CSP → cloud service provider
ISP → Internet service provider

cloud intro

AWS cloud resources

Learning how to use resources for auto-mation, IOT, electronics, storage resources. Accessing & Modifying according to the need of the consumer.

OS
Server - Client
Virtualization
Cloud (rented service)

Developers version of shell available in Windows OS is AWS cloud practitioner certification power shell.

- Cloud definition (No particular definition)
  - ↳ cloud characteristics
  - ↳ cloud services
  - ↳ cloud models

  } should explain whoever asks you.

All the data ~~concepts~~ centers around the world together is known as cloud.

Cloud characteristics :-

(1) NIST → National Institute of standards and Technology (like NAAC & NDA gives the standards to the cloud services like grades).

1 (2) On-demand self service.
2 (3) Broad network access.
3 (4) Elasticity
4 (5) Resource pooling
5 (6) Metered services (pay as you go)

- No maintainance/easy maintainance
- security.

a) On-demand self service

Before the claud came into light, w need a server of our own which makes difficult for them and takes more time i.e nearly 20 days. The server connection involves the following steps

→ Writing a letter
→ For the releasing of funds
→ Accounts
→ Giving order to the particular compan based on the requirement
→ Manufacturing
→ Delivering
→ Downloading os
→ Enter Details

This makes minimum of 1 month for the server placement.

The organizations will not be shopped working if they are lack of resources, they will switch to another one.

Like AWS, cloud, oracle, Azure web services, they provides the access for storing within minutes, if you need. They will be providing the servers virtually for storing the data.

We can create our own server with the data storage capacity you need.

Bare metal server → physical machines
→ hugh resources.

Traditional OS / Hypervisor (Virtualization, hypervisor)

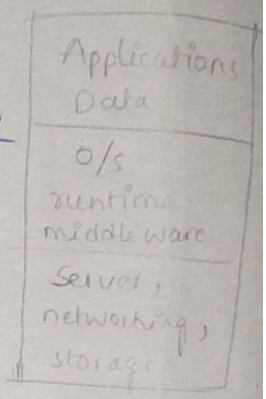
full control to user ⇒ control over hardware.

AWS → Nitro.

Cloud services :- 3 (sometimes 4)

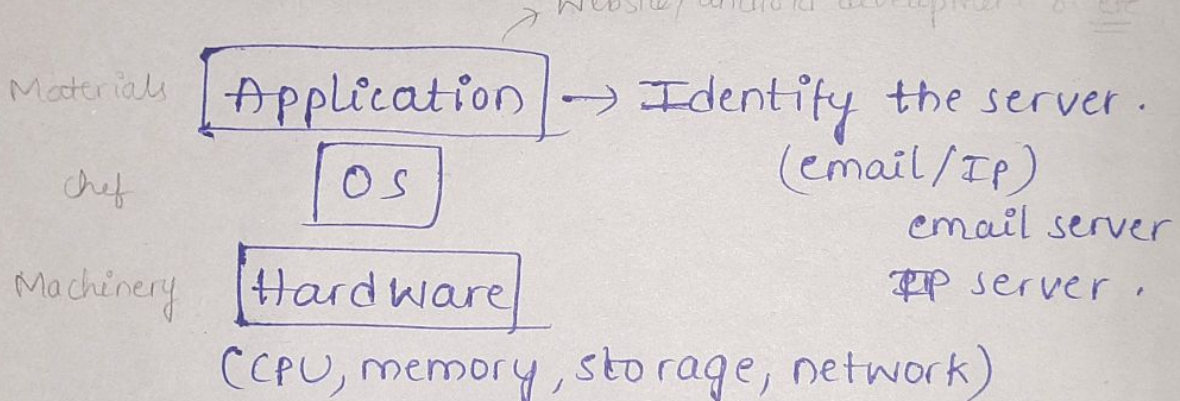
1) IaaS - Infrastructure as Service
2) PaaS - Platform as service
3) SaaS - Software as service.

- Cloud → maintaing servers.



IaaS

IaaS → machinary
PaaS → give materials
SaaS → order



- In data ~~structure~~ center / cloud we have hardware for infrastructure.
- Gives VM as service.
  (~~VM~~ Virtual ~~service~~ resources) ⇒ Dependent on physical resources.
  - We can extract virtual resources from physical resources
  - We need to decide OS according to our (end user) requirement.
    1) Windows
    2) Linux
    3) Unix 4) Mac Os

[Microsoft azure virtual machines, EC2 instances, IBM cloud virtual server]

- ~~Which~~ Who will decide which software is need to be installed?

  End user

- User have 2 responsibilities.
  Hardware → cloud responsibility.
- Hardware shutdown → cloud
  data server hurricans, flouds → cloud
  virus to computer → user.

Paas (Google App Engine) Development

Platform is OS. (System software)

- Cloud service provider provides hardware, OS. (2 responsibilities).
- Application → user.
- Cloud is not for personal purpose. It is used for enterprise, business, coorporate, company (they need to maintain servers).
- Thub
  1) Dev Dept
  2) Server Dept
  3) Administrator Dept.

⇒ Cloud service ~~Associator~~ / Engineer (~~CSA~~)
(support) CSA/CSE

Need a server.

- Going to Cloud.
- If We don't know about compatibility with hardware, we need to use Paas.

Saas (gmail, Outlook)

All 3 services.

- http
- file holder
- email
- apas

- Which who will decide which software is need to be installed?

End user

- User have 2 responsibilities.
  Hardware → cloud responsibility.
- Hardware shutdown → cloud
  data server hurricans, flouds → cloud
  virus to computer → user.

Paas (Google App Engine) Development

Platform is OS. (System software)

- Cloud service provider provides hardware, OS. (2 responsibilities).
- Application → user.
- Cloud is not for personal purpose. It is used for enterprise, business, coerporate, company (they need to maintain servers).
- Thub
  1) Dev Dept
  2) server Dept
  3) Administrator Dept.

⇒ Cloud service Associator / Engineer (~~CSA~~)
(support) CSA/CSE

Need a server.

- Going to Cloud.
- If we don't know about compatibility with hardware, we need to use Paas.

Saas (gmail, Outlook)

All 3 services.

- http
- file holder
- email
- apas

Gmail → Google
college → Microsoft
(Only working with service)

Cloud Models :- (C Deployment M)

1) Private PM → VM // Aditya servers.
2) Public AWS, AZURE, GOOGLE cloud, ORACLE etc
3) Community Govt ~~form of public cloud~~
4) Hybrid Public + Private.
(~~any~~ on primises)

① I have data center.
A company that is maintaining it's own servers, VM etc.
- Security PIN outside aditya also.

② Any one can access/login.
(On demand self service)
Any where.

③ For a community. Only for these people.
(Group of people together starts a community and maintains a server for them)

④ Gpay, Phone Pay PCI-CSS standard.
(should not maintain public cloud)
- Don't ~~maint~~ migrate info to cloud.
- Under premises.

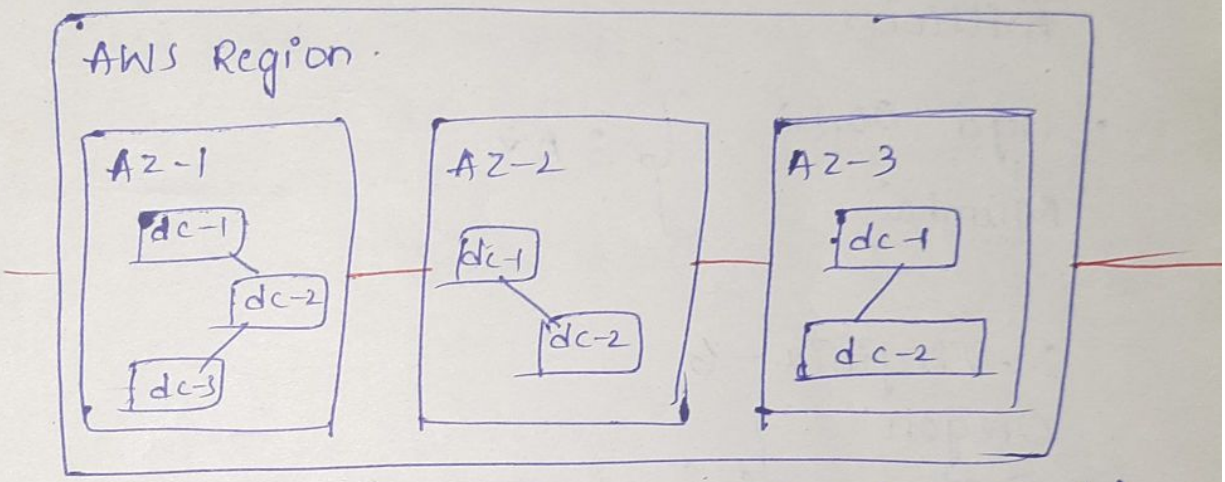
* Aditya
  - private (Normal servers)
  - Microsoft cloud (public)

AWS Global Infrastructure :-

AWS regions
AWS Availability zones (AZ)
AWS Datacenters (DC) - Physical servers - data

1) Geographical location.
   1 region ≥ 3 availabity zone (AZ)
   - Hyd, Mumbai, Virginia, California, Ohio, sydney etc.

2) 1 AZ contains ≥ 2 Data Centers (Individual discrete DC)



(By connecting ⇒ creating huge mesh)

- Networking
  high bandwidth
  low latency
  highly available — fiber optic cables.

Datacenter	very less	Distance. ~~min 100km~~ side by side buildings
AZ	moderate	min 100 km. (replicates data from one AZ to other easily) for security. (Natural calamities)

// Disaster recovery purpose.
down
AZ1 ↕ AZ2 ↑

31 Lamnced Regions.

(No china)

N. Virgina us-east-1
(code)

resources access by

Hyd ap-south-2
Mumbai ap-south-1

- We can select AZ as our wish to launch
- 99 AZ
  100's of DC
  millions
- Hyd 2022 } 3 AZ
  Mumbai

N. Virginia - 6
Oregon } 4
Seoul
Tokyo

Jaya@

Going to launch

1) Canada West
2) Israel
3) Thailand
4) Malaysia
5) Auckland.

EC2 (ECC) // IaaS

aws.instructor.com

- related to server
- server will provide the services. clients will access the services.
- Elastic compute cloud (ECC)
- related to virtual cloud.

Other the AWS VM service.

Services

service categories like compute

services EC2

- Region we want to launch. (local → available → Hyd) Comfortable for users
- Global → N. Virginia

① Instances (Virtual Machines) N. Virginia

Launch an Instance.

