastructure.
- Infrastructure as code (IaC) uses the DevOps methodology.
- ARM Templates basically depend on the JavaScript Object Notation (JSON) Syntax.



Reference: Microsoft Docs

Template has the following sections: Parameters, Variables, User-defined functions, Resources, and Outputs.

Governance and Compliance in Azure

Azure Locks and Policies

Azure Locks:

Azure locks allow you to guarantee that a resource isn't inadvertently destroyed or changed. Locks may be set at several scope levels, such as resource group or subscription level.

In Azure, there are two kinds of locks available:

- **CanNotDelete:** If this kind of lock is applied, the user will be unable to delete a resource but will view and change it.
- **ReadOnly:** If this kind of lock is applied, the user cannot change or delete a resource, but may read it.

Azure Policies:

- Azure policies are intended to help with resource control, Compliance, Cost Management, security, etc.
- Basically, With policy definitions that impose rules and consequences for your resources, Azure Policy assists you in managing and preventing IT problems.
- There are many inbuilt policies; if needed, we can create our own custom policy.

Examples of policies include:-

- Only virtual machines of this particular SKU should be created.
- Every resource should have a tag.

Azure BluePrints

- A blueprint is a step-by-step guide, design, or pattern for creating something.
- Azure blueprint is the declarative way to orchestrate the deployment of various resource templates and some other artifacts.
- Azure Blueprint Artifacts are something that can be used to build blueprints.

Azure Blueprint Artifacts are composed of four different things.

- *ARM Templates*
- *Resource Groups*
- *Azure RBAC*
- *Azure policies*

They can help you save some time and help to deploy resources quickly and efficiently.

Microsoft Service Trust Portal

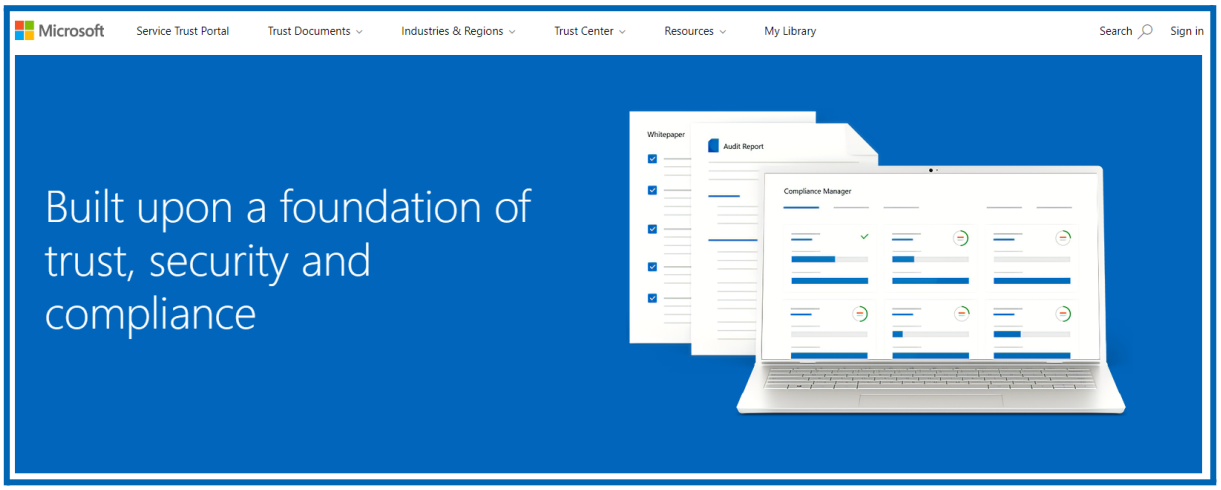
The Service Trust Portal is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

It provides a variety of content, tools, and other resources about how Microsoft cloud services protect

your data and how you can manage the cloud data security and compliance for your organization.

You must review and agree to the Microsoft Non-Disclosure Agreement for Consent Materials.

★ **You can access the Service Trust Portal at https://servicetrust.microsoft.com/.**



(Reference: Microsoft Docs)

Extra Learning

Azure Core Solutions

Azure Functions (Serverless):

Azure Functions is a serverless computing service that is available in Azure. It supports a variety of development languages, such as C#, F#, Node.js, Java, or PHP.

