Cloud Computing

→ virtualization : virtualizes physical hardware
↳ layer sits on the lowest level

Lecture - 1

→ when building a data centre, the first thing to do is the arrangement of networking b/w the servers / PC's.

→ Based on following
• compute • Networking • Storage

virtual machines → allows you to compact resources and use in a much better way.

→ Private cloud

• when database is created 2 files are created (~~saved on differ~~)
• data files • log files.

SQL server listens on port 1433. On high-level, the user is connecting to a Windo server service that accepts connections.

• HCI (Hyper converge Infrastructure)
↳ easily manage everything within your premesis..
• Owner of the hardware is responsible for everything.

→ Public Cloud

↳

- Database server highly depends on I/O. Critical part is disk.
- Web server do not use CPU much.
  ↳ some software is running that accepts request from Web.

Lecture - 2

→ Public cloud
- First, resources were available but not the reso services.
- To use services, the public cloud is invented.
- virtualization provides it's own interface to services.
- IIS to run Web server applications on Windows, Linux.

→ Hybrid cloud
  ↳ Private + Public

→ Even after the virtual machine is shut down, it still has storage allocated to it.

→ Buying a phone: capital expenditure (CapEx)
monthly bill : operational expenditure (OpEx)

→ Consumption based Model:
- You pay for what you use

→ GUI was missing.

→ The scripting language used under/behind the Windows is "powershell". First, the "powershell" is created and then the GUI.

→ The CPU is used very at minimum level. It gets minimal requests causing it to remain idle and use storage un-necessary. To handle this, virtualization was introduced/used (VMware).

→ Scalability is built-in.

→ SLA → Service Level Agreement

* IAC → Infrastructure As Code

- Database is made highly available by using clustering.

→ Public IP: accessible directly.
→ Dont assign public IP to virtual machine (one of the policies)
→ Governance: rights/responsibilities to make sure that everything is running smoothly & properly.
→ Reliability (part of SLA)
↳ when you get extremely / worst conditions or attacks, it is used.

→ Cloud Service Types
- IaaS (Infrastructure)
- PaaS (Platform)
  - You never touch virtual machine, you just use/get the services.
  - You never have to update anything.
  - We do nt have to worry about anything.
  - Dont have to focus on infrastructure.

Lift & Shift: Take virtual machine, copy it to the cloud & use it.

Lecture - 3

→ PaaS → not concerned with managing data center.
- responsible for configuring the application.
- everything is done by cloud vendor

→ Software as a Service (SaaS)
e.g Gmail
- You dont touch anything, you just use services.

→ PaaS shared responsibility (Network Controls) → allows you to control how the networking environment should work or who is allowed to access it or enter it.

→ move the databas to PaaS servers and code to web app (migration)

→ IaaS: More the flexible, more the headache as you have to do everything like update etc. It is not positive but you can use it in case of lift & shift etc.

Function Pointer → allows to invoke a specific action / function when the specified event is performed in the location

Disaster Recovery (DR)

→ Starting point of cloud environment
↳ Regions
↳ collection of data centres
↳ data centres are close enough to provide high availability.
↳ A region can be a city, country, state etc.

, Data centeres in regions are called availability

usually

- A region can have upto 3 data centres.

→ Region Pairs

If this region fails who will pick up the world. For example R1 & R2 are pairs, then if R1 fails. R2 will pickup the responsibilities of R1. it prioritizes R1, infront of other regions.

→ Everything in Azure (create/use) is a resource. Some are free, some are paid.

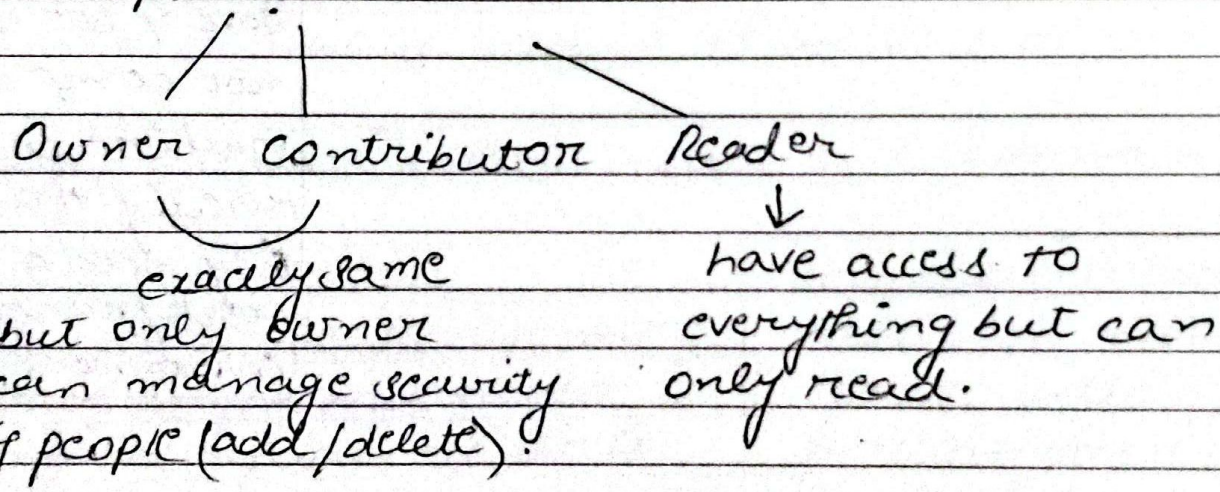
Java & Dot Net do not compile to machine code directly that's why they need a framework/runtime environment.