- Name to the server.
- Applications and os Images.

Quick sort

select image of OS & versions.

- Need to check that if OS is compatible with the applications.
- According to the requirement, we need to choose best OS.

Instances type:

1) General purpose. M, T
2) Compute Optimized C.
   (CPU power must be more)
3) Memory Optimized R, X.
   (more memory power)
4) Accelerated computing G
   (GPU based) Graphical processing unit.
   3D Games, virtual graphics.
5) Storage Optimized
   (more storage).
6) HPC
   (AIML related)

Instance
- Charges

Launch instance

- Key pair (password) //DR2025
  1) public & private keys.
  2) To connect to server.

  create new key pair:

  ◉ RSA ○ ED25519

  - pem (other terminal)
  ◉ ppk (PuTTY)

file downloaded. // password file.
// one time download
// first time must connect.
// otherwise data is lost.

- Network settings.
  * We can change / select A Z → North virginia
  * We can't select data center

US East 1f
1a
1b
1c
1d
1e.

ssh

Configure storage

8 GB (gp3) → SSD // semiconductor performance (good)
(Micro) HDD (Magnetic)
// performance is low
(pendrive type)

t2-nano

IP adress.

- PUTTY //software.

USERNAME
PASSWORD.

- to connect to this server, we need IP adress
//remotely located server → public IP adress (Internet IP adress).
// private IP adress → Internal IP adress.

Connect to instance.

- SSH → Secured shell → 22 (port)
//confidential data → encrypted mode to provide security
//no hacking.
// encrypting plain text ⇒ encryted mode.
- Port num + IP adress.

SSH → go down → before @

ec2-user

PUTTY

↳ IP adress

↳ SSH (port) [22] very dangerous // plain text.

• SSH ⇒ Auth → credintial.

private key for authentication.

Accept // certificate for security.

Login as:

ec2-user.

⇒ Stop instance. // stopped.

(Instance → Instance state).

• ec2-start – mem, storage, cpu

Incoming connection – free

outgoing connection – charged.

• ec2-stop – mem, storage (charged)

mem dump.

• Delete the Instance // no charges.

Terminate Instance. ✂ check if there is backup or not.

•ppk // PuTTY

⇒ Ubuntu MacOS.

.pem Key value pair.

terminal platform – pem – mobaxterm

~~public ip~~

doesn't accept ppk to pem

• ppk – putty
• pem – terminal
(3rd party) – mobaxterm
other than PuTTY
we can easily copy from our desktop to VM (drag & drop)

Ubuntu

(SSH)

IP adress — Instance ⇒ public

username — Connect Instance go down.

- Advance SSH settings.

  password · pem file.

OS-CONNECTION

- Windows

  * no ssh

  * Windows - RDP (Remoted desktop protocol).

    port no. 3389 - encrypted.

Core edition → No GUI (BASE)

(CLI)

Linux → 8GB
Windows → 30GB

  * public ip → click on instance → public
    username → connect → rdp client → Administrator
    password → decrypt it (Don't allow files)

    [get password]

- PuTTY

  IP adress : ——————

  SSH
  ↳ Auth
  ↳ credintials:

  - Private Key
    (.ppk file)

    [Accept]

  - login as: ec2-user

* Don't give root user, name & password, only give server username & password.

Command mode without PuTTY/Mobaxtren

ssh -i [.pem] ec2-user@[ ]

Keypair. IP adress.

1) Connect ⇒ Connect to instance ⇒ Connect.

① What is server & client

or

② All computers are connected without server-architecture, then this model is called.

③ Centralized administration is possible in.

④ Which one is secured connection model

⑤ DHCP, FTP, DNS, SMTP

⑥ Webserver provides
DHCP server provides,
DNS server provides
File server provides
Mail server provides

⑦ SMTP server provides.

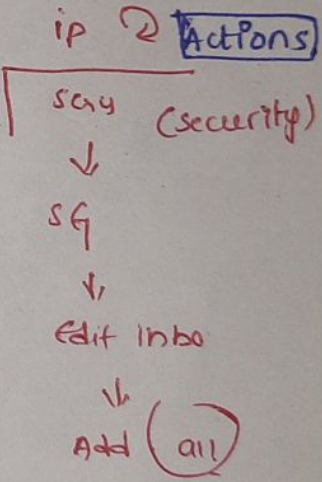
⑦ www.aec.edu.in ⇒ example of which service.

⑧ Which service maps

* The process that creates abstract layer
  // Virtualization
  used to create // hypervisor
* NIST
* Types of hypervisors
* On demand self service
* Resource Pooling
* The characteristic of cloud that enables user to create resources globally whereever they want
* Elasticity
* Pay as you go

---

1. sudo yum update
2. sudo yum install httpd
3. systemctl start httpd
4. systemctl enable httpd.



Activity in codemind
Lab in AWS Academy

How to protect instance?

Actions

↓

Instance settings

↓

- change termination protection
- change stop protection

↓

enable.

Zero down time
24×7
Ex:- WA.
Always must be running

→ Accidently if we stop instance, it won't be stopped. It gives error
// Failed to stop the instance.
- Disable protection.

→ ec2 instance - public ip
DHCP → ip adress is relased by this
// not const (ip) → shutdown → new ip adress is released.
// restart → news public ip is assigned.

→ google must have const ip
aec.edu.in must have const ip
// ip adress if changed → can't be accessed.
// end user don't knows ip adress if constantly changing.
elastic ip → constant ip is mapped.
// static ip address.

EC2 dashboard

↓

Elastic IPs (only 3 ~~hrs~~ ⇒ student account)

↓

Region // same region, IP should be used

↓

Allocate.

- IP address

↓

~~Adress~~ Actions

↓

- Release Elastic IP → to remove
- Associate Elastic IP // to associate to an Instance

chargable // monthly in India

Password 6-

// very difficult, can't remember
// how to change ?
// If password file is deleted ?
// Instance in control panel.

start

↓

run // dialog box

(control)

↓

control panel

↓

user accounts

↓

Manage accounts.

↓

~~change password.~~

~~change an account~~ Administrator

↓

change password.

Lab 3

On-demand Instances
Reserved Instances
Spot Instances
Dedicated Hosts
Dedicated Instances.

① Usecases Examples

1) Variable workloads.
2) Development & testing.
3) Unpredictable workloads.
4) short term projects.
5) Application migration.

→ Cost, Insufficient capacity errors.

- Don't run application having uneven workload
- short term projects, flexibity, stability ✓

② less flexibility, more commitment

- Must use resources since you committed to use.

Linux commands

Open source ⇒ source code is free.

OS

- shell → user
- Kernel (hardware level)

- shell is an interface that makes user interact with hardware (Kernel)
  → Increase volume. (GUI → shell)

Windows → 3 shells.

Shell → GUI, CLI, powershell

- We can execute a task either by using GUI or CLI.
- Powershell → use scripts.

For Linux

shell gnome (gui), shell, bash. [born-aided shell]
(client version, desktop interface)

CLI (server version).
- shell, bash
  ↓
  older.

Mac

shell - unix (kshell)
(Korn shell)

Linux Ps every where - rockets, smart watches, satellites, IOT etc.

- Digital devices → OS → Linux

1) Security (maintained by server) 2) flexibility

Linux commands:-

$ standard user

1) Standard user → root user
(least privilages)
sudo su $ #

2) creating file
cat > filename.
_____
_____
ctrl+z (save)
_____
_____ ctrl+z (not saved)

Windows
Administrator
(can do anything)
• Linux
root.

case sensitive.

3) List of files
ls
ls -l

4) contents of file
cate file1.

5) again cat > filename
• content is replaced.

6) cat >> filename
• append content to file.

7) clear the screen
clr

8) History of commands
history.

9) Calendar
cal

10) date - date
time - time

Linux directory structure.

/ (root folder)

↓

system directories (folder).

↓

user directories.

Windows → drives (file system)

dev, eve, home, root, etc

for server

- etc → save/customize services (install/uninstall)
  dev → devices

- c\user\user envt

  envt variables.

  home → standard user (working envt)
  (how many no's ⇒ 100/200 etc.)

- root → only for root user

11) present working directory.
pwd
/home/ec2-user

- root can ~~use~~ work any directories and lower levels.
- user can't touch other users and upper levels.

12) As a user can't switch
- As a root

change directory

cd

13) one step back

cd ..

17) home → etc

cd /etc

15) make directory

mkdir

sudo su ⇒ # (root user)

Create a directory called dir1 in ec2-user

mkdir dir1

In dir1 create dir2

① cd dir1

mkdir dir2

② ~~cd~~

mkdir dir1/dir2.

③

create dir3 in dir2

mkdir dir1/dir2/dir3

change to boot directory

cd /boot

From boot create a file in dir3.

cat > /home/ec2-user/dir1/dir2/dir3/file1

This is my file.

change to dev directory and read the file content in dir3.

cd /dev

cat /home/ec2-user/dir1/dir2/dir3/file1

This is my file.

From dev, create a new file in dir2

cd /dev

cat > /home/ec2-user/dir1/dir2/file2

This is my file 2

16) @ Just create a file.

touch file1

touch file1 file2 file3

touch file → change the timestamp

17) diff file1 file2

(difference b/w the files)

18) top

(statistics, process, process running, sleeping, tasks etc)

task manager
- statistics

ctrl+c to kill any running process in linux

19) *vim - editor. # default

Vi - older editor, i - input / insert

* nano (new)

- Coming back to read only mode → esc.

shift + : wq (save & exit)

read only mode by default
- i to insert.

Iaas :- hardware (cpu, ram, storage)

personal website content (for website).

Power point software (ppt)
reader s/w (word & doc)
VLC Media player (videos/audio)

Web software - httpd, apache, nginix

OS - amazon linux

hardware (cpu, ram, storage)

allow http

- creating, managing, controlling → root user

users → web s/w.

package manazers

yum → amazon-linux

apt-get → Ubuntu

① Update OS. (sudo su)

yum update

yum update -y (doesn't ask for confirmation)

② install httpd service/ software

yum install httpd (yes/y)

yum install httpd -y

yum - to install & uninstall the service.

