MICROSOFT AZURE EXAM.

{AZ-900}

1) Describe Cloud Concepts.
2) Describe Azure Fundamentals, Architecture and Services.
3) Describe Azure Management and governance.

What is cloud?

→ Basically someone else's computer & not cloud.
→ A bunch of servers regulated and maintained by Amazon/google/Microsoft etc.
→ The ability to rent computing resources - on demand.

On Premises Server
Hosting Model.
Cloud Model
} Three ways.

What does "Computing Resources" mean?

→ Windows & Linux Servers.
→ Unlimited File Storage.
→ Databases
→ Queues.
→ Content Delivery Network.
→ Batch Processing Jobs

→ Big Data - Hadoop.
→ Media Services.
→ Machine Learning
→ Chat Bots
→ Cognitive Services.

Power of Azure? → How easy it is to get a Windows/Linux server and set it up according to my specification ~~so~~ & ~~that~~ two in such a less amount of time.

Exam (AZ-900) Requirement

→ Cloud Concepts
→ Azure Architecture & Services.
→ Azure Management & Governance.

Scanned with CamScanner

Shared Responsibilities

1) When you run services in your own office, you are responsible for:

- → Building security
- → Physical → Network Security
  → Computer security.
- → Operating System Patches.
- → Network and Firewall Settings
- → Application settings
- → Authentication Platform
- → User Accounts
- → Devices
- → Data.

2) When you run services in the cloud using a VM, you are responsible for →

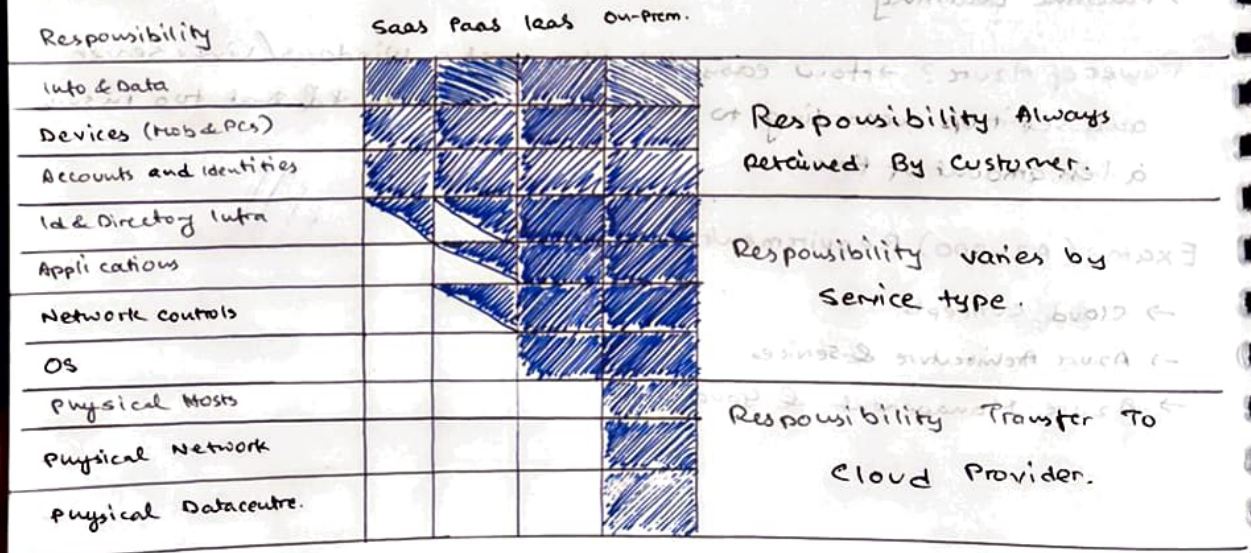
- → OS patches.
- → Network & Firewall Setting
- → Application settings
- → Authentication Platform
- → User Accounts.
- → Devices
- → Data.

*** (OS patches is not there), when we run services in the cloud using an App Service

3) When we use Software as a Service (SaaS), you are responsible for ⇒

- → Authentication Platform (shared)
- → User Accounts
- → Devices
- → Data

Model



Scanned with CamScanner

Public Cloud – "is defined as computing services offered by third party ~~provided~~ providers over the public Internet, making them available to anyone who wants to use or purchase them."

{ Azure owns the hardware, on their network and infrastructure. }

Private Cloud – "is defined as computing services offered either over the Internet or a private internal network and only to select users instead of a the general public."

My company owns the hardware and network. Looks and acts like a cloud except customer owns or leases or has exclusive access to the hardware.

Hybrid Cloud – is a computing enviornment that combines a private cloud with a public cloud, scales private infrastructure to the cloud.

Advantages :-

1) Control – your org can maintain ~~power~~ private infrastructure for sensitive assets or workload that require low latency.
2) Flexibility – you can take advantage of additional resources in the public cloud when you need them.
3) Cost Effectiveness – with the ability to scale to the public cloud, you pay for extra computing power only when needed.
4) Ease – transitioning to the cloud does not have to be overwhelming because you can migrate gradually – phasing in workloads over time.

