6/5/2023

Syallebus.

Basics of IT
1. Basic of Networking
2. Basics of IP
3. Basics of Sever
4. Basics of cloud computing
5. Account creations.

AWS.
1. Billing and account → theory part
2. EC2 → ASG = (Auto scaling group)
   → ELB = (Elastic load Balancing)
   → AMI - (Amazon Machine Image)
   → Snapshots - (a point-in-time copy of your data)
3. IAM - (Identity and Access Management)
4. Storage → EBS - (Elastic Block store)
   → EFS - (elastic file storage)
   → S3 - (Simple storage Service → Amazon S3)
5. Route 53 (Route 53 cloud domain name System Service)
   → DNS (Domain Name System)
6. AWC VPC (Amazon Virtual Private cloud)
7. cloud watch →
   (monitors your amazon Web Services (AWS) resources)
8. Azure (Azure has a virtual network cloud, where as AWS has virtual private cloud)

computer → Amazon EC2
Auto Scalling
Security & Identity → AWS IAM
Networking → Amazon VPC
Amazon Route 53
Elastic Load Balancing

Storage → Amazon S3
Amazon EBS
Amazon EFS

Managment Tools → Amazon cloud Watch.

Docker

1. Introduction
2. Docker image
3. Docker Architecture
4. Docker containers
5. Docker Volumes
6. Docker file
7. Docker compose
8. Docker Swarm

Nagios (monitoring tool)

1. Monitoring (windows performance Monitoring)
2. why Nagios
3. Nagios Architecture
4. NRPE (Nagios Remote Plugin Executor)

Other All

1. Linux (120 commands)
2. Shell Scripting → Scripting
3. Git and Git hub → Version control tool
4. Mavens
5. Jenkins → continuous integration tools
   Tomcat
   CI/CD Pipeline
6. SDLC, Agile & Jira → in theory class.

Automation:

1. Ansible
2. Terraform
3. kubernetes

Project

3 projects.

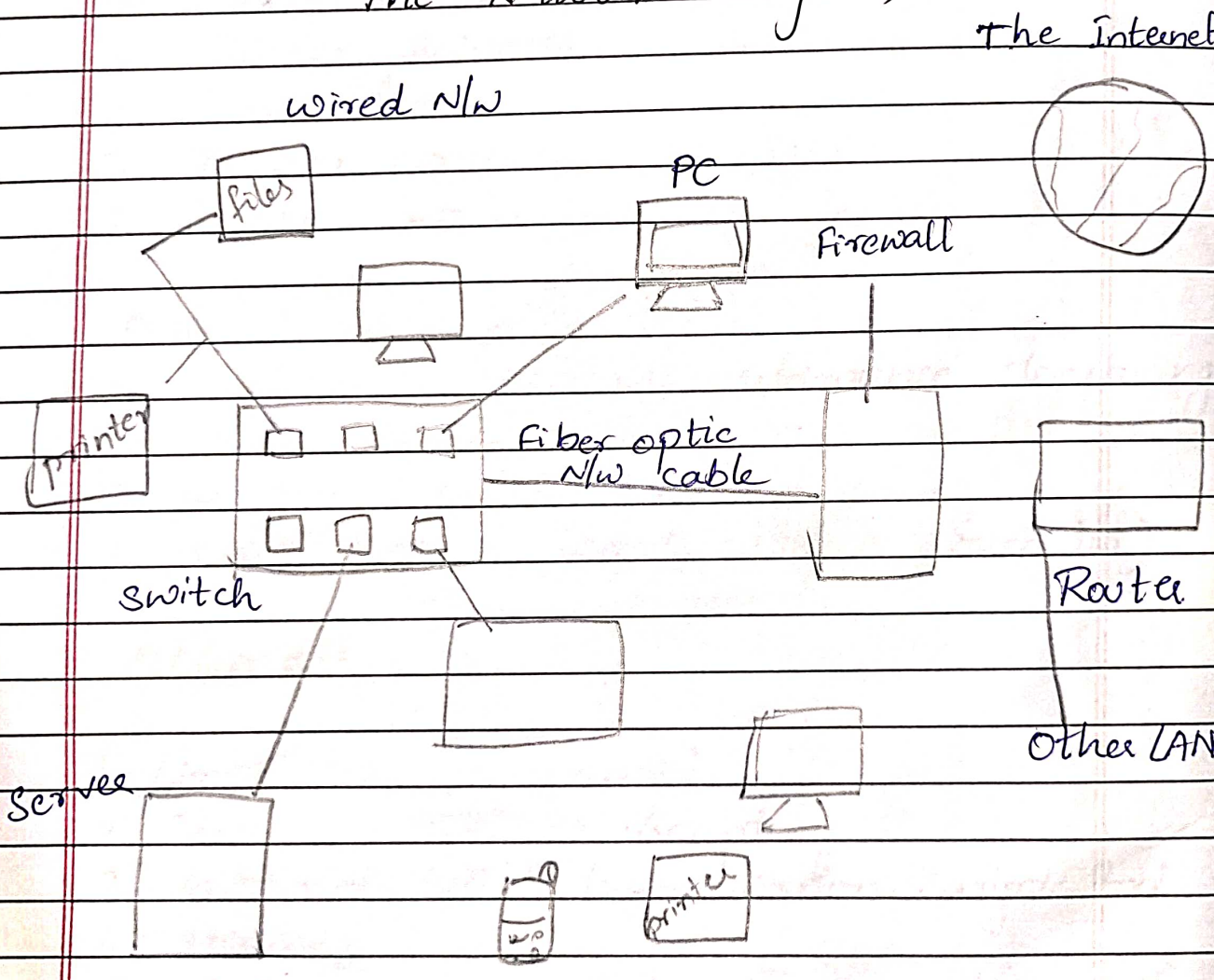
7/5/2023

Networking:

1. What is computer Networking

computer networking refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices use a system of rules called communications protocols to transmit information over physical & wireless technologies.

The Network Diagram



Switch:

A n/w switch connects devices in a n/w to each other, enabling them to talk by exchanging data.

Switches can be hardware devices or that

manage physical n/ws or s/w-based virtual devices

Firewall:-

A firewall is a n/w security device that monitors and filters incoming and outgoing n/w traffic based on an organizations previously established security policies.

