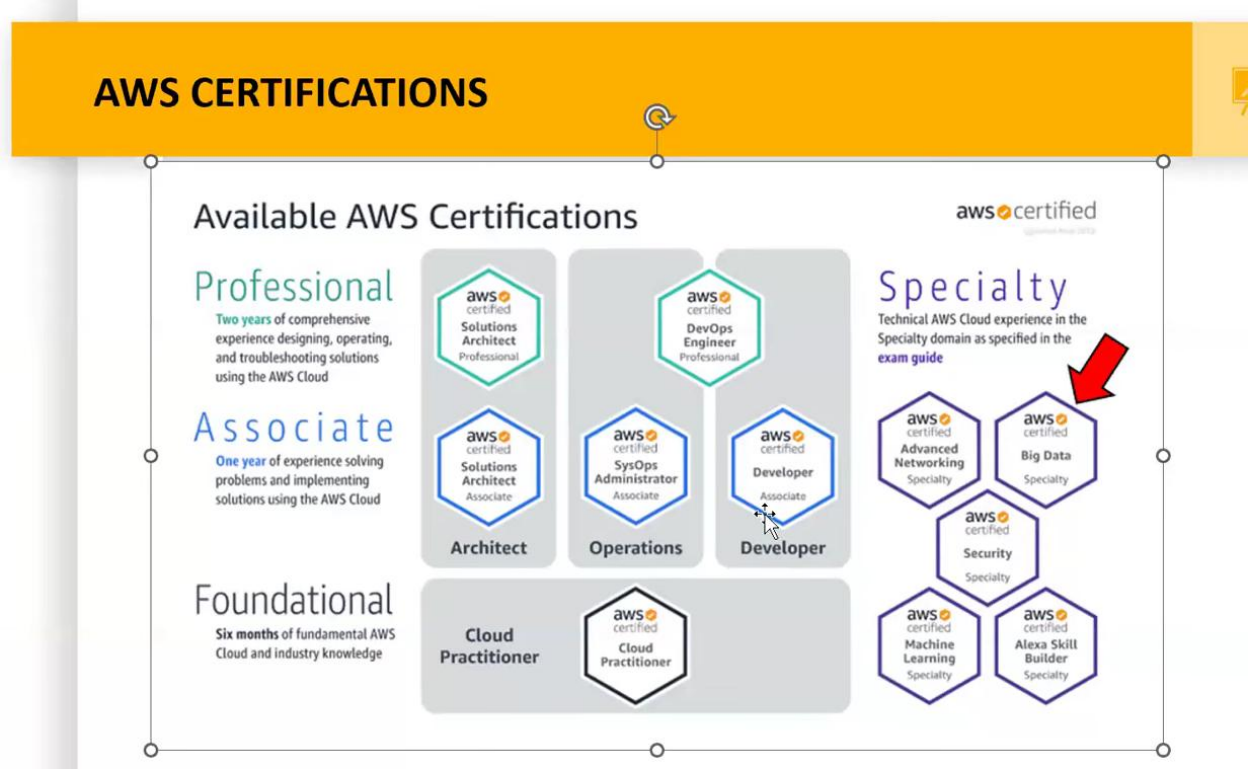
Contents

❖ COURSE OUTLINE

❖ AWS CERTFICATION

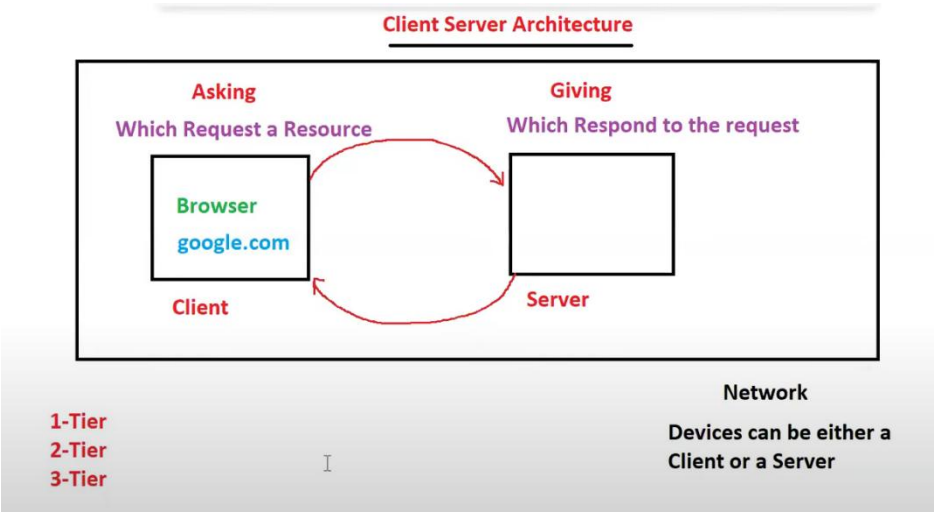


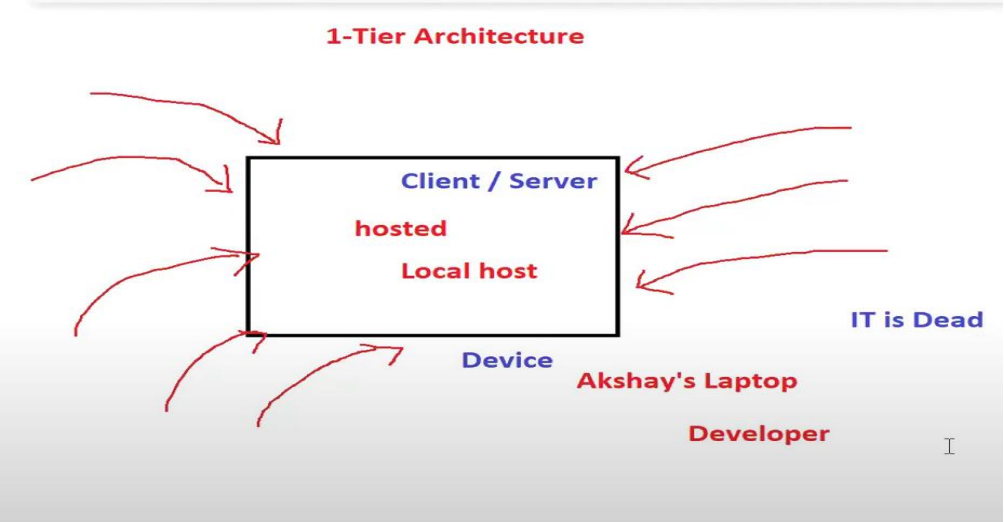
1ST SESSION AWS – INTRODUCTION

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

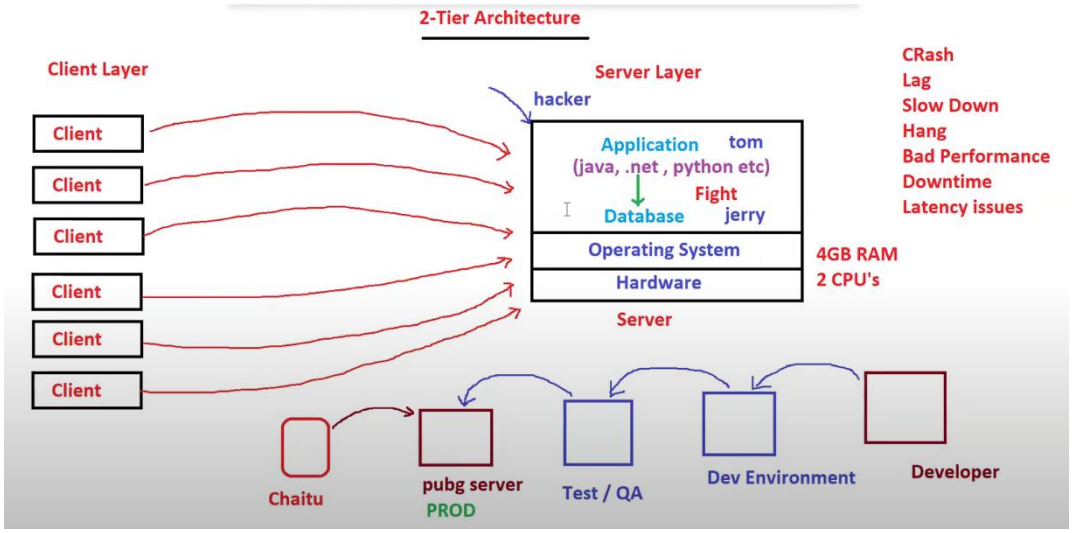
Introduction classes only.