imp

Lecture-4

→ Resource Group
- ↳ putting resources together in 1 place (box/ container)
- ↳ A thing cannot exist in 2 resources at ~~one ti~~ the same time.
- ↳ Everything you create must go in resource group.
- ↳ Resource Group cannot be nested.

→ Subscription Roles



- Generally, 2-3 owner
- The internal owner (administrator/someone who starts subscription) cannot be removed by another owner.
- Subscription on resource group allows the person to manage it ~~oo~~ on it's own ~~except~~ ~~fo~~ of rather than contacting higher authority to do that for that person.
- Subscriptions come in/located in management groups.
- If the admin of management group is owner

Monday: Quiz

then he will serve as an owner for all the things underneath "management group".

- You can nest management groups but not subscriptions.

Azure compute services

↓

providing computing services e.g virtual machines.

- In IIS, you get full access

~~IAAS~~ (chfrm)

→ virtual machines

↳ can be done by using 'HyperV' in the machines

↓

created/used.

- only critical pieces of hardware can be used in virtual machines.
- To come in VM, some public address is required for the traffic your

→ Azure Hybrid Benefit

Microsoft

In infrastructor, to distribute the load, load balancer is used (to handle multiple requests (VM's))

VM Scale Sets

- ~~Allows~~ Starting the VM on the conditions specified by user
- automate the on-premesis thing (scale)
- can scale up/scale down
- max/min instances.
- problem: we dont have functionality to scale automatically

VM availability sets

- Each data centre must have 3 sources of power.
- divided data-centres in 3 parts.
- Each have seperate power, pooling, networking.
- Each data centre is essentially an availability zone.

→ Fault ~~Zone~~ Domain. → physical (→ 3 set of racks - 3 fault domains.)

~~Servers that have it's own~~ ... / Group of racks which have seperate source of power, pooling, networking that can independently act as data centers.

- machine scale set consists of all functionality of availability sets but not vice versa.
- VM cannot be created across regions.
- while creating VM. if it is not put in availability sets: then it cannot be moved to it after the creation of VM.
- Method of placing VM's in seperate racks.
- Availabity zones & availability sets are independent of each other.

→ update Domains → conceptual thing (→ app doesn't go down (benefit))

(when VM's are getting updated)

mapped/configured in a software.

restricted by 3.

Remote desktop : to log-in remotely
IP address of own PC : 127.0.0.1
Network service → IP & Port

Lecture-5

→ Virtual Desktop

Security Problem : Remotely login to go to VM (need IP address)
↳ usage of public IP address to login can lead to hacking & more worst case scenarios concerning security.
↳ coming from outside the network to manage datacenters.

Windows client → only 1 session
Window Server → allow multiple session

→ Connection Broker : Will make a session and gives access to the user.

FTP → binary protocol (encryption)

• Protocol (RDP) → works on 3389.
↳ gives you a virtual connection is data centre, meaning they can go anywhere.

Server → accepting connection → dividing for load balancing

• Gives Protocol translation also.
• Charges every person for this.

IaaS → session host
SaaS → unpaid - manages connections

• RDP in cloud is called AVD (Azure Virtual Desktop)
• If a member/purchaser of MS 365 then the AVD is free.
• Servers are infrastructure of AVD.
• The machine (server) at which you create session is called session host
• IntraID → cloud based authentication service. gives a simple but strong security layer.

Lecture-6:

→ AZURE Virtual Desktop (AVD) → how it uses compute

- Windows 10/11 allows multi-session.
- Risk of Resources being left behind:
  Log in to the session host. Once logged-in, you are sitting on the data-centre. If you close your session, nothing will be lost as every compute/code/anything will be done in the machine in the data-center.

→ Azure Container Services.

- We are telling the application that it is being used/installed on OS.
- Motivation/Problem:
  How can I have multiple applications running in the same OS independently without touching anything?
- You cannot touch/modify OS but you can get services.
- Container Image is created where it contains all required things like Web server, Python, Node.js etc.