Router:-

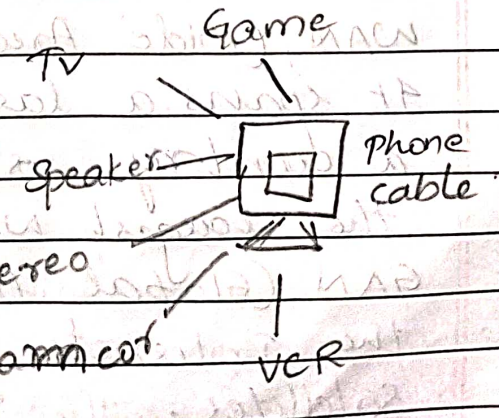
A router is a gateway that passes data b/w one & more local area n/w (LANs). It is a device that connects two or more packet-switched n/ws

2. Types of N/ws:

1. PAN (Personal Area N/w)
2. LAN (Local Area N/w)
3. MAN (Metroplitan Area N/w)
4. WAN (Wide Area N/w)
5. GAN (Global Area N/w)

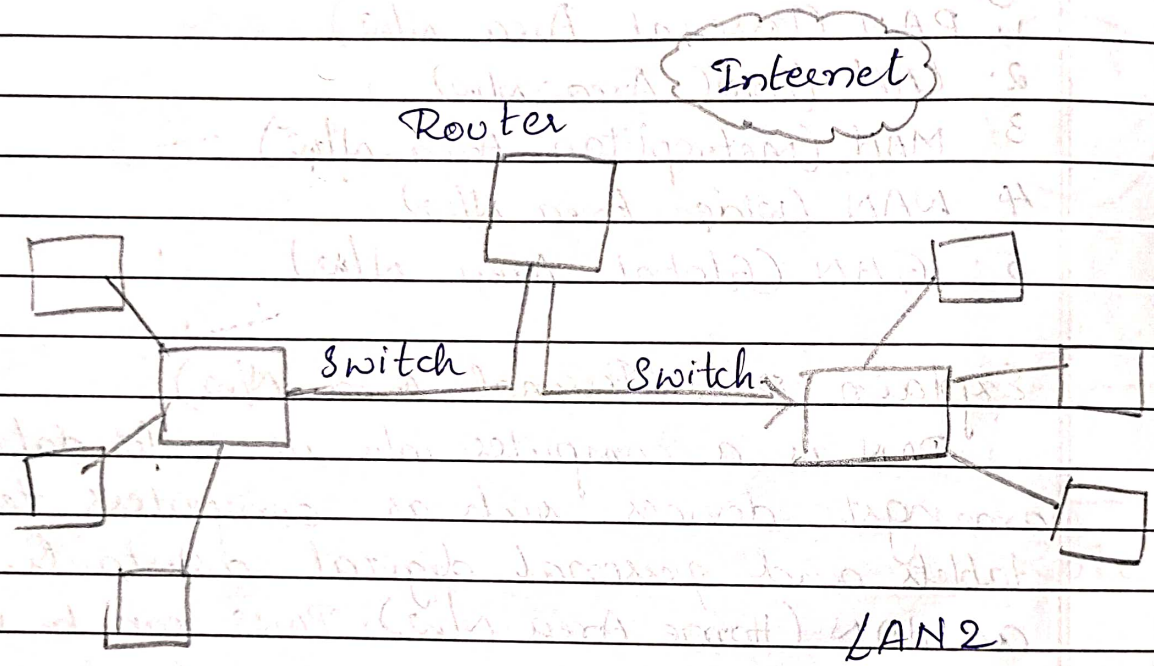
Explain PAN (Personal Area N/w)

PAN is a computer n/w used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants. Also known as HAN (Home Area N/w). PANS can be used for communication amongst personal devices themselves (Interpersonal communication) or for connecting to a higher level n/w & the internet (an uplink) where one "master" device takes up the role as internet router.



Explain LAN (Local Area N/W)

LANs are widely used to connect computers/ laptops and consumer electronics which enables them to share resources (eg - printers, fax machines) and exchange information. When LANs are used by companies or organizations they are called enterprise n/ws. There are two different types of LAN n/ws i.e wireless LAN (no wires involved acheived using wifi) and wired LAN (acheived using LAN cables)



MAN (Metropolitan Area N/W)

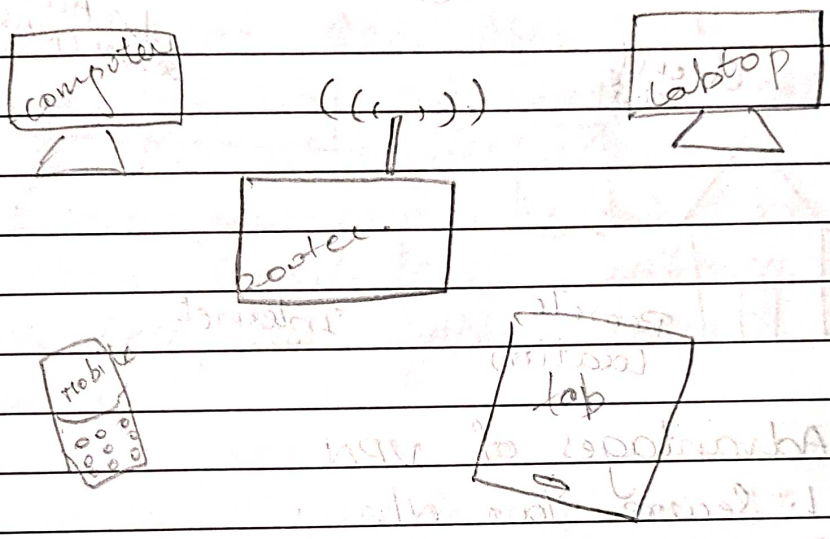
It connects and covers the whole city Eg. TV Cable connection over the city.

WAN (wide Area N/W)

It spans a large geographical area, often a country or continent. The Internet is the largest WAN

GAN (Global Area N/W) It is also known as the Internet which connects the globe using Satellites. The Internet is also called the N/W of WANS

Wireless Networking :-
Computer n/ws that are not connected by cables are called wireless n/ws. They generally use radio waves for communication b/w the n/w nodes. They allow devices to be connected to the n/w while roaming around with in the n/w coverage (wifi & Bluetooth)



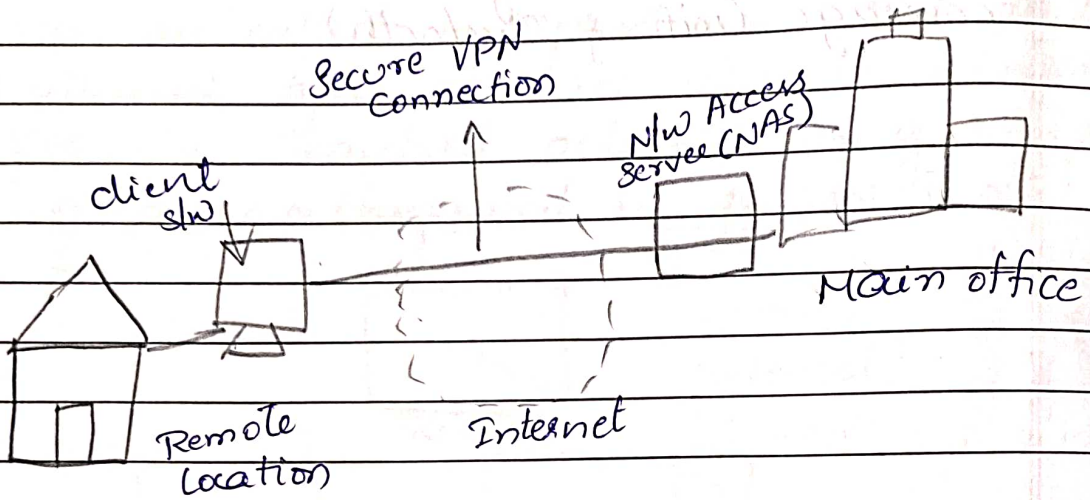
Types of wireless N/ws :-
1. Wireless LANS - connects two or more n/w device using wirless distribution techniques.
2. Wireless MANS :- connects two or more wireless LANs spreading over a metropolitan area.
3 wirless WANS :- connects large area comprising LANS, MANS & personal n/ws.