Advantages :-

Public Cloud.

1) Lower Costs
2) No Maintenance
3) Near unlimited scalability
4) High Reliability.

Private Cloud.

1) More flexible
2) More control
3) More scalability.

Scanned with CamScanner

Cloud Pricing → can be complicated.

Usually any service is priced by 2/3 metrics combined.

Example: Cosmos DB.

Operations ⊕ $23.36+
Consumed storage ⊕ $25.00+
Optional Dedicated Gateway ⊕ $277.40 & +
Backup storage ⊕ $60.00 (7 day backup).

1) Free Services

1) Virtual Network
2) Private IP Address
3) Azure Migrate.
4) Inbound Internet Traffic.
5) 5GB of outbound Internet Traffic.
6) Azure Policy
7) Azure AD
8) 1 million executions of Azure functions.
9) Azure App Service

2) Pay for Time

1) Virtual Machine
2) App Services
3) Databases
4) Load Balancers
5) Managed storages
6) Public IP address.

A very common and logical way to pay for something. Some services charge by the minute or by the hour. Varies (greatly) based on the specific service you choose, performance, options, etc.

3) Pay per GB (gigabyte).

1) DB storage
2) Backups
3) Unmanaged Disks
4) Network Traffic (b/w regions)
5) Network Traffic (more than 5GB/month egress from Azure)

4) Pay for Operations

Each operation can also cost a fraction of a penny.

Scanned with CamScanner

1) Unmanaged storage (reads, writes, deletes)
2) Databases (queries)
3) Messaging.

} Usually charged in bulk, per 10,000 requests / per million requests etc

3) Pay for Execution

Some serverless offers just charge you for each time the program runs.

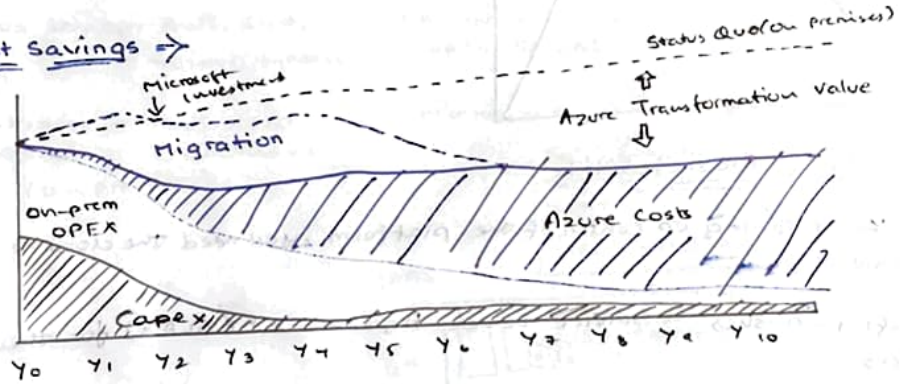
a) Azure Functions (consumption Model)
b) serverless DB
c) Messaging services
d) Logic Apps (consumption Model).

[Pricing changes between regions.]

Benefits of Cloud Computing :-

1) cost savings - both real & accounting.
2) Availability and scalability.
3) Reliability and predictability.
4) security and governance.
5) Manageability
6) Global Reach.
7) Range of ready-on-demand services
8) Range of tools.

Cost savings =>



REAL

1) Economies of scale
2) Total Cost of Ownership (TCO) → Electricity, Internet, Cooling, Employees
3) Microsoft can run a server cheaper than anyone else with a few exceptions
4) vCPU server - as low as $187/mo.
5) You can take actions to reduce your costs {i.e Auto scaling.}

Scanned with CamScanner

High Availability

It is expressed as a percentage, its the ability of a system to respond to users.

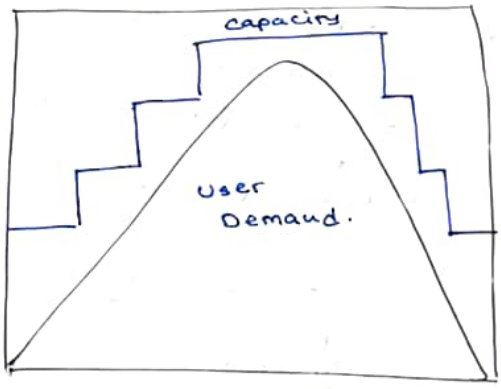
99.99% → 4 mins a month (Downtime).
(Efficiency)

Why not 100% uptime?

It is very difficult to acheive. Even Multi global companies cant do it.

Elasticity

The ability of a system to automatically grow and shrink based upon application demand.



Reliability & Predictability

Since you're giving up control of the platform, you need the cloud to be reliable.

→ Microsoft publishes "Service Level Agreement" (SLA's) for their services.
→ Financial guarantee of their performance. (Refund if Microsoft cant keep their words).
→ Azure has established procedures for rollouts and regional recovery.

{Availabitity sets and Zones}

→ Give you the tools for backup & site recovery.
→ Simulate failures using Chaos Studio.