★ Technical Part of containers:
- You can touch only containers
- Have 2 file system: Your own & container file system.
- Creates a union, so it feels its installed in OS but actually it is in the container.
- Everything/changes are done in the container.

To enable virtual machines, virtualization is needed.

↳ Runtime for VM : HyperVM, VMware
↳ ACI : Azure Container Instances.
↳ underneath is a VM
↳ AKS : Azure kubernetes file.

Containers → another way/level of compacting.
• Docker Containers
↳ Runtime : to run containers
company that owns container

• Difference b/w ACI & VM
• In containers, only thing you specify is the OS. For web app, you need webserver, runtime, dependencies, server features etc.
→ and size of the compute

→ What happens in if app crashes bez if that happens container also crashes?
• Google was the first one to enable a feature which can monitor containers known as Kubernetes Service. → config file/container.
• Scale Set is a configuration container. VM has no configuration
• If you want something, tell me all the requirements to manage it in the deployement/yaml/AKS file.
• Orchastrate the life cycle of container. defined in yaml file (AKS)

→ Azure Functions
Problem : Sometimes you wants to execute some piece of code, you dont want a VM/container to be created or you dont want to purchase anything.

- Serverless → I am not paying for the server but for transactions.
- Random & Round Robin algo for load balancer (confirm krna abhi)

- used for event-based execution of the code.

→ Azure App Services → Ability to give container for runtime
- Synonymus with web app. used to deploy web app.
- Problems:
  everyone is creating apps and everyone has their own requirements/choices causing a conflict.
- what OS you need, what runtime environment you need
- container in web apps gives you scalability, (automatically), scale-up, scale-down.
- If we dont use containers, we would need (to create) a yaml/deployment file.
- App Service Plan → compute part of the app service.
- PaaS environment. fully updated all the time.

→ Azure Networking Services
- Segmentation → allows you to control, what is source/destination, what is allowed etc.
  → imp to control the traffic flow.

Quiz: Next Monday.

Software Defined Networking

Sub-net Masking
IP addressing.

AVNet / Sub-netting

Lecture • 7

→ Azure Networking Services.

→ Subnet mask

• In Azure, nothing is smaller than /29 address space.

• we use subnetting bcz we need to do the segmentation

→ VPN Gateway

↳ Virtual Private Network.

↳ used to create a virtual private network to connect them and make a big network.

↳ any 2 disconnect ~~devices~~ networks, you can connect them, making a big network.

↳ Both need to know each other's address space so that they can send packets to each other.

↳ To ensure, the parties involved belong to 1 ~~perso~~ party, they share a specific key.

↳ Public IP is known by the VPN appliance but nobody (internal parties) know about them.

↳ Both networks talk to each other as if they are on the same cable.

↳ individual level : point-to-site

↳ At start, Azure had 2 network gateways, so to connect them VPN was used.

↳ To solve this Microsoft introduced "Peering"

acts like

public IP address is not needed to go outside the network

NAT → maps private IP to public IP.

→ Peering:

↳ connect 2 or more virtual networks in Azure.

How to connect? Create VPN → actual network → physical → cable

- Azure-to-anything → "VPN"
- Azure-to-Azure → "Peering"
  ↳ allows us to connect "VNets" without VPN.

→ Gateways are expensive, managing VPN is not easy.

→ In Azure-to-Azure, you have to be the "owner" (able to modify them) of both the Azure's.

→ Express Route (Private connection)
  ↳ on premise to Azure through private connection
  ↳ my line → local data center → Karachi data-center → Azure
  ↳ residing in Lahore wants to connect to the Karachi/Azure
  ∴ my line → physical cable/fibre.
  ↳ If no data center in your country, Edge (Microsoft) is used to connect cables.
  - make a connection using cables. ↳ or manage.

- Diff b/w deploying vs container in Azure App Service?

• IP address comes from Vnet.

Lecture - 8

DNS → translates the name to the IP address.

→ Azure DNS
We need to look at 2 records when DNS is record.
→ Alias
• A-record: Mapping of an ip-address to domain name
record
• CName: Mapping of domain name to domain name. : C → canonical
↳ when you have an existing domain name but want to change/get a new domain name.
• Microsoft gives you a domain name already (by default) (based on the name of your storage account).
• Role Based Access Control
• You can do all this externally as well as internally.
↳ VM starts up automatically & register in DNS.

→ Storage
↳ on premises : expensive (most)
• on cloud
↳ very cheap
↳ available for all worst case scenarios
↳ available for storing compute etc.

• For getting started, we need a storage account

• Anything that allows you to enter/access the file system/storage e.g file explorer.