③ systemctl start httpd ⇒ optional

(Start the service)

-manage the services (systemctl)

- Personal website content ⇒ public IP

3.87.64.158 ---> website name

(DNS user, ISP)

(goDaddy.com)

- website is not enabled (troubleshoot)

④ ssh-22 (only allowing this)

Now allow http-80

(Must be allowed, to make website appear).

https ⇒ 443

↓

secure

- Change security settings.

select instance

↓

security

↓

security groups

↓

Select on instance

↓

Inbound rules

(SSH enabled)

- Edit Inbound rules

↓

Add rule

↓

HTTP, Anywhere IPV4

↓

save rules.

- Ubuntu doesn't support httpd. (old version).

① apt-get update -y
② apt-get install apache2 -y (http)
③ systemctl start apache2
④ Enable http-80

⇒ amazon-linux -/usr/share/httpd/noindex/index.html.

cat index.html

(edit) vim index.html

/var/www/html/ index.html ubuntu

cd /usr/share/httpd/noindex

cat index.html cat /usr/share/httpd/noindex/index.html

---

cd /var/www/html

cat index.html.

rm index.html

forbidden.

SSH browser menu

/home/ec2-user.

↓

/usr/share/httpd/noindex

copy files

not giving permissions

- root user (#)

- chmod 777 /usr/share/httpd/noindex/.
  (Same in ubuntu)

⇒ permissions to the directory.

full permission.

folder ⇒ index.html
js, css
} ctrl+A
drag & drop

putty complicated

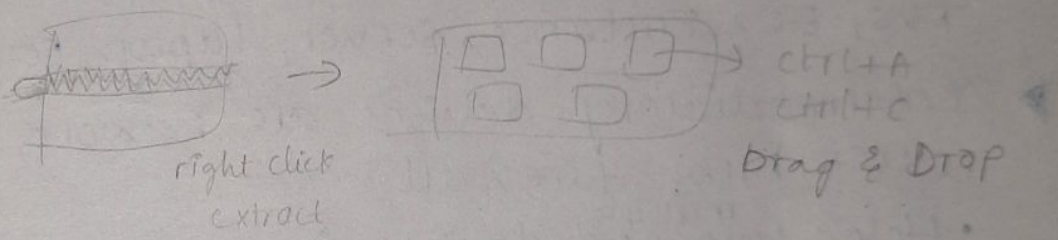
~~SSH browt~~

1) Create Instance (Ubuntu)

2) ① apt-get update -y
② apt-get install apache2 -y
③ systemctl start apache2
④ Give permission http-80 / Anywhere IPV4
chmod 777 /var/www/html
0.0.0/0

3) cd /var/www/html
rm index.html

4) SSH browser
/home/ubuntu
/var/www/html



bash script ⇒ file automation

PWD (print)

nano file1

directories → bleue colour
files → which.

⇒ ls -l (long list, permission)
ls -al (hidden files)

⇒ [root@ip-172-31-93-14 dir1]# rm dir1.

not possible.

cd..
rm -rf dir1.

⇒ chmod (changemode)

Networking

→ ip addresses
→ Basic networking commands.
→ AWS VPC. (design our own network)

* Network access can be controlled by VP
(Virtual private cloud)

- Network - 3 Types
End devices
Intermediatary devices.
Connections.

➡ User who is using End devices ⇒ End
TVs, EC2 Instance, server, laptop, com

➡ Intermediatery devices are network, s
router, hubs, firewalls
- Helps ~~two~~ multiple end devices to connect.

➡ To make sure end devices to connec
use connections i.e; cables, wifi

Submarine cable map.

https://www.submarinecablemap.com/

- fibre optic cables ⇒ optical (light)
(underneth the seas & oceans)
- No one owns internet.
To connect with Google ⇒ active browser
~~inter~~ net
connecti
- Internet (untrusted network)
Intranet (~~ont~~ own server)

logical things – ip address. (call to another comp, machine, ...)
language – protocol (mediator)

* ssh protocol 22
  http protocol 80
  https protocol 443
  RDP protocol 3389

- In windows (case insensitive)

* ipconfig → to check details of comp (ip address)

  IPV4 address . . . . . [ ]

  * Bluetooth, hotspot, wifi has diff ip adresses.

  * ping → ping to any end device.

    ping www.google.com. (connectivity check)

  - pinging www.google.com [142.250.205.228] with 32 bytes of data.

    (To troubleshoot / rectify the problems).

    ____
    ____
    ____
    ____ } 4 times requests.

    (default)

→ ping www.facebook.com.

maximum of 30 hops

- In how many devices, end user is connected to devices.

→ load balancer (directs to a server)
Not everyone connects to same server

→ ec2 · instance - public ip ·
request
~~server~~ timed out (ping)
Website is reflecting ·

→ ping protocol, tracert ⇒ icmp protocol
(Internet control messaging protocol)

security groups
↓
Edit Inbound rules
↓
Add rule ·

- ipV4 address → 4 parts
ipV6 address

ip → internet protocol ·

1) ipV4 address
Every part is called octet ·
(8 bits) → 32 bits · total
- 4 octets/parts seperated by dot
- 32-bit binary address ·

00000000 · 00000000 · 00000000 · 00000000

0 · 0 · 0 · 0

11111111 · 11111111 · 11111111 · 11111111

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

Octet min number = 0
max number = 255

range (0, 255)

⇒ 11111111.11111111.11111111.11111111
255.255.255.255.

- Any website in world used ipV4 address.

⇒ 10101010.01010101.00001111.00111100
170.85.15.60

⇒ standards og, iso, iana, ietf

* ip address is also called as logical
version 4 - changable.
ipV4 - logical address.

* MAC address - physical address
(Media access control)
48-bit hexa decimal address
- cannot be changable
- Every physical machine has MAC address
→ provided by manufacturer - on mother board/chip.
- Command to see it → getmac
- Hexa decimal accepts -, : . (hyphen, colon)

* ipaddress + MAC address

ipconfig /all

ipaddress x → not connected.

When disconnected to internet → ip address

- 10101010.01010101.11001011.00110100.

128 64 32 16 8 4 2 1

170.85.203.52

⇒ IP V4

5 classes.

a b c d e.

using in networking

1st octet number ⇒ 0-127 (a class)

128-191 (b class)

192-223 (c class)

Unicasting (1-1) dedicated casting

multicasting 224-239 (d class)

rkd, special use 240-255 (e class)

- 25.78.78.250 not in range of octet

(Invalid)

- d class ⇒ subscription based (group of mem opt for something)
  - set off boxes, dish.
- e class ⇒ for standards.

How to write ?

① a class 0-127

N.H.H.H

N → network

H → host

something that do not change (network)

something that change (hosts)

Lab 1 ⇒ com 1, com 2 .... com 70

(network) (hosts)

N → must not change

H → changes.

No IP has 0. 1.0.0.0 / 1.0.0.1

② ~~b class @ 128-191~~

1.0.0.0

1.0.0.1 (switching)

1.0.0.2

⋮

1.0.0.255

1.0.1.255

1.0.2.255

⋮

1.0.255.255

1.1.255.255

1.2.255.255

⋮

1.255.255.255

~~2.0.0.0~~

~~2.255.255.255~~

~~127.255.255.255~~

Occupancy

1.0.0.0

1.255.255.255

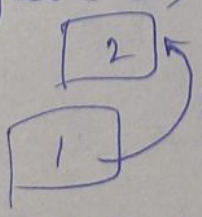
2.0.0.0.

↳ lab changed

① should not be changed to ②

③ To communicate with 2nd lab, we need to open gate/route and enter into another gate ⇒ gateway

Router/gateway.



- Within the network, for communication we can use switch (gate switch)

IP's ⇒ 256 * 256 * 256 (3 octets)

~~1 3 x 2 5 6~~ = 1,67,77,216

~~1 6 8~~

Network number 1 has IP's

1,67,77,216 → 1

1,67,77,216 → 2

⋮

1,67,77,216 → 127.

• 127 x 1,67,77,216 in class A.

② b class [128-191] only for 1st octet.

128.0.0.0 — 128.0.0.255

128.0.1.255

(128.0.255.255)

— 128.[1].0.0 (network change)

~~128~~.

IP's ⇒ 256 x 256

= 65,536 (1 Network)

128.1.0.0 → 65,536

[191.255.0.0 ↔ 192.255.255.255]

b class IP's ⇒ 64 x 256 x 256 x 256

⇒

③ cdass 192-223

n.n.n.h

192.0.0.0 _ 192.0.0.255

Same network ⇒ 256

C class IPs ⇒ 32 × 256 × 256 × 256.

→ • 256 comp → C class

10000 comp → b class

>65000 comp → a class.

70000

More networks ⇒ C class

More hosts ⇒ a class.

Q) 192.78.95.78 ©

100th (host) from above network

from 0

192.78.95.098

78
100
178

If 100th N/W

192.78.195.098 (c class)

• 256th IP

192.78.95.255

• 257th IP

Q) 10.78.98.89 (a class)

257th in network 10.0.0.0

~~10.78.1.0~~

10.0.1.0

Q) 172.89.65.96 (b class)

100th in N/W

172.89.0.0 (N/W)

⇒ 172.89.0.99.

* 10.78.98.56 – 10.86.255.244.

same N/W → communicates
→ can ping

* 10.78.98.56 – 11.86.255.244

(a class ⇒ N.H.H.H)

* 192.168.90.254 – 192.168.91.254

(c class ⇒ N.N.N.H)

N/W changed.

* 128.9.70.89 – 128.8.80.89

(b class ⇒ N.N.H.H)

N/W changed.

communication is not possible.

Subnet mask

a – 255.0.0.0 (default)
const/fixed open
N.H.H.H

b – 255.255.0.0 N.N.H.H

c – 255.255.255.0 N.N.N.H.

IP address + Subnet mask → IP stack
(is used for communication).

→ Humans → ip address
computer → subnet mask.

N/w IP address

192.168.90.67 — 192.168.91.67

255.255.255.0 — 255.255.255.0

⇒ Cisco packet tracer

pick and drop.

- PCs, switch, copper straight through, fast ethernet

- IP configuration

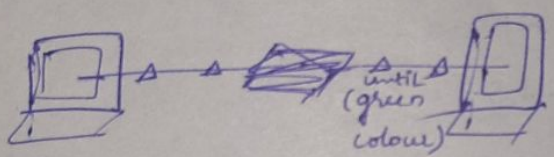
Comp ⇒ desktop ⇒ IP configuration

IPV4 → tab.

- command prompt

ip config.

ping [ ] connected/not



192.37.90.67 — 192.37.90.58

→ IPV4 system ⇒ specialised/ reserved ip addresses are present.