Scanned with CamScanner

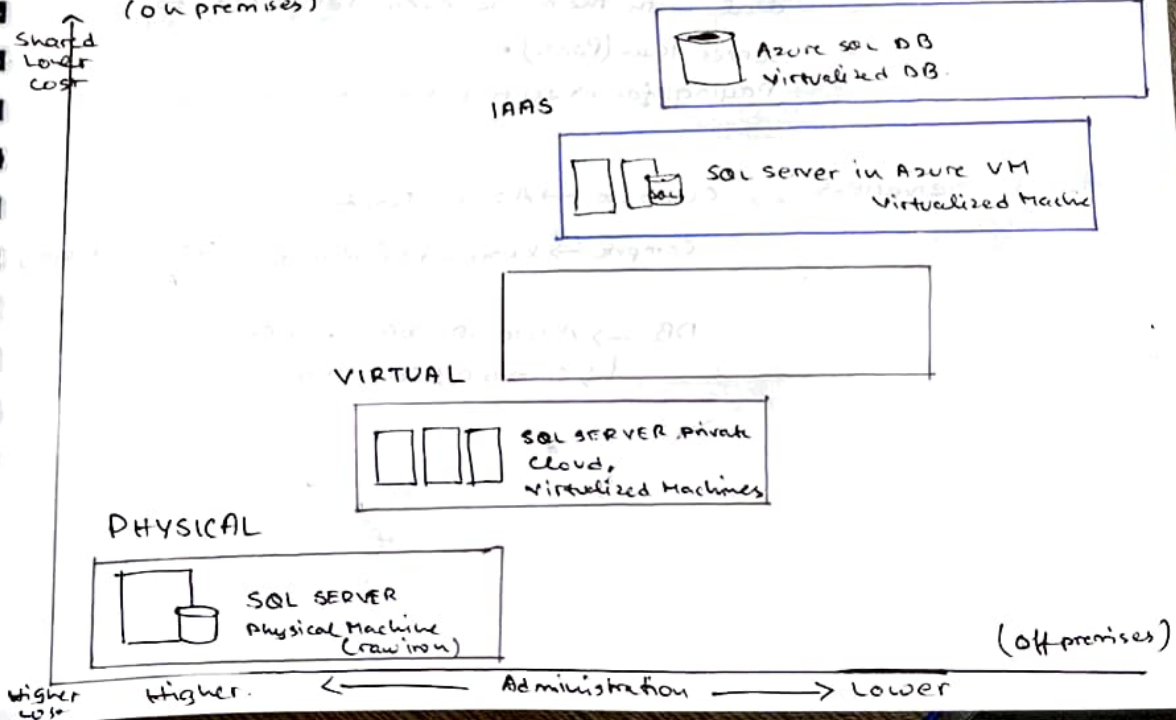
Global Reach -> Its not possible for most businesses to run data centers in multiple countries.

Cloud Services Type:-

There are three types of cloud services =>

1) Iaas 2) Paas 3) saas

Basis of	IAAS	PAAS	SAAS
1) Stands for -	Infrastructure as a service	Platform as a Services	Software as a services
2) uses -	IAAS is used by Network Architects	PAAS is used by Developer	SAAS is used by end user.
3) Access -	IAAS gives access to the resources like VM & Virtual Storage	PAAS gives access to run time environment to deployment & developers tools for application	SAAS gives access to the end user.
4) Model -	It is a service model that provide visualized computing resources over Internet.	It is a cloud computing model that delivers tools that is used for development of application.	It is a service model in cloud computing that host software make available for client.
5) Cloud Services -	AWS, SUN, VCLOUD EXPPESS	FACEBOOK, GOOGLE SEARCH ENGINE	MS OFFICE WEB, GOOGLE APPS, F B.
6) Enterprise Services -	AWS Virtual private cloud (on premises)	Microsoft Azure	IBM cloud Analysis



Scanned with CamScanner

Infrastructure-as-a-Service (IaaS) — is a type of cloud computing service that offers essential compute, storage and networking resources on demand, on a pay-as-you-go basis.

VM, Networking, Load Balancer, Firewall.

Platform-as-a-Service (Paas) — is a complete developement and deployment enviornment in the cloud. Paas includes infrastructure, —servers, storage & networking. But also middle ware, developemant tools, business intelligence services (BI), DBMS & more.

Paas is designed to support the complete web ~~de~~ application life cycle: building, testing, deploying, managing & updating.

→ Upload code packages & have them run, without access to the hardware.

Software-as-a-Service (saas) — allows user to connect to & use ~~all~~ cloud-based apps over the Internet.
eg:- Email / Calender / Microsoft office 365.
(Access to configuration only.)

Serverless → There are still servers, you just dont ever have to deal with them. So even less access to server than (Paas).
Paying for execution & not how it works.

Azure Serverless Offers → Compute → Azure Functions
Compute → Kubernetes (Serverless) (Virtual Nodes w/ ACI)
DB → Azure SQL DB serverless
↳ Cosmos DB Serverless

Scanned with CamScanner

CORE ARCHITECTURAL COMPONENTS OF AZURE

1) **Regions** – geographical areas where microsoft azure has servers. (60+) It is not accessible for everyone.