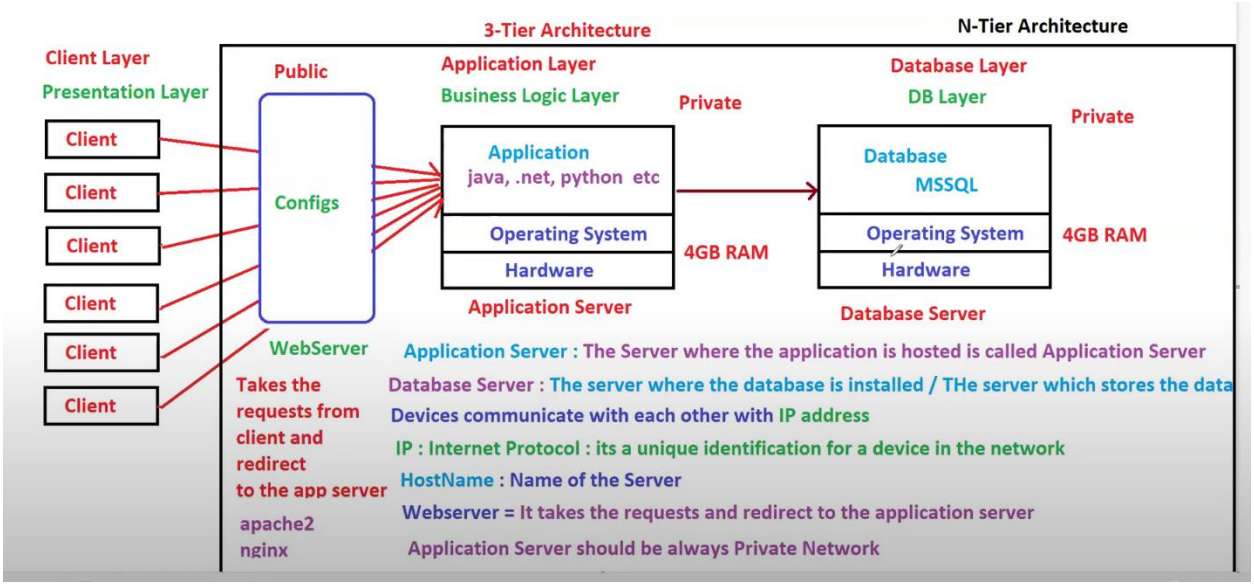
2ND SESSION AWS - CLIENT SERVER ARCHITECTURE



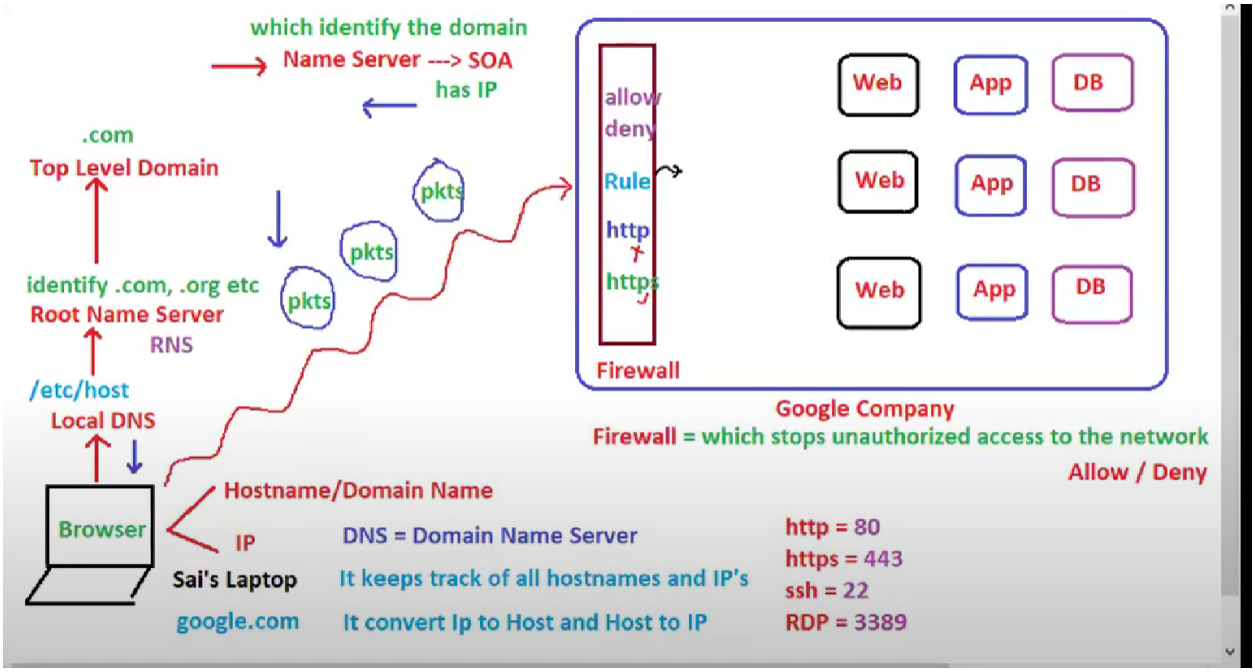


- What is Application SERVER (I.Q)?
- SERVER Where application is Installed.


2-Tier Architecture
Client Layer
Server Layer
hacker
Client
Client
Client
Client
Client
Client
Application tom
(java, .net , python etc)
Fight
Database jerry
Operating System
Hardware
Server
4GB RAM
2 CPU's
CRash
Lag
Slow Down
Hang
Bad Performance
Downtime
Latency issues
Chaitu
pubg server
PROD
Test / QA
Dev Environment
Developer

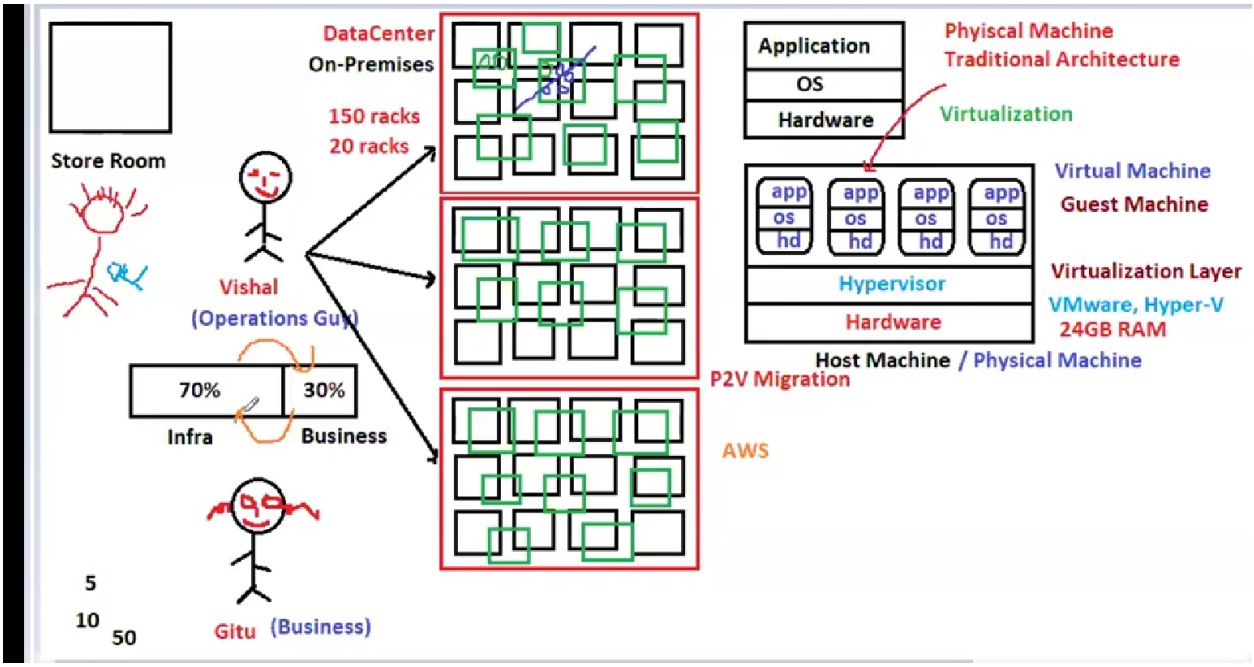

3-Tier Architecture
N-Tier Architecture
Client Layer
Presentation Layer
Public
Application Layer
Business Logic Layer
Private
Database Layer
DB Layer
Private
Client
Client
Client
Client
Client
Client
Configs
Application
java, .net, python etc
Operating System
Hardware
4GB RAM
Application Server
Database
MSSQL
Operating System
Hardware
4GB RAM
Database Server
WebServer
Takes the requests from client and redirect to the app server
apache2
nginx
Application Server : The Server where the application is hosted is called Application Server
Database Server : The server where the database is installed / THe server which stores the data
Devices communicate with each other with IP address
IP : Internet Protocol : its a unique identification for a device in the network
HostName : Name of the Server
Webserver = It takes the requests and redirect to the application server
Application Server should be always Private Network