Iana – Internet assigned numbers authority

(iana.org)

* network id → first ip in the network
broadcast id → last ip in the network

- id → only for identification purpose (unusable ip)
- only for reference.

10.0.0.0 net id
10.255.255.255 broadcast id

In 256 × 256 × 256, 2 are not allowed to use.

c class
192.168.10.0 net id
192.168.10.255 broadcast id

b class
128.0.0.0 net id
128.0.255.255 broadcast id

0-127
128-191
192-223

176.87.78.90

(b class)

176.87.0.0

- 100th usable ip → 176.87.0.100
- last usable ip → 176.87.255.254

Q) 126.98.87.90

256th usable ip

126.0.0.0
126.255.255.255

126.0.0.0 → unusable

255

126.0.0.255

~~254~~

126.0.1.0 → 256

126.0.1.1

126.0.1.2

Q) 192.168.90.89 (c class)

255th usable.

192.168.90.0 ⊗

⋮ } 254

192.168.90.255 ⊗

255th → not available.

• 128.50.90.89 (b class)

128.168.0.0 ⊗

⋮

128.168.255.255

256+254 = 510

128.168.0.0 → ⊗

⋮ } 255

128.168.0.255

128.168.1.0 → 256.

subnet mask ⇒ 255.0.0.0 (a class)
255.255.0.0 (b class)
255.255.255.0 (c class)

Unusable ids → 127.0.0.0
127.255.255.255 } a

128.1.0.0
128.1.255.255 } b

192.0.9.0
192.0.9.255 } c

0-127 a
128-191 b
192-223 c
224-239 d
240-255 e

(a class) 127.0.0.0 — 127.255.255.255
complete range — loop back purpose.

(b class) 169.0.0.0 — 169.254.255.255
complete range — apipa.

** communication ⇒ hardware + logic
Loop back :-
- ip stack ⇒ self pinging ip address.
  127.0.0.0 (ping)
  self - 127 wifi/ethernet is problem, it will not ping.
- health status of a wifi card/ethernet card.
  ⇒ local host
- Without any wiff/ethernet connection

Linux

SSH → 22 (default allowed)
http (web browser traffic)

- ICMP → to ping public ip
  (Internet control messaging protocol)
  tracert, ping works, when icmp is enabled.
- nacl
  (Network access control ~~protoco~~ list)

Loob back
127.0.0.0 (always active)

apipa → absence of dhcp server, os gives
(automatic private ip addressing) 169.254

dhcp
(dynamic host configuration protocol).
↳ server

Application
os
hardware

- defaultly installed in os (dhcp server) → wifi, laptop.
- ssh → linux
  RDP → windows

Assign ip address

run → ncpa.cpl

Ethernet
↳ properties
↳ TCP/IP 4
↳ properties
↳ Use the following ip address

→ Giving manually (static assignment, static ip address)
- Human errors

→ DHCP Servers gives ip address (end device)

Server
↳ services
↳ DHCP
↳ service
on

Desktop
↳ give ip address to make it work (static ip)

Select range

192.168.10.2

DHCP server 192.168.10.1

Users 6-100

253 (c class)

1 → network ip
1 → broadcast ip
1 → server

⇒ hosts ⇒ desktop → ip configuration

DHCP

DHCP → 1Q for interview

① DHCP is default enabled in laptop when we connect to internet, ip is generated automatically.

⇒ DHCP server failed/down.
ip adress is given by apipa.

- ip configuration
  - ↳ requesting ip address
    - ↳ DHCP failed. APIPA is being used.

- When DHCP fails, OS generates a random ip address given by

169.254.__.__

Process is called APIPA

When ip is not assigned/exhausted.

- 169.254.__.__ (reserved in b class)

Private IPv4 Address Space:

Class	Address Range	Network Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

private ip addressess - intranet (with in the clg, with in the lab)
public ip addresses - internet ips
(designed by iana)
↳ internal / private purpose.

- When an EC2 instance wants to connect to another EC2 instance, we use private ip addressess.
- Organizations, lab → private
  jio, ~~set~~ idea etc → public
- Servers (2 ip address)
  - private → to another server
  - public → to any other device.

⇒ EC2 instance (No public IPV4 address is generated)
↳ Network settings → Edit
↳ Auto-assign public IP (Disable)

1-127	10.0.0.0 - 10.255.255.255
128-191	172.16.0.0 - 172.31.255.255

Neither private/public (a class)

127.0.0.0 to 127.255.255.255 (loop back)

subnet
internet gateway (router)
routing table
nat

out of this network to the world.
(internet)

→ Transfer to internal N/W → routing table.
(Intranet gateway)

Router

SUBNET :-

Subnet mask → computer identifies host and network octet by comparing each bit.

- It checks whether source and destination are matching or not.

10.67.89.90 → S ← 11.67.89.98

255.0.0.0 — must be const — open no (n/w)

255.0.0.0

(Diff networks → no communication)

- Using all default values → classful ~~subnet~~ ip address

Classless ip address

Subnet

matching bit - 1 - N/W

ignore bit - 0 - host

→ Subnetting

10.0.0.0 network

255.0.0.0

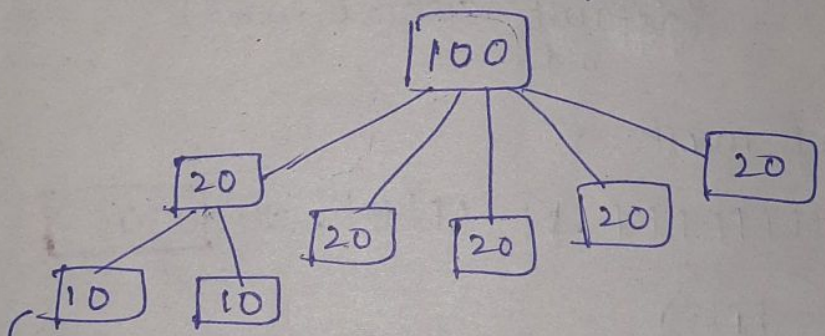
For 10.0.0.0 N/w → 1670000 + host can be connected.

- If one router, manages then performance decreases and security decreases.
- If hacker enters N/w, if one computer is hacked all 1670000 computers are hacked.
- In terms of cloud, computer → server
  - server down.

- Split big N/w to small N/w's (subnetworking)

* 3rd floor → 5 bays
  classes → 5
  seminor → 1 (no partition door)

- Down time reduces, performance increases



If one server down, only 10 are effected.

255.0.0.0/8
255.255.0.0/16
255.255.255.0/24

/ value → only N/w bits (matching bits)

Q) 192.168.10.0 254 usable

255.255.255.0/24

Subnetting ⇒ 30 servers
(management/sr Administrator says)

30 ⇒ 20 needed + 10 backup.

① Requirement → 30 servers (30 ip addresses)
Host

② ip − 2^h
(nearest 2^h value)

$2^5 = 32$ [We can take more 2^n if exact value is not available]

$2^h - 2 = 32 - 2 = 30$ ips
network id & broadcast id

③ new subnet mask

30 ⇒ C class ⇒ 255.255.255.0/24
(default subnet mask)
old.

new subnet mask →

11111111.11111111.11111111.00000000

$2^5 = 32$ (5 bits)

255.255.255.11100000
change to N/W

255.255.255.224 / 27

④ How many networks = $2^n = 2^3 = 8$
How many hosts = $2^h = 2^5 = 32$

n → no. of bits converted.

111

$2^3 = 8$

⑤ Writing range → 30 $2^h = 32$
(inclusive)

192.168.10.0 – 192.168.10.31 (+31)
192.168.10.32 – 192.168.10.63
192.168.10.64 – 192.168.10.95
192.168.10.96 – 192.168.10.127
192.168.10.128 – 192.168.10.159
192.168.10.160 – 192.168.10.191
192.168.10.192 – 192.168.10.223
192.168.10.224 – 192.168.10.255

each one has 30 hosts. (32).

8 networks = 2^3.

⇒ 192.168.10.96 – 192.168.10.127

192.168.10.224/24.

① Host requirement
② nearest 2^h value
③ new subnet mask
④ Identify N/W and hosts
⑤ Write range.

Q) Requirement → 60

① Required → 60
② Nearest 2^h value $h = 6$

32 (64) ✓

$2^h - 2 = 64 - 2 = (62)$

60 ≤ 62 ✓

③ New subnet mask

(256) 60 ⇒ C class ⇒ 255.255.255.0

11111111.11111111.11111111.00000000

11111111.11111111.11111111.11000000

255.255.255.192 / 26

128
64
192

④ No. of N/W = $2^2 = 4$

No. of hosts = $2^6 = 64$

⑤ Writing range (+63)

192.168.0.0 – 192.168.0.63

192.168.0.64 – 192.168.0.127

192.168.0.128 – 192.168.0.191

192.168.0.192 – 192.168.0.7

192.168.0.0 – 192.168.0.63

192.168.0.64 – 192.168.0.127

192.168.0.128 – 192.168.0.191

192.168.0.192 – 192.168.0.255

network id

broadcast id

N/W id	Broadcast id.
192.168.0.0	192.168.0.63
192.168.0.64	192.168.0.127
192.168.0.128	192.168.0.191
192.168.0.192	192.168.0.255

(Invalid)

Q) Requirement => 1000

① b class

② Nearest 2^h value

$1024 = 2^{10}$

$h = 10$

$2^{10} - 2 = 1022$

③ New subnet mask

b class => 255.255.0.0

11111111.11111111.00000000.00000000

11111111.11111111.11111100.00000000

255.255.252/22

④ No. of changed bits = 6 (n)

No. of N/w = $2^6 = 64$

No. of hosts = $2^{10} = 1024$

1023

128.10.0.0 - 128.10.0.1023

128.10.0.1024 - 128.10.0.2047

128.10.0.2048 - 128.10.0.3071

128.10.0.3072 - 128.10.0.4095

128.10.0.4096 - 128.10.0.5119

128.10.0.0 - 128.10.3.225

128.10.3.226 - 128.10.7.225

128.10.7.226 - 128.10.11.225

128.10.11.226 - 128.10.15.225

$2^n/256$ $1024/256 = 4$ (block)

0
1
2
3 → 4th b

172.16.0.0 - 172.16.3.255

~~172.16.3.256~~

172.16.4.0 - 172.16.7.255 (+3)

172.16.8.0 - 172.16.12.255

172.16.13.0 - 172.16.16.255

⋮

(64)

Q) 172.18.20.48/28 → last valid host.