- Like many Cloud Services, it uses a pay-as-you-go model. It is possible to connect it with a variety of Azure services. Charges are only incurred when a function is triggered, and also, Azure Functions scales automatically.
- We can execute the small pieces of code using Azure Functions without having to worry about the underlying infrastructure.

If you want to	Then
Build a web API	Using the HTTP trigger, create an endpoint for your web apps.
Build a serverless workflow	Utilizing durable functions, chain a sequence of functions together.
Respond to database changes	When a document is generated or modified in Cosmos DB, run custom logic.
Process data in real-time	Use SignalR and Functions to react to data in real time.

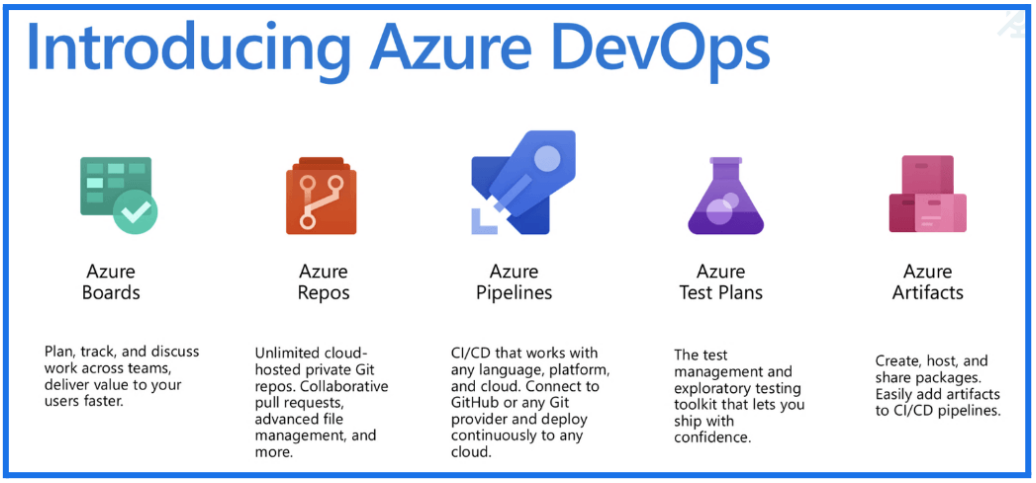
Azure DevOps

Azure DevOps is just an umbrella service for a plethora of different development services.
The various kinds of Azure DevOps Services are mentioned below.

Azure Boards: It is used to Deliver value to your users more quickly by using tried-and-true agile technologies to plan, monitor, and discuss work across your teams.

Azure Repos: It is a version control management tool available in azure. It supports both TVS and Git.

Azure Pipelines: Azure Pipelines is a continuous integration (CI) and continuous delivery (CD) solution with a lot of features. It integrates with your chosen Git provider and can be deployed to several big cloud providers, including Azure.



Reference:- Microsoft Docs

Azure Test Plans: This is a great tool for testers who are having difficulty communicating with developers about what sort of issues they have with their product.

Azure Artifact: This is a private package manager tool available in azure.

Azure DevTest Labs: This tool is used to create a dev-test environment for your developers.

Security features in Azure

Microsoft Sentinel:

Microsoft Sentinel is a scalable, cloud-native solution and is a Combination of **SIEM and SOAR**

- SIEM stands for *Security Information and Event Management*
- SOAR stands for *Security Orchestration, Automation, and Response*

Microsoft Sentinel is more powerful than the Microsoft Defender for Cloud because it is used for real-time threat intelligence.

It provides intelligent security analytics and threat intelligence across the enterprise.

It is a unified platform for threat visibility, Proactive threat hunting, Threat Response, and Security Alert Detection.

Azure DDoS Protection

An effort by a malign party to interrupt regular traffic on a website by flooding it with huge quantities of false traffic called a DDoS Attack. Azure offers two types of DDoS protection. They are:

- **DDoS Protection Basic:** It is already built-in to all the Azure services. It's completely free.

