

Contents

❖ COURSE OUTLINE.....	3
❖ AWS CERTIFICATION.....	3
1ST SESSION AWS – INTRODUCTION	4
2ND SESSION AWS - CLIENT SERVER ARCHITECTURE.....	5
3RD SESSION AWS – OVERVIEW	7
4TH SESSION AWS - DATA CENTER	8
5TH SESSION AWS - DATA CENTER INFRASTRUCTURE.....	9
6TH SESSION AWS - MANAGEMENT CONSOLE & GROUP OF SERVICE.....	10
7TH SESSION AWS - 3T'S ELASTICITY SCALABILITY HIGH AVAILABILITY	11
8TH SESSION AWS - REGIONS AND AVAILABILITY ZONES	13
9TH SESSION AWS - SERVICES EC2, ELASTIC BEANSTALK, LIGHT SAIL, LAMBDA	14
10TH SESSION AWS - STORAGE S3, EBS.....	16
11TH SESSION AWS - EFS, DATA SERVICES	17
.....	18
12 SESSION AWS - VPC, ROUTE53, CLOUD FRONT.....	19
13TH SESSION AWS - IAM, CLOUD WATCH, CLOUD TRAIL	20
14TH SESSION AWS - REVISION TILL NOW & INTERVIEW QUESTIONS	21
15TH SESSION AWS - IAM SERVICE.....	22
16TH SESSION AWS - IAM GROUPS IAM ROLES	23
17TH SESSION.IAM TAG INSPECTOR TRUSTED ADVISOR	23
.....	24
18TH SESSION AWS - IAM PRACTICALS AND AWS SIGN IN CONSOLE	26
19TH SESSION IAM ROLES AND POLICIES	27
20TH SESSION AWS - EC2 SERVICE, EC2 FAMILIES INSTANCE TYPE	28
.....	28
21ST SESSION AWS - EC2 VOLUMES, EBS VOLUMES, INSTANCE STORE VOLUME, EBS CENTRAL STORAGE.....	29
22ND SESSION AWS - EC2 INSTANCE, EBS SNAPSHOT STANDARD & ARCHIVE TIER, FSR (FAST SNAPSHOT RESTORE)	30
.....	30
23RD SESSION AWS - EC2 INSTANCE KEY-PAIR, CLUSTER NETWORKING INSTANCE	32

24TH SESSION AWS - EC2 SECURITY GROUPS, NACL.....	34
25TH SESSION AWS - EC2 INSTANCE AUTO-SCALING, ELASTIC LOAD BALANCER.....	36
26TH SESSION AWS - TYPES OF IP'S, GA (GLOBAL ACCELERATOR).....	38
27TH SESSION AWS - EC2 REVISION & INTERVIEW CERTIFICATE QUESTIONS	40
28TH SESSION - AWS EC2 PRACTICALS, AWS CONSOLE.....	40
29TH SESSION AWS - EC2 PRACTICALS 2 = EC2 INSTANCE CONSOLE	41
30TH SESSION AWS - EC2 PRACTICALS 3 = EC2 INSTANCE CONSOLE	42
31ST SESSION AWS - EC2 PRACTICALS 4 = EC2 INSTANCE CONSOLE	44
32ND SESSION AWS - EC2 INSTANCE LOAD BALANCER	45
33RD SESSION AWS - EC2 PRACTICAL 5 LOAD BALANCER	46
34TH SESSION AWS - EC2 PRACTICALS 6 = AUTO SCALING.....	47
35TH SESSION AWS - CLOUDWATCH ALARMS EVENTS & LOGS	48
36TH SESSION AWS - CLOUDWATCH PRACTICALS ALARMS EVENTS & LAMBDA AWS CONSOLE.....	49
38TH SESSION AWS - ELASTIC BEANSTALK, ELASTIC BEANSTALK ARCHITECTURE, BLUE GREEN DEPLOYMENT	50
39TH SESSION AWS - S3 = SIMPLE STORAGE SERVICE, S3 VERSIONING	51
40TH SESSION AWS - S3 STORAGE CLASSES, GLACIER, LCM RULES, CORS, CRR, SRR, ENCRYPTION	52
41ST SESSION AWS - S3 REQUESTER PAY S3 EVENT NOTIFICATION S3 BATCH OPERATIONS S3 ACCESS POINT S3 PRA	55
42ND SESSION AWS - S3 CORS BUCKET.....	56
43RD SESSION AWS - EFS SERVICE DEMO & PRACTICALS AWS CONSOLE	57
44TH SESSION AWS - CLI TUTORIAL & PRACTICAL IN AWS CONSOLE	58
46TH SESSION AWS - STORAGE GATEWAY SERVICE TUTORIAL & PRACTICALS	59
47TH SESSION AWS - RDS, RDS PROXY.....	60
48TH SESSION AWS - RDS PRACTICAL.....	62
49TH SESSION AWS - ELASTIC CACHE SERVICE, REDIS TUTORIAL & PRACTICAL.....	63
50TH SESSION AWS - DYNAMODB, INDEXES.....	65
51ST SESSION AWS - DYNAMODB PROVISIONING CAPACITY PRACTICAL IN CONSOLE	66
52ND SESSION AWS - ROUTE53 INTRODUCTION TUTORIAL	67
54TH SESSION AWS – VPC.....	70
55TH SESSION AWS - VPC PRACTICAL IN AWS CONSOLE.....	71
56TH SESSION AWS - VPC PEERING PRACTICAL IN AWS CONSOLE	72

❖ COURSE OUTLINE

COURSE OUTLINE



- Client Server Architecture
- Network Basic Concepts
- Virtualization Overview
- Cloud Computing
- Amazon Web Services Overview
- High Availability Architecture
- AWS Sign UP Procedure
- MFA Configuration
- AWS CLI
- Compute (EC2, Elastic Beanstalk, Light Sail, Lambda, GA)
- Storage (S3, EBS, EFS, Storage Gateway, Glacier, Snowball)
- Databases(RDS, Redshift, DynamoDB, ElastiCache)
- Network and Content Delivery(VPC, Route53, CloudFront, Direct Connect, Global Accelerator)
- Management Tools(CloudWatch, CloudTrail)
- Security(IAM, Trusted Advisor and Inspector)
- Application Services(SWF, Transcoder)
- Messaging (SNS, SQS and SES)
- Overview on Developer Tools(Code Commit, CodeBuild, CodeDeploy, Code Pipeline)
- Route53 Failover Project
- Architecting VPC from scratch(Project)
- Final AWS project including multiple services

6

❖ AWS CERTIFICATION

AWS CERTIFICATIONS

Available AWS Certifications

Professional

Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud



Associate

One year of experience solving problems and implementing solutions using the AWS Cloud



Foundational

Six months of fundamental AWS Cloud and industry knowledge



aws certified

Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the exam guide

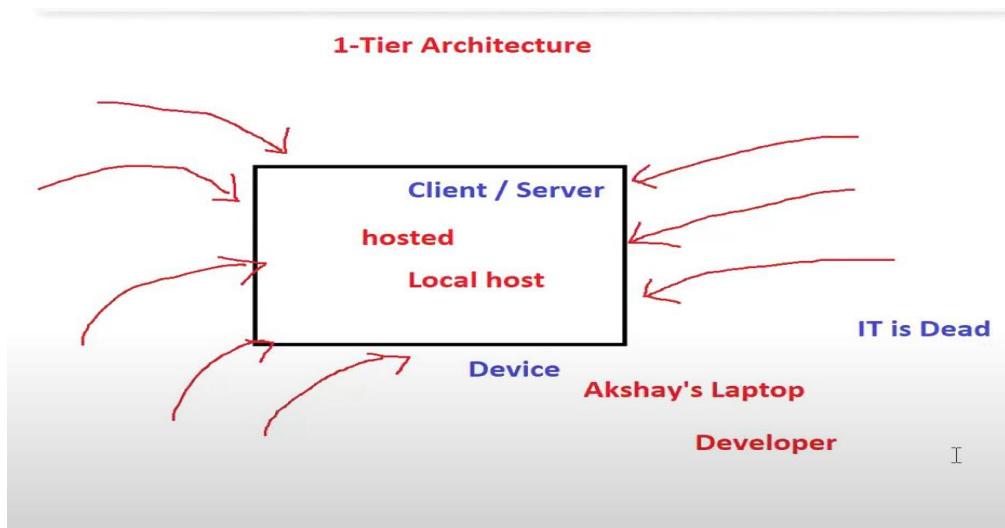
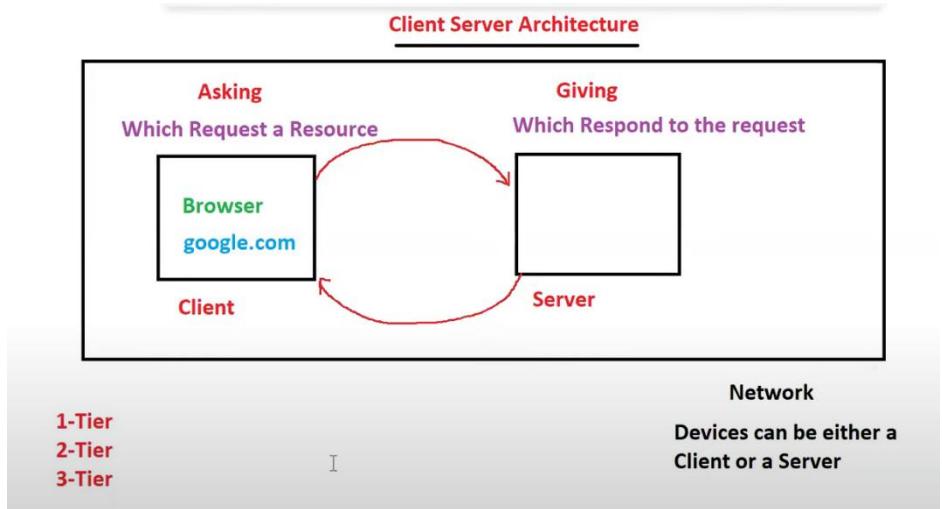


1ST SESSION AWS – INTRODUCTION

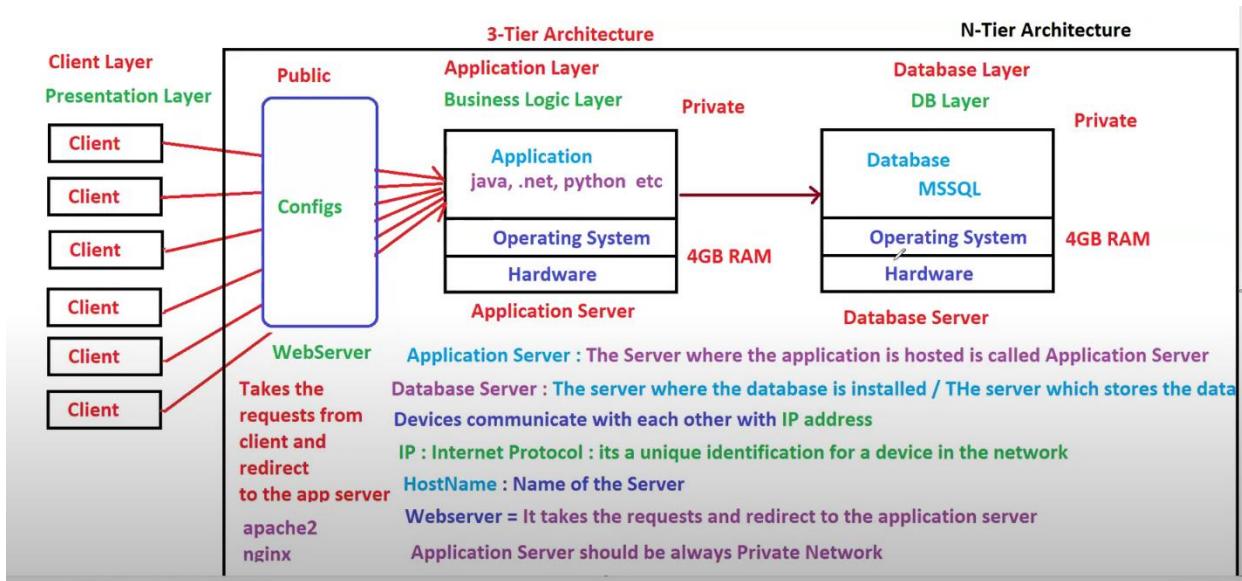
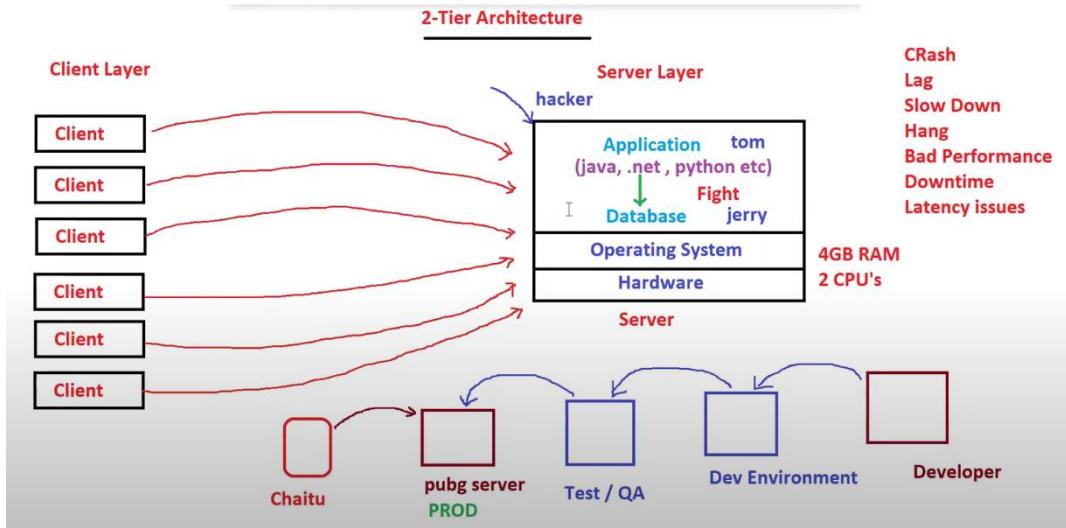
Introduction of trainer and Explained Course Overview. How we will Learn and What will be path to learn.

Introduction classes only.

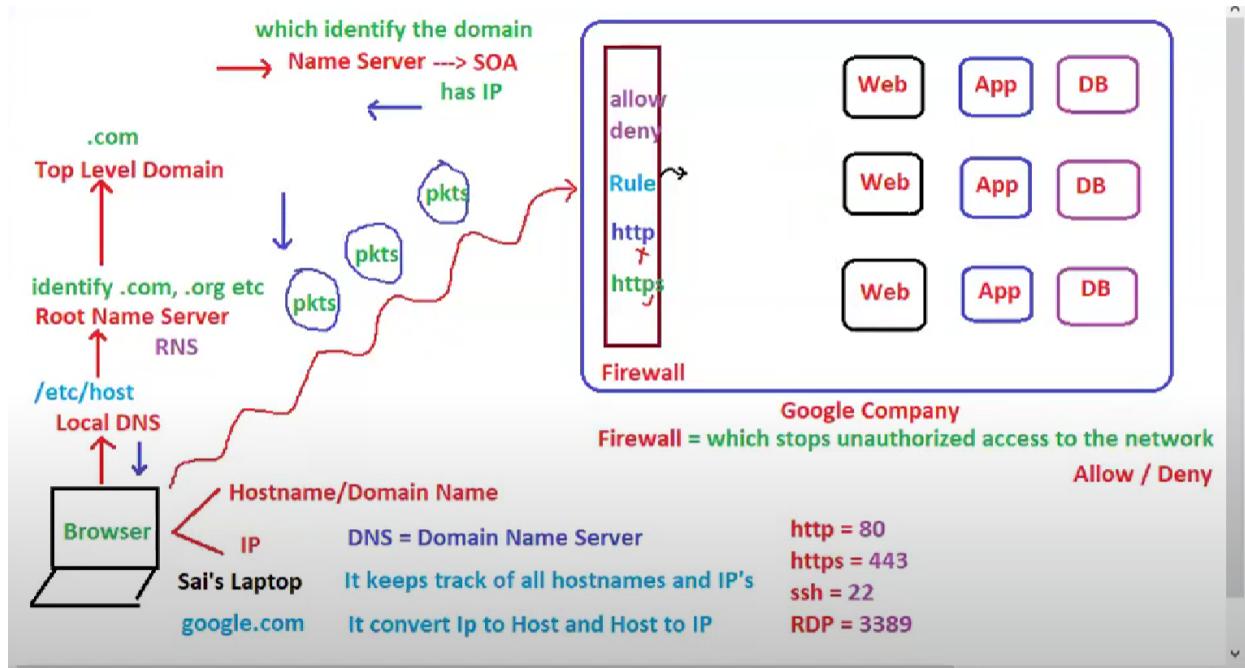
2ND SESSION AWS - CLIENT SERVER ARCHITECTURE



- What is Application SERVER (I.Q)?
- SERVER Where application is Installed.

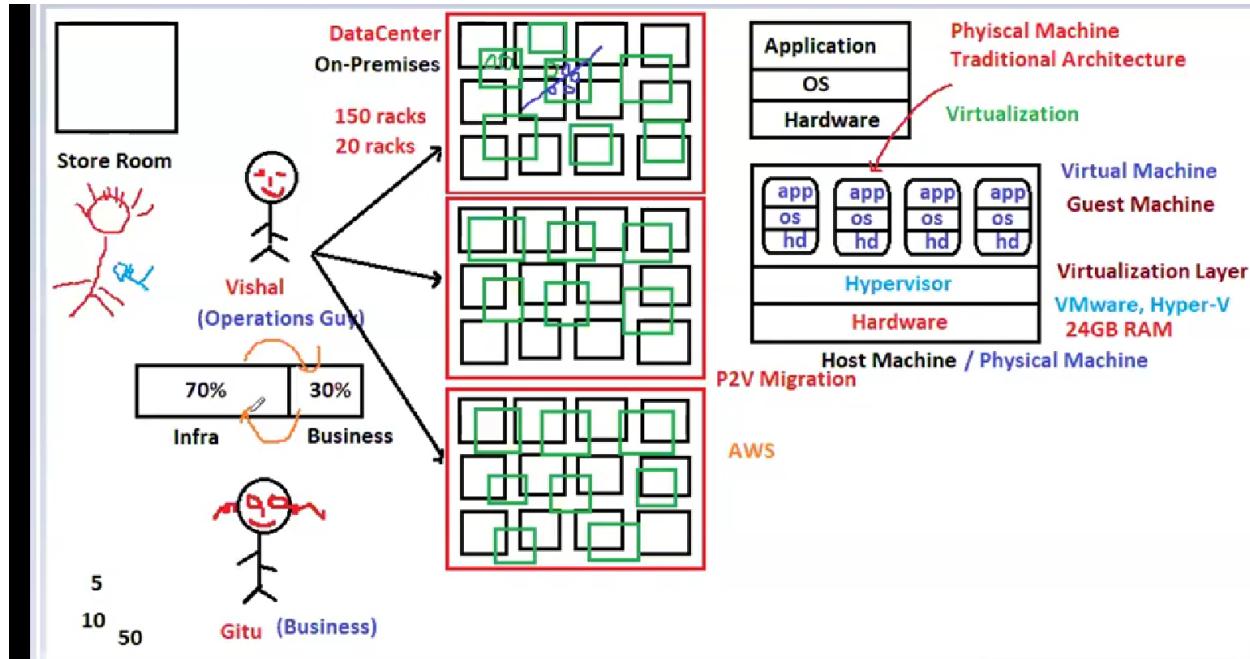


3RD SESSION AWS – OVERVIEW



- ELB = Distribute the traffic on Round Robin algorithm.

4TH SESSION AWS - DATA CENTER



- Offshore Development Center.
- WHY this Cloud? Where is this Cloud? What is this Cloud?
- p2v migration = physical to virtual machine migration
- v2c migration = migrating from virtual server to Cloud Provider

5TH SESSION AWS - DATA CENTER INFRASTRUCTURE

AWS has Global Infrastructure

AWS is providing Infrastructure as a Service

AWS has his Datacenter in India in Mumbai and hyd

That Datacenter place is called Region (Mumbai, Ireland etc etc)

Cloud is Present in the Remote Location

Remote Location = DataCenter

DataCenter = Infrastructure

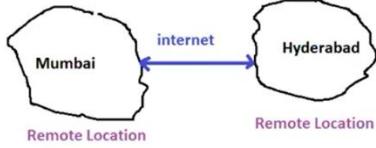
Infrastructure = Servers, DB's , storage, network etc

We need internet to connect to the Cloud (Remote location)

AWS is a Cloud Provider, who provides Infrastructure as a Service

Amazon Web Services

(Amazon Management Console)



KEY WORDS

Virtualization, Host Machine, DNS, VM's, Infrastructure, DataCenters, Load Balancer, Firewall, Protocols, Hypervisor, Cloud, Remote Location.