3RD SESSION AWS – OVERVIEW



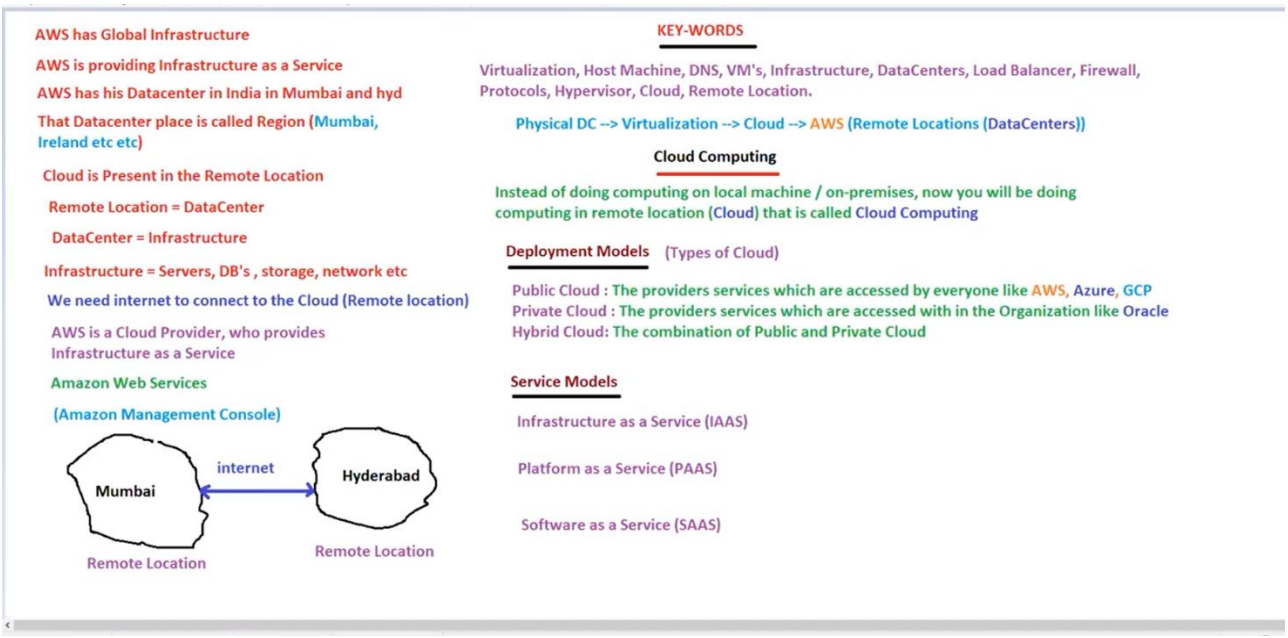
- ELB = Distribute the traffic on Round Robin algorithm.

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

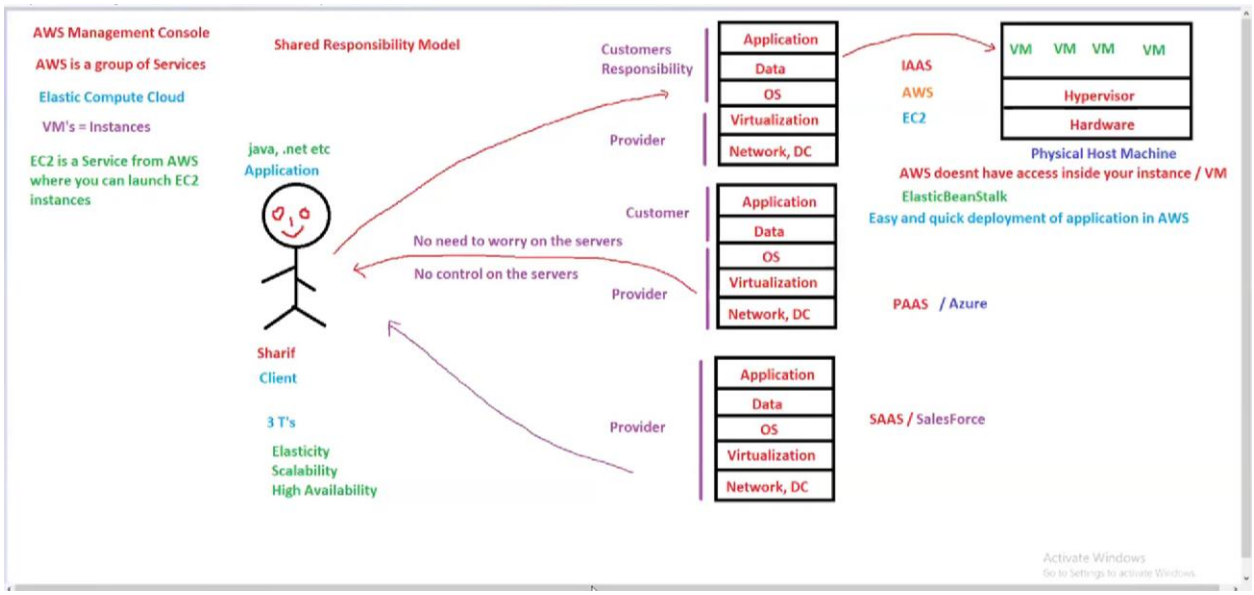


- Deployment Models:
  - Public Cloud: Provider that provide service to public. (all in cloud)
  - private Cloud: provider that provide service within an organization.
  - Hybrid Cloud: combination of Both private + public.