255.255.0.0 (32)

~~172.18.~~ 172.18.20 → 0-15, 16-31, 32-47, 48-63

11111111.11111111.11111111.11110000

2^{28} = $2^4 = 16$

172.18.20.48 - 172.18.20.63 broadcast

62 (+15)

→ classless ip addressing

10.0.0.0 250

Subnet mask :- 255.255.255.0 (256)

VPC → virtual private cloud.
(private network)

AWS → public n/w

10
172.16 - 172.3
192.168 - 192.168

127
169.254

- 10.0.0.0/8 1.6 million ip hosts.

10.0.0.0/24 255.255.255.0/24 . 256

10.0.0.0/24 255.255.255.0/24 256

10.0.0.0/8 VPC 1.6 million.

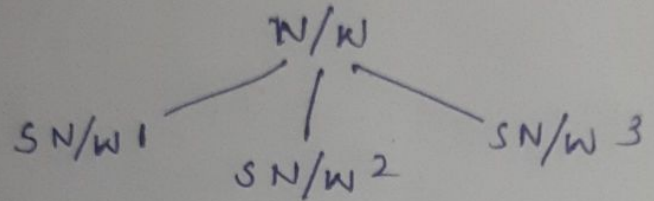
10.0.0.0/24 — 256 (254 hosts)

10.0.1.0/24 — 256

Split the N/W into sub networks (Required 2)

Value $\propto \frac{1}{\text{hosts}}$

VPC is a big network.



Once VPC is created, it can't be scaled.

We need delete it and resources are lost

once VPC region is created, can't be changed

64 — 10.0.0.0/26

2^6

8 — ~~10.0.0.0/29~~

2^3 SN/W /16 – /28

Q) 10.0.0.0/24

60 requirement

4 subnetworks

64 (2^6)

10.0.0.0/26 — 10.0.0.63 ... 32

10.0.0.64/26

10.0.0.128/26

10.0.0.192/26

1). Resources to create.

Networking & content Delivery

- VPC only

/8 ⊗ /16 - /28

2) Name.

3) CIDR (classless Inter Domain Routing).

Big N/w

10.0.0.0/24. (Before Q).

for

- VPC, DHCP server releases IPs.

Subnets

create subnet

↓

select the VPC (aec-VPC)

VPC ID

Subnet

↓

Subnet 1 — 10.0.0.64/26

Subnet 2 — 10.0.0.128/26

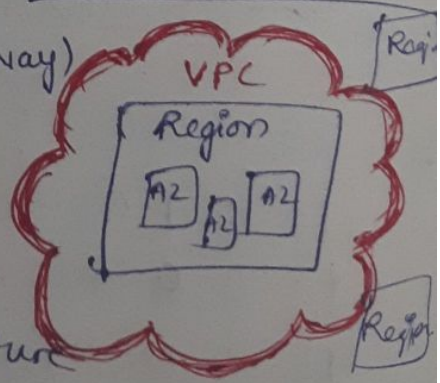
IPV4 CIDR block

VPC is region specific, we can create in multiple & diff AZ's but not in diff region

create

64 → 59 (-5)

- Router (Gateway)
- DHCP server
- Network ID
- Broadcast ID
- 1 reserves for future



/16 - /28

/8 is not possible

Req → 2000. 2048 = 2^{11}

172.20.0.0/16 VPC

subnet 1 → 4th

subnet 2 → 5th

4
4
4
4
4
2

11 hosts

32 - 11 = 21 N/W

21 networks.

2048 / 256 = $2^{11}/2^{8}$ = 8

(+20)

172.20.0.0/21 – 172.20.0.20/21

172.20.0.21/21 – 172.20.0.41/21

172.20.0.42/21 – 172.20.0.62/21

172.20.0.63/21 – 172.20.0.83/21 →

172.20.0.84/21 – 172.20.0.104/21 →

256 × 8 = 768

172.20.0.0/21 – 172.20.7.255/21 (+7)

172.20.8.0/21 – 172.20.15.255/21

172.20.16.0/21 – 172.20.23.255/21

172.20.24.0/21 – 172.20.31.255/21

172.20.32.0/21 – 172.20.39.255/21.

→ 10.0.0.0/16 VPC (200)

2nd & 3rd subnet

128 + 128 = 256 2

256 ⇒ 2^8 255.255.255.0/24

11111111.11111111.11111111.00000000

hosts = 2^8

N/W = 2^{24} 24 N/W

10.0.0.0 - 10.0.0.255 (256)

10.0.1.0 - 10.0.1.255

10.0.2.0 - 10.0.2.255

private servers

we private ip (with in the organization)

- internal

public servers (ICICI)

uses public ip

- Websites connecting in internet
  (https://www.google.com)
  https://www.aec.edu.in
- facebook, instagram, youtube.

* codemind → public codemind.io
  - ↳ got website (public)
  - ↳ icici x (can't login) Aditya student ✓ (can login)
  - ↳ Credentials (username, password)
    Database (private)
    (2 Her application)

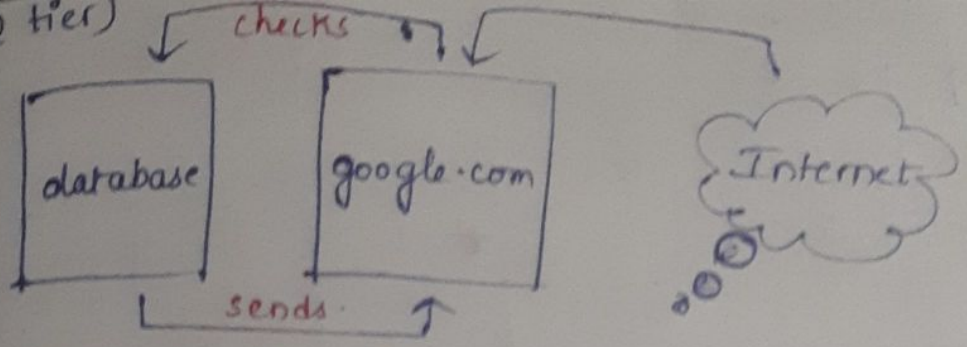
* codemind → application public server
  → database private server

(diff servers
- server down
- security, hacked)

For google → website (app)
→ gmail (database)

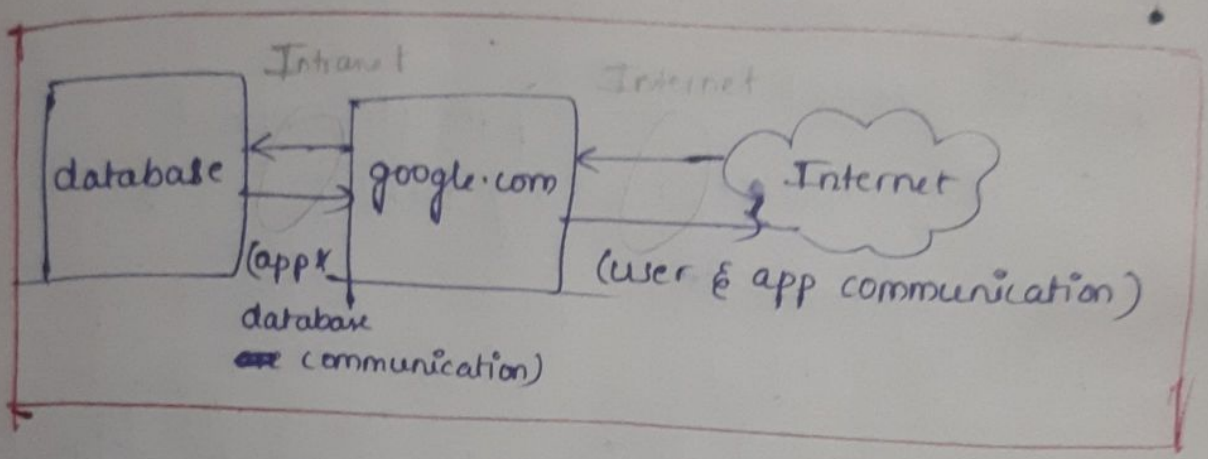
Q) If we are giving password, username How can we access without internet?

(2 tier)



(not facing internet, facing application)

- Database server is connected with application server. (although it doesnot use internet).



database ⇌ codemind.io ⇌ internet
(frontend application)

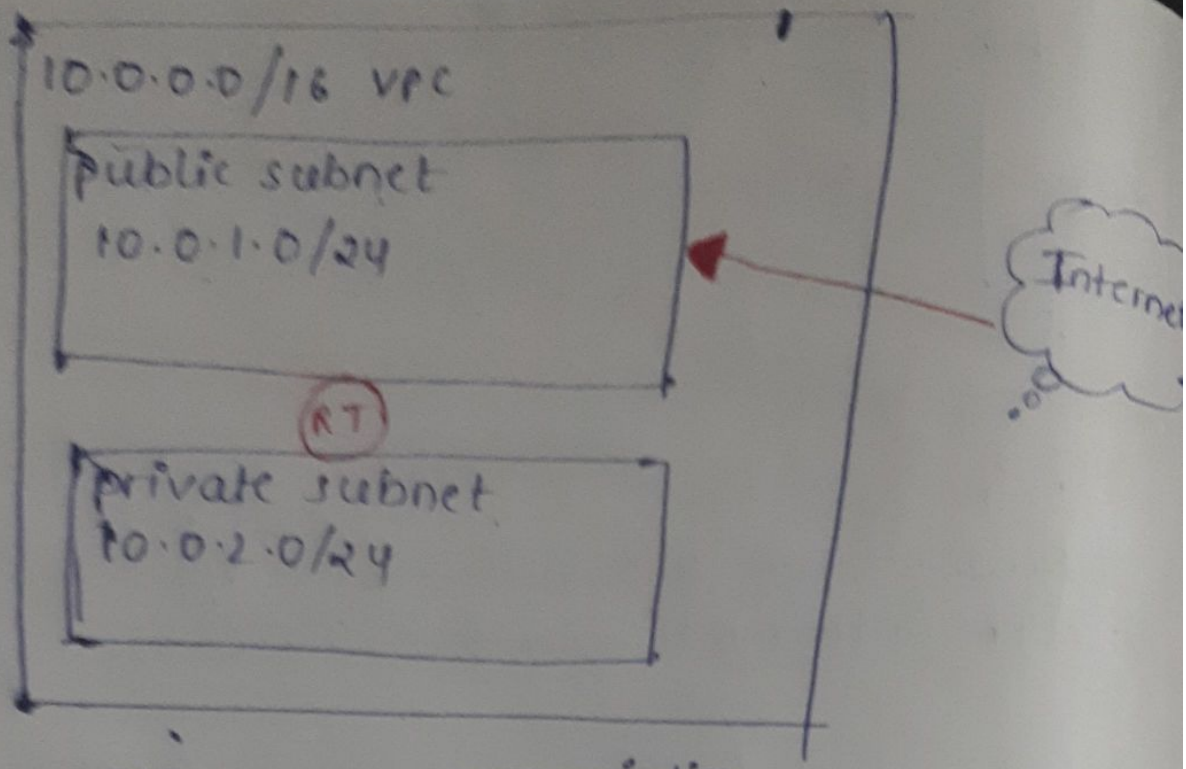
- our info comes from database

Hackers  database codemind.io internet

bypass

- Demands only saying that they will crash the server

→ Subnetting ↗ public server (App)
↘ private server (Database)



public subnet ⟶ communication ⟶ private subnet

[Gateway, router/routing table]