Physical DC --> Virtualization --> Cloud --> AWS (Remote Locations (DataCenters))

Cloud Computing

Instead of doing computing on local machine / on-premises, now you will be doing computing in remote location (Cloud) that is called Cloud Computing

Deployment Models (Types of Cloud)

Public Cloud : The providers services which are accessed by everyone like AWS, Azure, GCP
Private Cloud : The providers services which are accessed within the Organization like Oracle
Hybrid Cloud: The combination of Public and Private Cloud

Service Models

Infrastructure as a Service (IAAS)

Platform as a Service (PAAS)

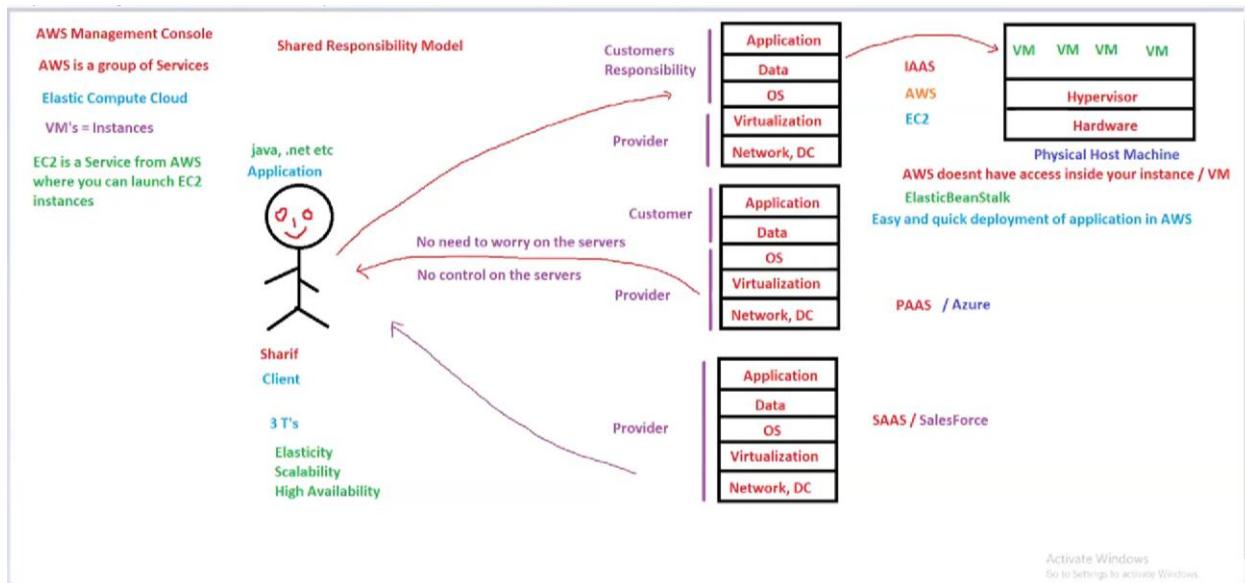
Software as a Service (SAAS)

- Deployment Models:
 - Public Cloud: Provider that provide service to public. (all in cloud)
 - private Cloud: provider that provide service within an organization.
 - Hybrid Cloud: combination of Both private + public.

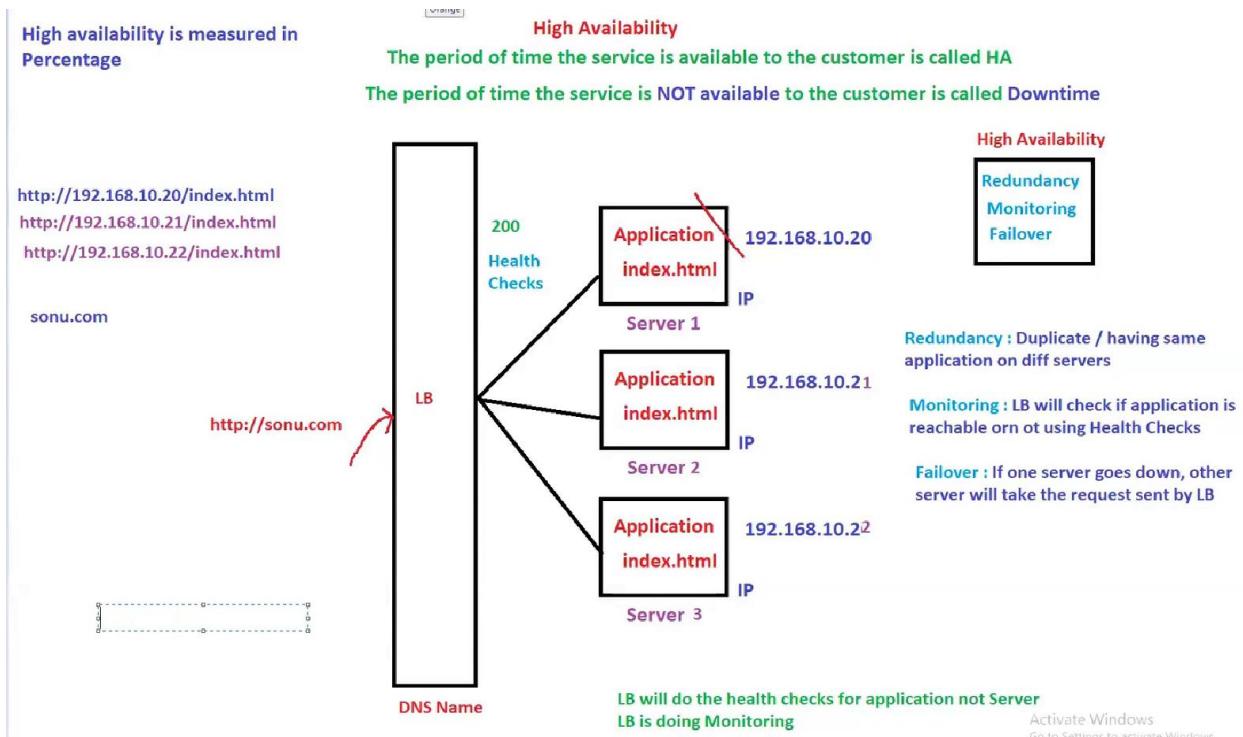
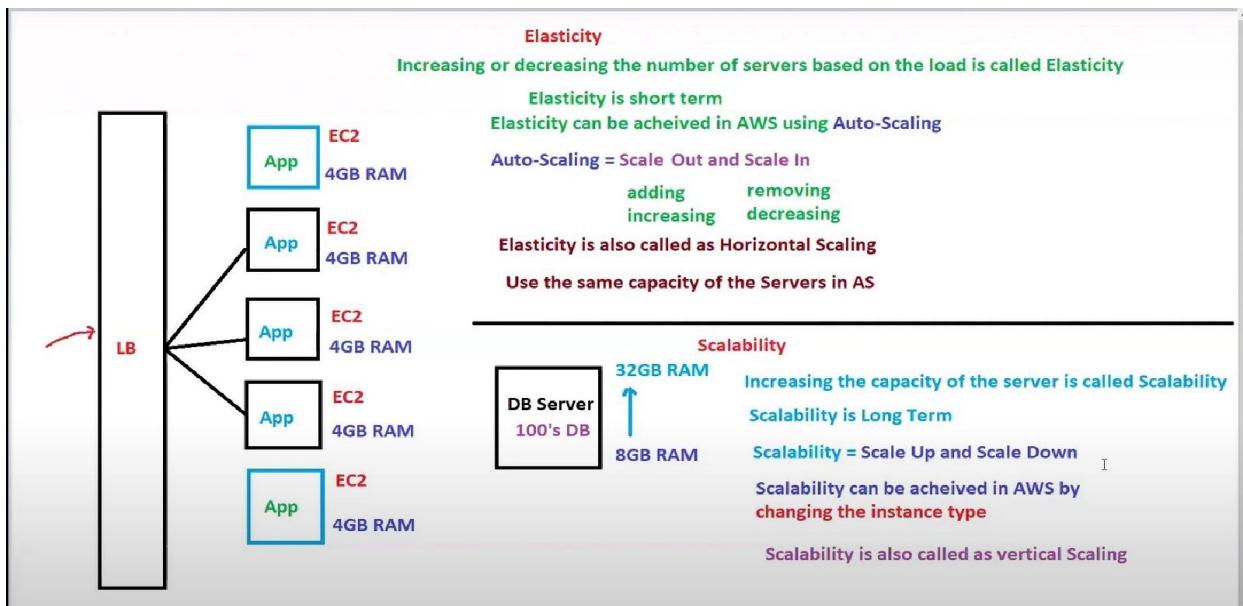
Three types of Service Models (Biryani Example)

- Infrastructure as service (IAAS): Customer is responsible Application + Data and OS, Provider is responsible for (Network + Virtualization and Data Center). Example (Ec2 Service). user have full control over infrastructure like network, server, storage etc.
- Platform as a Service (PAAS): Customer is responsible for Application and Data. Example (Elastic Beanstalk).
- Software as a Service (SAAS): Customer is responsible for Using Software Only; Provider is responsible OS + Data + Application. Everything is responsible for Cloud Provider. example (S3), E-mail service provider, Nakivo Backup and Replication.

6TH SESSION AWS - MANAGEMENT CONSOLE & GROUP OF SERVICE



7TH SESSION AWS - 3T'S ELASTICITY SCALABILITY HIGH AVAILABILITY



- **Elasticity/ Horizontal-Scaling:** Increasing the **Number of servers** based on the workload.
 - Scale Out: Increasing the number of Server.
 - Scale In: Decreasing the Number of Server.

Elasticity is possible for web server and for a short term.

We can achieve Elasticity by Auto-Scaling Group in AWS

- **Scalability / Vertical-Scaling:** Increasing the Capacity of Server.

Scalability is possible for stand-alone server like Database Server and it is for long term.

- Scale UP: Increasing the Capacity of Server.
- Scale DOWN: Decreasing the Capacity of Server.

High- Availability: Fail-Over, Down Time

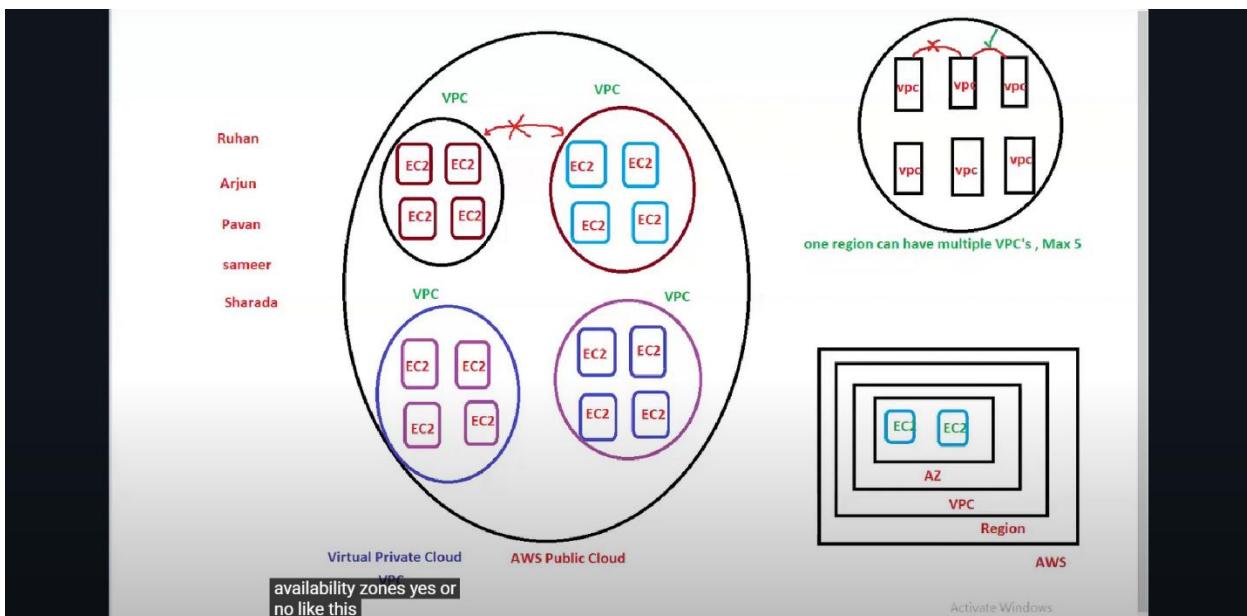
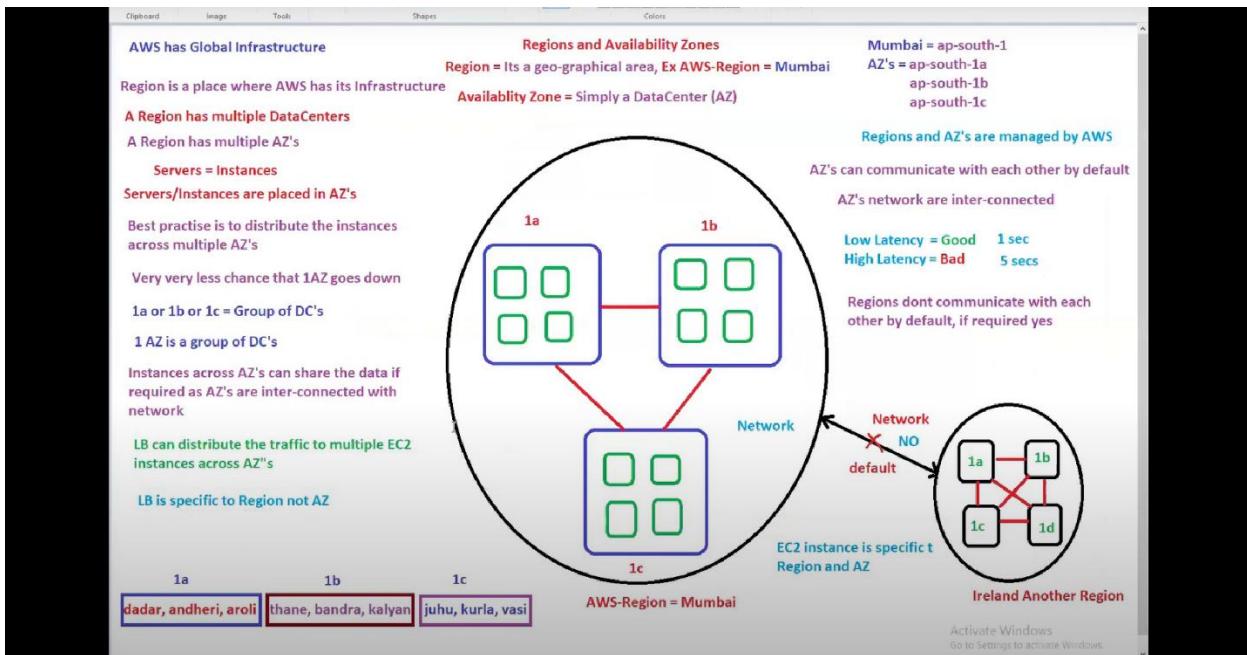
- Redundant Server = Duplicate server

Load Balancer doing the Monitoring with application, perform regular Health check up with application (C.Q)

Redundancy:
Monitoring:
Fail-over:

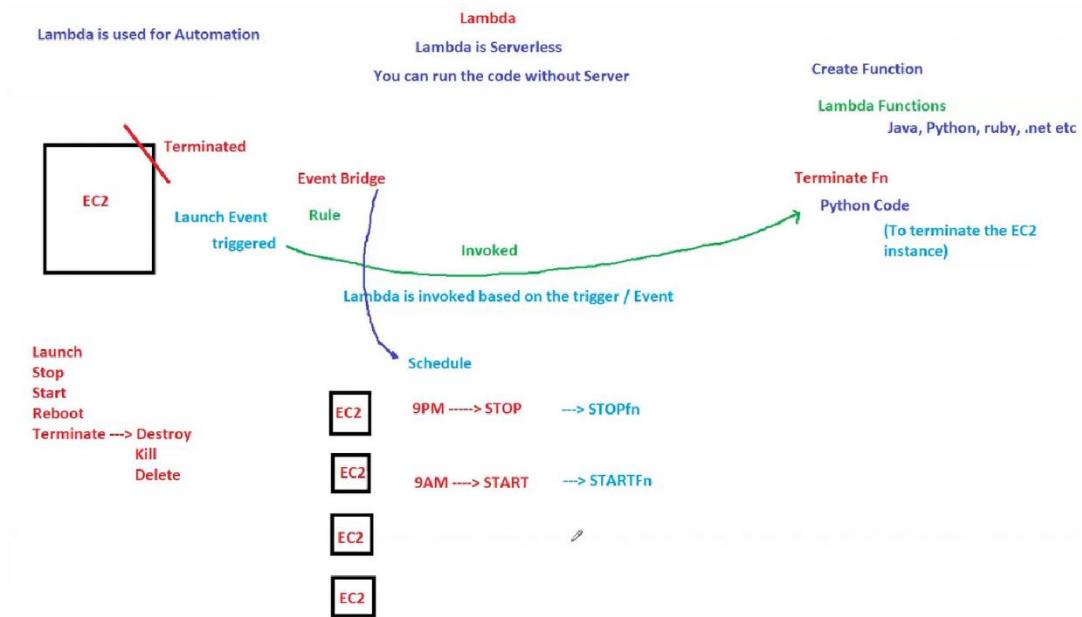
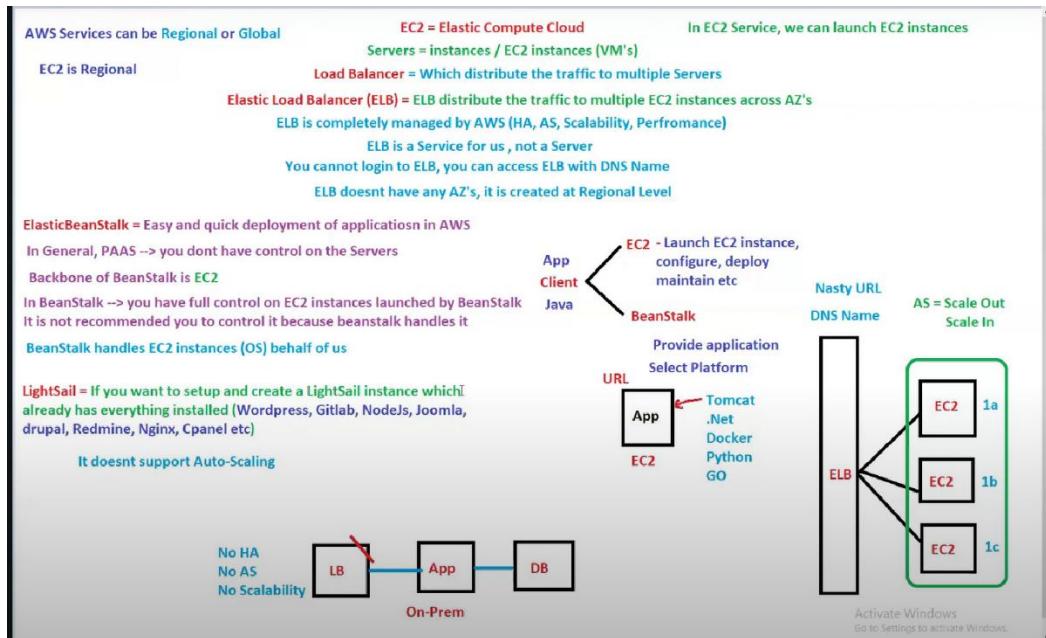
are three key things to achieve the high-availability

8TH SESSION AWS - REGIONS AND AVAILABILITY ZONES



- It is recommended to launch ec2 instance in different availability zone. By Default, two AWS region cannot communicate (C.Q) but if require we can setup communication.

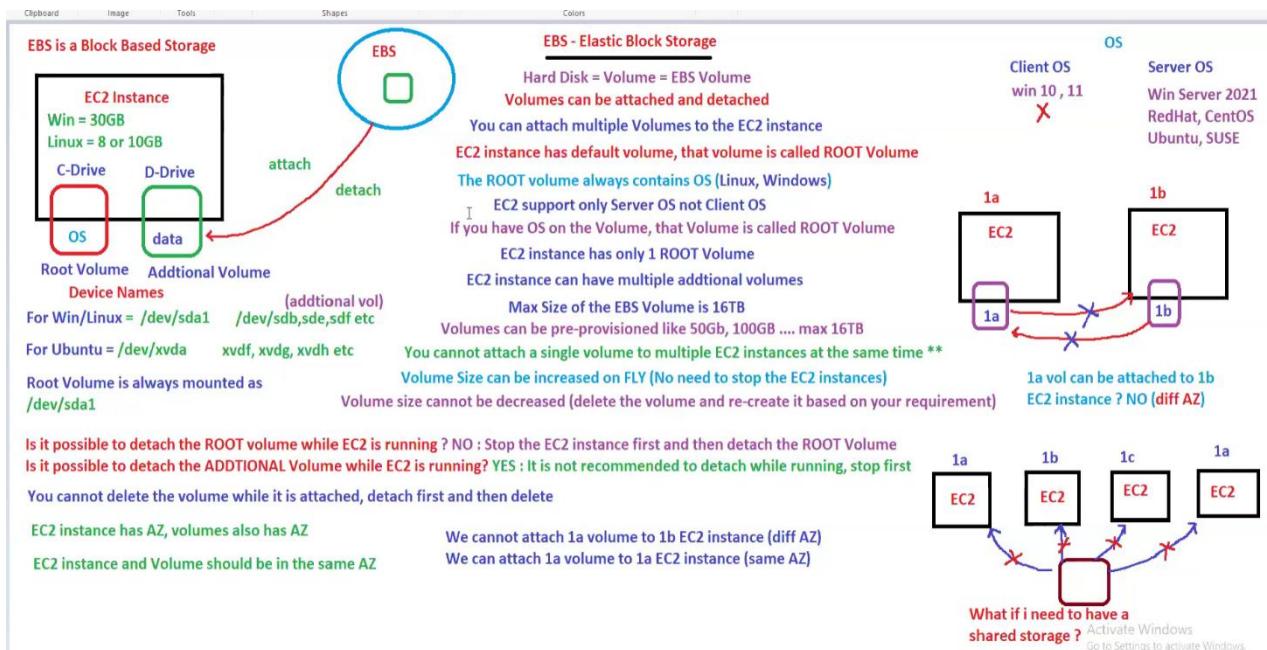
9TH SESSION AWS - SERVICES EC2, ELASTIC BEANSTALK, LIGHT SAIL, LAMBDA



- Ec2 is regional Service (C.Q)
- Services are either or Regional
- Elastic Load Balancer (ELB) is a service not a server. It will not go down.
- Lambda is used for automation (C.Q)
- EC2 is a Backbone of Elastic Beanstalk and does not provide control over server.
- In Beanstalk we have application that is deployed, but in light sail application like word press, git lab, Rubal is also already deployed by aws.
- In light sail there is no Auto Scaling