Microsoft Azure has the largest cover of servers.

Region - Pairs – Each region has another region which is treated as its "pair"

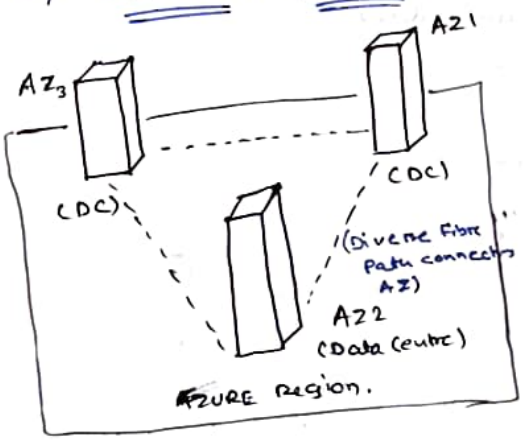
→ Almost always in the same geography – data storage laws
→ The data connection b/w pairs (region) is the highest speed available.
→ Software rollouts are deployed to one region of a pair & the other is not touched.
→ If multiple regions go down, one region of each pair is treated as a priority.

Canada	canada Central - Canada East
Europe	North Europe - west Europe.
USA	East US - West US
USA	East US 2 - central US
USA	North Central US - South Central US
Brazil	Brazil South - South Central US

Sovereign Regions

Azure Government (US)
China

2) **Availability Zone**



Physical separation of servers into multiple places so that if one goes down, the rest is still working.

→ Reduces Risk

Americas

Brazil South
canada central - East
Central US - East US - East US 2
SC US - West US 2 - West US
US Gov Virginia

Europe

France Central
Germany West Central
N Europe
Norway West
UK South
West Europe
Sweden Central.

Scanned with CamScanner

Asia Pacific

Australia East
Central ~~East~~ INDIA
Japan East
Korea Central
SE Asia - E Asia
China North (3).

Africa

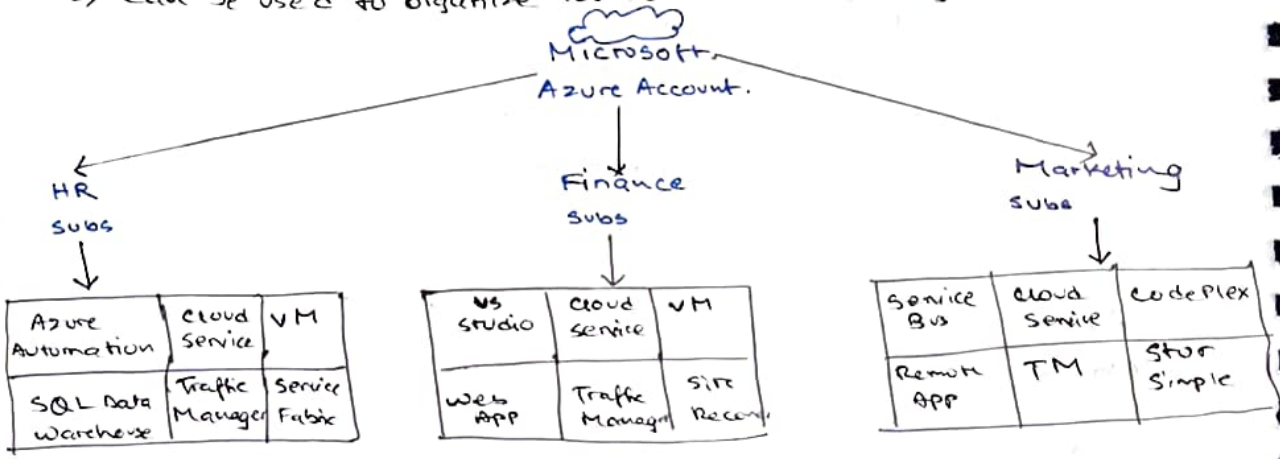
South Africa North

Data Centre ⇒ is a unique physical building that contains thousands of physical servers with its own power / cooling & networking infrastructure.

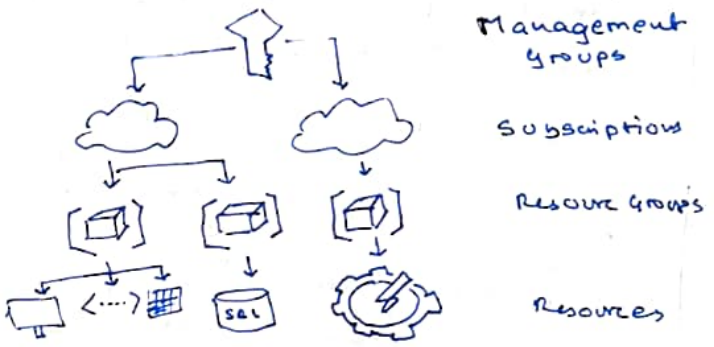
Resource Groups – is a container that holds related resources for an Azure solution. Includes resources that you want to manage as a group.

Azure Subscription – Subscription is a billing unit. It's better to be having multiple subscription according to clients.