Q) How to create private subnet or public subnet

select ↓ Actions ↓ Edit subnet settings ↓

Give availability zones (diff)

Enable auto-assign public ipv4 address

(To make it public ipv4)

steps :-

- VPC
- 2 subnets → private
- change one private to public
- Routing table (local N/W)

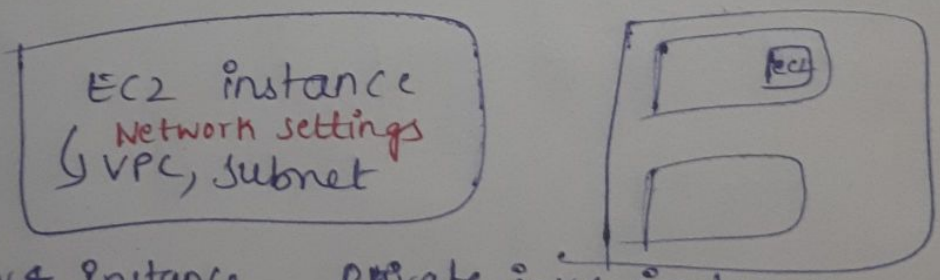
Route table 6-

create Route table
↓
Name
↓
select VPC
↓
create

Establish connections

- click on link
↓
subnet associations
↓
Edit " "
↓
select
↓
Save

→ Want to see route ⇒ click on link
↓
route.

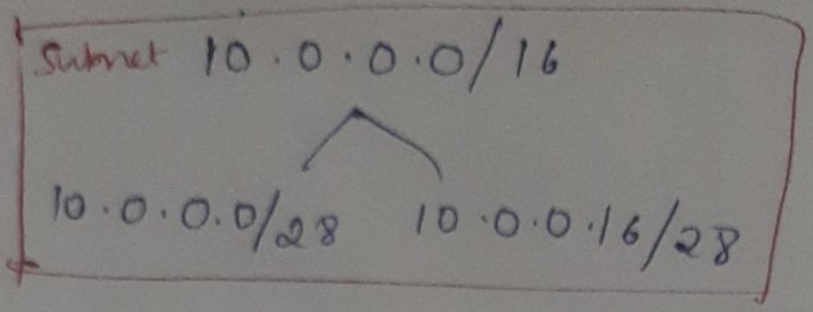


public ipv4 instance — AWS

private ipv4 instance — DHCP

- Enable

icmp traffic [ping public ipv4] ✓



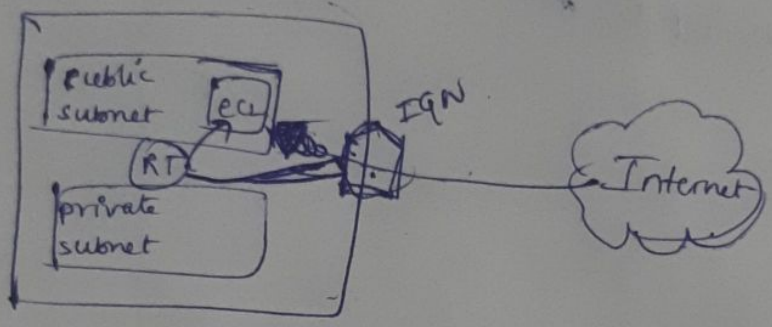
(16) 24

32-4
=28

* Between N/W → it will ping (:RT)
  ~~Test~~ cmd ~~(cn~~ → doesn't ping.
  (No connection established)

- Internet gateway

  Connection b/w internal & external N/W's



- ~~Create~~ internet gateway
  ↓
  Create internet gateway
  ↓
  name ~~ges~~ ✓

→ Attachment
  Internet gateway
  ↓
  Attach to VPC

- Internet → IGW → RT → public subnet

Route decides where to go :-

RT → Pd
↓
Routs
↓
edit
↓

add
↓
destination (0.0.0.0/0)
↓
~~create~~
Target (igw) → create

Source → IGW
(Target
Destination →)
Every ec2 instance

Now it will ping

- If route is deleted, it will not ping
  (It is dropping the connections)

ping ○ -t (∞)
ping ○

→ VPC

1) free of cost.
2) can't be extended to another region.
   (within the region)
3) 5 subnets are excluded.

Q) 172.170.0.0/24 → 50 requirement.
subnet 2, subnet 3.

64
(5)
59

A) 128 ⇒ 2^7 /25

32-7 = 25

172.170.0.0/25 — 172.170.0.127/25
172.170.0.128/25 — 172.170.0.255/25 → public
172.170.1.0/25 — 172.170.1.127/25 → private

N/w changed
/26

2^6

32-6 = 26

172.17.1.0/25

!!!!!!

public subnet → ping ✓
private subnet → ping ✗
from public subnet to private subnet → ping ✓
→ login to linux/Mobaxtreme

De-associate the private subnet from RT, assign elastic IP to private EC2 → ping to elastic IP (public ip of private)
public ip ✗

⇒ Reallocate private subnet to RT ✓

⇒ Dettach Internet gateway
1) public ip from public ~~subnet~~ server ✗
2) public ip from private server ✗

① From CLI, EC2 instance present in public subnet will ping.
② From CLI, EC2 instance present in private subnet will not ping.
③ If we connect ~~priv~~ EC2 instance present in public subnet and then ping private subnet, it will ping.

172.18.0.0/25 /24 50 64 (26)

172.18.0.0/26 - 172.18.0.63/26

172.18.0.64

32-
=26

172.18.0.0/25 → 2^7 = 128.

VPC => /8 /16, /24

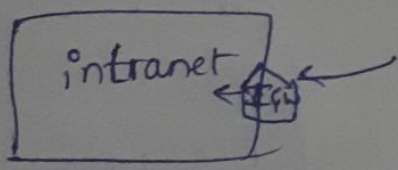
S/W ⇒ /16 - /28

→ Communicate b/w two networks → router/gateway

(either subnets / network)

→ Internet gateway

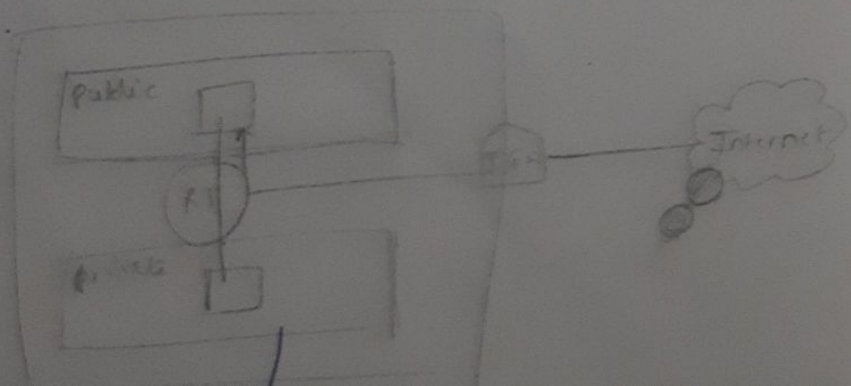
Router, (or) gateway b/w internet and intranet



Routing T → SN
• If we ask something
→ They OK (drop)
→ They x (route)

• IGW goes to RT (sign board), to make connection with any ec2 - instance.

* If subnet is not associated and route is not associated, packet is dropped.

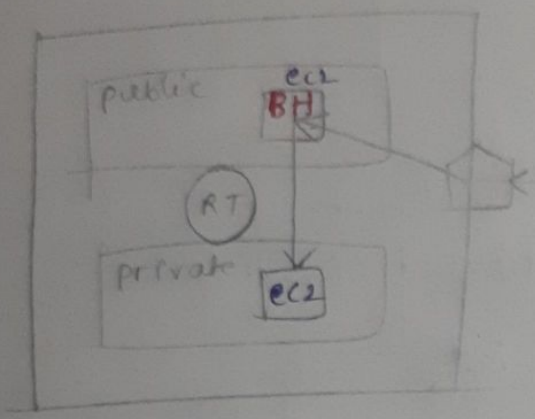


• Backup of the database ?