Advantages of wireless N/W :-
1. increased efficiency
2. Access and availability
3. Flexibility
4. cost Savings
5. Easy installation
6. wider reach

VPN (Virtual Private N/W)
VPN is a private WAN (wide Area N/W) built on the internet. It allows the creation

of a secured tunnel (protected n/w) b/w different n/ws using the internet (public n/w) By using the VPN a client can connect to the organizations n/w remotely.

Remote-access VPN



Advantages of VPN

1. Secure Your N/w
2. Hide your private Information
3. Prevent Data Throttling
4. Cost-Effective Security
5. Access region-blocked Services like PUBG Mobile
6. Provide n/w Scalability.

13/5/2023

Servers:

Server is a main computer that fulfills the request of other computers

Types of Servers

1) Application Server - It is a server dedicated to running certain s/w appl^n.
2) Database Server: Provides DB services to other computers
3) Web Server: A Server that HTTP clients connects to in order to send commands and receive responses along with

data contents

Adv of Sevens :-

1. Speed & automated backups
2. It will provide security
3. Scalability
4. Seemless connectivity. (n number of)

Disadv of Sesvers :

1. Customization of the hosting sevice is not possible at this time
2. It is possible for the host to get overloaded, causing the site offline
3. If you are running an e-commerce shop that stores Credits Card information on its own host the system, won't show in your results.

Server Scalling :

Server Scalling describes adjusting the computing power of sekvers, usually to increase power by scalling up, this called server scalling. This can be done either by scalling vertically or horizontally.

1. Vestical Scalling

1. It refers to adding more resources like CPU, RAM, disk to your server as on demand.
2. Most commonly used in appln & products of middle range as well as small & middle size companies

2. Horizontal Scalling

1. Its used when ever high availability of services (Seevers) are required then we will use horizontal scalling.
2. Horizontal scalling means increasing the no: of Seevers.

14/5/2023

Internet Protocol:-

1. What is the Internet?

The Internet is a global n/w that connects billions of computers across the world with each other and to the world wide web

2. What are the types of Protocols?

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secured (HTTPS)

3. What is an IP address?

IP address stands for Internet protocol address. An IP address is a unique no. provided to and every device
It is in the form of an integer number which is seperated by dot (.).

Ex: 192.168.10.26

IP address

we have 2 types of IP

1. IPV4
2. IPV6

4. Difference b/w IPV4 & IPV6

IPV4

length 32 bits
octet 4 (8*4 = 32)
0-255 range
4 billion (2^32)
192.168.10.26

IPV6

length 128 bits

octet 8 (16*8 = 128)

0 - 65535 Range

340 trillion (2^128)

➢ 2001 : 0db8 : 3c4d : 0015 : 0000 : 0000 : 1a2f : 1a2b

Uses of IP

Private IP → Static IP

Public IP → Dynamic IP

5. What are the different classes of IPV4?

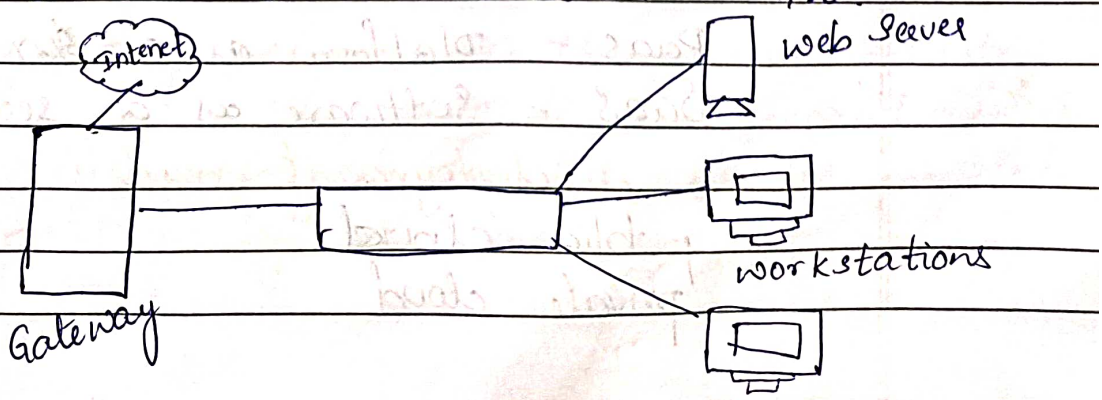
There are five types of IPV4 classes and are based on the first octet of IP addresses which are classified as classes A, B, C, D, & E

IPV4	IPV4 start Address	IP4 End address	Usage
A	0.0.0.0	126.255.255.255	Large Network
B	128.0.0.0	191.255.255.255	Medium Size N/W
C	192.0.0.0	223.255.255.255	local Area N/W
D	224.0.0.0	239.255.255.255	Reserved fa Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

NOTE: The IP address 127.0.0.1 is a special purpose IPV4 address and is called the local host & loop back address

6. Gateway:

Gateway is a hardware device that is used to connect 2 dissimilar / Similar types of n/w. It allows user to send & receive data through the internet even if it a LAN n/w.



Adv of Gateway.

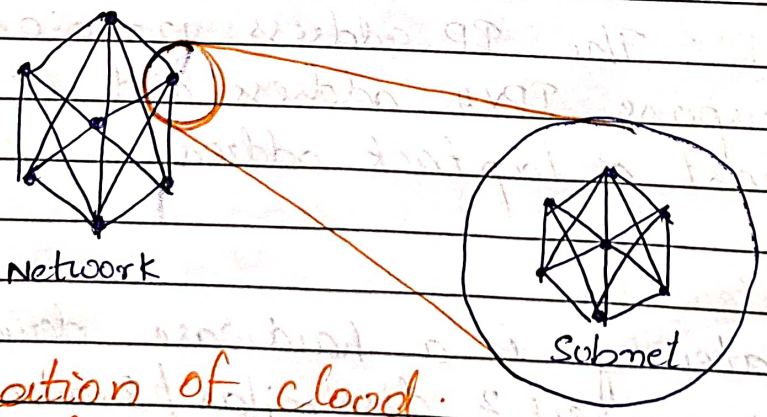
→ It connects two n/ws which have diff t protocols → (WAN to LAN)
→ we can't access the internet without a gateway
→ It provides security

Disadv of Gateway.

→ It is more expensive
→ Data transmission rate is slower.
→ difficult to mention as well as very comple
→ It is less intelligent

6. Subnet:

A Subnet, or subnetwork is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP n/w into multiple, smaller n/w segments. The internet protocol (IP) is the method for sending data from one computer to another over the internet



Classification of cloud.

Basis of Service models

IaaS - Infrastructure as a Service
PaaS - Platform as a Service
SaaS - Software as a Services

Basis of deployment models

public cloud
private cloud

community cloud
Hybrid cloud

Advantages of cloud computing:

→ Back-up and restore data
→ Improved collaboration
→ Excellent accessibility
→ Low maintenance cost
→ Services in the pay-per-use model
→ Unlimited storage capacity
→ Data security.

