Introduction to Microsoft Azure Fundamentals
What is Azure Fundamentals?

Azure Fundamentals is a series of three learning paths that familiarize you with Azure and its many services and features.

Whether you're interested in compute, networking, or storage services; learning about cloud security best Practices

[AI/ML]

Why should I take Azure Fundamentals?

Azure Fundamentals provides you with everything you need to get started.
No matter your goals, Azure Fundamentals has something for you. You should take this course if you:

- Have general interest in Azure or in cloud computing
- Want to earn official certification from Microsoft (AZ-900)

The Azure Fundamentals learning path series can help you prepare for Exam AZ-900:

AZ-900 Domain Area	Weight
Describe cloud concepts	25-30%
Describe Azure architecture and services	35-40%
Describe Azure management and governance	30-35%

→ Questions

Each domain area maps to a learning path in Azure Fundamentals. The percentages shown indicate the relative weight of each area on the exam.

Skills at a glance

Describe cloud concepts (25–30%)

Describe Azure architecture and services (35–40%)

Describe Azure management and governance (30–35%)

Describe cloud concepts (25–30%)

Define cloud computing

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

Describe the benefits of using cloud services

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

Describe cloud service types

- Describe infrastructure as a service (IaaS)
- Describe platform as a service (PaaS)
- Describe software as a service (SaaS)
- Identify appropriate use cases for each cloud service type (IaaS, PaaS, and SaaS)

Describe Azure architecture and services (35–40%)

Describe the core architectural components of Azure

- Describe Azure regions, region pairs, and sovereign regions
- Describe availability zones
- Describe Azure datacenters
- Describe Azure resources and resource groups
- Describe subscriptions
- Describe management groups

- Describe the hierarchy of resource groups, subscriptions, and management groups

Describe Azure compute and networking services

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

Describe Azure storage services

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

Describe Azure identity, access, and security

- Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services
- Describe authentication methods in Azure, including single sign-on (SSO), multi-factor authentication (MFA), and passwordless
- Describe external identities in Azure, including business-to-business (B2B) and business-to-customer (B2C)
- Describe Microsoft Entra Conditional Access
- Describe Azure role-based access control (RBAC)
- Describe the concept of Zero Trust
- Describe the purpose of the defense-in-depth model
- Describe the purpose of Microsoft Defender for Cloud

Describe Azure management and governance (30–35%)

- Describe cost management in Azure
- Describe factors that can affect costs in Azure
- Compare the pricing calculator and the Total Cost of Ownership (TCO) Calculator
- Describe cost management capabilities in Azure
- Describe the purpose of tags
- Describe features and tools in Azure for governance and compliance
- Describe the purpose of Microsoft Purview in Azure
- Describe the purpose of Azure Policy
- Describe the purpose of resource locks
- Describe features and tools for managing and deploying Azure resources
- Describe the Azure portal
- Describe Azure Cloud Shell, including Azure Command-Line Interface (CLI) and Azure PowerShell
- Describe the purpose of Azure Arc
- Describe infrastructure as code (IaC)
- Describe Azure Resource Manager (ARM) and ARM templates
- Describe monitoring tools in Azure
- Describe the purpose of Azure Advisor

- Describe Azure Resource Manager (ARM) and ARM templates
- Describe monitoring tools in Azure
- Describe the purpose of Azure Advisor
- Describe Azure Service Health
- Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

Cloud computing is the delivery of computing services over the internet.

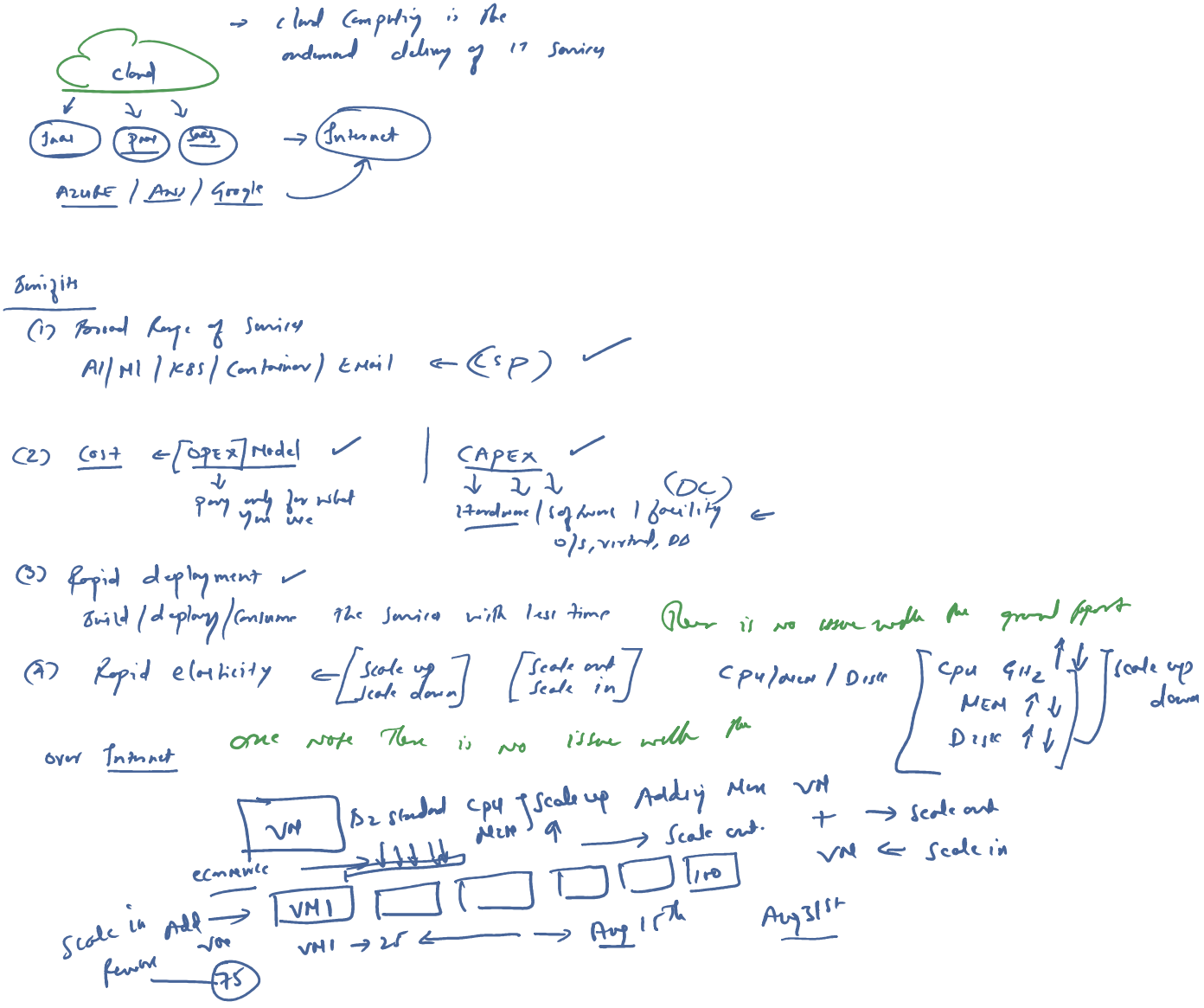
Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking.

Core
Compute
Storage
networking

Cloud services also expand the traditional IT offerings to include things like Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI).

Because cloud computing uses the internet to deliver these services, it doesn't have to be constrained by physical infrastructure the same way that a traditional datacenter is.

Increase your IT infrastructure rapidly, you don't have to wait to build a new datacenter—you can use the cloud to rapidly expand your IT footprint.

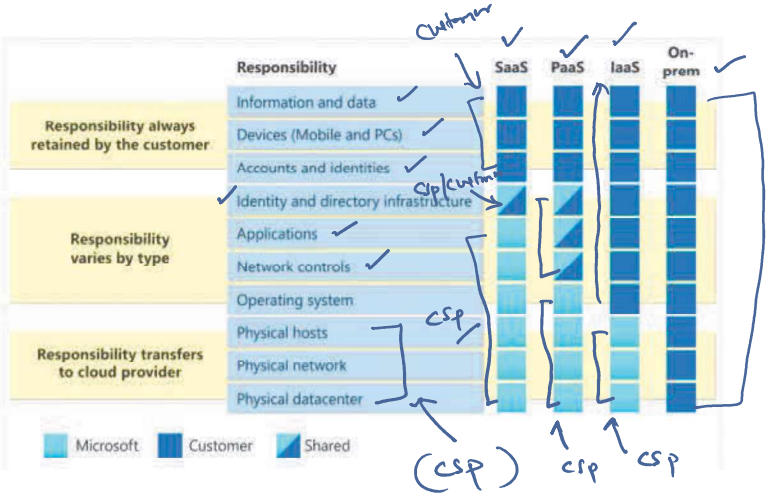


Corporate Datacenter / ON-PREM

- The company is responsible for maintaining the physical space, ensuring security, and maintaining or replacing the servers if anything happens
- The IT department is responsible for maintaining all the infrastructure and software needed to keep the datacenter up and running

Azure Cloud ✓

- With the shared responsibility model, these responsibilities get shared between the cloud provider and the consumer. Physical security, power, cooling, and network connectivity are the responsibility of the cloud provider



When using a cloud provider, you'll always be responsible for:

- The information and data stored in the cloud ✓
- Devices that are allowed to connect to your cloud (cell phones, computers, and so on) ✓
- The accounts and identities of the people, services, and devices within your organization

The cloud provider is always responsible for:

- The physical datacenter ✓
- The physical network ✓
- The physical hosts ✓

Your service model will determine responsibility for things like:

- Operating systems ✓
- Network controls ✓
- Applications ✓
- Identity and infrastructure ✓

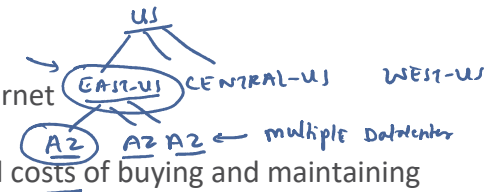
What is Azure ?

> Azure is a Microsoft public cloud computing platform (or) cloud service platform (or) cloud service provider (CSP)

> There are more than 200+ products / services which are offered by AZURE

NOTE: Not all the services are available in all the Regions check for the Resources in the Region on which you will be hosting your services

Microsoft Azure is a collection of services that connect you to that cloud via the Internet.



- Customers use the Cloud Services Offered by Azure using Subscription
  You can think of Azure as a **subscription IT service** delivered via the Internet
- Cloud-based IT can **save your business money** by eliminating the capital costs of buying and maintaining physical IT systems ✓
- Azure is far more cost-efficient, powerful, agile, reliable, and secure than off-cloud IT systems

Types of Cloud Services Offered:

IaaS ✓

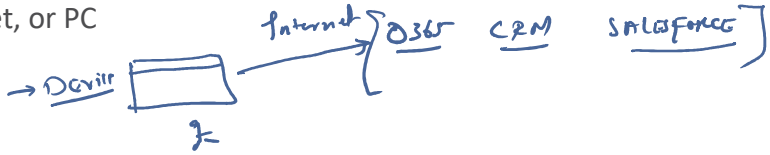
The most basic category of cloud computing services. With IaaS , you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems on a pay-as-you-go basis

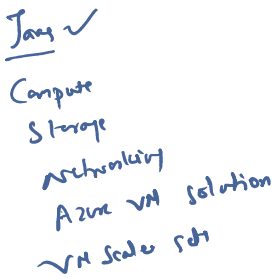
PaaS ✓

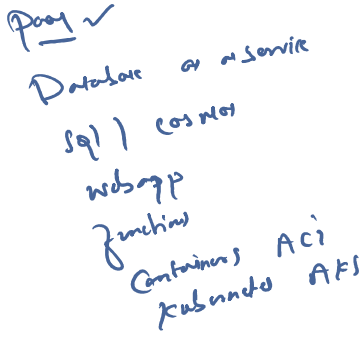
PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development

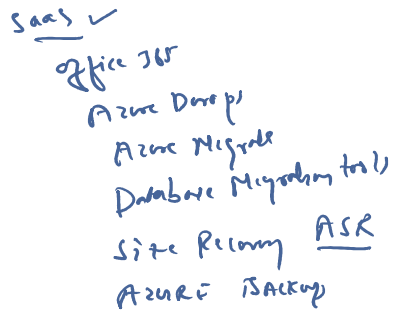
SaaS

SaaS is a method for delivering software applications over the internet, With SaaS, cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching. Users connect to the application over the internet, usually with a web browser on their phone, tablet, or PC









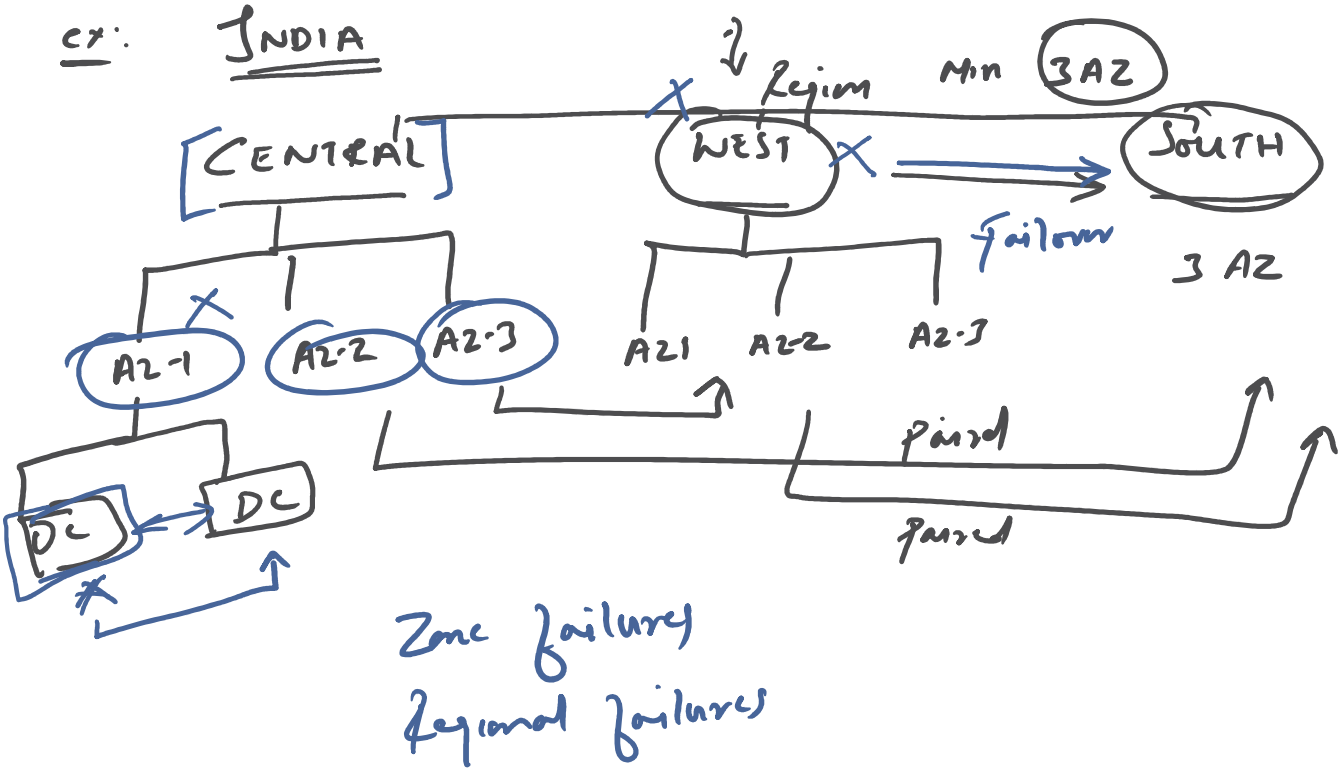
Regions

A Region is not a Country

Country ≠ Region

HA/DR

ex: INDIA



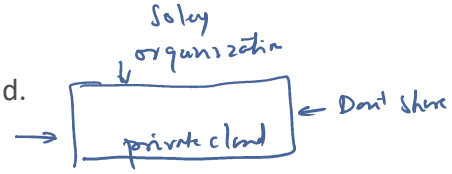
Zone failures

Regional failures

Cloud Deployment Models ✓

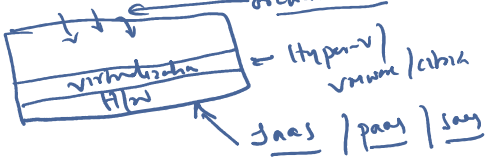
Define cloud models

The three main cloud models are: private, public, and hybrid.



Private cloud ✓

- A private cloud is, in some ways, the natural evolution from a corporate datacenter
- Private cloud provides much greater control for the company and its IT department ✓
- Cost is High as it has Capital Expenditure ✓
- Hosted in a dedicated datacenter even at a third party datacenter

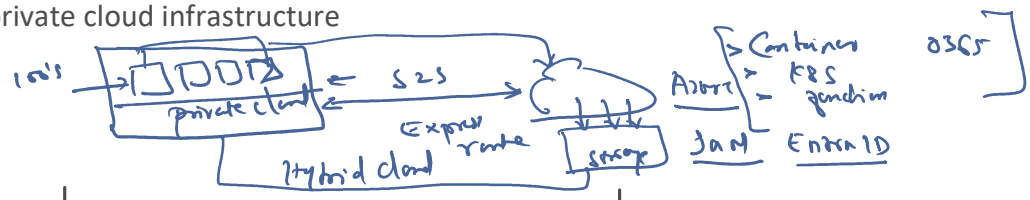


Public cloud ✓

- A public cloud is built, controlled, and maintained by a third-party cloud provider
- With a public cloud, anyone that wants to purchase cloud services can access and use resources
- The general public availability is a key difference between public and private clouds ✓

Hybrid cloud ✓

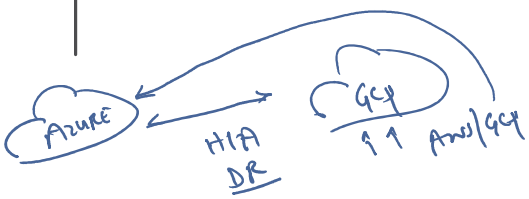
- A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment.
- If temporary demand not able to use Private Cloud, deploy resources on public cloud
- Hybrid cloud can be used to provide an extra layer of security. flexibly choose which services to keep in public cloud and which to deploy to their private cloud infrastructure



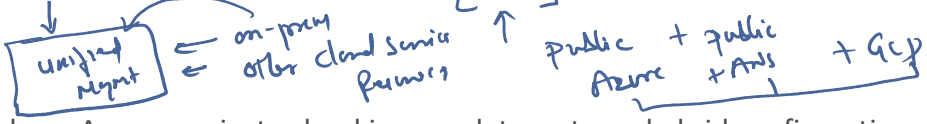
Cloud models Comparison ✓

Public cloud	Private cloud	Hybrid cloud
No capital expenditures ✓	Organizations have complete control over resources and security ✓	Provides the most flexibility ✓
Applications can be quickly provisioned and deprovisioned ✓	Data is not collocated with other organizations' data	Organizations determine where to run their applications ✓
Organizations pay only for what they use ✓	Hardware must be purchased for startup and maintenance	Organizations control security, compliance, or legal requirements
Organizations don't have complete control over resources and security ✓	Organizations are responsible for hardware maintenance and updates	

Multi-cloud



- In a multi-cloud scenario, you use multiple public cloud providers ✓
- Use different features from different cloud providers
- Or maybe you started your cloud journey with one provider and are in the process of migrating to a different provider
- In a multi-cloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments



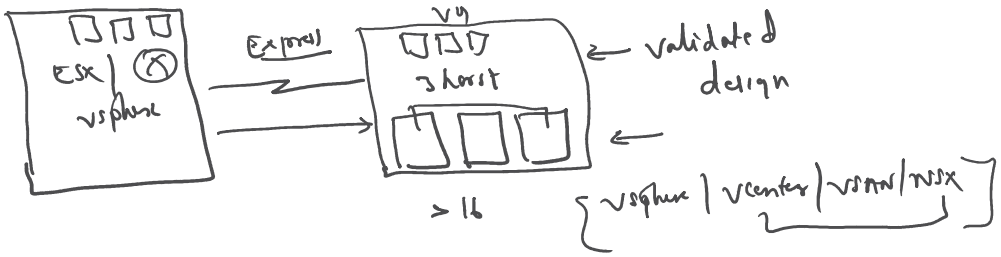
Azure Arc ✓

Manage public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration, or even a multi-cloud environment running on multiple cloud providers at once.

Azure VMware Solution ✓

Azure VMware Solution ✓

Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability



Cloud Deployment Models

(1) public

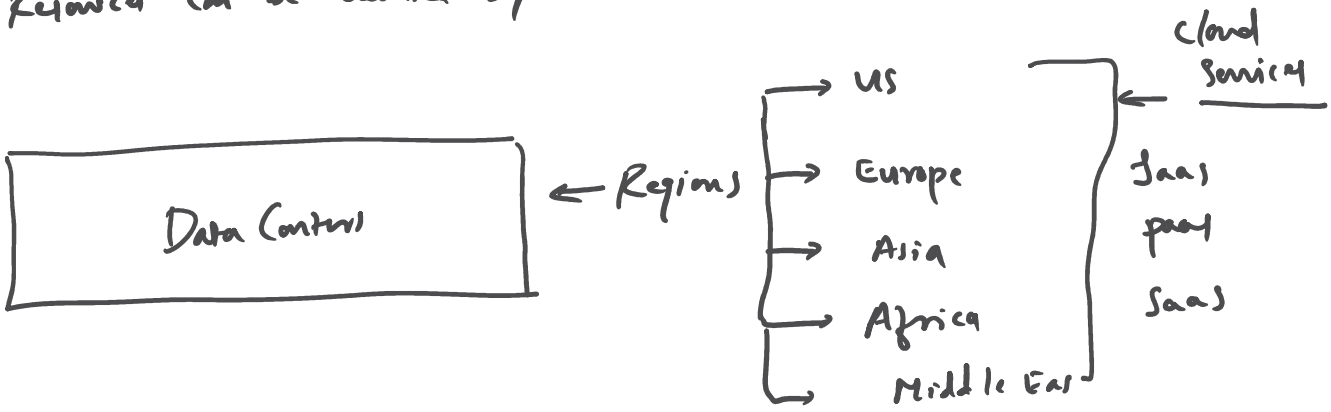
(2) private

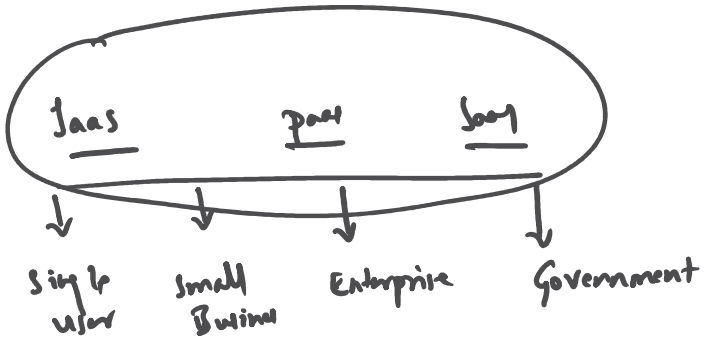
(3) Hybrid

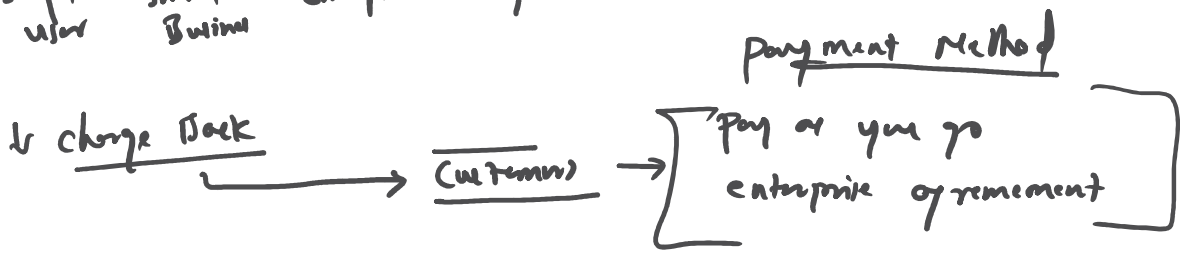
(4) Community

(1) public

> one organization owns
> Resources are shared to user
> Resources can be accessed by Internet







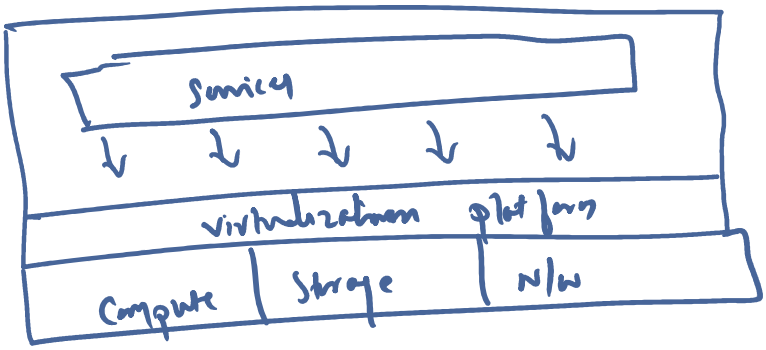
Summarize

pay for what you use

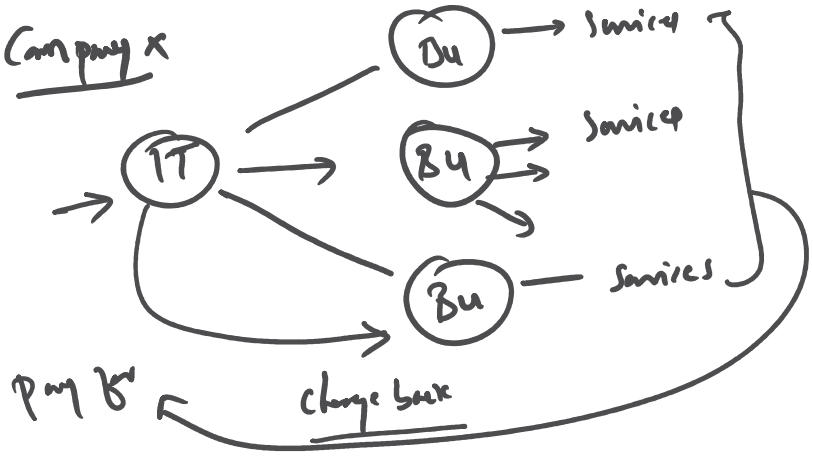
(2) private cloud

> an organization owns the complete cloud infra
  (or) solely owned by organization

> Resources will never be shared by any users or organizations

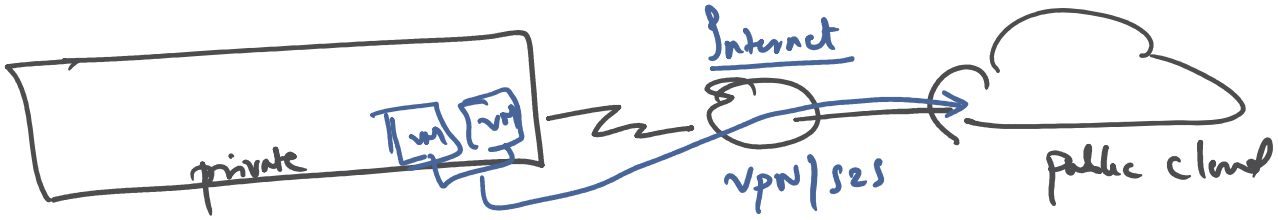


Hyper-V
VMware
citrix
← H/w layer



(3) Hybrid cloud ✓

(3) Hybrid Cloud



→ Container
→ A/D
→ Web
→ DB
→ file storage

Baas

private cloud + public cloud = Hybrid cloud

(4) Community cloud

→ agreement of the payment

> Common goal

Space agency

→ Insurance → Regulatory
→ Automobile →
→ Banking →

Cloud Deployment Models-Comparisons

Public cloud ← No Capital expenditure ✓
← OPEX Model ✓
← quickly provision the Resource (Rapid deployment)
← pay only for what we use ✓
← Security ← cloud provider owns the [DC | HW | software]
Responsible

CSP ↓ Control

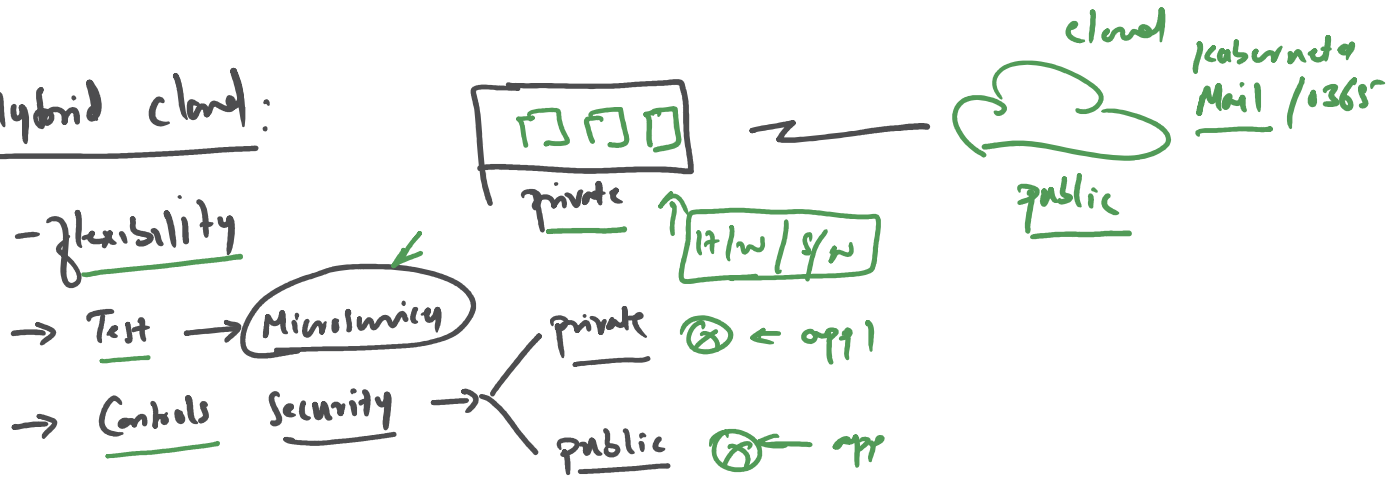
DC | Hardware | OS

Private cloud:

> organization has Complete Control
Datacenter | Hardware | Security | Data ←

> CAPEX Model Capital expenditure
Maintainance of Hardware / Software / DC

Hybrid cloud:



Multicloud

→ flexibility ✓
→ HA | DR
→ Cost ✓
→ Skills of Employees

Primary

Secondary

> organizations need upfront cost to purchase the hardware / software

DC

> organizations maintain the Assets

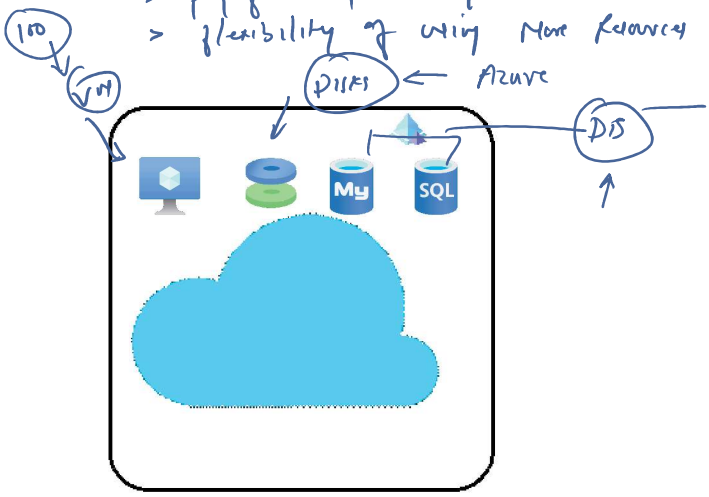
Assets = [Employee, Hardware, software, Datacenter]

Hardware, Storage, Networking

Consumption based Model

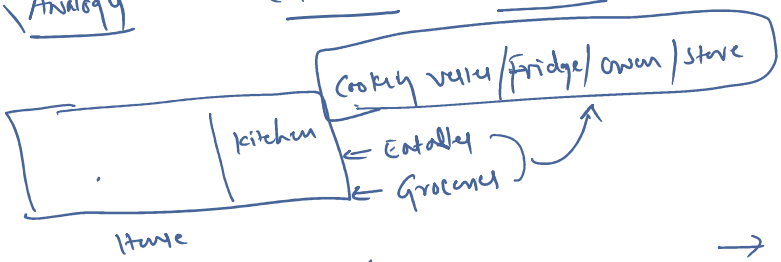
Opex ←

> upfront
> pay for only what you use
> flexibility of using more resources

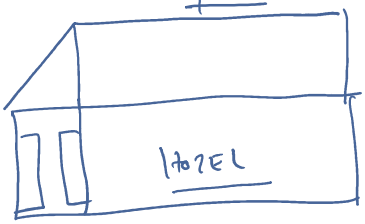


Analogy

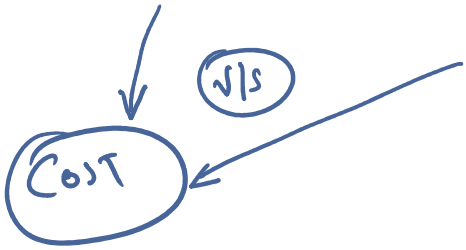
Customer X CAPEX



Opex



→ daily → pay for what he consumes
once in a month breakfast / Meals / dinner
→



→ Start up which they build → public cloud
CAPEX Model

→ Wanted to adopt for cloud native application
K8S → Microservices ← Containers
← functions
← Service bus
← Data Analytics

→ Test the application ← cloud ← delete

→ Deploy the services on cloud ← very fast

PRIVATE

→ Strict Regulatory Requirement ← private

→ Control of H/w / Data / facility

→ CAPEX → OPEX ← Time CMM

Hybrid cloud

→ flexibility of the services offered

→ Cashel app DB private → app public

→ TEST application ← private — Integrate

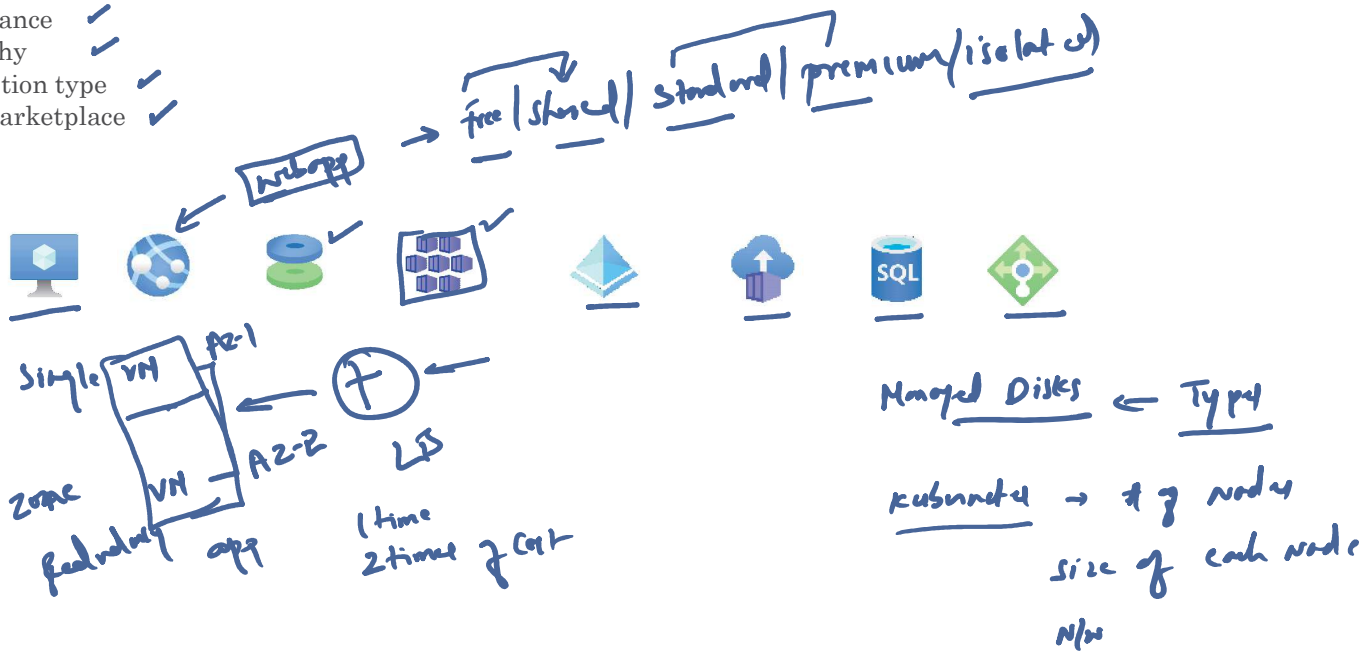
Hybrid cloud → private cloud + public cloud

Multi - cloud

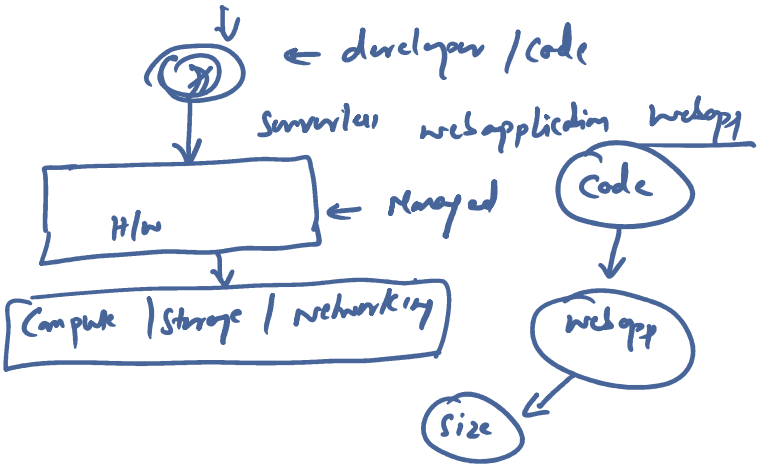
- flexibility of switching between the cloud vendors
→ keep all the services in multi - cloud
→ SLA
→ Cost → CSPA $$$ CSPB $$$$

That OpEx cost depends on these factors.