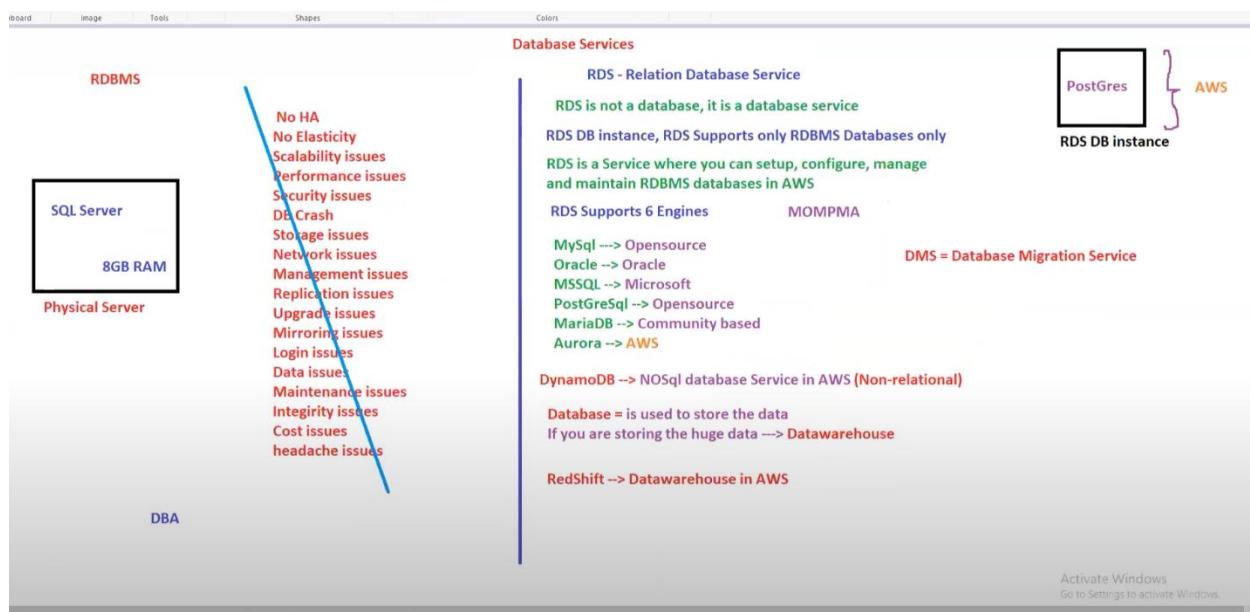
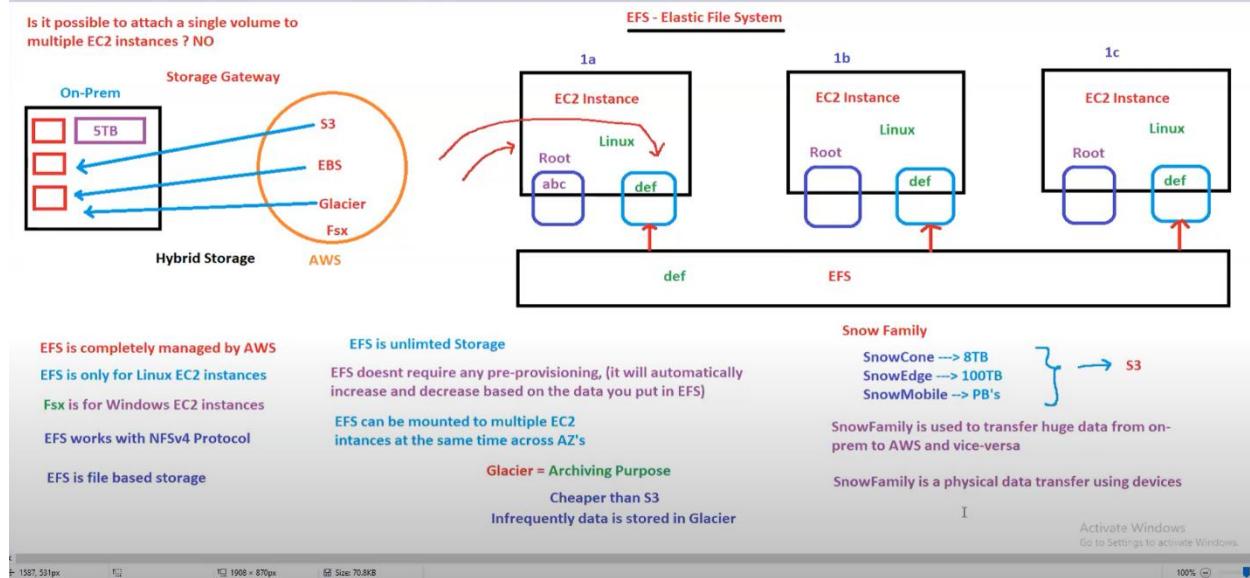
10TH SESSION AWS - STORAGE S3, EBS

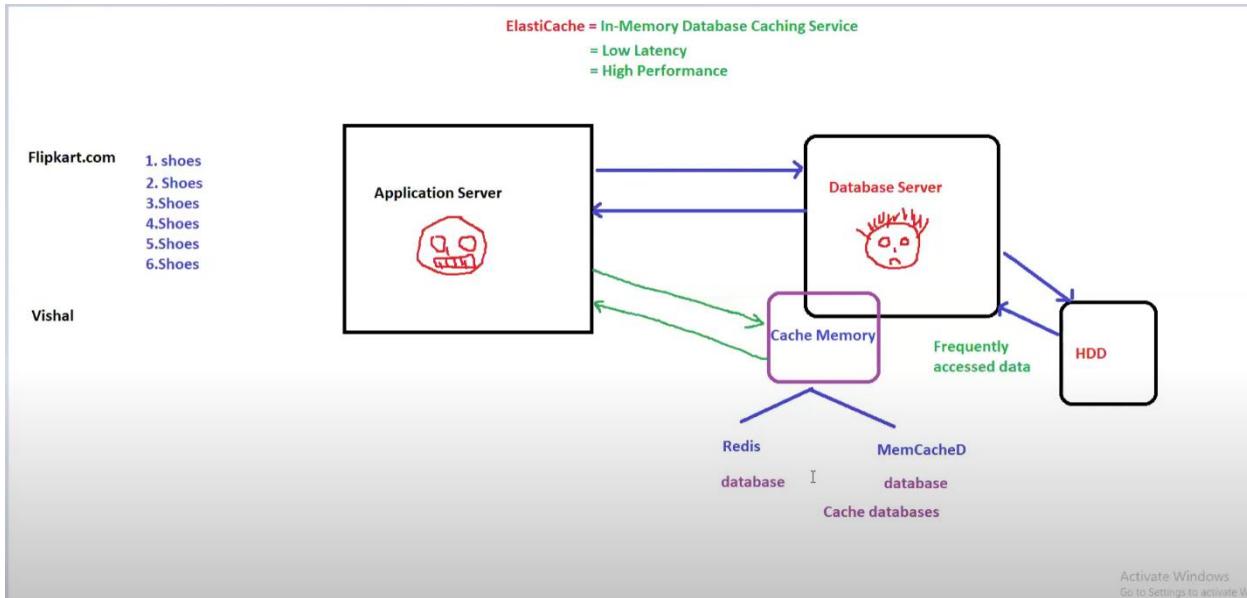
In AWS, all services will start with Simple and end with Service	S3 = Simple Storage Service S3 is unlimited storage	Floppy --> 2MB CD's --> 700MB DVD's --> 4.7GB Pen Drive --> 128GB Hard Disks --> 2TB
SNS ---> Simple Notification Service	S3 is used to just store the files (any type of files)	
SES ---> Simple Email Service	S3 can store all FLAT files	
SQS ---> Simple Queue Service	With S3, we can upload, download and access the files You cannot execute any files in S3	
S3 is Object Based Storage	S3 is Serverless AWS handles HA, Performance, Scalability etc for S3	
Laptop	S3	Bucket is a Container of Objects
Windows		Object is a File
Folder	Bucket	Name of the Object is a KEY S3 Support Static Website Hosting
Files	Objects	Create a bucket, upload all your html files and enable static website hosting
bahubali.mp4	KEY	Buckets are Regional No need to worry about HA, Performance, Scalability etc because S3 handles it



- It is best to host static website on s3(Simple Storage Service).
- S3 is object Based Storage.
- Elastic Block Storage (EBS): EBS is a Block based storage.
 - maximum volume = 16 TB
- Can we attach one volume with multiple ec2 instance (C.Q) = No
- Volume Size can be increase on FLY (i.e., while running the ec2 instance)
- Volume size cannot be decreased.

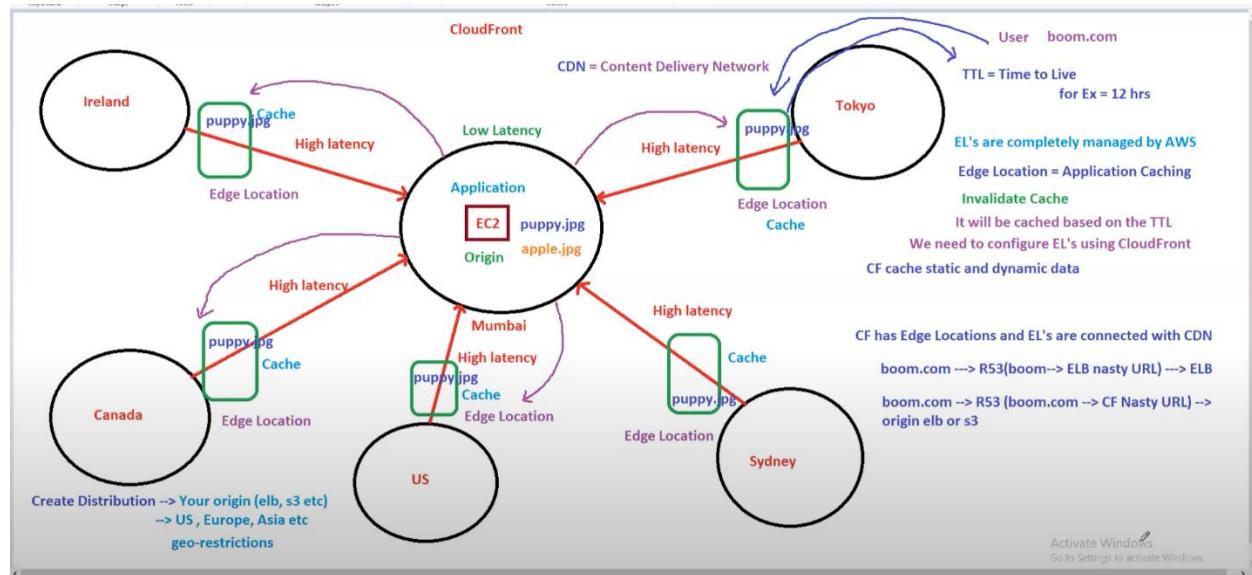
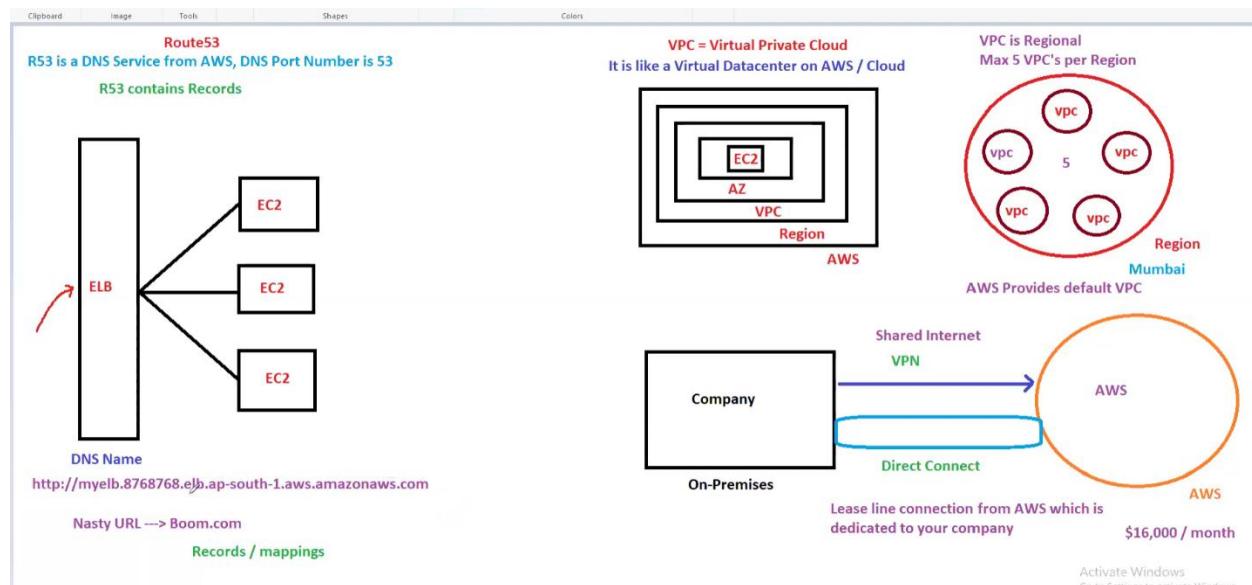
11TH SESSION AWS - EFS, DATA SERVICES



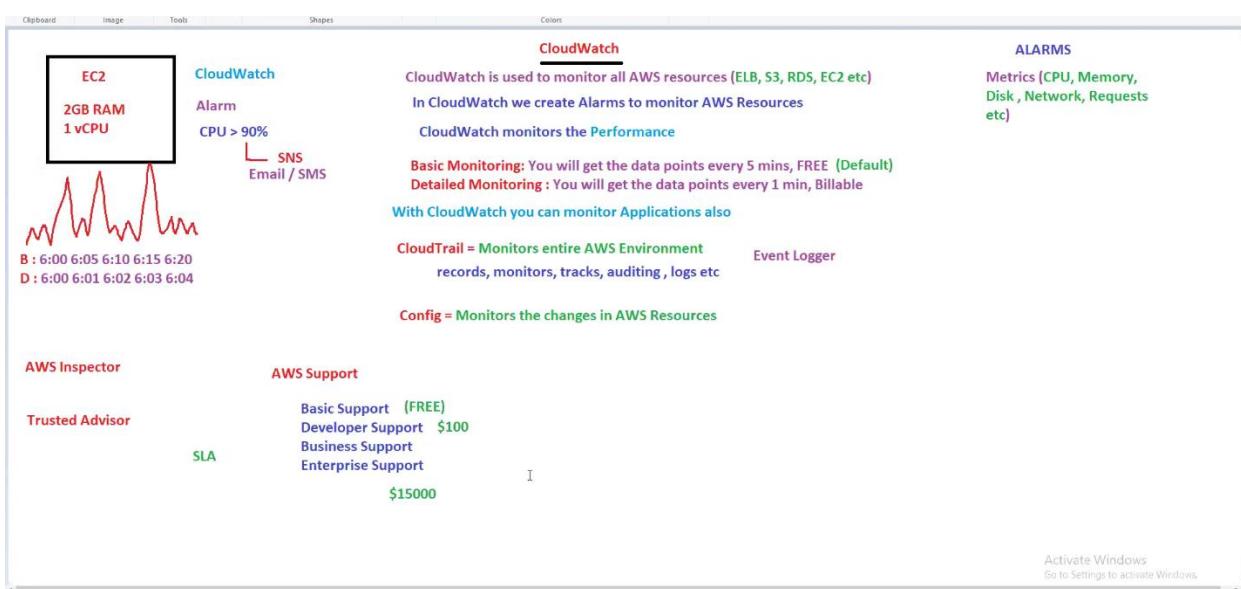
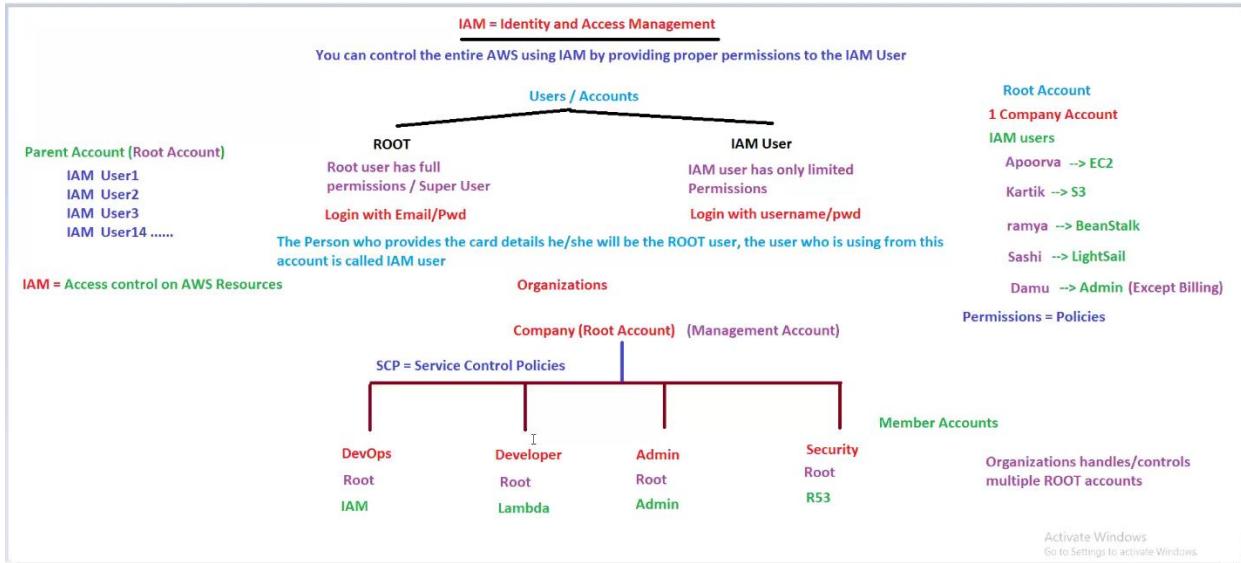


- NFS (Network File System) = EFS (Elastic File System in aws), and EFS is only for Linux System
- EFS is for Linux system and Fsx is for window system (C.Q)
- EFS can be mounted on multiple ec2 instance across different availability zone (C.Q)
- Which is the service in aws worked as hybrid storage = storage gateway (C.Q)
- AWS support six database engine (C.Q) = MOMPMA
 - M = MariaDB —> Open Source
 - O = Oracle —> Oracle
 - M = MSSQL —> Microsoft
 - P = Postgre SQL —>Community Service
 - M = MySQL —> Opensource
 - A = Aurora —> Amazon
 - DynamoDB = NoSQL based non-relational database
 - Redshift = Data Warehouse

12 SESSION AWS - VPC, ROUTE53, CLOUD FRONT

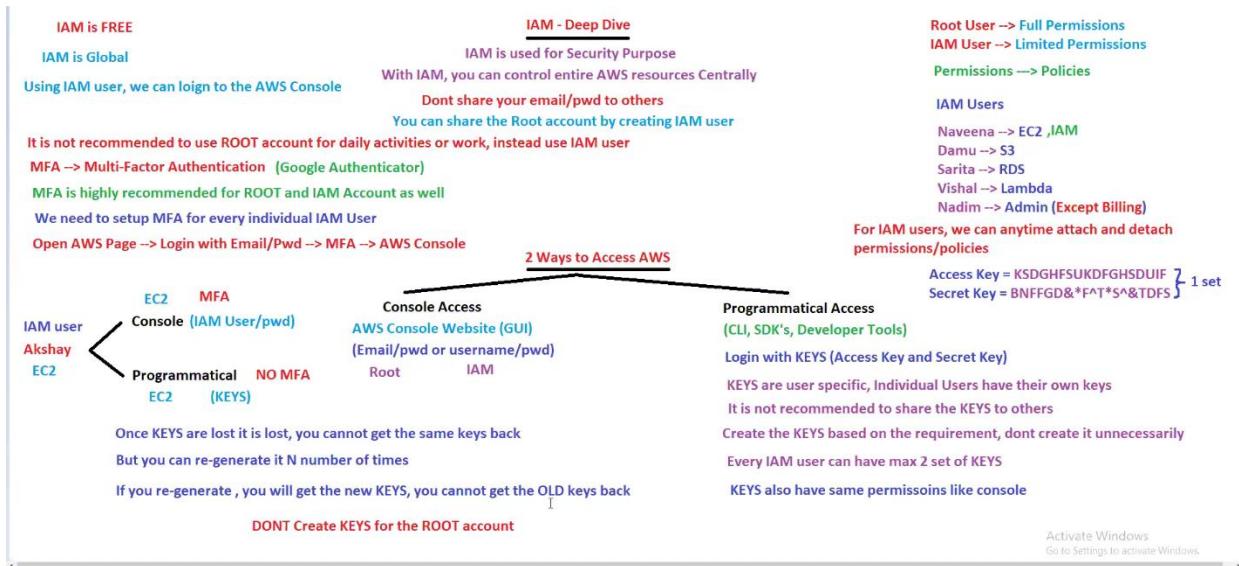


13TH SESSION AWS - IAM, CLOUD WATCH, CLOUD TRAIL



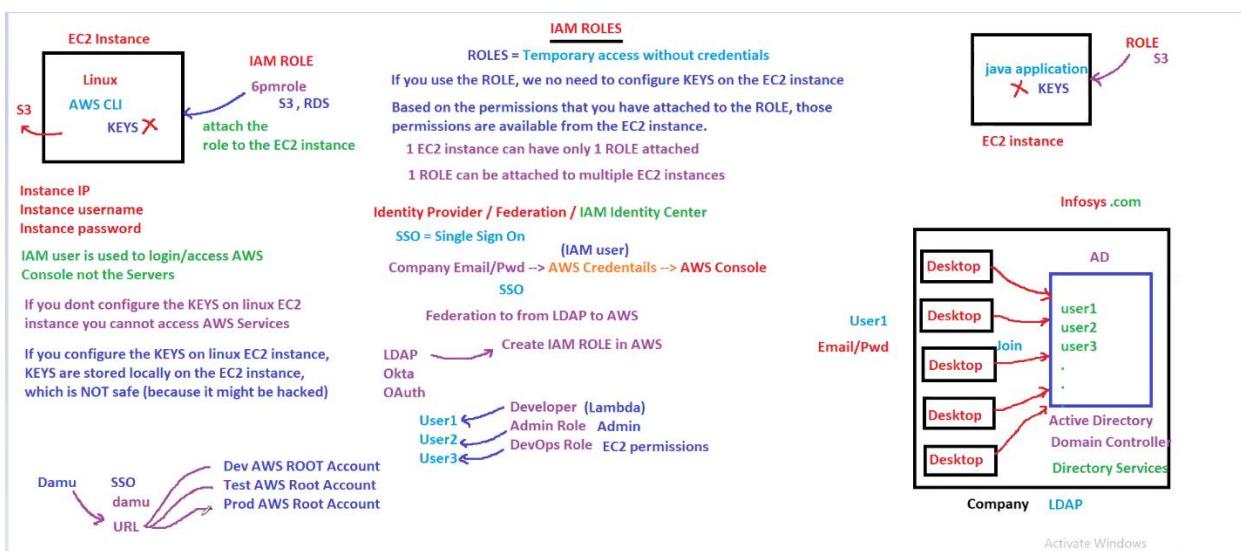
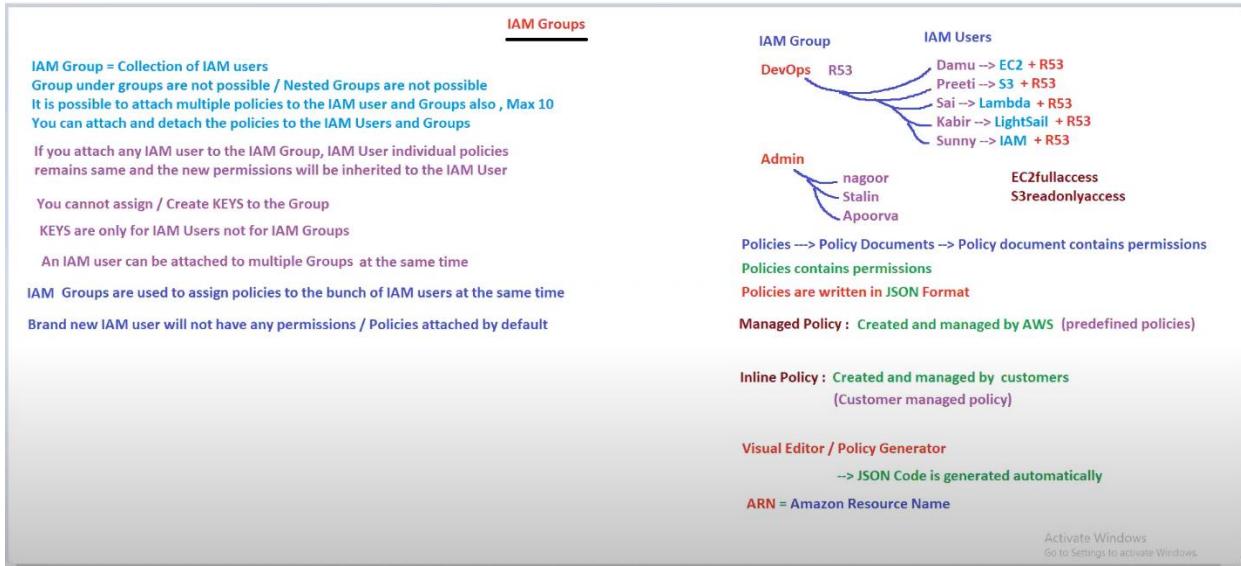
14TH SESSION AWS - REVISION TILL NOW & INTERVIEW QUESTIONS