What is CC

Cloud computing is a develop. delivery of on-demand IT services over the internet on a pay-as-you-go basis.

Cloud Deployment Models.

The cloud deployment model Identifies the specific type of cloud environment based on ownership, scale, access, and the clouds nature and purpose. There are various deployment models based on the location and who manages the Infrastructure.

Types of cloud Deployment models.

Private cloud: Resource managed and used by the organization
Public cloud: Resource available for the general public under the pay as you go model.
Community cloud: Resources shared by several organizations, usually in the same industry.
Hybrid cloud: This cloud deployment model is partly managed by the service provided and partly by the organization.

Cloud Service Model

1. Infrastructure as a Service (IaaS)

It is a self-service model for managing remote data center infrastructures. IaaS provides virtualized computing resources over the internet hosted by a third party such as amazon web Services, microsoft Azure and Google. Instead of an organization purchasing h/w (hardware) companies purchase on a consumption model. It is like buying electricity and this model enables companies to add, delete & reconfigure of IT infrastructure on demand.

Adv of IaaS.

Cost-effective
Website hosting
Security
Maintenance

2. Platform as a Service (PaaS)

PaaS allows organizations to build, run and manage appl^n without the IT infrastructure. this makes easier and faster develop, test and deploy appl^ns.

Developers can focus on writing code and creating applications without worrying about time-consuming of IT infrastructure activities such as provisioning severs, storage and backup.

Paas brings more value to the cloud. It can reduce your managment overhead & lower your costs. PaaS also makes it easier for you to innovate & scale your services on demand.

Adv of PaaS

Simple and convenient for users
cost - effective
Efficiently managing the lifecycle efficiency.

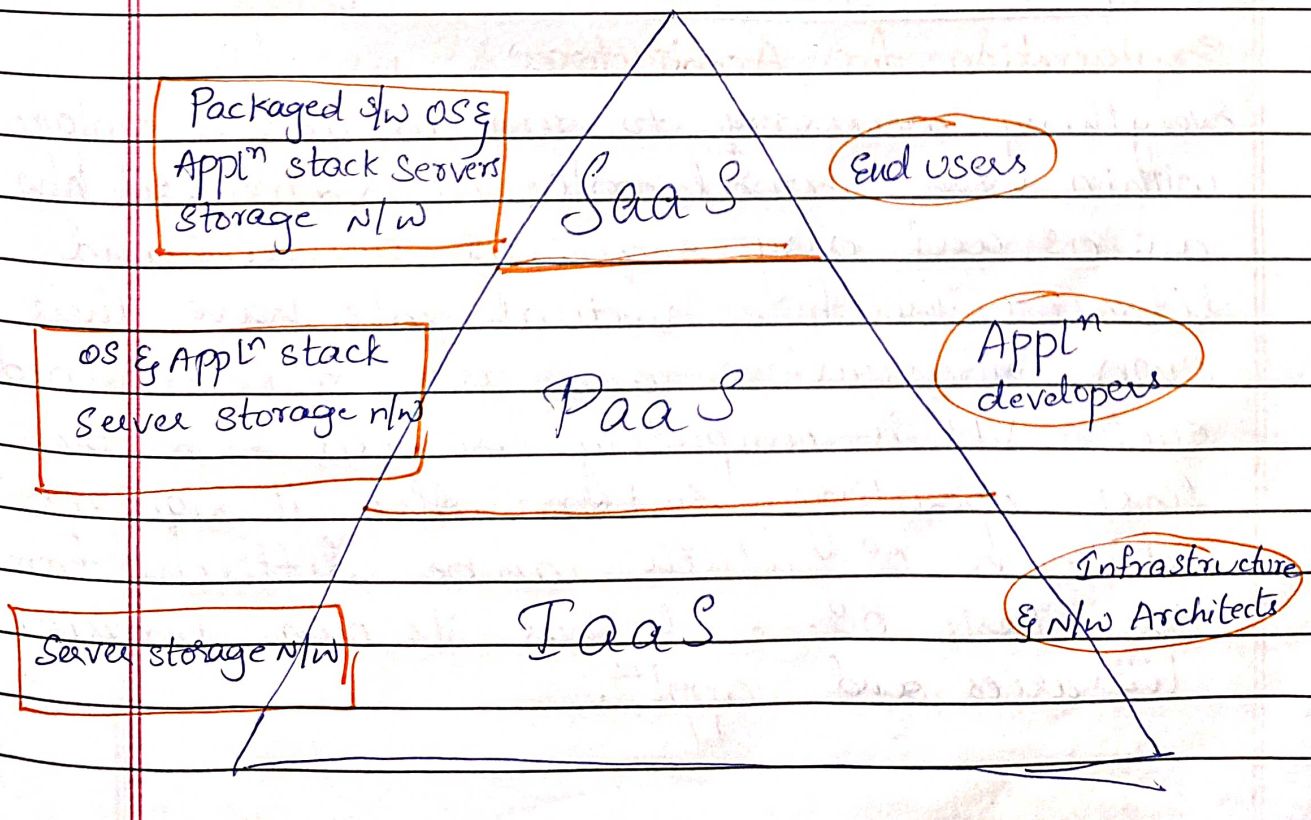
Software as a Service (SaaS)

S/w as a Service (SaaS) replaces the traditional on-device s/w with S/w that is licensed on a subscription basis. It is centrally hosted in the cloud.

Most SaaS applns can be accessed directly from a web browser without any downloads or installations required. However, some SaaS applns require plugins.

Adv of SaaS.

cost - effective
Accessibility
Reduced time
Automatic updates
Scalability

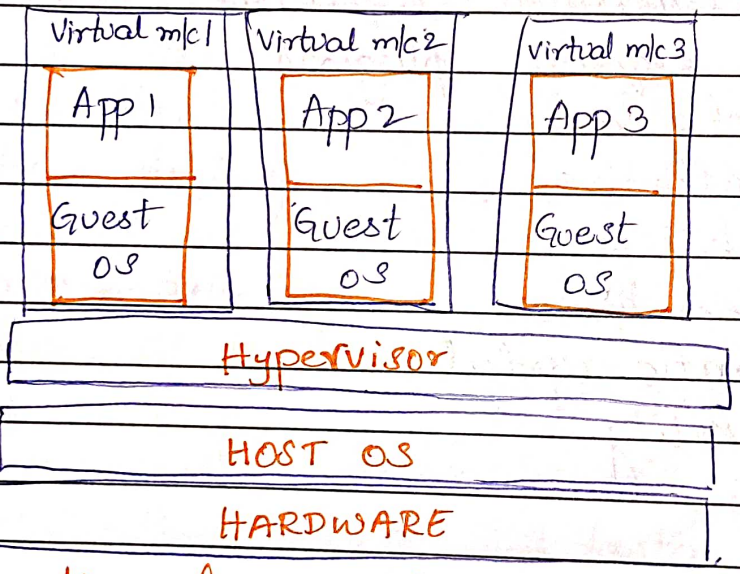


20/5/2023

Virtual Machines:

In computing, a virtual m/c is the virtualization/emulation of a computer system. Virtual m/c are based on computer architectures and are based on comp provide functionality of a physical computer. Their implementations may involve specialized hardware, s/w or a combination.