- Resource type ✔
- Consumption ✔
- Maintenance ✔
- Geography ✔
- Subscription type ✔
- Azure Marketplace ✔



With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code.

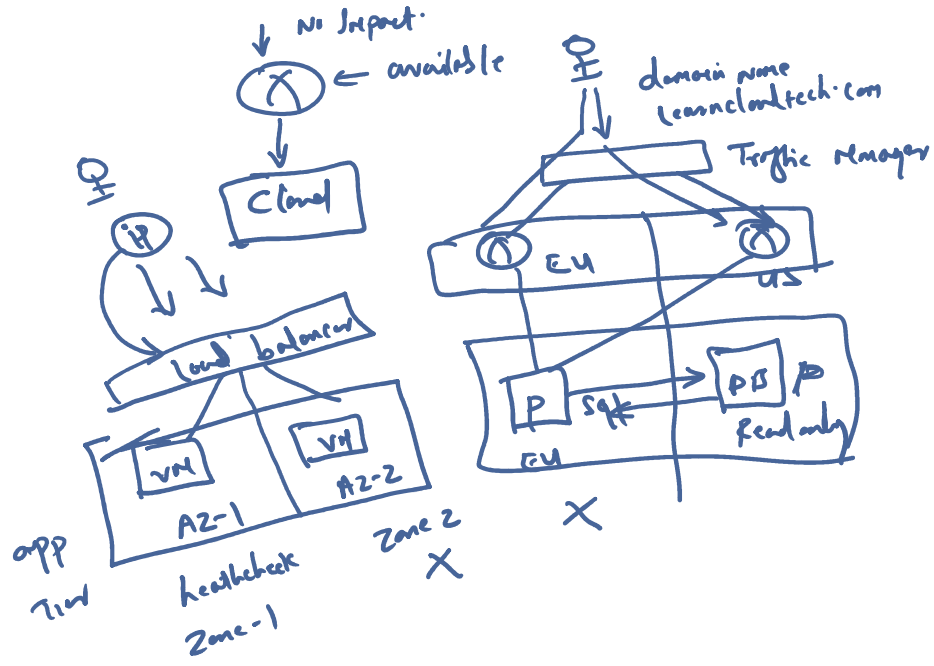


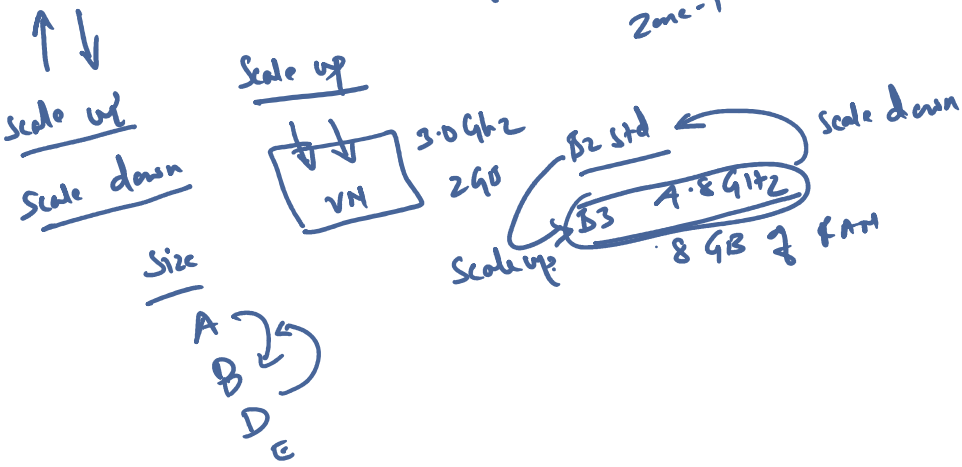
High availability

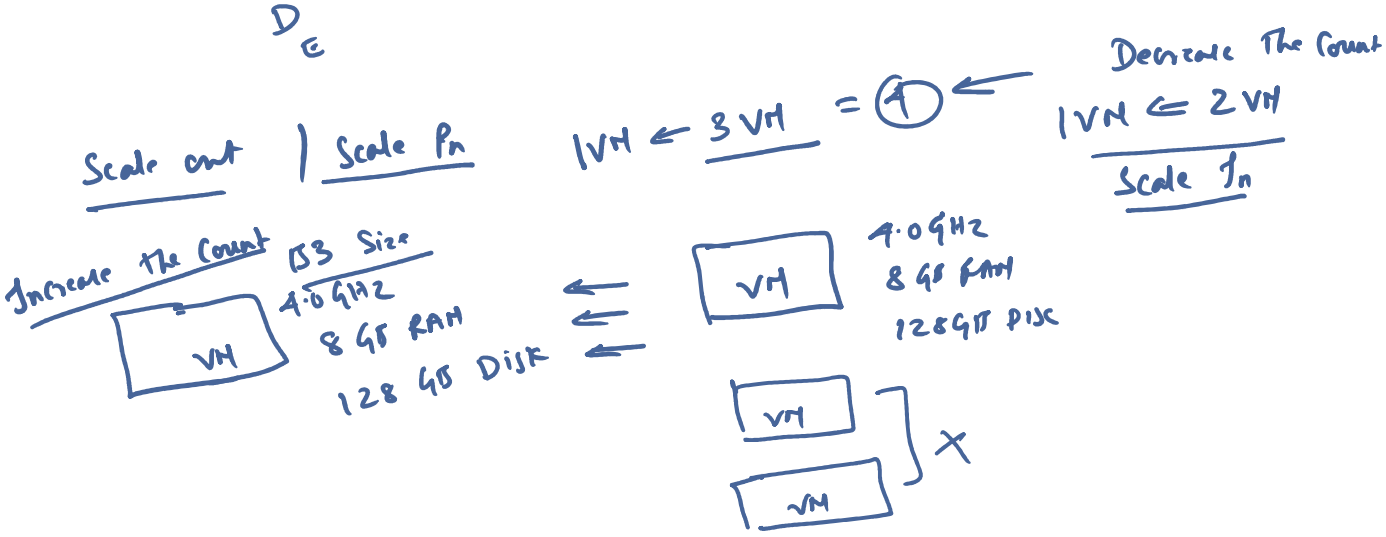
Deploy the Services with no downtime, even if there is an event or Outage

Scalability

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







SLA → Service level agreement

← Services

SLA's

SLA

- Standard HDD → 95%
- Standard SSD → 99.5%
- premium SSD → 99.9%

VM ← Availability set = 99.95%

DC-1

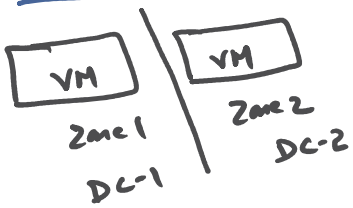
Multiple Racks

(function / Kubernetes / webapp)

Containers ← PaaS

99.95%

Availability zone = 99.99%

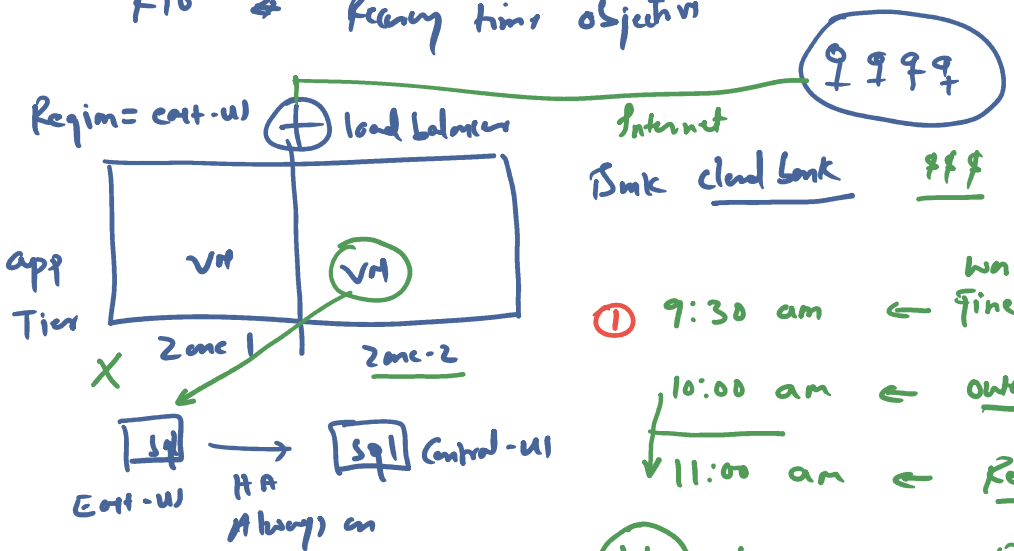


Traffic Manager = 99.99%

AZURE DNS = 100%

Rpo ← Recovery point objective

RTO ← Recovery time objective

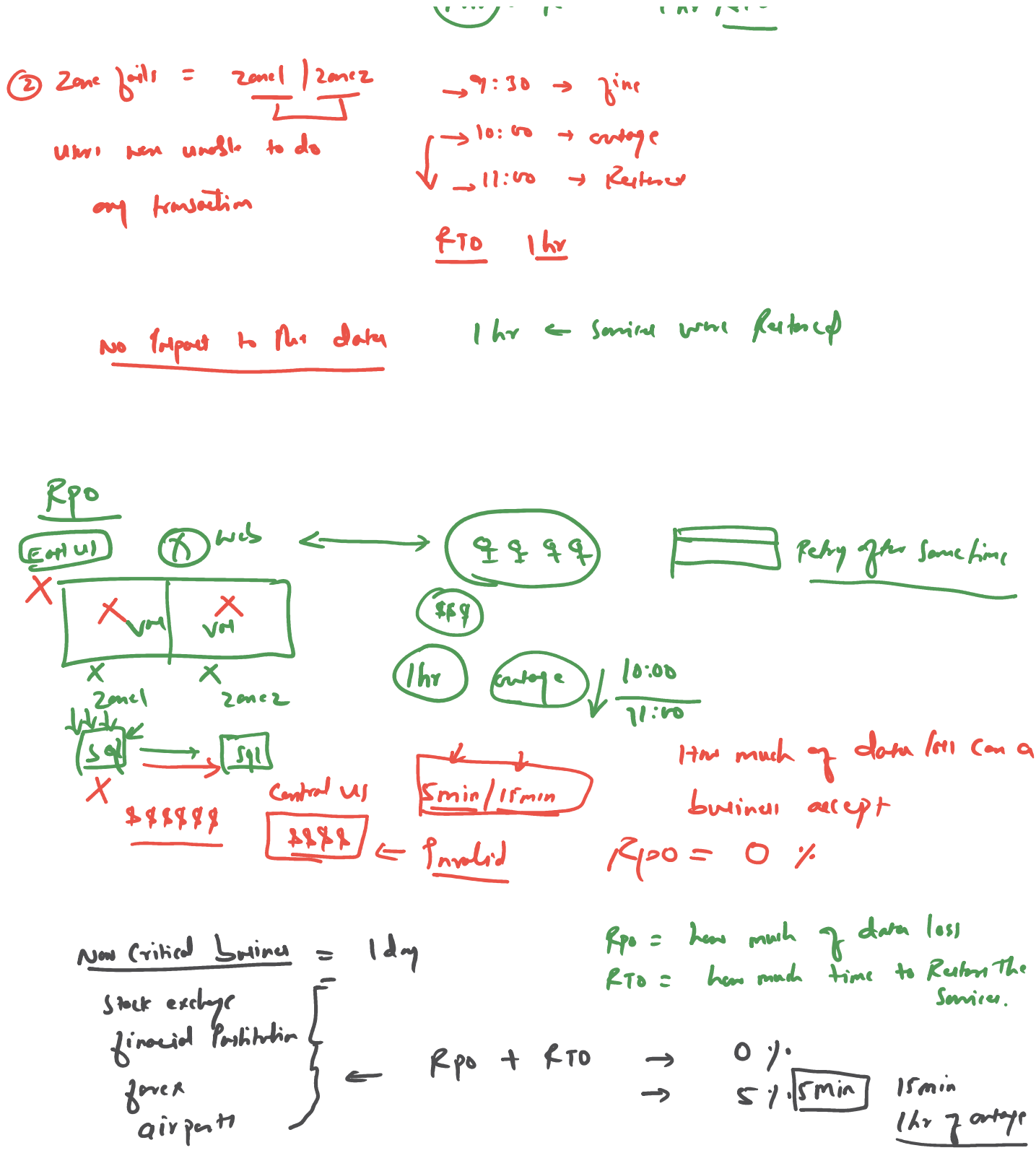


① 9:30 am ← working fine

10:00 am ← outage

11:00 am ← Restored ←

1 hr outage — 1 hr RTO

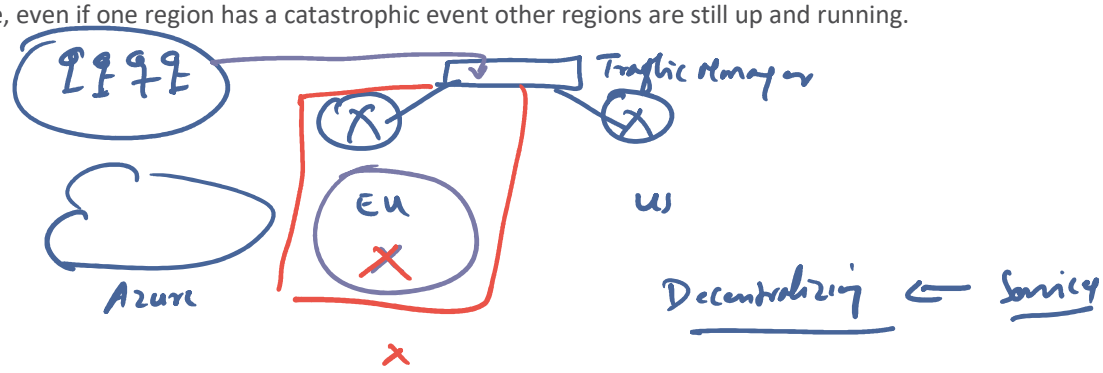


Reliability

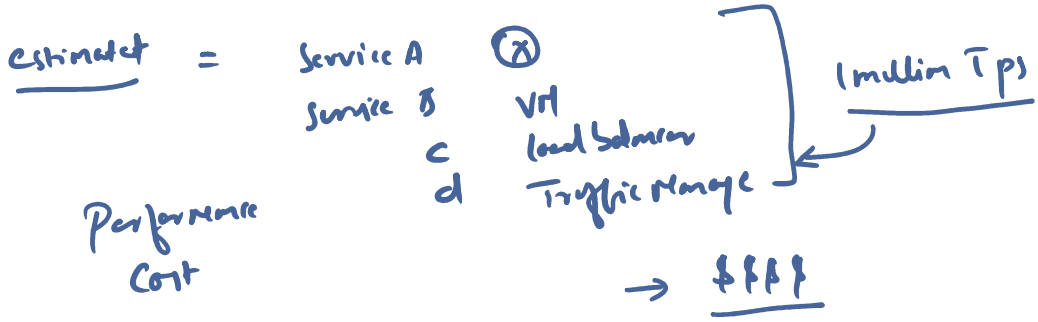
Reliability is the ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework

With a decentralized design, the cloud enables you to have resources deployed in regions around the world. With this global scale, even if one region has a catastrophic event other regions are still up and running.

this global scale, even if one region has a catastrophic event other regions are still up and running.

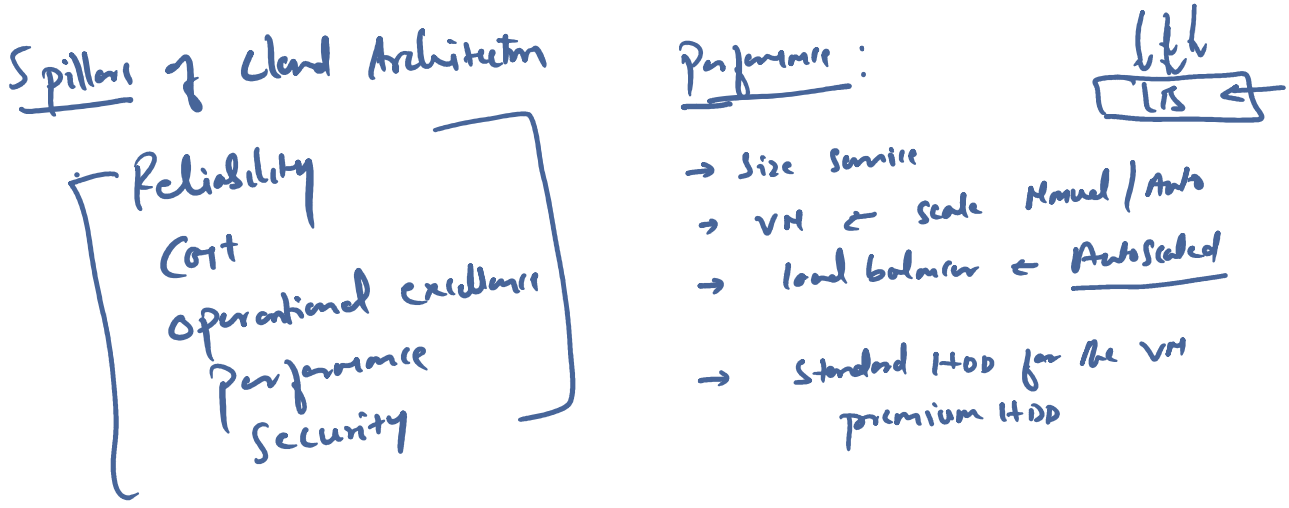


Predictability
Predictability in the cloud lets you move forward with confidence.
Can be focused on performance predictability or cost predictability.



Performance
Predicting the resources needed to deliver a positive experience

We can Achieve by Using:
Autoscaling, load balancing, and high availability, Proper Sizing of VM, Using Right Disks for VM's



- Reliability
  Cost
  operational excellence
  Performance
  Security

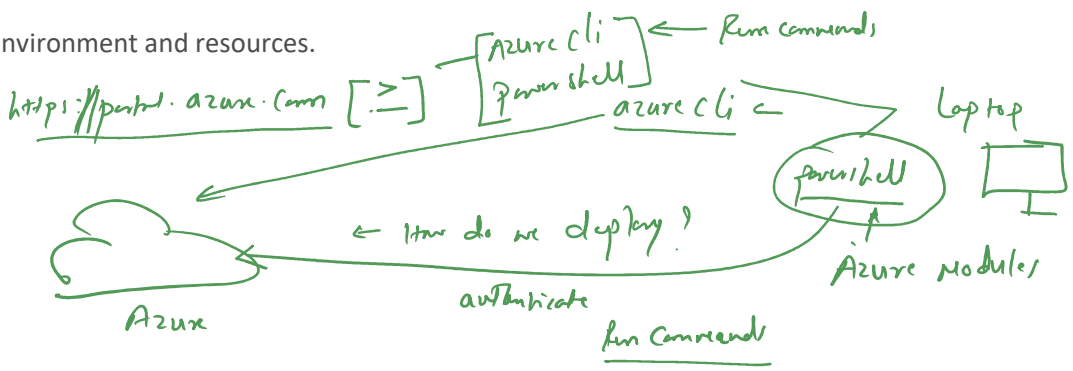
→ Size Service
→ VM ← Scale Manual / Auto
→ load balancer ← AutoScaled

→ Standard HDD for the VM
  premium HDD

Management in the cloud

How you manage your cloud environment and resources.

- Web portal. ✓
- CLI ✓
- PowerShell. ✓
- Using APIs. ✓



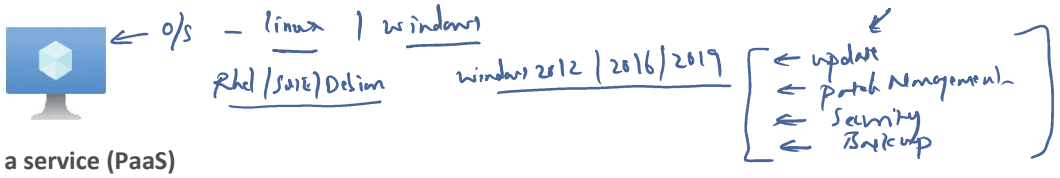
> portal
> cli Azure cli / powershell
> SDKs / Api
> Terraform ← Automate ← build of Infrastructure
3rd party → IAC

> Azure Resource Manager
Template
IAC
ARM

Infrastructure as a service (IaaS)
Flexible category of cloud services.
Maximum control of your cloud resources.
Cloud provider is responsible for maintaining the hardware

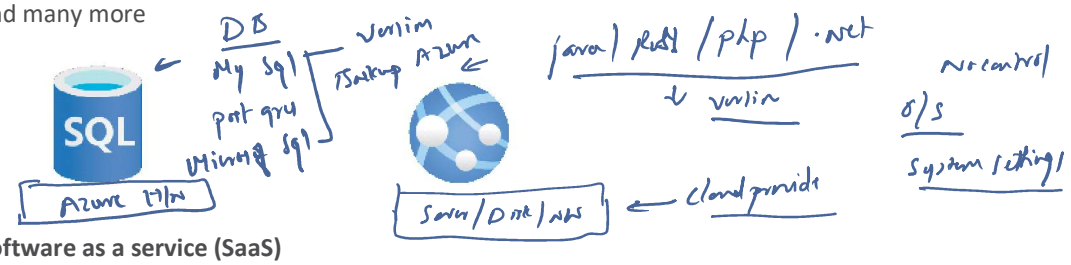
You're responsible for: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on.

Iaas Services: Virtual Machines, Network, Storage, Dedicated Hosts, Traffic Manager, Load Balancer, Express Route



Platform as a service (PaaS)
In a PaaS environment, cloud provider maintains the physical infrastructure, physical security,
They also maintain the operating systems, middleware, development tools
In a PaaS licensing or patching for operating systems and databases will be taken care by Cloud Service Provider

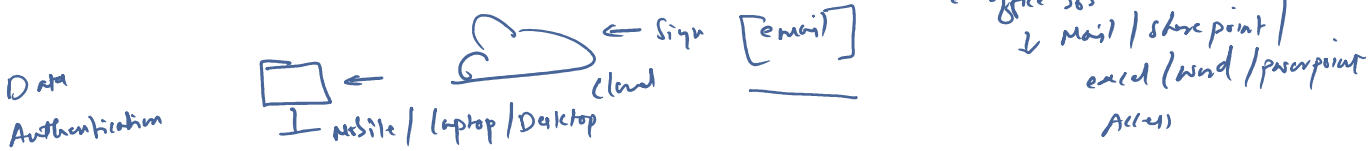
Paas Services: Webapp, Batch, Functions, Containers, Container Registry, Azure Kubernetes, SQl, Redis, Service Bus
and many more

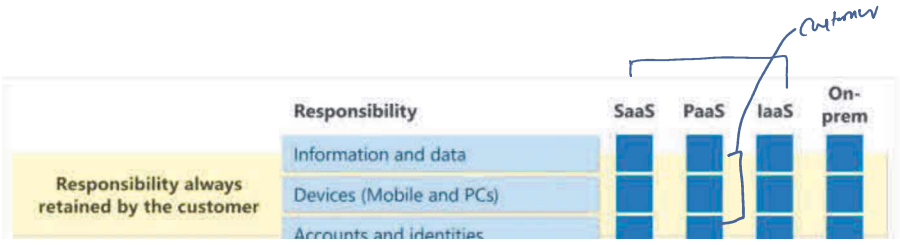


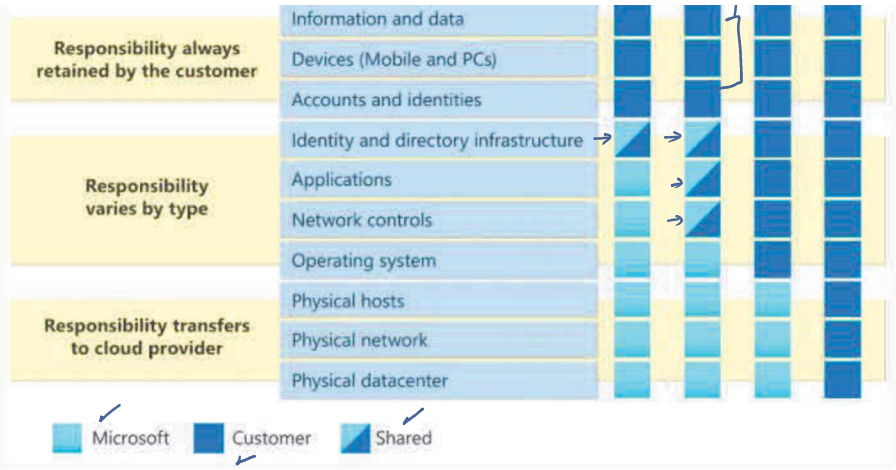
Software as a service (SaaS)
With SaaS, You sign in and access the services without deployment of any underlying Servers/Storage/Networking/Databases

Like Email, financial software, messaging applications

Paas Services: Office 365,Azure Devops, Power BI, Azure Advisor, Azure migrate







Database ← VM ← OS — (linux/windows) ← DB version ← configuration/settings

MySql

— Iaas

Database ← type ← version ← size ← Security ← patch management ← Backup ← Configuration/setting

Infrastructure

Paas

CRM / ENGil / Azure DevOps

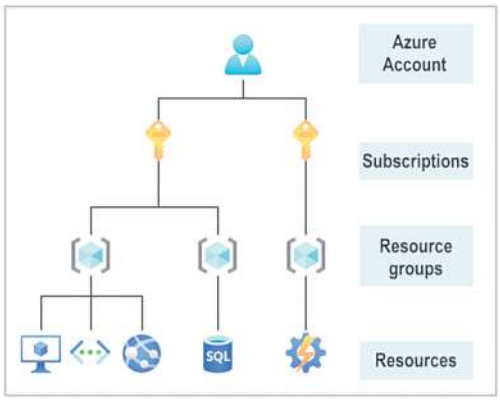
Saas

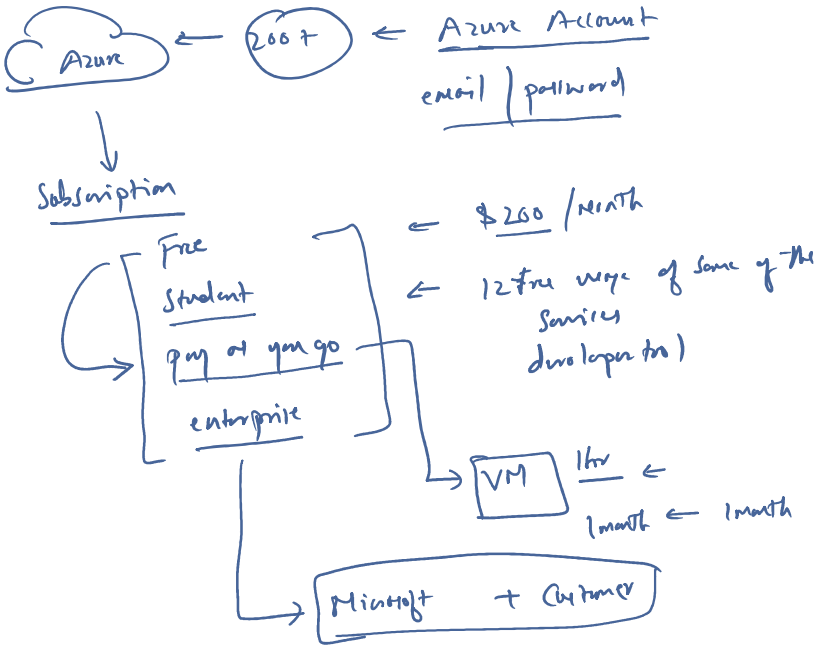
laptop/mobile

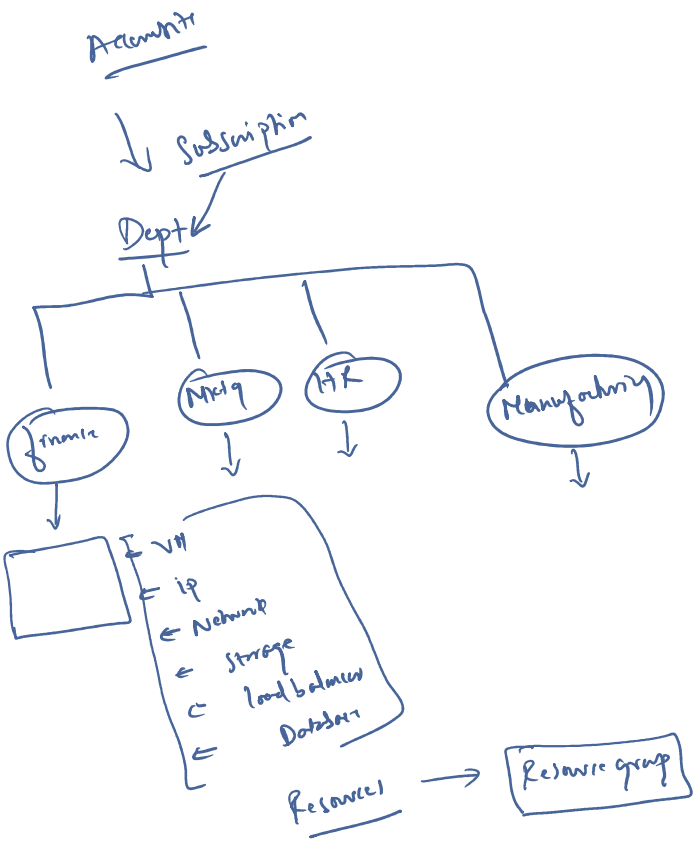
Azure cloud

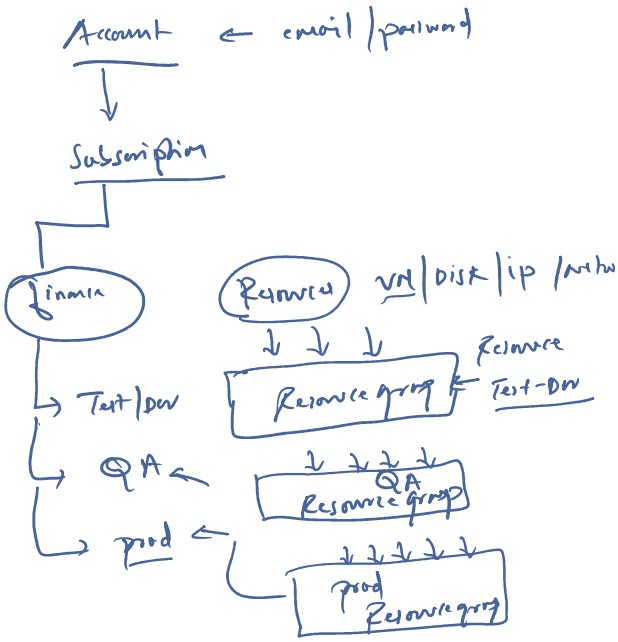
↳ Data

↳ Authentication

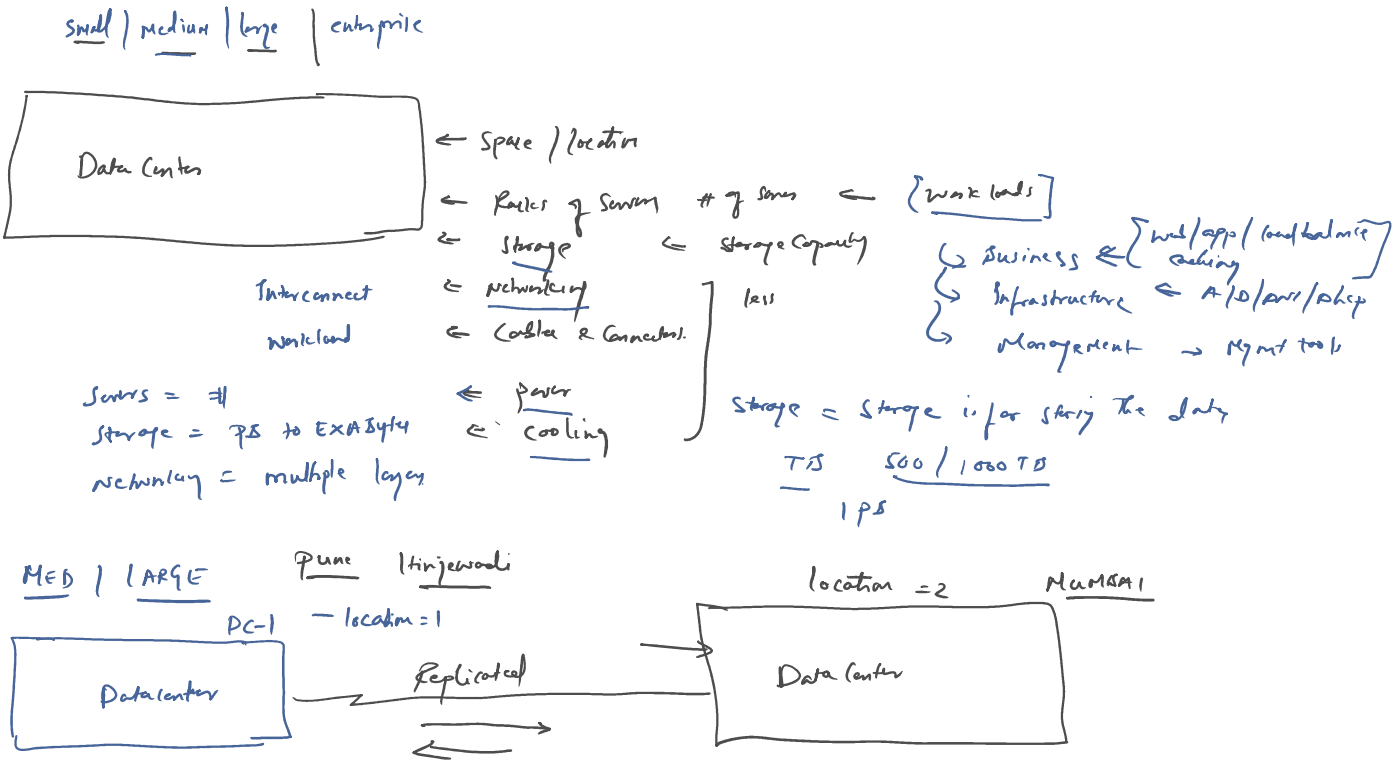

Azure Account
Subscriptions
Resource groups
Resources
SQL


Azure
2007
Azure Account
email | password
Subscription
Free
Student
pay as you go
enterprise
$200 / month
12 free ways of some of the services
VM
1hr
1month
1month
Microsoft + Customer


Account
Subscription
Dept
finance
HR
Manufacturing
VM
ip
Network
storage
load balancer
Database
Resources
Resource group

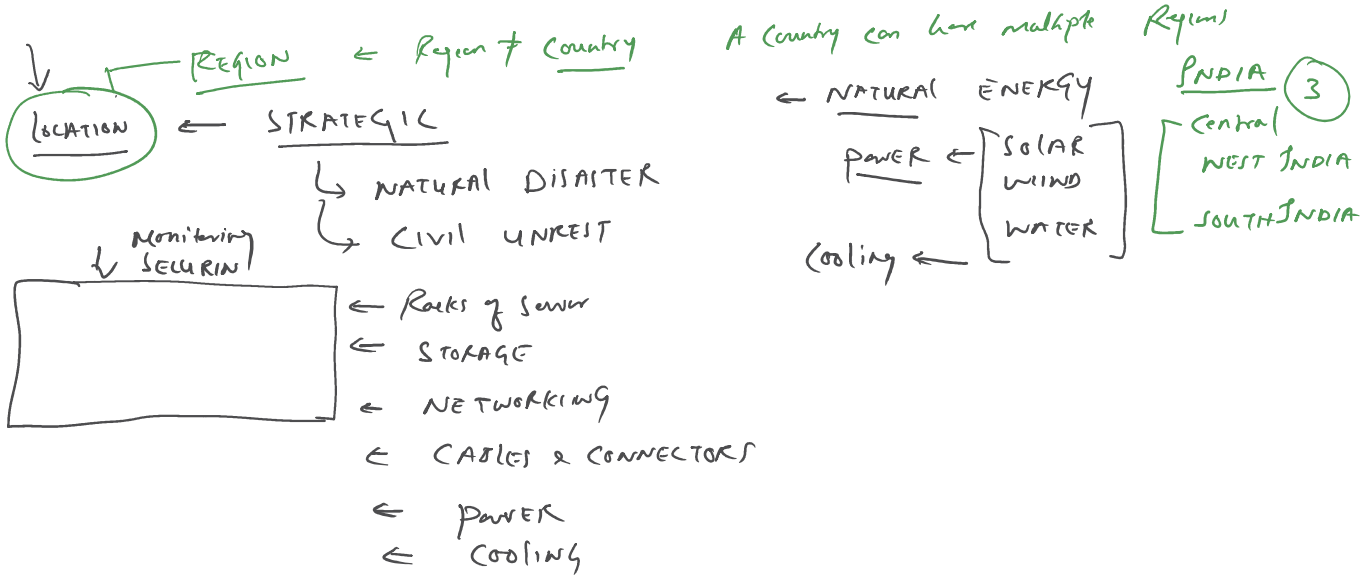

Account
email | password
Subscription
finance
Resources
VM | DISK | ip | network
Resource group
Resource
Test-Dev
Test|Dev
QA
Resource group
QA
prod
prod
Resource group

The datacenters are the same as large corporate datacenters.