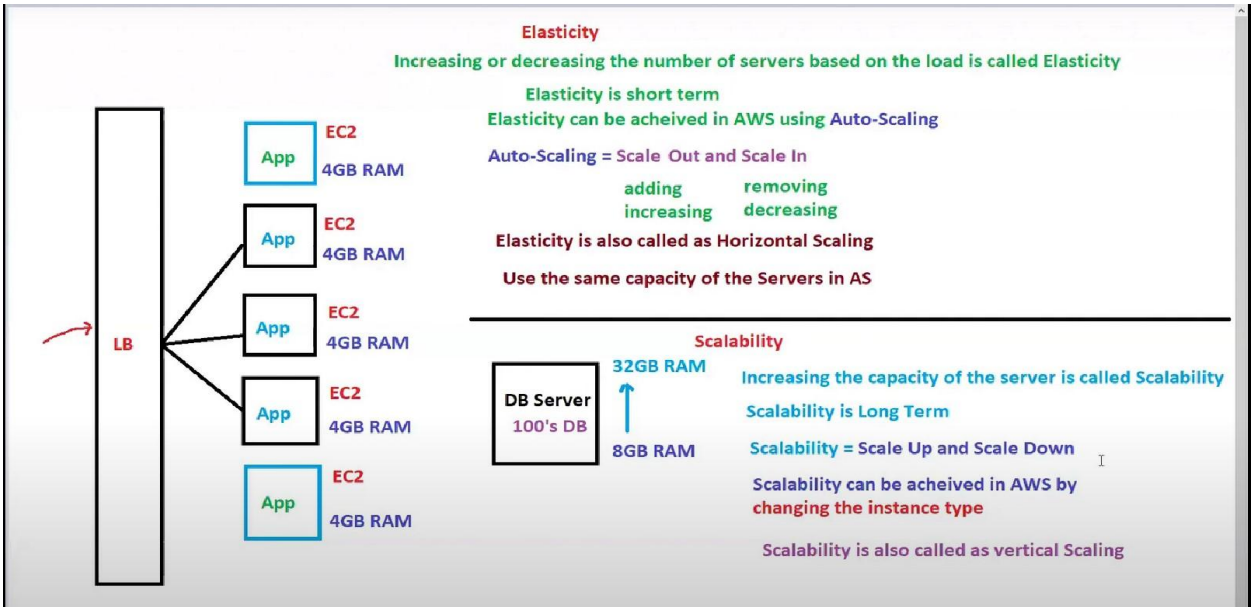
Three types of Service Models (Biryani Example)

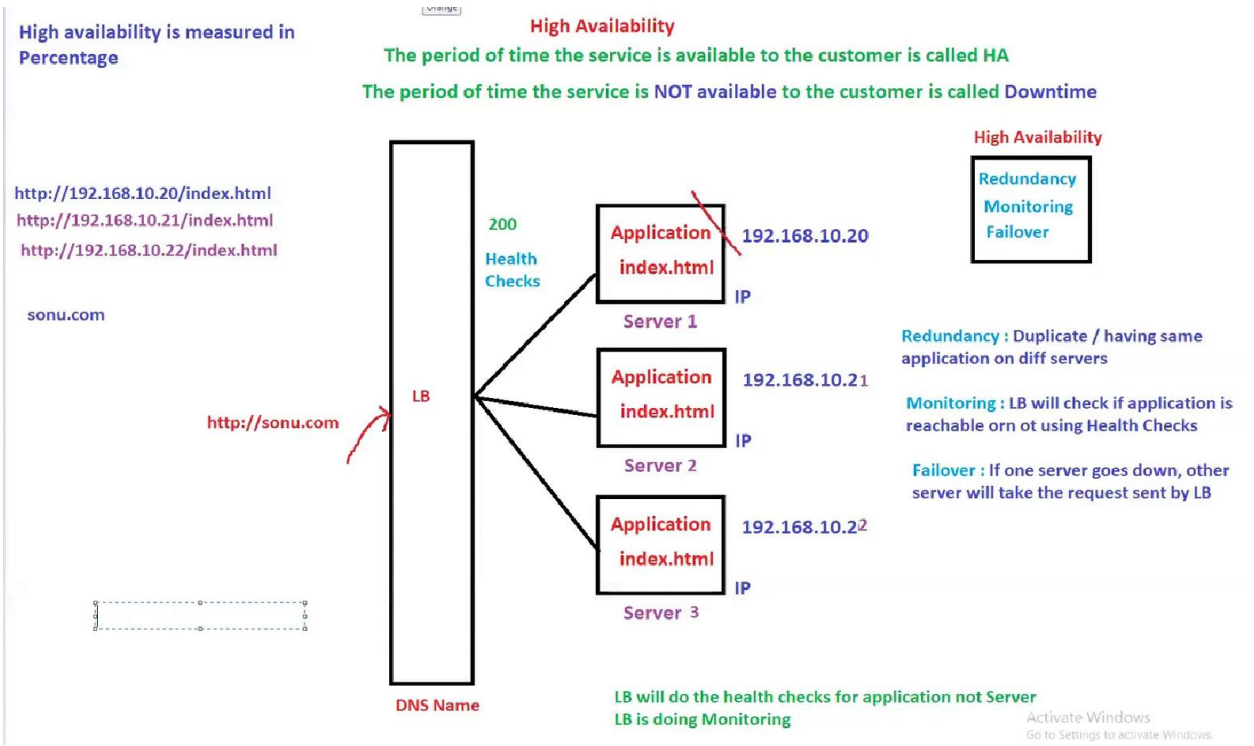
- Infrastructure as service (IAAS): Customer is responsible Application + Data and OS), Provider is responsible for (Network + Virtualization and Data Center). Example (Ec2 Service). user have full control over infrastructure like network, server, storage etc.
- Platform as a Service (PAAS): Customer 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