15TH SESSION AWS - IAM SERVICE



- Every Root and IAM account should be MFA Configured.
- IAM is a Global Service (C.Q)
- Every Account, Either Root account or IAM Account, it is recommended to have (MFA). (C.Q)
- If any User either root account or IAM user, either they login from aws management console or aws cli they can use same permission. (C.Q)
- For Programmatical access, every user can have maximum 2 set of keys. (C.Q)

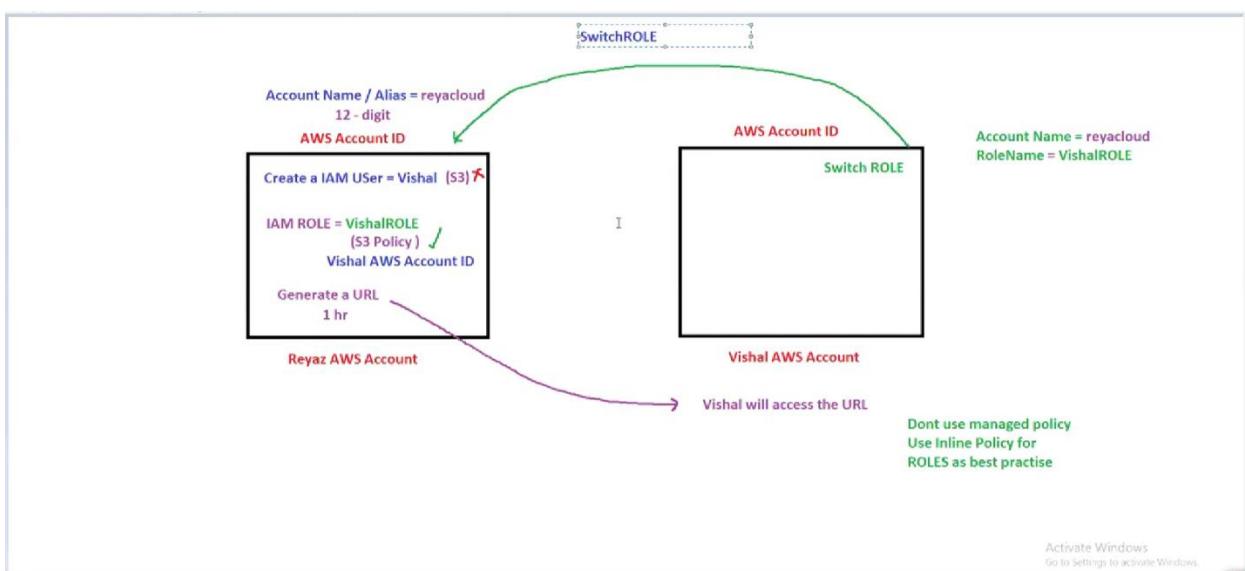
16TH SESSION AWS - IAM GROUPS IAM ROLES



- we can attach policies to the group (C.Q)
- Policies are written in JSON Format (C.Q)
- ARN = Amazon Resource Name (not number) (C.Q).
- One Ec2 instance can have one role only, and one role have maximum 10 policies.
- one role can be attached to multiple ec2 instance.
- Identity Provider / Identity Federation / Identity Center.
- Single sign On
- Directory Services in AWS =

17TH SESSION.IAM TAG INSPECTOR TRUSTED ADVISOR

 <p>EC2</p> <p>Name = WebServer Key = Value</p> <p>500 IAM Users Hard Worker</p> <p>DevOps Admins HR Security</p> <p>Manually 500 users delete HR users</p>	<p>IAM - TAGS</p> <p>TAGS are Key-Value Pair TAGS are used for identification purpose TAGS are not IAM specific, it is for entire AWS Services ARN's are auto-generated by AWS, whereas tags are provided by customer</p> <p>Tags are used for automation purpose Tags are also used for cost optimization purpose</p> <p>Per Resource = 50 tags</p> <p>Tags are important but TAGS are optional</p> <p>Smart Worker</p> <p>delete all IAM users where key = name, value = HR</p> <p>Python</p> <p>IAM Service</p> <p>IAM Users IAM Groups IAM Roles IAM Policies Federation</p>	<p>Jean</p> <p>TAG</p> <p>Price = 10k Size = Brand = Puma Key = value</p> <p>Organizations</p> <p>Root (Management Account)</p> <p>SCP's Root Root Root Root</p> <p>Dev Test Pre-Prod Prod</p> <p>Member Accounts</p>
<p>IAM user Akshay</p> <p>Name = Akshay Team = Admin Email = ak@gmail.com Address = Hyd</p> <p>---</p> <p>MAX 50 TAGS</p> <p>Access Analyzer</p> <p>It is used to analyze the access for all IAM users and take actions on the findings</p>	<p>100 EC2 instances</p> <p>50 DevOps</p> <p>Name = DevOps</p> <p>Credentials Report Password Policies</p> <p>Best Practise is to Rotate the Password and KEYS also for every 3 months based on your company policy</p> <p>Access Advisor</p> <p>. It shows the service permissions granted to the user and when those were last used . It is used to revise your policies to the Users</p>	<p>Activate Windows Go to Settings to activate Windows.</p>



- Tags are used for automation Purpose and cost optimization purpose (C.Q).
 - How many tags can be assigned per resources 50 (C.Q)
 - Tags are optional, it is used for identification and automation purpose (C.Q)
1. **Credentials Report** = To generate the report about the credentials.
 2. **Last Access** = for auditing purpose, which users access which service are used.
 3. **Access Analyzer** = to analyze the used and used services of the principle.
 4. **Root account are under Management Account and control via SCP (Service Control Policies) Policies.**

Use Case	Best Policy Type
Ad hoc, one-time access	Inline
Permissions tightly bound to a single identity	Inline
Reusable across multiple users/roles	Customer Managed
Standard AWS-wide access	AWS Managed
Organizational guardrails	SCP
Temporary session-based control	Session Policy

18TH SESSION AWS - IAM PRACTICALS AND AWS SIGN IN CONSOLE

Login to the ROOT account --> Navigate to IAM service

1. Create Alias , Customize IAM user sign-in Link and bookmark it.
 2. Create your own IAM user with admin policy attached
 3. Setup MFA for the IAM user that you have created(yourownname)
 4. Setup MFA for Root account
- **** Signout from root account and login as IAM user that you have just created. From now onwards always login with IAM user with that bookmarked IAM signlink
5. Create another sample IAM user(testuser1)
 6. Attach/add and detach/remove policies for sample IAM user testuser1(not your main IAM user)
 7. Create 2 groups and attach users to the groups. Remove users from the group
 8. Try to disable console to the test IAM user and try to login with that disabled IAM user(see what message you get)
 9. Reset the IAM user password and try to login with the reseted password
 10. Create Access key and Secret Keys for the test IAM user
 11. Make the Keys inactive.
 12. Delete the KEYS.
 13. Delete the sample IAM Users not yours []

19TH SESSION IAM ROLES AND POLICIES

14: Create a role and assign permissions
15. Create a Inline policy

16. Create 2 IAM Users(test1 and test2)
--> Test1 assign IAMFULLPERMISSIONS
--> TEST2 assing IAMREADONLY
Logout and login with test1 and verify IAM permissions
Logout and login with test2 and verify IAM permissions

This user should able to only `create users`,`list users`,`Get users`, `create group`, `list group`
17. Create IAM Users(test3)
--> Test3 custom policy(the one which you just created)

Logout and login with test3 and verify permissions what test3 can do or cannot do

Switch Roles (account id) : Create a test IAM User in your friends account using switch role (while creating role, attach IAM permissions)

Optional: Federation: Create a free tier account in Okta and setup to AWS /
or AWS Identity Center

20TH SESSION AWS - EC2 SERVICE, EC2 FAMILIES INSTANCE TYPE

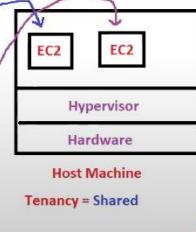
EC2 is Regional
Servers = Instances
Price = Pay as you go model
Pay every hour
750 hours are free per month

EC2 = Elastic Compute Cloud
EC2 is a WebService from AWS that provides Resizable Compute Services in the Cloud
Resizable = Scale Out and Scale In and Scale Up and Scale Down

Elasticity **Scalability**

5 mins → terminated → 2 hours
5 mins → terminated

Pricing Models in AWS

On-Demand Instances	Reserved Instances	SPOT Instances	Dedicated HOST
Fixed Price (Hourly) Pay for what you have used Pay per hour No Commitment No Upfront Payment No Predictable Usage	Long term commitment 1 or 3 years Upfront payment [Full, partial] ~ 75% discount on hourly price Standard RI : 75% discount Convertible RI : to change the capacity of the instance anytime Scheduled RI : Reserve it for short term like fraction of a day, week or a month	Bidding Auctioning Huge Capacity for cheaper price 90% discount	If you need a physical machine with VM's for this model
			
			

Savings Plans
it is same as RI but it has different strategy

Damu Shareef **Sashi**

Activate Windows
Go to Settings to activate Windows.

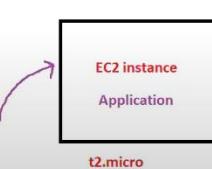
General Instances = For General Purpose
Memory Instances = If you need more memory for your application
CPU Instances = More CPU's
Storage Instances = More Storage
GPU Instances = for heavy machines, Graphics etc

EC2 Families / Instance Type

Instance Type = CPU + Memory

t2.nano = 0.5GB RAM + 1 vCPU
t2.micro = 1 GB RAM + 2 vCPU (highlighted)
t2.small = 2GB RAM + 2 vCPU
t2.medium = 4 GB RAM + 2 vCPU
t2.large = 8 GB RAM + 4 vCPU
t2.xlarge = 16 GB RAM + 8 vCPU
t2.micro is a free tier instance type

Burstable Performance Instances **(Billable)**

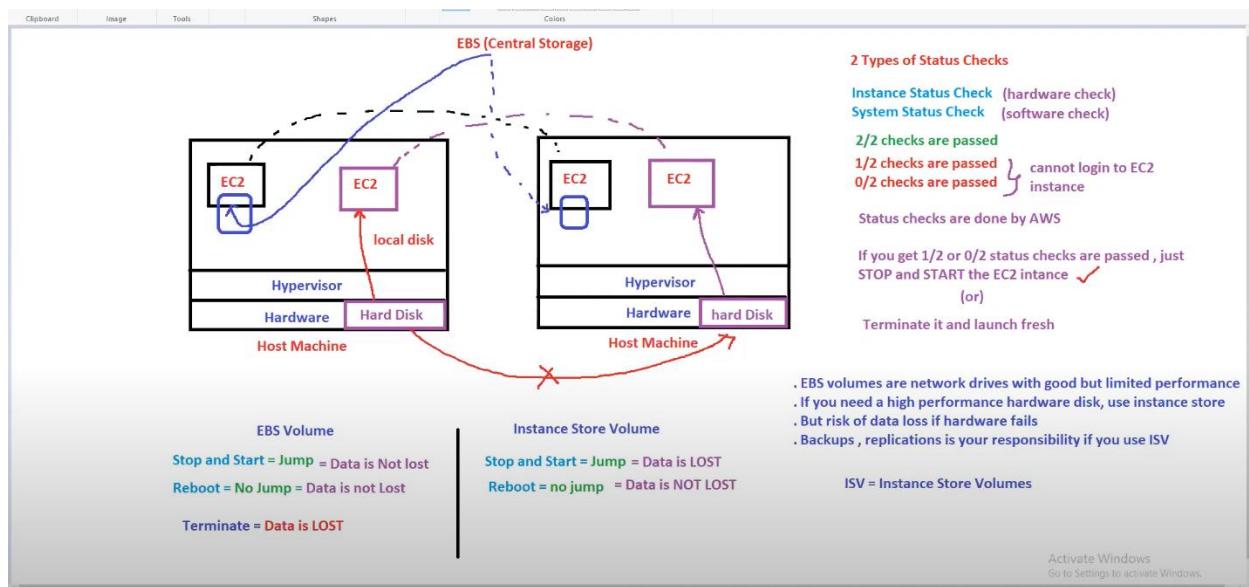
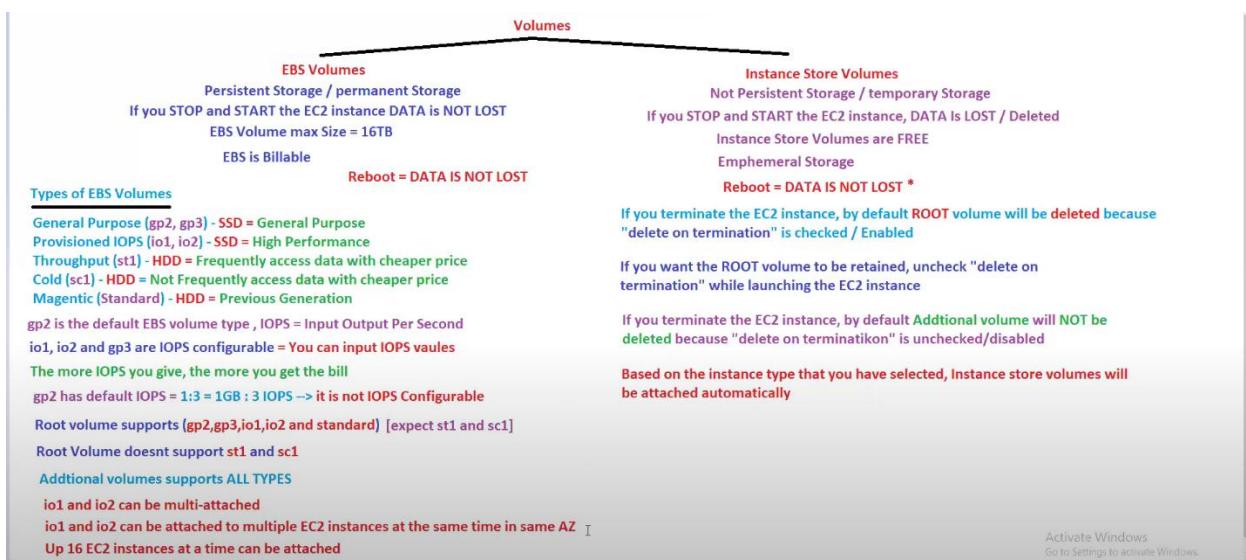


CPU Credits (For example 6 CPU Credits)
EC2 instance will enter into the burstable mode and it give high performance for limited period of time only

CPU credits depend upon the type of instances Only t2 and t3 types support burstable instances

Activate Windows
Go to Settings to activate Windows.

21ST SESSION AWS - EC2 VOLUMES, EBS VOLUMES, INSTANCE STORE VOLUME, EBS CENTRAL STORAGE



22ND SESSION AWS - EC2 INSTANCE, EBS SNAPSHOT STANDARD & ARCHIVE TIER, FSR (FAST SNAPSHOT RESTORE)

EC2 Instance

1a 1a 1a 1a

SNAPSHOTS

- Snapshot is a point in time copy of the Volume
- Backup of the Volume is called Snapshot
- EBS Snapshots are created from EBS Volumes
- You can create Snapshots from Volumes
- EBS Volumes → EBS Snapshots → EBS Volumes
- You cannot attach a snapshot directly to the EC2 instance, you have to create a volume and attach it to the EC2 instance.
- It is not possible to login to the Snapshot directly
- Snapshots are Stored in S3 (Providers S3)
- Snapshots are visible from the EC2 console
- Snapshots doesn't have any AZ
- Snapshots are Regional
- By default, Snapshots are private, if required we can make it public
- You can copy the snapshot from one region to another region in the same account
- Snapshots can be shared from one AWS account to another AWS account (Private)
- EBS volumes cannot be moved directly to any AZ, instead create snapshot.

EBS Volumes are created from Snapshots
Instance store volumes are created from a template stored in S3

To Create a snapshot we need to STOP the EC2 instance

Data Life Cycle Manager: It is used to take the snapshots automatically / Schedule.

Volumes that should get snapshot will be identified by TAGS

Retention Period = 7 days for example

EBS Snapshot Standard and Archive tier

- Move the snapshot to an Archive tier that is 75% cheaper
- Takes 24 to 72 hours for restoring from archive

Recycle Bin

Setup rules to retain deleted snapshots so you can recover them after accidental deletion, (Retention period 1 day to 1 yr)

Fast Snapshot Restore (FSR)

Force full initialization of snapshot to have no latency on the first use

By default volumes, snapshots are not encrypted
Decryption is handled by AWS

NOT Encrypted → NOT Encrypted
Encrypted → Encrypted
NOT Encrypted → Encrypted (Copy Option)

All encryption keys are stored in KMS (Key Management Service)
Access and Secret Keys are for access purpose, / But encryption keys are for encryption purpose / security

Default encryption key aws/efs, aws/s3, ebs/rds
Encrypted Snapshots cannot be shared

Activate Windows
Go to Settings to activate Windows.

AMI → Copy of the entire EC2 instance (includes volumes)

AMI

IMAGES

Copy of the OS is called Image
Image = AMI = Amazon Machine Image
Template of OS is called AMI
AMI contains OS or OS + Apps

Copy of the image includes all configuration that we did on original instance

EC2 Instance → IMAGE (AMI) → EC2 instance

1 AMI, can be used to launch multiple EC2 instances
AMI's are re-usable, AMI doesn't have any AZ's

You cannot directly login to the IMAGE(AMI), Launch EC2 instance from the AMI and use it

By default AMI's are private, if required we can make it public
AMI's are Regional

AMI's can be copied from one region to another Region
AMI's can be shared from one AWS account to another AWS account using AWS ID
All public images are located at Market Place

Image contain OS → Root Volume (EBS)
→ Root Volume (ISV)

Images are backed by either EBS volumes and Instance store volumes

AMI's are also stored in S3

OS

Windows	Linux
win server 2022 2023, 2021 etc	RedHat, CentOS SUSE, Ubuntu
Plain OS + OS with Application also	

If you customize the app on OS, and then take the image → Custom AMI Golden AMI's manually
automatically

Creating images can be automated using EC2 image builder → Golden AMI's

EC2 instance

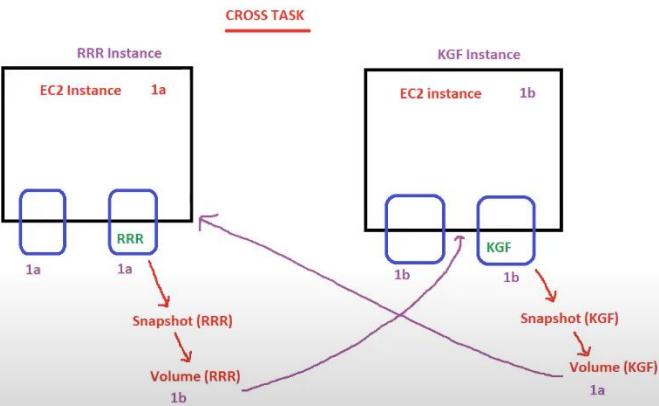
Image (2 Volumes)

2 Snapshots

No need to stop the EC2 instance if you want to take the image. It is recommended to stop and take it

Activate Windows
Go to Settings to activate Windows.

How to move a volume from 1 AZ to another AZ through snapshots



Activate Windows
Go to Settings to activate Windows.