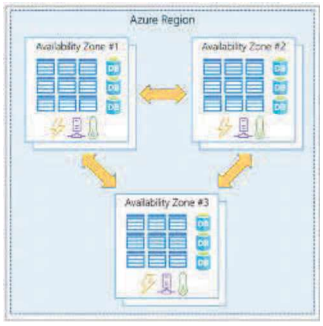
Regions

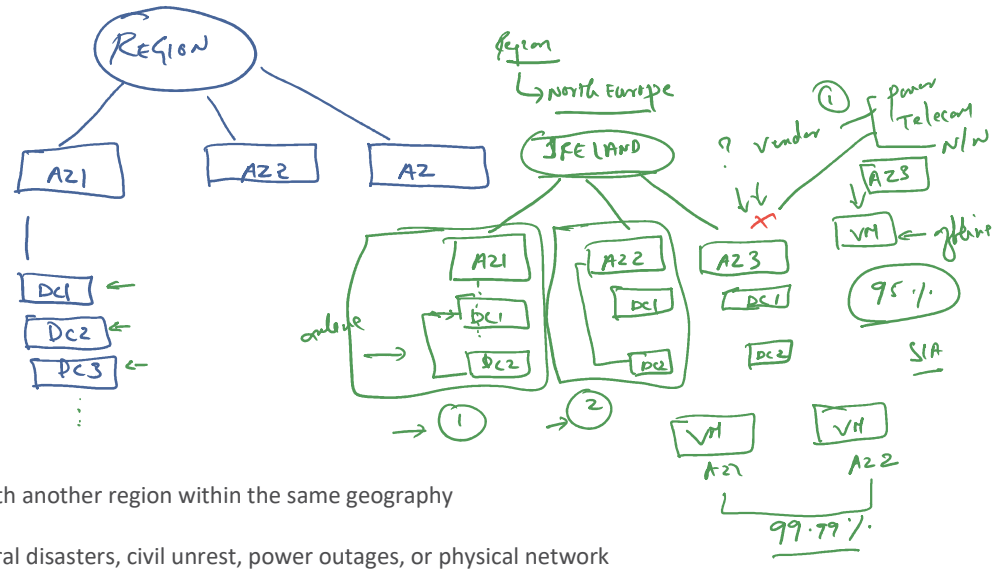
A region is a geographical area where Azure has placed their Data Center



Availability Zones

Availability zones are physically separate datacenters within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.



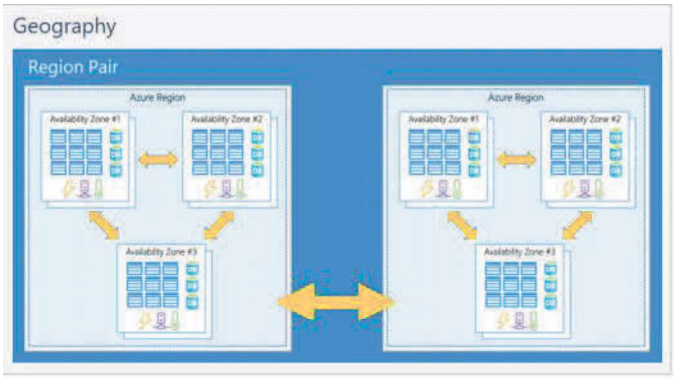


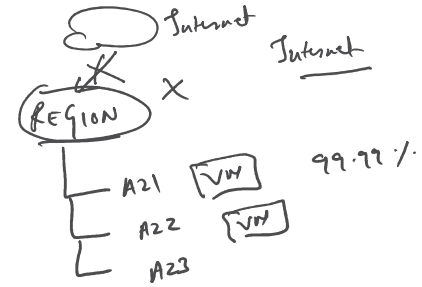
Region pairs

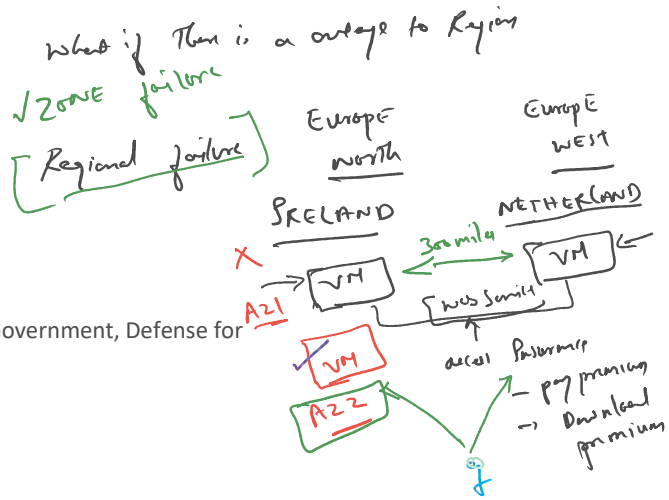
Most Azure regions are paired with another region within the same geography

At least 300 Miles away

To Avoid interruptions from natural disasters, civil unrest, power outages, or physical network outages that affect an entire region.



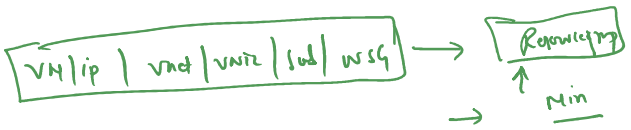




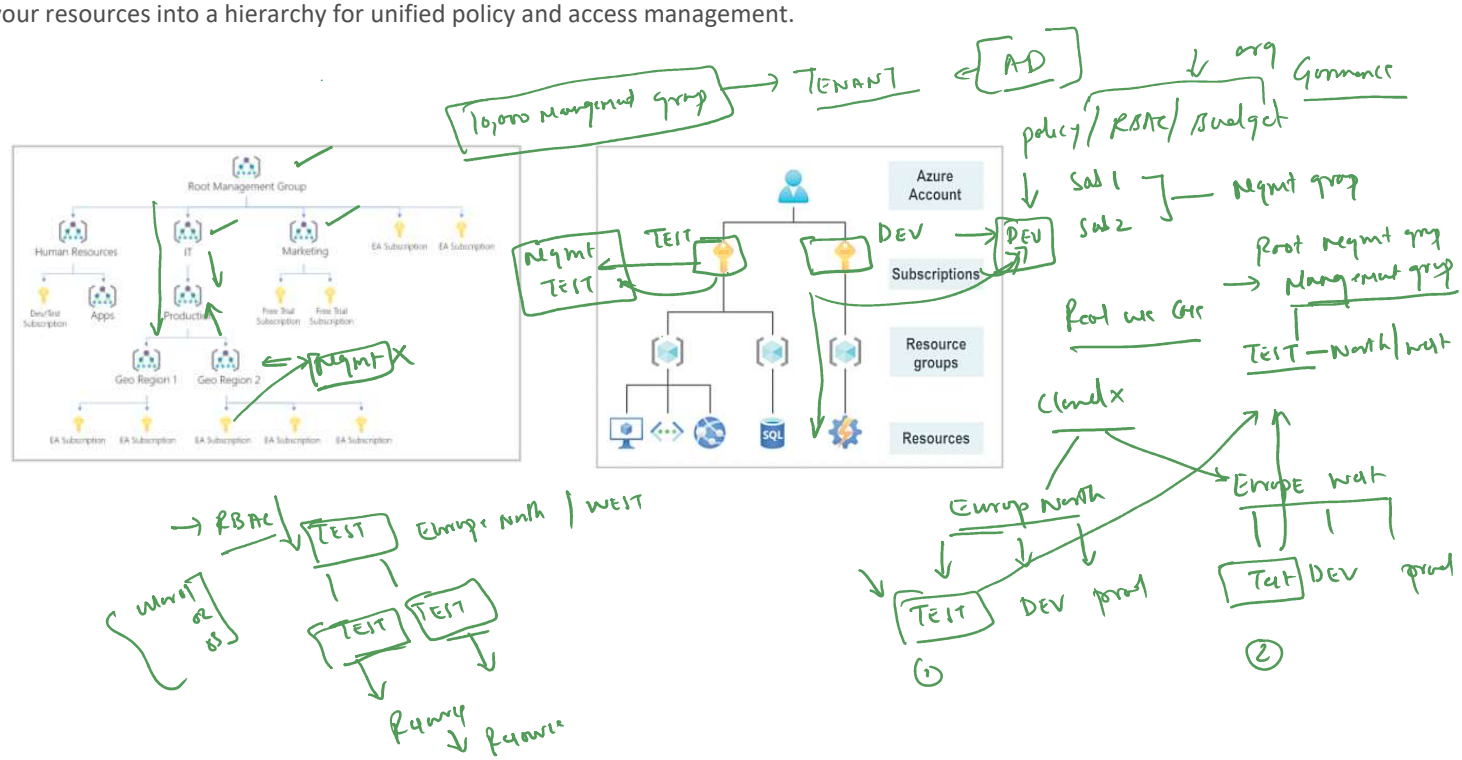
Sovereign Regions

Isolated from Main Azure Regions, there are exclusive for Government, Defense for compliance and regulatory reasons

The management infrastructure includes Azure resources and resource groups, subscriptions, and accounts.



You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management.

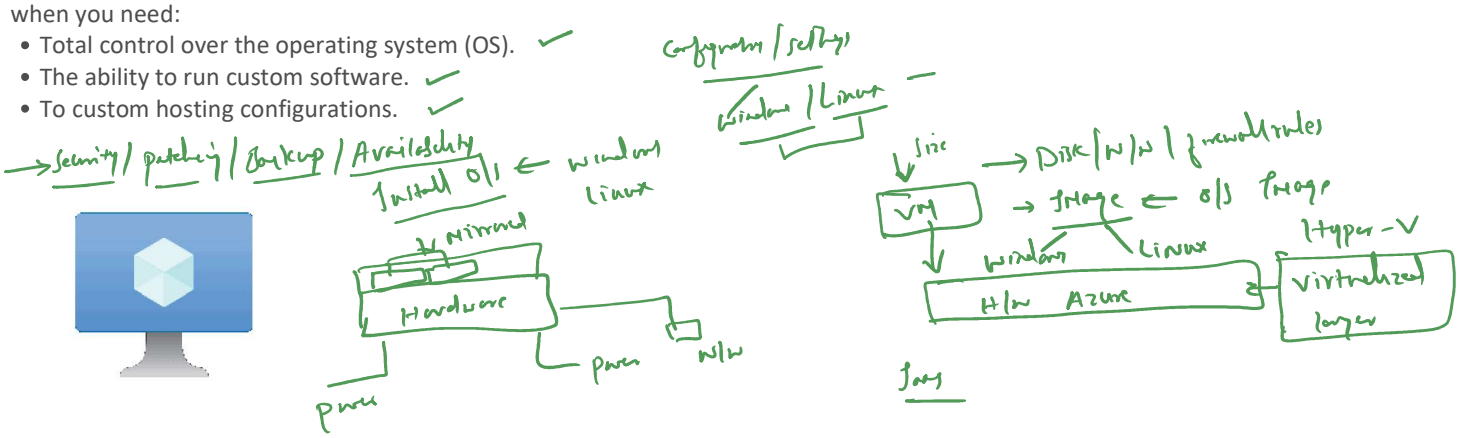


Create a hierarchy that applies a policy. You could limit VM locations to the US West Region in a group called Production

Provide user access to multiple subscriptions. By moving multiple subscriptions under a management group, you can create one Azure role-based access control (Azure RBAC) assignment on the management group.

VMs provide infrastructure as a service (IaaS) in the form of a virtualized server and can be used in many ways. Just like a physical computer, you can customize all of the software running on your VM. VMs are an ideal choice when you need:

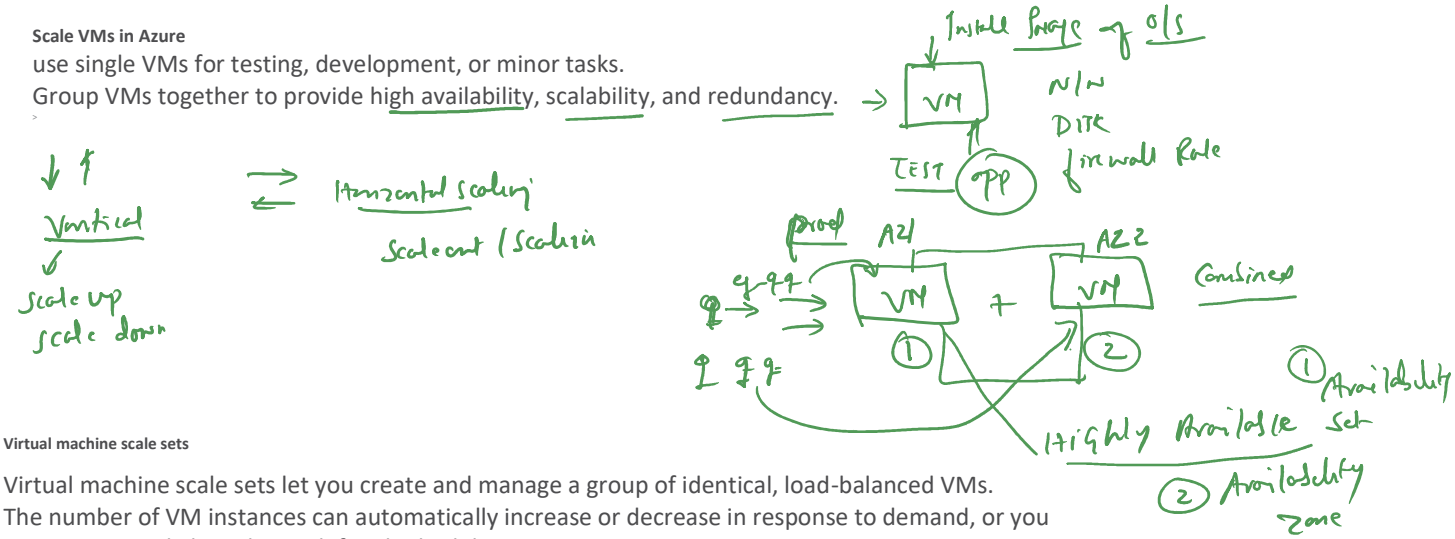
- Total control over the operating system (OS).
- The ability to run custom software.
- To custom hosting configurations.



Scale VMs in Azure

use single VMs for testing, development, or minor tasks.

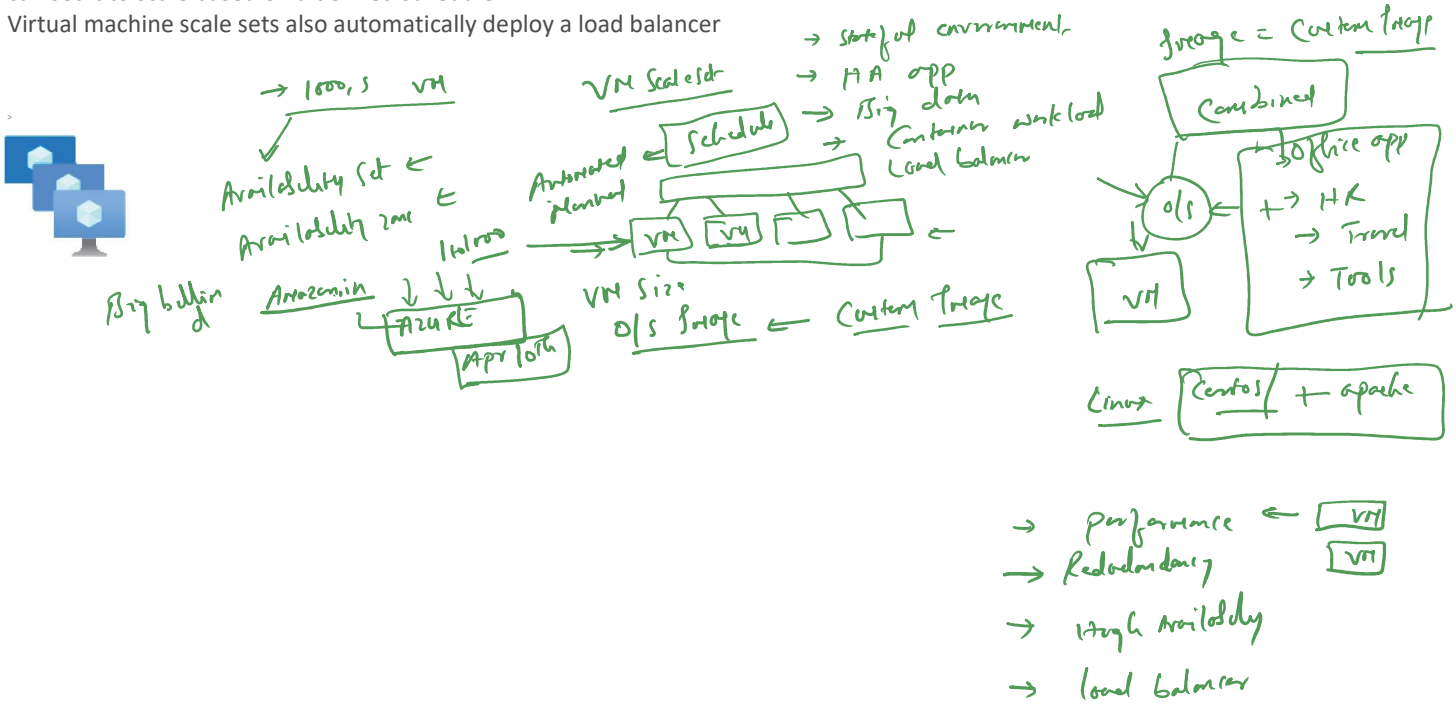
Group VMs together to provide high availability, scalability, and redundancy.

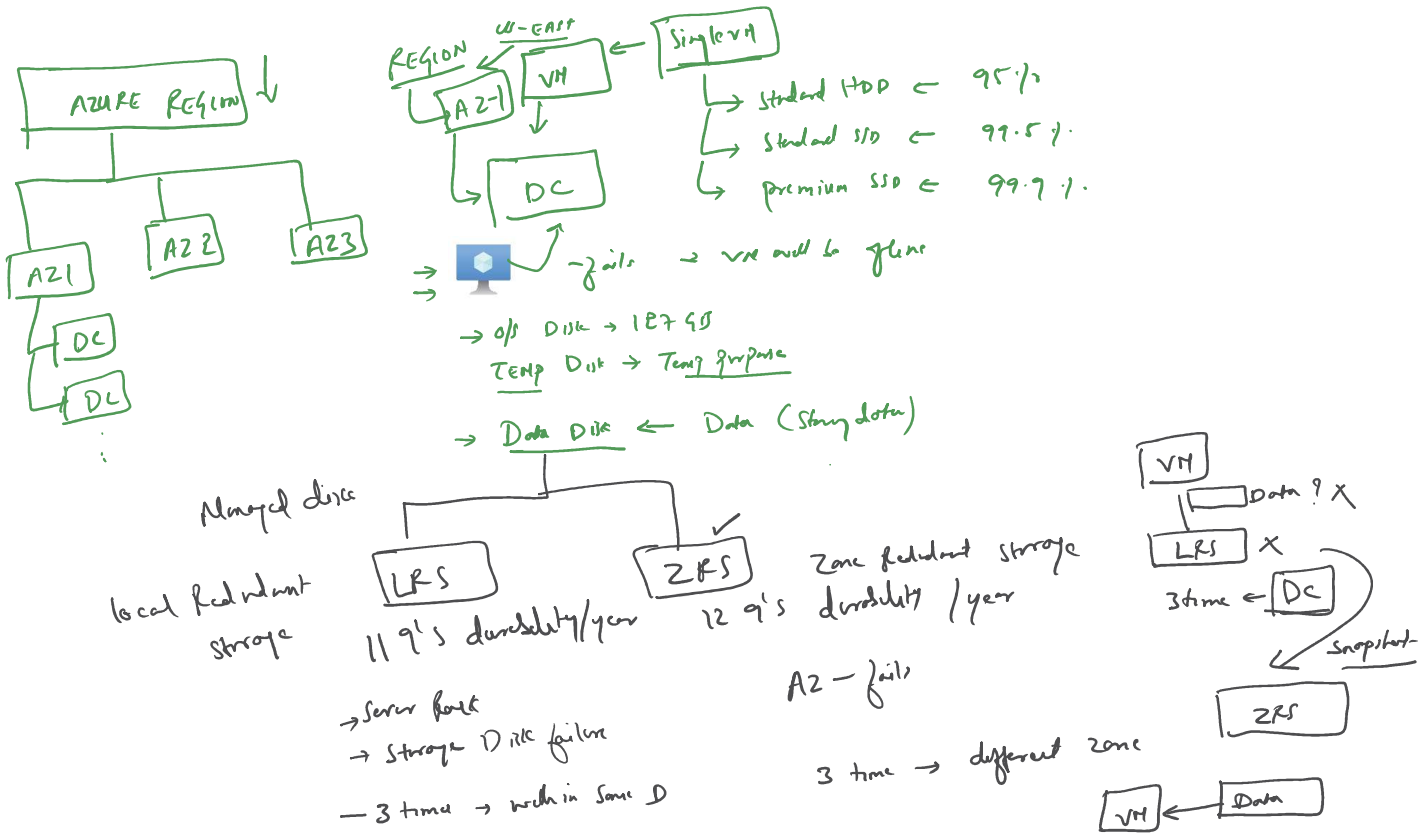


Virtual machine scale sets

Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs. The number of VM instances can automatically increase or decrease in response to demand, or you can set it to scale based on a defined schedule.

Virtual machine scale sets also automatically deploy a load balancer



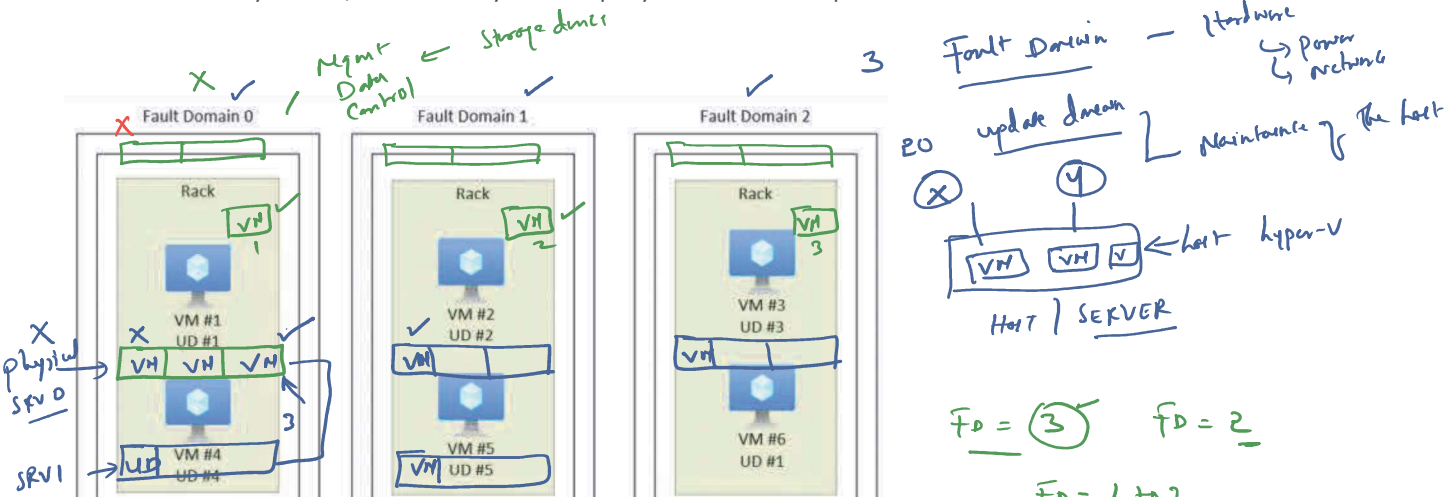


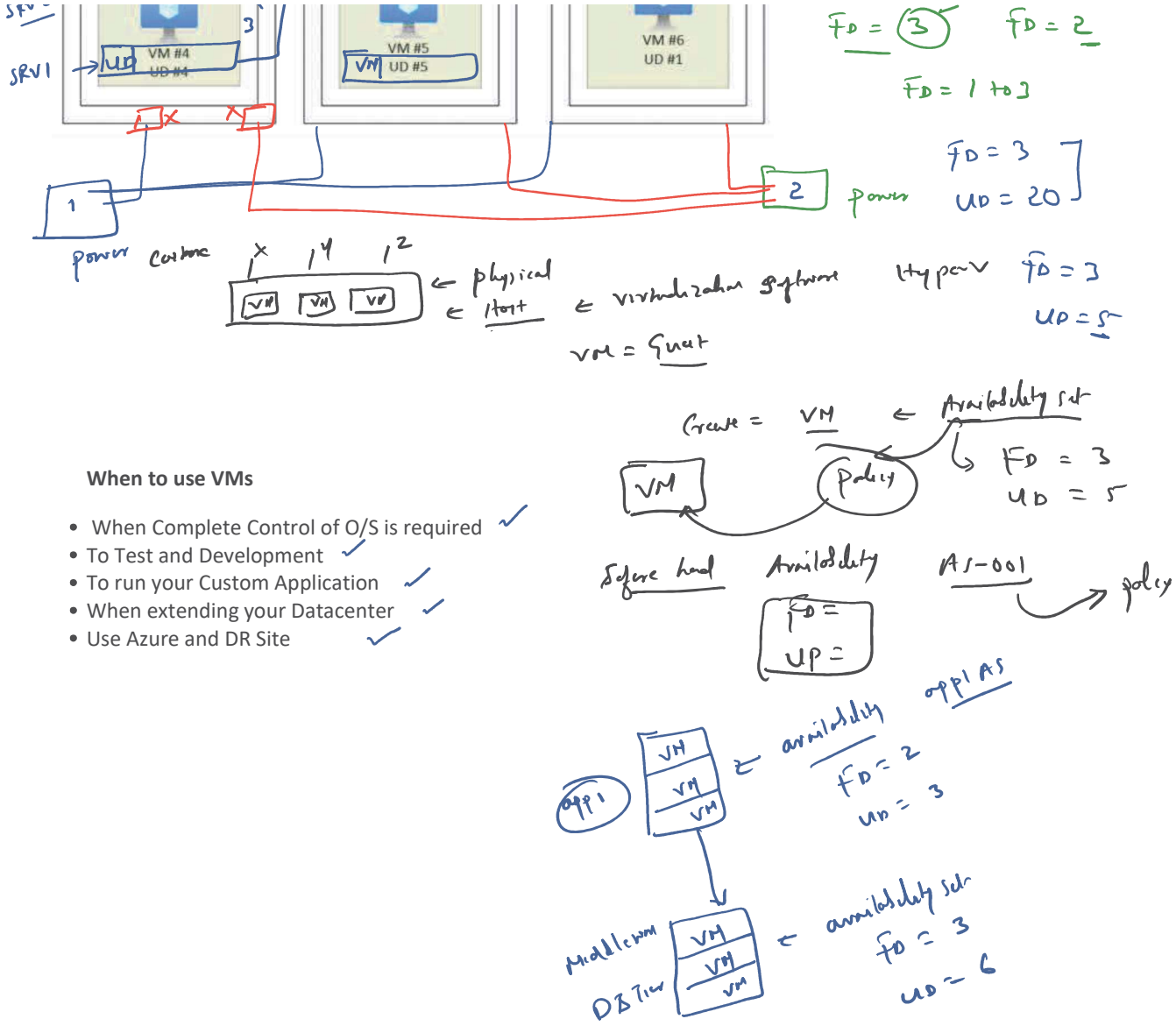
Virtual machine availability sets

Availability sets are designed to ensure that VMs are in different Power and Network connectivity, preventing you from losing all your VMs with a single network or power failure.

- **Update domain**: The update domain groups VMs that can be rebooted at the same time. the update process is given a 30-minute time to recover before maintenance on the next update domain starts.

- **Fault domain**: By default, an availability set will split your VMs across up to three fault domains.





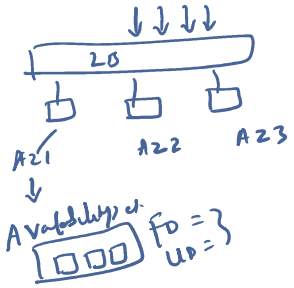
When to use VMs

- When Complete Control of O/S is required
- To Test and Development
- To run your Custom Application
- When extending your Datacenter
- Use Azure and DR Site

Virtual Machine Scale Sets, Availability Sets and Availability Zones

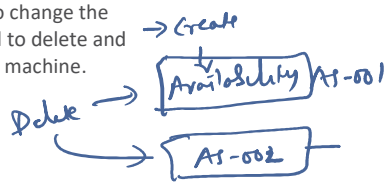
Virtual Machine Scale Sets

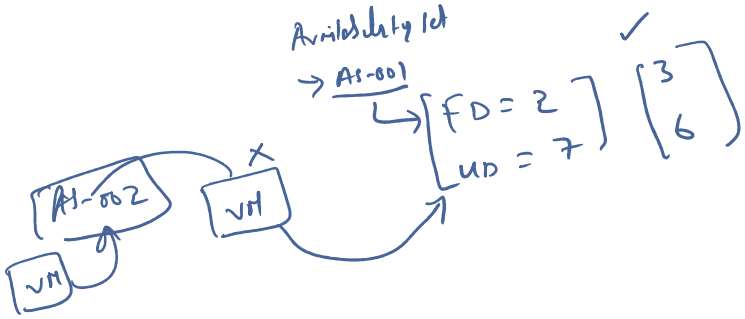
- Azure Virtual Machine Scale Sets let you create and manage a group of load balanced VMs.
- Automatic scaling of resources, and load balancing of traffic.
- VM size, disk configuration, and application installs should match across all VMs
- Scale sets support up to 1,000 VM instances for standard marketplace images and custom images
- High Availability, Can use Availability Sets and Availability Zones for VMSS



Availability Sets

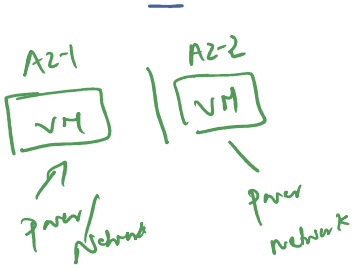
- Availability sets are logical groupings of VMs
- Availability sets use Fault Domain and Update Domain to Spread the VMs in Different Racks and Different Update Domain Groups
- When using availability sets, create two or more VMs within an availability set
- Availability sets offer improved VM to VM latencies compared to availability zones
- Availability sets are still susceptible to Data Center failures
- A VM can only be added to an availability set when it is created. To change the availability set, you need to delete and then recreate the virtual machine.





Availability Zones

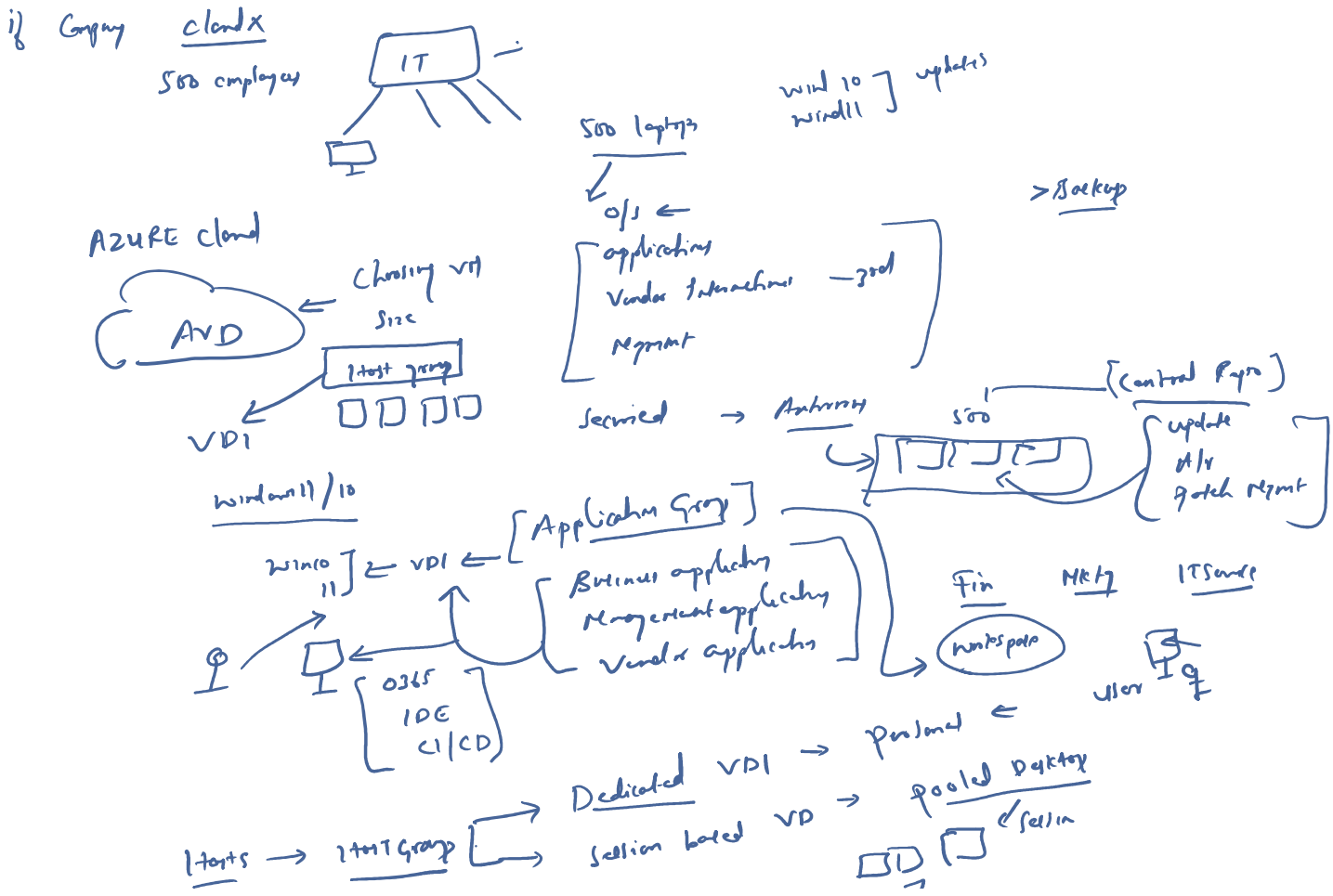
- Availability zones, which are separated groups of datacenters within a region
- Availability zones have independent power, cooling, and networking infrastructure
- Azure services to a single availability zone at a time.
- Round-trip latency of less than 2ms

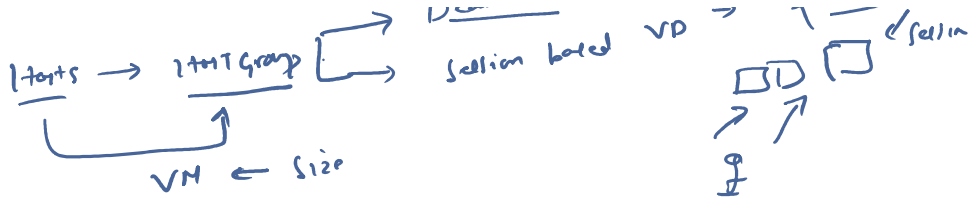


Azure Virtual desktop

Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. Deliver a full Windows experience with Windows 11, Windows 10, or Windows Server.

- Offer full desktops or use RemoteApp to deliver individual apps.
- Present Microsoft 365 Apps for enterprise and optimize it to run in multi-user virtual scenarios.
- Install your line-of-business or custom apps
- Manage desktops and apps from different Windows and Windows Server operating systems with a unified management experience.
- Host desktops and apps on-premises in a hybrid configuration with Azure Stack HCI.
- Bring your own image for production workloads or test from the Azure Gallery.
- Provide individual ownership through personal (persistent) desktops.
- Automatically increase or decrease capacity based on time of day, specific days of the week, or as demand changes with auto scale, helping to manage cost.
- You can deploy and manage virtual desktops and applications
- Use the Azure portal, Azure CLI, PowerShell and REST API to configure the host pools, create application groups, assign users, and publish resources.

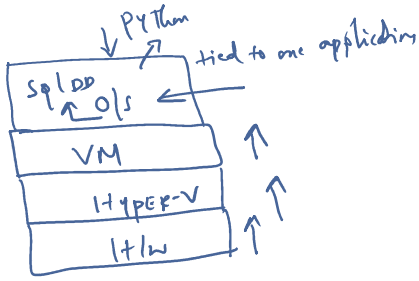



Starts
Start Group
VM
Size
VD

Azure Containers

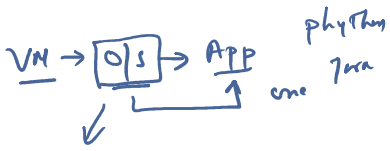
- Containers are a virtualization environment.
- Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host
- Containers are lightweight and designed to be created, scaled out, and stopped dynamically
- Azure supports Docker.

Docker is open source platform for running the Containers



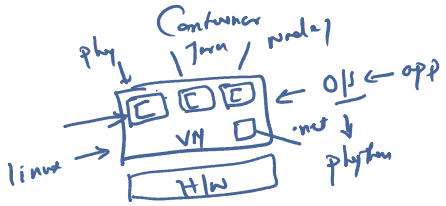
Azure Container Instances

- Azure Container Instances offer the fastest and simplest way to run a container in Azure
- Azure Container Instances are a platform as a service (PaaS) offering.
- Azure Container Instances allow you to upload your containers and then the service will run the containers for you.