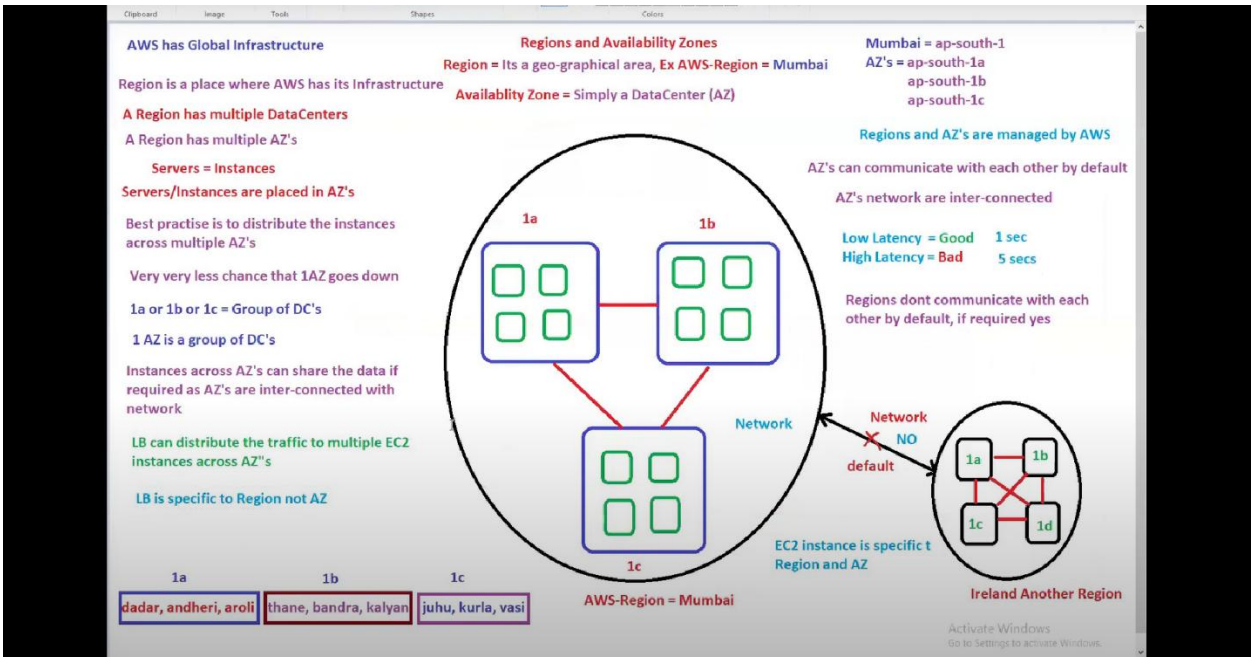
- Redundant Server = Duplicate server

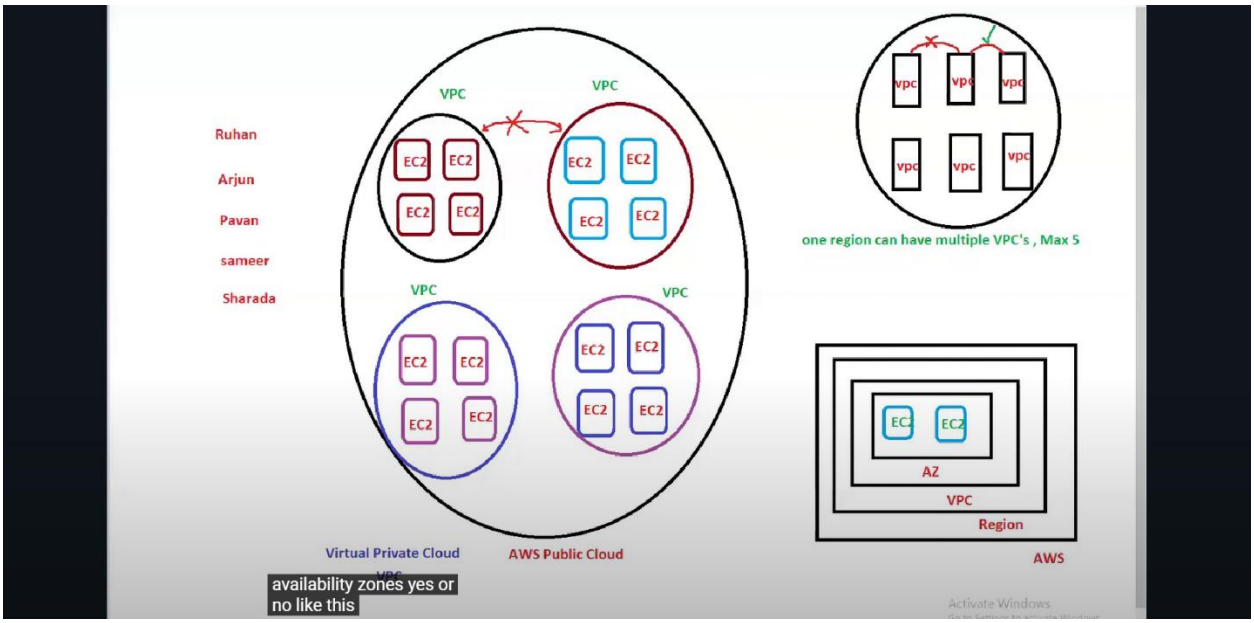
Load Balancer doing the Monitoring with application, perform regular Health check up with application (C.Q)