Virtual m/c allow you to run an operating system in an app window on your desktop that behaves like a full, separate computer.



Explanation for Architecture:

Everything necessary to run an app is contained within the virtual m/c. The virtualized h/w, an OS, and any required binaries and libraries. Therefore virtual m/c have their own infrastructure and are self-contained. Each VM is completely isolated from the host operating system. Also, it requires its own OS, which can be different from the hosts OS. Each has its own binaries, libraries and appl^ns.

* Virtual m/c monitor (VMM): another name for the hypervisor
* Host machine: The h/w on which the VM is installed.
* Guest m/c: another name for the VM.

Hypervisor:-

VMs run on top of a physical m/c using a "hypervisor". The hypervisors themselves run on physical computers, referred to as the "host m/c". The host m/c provides the VMs with resources, including RAM & CPU.
The VM that is running on the host m/c is also often called a "guest m/c".

Advantages of VM.

1. Sharing of resources helps cost reduction.
2. virtual m/cs are isolated from each other as if they are physically seperated.
3. Virtual m/cs encapsulate a complete computing environment.
4. VM run independently of underlying h/w.
5. VM can be migrated b/w diff hosts.

Disadvantages of VM.

1. It can have a high cost of implementation
2. It still has limitations
3. It creates a security risk
4. It creates an availability issue
5. It creates a scalability issue
6. It requires several links in a chain that must wok together cohesively.

21/5/2023

GIT Bash.

GIT SCM

download (2.40.1)

↳ standalone Installer

32 bit / 64 bit.

install with all next steps.

Finish.

AWS:

* Region → mumbai

EC2 – virtual server instances

* Server is a main computer to run all the IT operations. stores.

⇒ To launch windows instances in EC2 Service.

First select Region – Mumbai

→ click on instances

→ click on launch instance.

→ Name: Titan window

▽ Application & os images (Amazon M/c image)

AMI :- Amazon m/c image, an AMI is a template that contains the s/w configur-ations i.e os, appl^n servers & appl^n required to launch instances.

→ Select down window AMI (free eligible)

▽ instance type (free eligible)

t2.micro

▽ key pair.

keypair: keypair is used to securely connect to your instance.

keypair name – require

click → create new keypair

type

↳ titans

private key file formate

◉ .pem (select the radio button)

○ .ppk.

• pem :- privacy enhanced mail

→ click on [create key pair]

→ select key pairs → titans

▽ Network settings.

↳ Firewall (Security Group)

⊙ create Security group

Security Group :- A security group is a set of firewall rules that control the traffic for your instance and add rules to allow specific traffic to reach your instance

[✓] Allow

▽ Configure storage

1 x [30] GiB.

At final click on → [Launch Instance]

Success

→ After that check by clicking at the bottom [View all instances]

How Generate password

[✓] titanswindows

↳ Goto top → ~~connect~~

↳* Shortcut :- Goto top → Action → Security → Get windows password.

Copy the username & password → in one notepad.

Connecting to windows Server.

① Select instance name

[✓] titanswindow

Goto top connections

click [RDP client]

↳ Down

↓ Download remote desktop file

↳ open that file

↳ click connect & next page give password

next page ↳ click on Yes. (It will open to OS (virtual))

2 method

In device click on search → Remote Desktop Connection.

copy the public IPV4 DNS & type on compute [ ] connect.

& give password
↳ ok
↳ yes.

After this process teeminate the Instances on clicking instance state.

To launch Linux Instance.

Name & tags : titanslinux

▽ Appl^n & os Images
select [Amazon Linux aws]

Amazon Machine Image

Select Amazon Linux 2AMI(HVM) - kernel 5.10. (free tier)

▽ key pair
click on → Create new key pair
key pair name : titanslinux
⊙ RSA
⊙ pem

[create key pair]

click at Right corner [launch Instance]

[View all instances].

Linux is comman line Interface - open source.
It will connect directly in chrome.

Connecting to linux server.
Activating

→ ~~open - chrome new tab~~ → Select instance → top connect → EC2 Instance connect → connect (down)

cmd → sudo su - (ec2 user - root user) ↴

package → yum update (It will update linux system) ↴

In blw click yum update -Y ↴

yum install httpd ↴

Do you want to contine : Y ↴

systemctl status httpd ↴

Active : inactive (dead)

Systemctl start httpd ↴

Systemctl Status httpd ↴

Active : active (running)

To allow for incoming & outgoing traffic.

Go to instances

→ Select instances → Security → Security groups

→ Select down inbound rules → Edit inbound Rul

[Add rule]

select HTTP, under Source → IPV4.

[Save Rule]

Go back to instances: Select instance → Details

copy public Ip address → paste in new tab.

Test page will open.

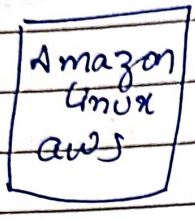
27/5/23

Launching a instance bypassing a user data

→ Name and tags

titanlinux

→ ▽ Appl" & OS Images



Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - kernel 5.10, SSD...

(Free tier) ▽

→ Instance type

t2.micro

→ key pair

create new key pair

titanlinux

→ Advanced details → click

at last

User data - optional

```
#!/bin/bash
yum update -y
Yum install -y httpd
Systemctl start httpd
Systemctl enable httpd
```

Launch Instance

→ Select Instance → security →

click on → Security group.

Inbounds → edit inbound

Add rule

type [Http] Source - [anywhere IPV4]

Save rule

→ Goto instance → Details → copy public address
→ Goto new tab → paste the Ip address
→ It will open Test page.

To Edit user data

→ Select the instance → at top Instance State
Select → Stop instance.
→ Select the Action → instance setting
→ Edit user data
add command & Save (ie yum install java -y
yum enable java)
→ Select instance → Instance state → Start instance

command is: yum install java -y
yum ~~install~~ enable java.

→ Select instance → connect at top →
connect.

Launching instance in command prompt

ssh → secure shell.

Terminal
1) Direct ~~command~~ connect
2) command prompt
3) Git Bash..
4) Mobaxteem.

Command prompt:

→ open command prompt in system

→ From instance → select connect →
Select SSH client tab
In that copy the path under
Example:

ssh -i "titanslinux.pem" ec2-user@ec2-13-126...
compute.amazonaws.com

28/5/23

IAM Service

IAM stands for Identity & Access Managment;
IAM is a web Service that helps you securely controll access to AWS resources, you can control who is authenticated and authorized to use resources.
IAM is a sevice from AWS using which you can give permission ~~to~~ to different users and you can give permissions to Groups

Features of IAM

1. Shared Access to your AWS a/c
2. Granular Permissions
3. Multifactor Authentication
4. Identity federation
5. Identity information for assurance
6. Secured Access to AWS resources

IAM Authentication:

IAM authentication verifies a users identity, once authenticated the verified user may use any of the resources from their account is authorized to access.