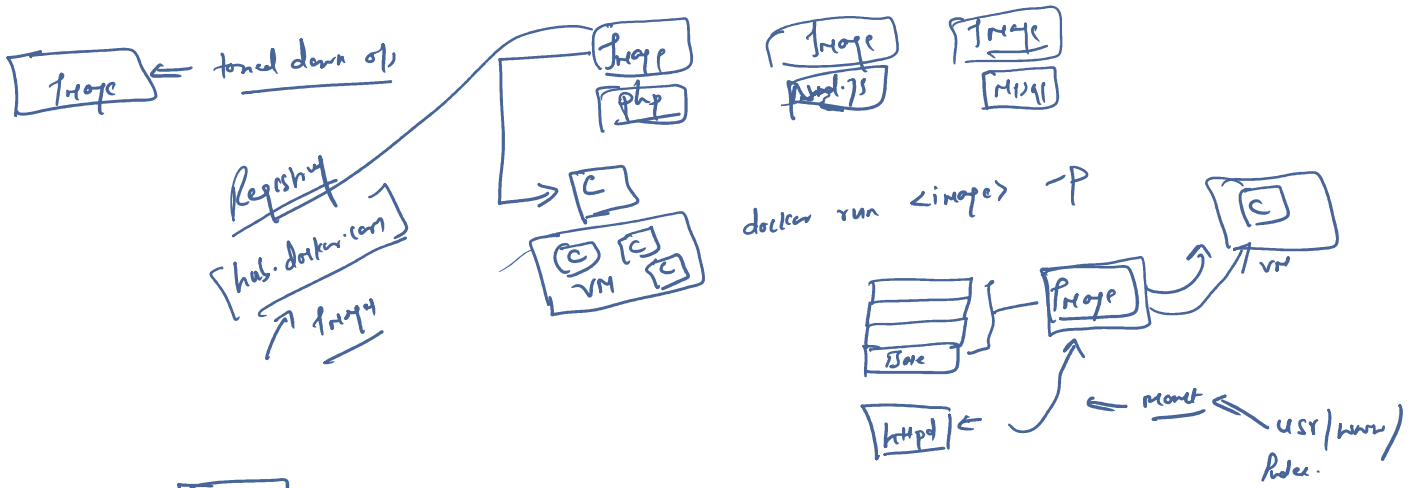
Azure Container Apps

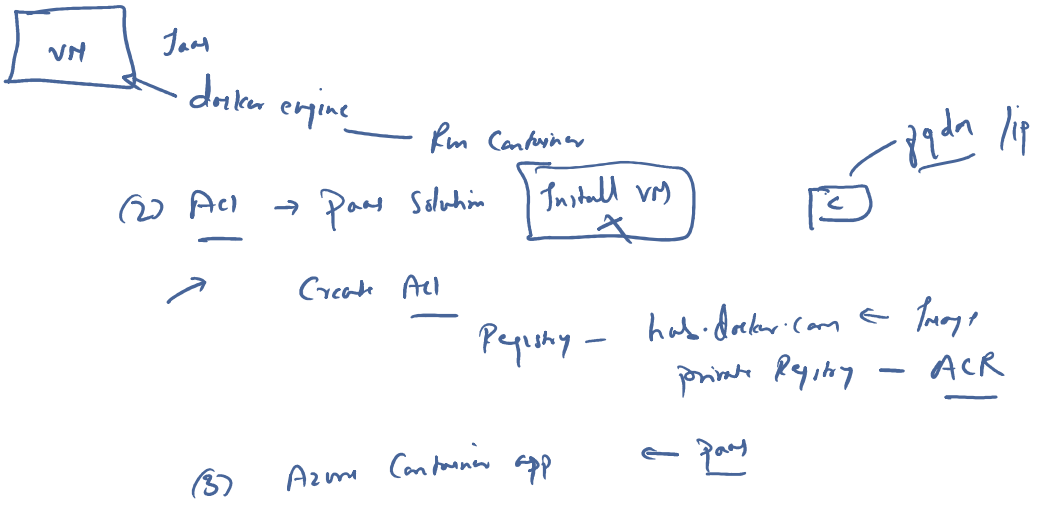
- Azure Container Apps are similar in many ways to a container instance.
- Container Apps have extra benefits such as the ability to incorporate load balancing and scaling.



Azure Kubernetes Service

- Azure Kubernetes Service (AKS) is a container orchestration service.
- An orchestration service manages the lifecycle of containers.



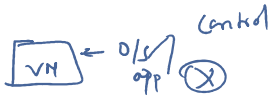


(8) Azure Container app ← Paas

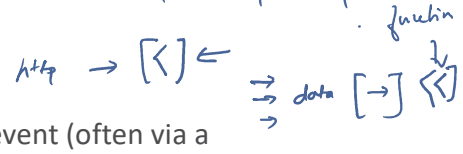
Container app Env → Scale
deployment slots
multiple runtime to choose
docker hub / ACR

(9) AKS
[pod]

Azure Functions



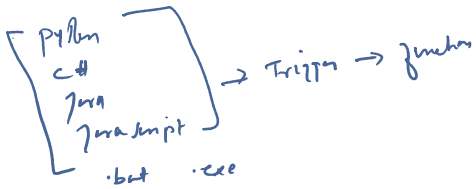
Microservices container | webapp | K8s

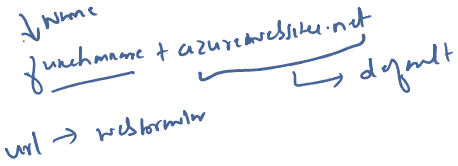


- Run the code and not worry about the underlying platform or infrastructure.
- Functions are commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service.
- Functions scale automatically based on demand. ✓

- Azure Functions runs your code when it's triggered and automatically deallocates resources when the function is finished. ✓
- Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event.
- When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.
- Functions are a key component of serverless computing.

→ https
→ queue
→ blob
→ Timer ✓
→ Event Grid based trigger





Hosting plans:

(1) Consumption ← event driven

(2) premium function ← N/W isolation
scale the function app on demand

(3) App Service plan ← choose the server / VM
↓ ↓ ↓
web app | mobile | web jobs | function

If you need to host your application on Azure Virtual machine (VM) or Containers.

Azure App Service

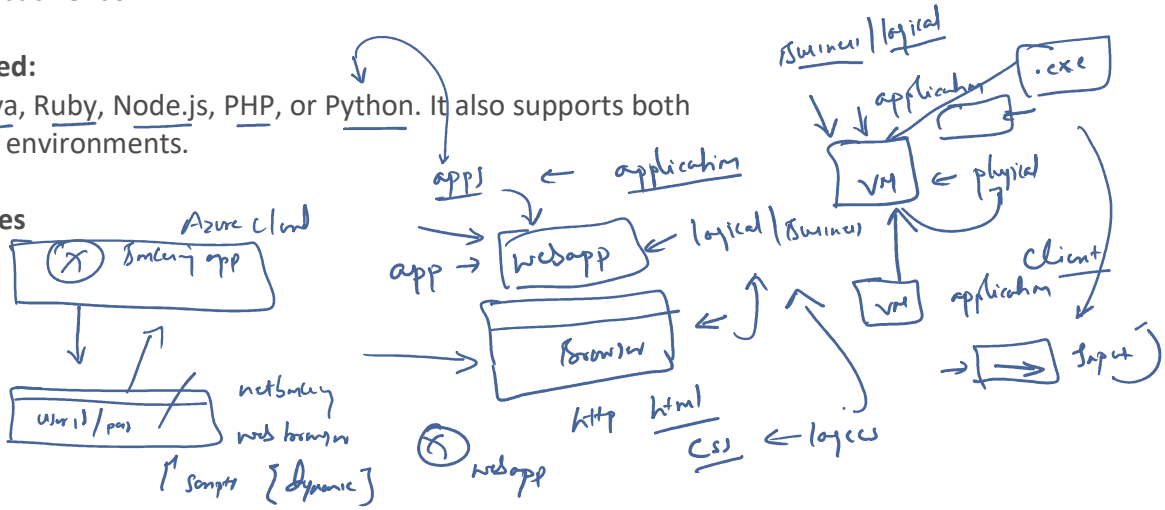
- App Service enables you to build and host web apps
- Automatic Scaling and High Availability.
- App Service supports Windows and Linux.
- Deployments are supported using GitHub, Azure DevOps, or any Git
- Build and Maintain your app, and Azure focuses on keeping the environment up and running.
- Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends.

Languages supported:

.NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.

Types of app services

- Web apps
- API apps
- WebJobs
- Mobile apps



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

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

All of these app styles are hosted in the same infrastructure and share these benefits. This flexibility makes App Service the ideal choice to host web-oriented applications.

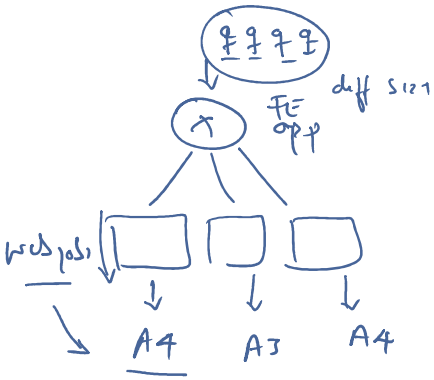
Web apps

App Service includes full support for hosting web apps by using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can choose either Windows or Linux as the host operating system.

API apps

Much like hosting a website, you can build REST-based web APIs by using your choice of language and framework. You get full Swagger support and the ability to

API apps
Much like hosting a website, you can build REST-based web APIs by using your choice of language and framework. You get full Swagger support and the ability to package and publish your API in Azure Marketplace. The produced apps can be consumed from any HTTP- or HTTPS-based client.



WebJobs
They can be scheduled or run by a trigger.

WebJobs are often used to run background tasks as part of your application logic.

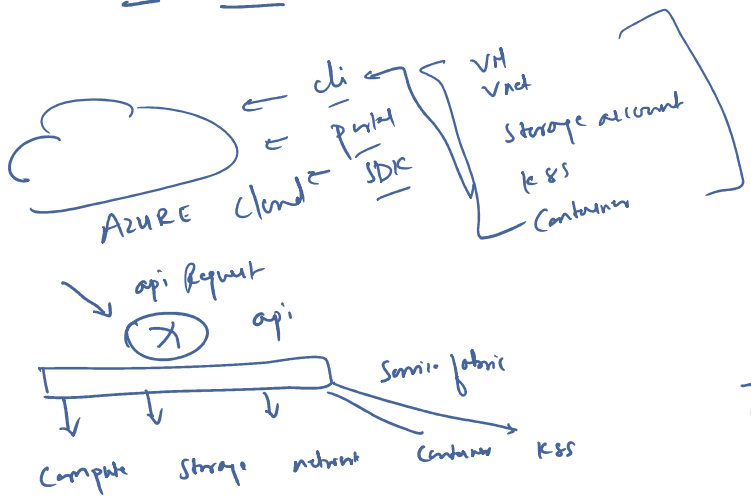
(.exe, Java, PHP, Python, or Node.js) or script (.cmd, .bat, PowerShell, or Bash) in the same context as a web app, API app, or mobile app.

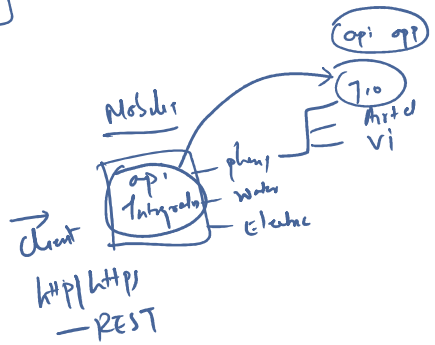
Mobile apps

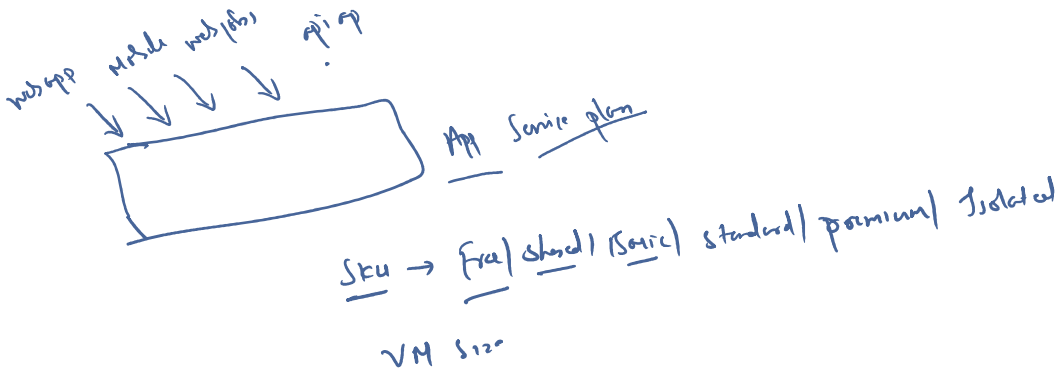
Build a back end for iOS and Android apps.

Store mobile app data in a cloud-based SQL database.

- Authenticate customers against common social providers, such as MSA, Google, Twitter, and Facebook.
- Send push notifications.
- Execute custom back-end logic in C# or Node.js.





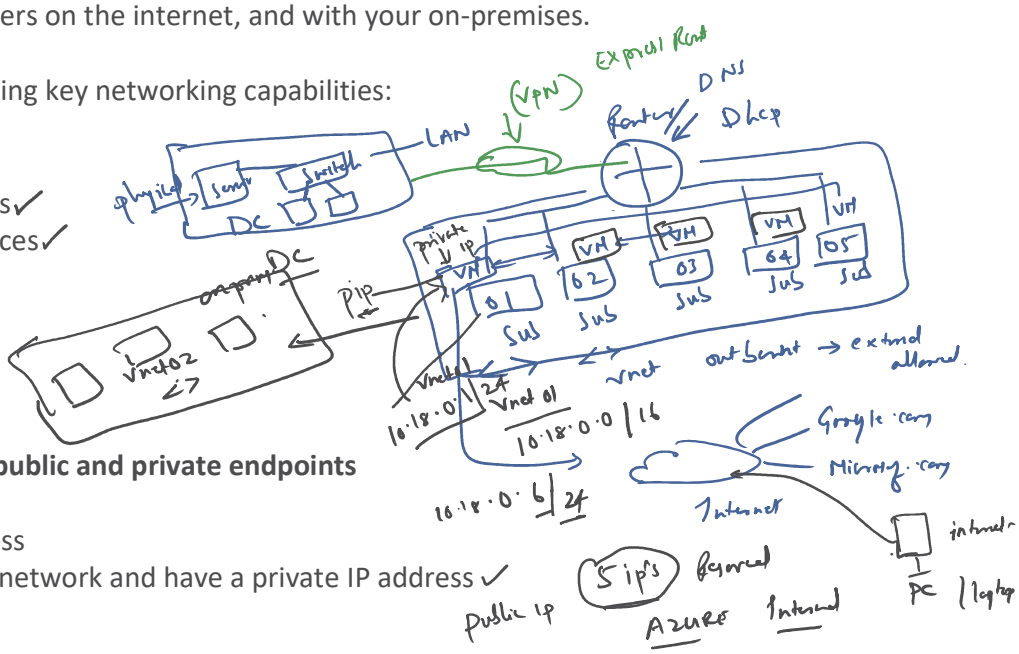


Azure virtual networking ✓ — Vnet → Jaas Resource

Azure virtual networks and virtual subnets enable Azure resources to communicate with each other
Also Vnet allows to Communicate with users on the internet, and with your on-premises.

Azure virtual networks provide the following key networking capabilities:

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

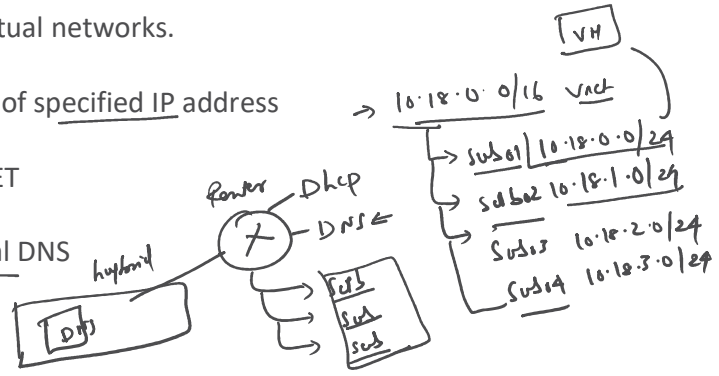


Azure virtual networking supports both public and private endpoints

- Public endpoints have a public IP address
- Private endpoints exist within a virtual network and have a private IP address ✓

Isolation and segmentation ✓

- Azure virtual network allows you to create multiple isolated virtual networks.
- Multiple networks are Subnets which is created with the range of specified IP address
- Each subnet gets and IP range from the defined IP range at VNET
- For name resolution, We can use Azure Internal DNS or External DNS

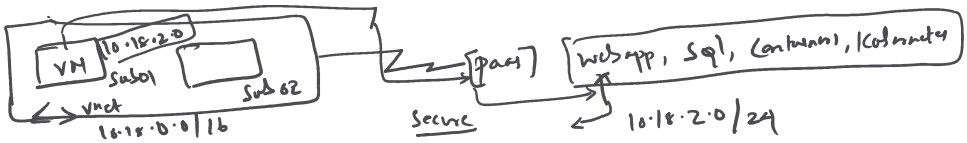


Internet Access ✓

You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer.

Communicate between Azure resources securely ✓

- Virtual networks can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
- Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. Azure resources on virtual networks to connect to other resources to improve security and provide optimal routing between resources.



On-Premises Connect ✓

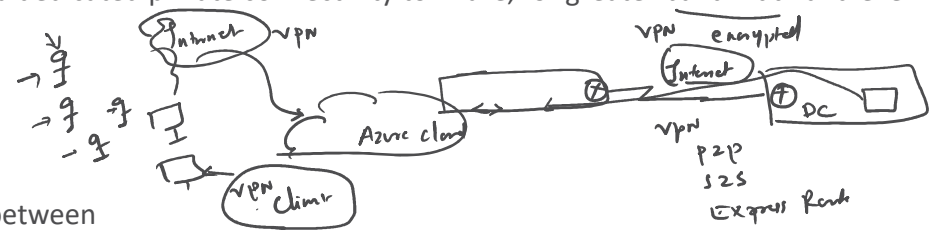
Azure virtual networks enable you to link on-premises environment and Azure subscription resources together
Setup a network that spans both your local and cloud environments.

- Point-to-site virtual private network connections, It will be encrypted VPN connection to connect to the Azure virtual network.

virtual network.

- Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. The connection is encrypted and works over the internet.

- Azure ExpressRoute provides a dedicated private connectivity to Azure, for greater bandwidth and even higher levels of security.



Route network traffic

By default, Azure routes traffic between

- Subnets
- On-premises networks
- Connected virtual networks
- Internet

Other Methods to Route:

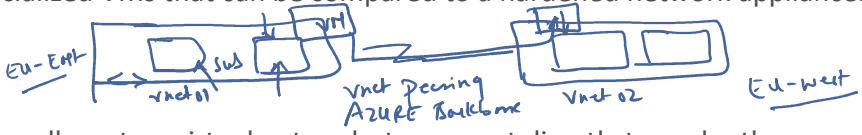
- Route tables allow you to define rules
- Border Gateway Protocol (BGP)

Filter network traffic

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

- Network security groups by using inbound and outbound security rules.
- Network virtual appliances are specialized VMs that can be compared to a hardened network appliance.

Connect virtual networks



- Use virtual network peering. Peering allows two virtual networks to connect directly to each other.

- Communicates Via the Microsoft backbone network, never entering the public internet.

- Peering enables resources in each virtual network to communicate with each other.

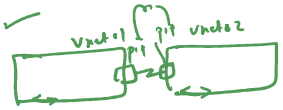
- These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

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

VPN gateways

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network

- Connect on-premises datacenters 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.



- All data transfer is encrypted inside a private tunnel as it crosses the internet.
- You can deploy only one VPN gateway in each virtual network.
- You can use one gateway to connect to multiple locations, which includes other virtual networks or on-premises datacenters.
- When setting up a VPN gateway, you must specify the type of VPN - either policy-based or route-based.

The primary distinction between these two types is how they determine which traffic needs encryption.

In Azure, regardless of the VPN type, the method of authentication employed is a pre-shared key.

- Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel.
- IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet.
- Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

S2S

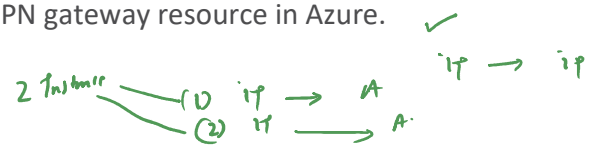
Use a route-based VPN gateway for Below (Recommended)

Connections between virtual networks
- Point-to-site connections
- Multisite connections
- Coexistence with an Azure ExpressRoute gateway

High-availability scenarios
If you're configuring a VPN to keep your information safe, you also want to be sure that it's a highly available and fault tolerant VPN configuration. There are a few ways to maximize the resiliency of your VPN gateway.

Active/standby
By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure.

By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure.

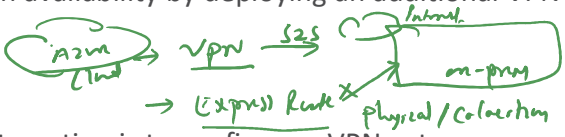


Active/active

With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration.

You assign a unique public IP address to each instance. You then create separate tunnels from the on-premises device to each IP address.

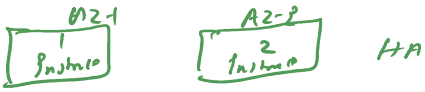
You can extend the high availability by deploying an additional VPN device on-premises.



ExpressRoute failover

Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections.

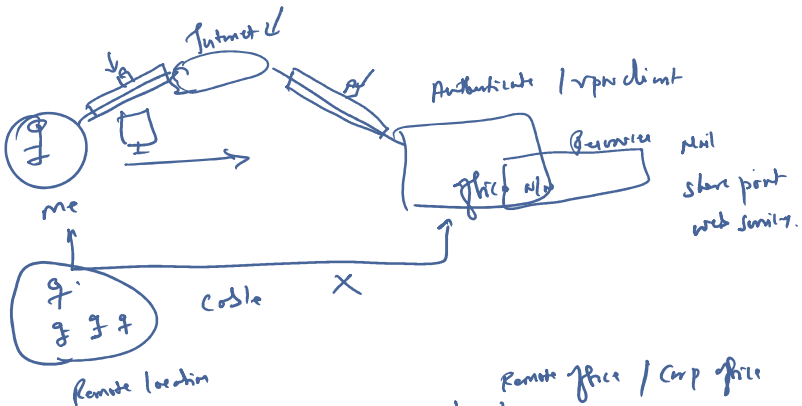
You can also provision a VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.

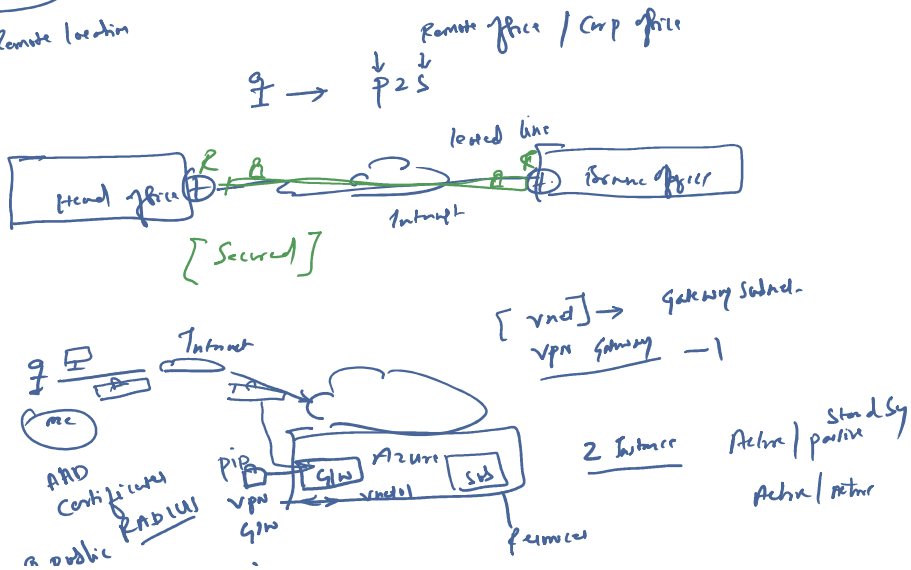


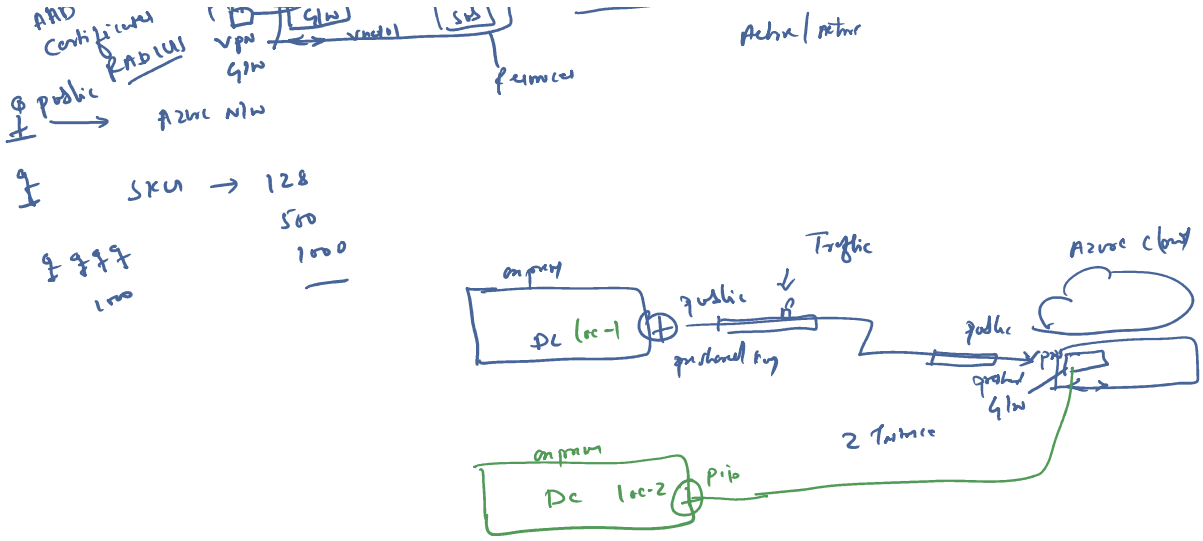
Zone-redundant gateways

In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration.

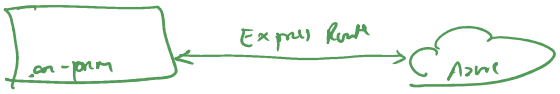
These gateways require different gateway stock keeping units (SKUs) and use Standard public IP addresses instead of Basic public IP addresses.

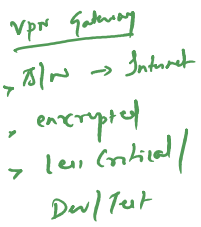





AAD
Certificate
RADIUS
VPN
GW
GW
SKU
Active/Active
Public
Azure NW
SKU → 128
500
1000
1000
Traffic
Azure Cloud
on prem
DC loc-1
public
public
gateway
gateway
GW
2 Tunnels
on prem
DC loc-2
P2P

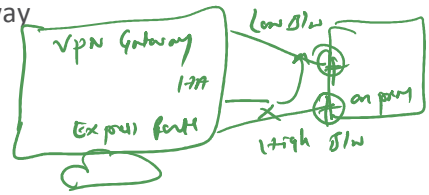
Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection.





Features and benefits of ExpressRoute

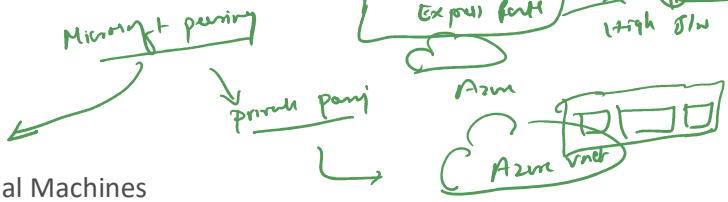
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute Global Reach.
- Dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP).
- Built-in redundancy in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



Connectivity to Microsoft cloud services

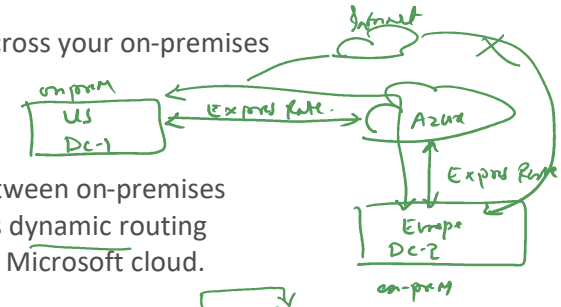
ExpressRoute enables direct access to:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage



Global connectivity

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits.



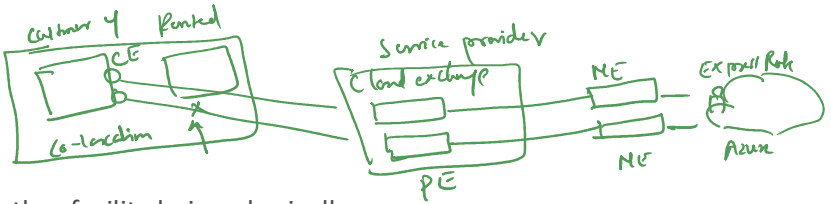
Dynamic routing

ExpressRoute uses the BGP. BGP is used to exchange routes between on-premises networks and resources running in Azure. This protocol enables dynamic routing between your on-premises network and services running in the Microsoft cloud.

Built-in redundancy ✓

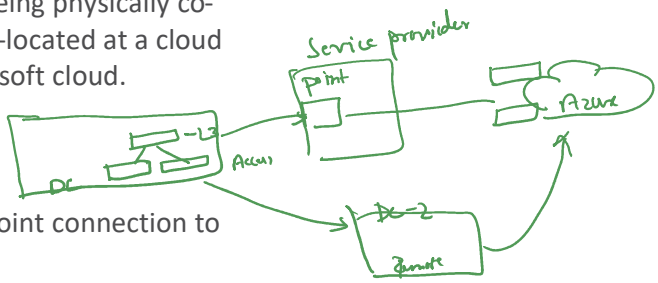
Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. You can configure multiple circuits to complement this feature.

ExpressRoute connectivity models ✓



Co-location at a cloud exchange ✓

Co-location refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP. If your facility is co-located at a cloud exchange, you can request a virtual cross-connect to the Microsoft cloud.



Point-to-point Ethernet connection ✓

Point-to-point ethernet connection refers to using a point-to-point connection to connect your facility to the Microsoft cloud.

Point-to-point ethernet connection refers to using a point-to-point connection to connect your facility to the Microsoft cloud.

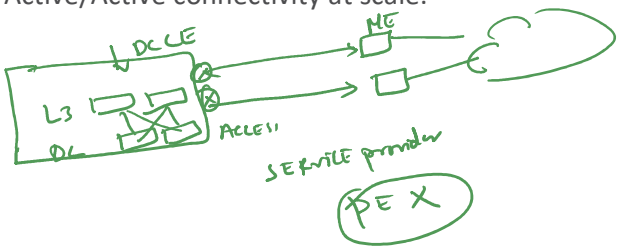
SERVICE provider

Any-to-any networks

With any-to-any connectivity, you can integrate your wide area network (WAN) with Azure by providing connections to your offices and datacenters. Azure integrates with your WAN connection to provide a connection like you would have between your datacenter and any branch offices.

Directly from ExpressRoute sites

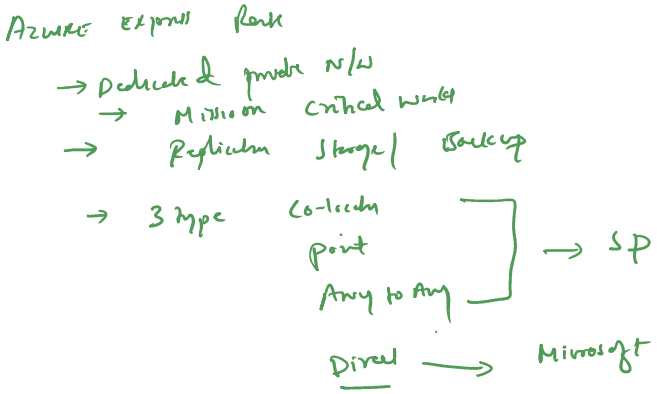
You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale.



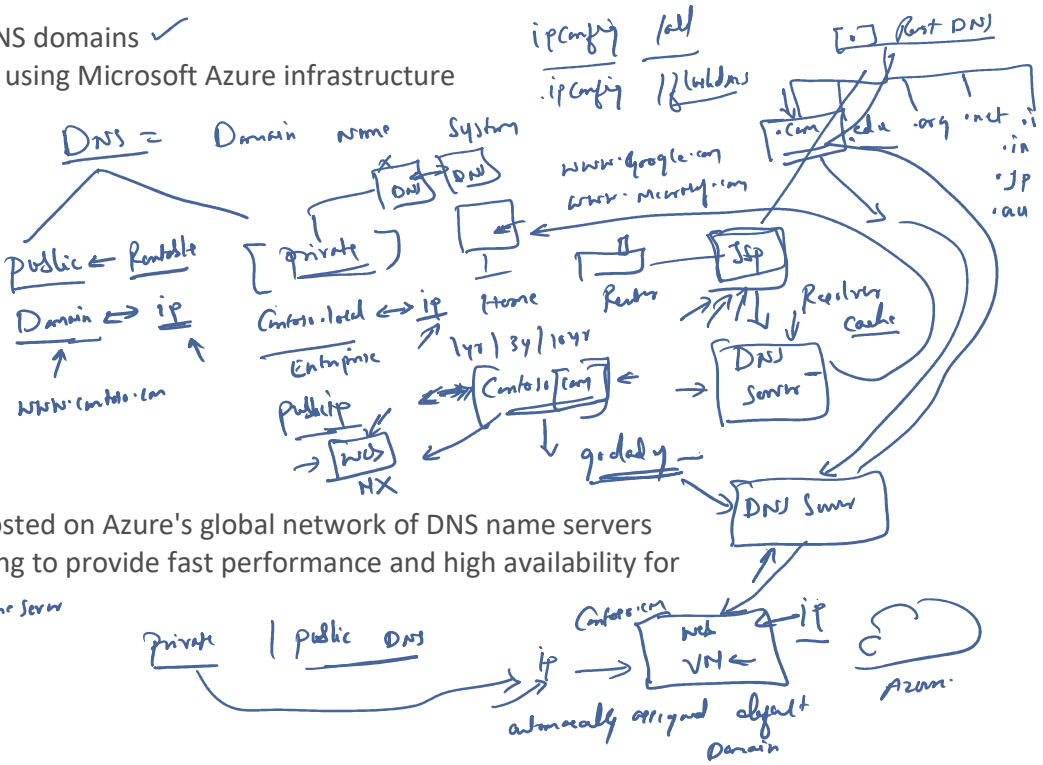
Security considerations

With ExpressRoute, your data doesn't travel over the public internet. ExpressRoute is a private connection from your on-premises infrastructure to your Azure infrastructure.

Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking, and Azure Content Delivery Network requests are still sent over the public internet.



Azure DNS is a hosting service for DNS domains
Used to Provide name resolution by using Microsoft Azure infrastructure



Benefits of Azure DNS

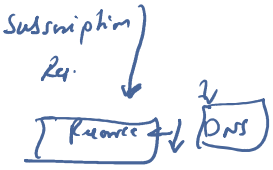
- Reliability and performance
- Security
- Ease of Use
- Customizable virtual networks
- Alias records

Reliability and performance

- DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers
- Azure DNS uses anycast networking to provide fast performance and high availability for your domain.

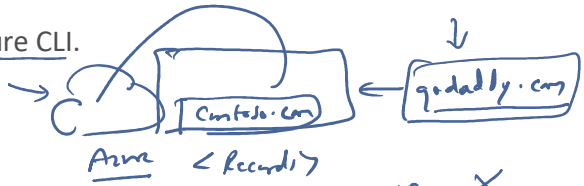
Security

- Azure DNS is based on Azure Resource Manager
- Azure role-based access control (Azure RBAC) to control
- Activity logs to monitor how a user in your organization modified a resource
- Resource locking to lock a subscription, resource group, or resource.



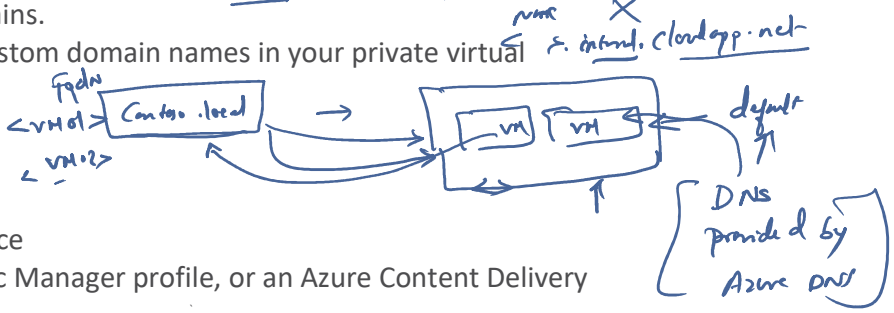
Ease of use

- Azure DNS can manage DNS records for your Azure services for external resources as well.
- Azure DNS is integrated in the Azure portal
- Azure PowerShell cmdlets, and the cross-platform Azure CLI.



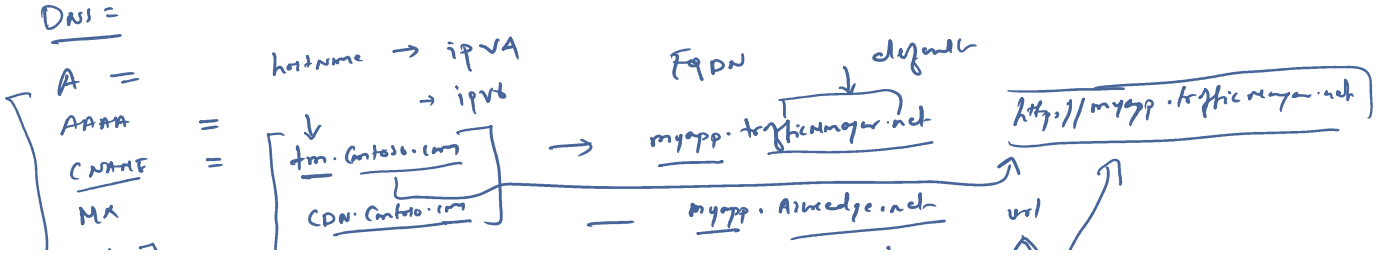
Customizable virtual networks with private domains

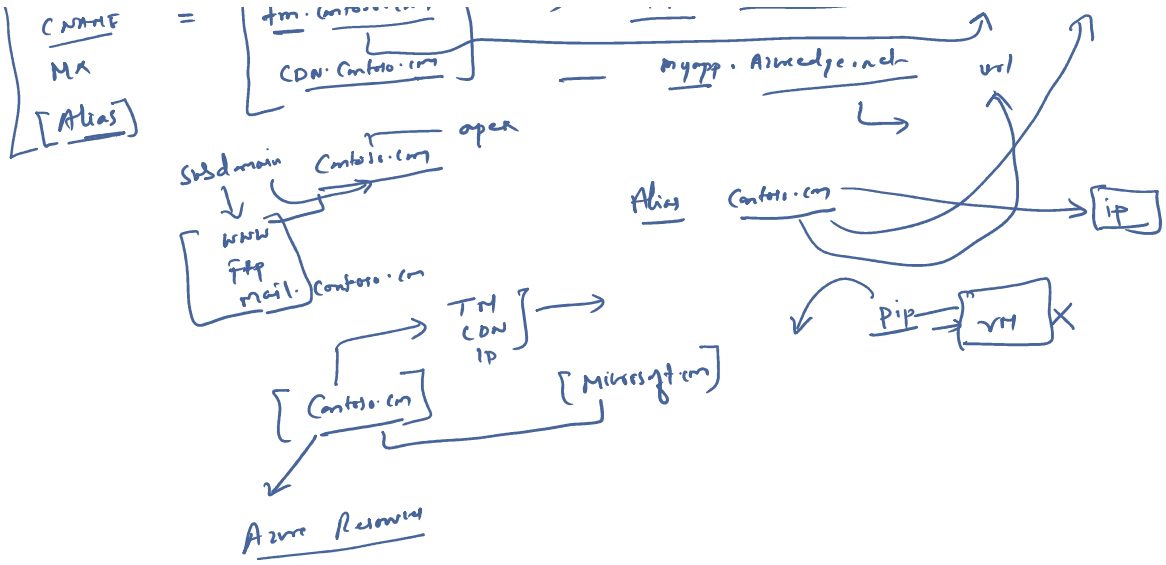
- Azure DNS also supports private DNS domains.
- This feature allows you to use your own custom domain names in your private virtual networks



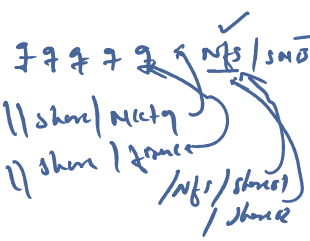
Alias records

- Azure DNS also supports alias record sets.
- Alias record set to refer to an Azure resource
  Ex: Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network (CDN) endpoint.