23RD SESSION AWS - EC2 INSTANCE KEY-PAIR, CLUSTER NETWORKING INSTANCE

EC2 Instance
Win / Linux

IP : Provided by AWS
Username : Windows: administrator
Password : you will get it through Key-pair

IP : Provided by AWS
Username : Linux: ec2-user
Password : you will get it through Key-pair

KEY-PAIR

Key-pair is used to retrieve the password of the EC2 instance
We don't have any key-pair by default, we have to create it
We have to create a key-pair, the extension of the key-pair is .pem

When ever we launch EC2 instance, the console will ask you to create a Key-pair and attach to the EC2 instance

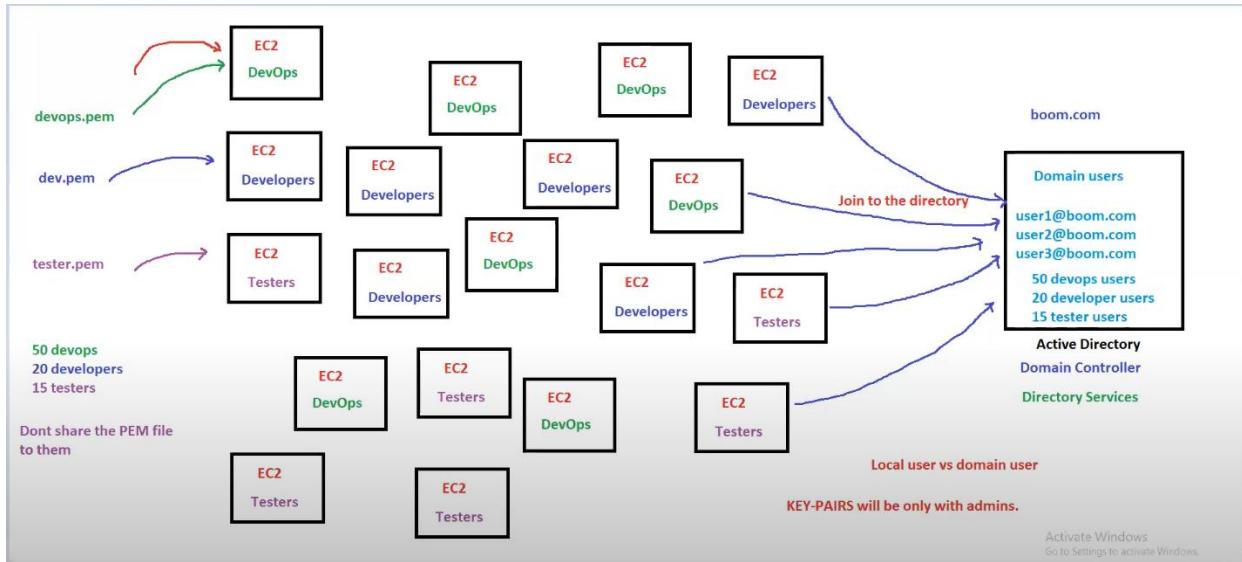
You can create multiple Key-Pairs
1 Key-pair can be attached to multiple EC2 instances at the same time
EC2 instance can have only 1 key-pair attached at any point
For every different EC2 instance, password is unique / different
Once the PEM file is attached, you cannot change the PEM file to the EC2 instance
Keep the PEM file in safe place and secure it
Every time you retrieve the password of the same EC2 instance, you will get the same password

Key-Pair = Combination of Public Key + Private key (pem file)
AWS has public key and Customer has private key(Pem)

For Windows EC2 instance --> administrator / Pem file
Protocol --> RDP / 3389 Remote desktop connection client

For Linux EC2 instance --> ec2-user / pem file
Protocol --> SSH / 22 --> Putty
Putty doesn't support pem file, it supports PPK file
PuttyGen --> Convert pem to ppk

Activate Windows
Go to Settings to activate Windows.

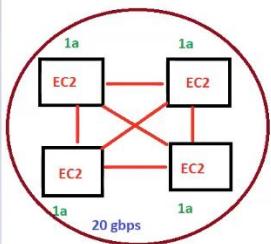


Cluster Networking Instances

Cluster = Group of Servers / EC2 instances --> this group is called **Placement Group**

When you launch a new EC2 instance, the EC2 service will place the instance such a way that all your instances are spread out across different hardware

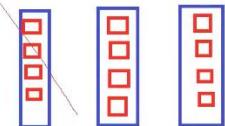
Cluster Placement Group : Grouping the instances in same rack same AZ, high performance, Low HA



Spread Placement Group : EC2 instances are spread across AZ's High HA, critical applications
Per 1 AZ = 7 EC2 instances

Partition Placement Group : Across AZ, Max partition = 7

Each partition has 100's of EC2 instance.

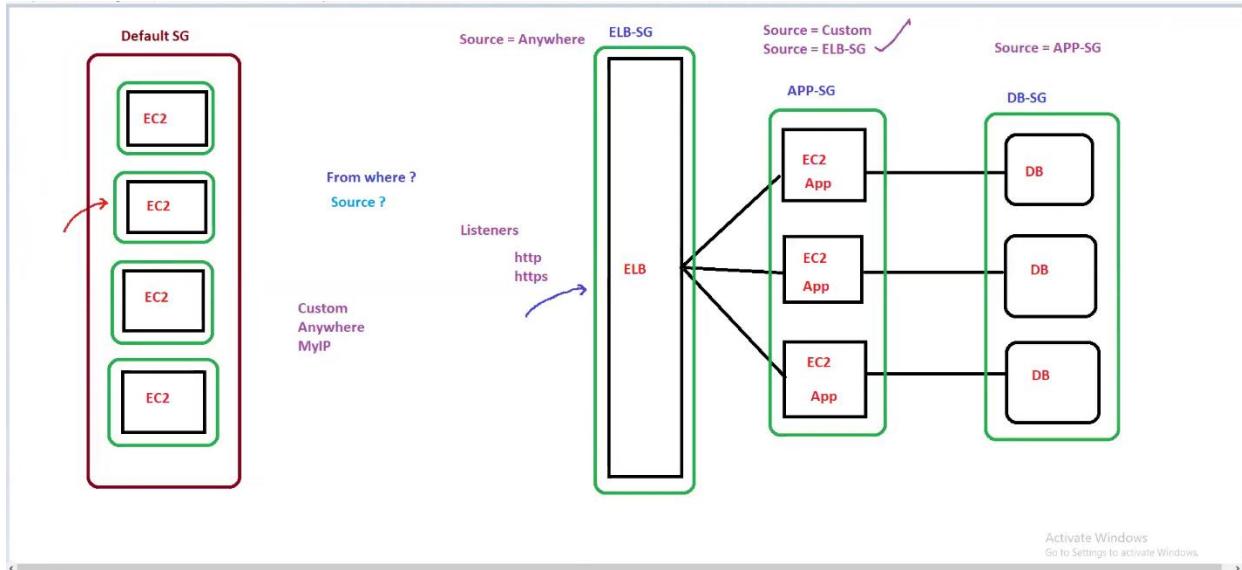
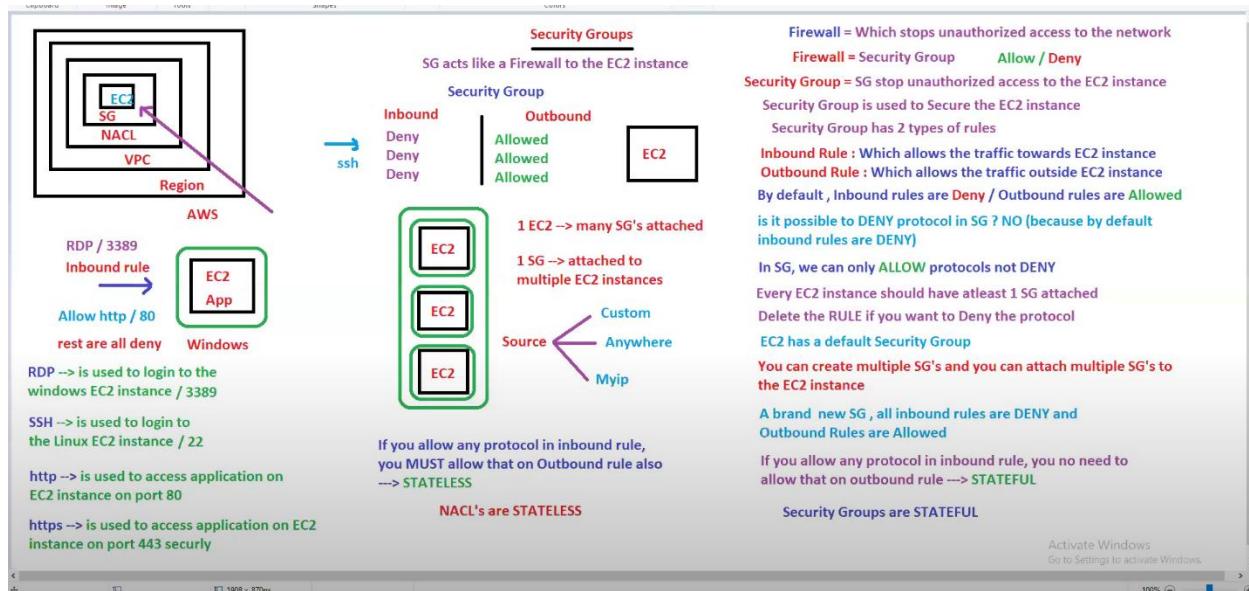


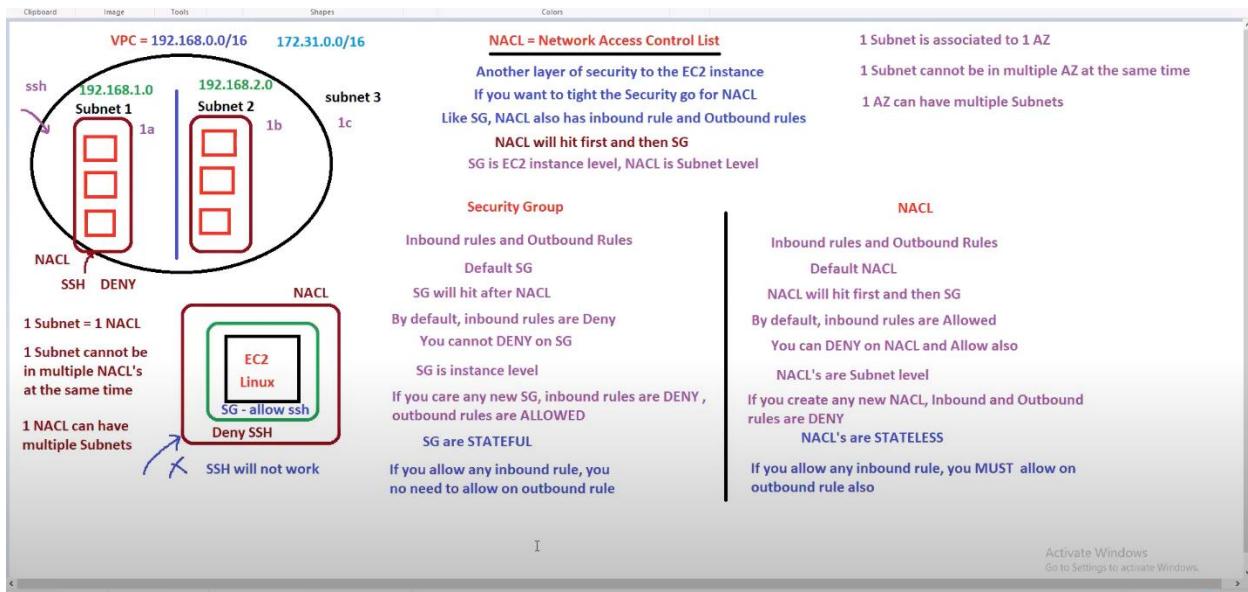
Placement Group recommended to have same homogenous instance type

When you are launching the EC2 instance, you can select which placement group you want to keep the instance

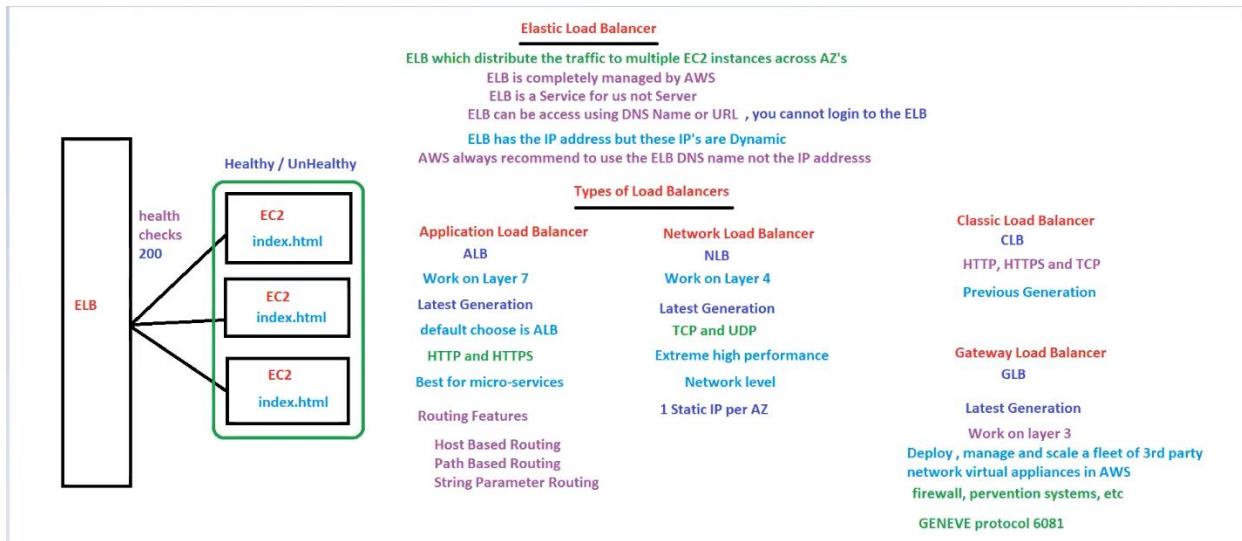
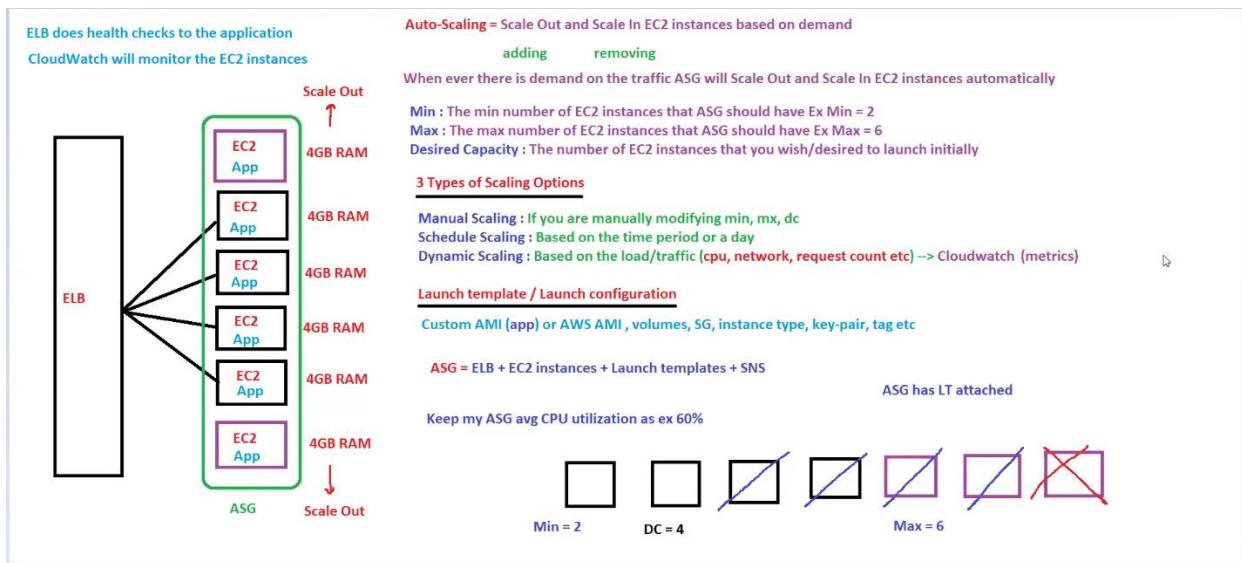
Activate Windows
Go to Settings to activate Windows.

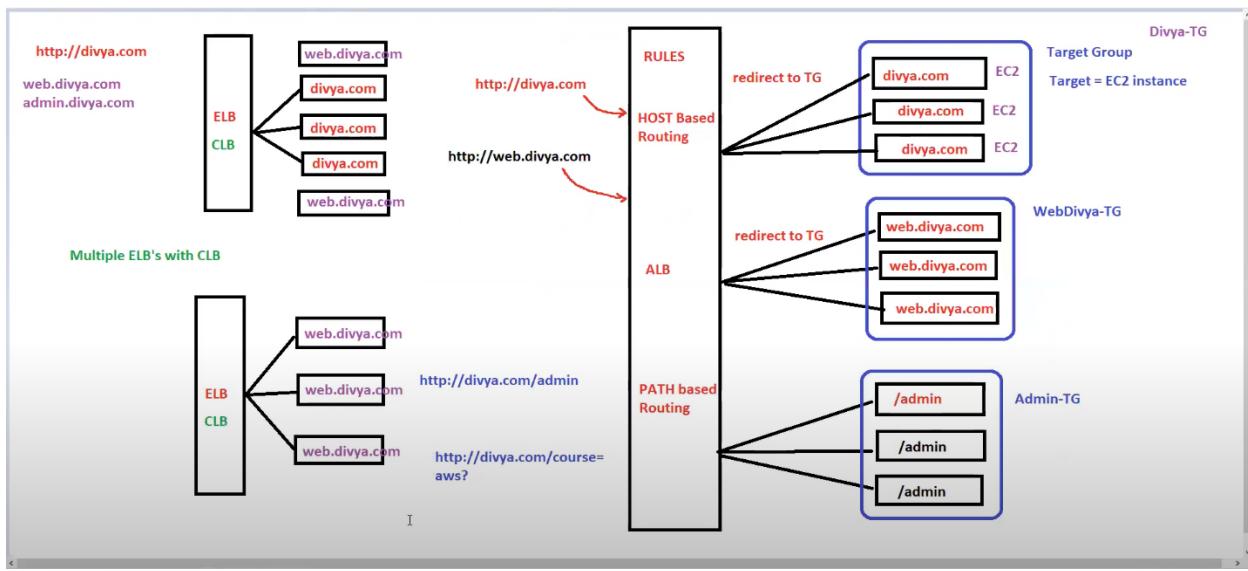
24TH SESSION AWS - EC2 SECURITY GROUPS, NACL

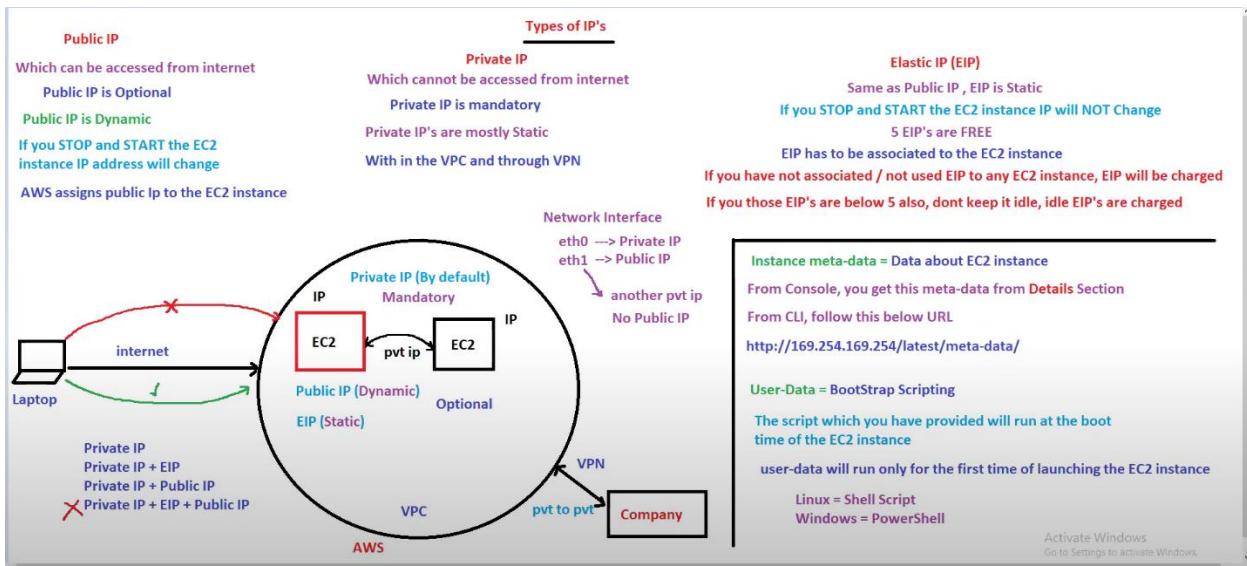




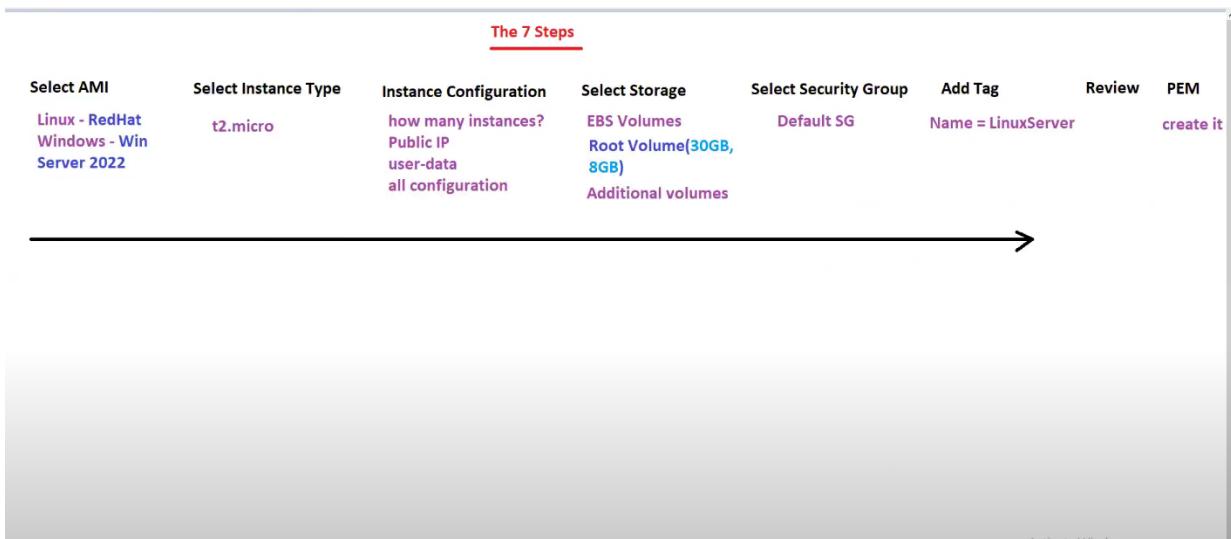
25TH SESSION AWS - EC2 INSTANCE AUTO-SCALING, ELASTIC LOAD BALANCER

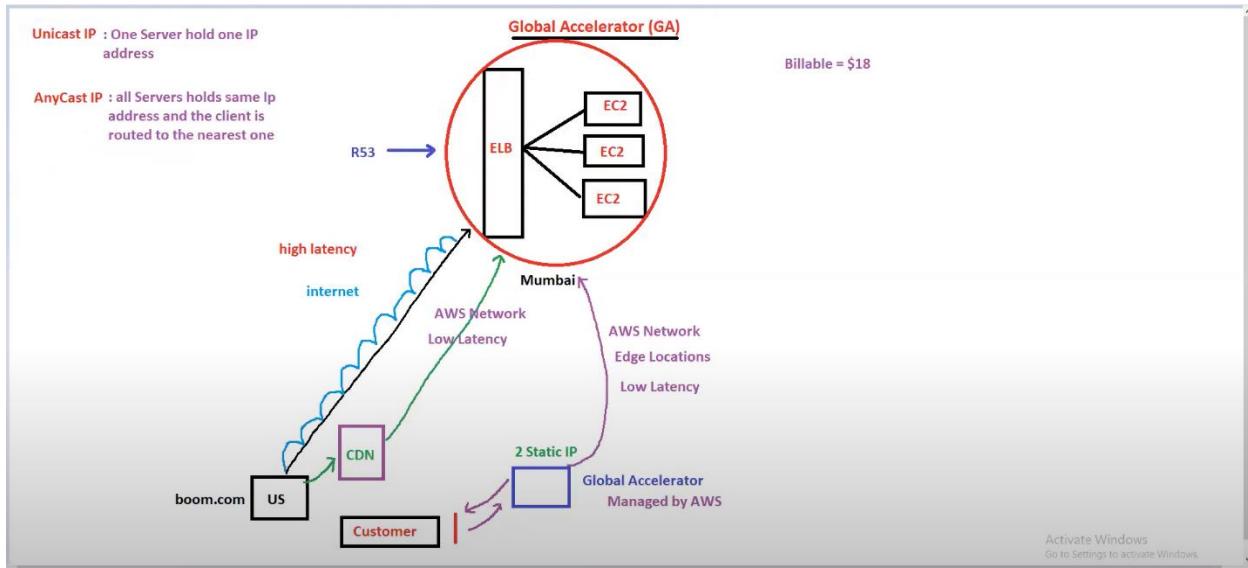






26TH SESSION AWS - TYPES OF IP'S, GA (GLOBAL ACCELERATOR)