IAM Authentication Methods:

1. User name & password
2. Access key
3. Session Token

IAM Components:

1. User 2. Groups 3) Roles 4) Policies.

IAM USER:-

An IAM User is an entity that you can create in AWS.
The IAM user represents the person who uses the IAM user to interact with AWS.

Date
Page

IAM Groups:

Groups are collections of users and have policies attached to them

A Group is not an identity and cannot be identified as a principal in an IAM policy.

use Groups to assign permissions to user.

IAM Roles:

An IAM Role is very similar to a user in that, it is an identity with permission that determines.

Roles doesnot have any credentials

Policies:-

Policies are documents that define permissions and can be applied to users groups and roles.

Policies are written in the JSON Languag

Hands on Experience on IAM.

How to create Security Groups.

Create security Group

Base

full access

Inbound Rules

[Add rule]

[SSH ▽]

[IPV4 ▽]

[All traffic]

[Any IPV4]

EBS

Block storage

Region → Mumbai

↳ Instance

Name : Linux devops

Instance type : t2

↳

EBC → left side

↳ volumes → Select the instance

Edit name → with same instance name

[Create volume] at top

→ check the instance availablity → it is 1a

Volume type

[SSD ▽]

Availability zone

ap-south-1a.

[create volume]

Now attache instance with name
External volume
Select volume → Action
Attach volumn

instance
instance name
Attach volume

Now data storage is created
checke in instance → storage

Detach
Volume → enteral-volume → Action
↳ force detach volume
Now you can attache instance another one.

Delete volume
Select volume → Action → delete volume

How to create Snapshot
Select volume → Action → create Snapshot

Description
create snapshot

Select Snapshots → at left side
Edit name → jspiders_httpd

How to create AMI
Select Snapshot → Action →
create image from Snapshot
image name
JSpiders_httpd - installed

Description

Architecture
x86-64

Root device
/dev/sda1

create image

Images at left side
Select AMIs
Edit name :- jsp-httpd

Launch instance by using AMI
Select AMI → Launch instance fro AMI

Name & tags
jsp-backup

Launch instance

4/6/2023

S3 - Simple Storage Service

S3 is a scalable, highspeed, web based cloud storage service

Amazon S3 features
low cost & easy to use .$
Secure
Scalable
High peformance
Integrated with AWS Service

S3 storage classes.
1) S3 Standard
2) S3 Intelligent
3) S3 Standard - IA
4) S3 One zone - IA
5) S3 Glacier
6) S3 Glacier deep Archive
7) S3 out post

How to create S3 Bucket.

Select S3 Services.
create a S3 bucket click.

How to or

→ Bucket name
demosample

→ AWS Region
Asia Pacific (Mumbai) ap-South-1

→ object ownership

⊙ ACLs enabled

→ object ownership
⊗ Bucket owner preferred
⊙ object writer

→ Block Public Access setting

☐ uncheck Block all public access

→ ⚠ Turning off block.
☑ I acknowledge

→ Bucket versioning
Bucket versioning

⊙ enable

→ Tags (0) - optional

→ Default encryption
Encryption key type
⊙ Amazon S3 managed keys (SSE-S3)

→ Bucket key
⊙ enable

Create Bucket

→ click on Bucket demosample

How to upload a file into S3 bucket:

Select the bucket i.e demoSample

[upload]

click on [Add files]

select to be uploaded & click upload

click on files → object reviwe

→ object URL → copy

paste in new tab.

How to provide access to object:

→ demosample

↳ file → permission

→ click on Eidt

[✓] Read [✓] Read

[✓] I undeestood the effects of changes

click on save changes.

Now the file can see on that new tab.

⇒ Replication Rules. (Same Region)

Create Bucket name srcbucketjsp

create Bucket name destbucketjsp

object same steps.

① Actly

Goto srcbucketjsp

Goto managment

Replication rules

use replication rules to define options that you want to peeform in S3.

[Create Replication rules]

Name

Sameregion 123

① enable

② Apply to all objects in the bucket

Destination

Browse S3

⊙ destbucket jsp
↳ click choose path
IAM role
⊙ choose from existing IAM roles
Select role ▽

save

Replicate existing object
⊙ No, do not replicate existing objects
⊗ Yes, replicate existing objects

Submit

How to upload files in src
upload
↳ select the file
↳ upload

// Replication Rules - Cross Region.

Create SrcBucket
Region-Mumbai

Create destBucket
Region: Osaka - ap-northeast

Goto SrcBucket
↳ Managment
↳ Replication rule
↳ Rule name: cross region
↳ Save.
↳ ⊙ No
↳ submit

Goto SrcBucket
↳ upload file.

Lifecycle Rule.

Select src Bucket
↳ Managment
↳ lifecycle Rule
create lifecycle Rule
↳ Name
updates only.
↳ choose a r
⊙ apply to all object
☑ acknowledge
↳ Lifecycle rule action
☑ Expire
☐ permanently delete
Days
create rule

1) Create S3 bucket
2) upload files
3) Permission
4) Versioning
5) Replication → SRR / CRR
6) lifecycle of S3

6/10/20 S3

Cloud Storage:.

what is cloud Storage?-

Cloud storage allows you to save data and files in an off-site location that you access either through the public internet or a dedicated private n/w connection.

Adv of cloud Storage:

* Data is accessible from any part of the world with the help of the internet as it is stored online on seevers.
* Data can be shared easily b/w

Auto Scaling Group

6/10/2023

Create Template

Goto EC2 Service
↳ launch template
↳ create template
↳ Name: first template
↳ description: eg: backup

Amazon Linux — 2AMI - kernel

Instance type: t2.micro
Key pair: Select (Titans)
Network → create security group
(if not present)
Select the security group ∀

Advance
user data

```
#!/bin/bash
yum update -y
yum install -y httpd
Systemctl start httpd
Systemctl enable httpd
EC2AZ = $(curl -s http://169.254.169.254/
latest/meta-data/placement/
availability-zone)
echo '<center><h1>This Amazon EC2 instance
is located in Availibity Zone:
AZ ID</h1></center>' > /var/www/html/
index.txt
Sed "s/AZID/$EC2AZ/" /var/www/html/
index.txt > /var/www/html/
index.html.
```

create Launch Template.

Auto Scaling Group.

Create New
Name eg: amazonproject
Template :: first template → already created one
Next.
VPC → default
Availability zone → take all [select 3 (all)]
Next
⊙ No load balancer
Next
Desired capacity → 2
Min capacity → 2
Max capacity → 2
Scaling policies → None
↳ Next
↳ Next
To check go to Instances
Edit names : amazon1
amazon2 (select instance)
public IPV4 → copy & check in browser.
Terminate any one then Refresh,
automatically one more instance will create.