CNAME
MX
[Alias]
=
CDN.Contoso.com
myapp.Azurecdge.net
url
Subdomain
Contoso.com
open
www
ftp
mail.
Contoso.com
Alias
Contoso.com
ip
TM
CDN
IP
Pip
VM
[Contoso.com]
[Microsoft.com]
Azure Resources

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 .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.



Storage account endpoints

- Every storage account in Azure must have a unique-in-Azure account name.
- The combination of the account name and the Azure Storage service endpoint forms the endpoints for your storage account.
- Naming your storage account:
- Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.
- Your storage account name must be unique within Azure. No two storage accounts can have the same name. This supports the ability to have a unique, accessible namespace in Azure.

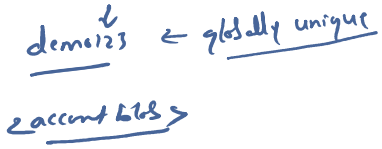
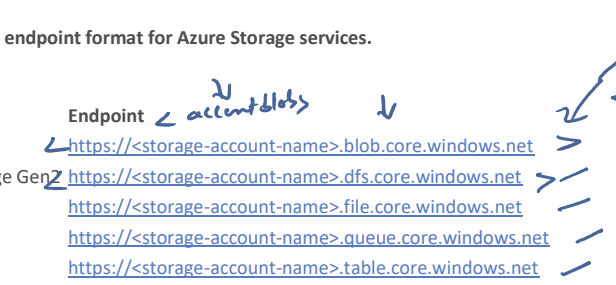
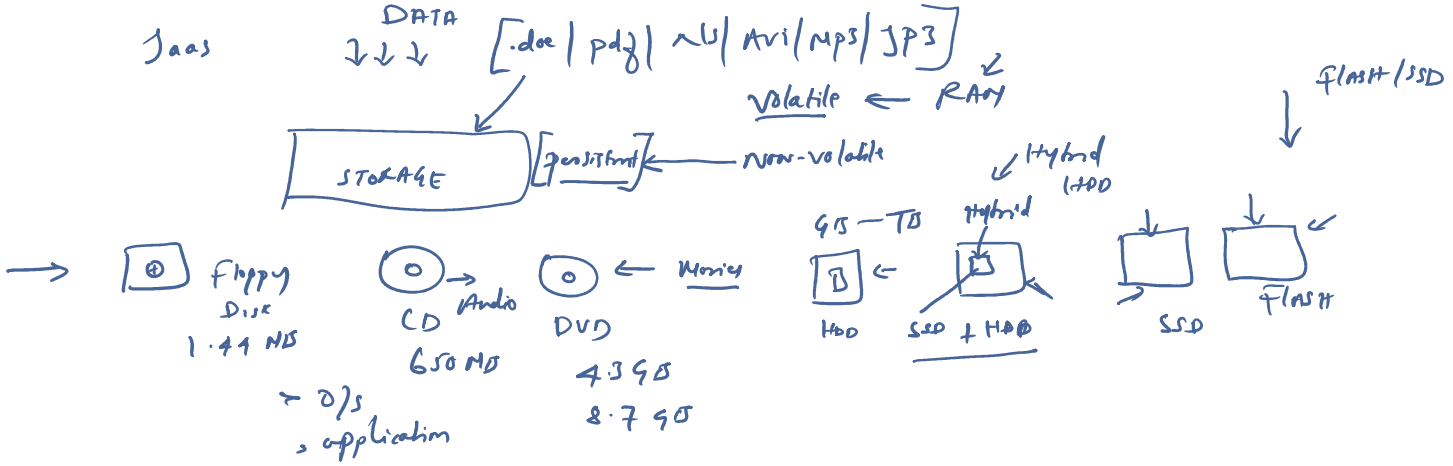


Table shows the endpoint format for Azure Storage services.

Storage service	Endpoint
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net





- Azure Storage always stores multiple copies of your data.
- Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.
- When deciding which redundancy option is best for your scenario, consider the tradeoffs between lower costs and higher availability.

The factors that help determine which redundancy option you should choose include:

- How your data is replicated in the primary region.
- Whether your data is replicated to a second region that is geographically distant to the primary region, to protect against regional disasters.
- Whether your application requires read access to the replicated data in the secondary region if the primary region becomes unavailable.

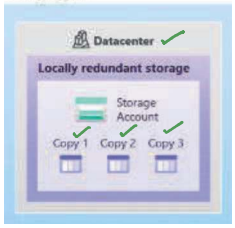
Redundancy in the primary region

- Data in an Azure Storage account is always replicated three times in the primary region.
- In the primary region Data Replication can be of locally redundant storage (LRS) and zone-redundant storage (ZRS).

Locally redundant storage

- Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region.
- LRS provides at least 11 nines of durability (99.999999999%) of objects over a given year.

Primary region

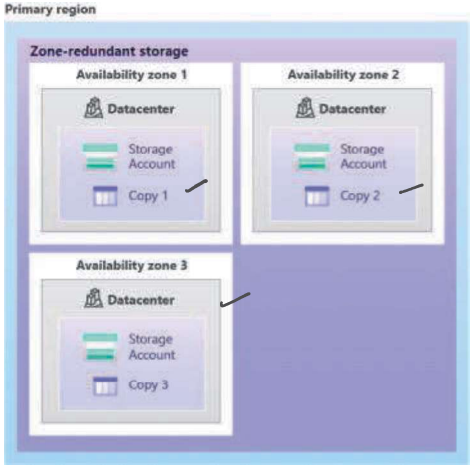


- LRS is the lowest-cost redundancy option and offers the least durability compared to other options.
- LRS protects your data against server rack and drive failures.
- Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

Zone-redundant storage

- For Availability Zone-enabled Regions, zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region.
- ZRS offers durability of 12 nines (99.9999999999%) over a given year.

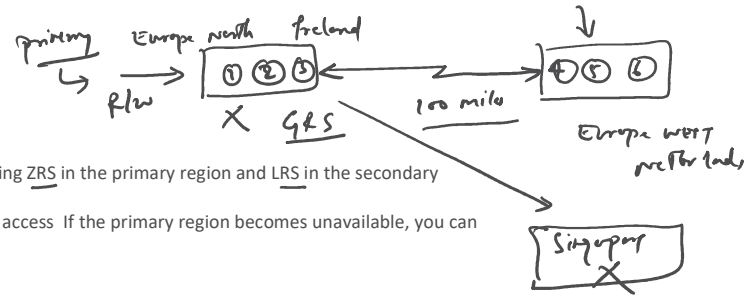
Primary region



- With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable.
- No remounting of Azure file shares from the connected clients is required. If a zone becomes unavailable,
- Microsoft recommends using ZRS in the primary region for scenarios that require high availability.
- ZRS is also recommended for restricting replication of data within a country or region to meet data governance requirements.

Redundancy in a secondary region

- For applications requiring high durability, you can choose to additionally copy to a secondary region that is hundreds of miles away from the primary region.
- Data is durable even in the event of a catastrophic failure that prevents the data in the primary region from being recovered.
- When you create a storage account, you select the primary region for the account. The paired secondary region is based on Azure Region Pairs, and can't be changed.

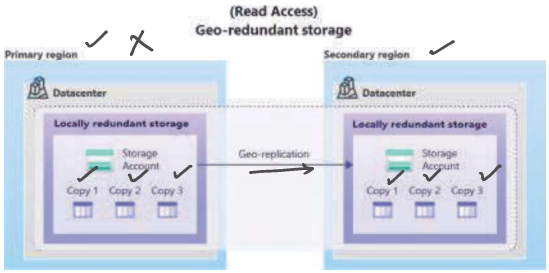


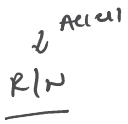
Azure Storage offers two options:

- geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS).
- GRS is similar to running LRS in two regions, and GZRS is similar to running ZRS in the primary region and LRS in the secondary region.
- By default, data in the secondary region isn't available for read or write access If the primary region becomes unavailable, you can choose to fail over to the secondary region.
- Data is replicated to the secondary region asynchronously

Geo-redundant storage

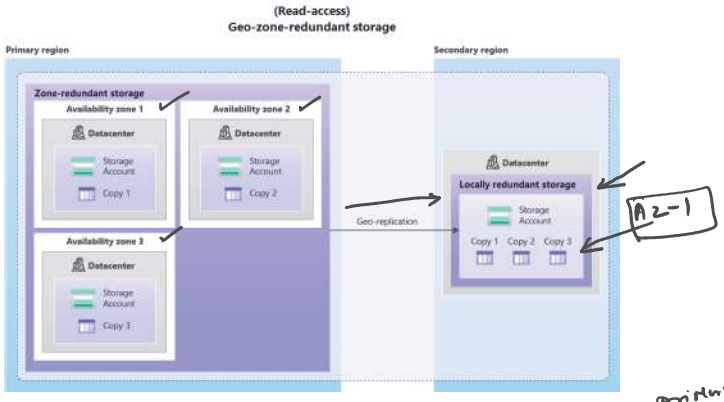
GRS offers durability for Azure Storage data objects of at least 16 nines (99.99999999999999%) over a given year.

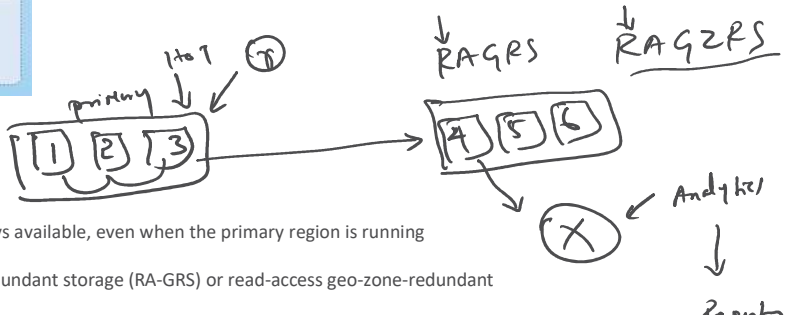




Geo-zone-redundant storage

- Data in a GZRS storage account is copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a secondary geographic region, using LRS, for protection from regional disasters.
- Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.
- GZRS is designed to provide at least 16 nines (99.99999999999999%) of durability of objects over a given year.

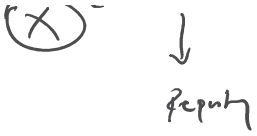




Read access to data in the secondary region

- If you enable read access to the secondary region, your data is always available, even when the primary region is running optimally.
- For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

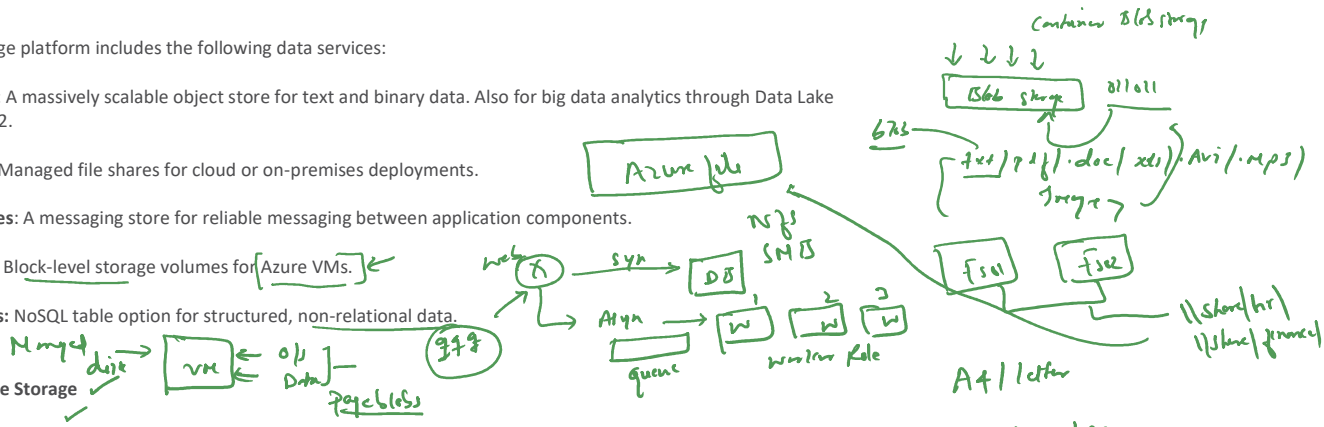
- If you enable read access to the secondary region, your data is always available, even when the primary region is running optimally.
- For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).



Azure storage services

The Azure Storage platform includes the following data services:

- **Azure Blobs**: A massively scalable object store for text and binary data. Also for big data analytics through Data Lake Storage Gen2.
- **Azure Files**: Managed file shares for cloud or on-premises deployments.
- **Azure Queues**: A messaging store for reliable messaging between application components.
- **Azure Disks**: Block-level storage volumes for Azure VMs.
- **Azure Tables:** NoSQL table option for structured, non-relational data.



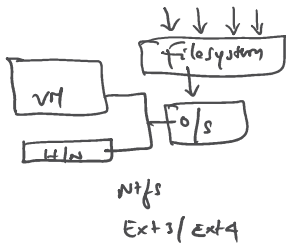
Benefits of Azure Storage

- **Durable and highly available.** Redundancy ensures that your data is safe if transient hardware failures occur/Regional Outage. Data replicated in this way remains highly available if an unexpected outage occurs.
- **Secure**. All data written to an Azure storage account is encrypted, Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable**. Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed**. Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible**. Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS.
  Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer

Azure storage services-Azure Blobs

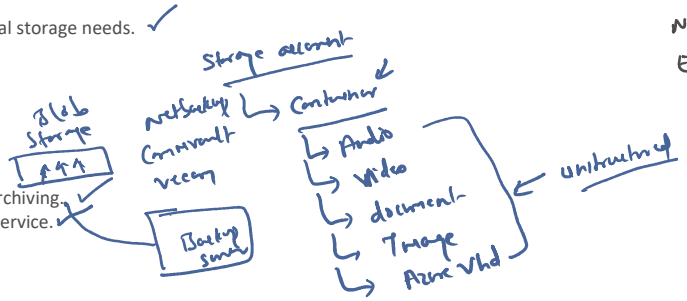
Azure Blobs

- Azure Blob storage is an object storage solution for the cloud. It can store massive amounts of data, such as text or binary data.
- Azure Blob storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold.
- Blob storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.
- Blobs aren't limited to common file formats.
- Data is uploaded as blobs, and Azure takes care of the physical storage needs.



Blob storage is ideal for:

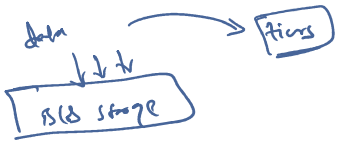
- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.



Accessing blob storage

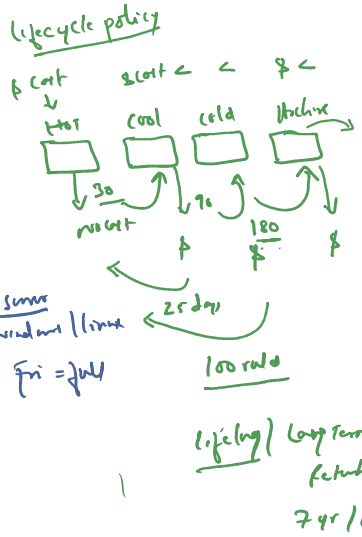
- Objects in blob storage can be accessed from anywhere in the world via HTTP or HTTPS.
- Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library.

The storage client libraries are includes .NET, Java, Node.js, Python, PHP, and Ruby.



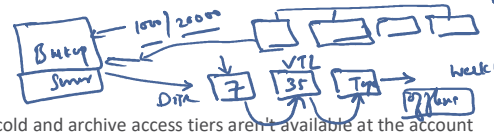
Blob storage tiers

- Organize your data based on attributes like frequency of access and planned retention period.
- Data stored in the cloud can be handled differently based on how it's generated, processed, and accessed over its lifetime. Some data is actively accessed, Some data is accessed frequently early in its lifetime, later it is rarely accessed.
- Some data remains idle in the cloud and is rarely, if ever, accessed after it's stored.
- Azure provides several access tiers to balance your storage costs with your access needs.



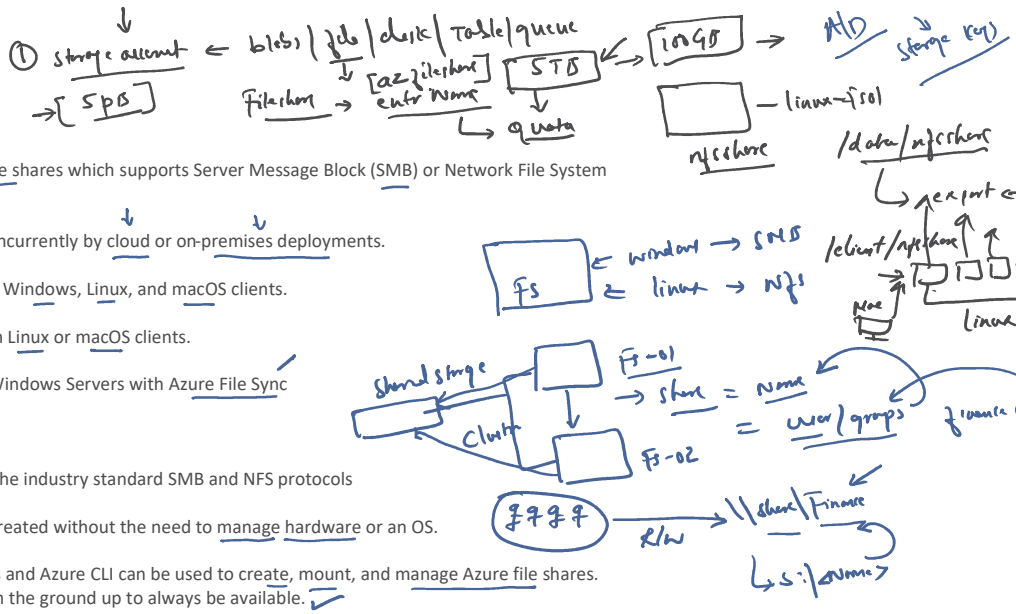
Access tiers:

- **Hot access tier**: Optimized for storing data that is accessed frequently (for example, images for your website).
- **Cool access tier**: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
- **Cold access tier**: Optimized for storing data that is infrequently accessed and stored for at least 90 days.
- **Archive access tier**: Rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).



Considerations of access tiers:

- Hot and cool access tiers can be set at the account level. The cold and archive access tiers aren't available at the account level.
- Hot, cool, cold, and archive tiers can be set at the blob level.
- Data in the cool and cold access tiers can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data.
- Archive storage stores data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.



Azure Files

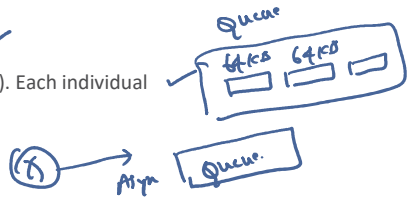
- Azure File storage offers fully managed file shares which supports Server Message Block (SMB) or Network File System (NFS) protocols.
- Azure Files file shares can be mounted concurrently by cloud or on-premises deployments.
- SMB Azure file shares are accessible from Windows, Linux, and macOS clients.
- NFS Azure Files shares are accessible from Linux or macOS clients.
- SMB Azure file shares can be cached on Windows Servers with Azure File Sync

Azure Files key benefits:

- **Shared access**: Azure file shares support the industry standard SMB and NFS protocols
- **Fully managed**: Azure file shares can be created without the need to manage hardware or an OS.
- **Scripting and tooling**: PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares.
  Resiliency: Azure Files has been built from the ground up to always be available.

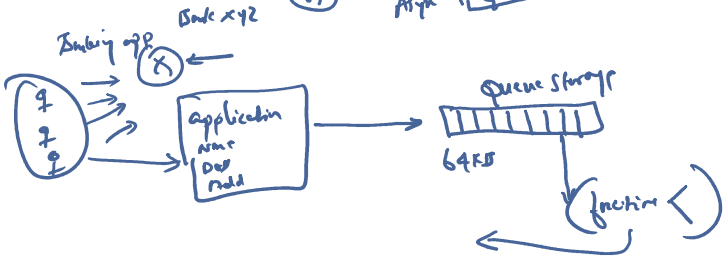
Azure Queues

- Azure Queue storage is a service for storing large numbers of messages.
- Access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS.
- A queue can contain as many messages as your storage account has room for (potentially millions). Each individual message can be up to 64 KB in size.
- Queues are commonly used to create a backlog of work to process asynchronously.



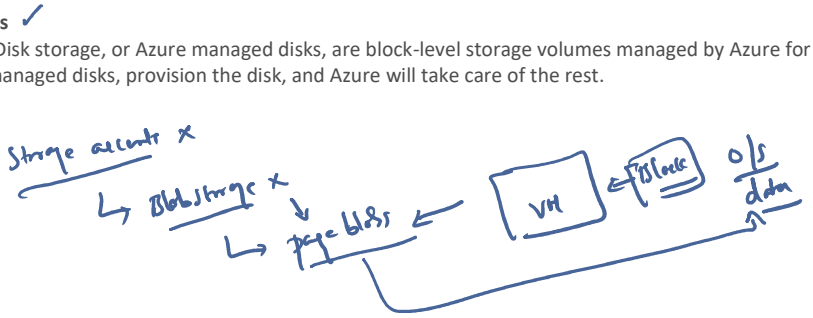
Azure Tables NoSql | Schema

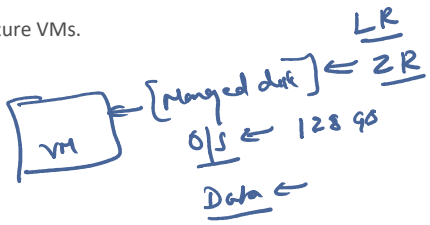
- Azure Table storage stores large amounts of structured data.
- Azure tables are a NoSQL datastore.
- Azure tables are ideal for storing structured, non-relational data.



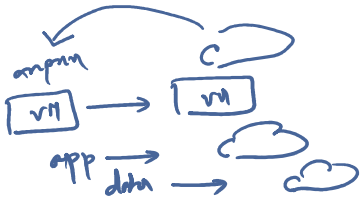
Azure Disks

- Azure Disk storage, or Azure managed disks, are block-level storage volumes managed by Azure for use with Azure VMs.
- With managed disks, provision the disk, and Azure will take care of the rest.





Azure Data Migration



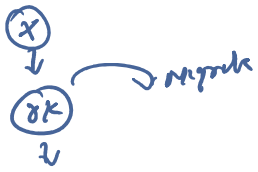
Azure data migration options

Azure supports both real-time migration of infrastructure, applications, and data using Azure Migrate as well as asynchronous migration of data using Azure Data Box.

Azure Migrate

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud.

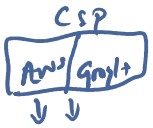
It provides the following:



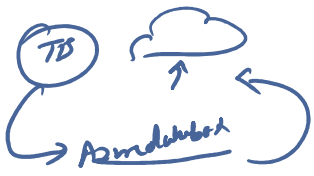
- **Unified migration platform**:
  A single portal to start, run, and track your migration to Azure.
- **Range of tools**:
  A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration.
- **Assessment and migration**: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

Integrated tools

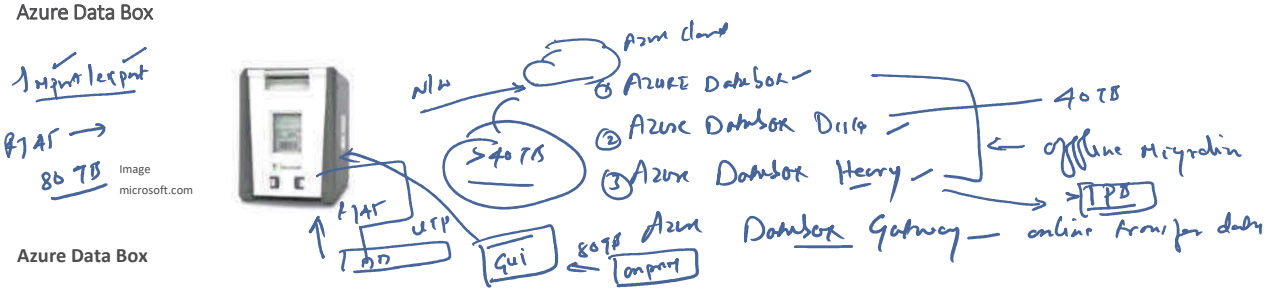
In addition to working with tools from ISVs, the Azure Migrate hub also includes



- **Azure Migrate: Discovery and assessment**.
  Discover and assess on-premises servers running on VMware, Hyper-V, and physical servers.
- **Azure Migrate: Server Migration**.
  Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
- **Data Migration Assistant**.
  Data Migration Assistant is a stand-alone tool to assess SQL Servers.
- **Azure Database Migration Service**.
  Migrate on-premises databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances.
- **Azure App Service migration assistant**.
  Azure App Service migration assistant is a standalone tool to assess on-premises websites for migration to Azure App Service. migrate .NET and PHP web apps to Azure.
- **Azure Data Box**.
  Use Azure Data Box products to move large amounts of offline data to Azure.

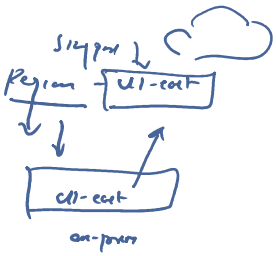


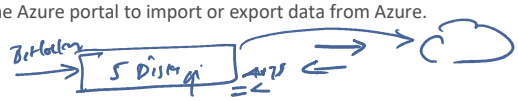
Azure Data Box



Azure Data Box

- Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliabl e way.
- Data Box storage device that has a maximum usable storage capacity of 80 terabytes.
- The Data Box is transported to and from your datacenter via a regional carrier. A rugged case protects and secures the Data B ox from damage during transit.
- You can order the Data Box device via the Azure portal to import or export data from Azure.



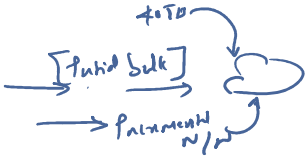


Use cases

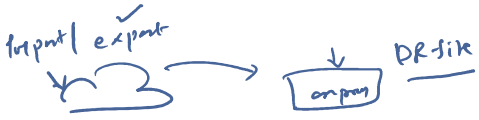
Data Box is ideally suited to transfer data sizes larger than 40 TBs in scenarios with no to limited network connectivity. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

Here are the various scenarios where Data Box can be used to import data to Azure.

- Onetime migration - when a large amount of on-premises data is moved to Azure.
- Moving a media library from offline tapes into Azure to create an online media library.
- Migrating your VM farm, SQL server, and applications to Azure.
- Moving historical data to Azure for in-depth analysis and reporting using HDInsight.

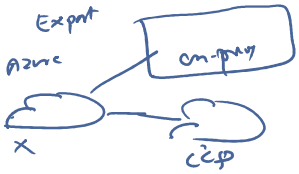


- Initial bulk transfer - when an initial bulk transfer is done using Data Box (seed) followed by incremental transfers over the network.
- Periodic uploads - when large amount of data is generated periodically and needs to be moved to Azure.



Scenarios where Data Box can be used to export data from Azure.

- Disaster recovery - when a copy of the data from Azure is restored to an on-premises network. In a typical disaster recovery scenario, a large amount of Azure data is exported to a Data Box. Microsoft then ships this Data Box, and the data is restored on your premises in a short time.
- Security requirements - when you need to be able to export data out of Azure due to government or security requirements.
- Migrate back to on-premises or to another cloud service provider - when you want to move all the data back to on-premises, or to another cloud service provider, export data via Data Box to migrate the workloads.



Once the data from your import order is uploaded to Azure, the disks on the device are wiped clean in accordance with NIST 800-88r1 standards. For an export order, the disks are erased once the device reaches the Azure datacenter.

Azure file movement options

Azure also has tools to interact with individual files or small file groups.

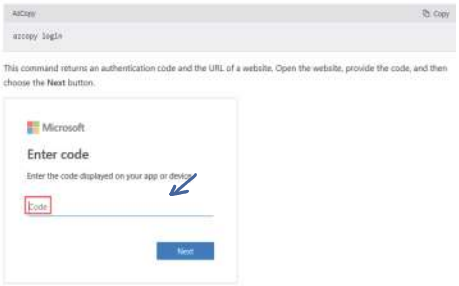
- AzCopy
- Azure Storage Explorer
- Azure File Sync

AzCopy

- AzCopy is a command-line utility
- Use to copy blobs or files to or from your storage account
- Upload files and download files
- Copy files between storage accounts
- Synchronize files

AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds.

Note:
Synchronizing blobs or files with AzCopy is one-direction synchronization. When you synchronize, you designated the source and destination, and AzCopy will copy files or blobs in that direction. It doesn't synchronize bi-directionally based on timestamps or other metadata.



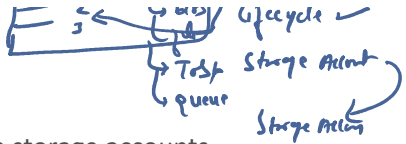
A sign-in window will appear. In that window, sign into your Azure account by using your Azure account credentials.

Syntax:
azcopy copy '<local-file-path>' 'https://<storage-account-name>.file.core.windows.net/<file-share-name>/<file-name>'

Azure Storage Explorer

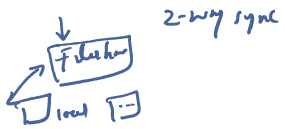
- Azure Storage Explorer is a standalone tool
- Graphical interface to manage files and blobs in your Azure Storage Account.
- Install on Windows, macOS, and Linux operating systems

- Azure Storage Explorer is a standalone tool
- Graphical interface to manage files and blobs in your Azure Storage Account.
- Install on Windows, macOS, and Linux operating systems
- It use AzCopy on the backend to perform all of the file and blob management tasks
- With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts



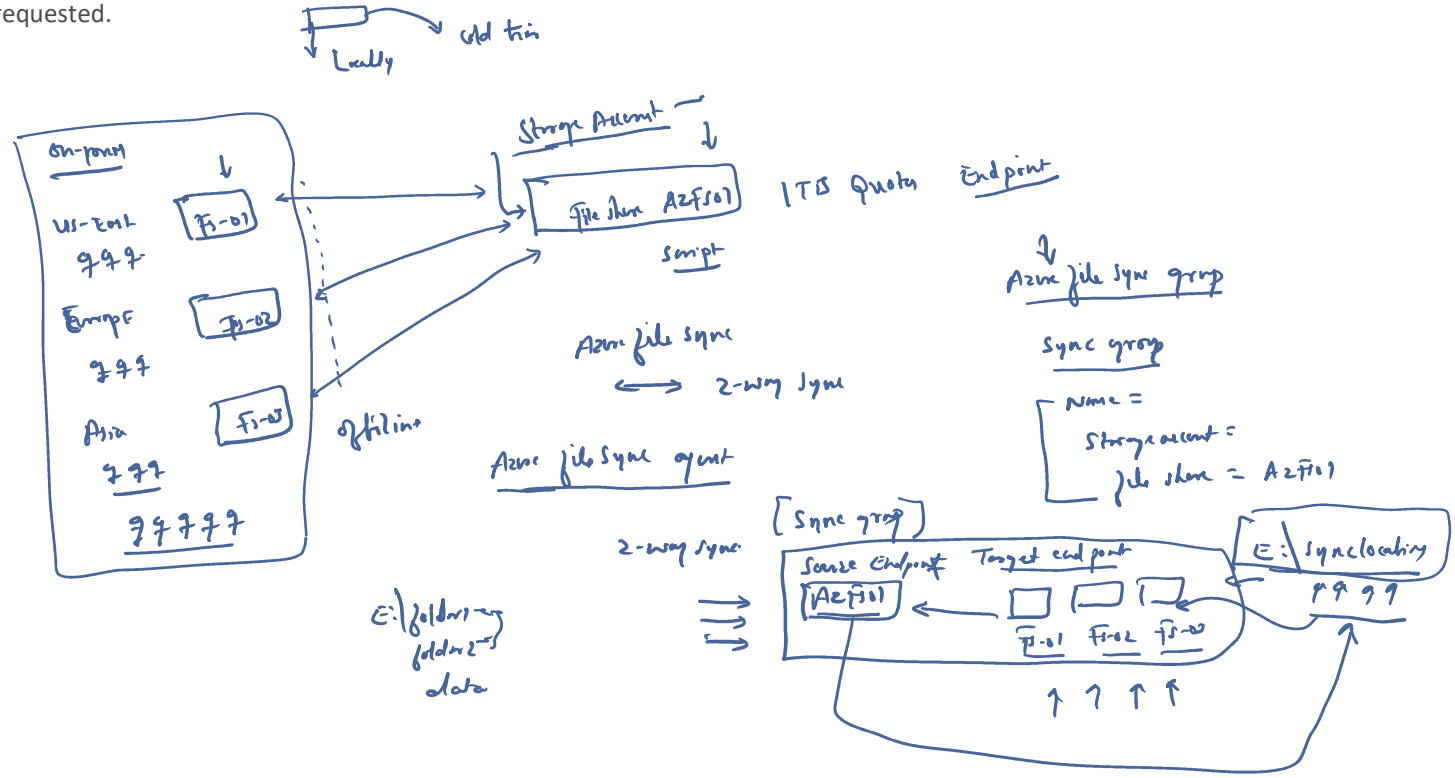
Azure File Sync

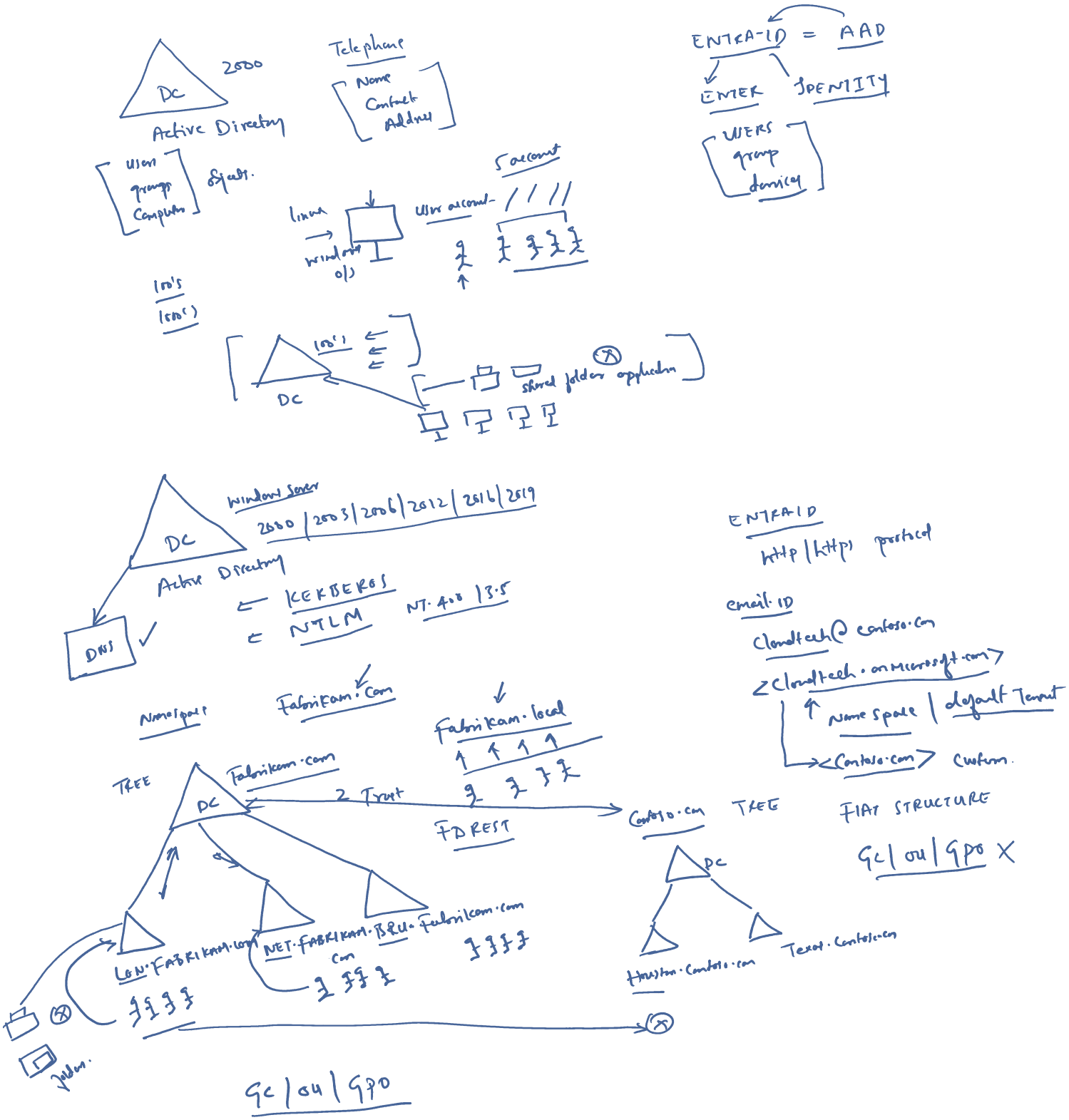
Azure File Sync is a tool that lets you centralize your file shares in Azure Files
Have flexibility, performance, and compatibility of a Windows file server.
Turning your Windows file server into a miniature content delivery network. CDN
Install Azure File Sync on your local Windows server to automatically stay bi-directionally synced with your files in Azure.