⇒ Should not give public ip / elastic ip (risk) Hackers. Secure

⇒ **Bastion Host** (public ec2)

The Host that is used to go to private instances



• pem file

ssh -i <Key file> ec2-user @ <ip address>

ssh -i <Key file> ubuntu @ <ip address>

• Key file of ~~public~~ private ec2

connect to public ec2 instance

↓

ssh -i <key of private> ec2-user@private ip

↓

⇒ 172.18.0.0/16

255.255.0.0 VPC (B class)

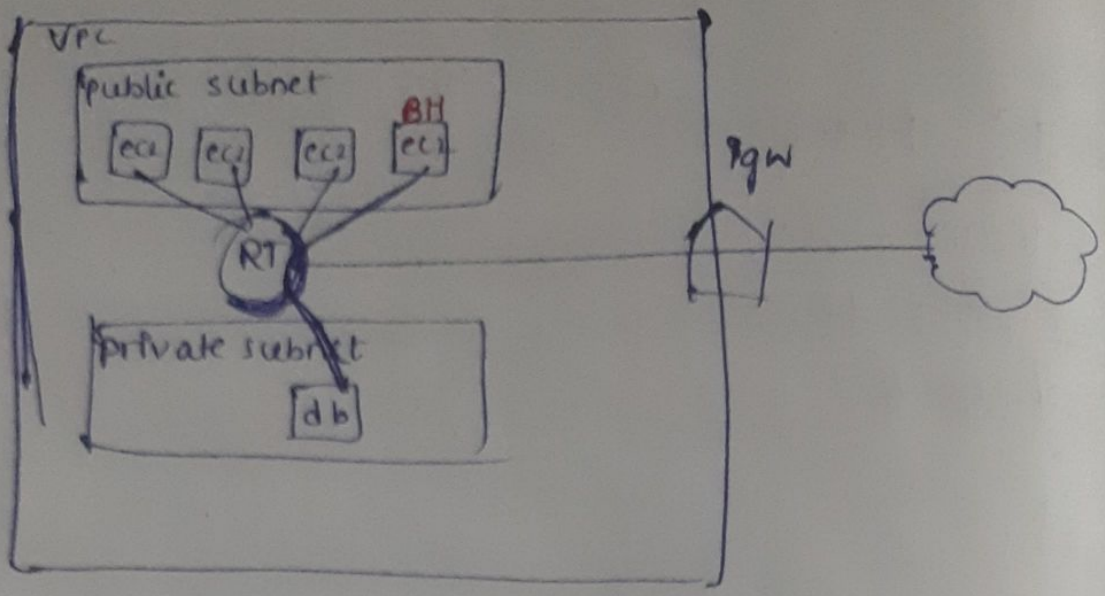
2^{13}

1) Public subnet
172.18.0.128/19

2) Private subnet
172.18.0.256/19 ⊗
1.0

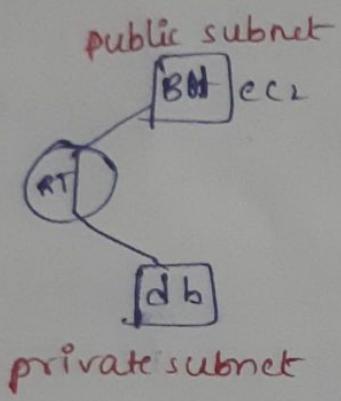
32 - 19 = 13

25 7



- for a secure connection to database server, we use a Bastian host. (dedicated ec2 instance).

  BH → either ssh or ~~http~~ icmp.



---

sudo su

1) ifconfig

172.18.0.60 → private ip of public server

. To know it is a public server

ping www.google.com

⇒ upload key file to /home/ec2-user
/home/ubuntu

* After work is done, ⇒ exit
(back to public server).

- To upload ... subnet we need to expose to the internet
  → But I don't want to give public ip.

  NAT gateway

  → computer can go to internet (1 way traffic)
  Network Address Translation.
  → public IP, Internet gateway (2 way traffic)

NAT → Network Address Translation
DNS → Domain name system
(maps name to ip)

Ex: name maps with mobile number.

- NAT gateway →
  Translation b/w public ip - private ip
  private ip - public ip.

⇒ Subnetting 1) security
2) Performance
3) Reduce ip address wastage

⇒ private server (Isolated → no public ips)
- Used bastion host to connect public ec2
- for updation of db server, we need internet but ~~they~~ there is no way to interact with internet. So, occassionally db server gets connected to internet using NAT gateway.
- If public ip is provided ⇒ security is lost but NAT gateway gives security
- Big organization ⇒ 200 servers ⇒ 200 public ips (It will charged)
  But by using NAT gateway we will be charged for only 1 public ip (i.e; it creates only one public ip).
- Acts as firewall (allows only authorized (auth) connections)

(request and reply)

INTRANET .... FIREWALL ..... INTERNET
(Trusted) (Untrusted)

- REQUEST google → google.com
  (Intranet / Internal N/w) (Internet)
  ← REPLY from google server
- If we don't send any request but also ~~they~~ we are getting REPLY from server (trying to connect out internal N/w) ⇒ firewall stops the connection. [drops the connection]
- NAT GATWAY acts as basic firewall.

Celebraty (user) — request → Security person — reply

  - One way connection
  - If we are requesting, update comes.
  - NATE gateway maps 15 ips to 1800 ips (users)
    ↳ translation.

⇒ NAT Gateway
↓
Create NAT Gateway
↓
name, subnet (public)
[∵ we need to connect a NAT Gateway to primary ~~public~~ ~~sear~~ ~~internet access~~) where internet is coming]
↓

Internet Gateway
↓
route table
↓
public subnet

connecting (public)

↓

② Allocate elastic ip

↓

create

(2 mins to create & activate).

① Elastic ip create, attach to NAT Gatway

Add route

Route table

↓

select

↓

Deassociate private subnet (Subnet associations)

- Create a new Route table for the private subnet

Create

↓

associate private subnet

↓

Add route

(0.0.0.0/0) (NAT gateway)

1 Route → 1 destination

0.0.0.0/0 already exists.

Private subnet is not required for Internet Gatway

⇒ Remove it

For NAT Gatway, we need ~~public~~ private subnet

→ create NAT gateway
→ de associate private subnet from route
→ Create new route with private subnet
→ route from NAT gateway to 0.0.0.0/0

nat - priv - Internet

private - elastic ip → ssh

⇒ NAT Gatway drops the connection for private ec2 elastic ip → doesn't ping, doesn't connect to mobaxtreme (ssh)
(basic firewall)

apps.technicalhub.io : 31/thubfeedback

74988302

EC2 Instance → AWS compute service.

IAM services → (Identity & Access Management)
AWS security.

- User is protecting data. (any type of data → bits type / encrypted / plain text) format

3 types of data

Data In Process → Process /os / Background process
Data ~~At~~ rest → H/w (or) storage ~~device~~.
Data in transit → sending through N/w in the form of (electrical signals / Light signals / wifi signals).

- Bastian host, ec2 instance → resources. (falls in any of the 3 categories)

AWS services
↳ If a server is shut down
Who's responsible ?
Let's explore

AWS Security (Whom to blame ?) [5 que in certification exam]

CSP is responsible for security of the cloud.
EC (End User) is responsible for security in the cloud.
Responsible for cloud infrastructure.

- As a Indian User, we have no access to China Region. (Internal compli conflicts)
- Rules of Internal Govt.
- Physical protection for not having future use.
  → VPC ⇒ china is available. (own risk)
- AWS makes sures ~~th~~ to isolate swiggy & Zomato if in ~~ec~~ same EC2-Instance (or) data centers.
- n no. of security attacks (to see other ec2 instances)

→ User (In the cloud)

- Selecting OS
- patches / licency / OS → users responsibility & answerable.
  (not updating, os hacked)
- All traffices opened → db is compromised (User responsibility)

  Bad N/W by user.
- ec2 stopped → AWS responsibility.
- credentials → users responsibility.

→ The firmware (physical) of server problem
1) User
~~2)~~ AWS

→ EC2 Instance → update
~~1) User~~
2) AWS

Managed service – AWS RDS DB – PAAS

- OS update [AWS responsibility]
- AWS shared responsibility model.

IAM →

Users → root (super user/owner)
→ standard

- Full access / control everything (root user ⇔ administrator).

2 types

1) root
2) IAM user (standard) < IAM user, IAM admin.
   - can't have all permissions.

Windows
Administor
guest (standard)

Android
root
standard
(rooting to get access of standard apps)

---

* root – full control
  IAM admin – full control by root

let three users — root (teacher)

storage Administrator (sports CR) — ec2 Administrator (study CR) — VPC Administrator (cultural CR)

- can delete AWS account? No.
- AWS ⇒ standard user.
  credit card ⇒ root user
- root is a sensitive account.

Root account

- closing the account (all are deleted with one click)
- paying the bills
- IAM admin → limited access provided by root.
  (2 users, 2 groups)
  (limited security)
- download aws cli

cmd → aws configure

AWS Access Key ID

→ root creates IAM

→ IAM → creates resources.

IAM

↓

user account

↓

create user.

- AWS Management Console (provide user access)

AWS CLI

↓

Custom password

☑ Next time change password.

☒ The custom password must be used by user in life time.

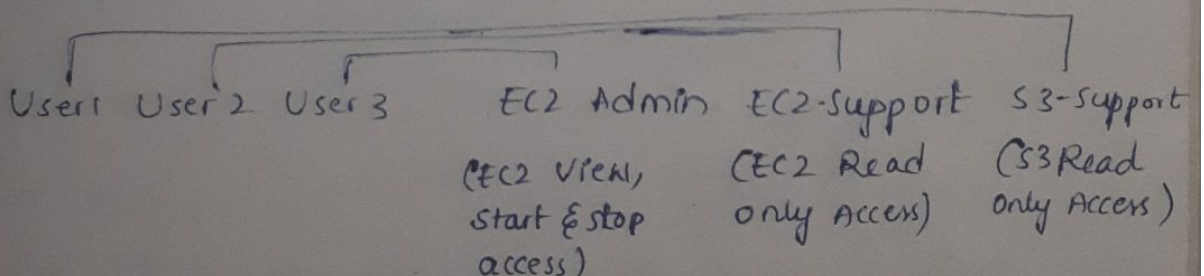
→ Add user to group

→ Attach policies directly (Individual)

- Permission policies

☑ AmazonEC2FullAccess

- Lab 1 → 2 users



Storage (roll)

IAM → role.

1) AWS S3 (Simple storage service).
2) AWS EBS (Elastic Block store/storage)

→ In mobiles & digital device
. 1) block (laptops, comp → OS)
2) object → everything is a object
hard disks

• Block storage → faster to store, faster to retri
• 2GB → entire (object)
↘ blocks (block)
200 MB blocks.
• faster access.

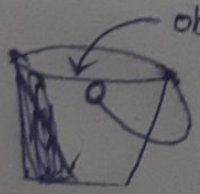
// happens in nano seconds (SSD, RAM)

① S3 (object storage) → Databases, img, videos etc.
② EBS (Block storage) → OS

→ Internal OS/storage ⇒ Block storage
(hard disk)
Extra storage ⇒ Object storage
(GB, TBs)

• EC2 → EBS
subnet objs → S3 (2KB, 65TB etc)

• S3 → unlimited sized bucket. (storage)



object have limited size (2KB to 65TB)
→ Not a region specific, global service. (S3 IAM)
(once you create in an region, service is global)

S3
↓
Bucket
↓
create Bucket
↓
name // unique in world
// only small ~~&~~ letters & numbers
· mobile num.
↓
☑ Block all public access → private.
☒ → public

even if we share link also, they can't download.