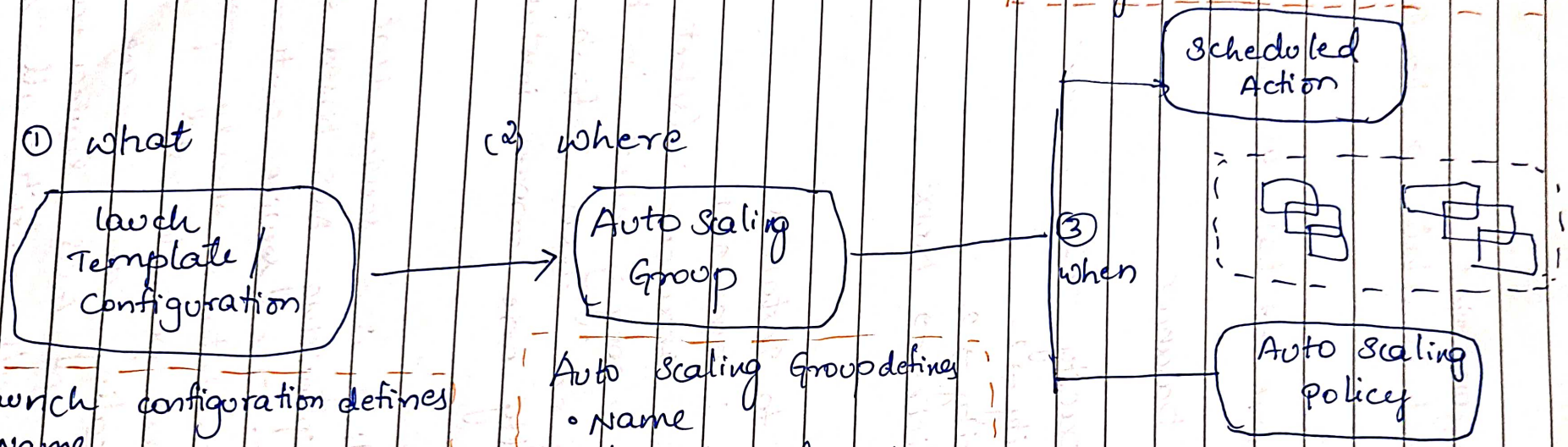
AWS - Autoscaling : ASG

AWS Autoscaling is a service that assists organiza-tions in supervising AWS-based s/w and infrastructure. The service automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.
Aws Auto Scaling can increase & decrease the capacity of AWS Services to optimize costs. The service will monitor all scalable cloud services and resources related to a user's applications.

AWS Auto scaling

AWS

Scheduled Action helps define rules to perform scaling action at a certain time in the future.



launch configuration defines
- Name
- AMI
- Instance type
- key pair
- use data
- Security group
- IAM Role.

Auto Scaling Group defines
- Name
- Launch configuration Name
- Az or Subnet
- Min & Max capacity
- Desired capacity
- load balancer
- Metrics & Health check.

Auto scaling policy helps define roles for dynamically increasing or decreasing the EC2 instance count based on cloudwatch alarms.

How Auto Scaling works:

1. Elasticity is one of the clouds greatest attributes. Auto-scaling facilitates elasticity by automatically adding resources to meet new work load demands and reducing them when demands decreases.
2. AWS will elastically scale your EC2 instances by launching new ones and terminating old unhealthy ones. If an EC2 instances status-check fails. AWS Auto scaling will replace the instance. This helps you develop more resilient applications.
3. Auto-scaling also utilizes peeformace-based metrics that are sent to cloud watch, for instances, you might set peeformance metrics based on CPU thresholds.

Auto scaling Groups (ASG) is a collection of EC2 instances. Thus, the size of the ASG is dependent on the capacity or the numbee of instances you have configured for the group. ASGs are free, no need to pay for them.

AWS Auto Scaling Groups are an integral part of the scaling process. In the case of EC2, they manage how instances are scaled using launch configurations or launch templates. They scale out, scale in, and ensure that theee are a minimum and a maximum numbee of instances running. They are also responsible for automatically registering new instances to the load balancer.

Types of Auto Scaling:

Vertical Scaling:

* In the same server, increasing resources is called a vertical scale-up.
* In the same server decreasing resources is called a vertical scale down.

Horizontal Scaling:

* when we are increasing the server is called a horizontal scale out.
* When we are decreasing the server is called horizontal scale in.

A Drawback of Vertical Scaling.

Single point failure

Advantages of Auto Scaling Groups.

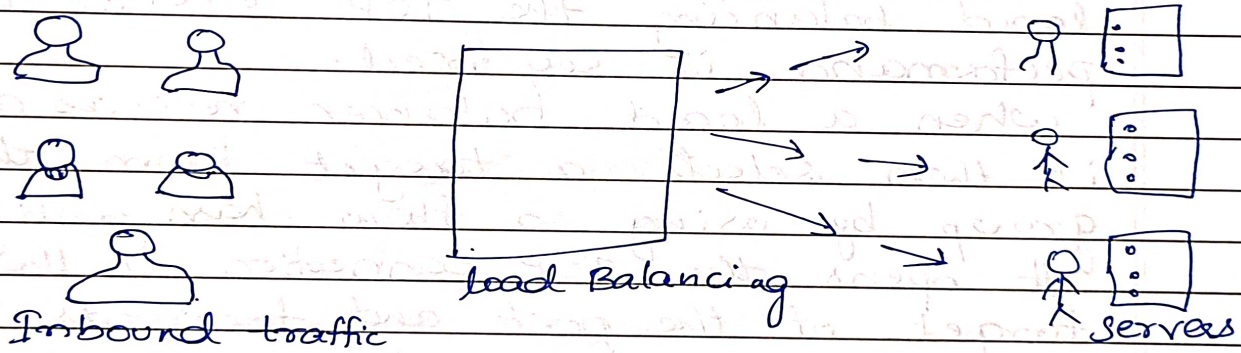
* Improved fault tolerance - AWS Auto scaling allows you to monitor your appl^n. It can help you terminate any corrupted instances and automatically launch new ones.
* Improved cost managment - you can scale-up or down depending on your organization's requirements. This allow you to save money on personal and equipment
* Reliability - Since scaling is done Automatically, its incredibley efficient and reliable. whenever scaling is initiated, AWS will send notifications to phone & email addresses.

AWS : Elastic Load Balancing (ELB):

Elastic load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers and IP addresses, in one or more Availability zones, It monitors the health of its registered targets and routes traffic only to the healthy targets.

* Elastic load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic. You can add and remove compute resources from your load balancer as your needs changes without disrupting the overall flow of requests to your applications.
* Elastic load Balancing supports the following load balancers. Appln load Balancers, N/w load balancers, Gateway load Balancers & classic load Balancers. You can select the type of load balancer that best suits your needs.