With Azure File Sync, you can:

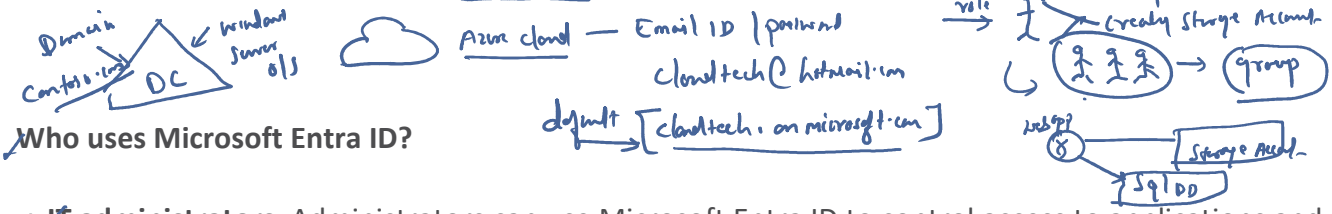
- Use any protocol on Windows Server to access your data locally, including SMB, NFS, and FTPS.
- Have as many caches as you need across the world.
- Replace a failed local server by installing Azure File Sync on a new server in the same datacenter.
- Configure cloud tiering
  >frequently accessed files are replicated locally, while infrequently accessed files are kept in the cloud until requested.




DC
2000
Active Directory
User
group
Computer
objects
Telephone
Name
Contact
Address
ENTRA-ID = AAD
ENTER
IDENTITY
USERS
group
device
linux
window
o/s
User account
S account
100's
1000's
DC
shared folder
application
Window Server
2000 | 2003 | 2006 | 2012 | 2016 | 2019
DC
Active Directory
DNS
KERBEROS
NTLM
NT 4.0 | 3.5
ENTRA ID
http | https protocol
email ID
Cloudtech@contoso.com
Cloudtech.onMicrosoft.com
Name space | default Tenant
Contoso.com
Custom
Namespace
Fabrikam.com
Fabrikam.local
TREE
DC
Fabrikam.com
2 Trust
FOREST
Contoso.com TREE
DC
LON.FABRIKAM.COM
NET.FABRIKAM.BRU.
Fabrikam.com
Houston.Contoso.com
Texas.Contoso.com
FLAT STRUCTURE
GC | OU | GPO X
Judo.
GC | OU | GPO

Azure Directory Services

- Microsoft Entra ID is a directory service
- Sign in and access both Microsoft cloud applications and cloud applications that you develop
- For on-premises environments, Active Directory running on Windows Server
- Microsoft Entra ID is Microsoft's cloud-based identity and access management service
- When you connect Active Directory with Microsoft Entra ID, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost

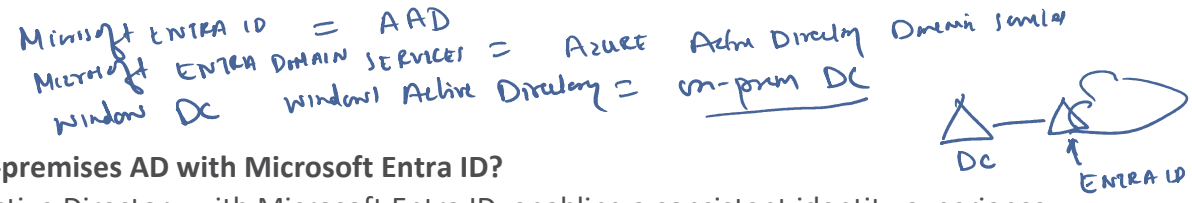


Who uses Microsoft Entra ID?

- **IT administrators**. Administrators can use Microsoft Entra ID to control access to applications and resources based on their business requirements
- **App developers**. Developers can use Microsoft Entra ID to provide a standards-based approach for adding functionality to applications
- **Users**. Users can manage their identities and take maintenance actions like self-service password reset
- **Online service subscribers**. Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online

What does Microsoft Entra ID do?

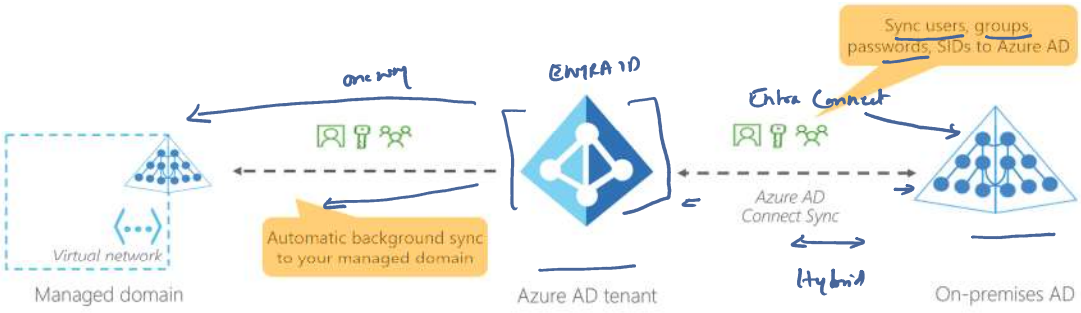
- **Authentication**: This includes verifying identity to access applications and resources
- **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications
- **Application management**: You can manage your cloud and on-premises apps by using Microsoft Entra ID
- **Device management**: Along with accounts for individual people, Microsoft Entra ID supports the registration of devices



Can I connect my on-premises AD with Microsoft Entra ID?

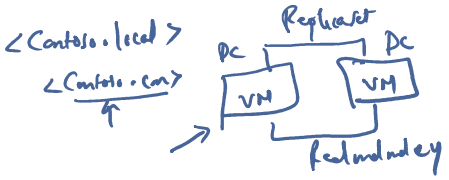
- you can connect Active Directory with Microsoft Entra ID, enabling a consistent identity experience between cloud and on-premises
  - One method of connecting Microsoft Entra ID with your on-premises AD is using Microsoft Entra Connect
- Microsoft Entra Connect synchronizes user identities between on-premises Active Directory and Microsoft Entra ID
  - you can use features like SSO, multifactor authentication, and self-service password reset under both systems

systems



What is Microsoft Entra Domain Services?

- Microsoft Entra Domain Services is a service that provides managed domain services
  - such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication.
- Get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.
- A Microsoft Entra Domain Services managed domain lets you run legacy applications in the cloud
- Microsoft Entra Domain Services integrates with your existing Microsoft Entra tenant.
  - This integration lets users sign into services and applications connected to the managed domain using their existing credentials.



How does Microsoft Entra Domain Services work?

- When you create a Microsoft Entra Domain Services managed domain
  - Define a unique namespace. This namespace is the domain name.
  - Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.
- You don't need to manage, configure, or update these DCs.
- Backups and encryption at rest using Azure Disk Encryption are Taken care by Azure

Is information synchronized?

- A managed domain is configured to perform a one-way synchronization from Microsoft Entra ID to Microsoft Entra Domain Services.

Hybrid environment with an on-premises AD DS environment

- Microsoft Entra Connect synchronizes identity information --> Microsoft Entra ID, which is then synchronized to the managed domain.

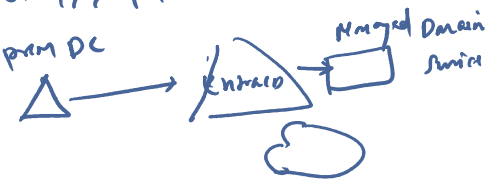
group

Computer
application

Microsoft Entra Domain Servic

↳ on-prem DC

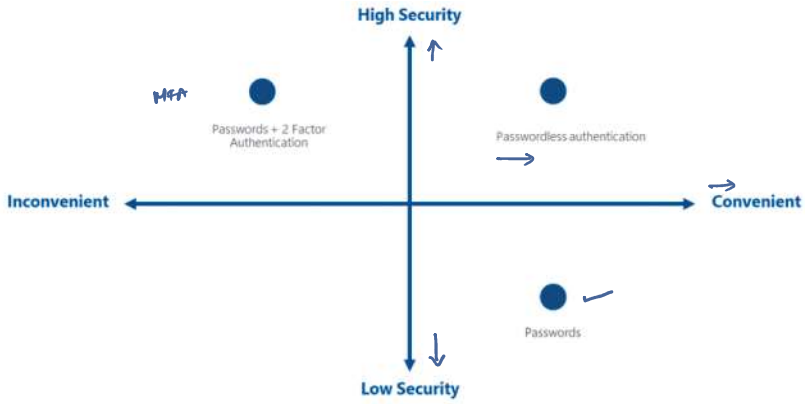
Microsoft Entra Connect → Sync → User / group / password



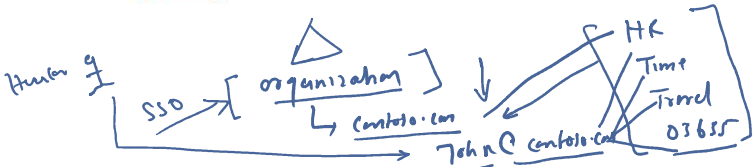
Describe Azure authentication methods

- Authentication is the process of establishing the identity of a person, service, or device
- It requires the person, service, or device to provide some type of credential to prove who they are
- Azure supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless
- New authentication solutions provide both security and convenience

The following diagram shows the security level compared to the convenience.

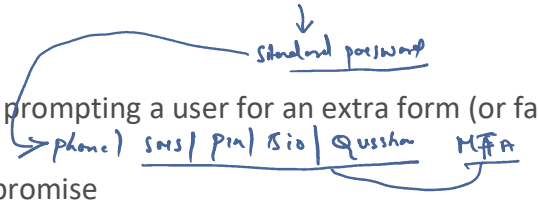


Single Sign-on:



- Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers
- For SSO to work, the different applications and providers must trust the initial authenticator
- More identities mean more passwords to remember and change. As complexity requirements increase, it becomes increasingly difficult for users to remember them
- The more passwords a user has to manage, the greater the risk of a credential-related security incident
- With SSO, you need to remember only one ID and one password
- Single sign-on is only as secure as the initial authenticator because the subsequent connections are all based on the security of the initial authenticator

Multifactor Authentication:



- Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process
- MFA helps protect against a password compromise
- Multifactor authentication provides additional security to fully authenticate two or more element is required

These elements fall into three categories:

- Something the user knows – this might be a challenge question

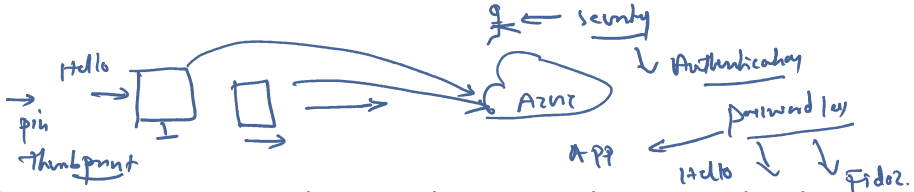
These elements fall into three categories:

- Something the user knows – this might be a challenge question
- Something the user has – this might be a code that's sent to the user's mobile phone
- Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan

Microsoft Entra MFA

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

Passwordless Authentication

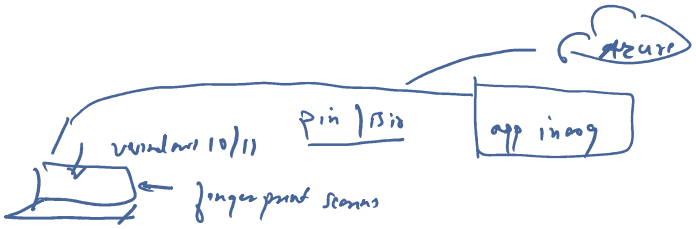


- Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are, or something you know
- Passwordless authentication needs to be set up on a device before it can work

Azure and Azure Government offer the following three passwordless authentication options that integrate with Microsoft Entra ID:

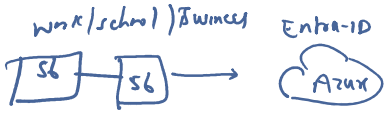
- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys

Windows Hello for Business



- The biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner.
- Seamless access to corporate resources on-premises and in the cloud.

Microsoft Authenticator App



- The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.
- Number displayed on the screen to the one on their phone

FIDO2 security keys

- The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication.
- FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.
- These FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC.

Authentication Methods

SSO

MFA ← Methods

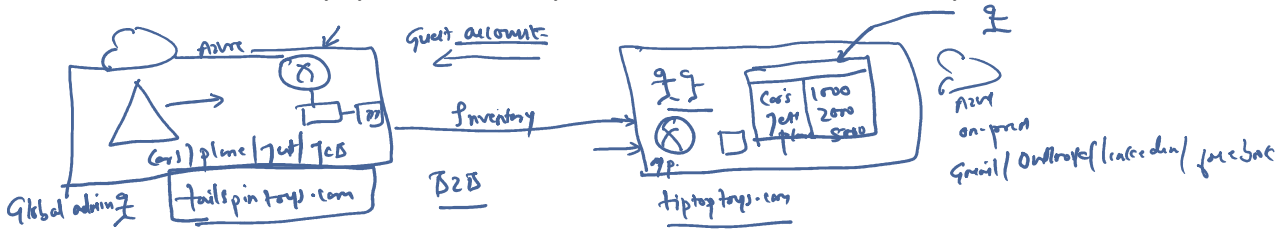
Passwordless Authentication

Describe Azure external identities

An external identity is a person, device, service, etc. that is outside your organization

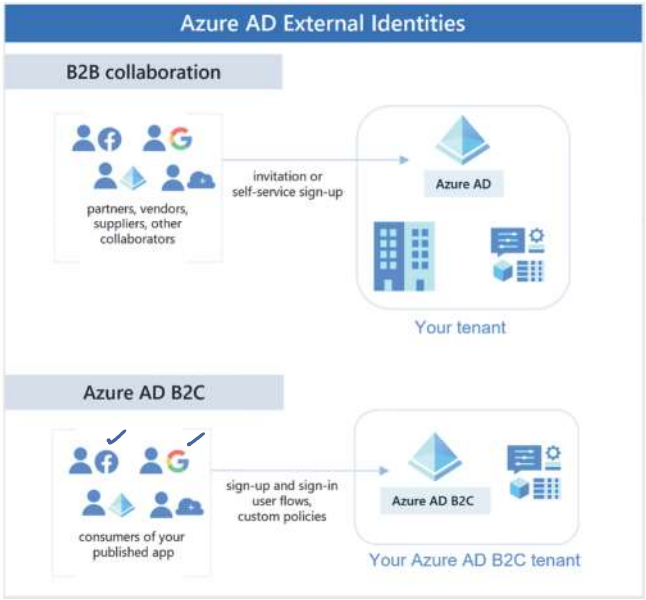
Microsoft Entra External ID refers to ways you can securely interact with users outside of your organization.

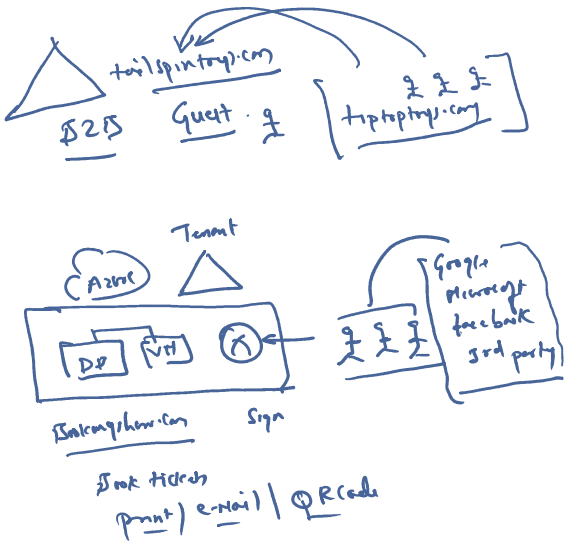
-Partners
-Distributors
-Suppliers
-Vendors



You can share your resources and define how your internal users can access external organizations.

The external user's identity provider manages their identity, and you manage access to your apps with Microsoft Entra ID or Azure AD B2C to keep your resources protected.





The following capabilities make up External Identities:

- **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 (SaaS apps, custom-developed apps, etc.)

  B2B collaboration users are represented in your directory, typically as guest users

- **B2B direct connect**
  Establish a mutual, two-way trust with another Microsoft Entra organization for seamless collaboration.

  B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams.

  B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.

B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.

- **Microsoft Azure Active Directory business to customer (B2C)** -
  Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

B2B B2C B2B Direct Connect

- Depending on how you want to interact with external organizations and the types of resources you need to share, you can use a combination of these capabilities.
- With Microsoft Entra ID, you can easily enable collaboration across organizational boundaries by using the Microsoft Entra B2B feature.
- Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.

Conditional Access

Describe Azure conditional access

Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals.

Conditional Access helps IT administrators:

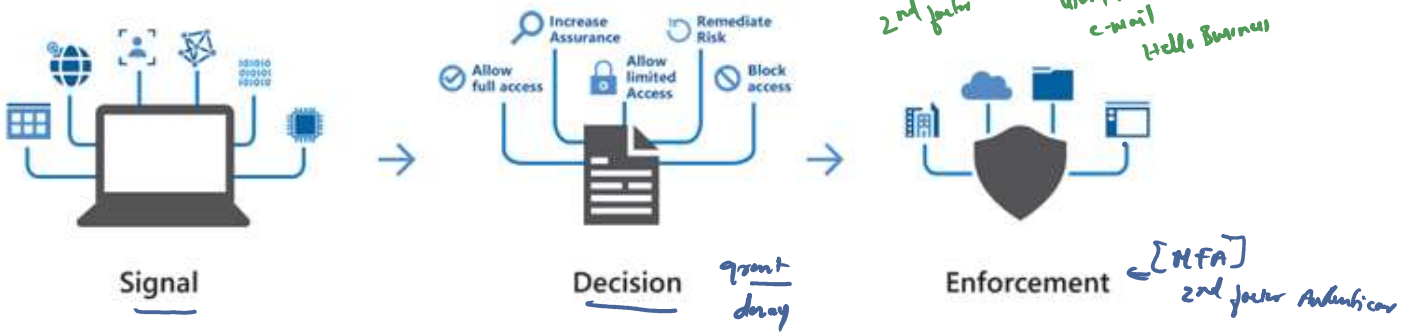
- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

Conditional Access also provides a more granular multifactor authentication experience for users.

For example, a user might not be challenged for second authentication factor if they're at a known location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

The following diagram illustrates this flow:



Here, the signal might be the

- User's location
- User's device
- Application

Based on these signals, the decision might be to allow full access

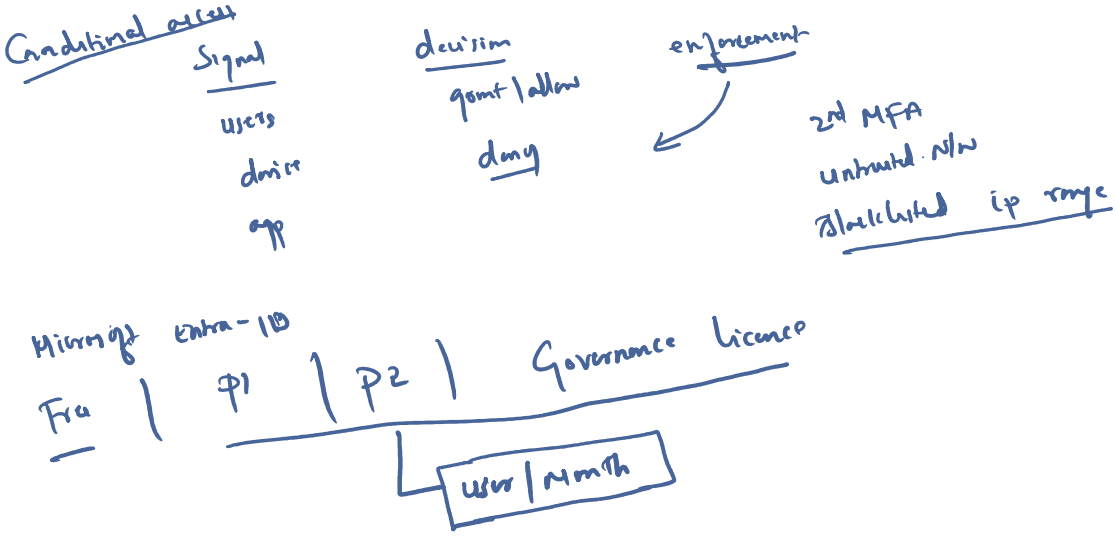
If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision.

When can I use Conditional Access? ✓

Conditional Access is useful when you need to:

- Require multifactor authentication (MFA) to access an application depending on the requester's role, location, or network. For example, you could require MFA for administrators but not regular users or for people connecting from outside your corporate network. ✓
- Require access to services only through approved client applications. ✓
- Require users to access your application only from managed devices. A managed device is a device that meets your standards for security and compliance. ✓
- Block access from untrusted sources, such as access from unknown or unexpected locations. ✓



Azure role-based access control (RBAC)

- How can you control, When you have multiple IT and engineering teams
- The principle of least privilege says you should only grant access up to the level needed to complete a task

Good security practice to follow is:
If you only need read access to a storage blob, then you should only be granted read access to that storage blob. Write access to that blob shouldn't be granted, nor should read access to other storage blobs.

However, managing that level of permissions for an entire team would become tedious

- Azure enables you to control access through Azure role-based access control (Azure RBAC)
- Azure provides built-in roles that describe common access rules for cloud resources
- You can also define your own roles
- Each role has an associated set of access permissions that relate to that role
- When you assign individuals or groups to one or more roles, they receive all the associated access permissions

How is role-based access control applied to resources?
Role-based access control is applied to a scope

The following diagram shows the relationship between roles and scopes.

Scopes include:
- A management group (a collection of multiple subscriptions).
- A single subscription.
- A resource group.
- A single resource.

Observers, users managing resources, admins, and automated processes illustrate the kinds of users or accounts that would typically be assigned each of the various roles.

Azure RBAC is hierarchical, in that when you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription.

How is Azure RBAC enforced?

- Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager
- Resource Manager is a management service that provides a way to organize and secure your cloud resources.
- You typically access Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI
- Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application

Azure RBAC uses an allow model

Ex: If one role assignment grants you read permissions to a resource group and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

Describe zero trust model

Zero Trust is a security model to protects resources with worst case scenario expectation.
Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.

Microsoft highly recommends the Zero Trust security model

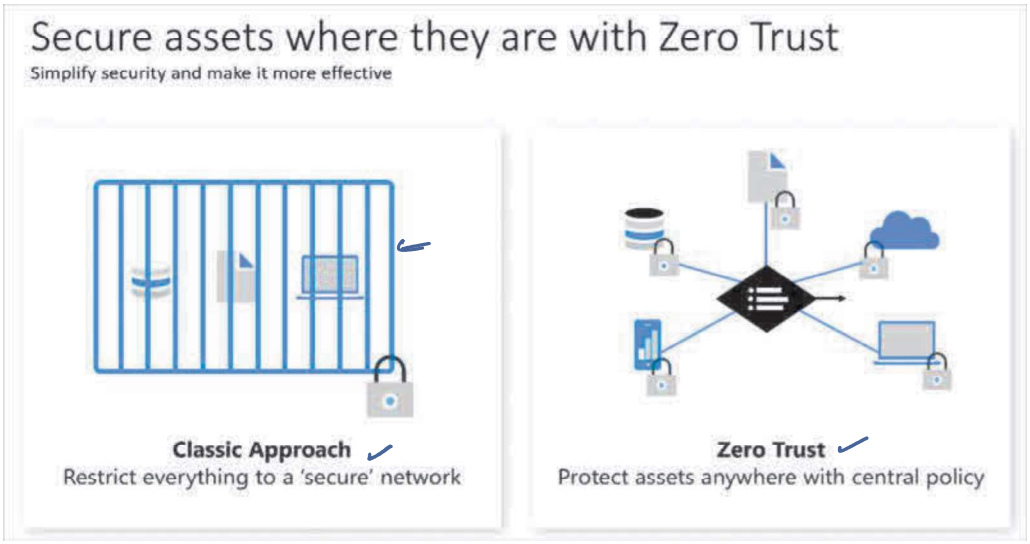
Guiding principles of Zero Trust security model:

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

Adjusting to Zero Trust

Traditionally, corporate networks were restricted, protected, and generally assumed safe.
Only managed computers could join the network, VPN access was tightly controlled, and personal devices were frequently restricted or blocked.

The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it's within the corporate network, it requires everyone to authenticate. Then grants access based on authentication rather than location.

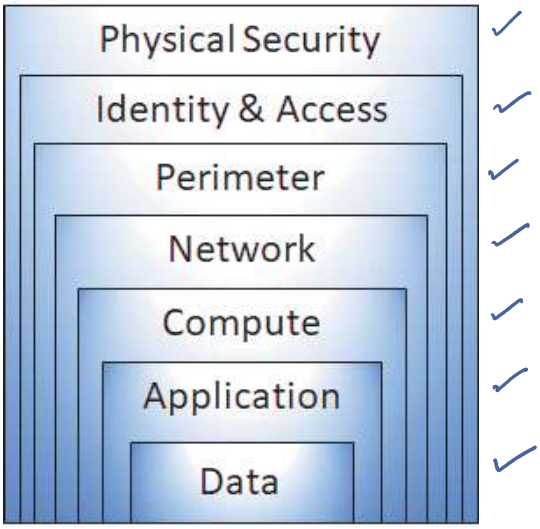


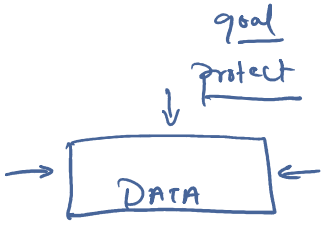
Describe defense-in-depth

The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it.

Layers of defense-in-depth

You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer.





Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.

This approach removes reliance on any single layer of protection.

Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security

- Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense
- With physical security, the intent is to provide physical safeguards against access to assets
- These safeguards ensure that other layers can't be bypassed
- Microsoft uses various physical security mechanisms in its cloud datacenters

Identity and access

- Ensure that identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged.
- Control access to infrastructure and change control.

and changes are logged.

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

Perimeter

- The network perimeter protects from network-based attacks against your resources
- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users
- Use perimeter firewalls to identify and alert on malicious attacks against your network

Network

- At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required.
- Reduce the risk of an attack spreading to other systems in your network

- Limit communication between resources
- Deny by default
- Restrict inbound internet access and limit outbound access where appropriate
- Implement secure connectivity to on-premises networks

Compute

- Malware, unpatched systems, and improperly secured systems open your environment to attacks

- Secure access to virtual machines
- Implement endpoint protection on devices and keep systems patched and current

Application

- Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code

- Ensure that applications are secure and free of vulnerabilities
- Store sensitive application secrets in a secure storage medium
- Make security a design requirement for all application development

Data

- Those who store and control access to data are responsible for ensuring that it's properly secured

- Regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data

➢ Stored in a database ✓
➢ Stored on disk inside virtual machines ✓
➢ Stored in software as a service (SaaS) applications, such as Office 365. ✓
➢ Managed through cloud storage ✓

Describe Microsoft Defender for Cloud

Defender for Cloud is a monitoring tool for security posture management and threat protection It monitors your cloud, on-premises, hybrid, and multi-cloud environments Deployment of Defender for Cloud is easy, it's already natively integrated to Azure

Azure-native Protections

- Azure PaaS services – Detect threats targeting Azure services including Azure App Service, Azure SQL, Azure Storage Account, and more data services
- Azure data services – Defender for Cloud includes capabilities that help you automatically classify your data in Azure SQL. You can also get assessments for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them
- Networks – Defender for Cloud helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access

Defend your hybrid resources

In addition to defending your Azure environment, you can add Defender for Cloud capabilities to your hybrid cloud environment to protect your non-Azure servers.

Defend resources running on other clouds

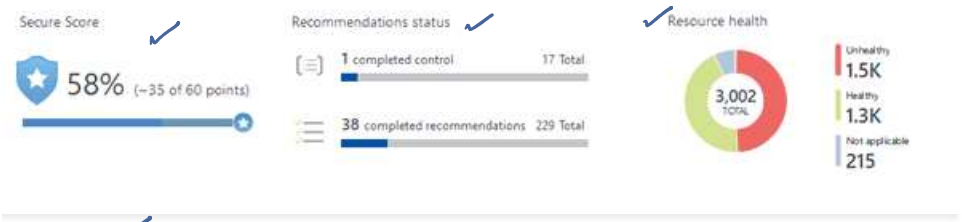
Defender for Cloud can also protect resources in other clouds (such as AWS and GCP)

- Defender for Cloud's CSPM features extend to your AWS resources. This agentless plan assesses your AWS resources according to AWS-specific security recommendations, and includes the results in the secure score. The resources will also be assessed for compliance with built-in standards specific to AWS (AWS CIS, AWS PCI DSS, and AWS Foundational Security Best Practices).
- Microsoft Defender for Containers extends its container threat detection and advanced defenses to your Amazon EKS Linux clusters
- Microsoft Defender for Servers brings threat detection and advanced defenses to your Windows and Linux EC2 instances

Assess, Secure, and Defend

Defender for Cloud fills three vital needs

- Continuously assess – Know your security posture. Identify and track vulnerabilities
- Secure – Harden resources and services with Azure Security Benchmark
- Defend – Detect and resolve threats to resources, workloads, and services



Controls	Potential score increase	Unhealthy resources	Resource Health
Remediate vulnerabilities	+ 10% (6 points)	171 of 219 resources	
Enable encryption at rest	+ 5% (3 points)	147 of 231 resources	
Manage access and permissions	+ 5% (3 points)	20 of 36 resources	
Remediate security configurations	+ 4% (3 points)	134 of 212 resources	
Protect applications against DDoS attacks	+ 3% (2 points)	14 of 156 resources	
Encrypt data in transit	+ 3% (2 points)	135 of 331 resources	
Apply system updates	+ 3% (2 points)	57 of 212 resources	
Apply adaptive application control	+ 2% (1 point)	75 of 165 resources	
Secure management ports	+ 2% (1 point)	14 of 151 resources	
Apply data classification	+ 2% (1 point)	16 of 53 resources	
Restrict unauthorized network access	+ 1% (1 point)	48 of 241 resources	
Enable endpoint protection	+ 1% (1 point)	75 of 192 resources	
Enable auditing and logging	+ 1% (1 point)	134 of 180 resources	
Implement security best practices	+ 0% (0 points)	168 of 797 resources	
Enable advanced threat protection	+ 0% (0 points)	8 of 11 resources	
Custom recommendations	+ 0% (0 points)	1033 of 2183 resources	
Enable MFA Completed	+ 0% (0 points)	None	

Defend

The first two areas were focused on assessing, monitoring, and maintaining your environment. Defender for Cloud also helps you defend your environment by providing security alerts and advanced threat protection features.

Security alerts

When Defender for Cloud detects a threat in any area of your environment, it generates a security alert. Security alerts:

- Describe details of the affected resources
- Suggest remediation steps
- Provide, in some cases, an option to trigger a logic app in response

Advanced threat protection ✓

Defender for cloud provides advanced threat protection features for many of your deployed resources, including virtual machines, SQL databases, containers, web applications, and your network.

Describe factors that can affect costs in Azure

Azure shifts costs from the capital expense (CapEx) to an operational expense (OpEx) of renting infrastructure as you need it, whether it's compute, storage, networking, and so on.

Some of the impacting factors are for OpEx cost :
- Resource type
- Consumption
- Maintenance
- Geography
- Subscription type
- Azure Marketplace

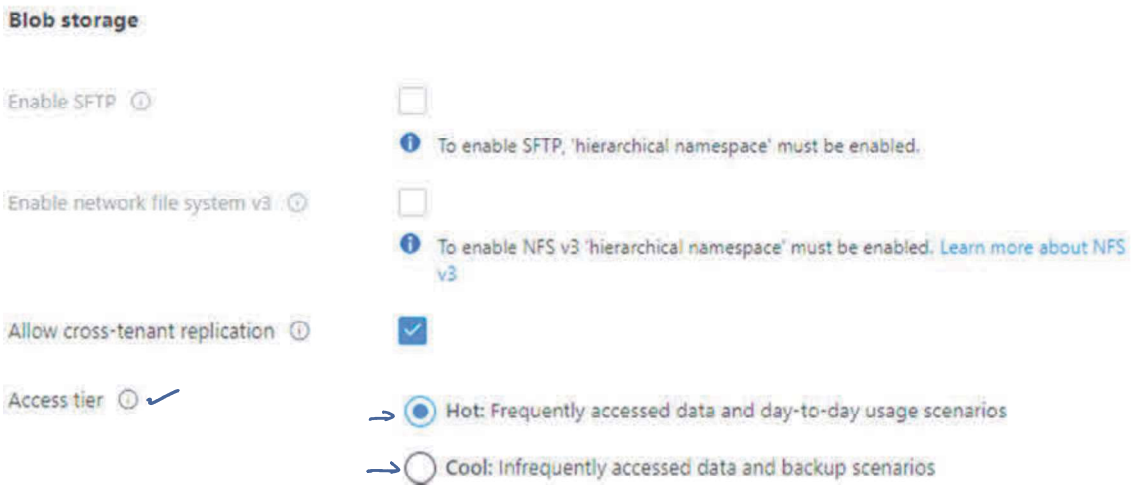
Resource type

A number of factors influence the cost of Azure resources
- Type of resources
- Settings for the resource
- Azure region

When you provision an Azure resource, Azure creates metered instances for that resource, used to calculate your bill

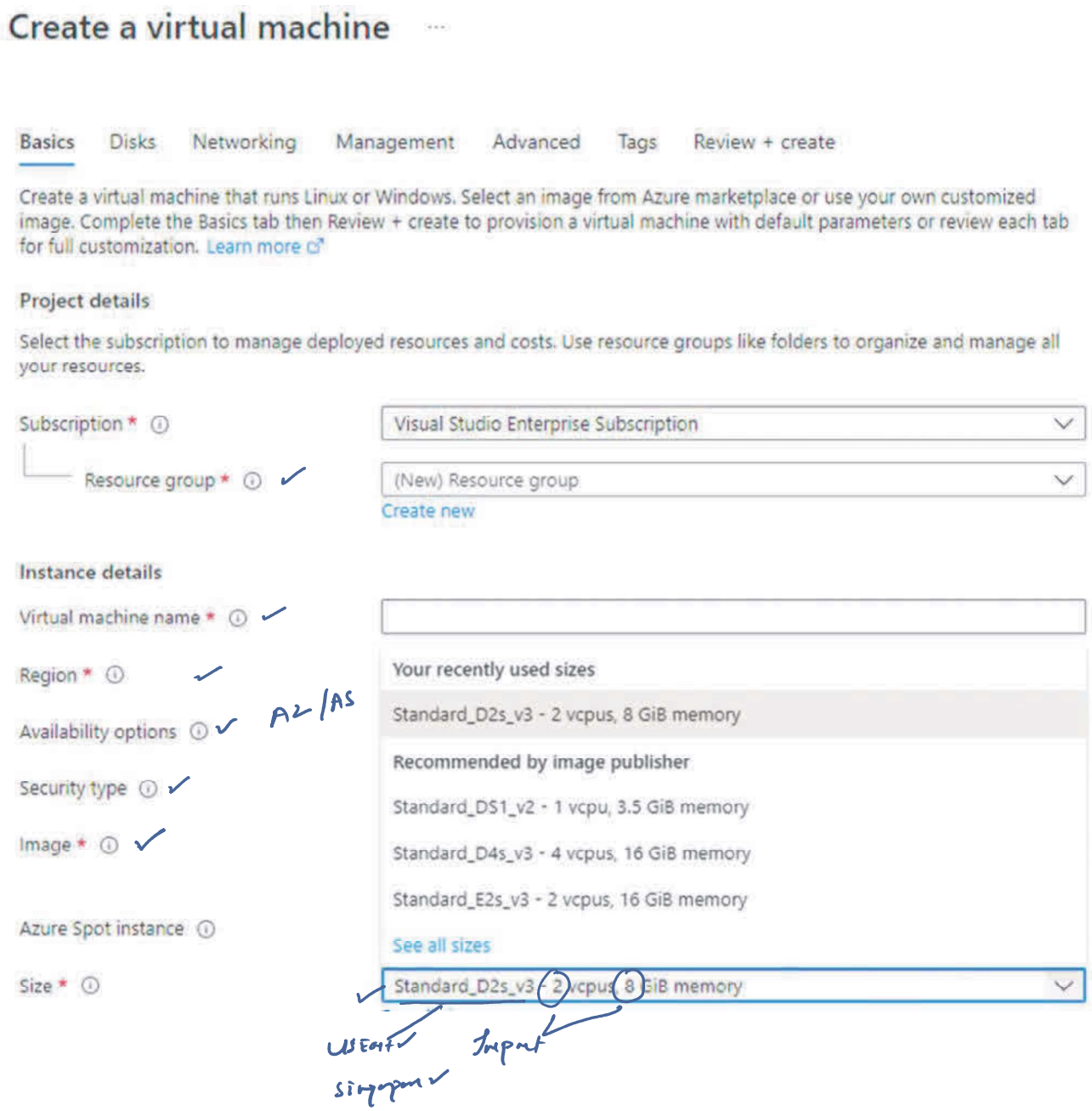
Examples

With a storage account, you specify a type such as blob, a performance tier, an access tier, redundancy settings, and a region
Creating the same storage account in different regions will show different price



With a virtual machine (VM)
- Licensing for the operating system or other software
- Processor and number of cores for the VM
- Attached storage
- Network interface

Provisioning the same virtual machine in different regions may result in different costs



Consumption
Pay-as-you-go where you pay for the resources that you use during a billing cycle

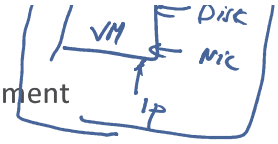
Reserved resources
Many services, including databases, compute, and storage all provide the option to commit to a level of use and receive a discount, in some cases up to 72 percent

When you reserve capacity, you're committing to using and paying for a certain amount of Azure resources during a given period (typically one or three years)

Maintenance
Using resource groups can help keep all of your resources organized
In order to control costs, it's important to maintain your cloud environment

Maintenance

Using resource groups can help keep all of your resources organized
In order to control costs, it's important to maintain your cloud environment

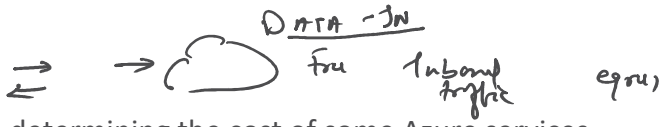


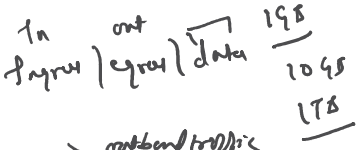
For example, every time you provision a VM, additional resources such as storage and networking are also provisioned

Geography ✓

When you provision most resources in Azure, you need to define a region
Azure infrastructure is distributed globally
With this global deployment comes global pricing differences
The cost of power, labor, taxes, and fees vary depending on the location. Due to these variations, Azure resources can differ in costs to deploy depending on the region

Network Traffic ✓





Billing zones are a factor in determining the cost of some Azure services
Bandwidth refers to data moving in and out of Azure datacenters
Some inbound data transfers (data going into Azure datacenters) are free
For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on zones

Subscription type ✓

Azure free trial subscription provides access to a number of Azure products that are free for 12 months.