Redundancy:
Monitoring:
Fail-over:

are three key things to achieve the high-availability

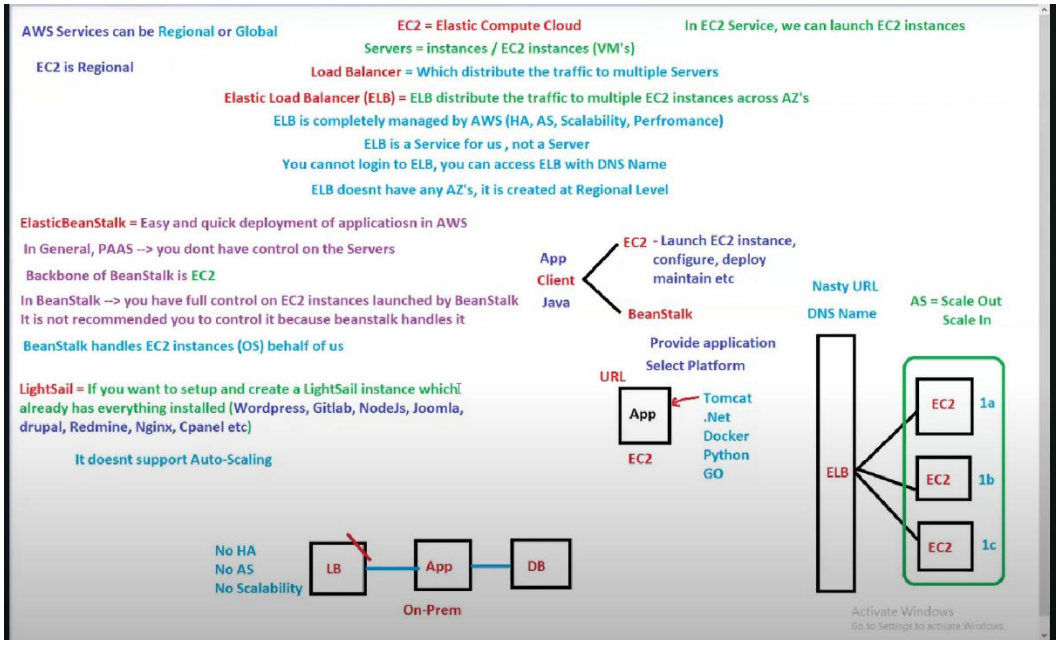
8TH SESSION AWS - REGIONS AND AVAILABILITY ZONES

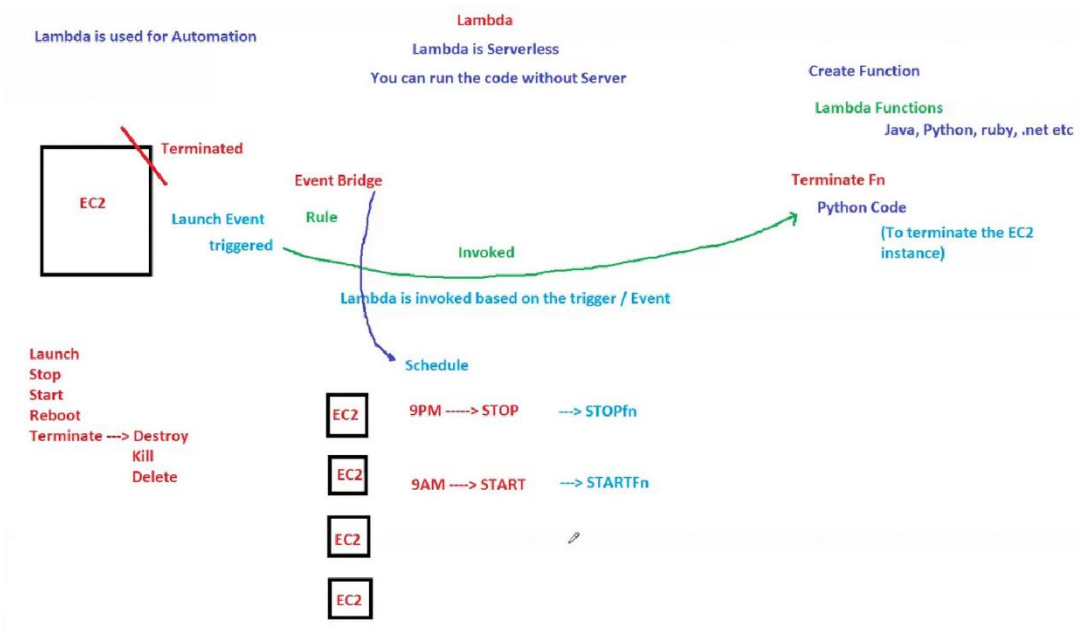




- It is recommended to launch ec2 instance in different availability zone. By Default, two AWS region cannot communicate (C.Q) but if require we can setup communication.