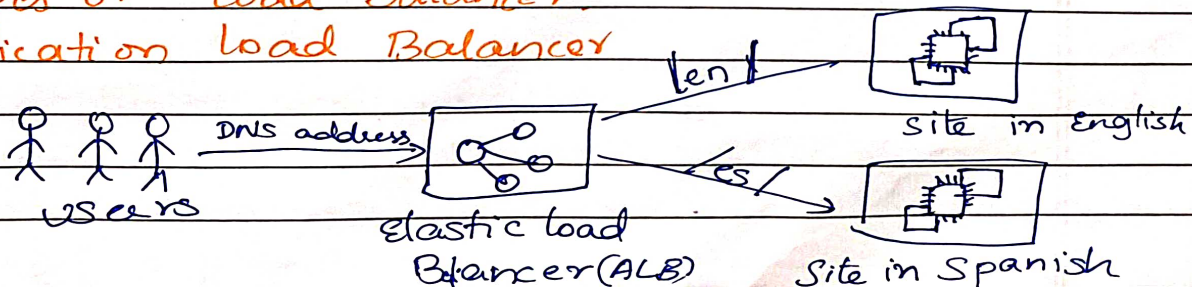
Load Balancer:



A load Balancer is a virtual m/c or appliance that balances your web applⁿ load which could be HTTP or HTTPS traffic that you are getting in. It balances a load of multiple web servers so that no web server gets overwhelmed

Types of Load Balancer:

1. Application load Balancer



* Amazon web Services (AWS) launched a new load balancer known as an appl^{n} load balancer (ALB) on August 11, 2016
* It defines the incoming traffic & forwards it to the right resource. For eg, if a URL has an API extension, then it is routed to the appropriate appl^{n} resources.
* Application load balancers are intelligent, sending specific requests to sepicific web seevers. It is best suited for load balancing of HTTP and HTTPS traffic.

2. Network load balancer.

It makes routing decisions at the transport layer (TCP/SSL) and it can handle millions of requests per second. It is best suited for load balancing the TCP traffic when high peeformance is required.

when a load balancer recieves a connection, it then selects a target from the target group by using a flow hash routing algorithm. It opens the TCP connection to the selected target of the port and forwards the request without modifying the headers.

3. classic load balancer:

classic load balancers are legacy Elastic load balancers. It routes the traffic b/w clients and backend services based on IP address.

11/6/2023

ELB. To create Target Group.

Go to load Balancing left corner
↳ Target Groups
↳ create Target group
→ choose a target type
⊙ Instance
→ Target Group name
flipkartload
→ protocol version
⊙ HTTP1
click on ↳ Next
Available instance
↳ select two instances ☑ ☑ which already creat

click on
include as perding below

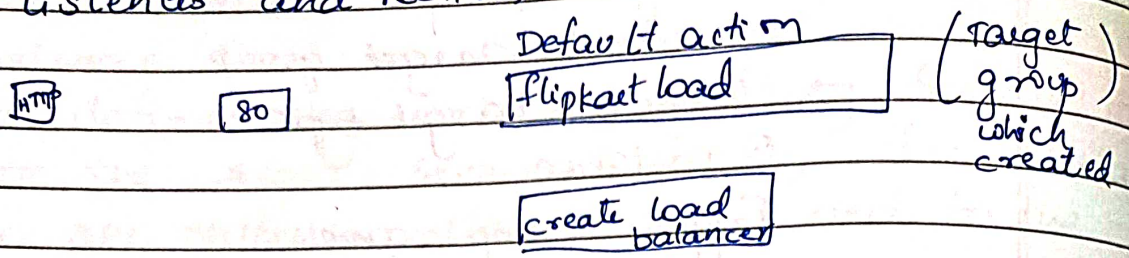
Create target Group.

To create load Balancer.

Left corner → click on
↳ load balancer
↳ create load balancer
↳ Go to Appl^n load balancer
↳ create
↳ load balancer name
flipkart users
→ Scheme
⊙ Internet-facing
○
→ IP address
⊙ IPV4
→ Network mapping

Mapping
☑ ap-south
☑ ap-south
☑ ap-south

→ Security group ▽ which already created
→ Listeners and routing



click on view load balancers.

To check the load balancer is working or not
Select load balancer
at bottom DNS name copy &
paste in new tab it will open Test page

Route 53.

Click on Route 53 Services
In dashboard
↳ create hosted zone
Domain name
sample.come
Type
⊙ public hosted zone

create hosted zone

Two records created with type: NS & SOA

Click on create record
Record name
demo
Record type
IPV4 address
value
192.0.8.16

create records

Now demo.sample.com created
~~Click on~~ ✓ demo.sample.com

Now click on ☑ sample.com type NS
at the Right corner copy the 4 ns paths
and put them in GoDaddy domain name.

17/6/2023

VPC

An amazon VPC is a isolated portion of an aws cloud

1. VPC is a isolated virtual n/w on AWS cloud, it has complete control over your virtual n/w.
2. We has two types of VPC
   1) Default VPC
   2) Custom VPC

Steps :- to VPC.

1. Search : VPC (on top search bar)
   create VPC
   Left side your PC's
   create VPC
   → Name tag : instagram
   → IPV4 CIDR block
   ⊙ IPV4 CIDR manual input
   ○
   → IPV4 CIDR → range
   10.0.0.0/24
   n/w id hosted id

   create VPC

2. click on subnets left side (public)
   create subnets
   → VPC ID
   Instagram

Subnet settings. → Add subnet.
→ Subnet name
public-subnet-insta
→ Availability zone
ap-south-1a
→ IPv4 CIDR block
10.0.1.0/26
create subnet

3. Route table (left side)
create Route table
→ Name
public-route-insta
→ VPS
VPC - instagram
create Route tables

4. Internet gateways. (left side)
creati IGW
→ Name
my-vpc-insta
create Internet gateway.

Creating APP server.

⇒ Goto EC2
launch instance
→ Name
app-serve-insta

→ amazon Linux 2 AMI
→ t2.micro
→ key pair : instaproject. → create key pair
→ network setting click
Edit
VPC : instagram
subnet : public-subnet-insta

→ Auto assign public IP
Enable

→ Firewall
⊙ create security group
→ Security group name
all traffic ▽

→ Advance setting
user data
#!/bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
System ctl enable httpd

↳ create instance.

⇒ click on Route tables
☑ public-route - insta
click on Action → edit subnet associations
☑ public-route-insta
Save association.

⇒ Select Route table
☑ public-route insta
Down click Routes
Edit → Add route
Destination Target
0.0.0.0/0 Internet gate

⇒ select Igw
☑ my-vpc-insta → Action → Attach VPC

Go to instance → connect → Test page.

Create Subnet
name: private-subnet-insta
IPV4 CIDR: 10.0.0.128/25 → create
Create Route table.
Name: private-route-insta
VPC: instagram
create.
Launch instance
name
db-serva-insta.
→ Network settings. → Edit
VPC: instagram
Subnet: private-sub-net
Auto: Disable
→ Inbound
all traffic
↳ create instance.
How to create NAT Gateway. (N/w Address transl
Goto VPC
Left corner → NAT Gateways.
Create NAT
→ Name: for-private-subnet
→ subnet
public-subnet-insta
→ Connectivity type
⊙ public
private
→ elastic IP allocation ID
Allocate click.
create NAT GATWAYS.
Goto Route table.
☑ private
Action → Edit Accessiable
☑ private
save

Goto Routes down
edit Routes
Destination Target
0.0.0.0/0 NAT Gateway. (select NAT created)
save changes.

Goto instances. → connect.
SSH client

go to downloads → .pem file → copy all.
~~vi~~ vi demo.pem

Goto instance → public → ☑ app-server
connect
cmd vi demo.pem (one page will open)
copy the download .pem file data
& paste in that page. esc + shift ;
cmd ping google.com
ctrl c & exit.