Azure Marketplace ✓

Azure Marketplace lets you purchase Azure-based solutions and services from third-party vendors
This could be a server with software preinstalled and configured, or managed network firewall appliances, or connectors to third-party backup services

Billing structures are set by the vendor

Compare the Pricing and Total Cost of Ownership calculators

- The pricing calculator and the total cost of ownership (TCO) calculator are two calculators that help you understand potential Azure expenses
- Both accessible from the internet, allow you to build out a configuration
- These two calculators have very different purposes

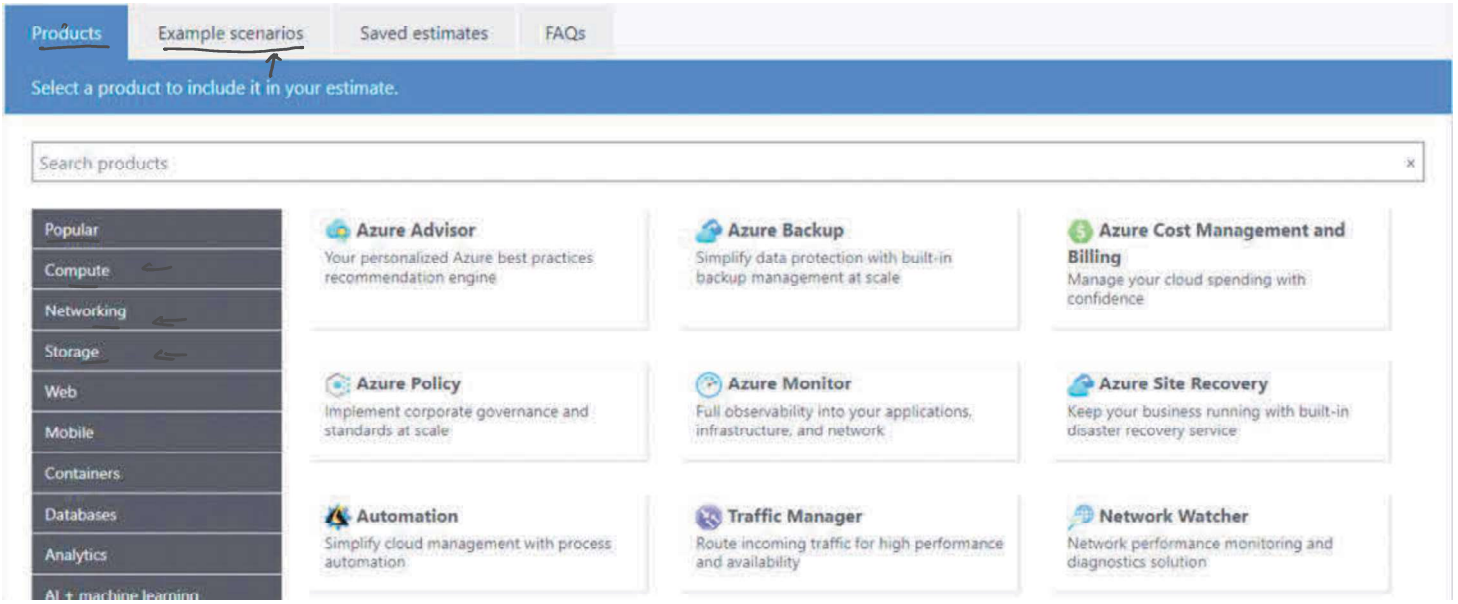
Pricing calculator ✓

- Gives you an estimated cost for provisioning resources in Azure
- You can get an estimate for individual resources, build out a solution, or use an example scenario to see an estimate of the Azure spend
- The pricing calculator's focus is on the cost of provisioned resources in Azure

Note:
- The Pricing calculator is for information purposes only
- The prices are only an estimate
- Nothing is provisioned

Get the estimated cost of any provisioned resources
- Compute ✓
- Storage ✓
- Network costs ✓

Storage options like storage type, access tier, and redundancy can also be estimated using the Pricing calculator



TCO calculator ✓

The TCO calculator is designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure

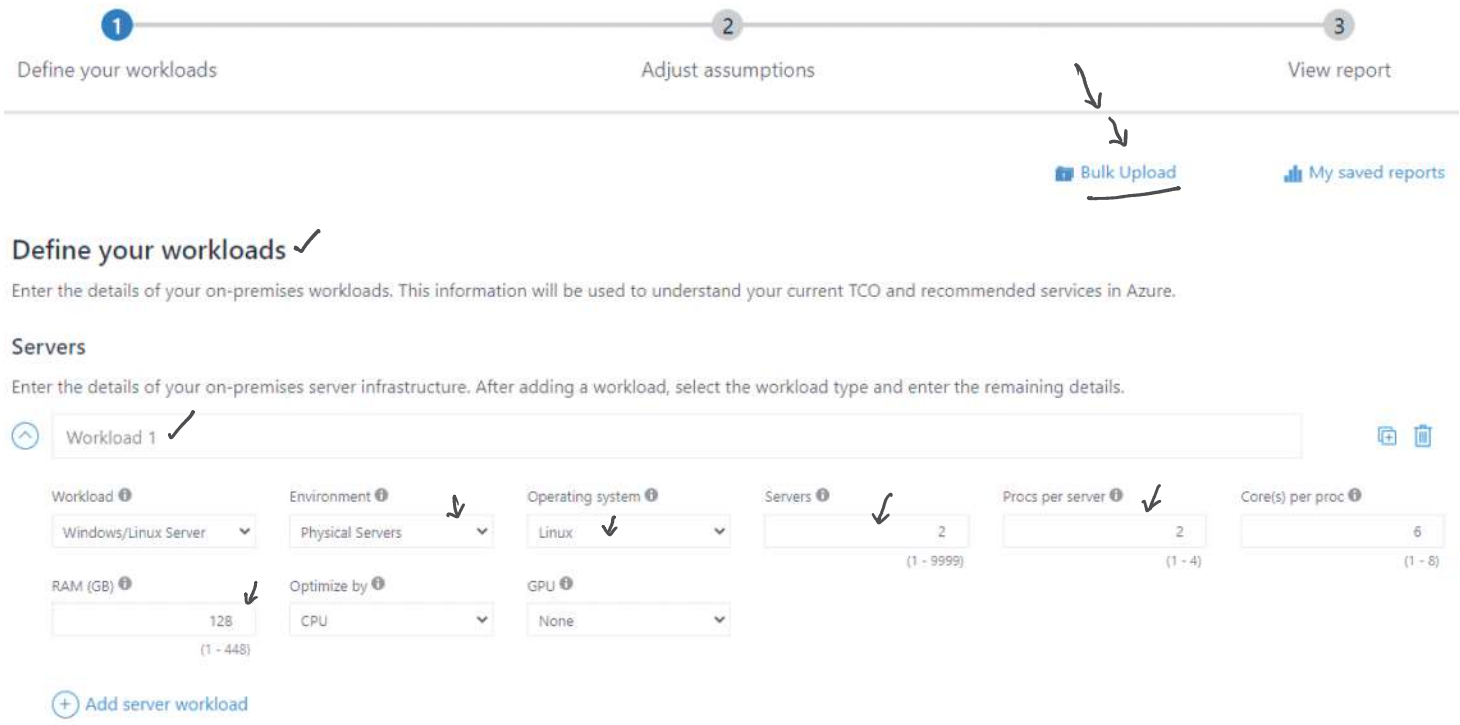
The TCO calculator is designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure

With the TCO calculator

You enter your current infrastructure configuration: Servers, databases, storage, and outbound network traffic

The TCO calculator then compares the anticipated costs for your current environment with an Azure environment supporting the same infrastructure requirements

Add in assumptions like power and IT labor costs



Microsoft Cost Management tool

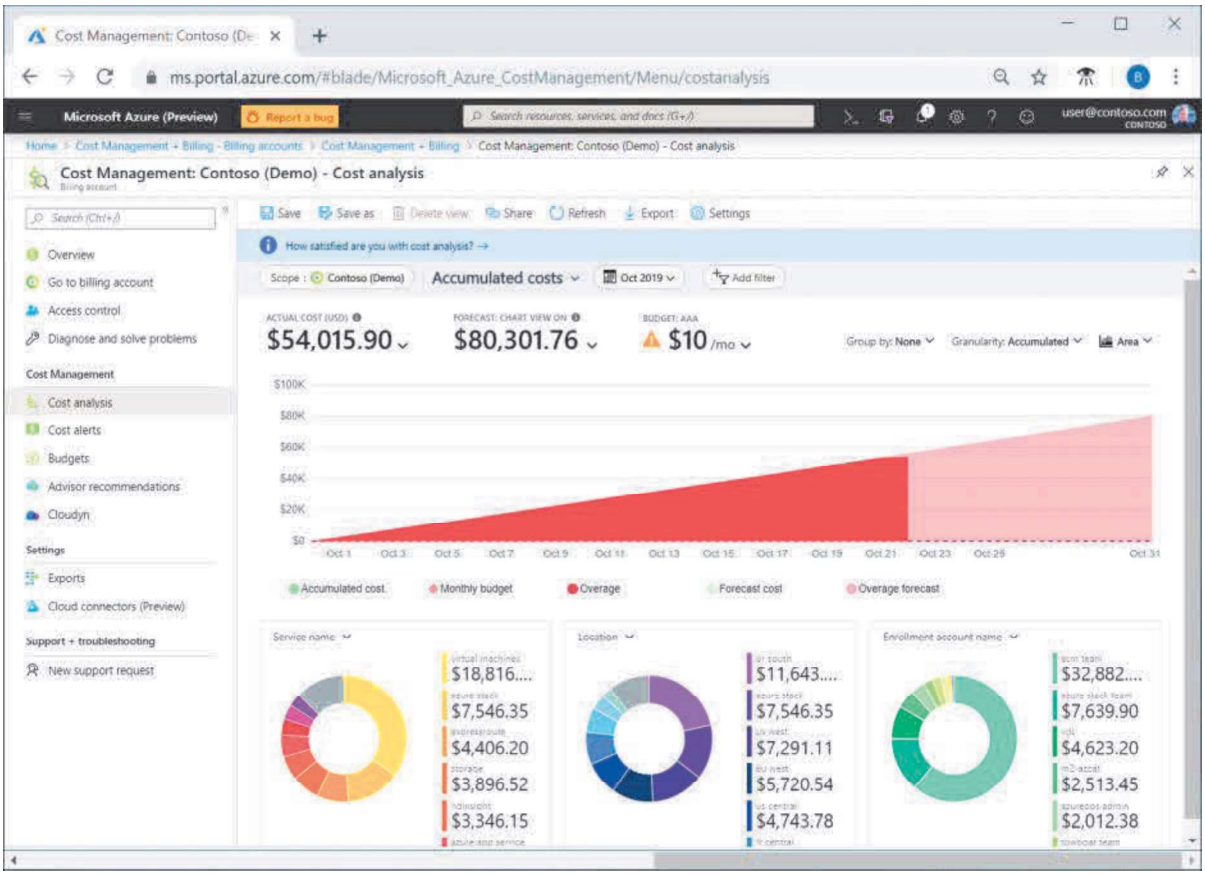
Describe the Microsoft Cost Management tool

Microsoft Azure is a global cloud provider, meaning you can provision resources anywhere in the world. You can provision resources rapidly to meet a sudden demand, or to test out a new feature, or on accident. If you accidentally provision new resources, you may not be aware of them until it's time for your invoice. Cost Management is a service that helps avoid those situations.

What is Cost Management?

Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

Cost analysis is a subset of Cost Management that provides a quick visual for your Azure costs. Using cost analysis, you can quickly view the total cost in a variety of different ways, including by billing cycle, region, resource, and so on.



You use cost analysis to explore and analyze your organizational costs. You can view aggregated costs by organization to understand where costs are accrued and to identify spending trends. And you can see accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.

Cost alerts

Cost alerts provide a single location to quickly check on all of the different alert types that may show up in the Cost Management service. The three types of alerts that may show up are:

- Budget alerts
- Credit alerts
- Department spending quota alerts.

Budget alerts

Budget alerts notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget. Cost Management budgets are created using the Azure portal or the Azure Consumption API. In the Azure portal, budgets are defined by cost. Budgets are defined by cost or by consumption usage when using the Azure Consumption API. Budget alerts support both cost-based and usage-based budgets. Budget alerts are generated

automatically whenever the budget alert conditions are met. You can view all cost alerts in the Azure portal. Whenever an alert is generated, it appears in cost alerts. An alert email is also sent to the people in the alert recipients list of the budget.

Credit alerts

Credit alerts notify you when your Azure credit monetary commitments are consumed. Monetary commitments are for organizations with Enterprise Agreements (EAs). Credit alerts are generated automatically at 90% and at 100% of your Azure credit balance. Whenever an alert is generated, it's reflected in cost alerts, and in the email sent to the account owners.

Department spending quota alerts

Department spending quota alerts notify you when department spending reaches a fixed threshold of the quota. Spending quotas are configured in the EA portal. Whenever a threshold is met, it generates an email to department owners, and appears in cost alerts. For example, 50 percent or 75 percent of the quota.

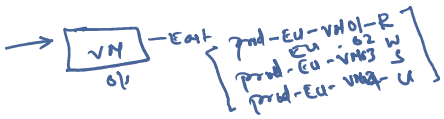
Budgets

A budget is where you set a spending limit for Azure. You can set budgets based on a subscription, resource group, service type, or other criteria. When you set a budget, you will also set a budget alert. When the budget hits the budget alert level, it will trigger a budget alert that shows up in the cost alerts area. If configured, budget alerts will also send an email notification that a budget alert threshold has been triggered.

A more advanced use of budgets enables budget conditions to trigger automation that suspends or otherwise modifies resources once the trigger condition has occurred.

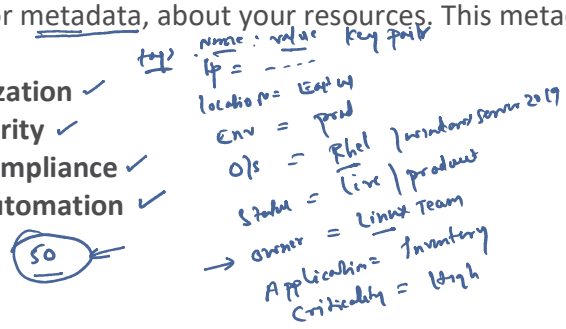
Tags

As your cloud usage grows, it's increasingly important to stay organized
One way to organize related resources is to place them in their own subscriptions
You can also use resource groups to manage related resources



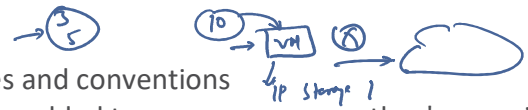
Tags provide extra information, or metadata, about your resources. This metadata is useful for:

- **Resource management** ✓
- **Cost management and optimization** ✓
- **Operations management Security** ✓
- **Governance and regulatory compliance** ✓
- **Workload optimization and automation** ✓



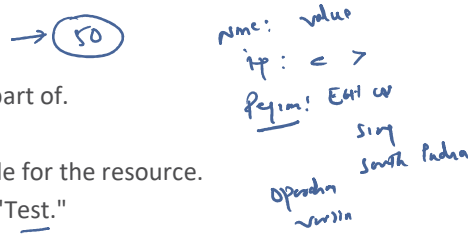
How do I manage resource tags?

You can add, modify, or delete resource tags through Windows PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.



You can use Azure Policy to enforce tagging rules and conventions
For example, you can require that certain tags be added to new resources as they're provisioned.
Resources don't inherit tags from subscriptions and resource groups

An example tagging structure
A resource tag consists of a name and a value. You can assign one or more tags to each Azure resource



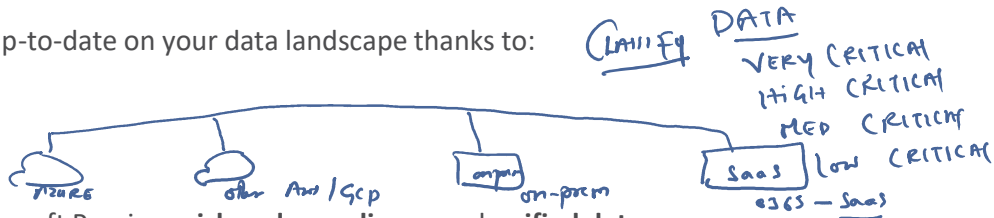
Name	Value
AppName	The name of the application that the resource is part of.
CostCenter	The internal cost center code.
Owner	The name of the business owner who's responsible for the resource.
Environment	An environment name, such as "Prod," "Dev," or "Test."
Impact	How important the resource is to business operations, such as "Mission-critical," "High-impact," or "Low-impact."

For example, you might decide that only mission-critical resources have the Impact tag. All non-tagged resources would then not be considered as mission-critical.

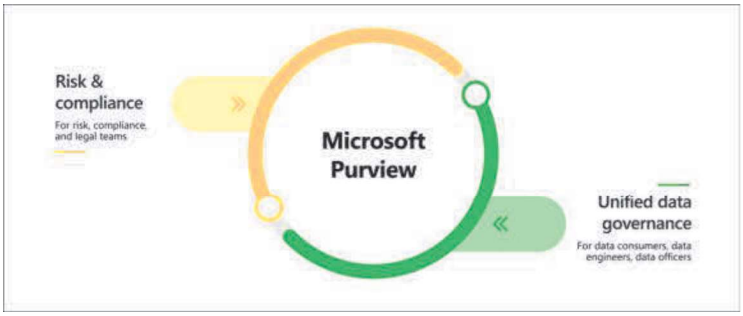
Microsoft Purview

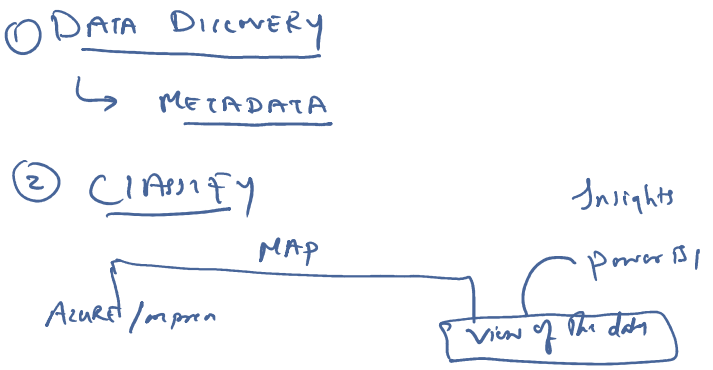
Microsoft Purview is a family of data governance, risk, and compliance solutions that helps you get a single, unified view into your data
Microsoft Purview brings insights about your on-premises, multicloud, and software-as-a-service data together

With Microsoft Purview, you can stay up-to-date on your data landscape thanks to:
- Automated data discovery
- Sensitive data classification
- End-to-end data lineage



Two main solution areas comprise Microsoft Purview: **risk and compliance** and **unified data governance**.





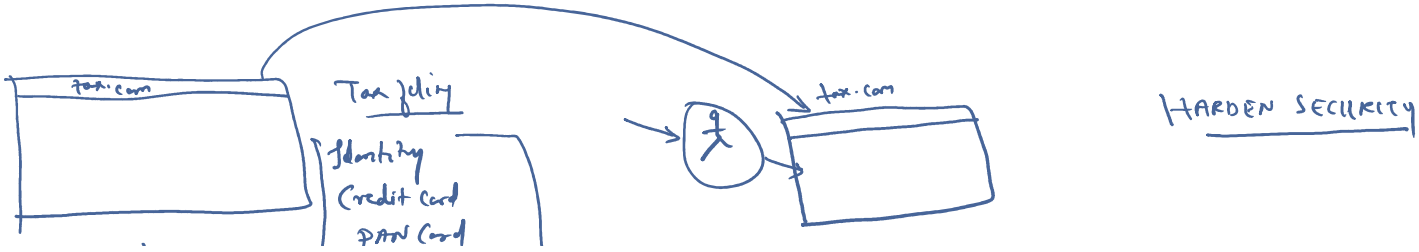
Microsoft Purview risk and compliance solutions

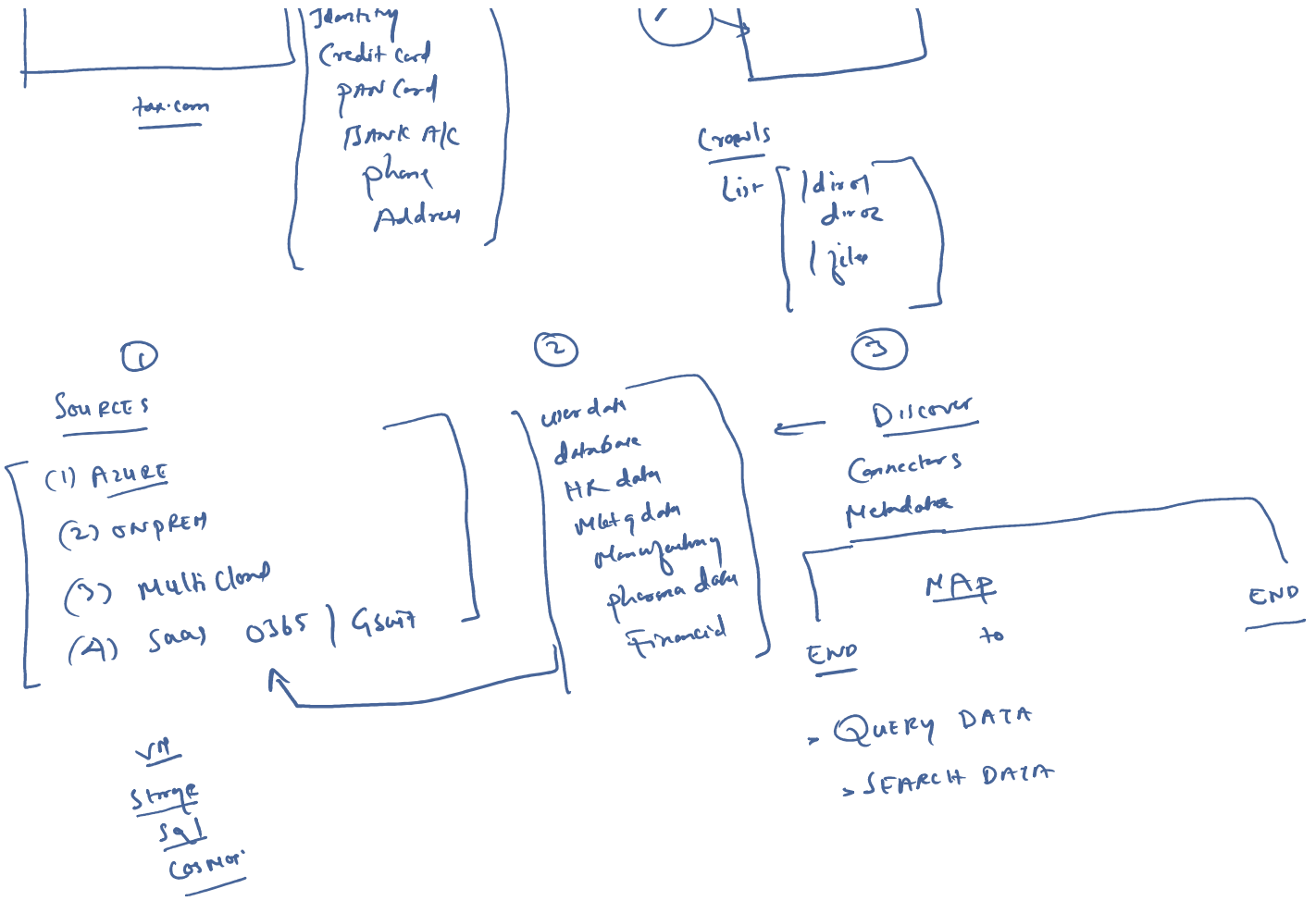
Microsoft 365 features as a core component of the Microsoft Purview risk and compliance solutions
Microsoft Teams, OneDrive, and Exchange are just some of the Microsoft 365 services that Microsoft Purview uses to help manage and monitor your data.

Microsoft Purview, by managing and monitoring your data, is able to help your organization:
- Protect sensitive data across clouds, apps, and devices.
- Identify data risks and manage regulatory compliance requirements.
- Get started with regulatory compliance.

Unified data governance

Microsoft Purview's unified data governance helps your organization:
- Create an up-to-date map of your entire data estate that includes data classification and end-to-end lineage.
- Identify where sensitive data is stored in your estate.
- Create a secure environment for data consumers to find valuable data.
- Generate insights about how your data is stored and used.
- Manage access to the data in your estate securely and at scale.



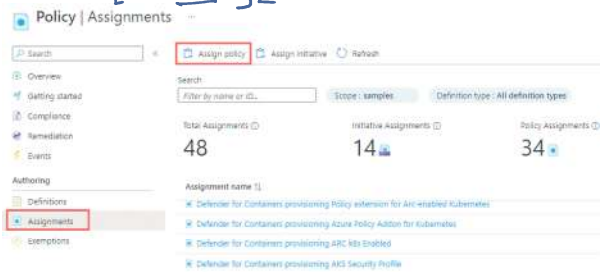

tax.com
Identity
Credit card
PAN Card
Bank A/C
phone
Address
Groups
List
Idirol
dirol
file
1
Sources
(1) AZURE
(2) ONPREM
(3) Multi Cloud
(4) Saas O365 | GSuit
VM
Storage
Sql
Cosmos
2
User data
database
HR data
Mktg data
Manufacturing
pharma data
Financial
3
Discover
Connectors
Metadata
MAP
to
END
END
> QUERY DATA
> SEARCH DATA

Azure Policy

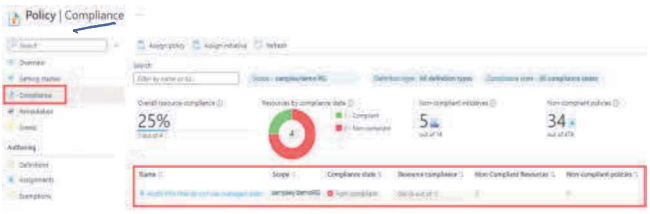
To create, assign, and manage policies that control or audit your resources. With Azure Policy configurations stay compliant with corporate standards.

How does Azure Policy define policies?

Azure Policy enables you to define both individual policies and groups of related policies known as initiatives.



Azure Policy evaluates your resources and highlights resources that aren't compliant



Azure Policy can also prevent noncompliant resources from being created.
Azure Policies can be set on a specific resource, resource group, subscription
Azure Policies are inherited
Azure Policy comes with built-in policy and initiative definitions for Storage, Networking, Compute, Security Center, and Monitoring.
For example, if you define a policy that allows only a certain size for the virtual machines (VMs) to be used in your environment, that policy is invoked when you create a new VM and whenever you resize existing VMs.

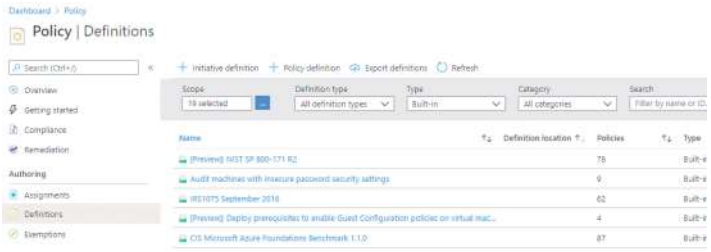
In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources.
For example, if all resources in a certain resource group should be tagged with AppName tag and a value of "SpecialOrders," Azure Policy will automatically apply that tag if it is missing.
However, you still retain full control of your environment.
Azure Policy also integrates with Azure DevOps

What are Azure Policy initiatives?

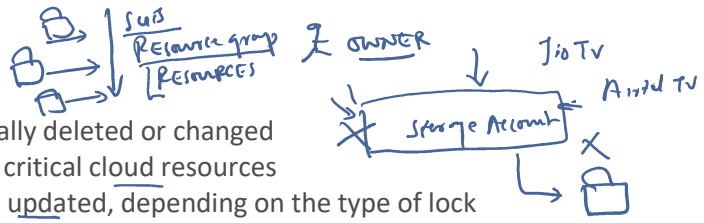
An Azure Policy initiative is a way of grouping related policies together.
For example, Azure Policy includes an initiative named Enable Monitoring in Azure Security Center. Its goal is to monitor all available security recommendations for all Azure resource types in Azure Security Center.
Under this initiative, the following policy definitions are included:

- **Monitor unencrypted SQL Database in Security Center** This policy monitors for unencrypted SQL databases and servers.
- **Monitor OS vulnerabilities in Security Center** This policy monitors servers that don't satisfy the configured OS vulnerability baseline.
- **Monitor missing Endpoint Protection in Security Center** This policy monitors for servers that don't have an

installed endpoint protection agent.



Describe the purpose of resource locks



- A resource lock prevents resources from being accidentally deleted or changed
- With the right level of access (Azure RBAC) could delete critical cloud resources
- Resource locks prevent resources from being deleted or updated, depending on the type of lock
- Resource locks can be applied to individual resources, resource groups, or even an entire subscription
- Resource locks are inherited, meaning that if you place a resource lock on a resource group, all of the resources within the resource group will also have the resource lock applied

Types of Resource Locks

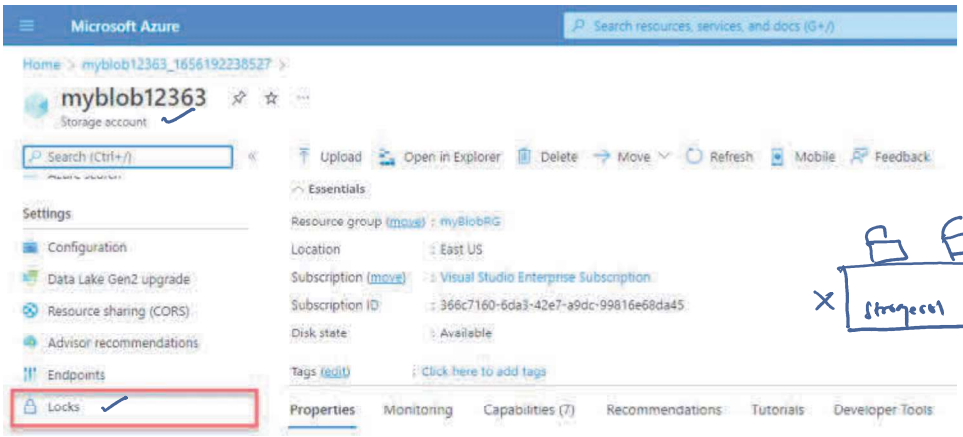
There are two types of resource locks ✓

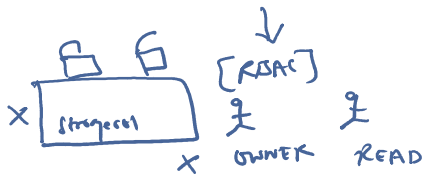
- **Delete** means authorized users can still read and modify a resource, but they can't delete the resource
- **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource

How do I manage resource locks?

You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template

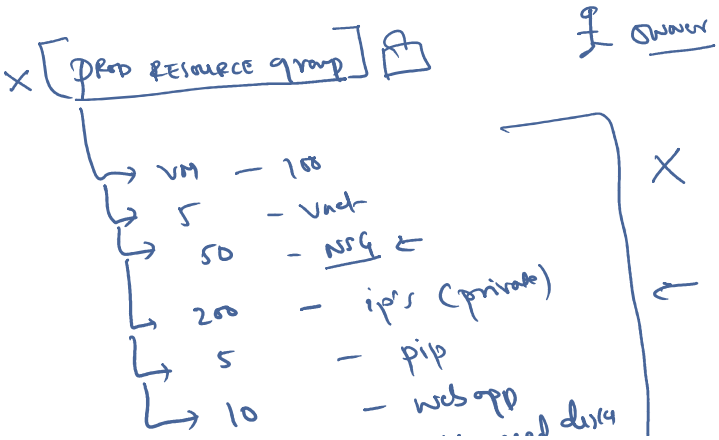
To view, add, or delete locks in the Azure portal, go to the Settings section of any resource's Settings pane in the Azure po rtal.

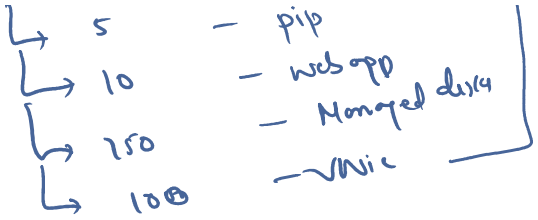




How do I delete or change a locked resource?

- To modify a locked resource, you must first remove the lock
- After you remove the lock, you can apply any action you have permissions to perform
- Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity




5 – pip
10 – web app
– Managed disks
250
– VNic
100

Service Trust Portal

Service Trust portal

The Microsoft Service Trust Portal is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

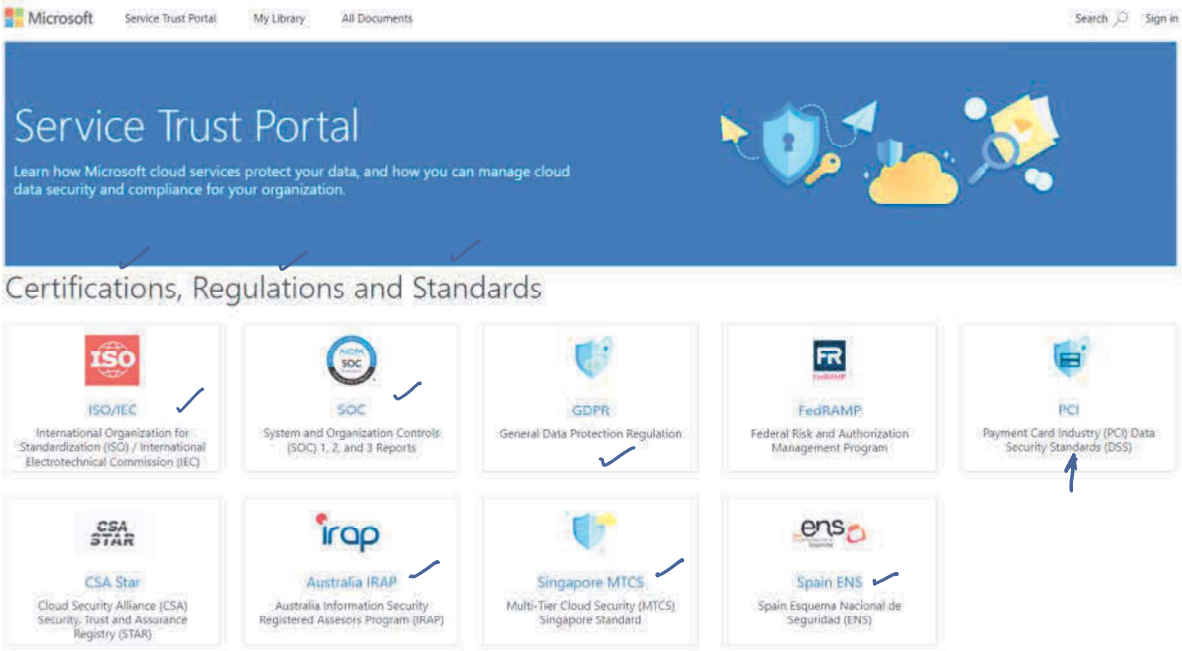
The Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data

To access some of the resources on the Service Trust Portal, you must sign in as an authenticated user with your Microsoft cloud services account (Microsoft Entra organization account).

You'll need to review and accept the Microsoft non-disclosure agreement for compliance materials.

Accessing the Service Trust Portal

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



Certifications, Regulations and Standards

- ISO/IEC
- SOC
- GDPR
- FedRAMP
- PCI
- CSA Star
- Australia IRAP
- Singapore MTCS
- Spain ENS

Reports, Whitepapers, and Artifacts

- AI Resources
- BCP and DR
- Pen Test and Security Assessments:
- Privacy and Data Protection:
- FAQ and Whitepapers

Industry and Regional Resources

- Financial Services
- Healthcare and Life Sciences
- Media and Entertainment
- United States Government
- Regional Resources

Tools for Managing Azure

To interact with the Azure environment, the management groups, subscriptions, resource groups, resources, and so on…

Tools:

- Azure portal
- Azure PowerShell
- Azure Command Line Interface (CLI)

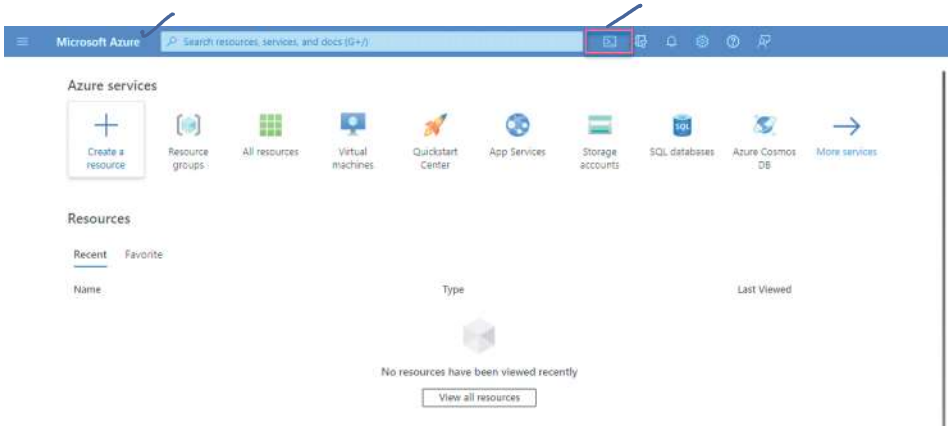
What is the Azure portal?