→ Users have access to one/more subscriptions, with different roles.
→ All resources consumed by a subscription will be billed to the owner.
→ Can be used to organize resources into completely distinct accounts



For multiple subscriptions, nesting can be done.



Scanned with CamScanner

AZURE COMPUTE AND NETWORKING

Compute Services → executing code in the cloud.

1) Virtual Machines (VM) — is the virtualization/emulation of a computer system. VM's are based on computer architectures & provide functionality of a physical computer.

2) Virtual Machine Scale Sets (VMSS) — provide the management capabilities for applications that run across many VM's, automatic scaling of resources & load balancing of traffic.

3) App Services (web apps)

4) Azure Container Instances (ACI) — is a managed service that allows you to run containers directly on the Microsoft Azure public cloud, without requiring the use of VM's.

5) Azure Kubernetes Services (AKS) — is a managed container orchestration service based on the open source Kubernetes system, which is available on the Microsoft Azure public cloud.

6) Windows Virtual Desktop

Virtual Machine → (Iaas)

1) Take an existing machine from your ~~XXX~~ enviornment into the cloud - a copy.
2) A "slice" of physical machine shared with other customers
3) Full control over it, as if it was your machine.

[VM Types → Over 200 to choose from] → No of CPU cores, CPU speed, RAM size, IOPS } Predefined

VM Scale Set → (Elasticity).

1) Two/more VM running the same code.
2) with a "load balancer" in front to direct traffic randomly to one of the machines.
3) Autoscaling → ability to add/remove machine depending on demand.
4) Can handle upto 100 VMs in a single scale set.
   ↳ can be increased to 1000 VMs.

Scanned with CamScanner

(PaaS) → Give your code & config to Azure & they will
→ Promise of performance / No access to hardware

Containers → → Another paradigm for running code in the cloud.
→ container contains everything the app needs to run in a "container image".
→ Fastest & Easy to Deploy.

ACI – single instance, quickest way to deploy a container.

AKS – runs on a cluster of servers, enterprise grade.

Azure Virtual Desktops → → Desktop version of windows that runs in the cloud.
→ Can even see your desktops on iOS & Android or from any web browser

Networking Services → 1) Virtual Network 4) Express Route.
2) VPN Gateway
3) VNet Peering

In AWS, a Virtual Network is called Virtual Private Cloud. (VPC)

Types of Networking Services → 1) Connectivity Services 4) Monitoring services.
2) Protection services
3) Delivery Services

1) Connectivity services →

a) Virtual Networks – emulating a physical network. Microsoft global Network already exists, so a virtual Network is just a software configuration.

b) subnet – a subdivison of virtual networks that you control, that has its own security rules.

c) Virtual Private Network (VPN) – connecting two networks as if they were on the same network, uses a Network gateway.

d) Express Route – high speed private connection to AZURE.

e) DNS services – domain name resolution.
(Phonebook) (Hostitin Azure)

Scanned with CamScanner

2) Protection Services —

a) DDOS Protection — Distributive Denial of service

b) Azure Firewall

c) Network Security Groups

d) Private Link.

3) Delivery Services — (Not in Exam).

a) Load Balancer – distribute traffic evenly b/w multiple backend servers.

b) Application Gateway – a higher level of load balancer with an optional firewal.

c) Content Delivery Network (CDN) – stores common static files on the edge, closer to the user for (perceived) improved performance

d) Azure Front Door Service – a load balancer, CDN & firewall all-in-one.

4) Monitoring Services —

a) Network Watcher

b) ExpressRoute Monitor.

c) Azure Monitor.

AZURE STORAGE

1) Container (Blob) Storage.

2) Disk Storage

3) File Storage

4) Storage Tiers.

{ Storage – one of the foundational technologies on which much is built. }

The Azure Storage account:-

→ General Purpose v2 (gpv2) is the most common type

Blobs, Tables*, Queue*, Files.

=> AZURE DATA LAKE STORAGE (GEN 2)

Cheapest type of Storage. Pay/GB (~1.8 cents per GB).

Scanned with CamScanner

App Services

1) BLOB is an "acronym" for Binary Large OBject. A collection of binary data could be in the form of a file (stored in a storage account) or data stored in a DB.

In AWS, a storage account is called SW3 service.

Many Options for Storage Accounts =>

a) Access tiers → Hot / Cool / Archive.

b) Performance tier → standard / Premium.

c) Location → Geographical

d) Redundancy / Replication → Replication of files in multiple locations.

e) Failover options → when one DC fails, the backup that we have in Azure can be used as primary storage account. This is called "Failover"

2) Disk storage

a) Azure Virtual Machine Disks

b) Managed Disks – stores C Drive of a Virtual Machine.

c) Reserve capacity in Advance.

d) Optimized to virtual hard disks

Storage Account → Create Resource group → Give unique name.

Select → Region
→ Performance → Standard / Premium → Page Blob / Block Blobs.
→ Redundancy.
↓
Zone Redundancy Storage (Multiple DC) → Locally Redundancy storage. (1 DC)

Access Tier → Hot (Default) - Day to Day Scenario (frequent data access)
Cool :- save money on storage, pay more when update.
(cost storage price in half.)
Archive - putting files in a storage where its difficult to access. (→ Only 10% money required)

Even the storage Account is public access, still it requires a key to get in.