- **DDoS Protection Standard:** Use the Standard tier if the attacks on your application are sophisticated. It costs approximately $3000 each month. It provides SLAs for Application and Cost Protection.

Azure Key Vaults:

- Azure Key Vault is a cloud service for storing and safely accessing secrets.
- It is used for *key management, secret management, certificate management, and storing secrets supported by hardware models.*
- Azure Key Vault can centralize application secrets, monitor access, and use, and simplifies resource management.

Azure Network Security Group(Azure NSG)

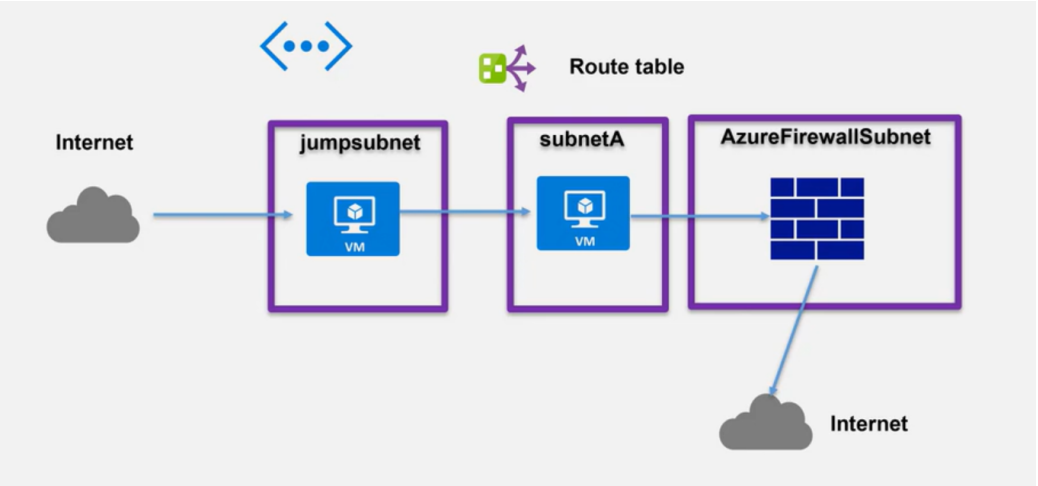
Its purpose is to use certain rules to filter traffic to and from Azure resources in a Virtual Network.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

- The above picture shows the default rules that are present in the Network Security Group.
- We can manually create our own inbound and outbound port rules to deny or allow the traffic into the azure resources.

Azure Firewall

- This is a fully managed and automatically scalable cloud-based network security service that can be used to protect the resources in an Azure Virtual Network.
- This service allows you to define and enforce policies for application and network connection.



Reference:- Whizlabs AZ-900 Course

Azure Service Level Agreements

- Microsoft's commitment to an Azure Service or Product is defined as SLAs. Individual service level agreements (SLAs) are offered for each Azure product and service.
- The service level agreement (SLA) specifies what happens if a service or product fails to fulfill the specified availability obligations.
- Performance targets are expressed as uptime and connectivity guarantees.
- The performance goals vary from 99.9% (three nines) to 99.99%. (four nines).
- If a service fails to fulfill the promises, you may be entitled to a refund of a portion of your monthly subscription costs.
- When 2 services are integrated & utilized, Azure employs a technique called *composite SLA.*

  Composite SLA = SLA of service 1 * SLA of service 2

Azure Service Lifecycle

Every service in Azure follows its own service lifecycle. Almost all the services in azure

have three stages.

Private Preview: These services are only available for specific types of customers.

Public Preview: All clients have access to these services. This kind of service is not completely finished, implying that it is unsuitable for production stages; furthermore, the service under public preview doesn't have SLAs.

General Availability: These services are accessible to the whole community, support SLAs, and are appropriate for production environments.

Success. Certified.

Learn on real-time with [AZ-900 Course]

[375+ Practice Questions | 95+ Videos | 12+ Hands-on Labs | Free Updates for 2 year]

Looking for [Subscription Plans]?

[200+ Courses | Unlimited Labs & Sandboxes 25,000+ Practice Questions | 4500+ Videos]

5 Million+ Global Learners