→ Storage Account.
• Globally unique name. Bcz it is becoming a part of DNS

→ Redundancy
↳ LRS
• cheapest of all
• can survive ~~a part~~ failure of a part of a data-centre but not the whole data centers.
• ~~refer~~ 3 copies of data. one in each fault domain in a single data-center (provides resilleance)

↳ ZRS
• gives 3 copies in 3 different zones.
• more expensive
• copied out of data centre
• can survive data centre failure.

↳ GRS
• can survive region failure
• 2 LRS in different regions.
↳ LRS in primary & secondary regions

↳ GZRS
• primary region → ZRS
• secondary region → GRS.

↳ RA-GR
• ◊ m
• m
• MOS
on

→ Azure
• Stor
nec

↳ Az

↳ A

↳ G

↳

Premium : High... storage

↳ RA-GRS / RA-GZRS
- most expensives
- makes it or read-only
- Mostly used, when you want a back-up on reportingas it will not affect the app.

→ Azure Storage Services
- Storage itself has no services. A software is needed to provide services.

↳ Azure Blob
- generally used for unstructured data.
- e.g audio, binary data.
- Data of log file of database are used in Azure Blob.

database
↳ log file
↳ data file

↳ Azure Disk
- dont have to create a storage account

↳ Queue
- First in first out (FIFO)

↳ Azure Files
- Something that is shareable among multiple machines/users
  (NFS / ~~SMB~~ SMB)
  if want to talk to Linux
- when we go through "Network" name, we are going under SMB protocol.
- Multiple people can write to it.

Block lifestyle management

↳ Tables
- You need a structured data but you dont have to pay for this.

↳ Schema-less:
doesn't enforce columns. Keeps installing whatever you give it.

↳ Data Lake Storage Gen2.
used for big data storage system. used for analytics.

→ Storage Access Tiers

HOT cool cold Archive

- reduces cost with every tier.

→ why use 'CName'?
BCZ Microsoft gives us a unique domain name already.

• appliance → a VM with some specialized software running.

Lecture-9

→ Azure Migrate → gives the capability to go inside VM.
• It explore the VM's and also checks what and how many resources are used by the VM. Then, gives a reccomedation (Assessment)

• After Assessment, migration is done.
↳ • Web server, runtime frame works are used when a web app needs to be migrated
↳ • Check runtime environments, frame works and create

→ what is needed to configure "App Service"?
Web server, runtime environment.
containers

• Containers can be deployed in ACI, AKS, App Service

• ~~First containerize~~ Creates a docker file for containerization & deploys a yml file (key service used in all migrations).

• A group of nodes managed by AKS is called ~~k8s~~ kurbernetes cluster

→ Azure Data Box:

- When copying tera-bytes of data, it can take months because of the bandwidth.
- constraint: Bandwidth (expensive)
- To solve this, a data box is provided by the Microsoft. that is shipped to the user. After the service is used, it is shipped back. Microsoft sends data box of multiple sizes, multiple disks sizes, etc.

→ File Management option

↳ AZCopy → program of C#

- Takes all bandwidth. It can create threads and copies everything quickly. Can do 1-way synchronization.

↳ Azure storage explorer

GUI version of AZCopy.

↳ Azure File Sync (Not a backup of data but the copy of data)

- allows you to connect to storage account and keeps you in sync with your own file system (into your machine: File Server)
- Bi-directional synchronization.

• Online service has to be HTTP unless you have used some special/specific service.

→ Identity . Access . Management

→ Microsoft Entra ID.
↳ controlling the access to Azure
↳ ID service, directory service (identity & access management).
↳ B2B → bring your ID and I will authorize you
↳ It has B2B and also bussiness 2 consumer.
↳ Benefit : You dont have to manage your server.
↳ This is how bussinesses collaborate.
↳ Role based Access control
↳ First authentication & then authorization.
↳ cloud based authentication & management service

→ Microsoft Entra Domain Service
• LDAP (Port : 389)
protocol ↳ used by directory service
↳ password hash.
• Synchronizes groups, passwords, SID to ID.
• Directory Service (Special configuration) : Setup 2 way hash
↳ very week encryption
↳ e.g send password in email, SMS when retrieved.

• Very first thing on Azure is to set ...

• If Entra ID goes down, everything goes down as everything has to be accessed through Entra ID. ID actually acts as a door.

• Provides only authentication & access management

• PaaS service

• On premises <u>sync</u> → Entra ID <u>sync</u> → Managed domain

→ Diff b/w authentication & authorization

→ Multifactor Authentication (MFA)
  • Provides additional security e.g OTP.

→ Conditional Access
  • can have multiple signals based on what you allow (conditions).

(Mid : 01)