Scanned with CamScanner

Immutability of files → a file cannot be changed or deleted.

Types of Storage → Containers (Blob) (For exam).
File Shares
Queues
Tables.

Keys to Storage Account should be kept private at all costs.

We need a shared Access key to access the storage of someone else. (→ Click ... on the file → Generate SAS → Share it for file Access).

Q How Azure manages file storage automatically ?

Azure manages automatic file storage & storage update by "Life Cycle Management" in order to change the Access tier of a storage from HOT → COLD → ARCHIVE. This change happens depending on some rules.

Azure Storage should be manipulated by functions or codes, to listen for some events etc or by using Azure Storage Explorer / Azure Storage Browser (Online).

Azure Storage Explore → manipulate storage here, it runs on the local machine & not on the Browser.

AZURE IDENTITY, ACCESS AND SECURITY.

Identity - In computing "Identity" is a representation of a person, application or device.

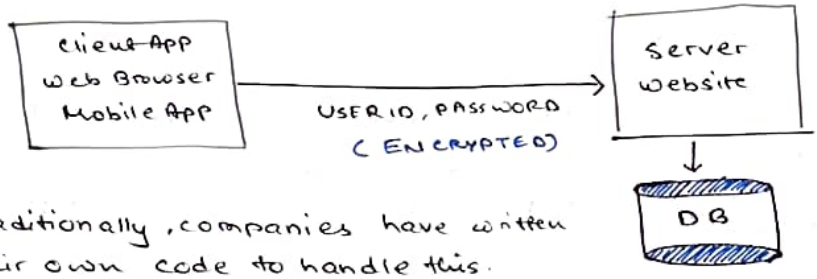
eg:- John Henry Doe
johndoe@example.com
Monthly Payroll Application

Usually requires a password, a secret key or a certificate to prove.
Many to apps require you to login to use some of its functionality.

How its handled ?

Scanned with CamScanner

Client-Server Model



Traditionally, companies have written their own code to handle this.

So if there is no one universal way to access the website, then there might be several bugs introduced by different people.

Some of the more famous "hacks" have been ~~cracked~~ on custom created identity system.

Hash

→ Some companies were storing the password in "plain text"
→ " " " using a simple, reversible hash algorithm (MD5)
→ some companies were storing the "salt" along ~~the~~ with the data.
→ Not enforcing password change policies
" " " complexity analysis

Azure provides an identity management system based on their popular "Active Directory"
↳ this checks our password whenever we login somewhere/anywhere.

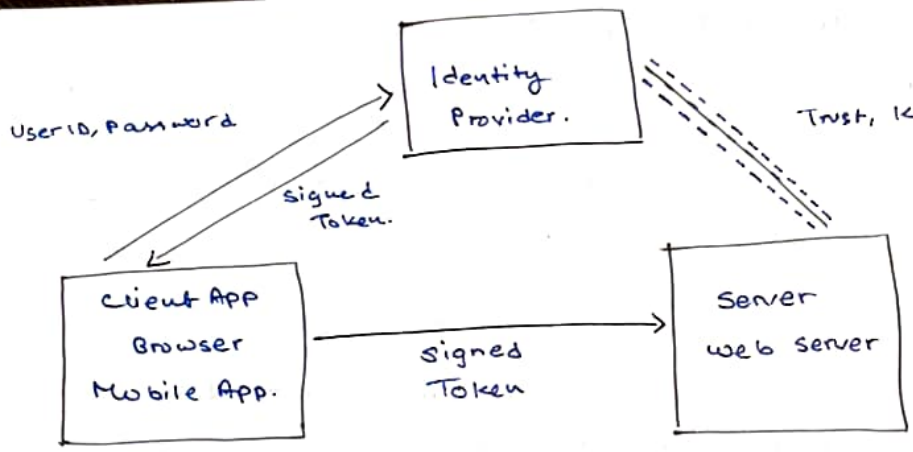
Azure Active Directory is not the same as Active Directory.

→ Traditional AD does not work with Internet protocols.

~~AZURE~~ AZURE AD provides "Identity as a Service"

Benefit? → Instead of having to write code to handle users, passwords, resets etc

Scanned with CamScanner



[AZURE ACTIVE DIRECTORY MODEL.]

Benefits of Azure AD :-

1) Security – Reduced development time, easier support.
Reduces bugs in gateway code.
Dev dont have to worry about id&pass.

2) Features – tons of them.
a) Access Review → review user's permission

3) Centralized Administration → useful when my company has 1000's apps & all needs Admins.

4) ~~One~~ Single Sign On → Only one user ID & password.

5) Integration with other Azure services → Different teams can act together.

Authentication

a) Authentication is a user proving who they are - user id & password.

b) Move away from all authenticated users having admin cases.

Authorization

a) Authorization is ensuring that a user is ~~perto~~ permitted to perform an action or not.

b)

Conditional Access.