The Azure portal is a web-based

- Build, manage, and monitor everything from simple web apps to complex cloud deployments
- Create custom dashboards for an organized view of resources
- Configure accessibility options for an optimal experience
- The Azure portal is designed for resiliency and continuous availability
- Azure portal has presence in every Azure datacenter
- This makes resilient to individual datacenter failures and avoids network slowdowns
- The Azure portal updates continuously and requires no downtime for maintenance activities

Azure Cloud Shell

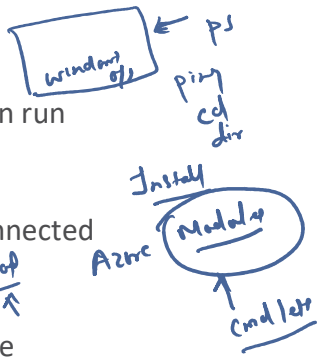
- Azure Cloud Shell is a browser-based shell tool that allows you to create, configure, and manage Azure resources using a shell
- Support both Azure PowerShell and the Azure Command Line Interface (CLI), which is a Bash shell
- You can access Azure Cloud Shell via the Azure portal



Azure Cloud Shell has several features

- It is a browser-based shell experience, with no local installation or configuration required
- It is authenticated to your Azure credentials
- You choose the shell Azure PowerShell and the Azure CLI (which uses Bash)

- You choose the shell Azure PowerShell and the Azure CLI (which uses Bash)



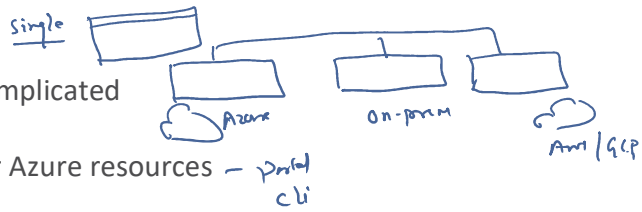
What is Azure PowerShell?

- Azure PowerShell is a shell with which developers, DevOps, and IT professionals can run commands called command-lets (cmdlets)
- These commands call the Azure REST API to perform management tasks in Azure
- The routine setup, teardown, and maintenance of a single resource or multiple connected resources
- The deployment of an entire infrastructure
- Capturing the commands in a script makes the process repeatable and automatable
- Install and configure Azure PowerShell on Windows, Linux, and Mac platforms

What is the Azure CLI?

- The Azure CLI is similar to Azure PowerShell, the difference is syntax of commands
- While Azure PowerShell uses PowerShell commands, the Azure CLI uses Bash commands
- Installable on Windows, Linux, and Mac platforms
- Due to the similarities in capabilities and access between Azure PowerShell and the Bash based Azure CLI, it mainly comes down to which language you're most familiar with

Azure Arc



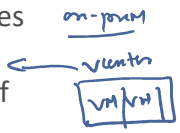
Describe the purpose of Azure Arc ✓

- Managing hybrid and multi-cloud environments can rapidly get complicated
- Azure provides a host of tools to provision, configure, and monitor Azure resources – Portal CLI

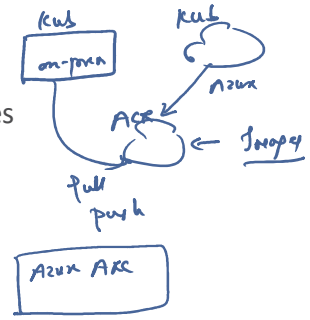
What about the on-premises resources in a hybrid configuration or the cloud resources in a multi-cloud configuration?

- Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform

Azure Arc Allows to:



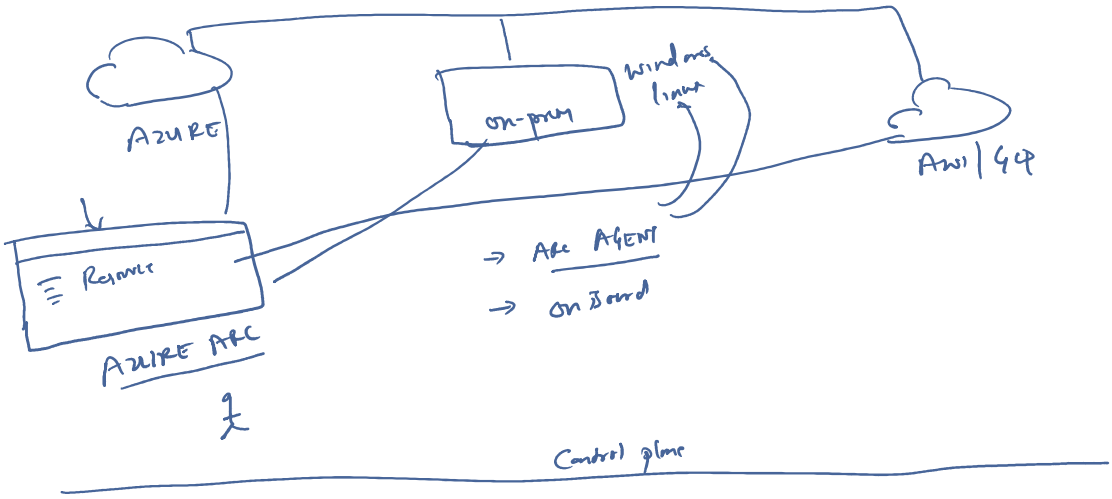
- Manage your entire environment together by projecting your existing non-Azure resources into ARM
- Manage multi-cloud and hybrid virtual machines, Kubernetes clusters, and databases as if they are running in Azure
- Use familiar Azure services and management capabilities, regardless of where they live
- Continue using traditional ITOps while introducing DevOps practices to support new cloud and native patterns in your environment CI/CD
- Configure custom locations as an abstraction layer on top of Azure Arc-enabled Kubernetes clusters and cluster extensions ✓



What can Azure Arc Manage ?

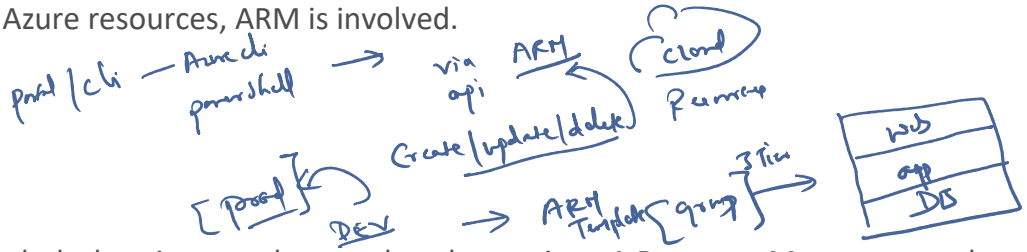
Currently, Azure Arc allows you to manage the following resource types hosted outside of Azure:

- Servers ✓ windows / linux
- Kubernetes clusters ✓ 9500 VM
- Azure data services ✓ VCENTER | SCVMM
- SQL Server ✓
- Virtual machines ✓



Describe Azure Resource Manager and Azure ARM templates

Azure Resource Manager (ARM) is the deployment and management service for Azure.
It provides a management layer that enables you to create, update, and delete resources in your Azure account.
Anytime you do anything with your Azure resources, ARM is involved.

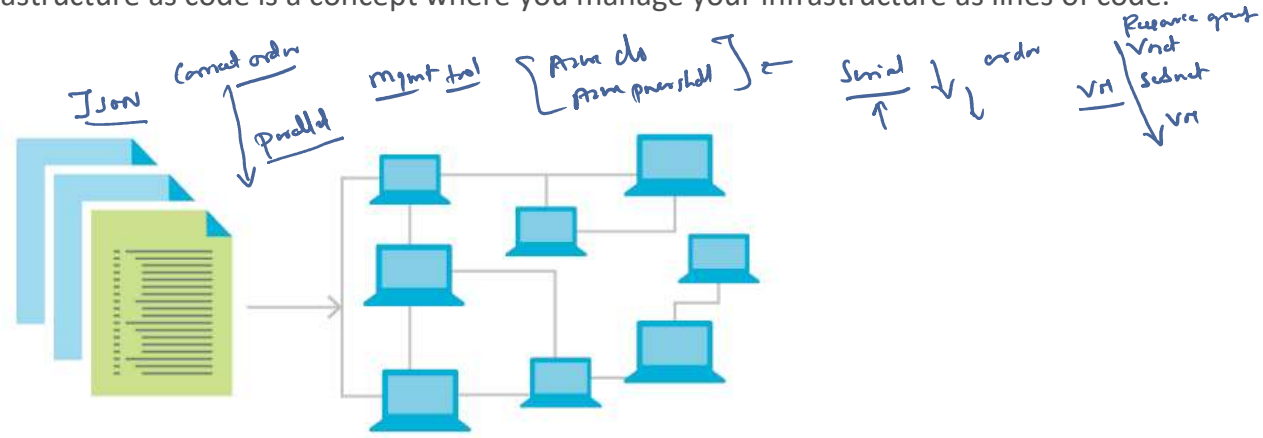


Azure Resource Manager benefits

- Manage your infrastructure through declarative templates rather than scripts. A Resource Manager template is a JSON file
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually
- Re-deploy your solution throughout the development life-cycle and have confidence your resources are deployed in a consistent state
- Define the dependencies between resources, so they're deployed in the correct order
- Apply access control to all services because RBAC is natively integrated into the management platform
- Apply tags to resources to logically organize all the resources in your subscription
- Clarify your organization's billing by viewing costs for a group of resources that share the same tag

Infrastructure as code

Infrastructure as code is a concept where you manage your infrastructure as lines of code.



ARM templates

By using ARM templates, you can describe the resources you want to use in a declarative JSON format. With an ARM template, the deployment code is verified before any code is run. This ensures that the resources will be created and connected correctly. The template then orchestrates the creation of those resources in parallel. That is, if you need 50 instances of the same resource, all 50 instances are created at the same time.

Benefits of using ARM templates

- **Declarative syntax**: ARM templates allow you to create and deploy an entire Azure infrastructure declaratively.
- **Repeatable results**: You can use the same ARM template to deploy multiple dev/test environments, knowing that all the environments are the same.
- **Orchestration**: Azure Resource Manager orchestrates the deployment of interdependent resources, so they're created in the correct order. When possible, Azure Resource Manager deploys resources in parallel
- **Modular files**: You can break your templates into smaller, reusable components and link them together at deployment time. You can also nest one template inside another template.
- **Extensibility:** You can add PowerShell or Bash scripts to your templates. A script can be included in the template or stored in an external source and referenced in the template.

JSON ←

Bicep

Bicep is a language that uses declarative syntax to deploy Azure resources.
A Bicep file defines the infrastructure and configuration. Then, ARM deploys that environment based on your Bicep file.

→ Easy | Bicep → Azure Cloud

Benefits of Bicep are:

- **Support for all resource types and API versions**: Bicep immediately supports all preview and GA versions for Azure services.
- **Simple syntax**: When compared to the equivalent JSON template, Bicep files are more concise and easier to read. Bicep requires no previous knowledge of programming languages. Bicep syntax is declarative and specifies which resources and resource properties you want to deploy.
- **Repeatable results**: You can develop one file that represents the desired state, rather than developing lots of separate files to represent updates.
- **Orchestration**: You deploy the file through one command, rather than through multiple imperative commands. Resource Manager orchestrates the deployment of interdependent resources so they're created in the correct order.
- **Modularity**: You can break your Bicep code into manageable parts by using modules. The module deploys a set of related resources.

→ open
↳ Bicep cli windows | linux | mac
Azure cli | Azure powershell
VS code ← Bicep templates

Azure Advisor

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

Azure Advisor is designed to help you save time on cloud optimization.
The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

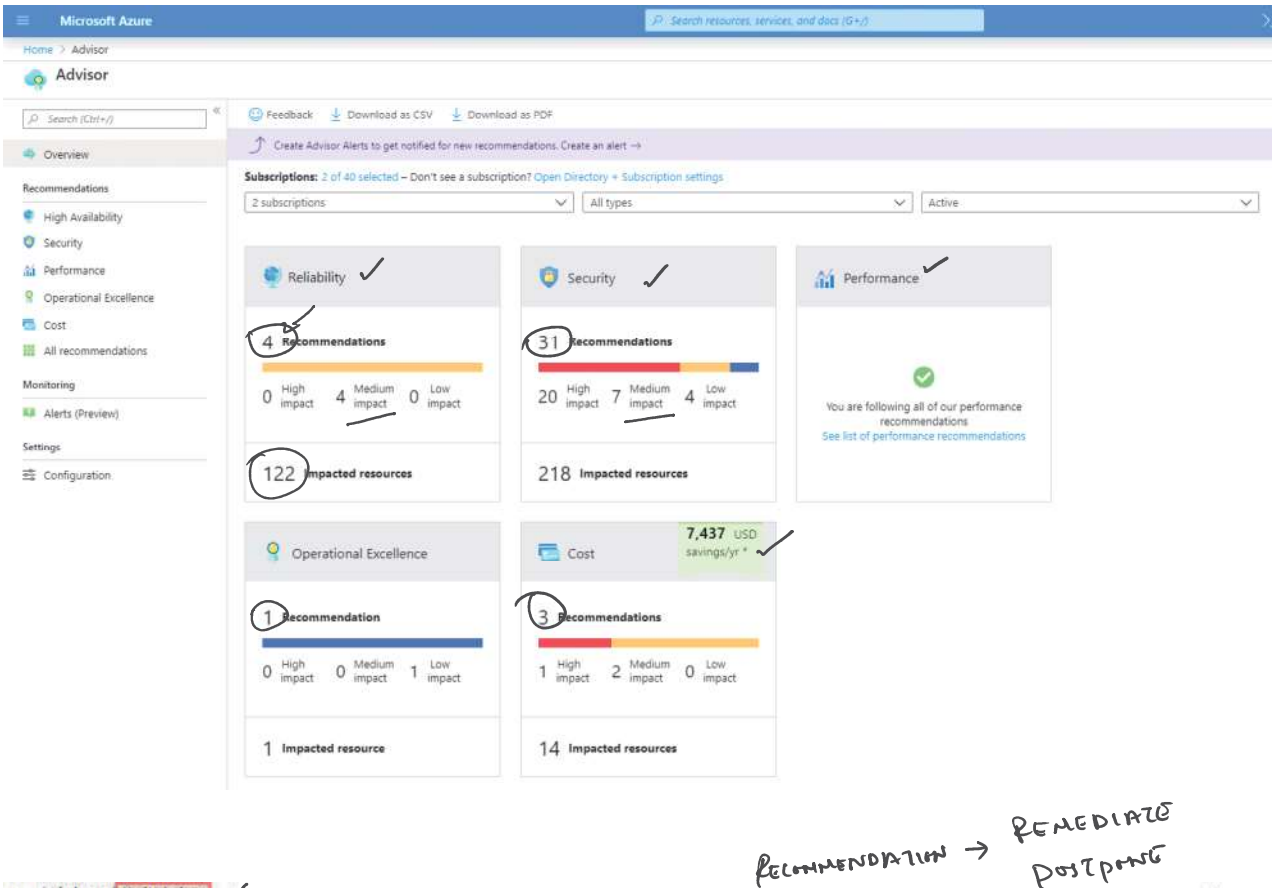
The recommendations are available via the Azure portal and the API, and you can set up notifications to alert you to new recommendations.

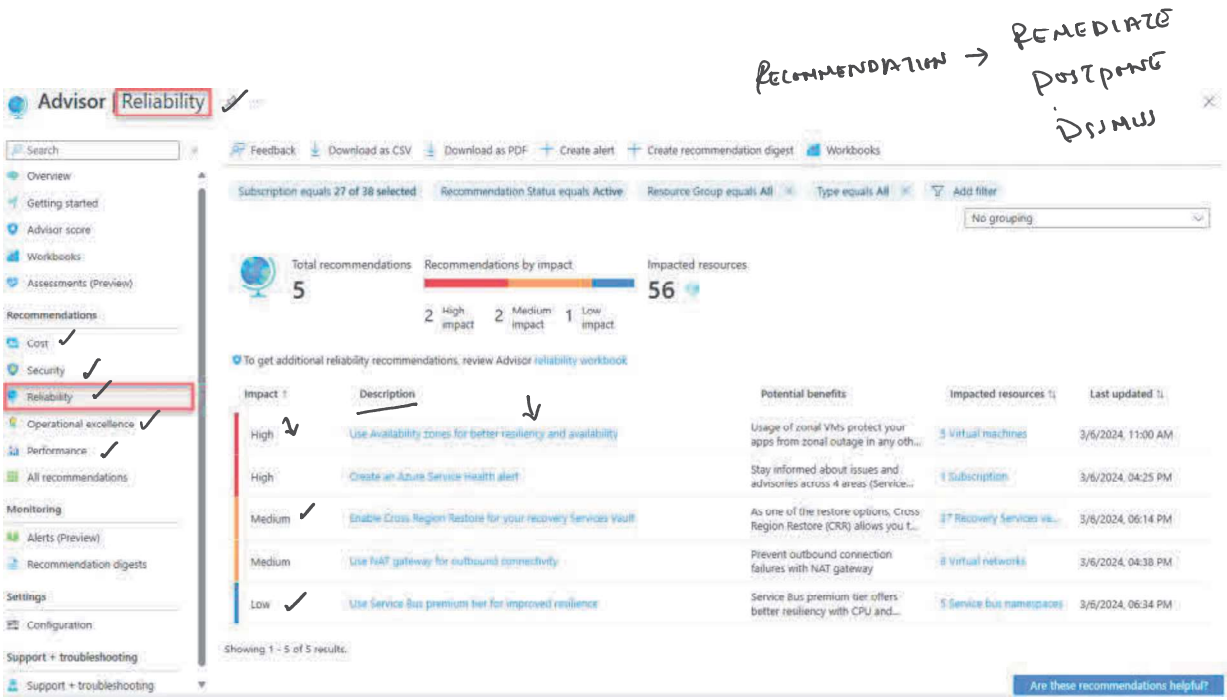
Azure Advisor dashboard displays personalized recommendations for all your subscriptions.
You can use filters to select recommendations for specific subscriptions, resource groups, or services.

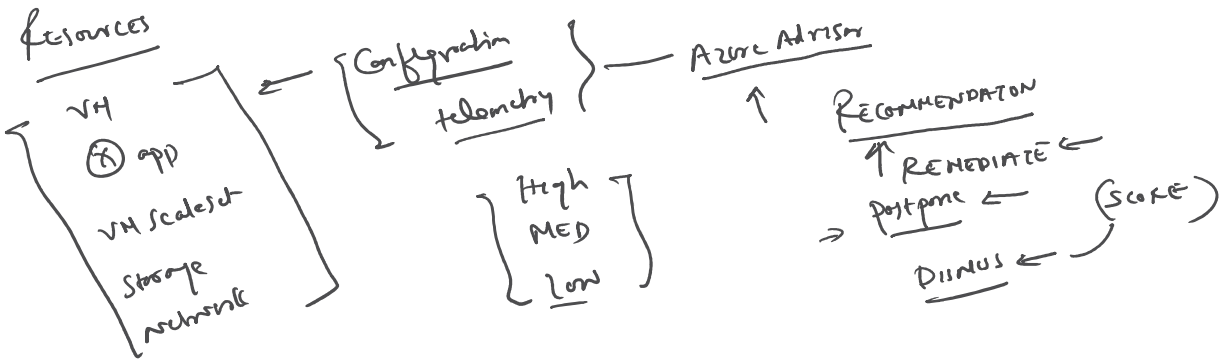
The recommendations are divided into five categories:

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

The following image shows the Azure Advisor dashboard.



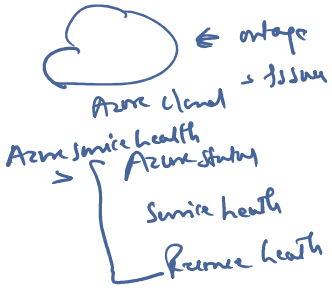

Advisor Reliability
Search
Overview
Getting started
Advisor score
Workbooks
Assessments (Preview)
Recommendations
Cost
Security
Reliability
Operational excellence
Performance
All recommendations
Monitoring
Alerts (Preview)
Recommendation digests
Settings
Configuration
Support + troubleshooting
Support + troubleshooting
Feedback
Download as CSV
Download as PDF
Create alert
Create recommendation digest
Workbooks
Subscription equals 27 of 38 selected
Recommendation Status equals Active
Resource Group equals All
Type equals All
Add filter
No grouping
Total recommendations
5
Recommendations by impact
2 High impact
2 Medium impact
1 Low impact
Impacted resources
56
To get additional reliability recommendations, review Advisor reliability workbook
Impact
Description
Potential benefits
Impacted resources
Last updated
High
Use Availability zones for better resiliency and availability
Usage of zonal VMs protect your apps from zonal outage in any oth...
5 Virtual machines
3/6/2024, 11:00 AM
High
Create an Azure Service Health alert
Stay informed about issues and advisories across 4 areas (Service...
1 Subscription
3/6/2024, 04:25 PM
Medium
Enable Cross Region Restore for your recovery Services vault
As one of the restore options, Cross Region Restore (CRR) allows you t...
17 Recovery Services va...
3/6/2024, 06:14 PM
Medium
Use NAT gateway for outbound connectivity
Prevent outbound connection failures with NAT gateway
8 Virtual networks
3/6/2024, 04:38 PM
Low
Use Service Bus premium tier for improved resilience
Service Bus premium tier offers better resiliency with CPU and...
5 Service bus namespaces
3/6/2024, 06:34 PM
Showing 1 - 5 of 5 results.
Are these recommendations helpful?


Resources
VM
app
VM Scaleset
Storage
Network
Configuration
telemetry
Azure Advisor
Recommendation
Remediate
Postpone
Dismiss
(Score)
High
MED
Low

Azure Service Health

Knowing the status of the global Azure infrastructure and your individual resources may seem like a daunting task.

Azure Service Health helps you keep track of Azure resource, both your specifically deployed resources and the overall status of Azure.



Azure service health does this by combining three different Azure services:

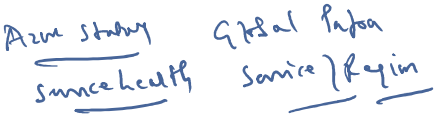
Azure Status

- Status of Azure Services globally.
- Azure status informs you of service outages in Azure on the Azure Status page.
- The page is a global view of the health of all Azure services across all Azure regions.
- It's a good reference for incidents with widespread impact.

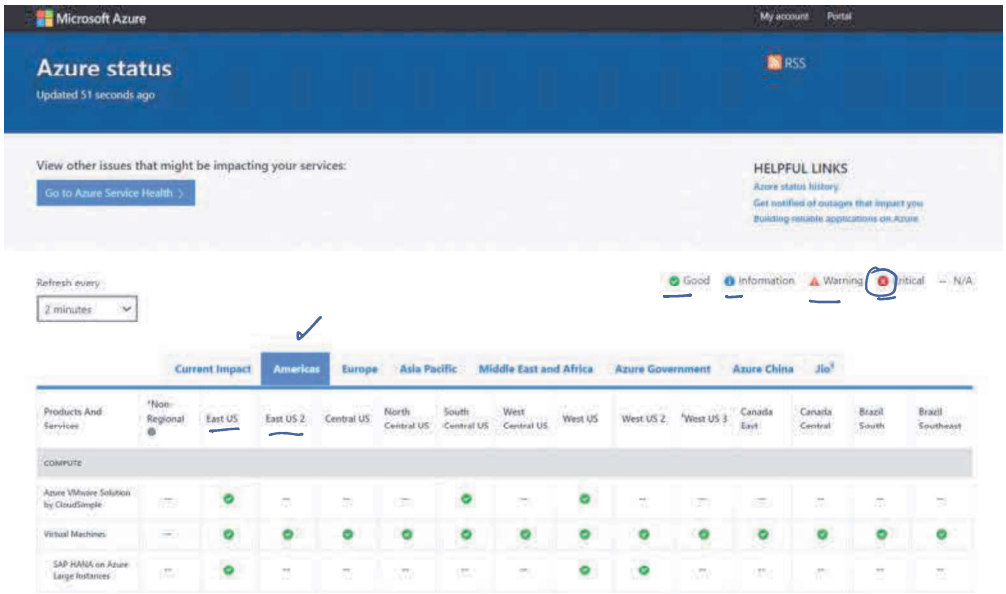
- **Service Health**
  Provides a narrower view of Azure services and regions.
  It focuses on the Azure services and regions you're using.
  Service Health experience knows which services and resources you currently use.
  You can even set up Service Health alerts to notify you when service issues.

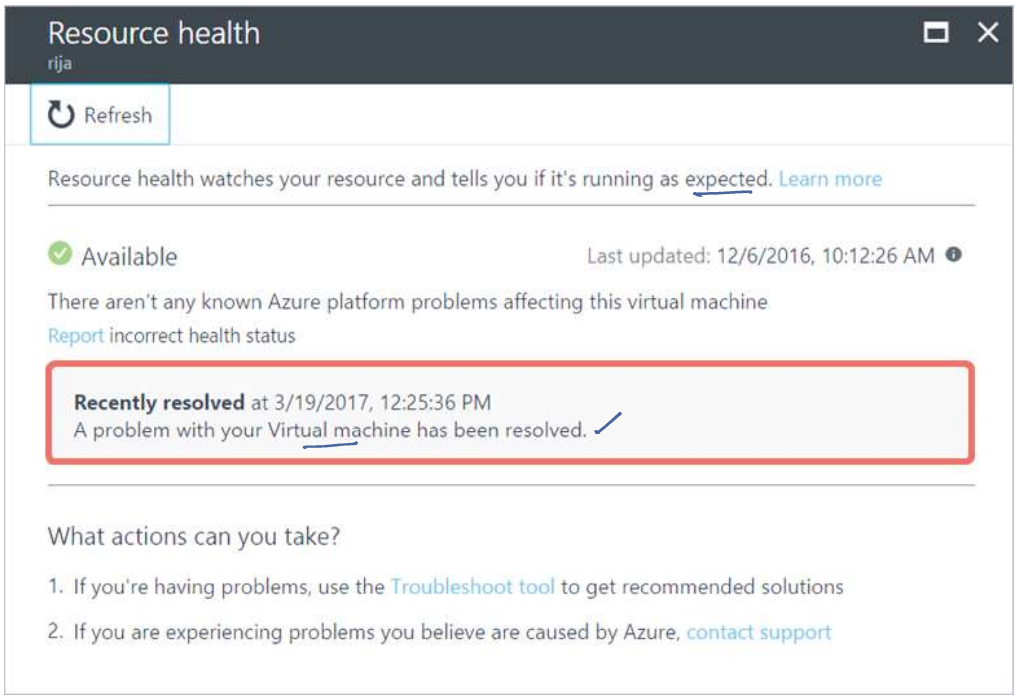
Resource Health

- Is a tailored view of your actual Azure resources.
- Using Azure Monitor, you can also configure alerts to notify you of availability changes to your cloud resources.

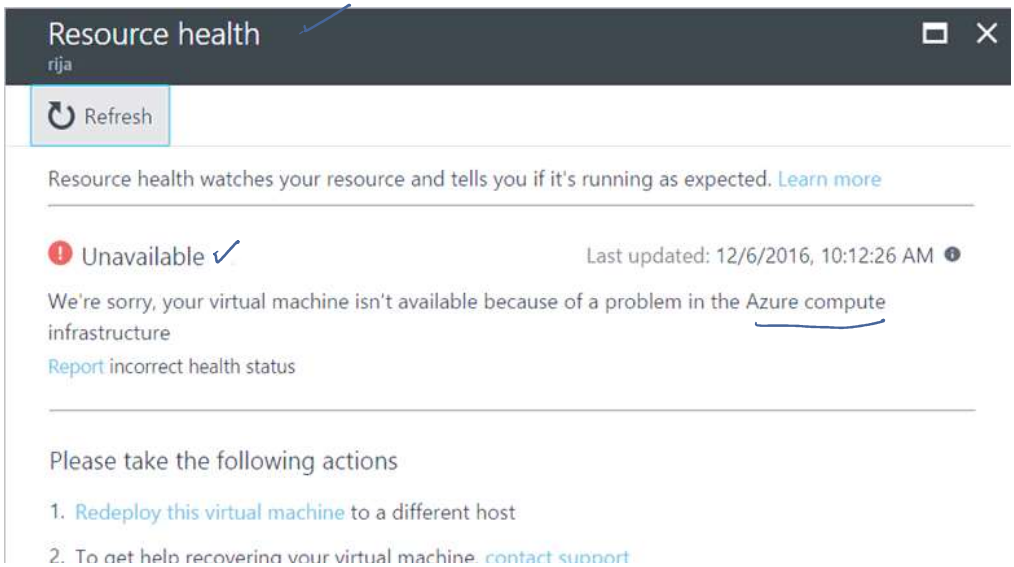


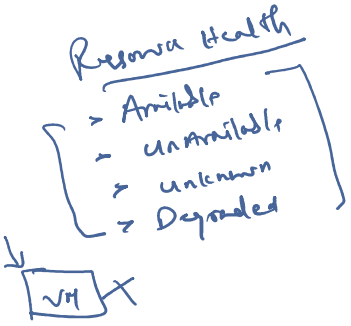
- By using Azure status, Service health, and Resource Health, Azure Service Health gives you a complete view of your Azure environment-all the way from the global status of Azure services and regions down to specific resources.
- Additionally, historical alerts are stored and accessible for later review.


Microsoft Azure
My account
Portal
Azure status
Updated 51 seconds ago
RSS
View other issues that might be impacting your services:
Go to Azure Service Health
HELPFUL LINKS
Azure status history
Get notified of outages that impact you
Building reliable applications on Azure
Refresh every
2 minutes
Good
Information
Warning
Critical
N/A
Current Impact
Americas
Europe
Asia Pacific
Middle East and Africa
Azure Government
Azure China
Products And Services
Non-Regional
East US
East US 2
Central US
North Central US
South Central US
West Central US
West US
West US 2
West US 3
Canada East
Canada Central
Brazil South
Brazil Southeast
COMPUTE
Azure VMware Solution by CloudSimple
Virtual Machines
SAP HANA on Azure Large Instances


Resource health
rija
Refresh
Resource health watches your resource and tells you if it's running as expected. Learn more
Available
Last updated: 12/6/2016, 10:12:26 AM
There aren't any known Azure platform problems affecting this virtual machine
Report incorrect health status
Recently resolved at 3/19/2017, 12:25:36 PM
A problem with your Virtual machine has been resolved.
What actions can you take?
1. If you're having problems, use the Troubleshoot tool to get recommended solutions
2. If you are experiencing problems you believe are caused by Azure, contact support


VM


Resource health
rija
Refresh
Resource health watches your resource and tells you if it's running as expected. Learn more
Unavailable
Last updated: 12/6/2016, 10:12:26 AM
We're sorry, your virtual machine isn't available because of a problem in the Azure compute infrastructure
Report incorrect health status
Please take the following actions
1. Redeploy this virtual machine to a different host
2. To get help recovering your virtual machine, contact support


Resource Health
= Available
= Unavailable
= Unknown
= Degraded
VM

Please take the following actions

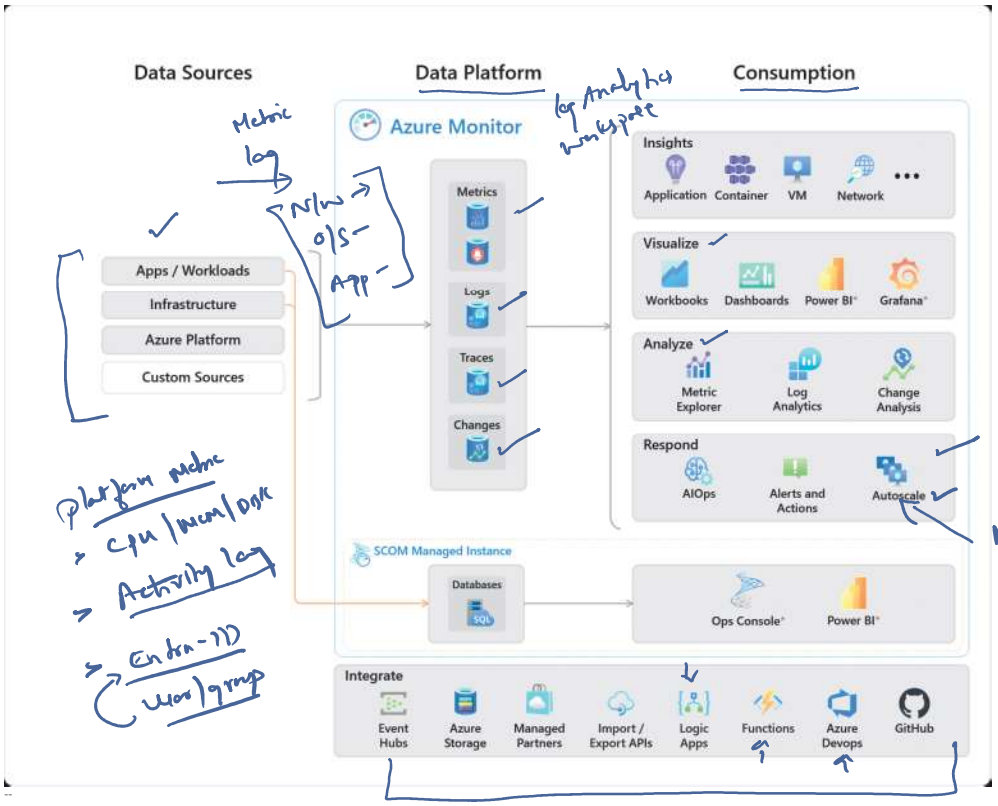
1. Redeploy this virtual machine to a different host
2. To get help recovering your virtual machine, contact support

Azure Monitor

Azure Monitor is a platform for collecting data on your resources, analyzing, visualizing and Taking actions on the alert.

Azure Monitor can monitor Azure resources, on-premises resources, and even multi-cloud resources.

The following diagram illustrates Azure Monitor



Azure Log Analytics

Azure Log Analytics is the tool where you'll write and run log queries on the data gathered by Azure Monitor.

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

You can write a simple query, use features of Log Analytics to sort, filter, and analyze the records.

You can write an advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend.

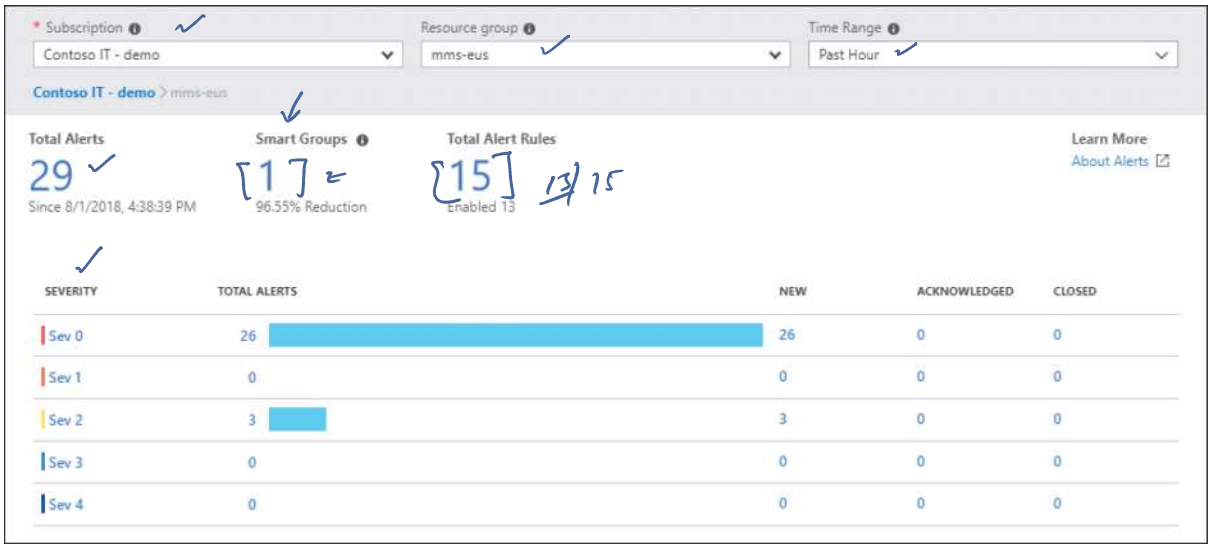
Azure Monitor Alerts

Azure Monitor Alerts are an automated way to stay informed when Azure Monitor detects a threshold being crossed.

You set the alert conditions, the notification actions, and then Azure Monitor Alerts notifies when an alert is triggered.

Depending on your configuration, Azure Monitor Alerts can also attempt corrective action.

an alert is triggered.
Depending on your configuration, Azure Monitor Alerts can also attempt corrective action.



Alerts can be set up to monitor the logs and trigger on certain log events

Azure Monitor, Service Health, and Azure Advisor all use actions groups to notify you when an alert has been triggered.

Application Insights

Application Insights, an Azure Monitor feature, monitors your web applications.
Application Insights is capable of monitoring applications that are running in Azure, on-premises, or in a different cloud environment.

There are two ways to configure Application Insights
Install an SDK in your application, or you can use the Application Insights agent.
agent is supported in C#.NET, VB.NET, Java, JavaScript, Node.js, and Python.

Monitor information, such as:

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates, to show whether external services are slowing down performance
- Page views and load performance reported by users' browsers
- AJAX calls from web pages, including rates, response times, and failure rates
- User and session counts
- Performance counters from Windows or Linux server machines, such as CPU, memory, and network usage

Benefits of Using the Cloud Services