27TH SESSION AWS - EC2 REVISION & INTERVIEW CERTIFICATE QUESTIONS

28TH SESSION - AWS EC2 PRACTICALS, AWS CONSOLE

29TH SESSION AWS - EC2 PRACTICALS 2 = EC2 INSTANCE CONSOLE

```
*****
EC2
*****
```

TASKS:

1. Launch Windows 2022 EC2 Instance(step 1 to step7(create a key pair and save it safe))
Add a new rule RDP protocol to the Security Group (dont do any changes to the default rule)
use remote desktop protocol to connect to windows machine(username: administrator, pwd: key-pair)
 2. Launch Linux redhat EC2 Instance and try to connect it
Download Putty
Download PuttyGenerator
 convert PEM to PPK using PuttyGen
 --> Open PuttyGen
 --> Load your Pem file (Load --> Choose Pem file --> save private key as xxxx.ppk)
 Add a new rule SSH protocol to the Security Group(dont do any changes to the default rule)
 Use Putty to connect to Linux machine(hostname: publicIP --> expand SSH --> select Auth--> credentials --> browse ppk file) --> Connect it
 3. Try to stop and start and reboot EC2 instance --> public IP changes or not
Try to stop and start the EC2 instance and see Private IP is changing or not
 4. Assign EIP to the Instance and try to stop and start --> EIP will change or not
 5. Disassociate EIP from the Instance and release it to AWS.
 6. Create Launch template and launch EC2 instances from it and then and delete it (launch ec2 instances from template)
 7. Try shutdown behaviour from ec2 instance and see if the instance is stopped or terminated, change to terminate and then shutdown again and see the difference.
 8. Review options in ACTIONS
- I
9. Terminate EC2 instances.(if you have protection enabled --> disable that first from instance settings --> change termination protection)
 10. Enable Shutdown behaviour = stop and terminate, and login to the EC2 instance, and shutdown the EC2 instance, see what happens

30TH SESSION AWS - EC2 PRACTICALS 3 = EC2 INSTANCE CONSOLE

IMAGES TASKS

Launch a windows instance -->login to that instance --> create some files or install a software --> Create image --> launch instance from image --> login to the newly created instance(password?) --> Check the files or software are available

Copy the image to another ireland region --> once verified, delete the image in ireland region

Encrypt the image --> use copy option --> check encryption option --> create image --> launch ec2 instance --> login and see the difference

Copy the encrypted image to same region and another region (?)

Copy the Snapshot to another region --> once verified ,delete the snapshot

Encrypt the Snapshot and share it to the other AWS account ?

Try share the image and snapshot to another account

Create a image from the snapshot

First try deleting the snapshot and then AMI --> see if this works
First try deleting the AMI and then snapshot--> see if this works

Archive snapshot and restore it again(Dont do, it will take 24 hours)

Delete the snapshot and restore it again

Terminate EC2 instances, Delete images, Delete snapshots

Activate Windows
Go to Settings to activate Windows.

Copy the encrypted image to same region and another region (?)

Copy the Snapshot to another region --> once verified ,delete the snapshot

Encrypt the Snapshot and share it to the other AWS account ?

Try share the image and snapshot to another account

Create a image from the snapshot

First try deleting the snapshot and then AMI --> see if this works
First try deleting the AMI and then snapshot--> see if this works

Archive snapshot and restore it again(Dont do, it will take 24 hours)

Delete the snapshot and restore it again

Terminate EC2 instances, Delete images, Delete snapshots

I

Data Life Cycle Manager --> See the UTC time and create a policy and see the snapshot got created or not. and then delete the policy.

EC2 Image Builder --> Optional --> Create some Golden AMI --> Once done delete the complete pipeline, recipes, configs ad AMI's

TASKS

Launch 4 EC2 instances (2 in 1a 2 in 1b)
1. CROSS TASK (additional volumes + Root Volumes) - different AZ's
2. Increase the root volume size

Activate Windows
Go to Settings to activate Windows.

Launch a windows instance --> login to that instance --> create some files or install a software --> Create image --> launch instance from image --> login to the newly created instance(password?) --> Check the files or software are available

Copy the image to another ireland region --> once verified, delete the image in ireland region

Encrypt the image --> use copy option --> check encryption option --> create image --> launch ec2 instance --> login and see the difference

Copy the encrypted image to same region and another region (?)

Copy the Snapshot to another region --> once verified ,delete the snapshot

Encrypt the Snapshot and share it to the other AWS account ?

Try share the image and snapshot to another account

Create a image from the snapshot

First try deleting the snapshot and then AMI --> see if this works

First try deleting the AMI and then snapshot--> see if this works

Archive snapshot and restore it again(Dont do, it will take 24 hours) |

Delete the snapshot and restore it again

Terminate EC2 instances, Delete images, Delete snapshots

Data Life Cycle Manager --> See the UTC time and create a policy and see the snapshot got created or not. and then delete the policy.

Activate Windows

31ST SESSION AWS - EC2 PRACTICALS 4 = EC2 INSTANCE CONSOLE

Archive snapshot and restore it again(Dont do, it will take 24 hours)

Delete the snapshot and restore it again

Recycle bin (assign tag to AMI or Snapshot, Create a retention rule --> delete the image, snapshot, and recover)

Terminate EC2 instances, Delete images, Delete snapshots

Data Life Cycle Manager --> See the UTC time and create a policy and see the snapshot got created or not. and then delete the policy.

EC2 Image Builder --> Optional --> Create some Golden AMI --> Once done delete the complete pipeline, recipes, configs ad AMI's

TASKS

Launch 4 EC2 instances (2 in 1a 2 in 1b)

1. CROSS TASK (additional volumes + Root Volumes) - different AZ's

2. Increase the root volume size

3. Add additional volume and make it available to the user.

4. Play with attach and detach volume for Root and Additional volumes

--> detach 1a root volume and attach it to other new 1a EC2 instance as root vol (same AZ)

--> detach 1a root vol and attach it to other new 1a EC2 instance as additional vol (same AZ)

--> Assume you lost your pem file, and we need to login to the EC2 instance how?

--> Take a snapshot (Mumbai region) and copy to another region(Ireland region) --> from snapshot --> create volume --> attach it to ec2 instance(Ireland)

5. Extend the existing volume on Linux

6. New additional volume for Linux

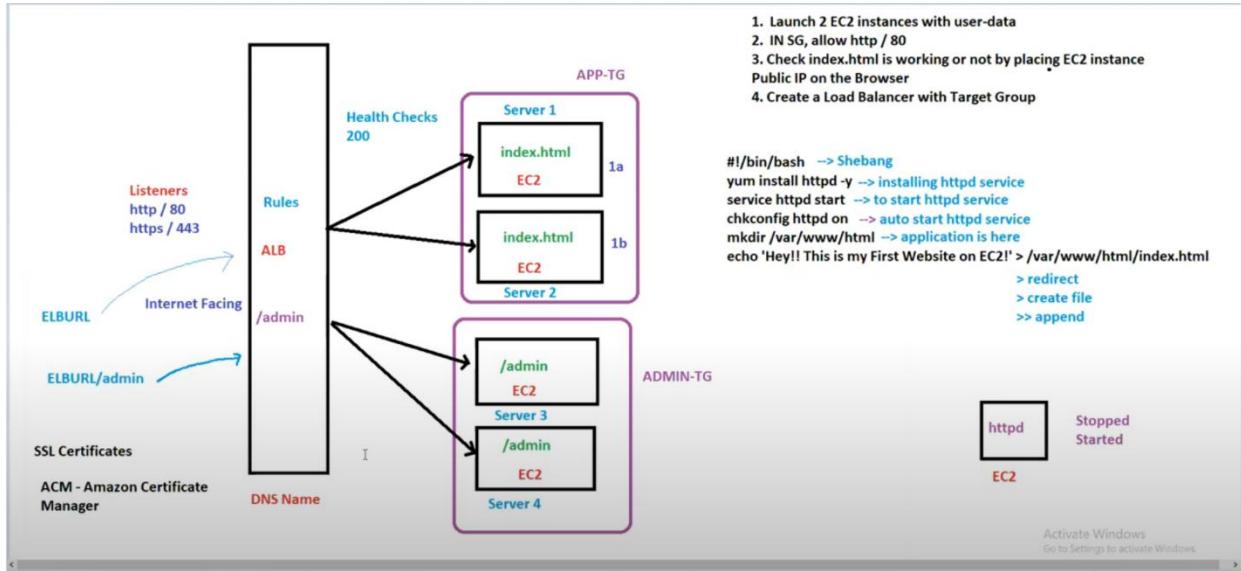
7. Life Cycle Manager policy and delete it --> make sure snapshots are created using UTC time (tag volumes properly)

8. Terminate EC2 instances

9. Delete additional volumes, life cycle policy [I](#)

Activate Windows
Go to Settings to activate Windows.

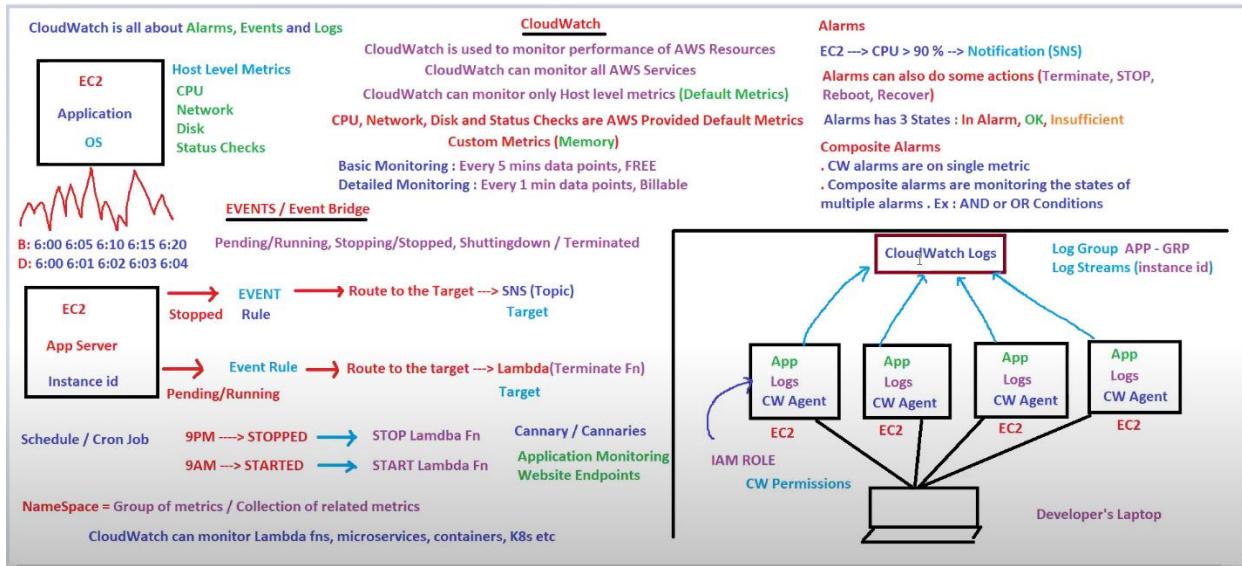
32ND SESSION AWS - EC2 INSTANCE LOAD BALANCER



33RD SESSION AWS - EC2 PRACTICAL 5 LOAD BALANCER

34TH SESSION AWS - EC2 PRACTICALS 6 = AUTO SCALING

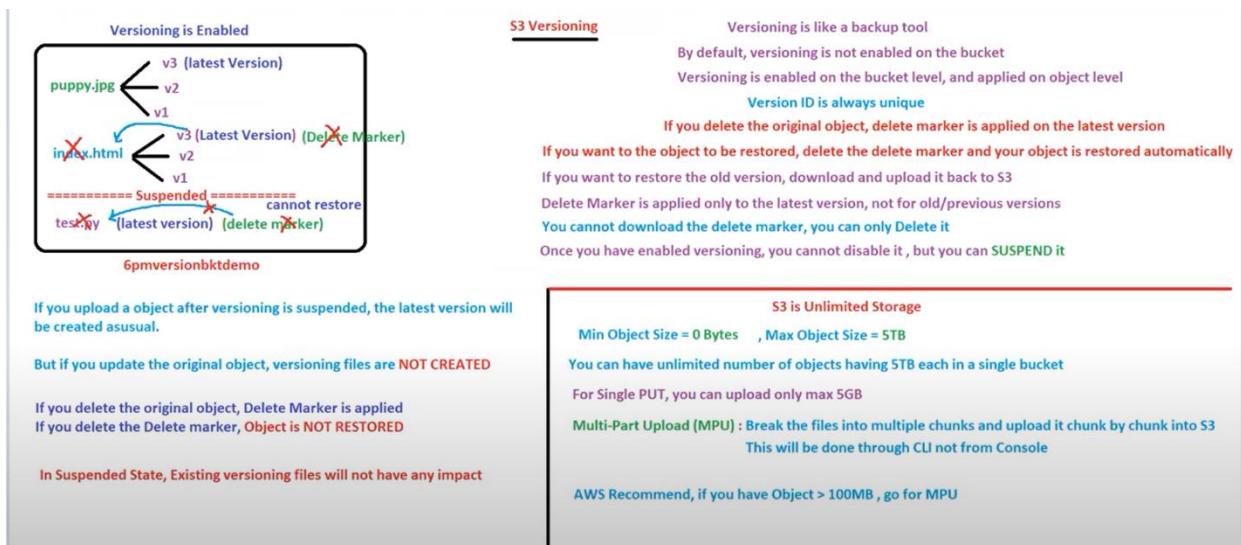
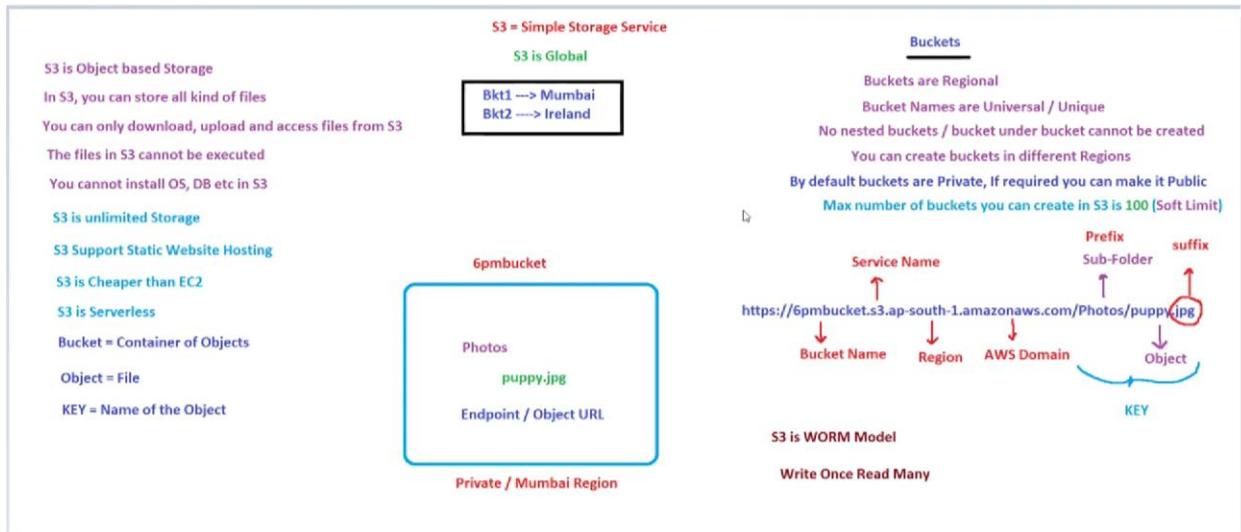
35TH SESSION AWS - CLOUDWATCH ALARMS EVENTS & LOGS



36TH SESSION AWS - CLOUDWATCH PRACTICALS ALARMS EVENTS & LAMBDA AWS CONSOLE

38TH SESSION AWS - ELASTIC BEANSTALK, ELASTIC BEANSTALK ARCHITECTURE, BLUE GREEN DEPLOYMENT

39TH SESSION AWS - S3 = SIMPLE STORAGE SERVICE, S3 VERSIONING



40TH SESSION AWS - S3 STORAGE CLASSES, GLACIER, LCM RULES, CORS, CRR, SRR, ENCRYPTION

While uploading the objects into S3, Selecting the Storage Class is Mandatory				Storage Classes	Availability : Anytime, Durability : Long time
Standard Frequently Access (FA)	Standard Infrequently Access (IA)	Reduced Redundancy Storage (RRS)	One Zone IA		
This is used for frequently access data	This is used for infrequently access data	Frequently access but NOT CRITICAL	Infrequently access data but NOT CRITICAL		
Default Storage Class	Retival Charges apply	No Retival Charges	Retival Charges apply		
Regular Purpose	Cheaper than FA	AWS doesnt recommend to use this Storage Class	Availability : 99.5%		
No Retival Charges	Availability : 99.9%	Cheaper than others	Durability : 11 9's		
Availability : 99.99%	Durability : 11 9's	Availability : 99.99%	Min Object Size = 128KB		
Durability : 11 9's	Min Object Size = 128KB	Durability : 99.99%	Min Duration = 30 days		
Min Object Size = 0 Bytes	Min Duration = 30 days				
Intelligent Tier		Glacier	Glacier has Retival Options	Deep Glacier	Life Cycle Management
Unknown Access Patterns		Infrequently access data	Expedited : 1 to 5 mins Standard : 3 to 5 hours Bulk : 5 to 12 hours	Min Duration = 180 days	Life Cycle Rule
Availability : 99.9%		Archiving Purpose	Availability : 99.99%		It is possible to move the objects from one Storage Class to another Storage Class automatically by created Life Cycle Rules
Durability : 11 9's		Vault : Container of Archives	Durability : 11 9's		Life Cycle Rules can be applied for entire bucket or for Prefix(Sub-folder)
Min Duration = 30 days		Archive : Object / .zip	Min Duration = 90 days		
		1 Archive can be upto 40TB	1000 Vaults		
		Unlimited number of archives in 1 Vault	Retival Charges apply		

Life Cycle Rules are created on bucket level but applied on object level

Transistion and Expiration

LCM Rules	Current version	Previous Versions
FA ---> IA (30 days) ---> Glacier (60 days)	Transistion	
0th day ---> 30th day ---> 60th day		
---> Delete after 365 days	Expiration	

Object Lock

Permanently
Certian period of time

Object Level logs

can be seen / captured in CloudTrail

Life Cycle Management

Athena : Analyze the logs directly from S3

Server Access Logs (Bucket Access Logs)