{ When users outside the company hack / find an admin credentials. }
↳ this will trigger an ~~as~~ unusual event.

eg 1) "User A" attempts to login to the app from within the company office, as she does everyday.

2) "User B" attempts to login to the app for the 1st time in 4 months.

Scanned with CamScanner

3) Admin C attempts to login to the app from their phone.
" D " " " " " from 1020 miles away.

You can treat some access attempts as "routine" & some "not normal".

Azure AD combines all three parameters of SIGNAL, DECISION & ENFORCEMENT in order to determine how to categorize an attempt to access

DECISION → Allow full access
" → Limited "
" → Remediate Access.
" → Block Access

(MFA / 2FA)
Multifactor Authentication → Require 2 / more pieces of evidence (factors) in order to login.

Three Factors → Something you know - (password)
→ Something you have - (mobile with email account)
→ Something you are - (fingerprint).

→ Your unique password could be 1 piece of evidence
→ But a second piece of ~~code~~ evidence is required - a unique, time limited code sent to you.
AZURE provides :-
→ SMS / EMAIL / AUTHENTICATOR APP / PHONE CALL.

Passwordless → gestures to sign in → Face
↳ Patten
↳ Finger Print
→ High security
→ convenient.

How is a pattern lock more secure than a password?
→ Because its restricted to device.
→ Can't be used outside my country.
→ Can't be used without the device.

Signin using a ~~VPN~~ PIN or biometric recognition (facial / iris / fingerprint) with windows devices.

Scanned with CamScanner

Role Based Access Control (RBAC) ⇒ Microsoft's preferred

→ solution for access control.
→ Create roles that represent the common tasks of the job.

Accountant, Developer, Manager, HR] Diff roles have different access requirements

→ Assign granular permission to that role / every role
→ Assign users to that role.
→ Do not assign granular permissions to an individual.

Reader
Contributer
Owner.
} Types of permission in Azure.

ZERO TRUST METHODOLOGY ⇒ says dont trust each other to apps.

⚠ Dont trust everything behind the firewall is safe.

Principles →
1) Verify explicitly → use every available method to validate identity & authorization.
2) Use least privileged access.
3) Assume breach

Concepts → Just-In-Time (JIT)] - when admin control is used in emerg
Just-Enough-Access (JEA)] admin is granted control for some time.

Security even inside the network → encryption, segmentation & threat detection.

eg → Multi try to access an account, the account gets locked for 24hrs.

1) Identity → verify & secure each identity
2) Devices → ensure compliance & health status.
3) Applications → appropriate in-app permissions, monitor user actions
4) Data → data driven protection, encrypt & restrict access.
5) Infrastructure → more robust monitoring to detect attacks, block & flag risky behavior.

Scanned with CamScanner

Defense in Depth → dont rely on a single tool/security to protect you.

Depth comes from all the layers of security that you can apply.

1) Data – virtual Network endpoint
2) Application – API Management
3) Compute – i.e Limit Remote Desktop Access, Windows Update.
4) Network – ie. NSG, use of subnets, deny by default.
5) Perimeter – i.e DDOS, Firewalls.
6) Identity & Access – i.e Azure AD.
7) Physical – i.e Door locks & key cards.

Identity & Access	Apps & Data security	Network security	Threat Protection	Security Management.
Role based Access	Encryption	DDOS Protection	Antimalware	Log Management
MFA	Confidential computing	NG Firewall	AI based detection & response	Security Posture Assessment
Cental Identity Management	key Management	web APP Firewall	cloud workload protection	Policy & Governance
Identity Protection	Certificate MGMT	Private connect	SQL Threat protection	Regulatory Compliance
Priviledged Identity Management	Info protection	Network segmentation	IOT Security	SIEM

(#) Missed ⇒ Microsoft Defender.

Cost Management (in Azure).

Factors that Affect cost →

1) Different Services are billed based on different factors.

FREE SERVICES → Free tier web apps

- → Resource Group
- → Virtual Network
- → Load Balancer
- → Azure Active Directory
- → Network Security Groups

Scanned with CamScanner

Pay per Usage Model → depends on usage models.

Opportunity for Cost savings → Azure functions :-

1) 1 million executions free per month.
2) $0.20 million executions.
3) cheapest Virtual Machine is $20/month.

Pay per Usage Service → a) Functions
b) Logic Apps
c) Storage
d) outbound Bandwidth.
e) Cognitive services API.

Pay for Time (Per second) billing means billing stops when the VM stops

Stability in Pricing → Pay a fixed price per month for computing power or storage capacity, whether you use it or not.
→ Discounts for 1/3 yr commitment in VM.
→ Multi tenant / Isolated Environment.

Pay / Bandwidth costs → 5GB data is free.
Inbound data is free.
Outbound data price chart → 0.05 $ to $0.0575/GB for zone 1
$0.08 to $0.12/GB for zone 2
$0.16 to $0.18/GB for zone 3.

1 PB of Data transfer = $52,000 for download.

AZURE Pricing Calculator. → Estimates are hard to make 100% accurate

Config options → 1) Region
2) Tier
3) Subscription Type
4) Support options
5) Dev/Test Pricing.