↓
create

Google drive

Versioning

Select bucket
↓
objects → upload
add file / add folder (~~add~~) (upload)
↓
Download

~~for~~

Object
↓
~~properties~~
↓
object ~~file~~ URL

To make it public
permission
↓
Block ~~allow~~ public access ☒
↓
~~save~~.
confirm
↓
save

④

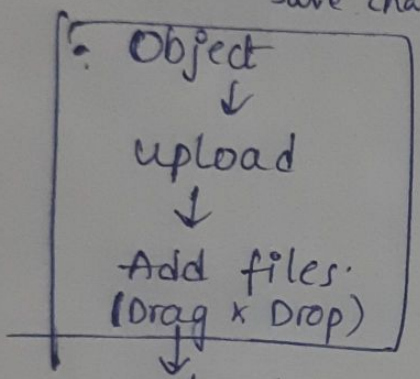
for Bucket & object.

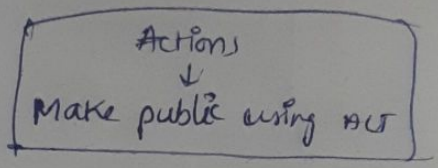
Public Access
✓ List
✓ Read

object ownership
↓
ACLs enabled
save.

S3 - host a static website

Bucket -> public.
↓
properties
↓
static website hosting
↓
Enable
↓
Index.html
save changes





---

1) Launch windows ec2 instance.
2) Create new volume in same AZ
3) attach the volume to ec2.
4) make the volume available & create partition
5) Create snapshot of volume.
6) detach & delete the volume.
7) Create volume from snapshot.
8) attach the volume of ec2
9) check the restored data.

EC2 Instance

↓

launch with Windows 2019 Base

↓

RDP client → get password → Decrypt password (4 mins).

↓

connect to remote desktop connection.

Add volume

- EBS

↓

volumes.

↓

size (5 GB)

↓

Availability zone (same as instance) (to attach)

↓

create volume.

- diskmgmt.msc

↓

Disks (check).

Attach to ec2 instance

- click volume

↓

Actions

↓

Attach volume

↓

Select Instance

↓

Attach volume.

Linux → mount

Lab 4

⇒ diskmgmt.msc

↓

Disk1 is created

(offline → right click → online)

- Initialize Disk (by right click)
- ~~D~~allocate (new simple volume) ⇒ Give drive letter

// Drive is created

Put some files in drive.

---

volume → hard disc
drives → partitions.

- when we backup a volume – snapshot
  (backup of virtual volume)

→ select volume
↓
Actions
↓
Create snapshot
↓
details (description)

- Available in EBS
  ↓
  snapshot

* By a single snapshot, we can backup files, folders etc.
- Someone deleted / corrupted / we deleted.
  → In backup (snapshot) everything is available.
- detach the volume
  ↓
  delete the volume.

To restore

↓

snapshots ☑

↓

~~Snapshot Id~~

↓

Actions

↓

create volume from snapshot

- volume is created

↓

Attach

Linux

1) df -h (diskmgmt.msc)

2) mkfs ext3 (create a volume in file system)
ntfs → partition.

3) mount online → partition → d, e, f ...
(part)
- In Linux sda, sdb instead of drives.
- We have to mount. (volume → mount)

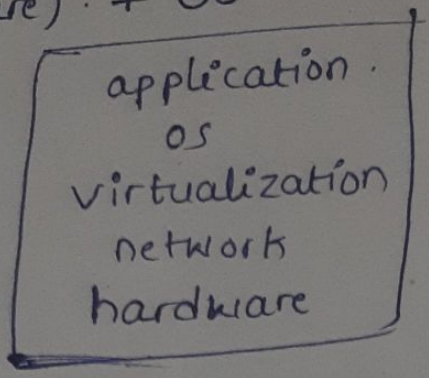
4) /etc/fstab conf file for mount points.
- Restart → unmount
& again mount

fstab → although how many times we restart it will not ~~no~~ unmount.
(permanent mount points)

5) echo ⇒ to send info to a file.

PaaS :- (aws beanstalk)

Underlying infrastructure (networking, virtualization, hardware) + OS



- Deploy web server, mail server

→ PaaS - managed services

1) Partial → paas
2) fully → saas

* amazon.in → website

ec2 instance - amazon -- 500 max (simultaneously) [concurrent users]

→ If 1000 are coming

* server - ec2

(~~ev~~ make it available)

⇒ high available

24x7 no down time.

99999999999 - 11 9s

(WA, FB, insta)

* Server down reasons

1) Power sources (2/3 T/f (or) more)
2) More mem targetting.

load balancing (high availability)

1 server → 500 max

- 1000 → 2 servers < 500 to 1 ec2 - instance / 500 to 2 ec2 - instance.
- 1500 → 3 servers

⇒ As a developer, we need to take care of website. (codemind)

- Infrastructure, OS → system/ N/W administrator

⇒ EBS

↓

create application

↓

environment < web server envt (short time) / worker envt (long time)

↓

application name

↓

Domain // technical hub

(optional)

↓

platform (managed)

↓

platform (Tomcat) // don't take new version

- later update.

↓

version.

↓

application code

✓sample app"

- Upload your code.

↓

Configuration presets

- Single instance.

↓

Service access

↓

service role.

- Use an existing service role.

// for giving permissions for ec2 - instance.

↓

EC2 Key pair

↓

EC2 instance profile.

- VPC. // default.
- Public ip adress ☑
- Instance subnets.

  select

  - load balanced
  - Instances → min 1 to max 4.

* Monitoring // dont change anything.
* Upload and Deploy

  Max size. (500MB).

  - Upload application

  // not compressed (not zipped).

  zipp → all files folder

  Deploy

Role :- Interconnection b/w more services

1) IAM policy → permissions
2) IAM user
3) IAM role

- IAM role communicates with other services → It gives permissions to users.
- EBS needs permission to EC2, VPC, autoscaling, load balancing.

⇒ Beanstalk service role (create) < Existing / new

EC2 profile (create manually and attach to Beanstalk)

⇒ IAM role
↓
Create role
↓
AWS service
↓
EC2
↓
11:29
Permission policies (~~create policy~~)
↓
Beanstalk
(AWS Beanstalk Web tier)
↓
Create policy
↓
Specify permissions (Resources ☑ all)
↓
Create & update.

dr-ec2 profile appears in IAM role.

Now select

1) AWS Elastic Beanstalk Web Tier
2) AWS Elastic Beanstalk Worker Tier
3) AWS Elastic Beanstalk Multicontainer Docker
4) ec2 • profile

↓

~~dr-~~
~~IAM ec2 profile~~

(name).

dr-ec2-iam-role.

→ user → manual process

role → automated → resource works with another resource.

* If we are creating any service / using it / provisioning → then it is chargable.
  - Else it is a free service.

// When we create it, automatically all services are created.

Benefits

1) Fast & simple to start using
2) Developer productivity.
3) Difficult to outgrow
4) Complete resource control

AWS Lambda:- (Serverless)

- Most of the organizations are using to automate their tasks.
  Like a power shell.

Schedule task (cron job)
- Automated execution.
- Scheduling some tasks to make it work in future
- In user's absence if task should be completed.

  Ex:- 1) Off codemind instance at night

Windows
↓
task scheduler
↓
schedule a task

- Requirements

1) We need OS ↔ hardware

EC2 instance.

OS → cron / task scheduler

- To perform task for 5 min, we are using EC2 instance, is it fair?
  (To turn on / turn off EC2 instance)

⇒ It is extracting from OS to schedule any task.

5 mins < ec2 - instance - 1000 ₹
aws lambda - < 50 paise ☑

⇒ Serverless // It has a server but user is not maintaining any servers to perform a task.

// Usage of servers is
// 15 mins max (scripting)

Lambda Benefits :-

1) It supports multiple programming languages
2) Can be integrated with other clouds.
3) Pay-per-use pricing

AWS lambda

1, function → what to execute
2, trigger → when to execute

→ create function
↓
Author from stratch
↓
Name (stop-instance)
↓
phython 3.9
↓
Archeticture
↓
Role

Role for AWS lamda

IAM
↓
Roles
↓
Create Role
↓
AWS service
↓
lambda
↓
policy
↓
Create policy

↓

specify permissions

↓

ec2

↓

EC2

All actions ☑

↓

All resources ⊙

↓

Next.

• policy details •

↓

dr-policy-lambda.

IAM

↓

roles

↓

create role

↓

⊙ lambda

• ec2

↓

~~create ro~~ next

↓

select policies

If we want to create, we can.

AWS lambda_full Access.

↓

preview

↓

create.

⇒ Role

↓

select

i) dr-policy-lambda.

↓

next

↓

Role name

(start_stop-ec2)

↓

create.

↓

Use existing role (select)

↓

create function.

code

↓

upload code // boto3 (Amazon SDK)

↓

deploy

↓

Test

↓

Name

↓

save.

↓

Test

---

configuration

↓ // resolve timedout issues.

Time out

↓

set to required min (default 3 sec)

Trigger

~~Add~~

↓

Trigger configuration (*)

(Event Bridge)

↓

~~*~~ Role

(create a new role)

↓

Schedule expression.

rate (1 min) // how frequently we want to execute it.

Cron (*)

) → Add

Event Bridge service

↓

Event Bridge schedule.

Events ⇒ System Design

default in AWS.

web-ec2-automation.

rdp - 3389

Wind 2019 base (gui)

run → mstsc

connect to rdp

- Administrator
- decrypted password

→ Windows ec2 instance

start

↓

server manager.

↓

Add roles x features.

↓

Next → Next → Next → Roles

↓

Web Server (IIS)

↓

Add features

↓

next → next → next → next → Install

↓

close & ⊠

http, apache } Linux

IIS → windows (Internet Information service).

- We can install Nginx, apache2

↔ public ip in normal comp

(Sample page is appeared)

→ EC2 instance

↓

file explorer

↓

This PC

↓

C drive

↓

inetpub (internet publishers)

↓

wwwroot → iisstart

delete those files

↓

Create new text docx

↓

Write something

↓

Save as [index.html]

[All files]

(completed) ✓

→ Unzipped template

↓

copy to laptop's C drive / D drive

↓

public ip (mstsc) reconnect

- show options

↓

Local Resources

↓

Local devices & Resources

- More

☑ Drives

↓

OK

↓

connect

→ Drive appears on ec2-instance

↓

copy to wwwroot.

- wwwroot → direct content
  → not directory.

ec2 instance (ubuntu)

connect - putty

commands - update, apache2, service

Index --> deploy

⇒ EC2 instance

Ubuntu

- Allow HTTP traffic
- Advanced details

User data

```
#!/bin/bash
```
shebang

```
sudo apt-get update -y
sudo apt-get install apache2 -y
sudo systemctl start apache2
```

- Launch Instance