Bucket Name : Movies

movieaccesslogs

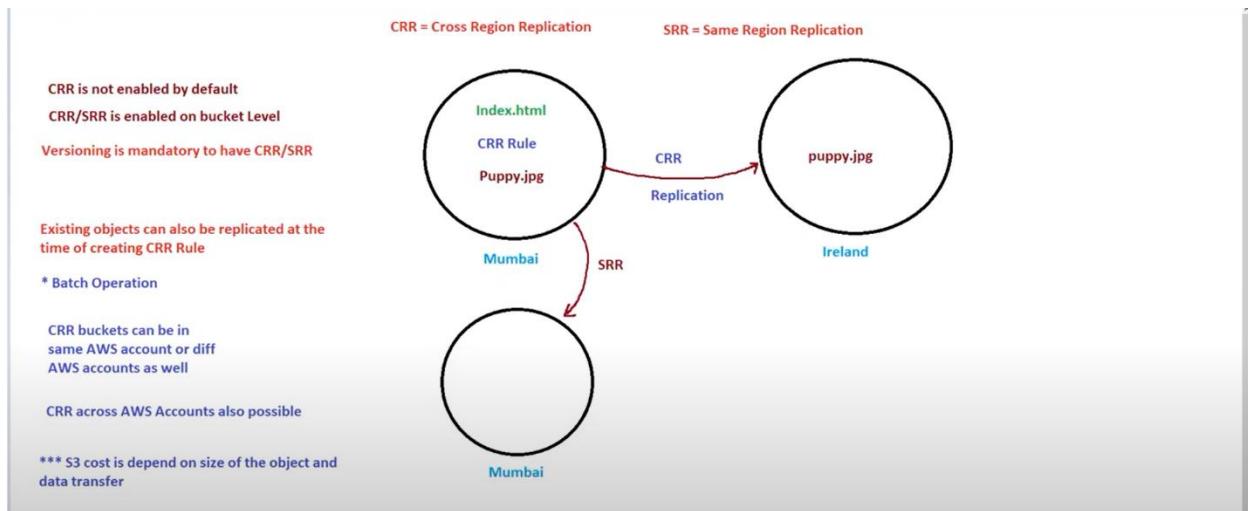
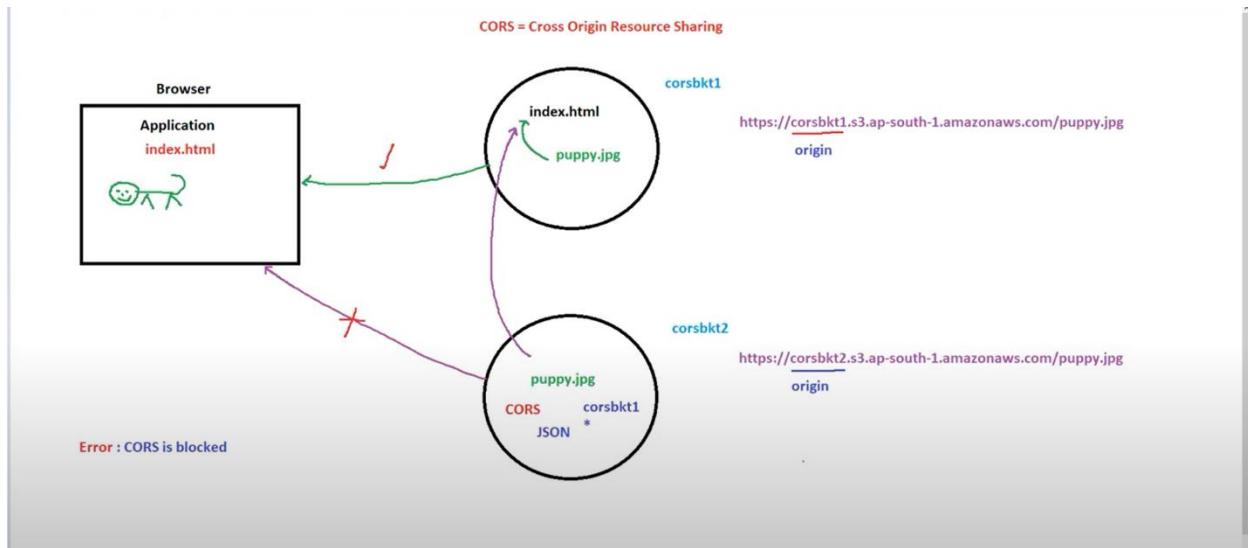
Server access logs are bucket level

Who is accessing your bucket

192.168.10.106pmbucketpuppy.jpgGETsuccess200

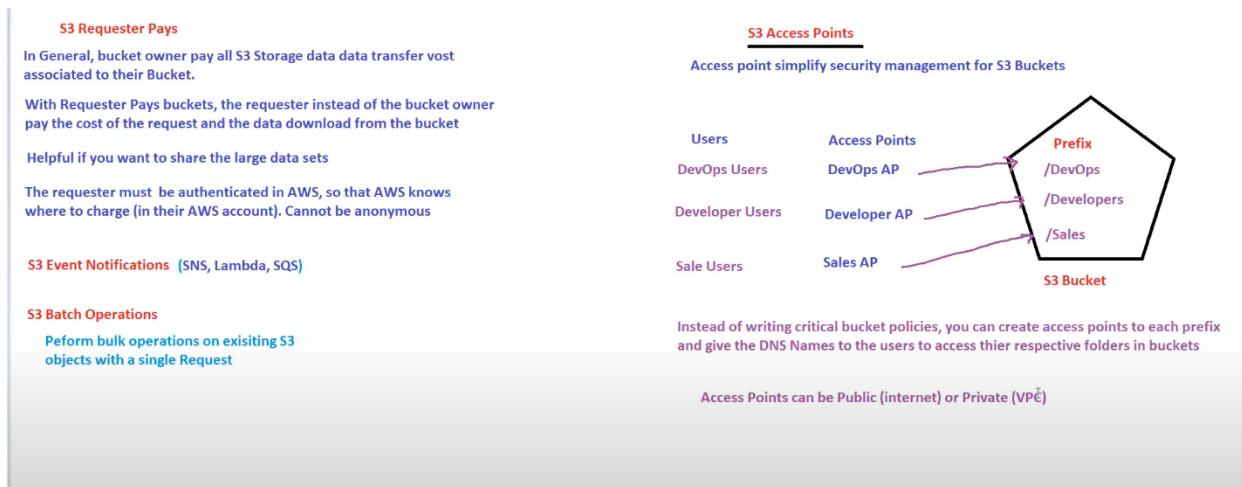
SQL Queries

IP	Src	Dest	Obj	Method	URL	Time



<p>Encryption can be done in 2 ways</p> <p>In-Transit Encryption : Encryption while data is moving / Transferring HTTPS</p> <p>Data at Rest Encryption : Encryption while data is at Rest , KMS</p> <p>Amazon Certificate Manager (ACM)</p> <p>is where you can generate HTTPS Certs (In-Transit)</p> <p>Key Management Service (KMS)</p> <p>is where you can create Encryption keys for data at Rest</p> <p>Pre-Signed URL</p> <p>(Temporary access for certain period of time to the user through a temporary object URL)</p>	<p>Encryption</p> <p>Amazon S3 has 3 types of Encryptions</p> <ul style="list-style-type: none"> Server Side Encryption SSE - S3 (AWS Managed Key) * SSE - KMS (AWS KMS Key) SSE - C (Customer Provided Keys) <p>By Default , Bucket Encryption is Enabled</p> <p>AES - 256</p> <p>Advance Encryption Standard</p> <p>Client Side Encryption : Should be handled by Customer</p> <p>In-Transit Encryption : HTTPS</p> <p>S3 Data Consistency Models</p> <p>Read after write for PUTS of New Objects</p> <p>Eventually Consistency for OVERWRITES of PUTS and DELETES</p> <p>Transfer Acceleration</p> <p>Ireland → Ohio → Tokyo → Sydney</p> <p>AWS network → CDN → internet - 5mins → Hyderabad</p> <p>Faster upload</p>	<p>Bucket</p> <p>ACL - Access Control List</p> <p>Using ACL you can control buckets permissions/access</p>
--	--	--

41ST SESSION AWS - S3 REQUESTER PAY S3 EVENT NOTIFICATION S3 BATCH OPERATIONS S3 ACCESS POINT S3 PRA



--> Delete the Application
Upload your own application and redeploy with latest application

S3: Simple Storage Service

TASKS

1. Create private bucket(Disabled ACL) and upload the objects and access it
2. Create a public bucket(enable ACL) and upload the object and access the object using Object URL
--> Make sure you make the object public --> Action --> "Make Public"
3. Create a bucket (public or private) with versioning enabled
upload the objects and check versioning
4. Suspend the versioning and perform few tasks on the objects
upload the objects and check versioning
5. You should receive the notification if anyone upload a object inside the bucket (you should use S3 EVENT)
6. Enable Server access logs on S3 Bucket
7. Setup static website hosting on S3.
--> create a public bucket with ACL enabled
--> upload all your images, html files (download sample html template from internet)
--> select all objects and make public
--> go to bucket properties --> enable static website hosting --> index.html and error.html --> Access the URL
8. Delete all buckets
9. Exploring Task: Access Points

42ND SESSION AWS - S3 CORS BUCKET

8. Simulate CORS

Create 2 buckets name bkt1 and bkt2 --> public

upload index.html and load.html on bkt1 --> enable website hosting

Access the bkt1 website endpoint, load.html will load because load.html is in same bucket

upload load.html only on bkt2, make it public

take the load.html url/Endpoint from bkt2

update the URL on index.html on bkt1 (load load.html from bkt2 on bkt1)

Access the bkt1 website endpoint, load.html will NOT load, because load.html is in another bucket

enable cors on bkt2

Now, access the bkt1 index.html, load.html will work now, because CORS is enabled

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html> ---> get json from here

8. CORS Task

9. Setup Life cycle rules

11. CRR implementation

bkt1 --> bkt2

bkt2 --> bkt3

12. SRR implementation (Create 2 buckets in the same region and enable SRR)

13. From your account --> Create 2 IAM users called user1 and user2

Create 2 buckets in S3, user1bkt and user2bkt

1. create IAM policy and achieve it

2. Try with bucket policy also

logout from your account

login as user1 and access user1bkt (should be access) , access user2bkt(should not access)

logout user1

login as user2 and access user2bkt (should be access) , access user1bkt(should not access)

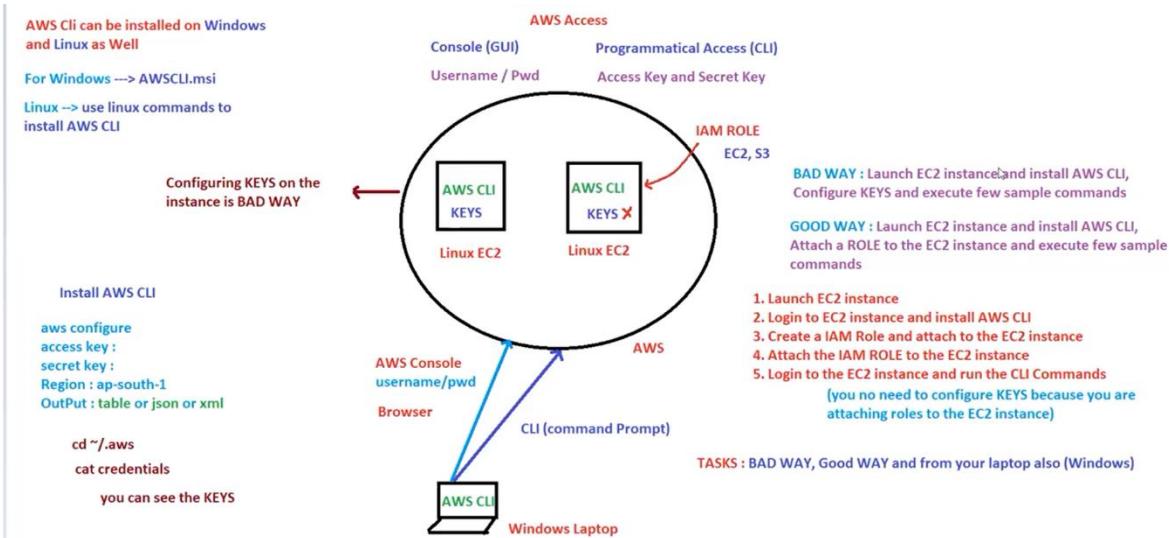
S3 Acces Point setup

14. Download S3 browser --> Add account --> Provide KEYS --> Start accessing S3 or put the data in buckets

15. Download Fast Glacier

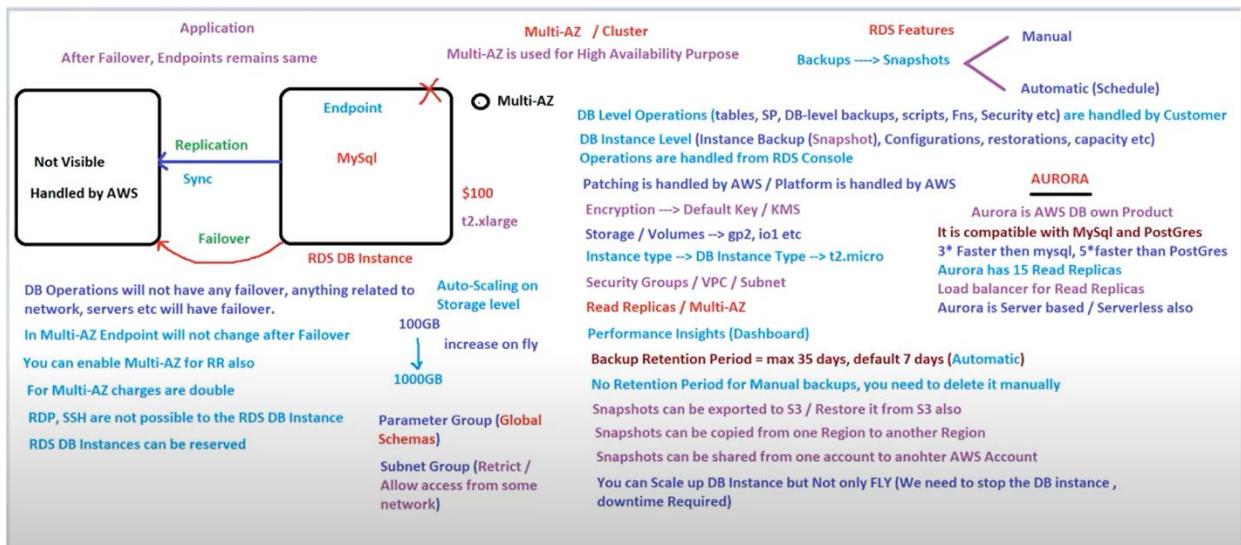
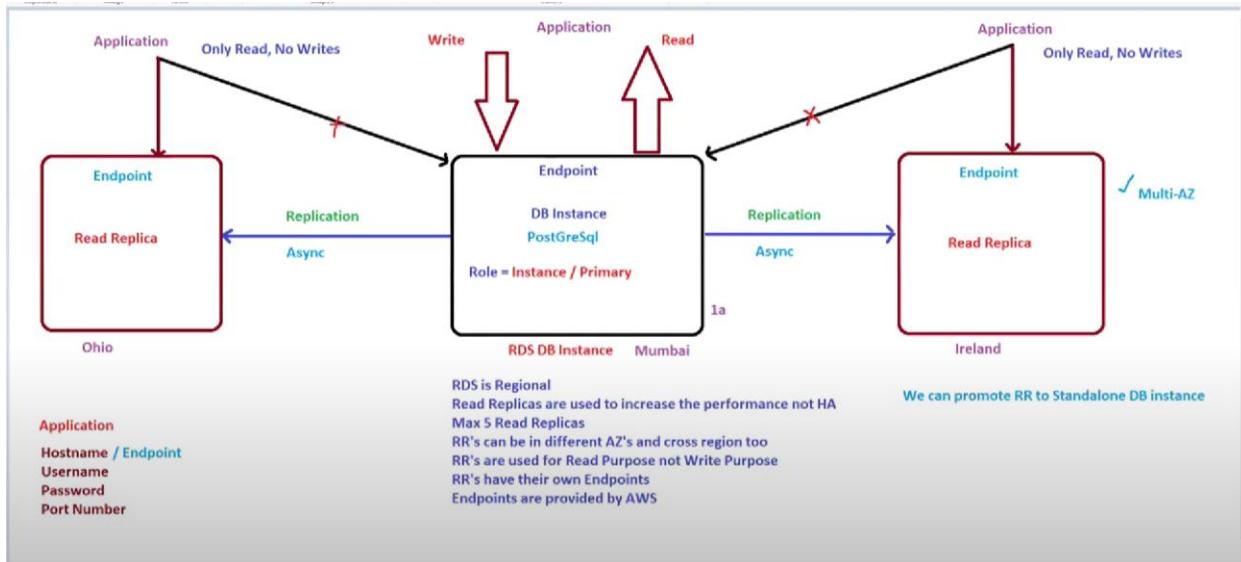
43RD SESSION AWS - EFS SERVICE DEMO & PRACTICALS AWS CONSOLE

44TH SESSION AWS - CLI TUTORIAL & PRACTICAL IN AWS CONSOLE



46TH SESSION AWS - STORAGE GATEWAY SERVICE TUTORIAL & PRACTICALS

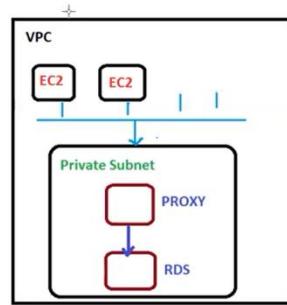
47TH SESSION AWS - RDS, RDS PROXY



AWS RDS PROXY

- . Fully managed database proxy for RDS
- . Allows apps to pool and share the DB Connections established with the database
- . Improving database efficiency by reducing the stress on the database resources (Eg CPU, RAM) and minimize open connections (and timeouts)
- . Serverless, AutoScaling, HA
- . Support MySql, Postgres, MariaDB, MSQL and Aurora
- . Secret Manager is a AWS Service where you can store all secrets (keys, usernames, passwords etc).
- . RDS Supports Secret Manager to get credentials
- . RDS PROXY is never Publicly accessible (must be accessed from VPC)

RDS Proxy will allow your applications to pool and share the db connections established with the db instead of having every single app connect to rds instance they will be instead connecting to the proxy and proxy will pool these connections together into less connections to the RDS DB Instance



48TH SESSION AWS - RDS PRACTICAL

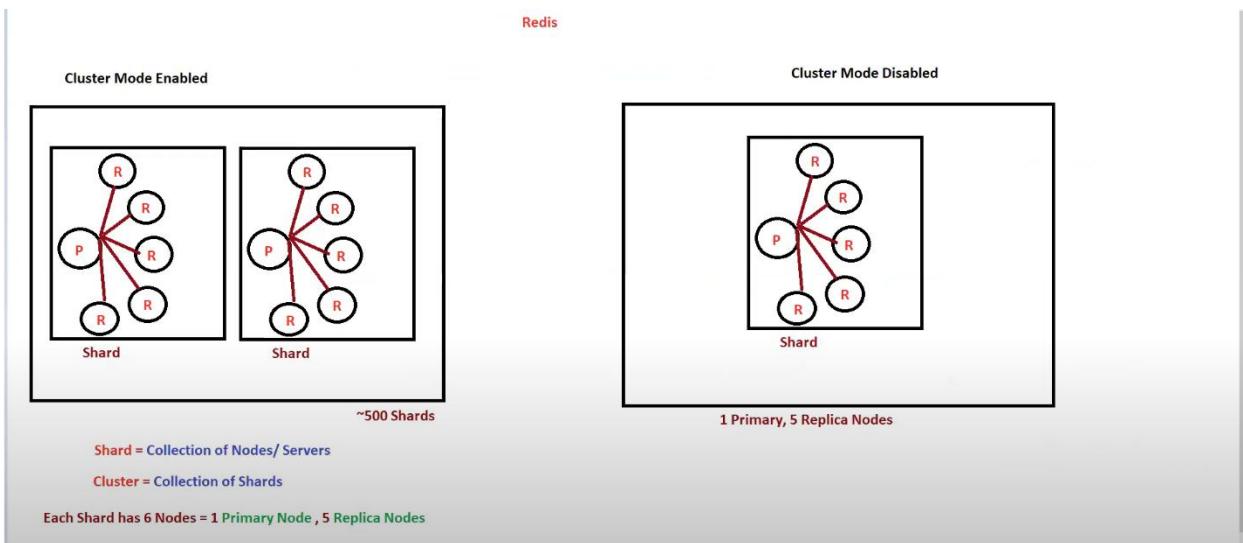
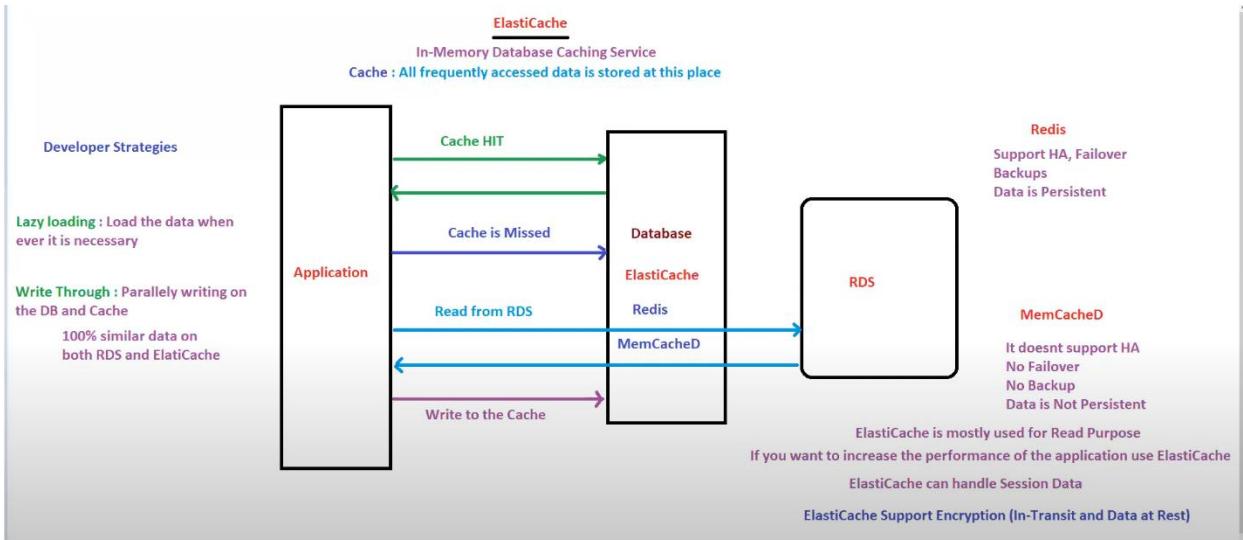
```
sudo yum install nfs-utils -y
mount -t nfs -o nolock,hard 172.31.29.167:/filegateway730am filegateway/
cd filegateway
mkdir filegateway
```

```
*****
RDS TASKS
*****
```