→ Export & share the Estimate

Total Cost of ownership (TCO) Calculator → Costs other than hardware

Other costs → 1) Electricity
2) Cooling.
3) Internet connectivity
4) Rack space.
5) setup Labor
6) Maintenance Labor
7) Backup.

Azure Cost Management → Another free tool inside Azure to analyze spending.
2) Analyze spending over time (Forecasting).
3) Tracking against budgets (notifies when charges go over budget).
4) All your past invoices.
5) Schedulere reports

Scanned with CamScanner

Resource Tag → allows us to tag meta data to our code/resources.
→ Helps with billing & support issues.

Tags are (Name – Value) pair.

AZURE Governance and Compliance → The leaders are your company might have certain IT rules that they want to implement.

Q1) Send an email with the rules & assume everyone reads it & remembers it.

Q2) Use Azure tools to enforce the rules (or simply audit compliance).

Q3) Several tools in Azure to support Governance & Compliance

- → Azure Blueprint → Service Trust Portal.
- → Azure Policy
- → Resource Locks

Azure Blueprints

→ Azure Subscription templates with roles and policies already defined.

Azure Policy → Create rules across all of your Azure resources.
Evaluate compliance to those rules. (If no backup is taken).

Ex of BUILT IN POLICIES :-

1) Require SQL server 12.0
2) Allowed Storage Account SKU's
3) Allowed Locations
3) Allowed Virtual Machines SKUs
4) Apply tag & its default value.
5) Not allowed resource type.

Can create custom policies using JSON definition.

Locks → Read Only resource (can not Delete)
↳(LOCK)

We can add a DeleteLock to VM.
{Using RBAC, you can restrict who has access to locks.}

//service trust.
// aka.ms.stp.

Scanned with CamScanner

AZURE PORTAL AND COMMAND LINE →

1) AZURE PORTAL → to manage Azure Resources forever.
Powershell/CLI command line → Scripting Language. if we don't use Azure Portal.

Cloudshell.azure.com → From here we can go to CLI / Powershell.

{CLI command}

az group create --name newrg --location eastus

- az group create → creating a resource group.
- --name newrg → naming the resource group.
- --location eastus → providing the location of resource group.

az vm create --resource-group newrg --name newvm --image win2019Datacenter --public-ip-sku Standard --admin-username [redacted]

→ Admin Password:
Confirm Admin Password:

az vm open-port --port 80 --resource-group newrg --name newvm.

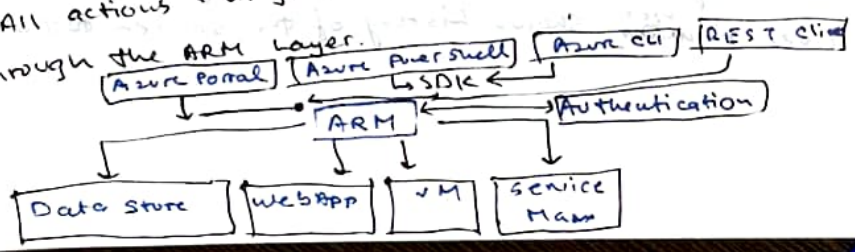
az group delete --name newrg.

2) AZURE ARC → allows us to see & run all resources/infra-structures in our premises regardless of where it is running. (eg:- other cloud like AWS or other premises).

We can add a Kubernetes cluster with Azure Arc.

Azure Stack HCI.

3) ARM (Azure Resource Manager) Template → The deployment & management service of Azure. Management Layer that allows you to create, update & delete resources called "deployments".
All actions that you take to manage your Azure resource goes through the ARM Layer.



Scanned with CamScanner

```
"resources": [
  {
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2019-06-01",
    "name": "[parameters('storageAccountName')]",
    "location": "[parameters('location')]",
    "sku": {
      "name": "Standard_LRS",
      "tier": "Standard"
    },
    "kind": "StorageV2",
    "properties": {
      "accessTier": "Hot"
    }
  },

"resources": [
  {
    "type": "blobServices/containers",
    "apiVersion": "2019-06-01",
    "name": "[concat('default/', parameters('containerName'))]",
    "dependsOn": [
      "[parameters('storageAccountName')]"
    ]
```

creating resource using ARM Template.

ARM takes all parameters and change it into JSON format.

MONITORING TOOLS

1) AZURE ADVISOR - reccomends based on certain patterns.
   - → Analyzes performances of apps.
   - → Analyzes ports for any to be open (security).
   - → Analyzes & recomends to keep your AZ running.

2) AZURE SERVICE HEALTH - alerts the user of any problems regarding any service issue from any data centre in any server of user shows history of the server to the user.

AZURE MON

AZURE DIA

platform
& one of

1) Storage
2) Storage

Scanned with CamScanner

AZURE MONITOR → shows all my resources at one place.

AZURE DIAGNOSTICS → specifies a list of categories of platform logs &/or metrics that you want to collect from a resource & one or more destinations that you would stream them to.

1) StorageRead
2) storage Write
3) storage Delete.

Scanned with CamScanner