1. Launch Postgres or MySQL DB Instance in free tier
2. Modify Default Security Group: add postgres and mysql ports
3. Download PgAdmin or Sqlectron or any client tool
4. Connect to the RDS Db Instance using endpoint, username and Pwd(try to create a small table or a database)
5. Take a manual snapshot, copy snapshot, try encrypted snapshot, upgrade snapshot, share snapshot, migrate snapshot, export to S3, restore from S3.
6. Create a Read Replica in another region(modify Ireland SG(add port numbers), connect to it and try to create a DB or table)
7. Restore a DB from the snapshot
- Check the logs in CloudWatch logs
8. Delete the RDS instances in Mumbai and RR in Ireland
9. Delete the manual snapshot and logs in CW
10. Promote RR to standalone
11. Delete RDS instance, replica, Manual snapshot, any snapshot in S3 and CloudWatch logs
12. Launch one EC2 instance and connect to RDS
13. Export Snapshot to S3 and Restore it to RDS instance (Postgres or MySQL)

Sample application with a registration form and update details to RDS Database (submit and fetch the data from RDS)

49TH SESSION AWS - ELASTIC CACHE SERVICE, REDIS TUTORIAL & PRACTICAL



```

# App code
save_user(17, {"name": "Kevin McGehee"})
user = get_user(17)

# Write Through
def save_user(user_id, values):
    record = db.query("update users ... where id = ?", user_id, values)
    cache.set(user_id, record, 300) # TTL
    return record

# Lazy Load
def get_user(user_id):
    record = cache.get(user_id)
    if record is None:
        record = db.query("select * from users where id = ?", user_id)
        cache.set(user_id, record, 300) # TTL
    return record

```

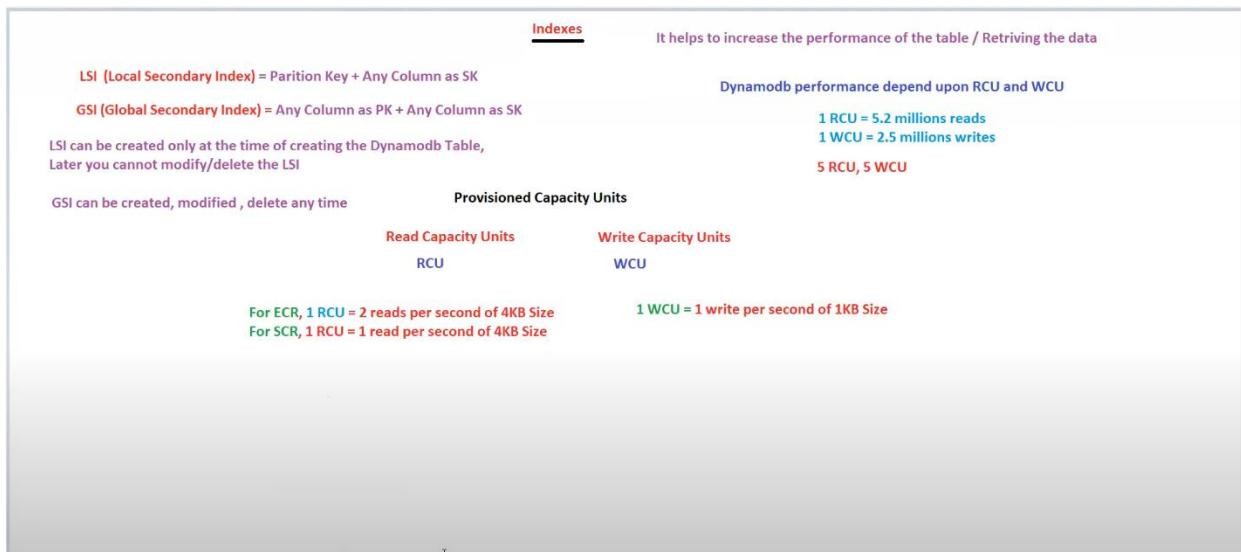
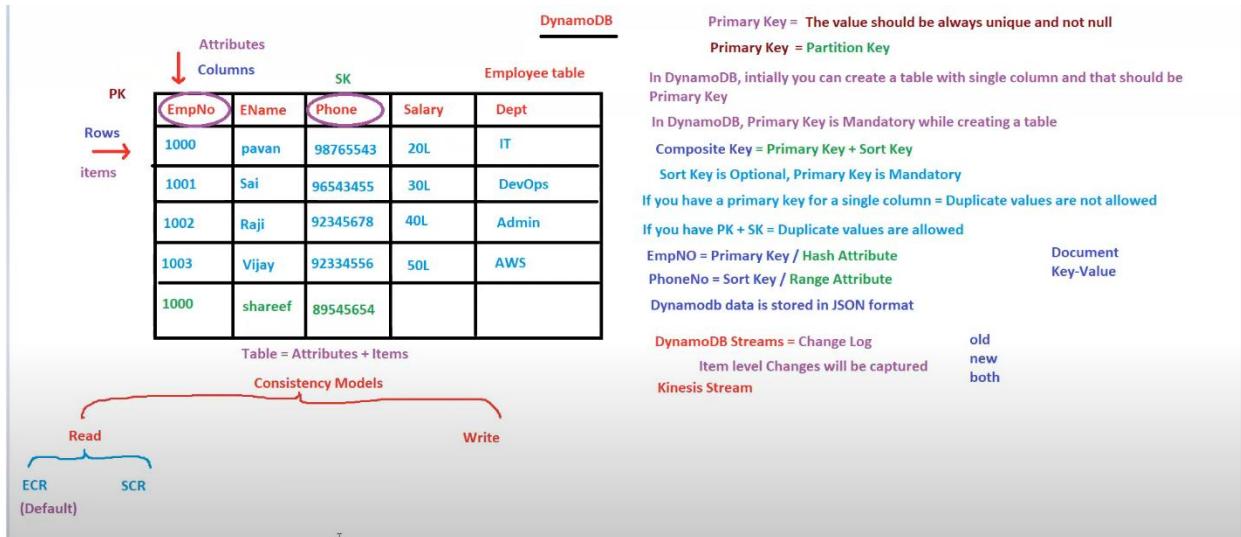
Write Through

1. Updated DB
2. SET in Cache

Lazy Load

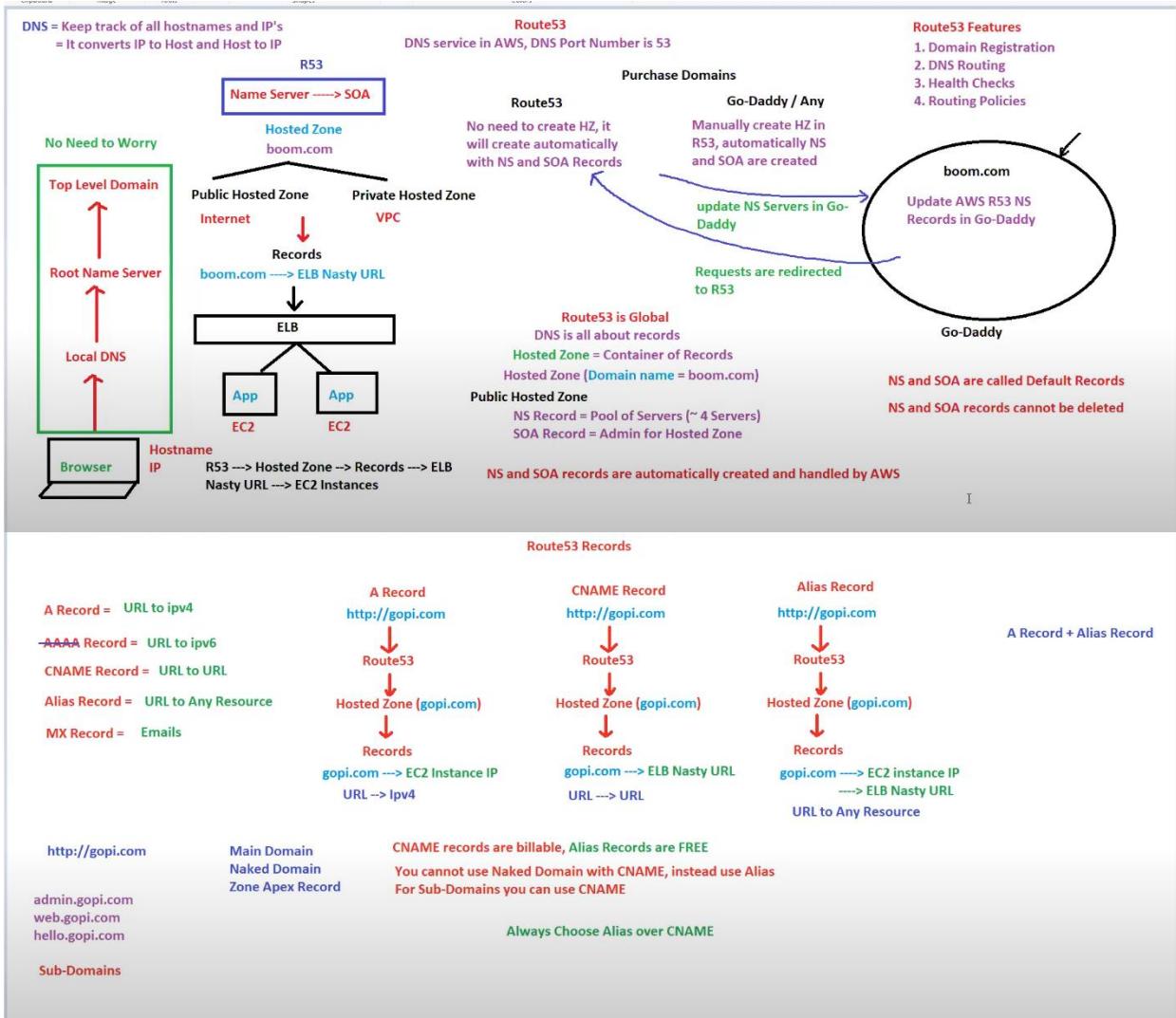
1. GET from cache.
2. If MISS get from DB
3. Then SET in Cache

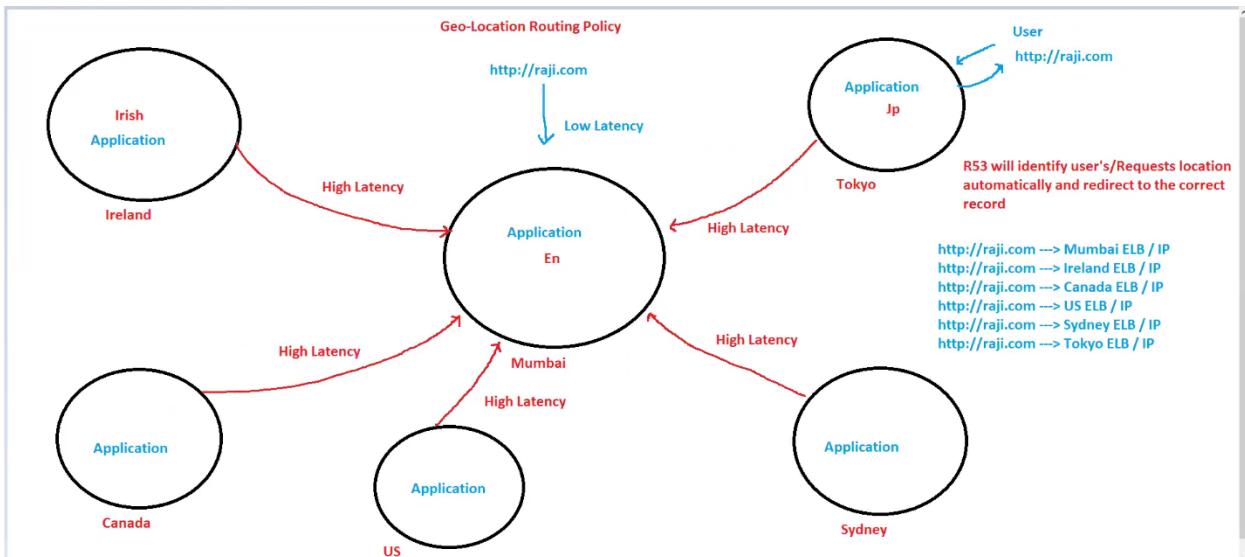
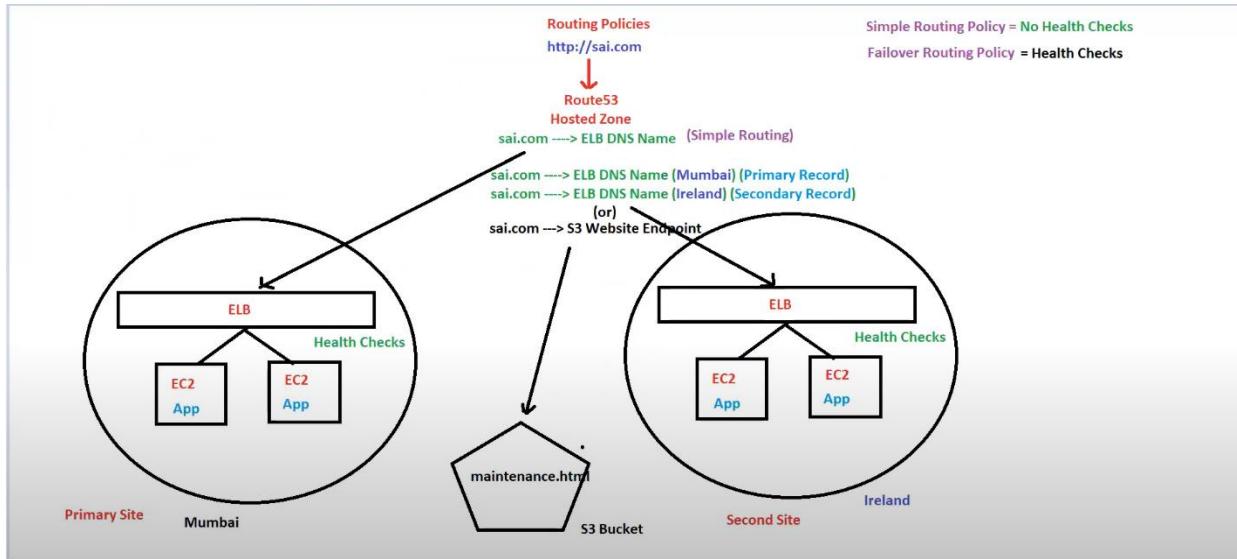
50TH SESSION AWS - DYNAMODB, INDEXES

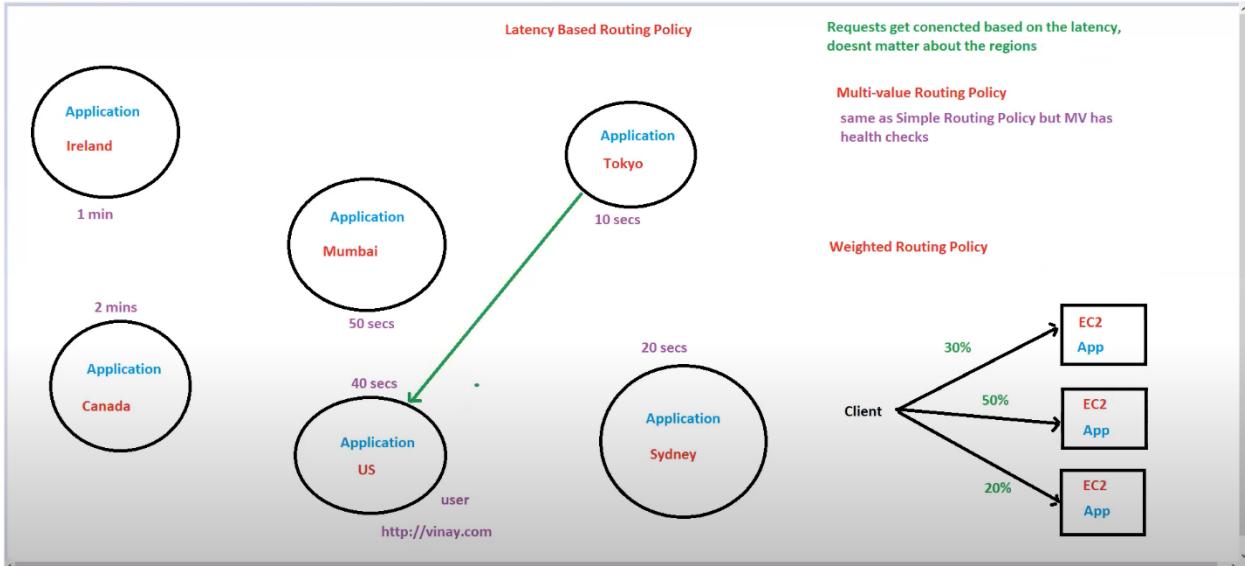


51ST SESSION AWS - DYNAMODB PROVISIONING CAPACITY PRACTICAL IN CONSOLE

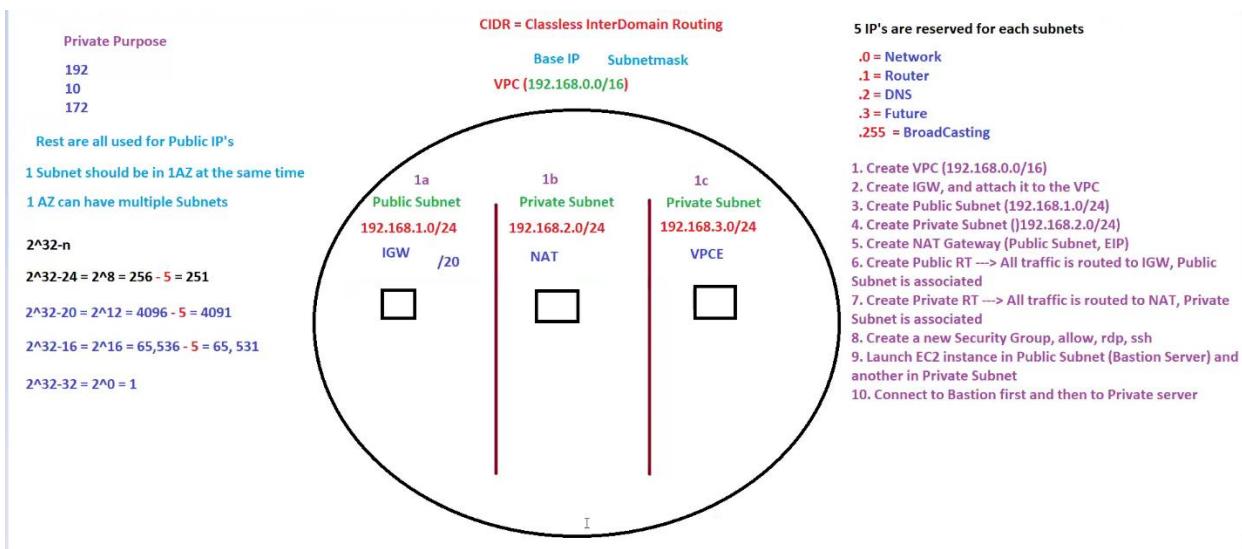
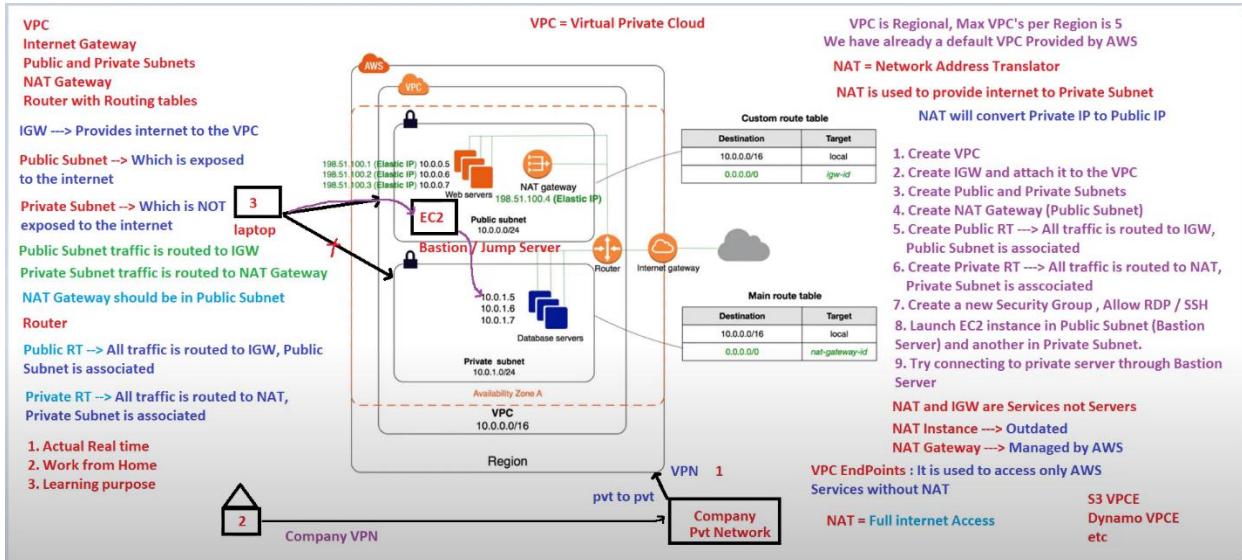
52ND SESSION AWS - ROUTE53 INTRODUCTION TUTORIAL







54TH SESSION AWS – VPC



55TH SESSION AWS - VPC PRACTICAL IN AWS CONSOLE

Login to the Bastion Server

Login with ec2-user

sudo -s

vi 6PMBATCH.pem --> copy paste all the data in here and save it

chmod 400 6PMBATCH.pem

ssh -i "6PMBATCH.pem" ec2-user@192.168.2.192(change this ip to your pvt server ip)

sudo -s

There are three types of VPC endpoints –

Interface endpoints, : has private link and uses ENI

Gateway Load Balancer endpoints : has private link and uses ENI

Gateway endpoints. works with Routing tables

|
|

56TH SESSION AWS - VPC PEERING PRACTICAL IN AWS CONSOLE