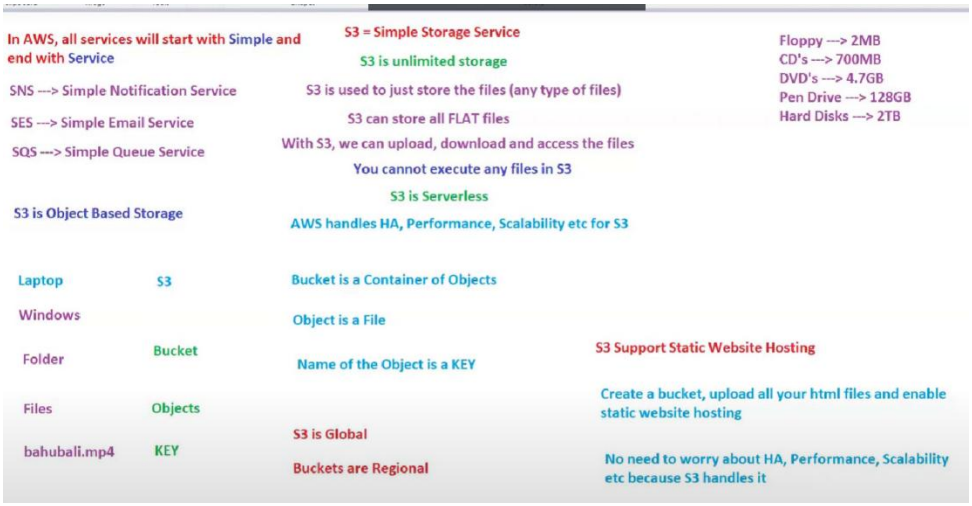
9TH SESSION AWS - SERVICES EC2, ELASTIC BEANSTALK, LIGHT SAIL, LAMBDA

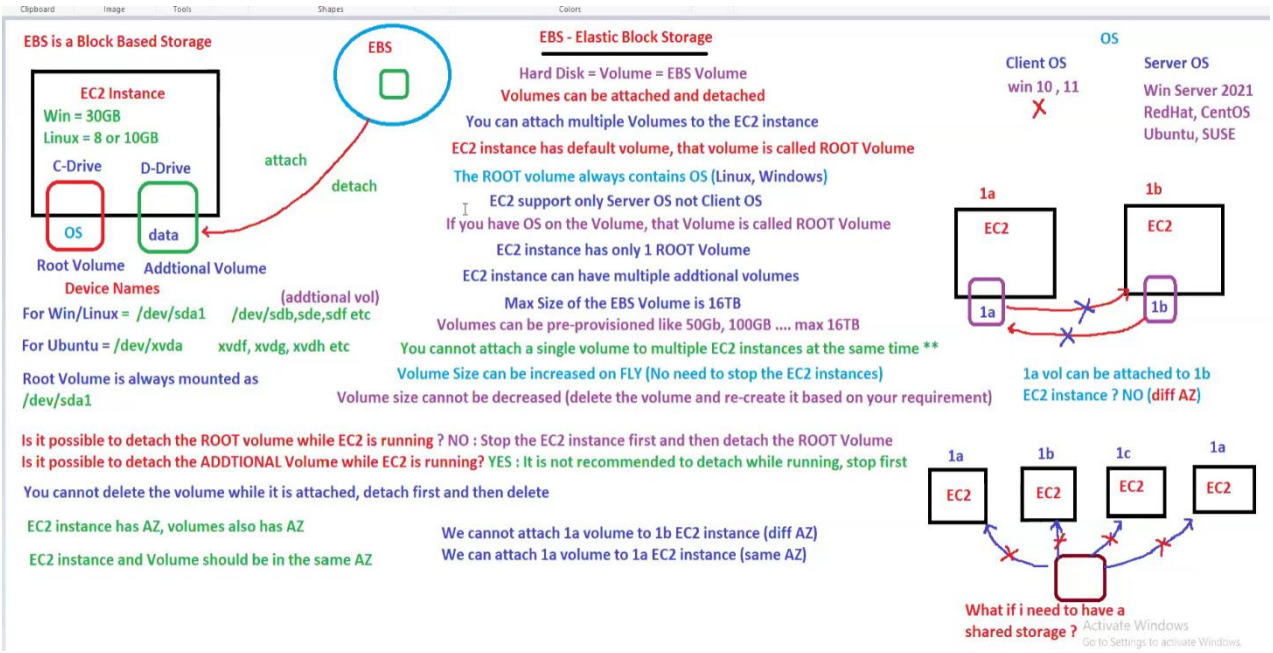




- Ec2 is regional Service (C.Q)
- Services are either or Regional
- Elastic Load Balancer (ELB) is a service not a server. It will not go down.
- Lambda is used for automation (C.Q)
- EC2 is a Backbone of Elastic Beanstalk and does not provide control over server.
- In Beanstalk we have application that 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

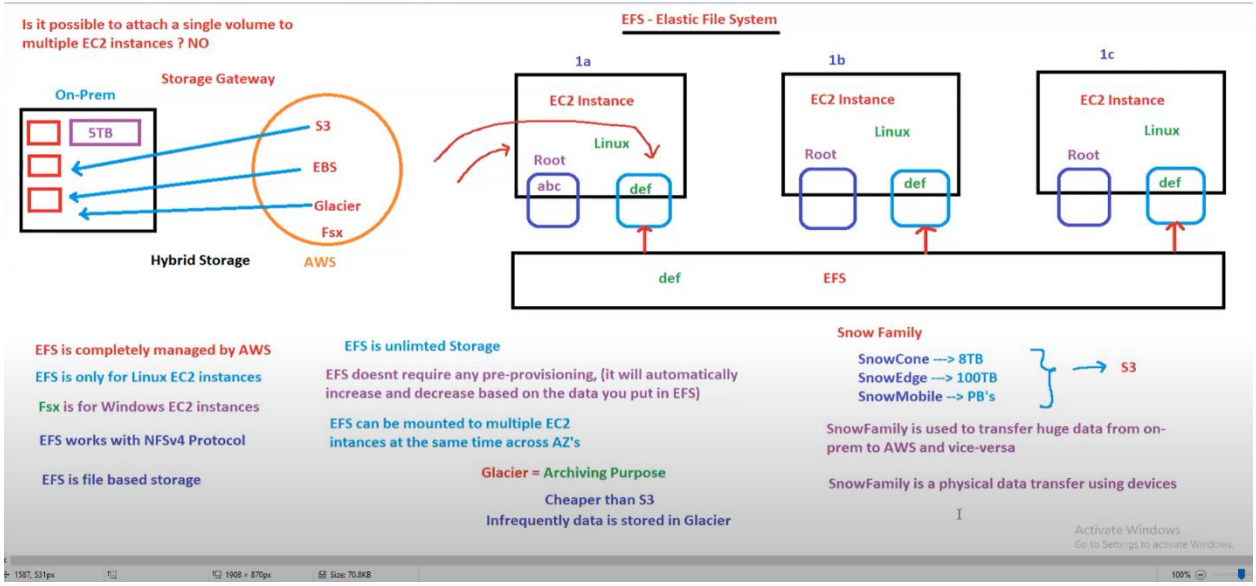
10TH SESSION AWS - STORAGE S3, EBS

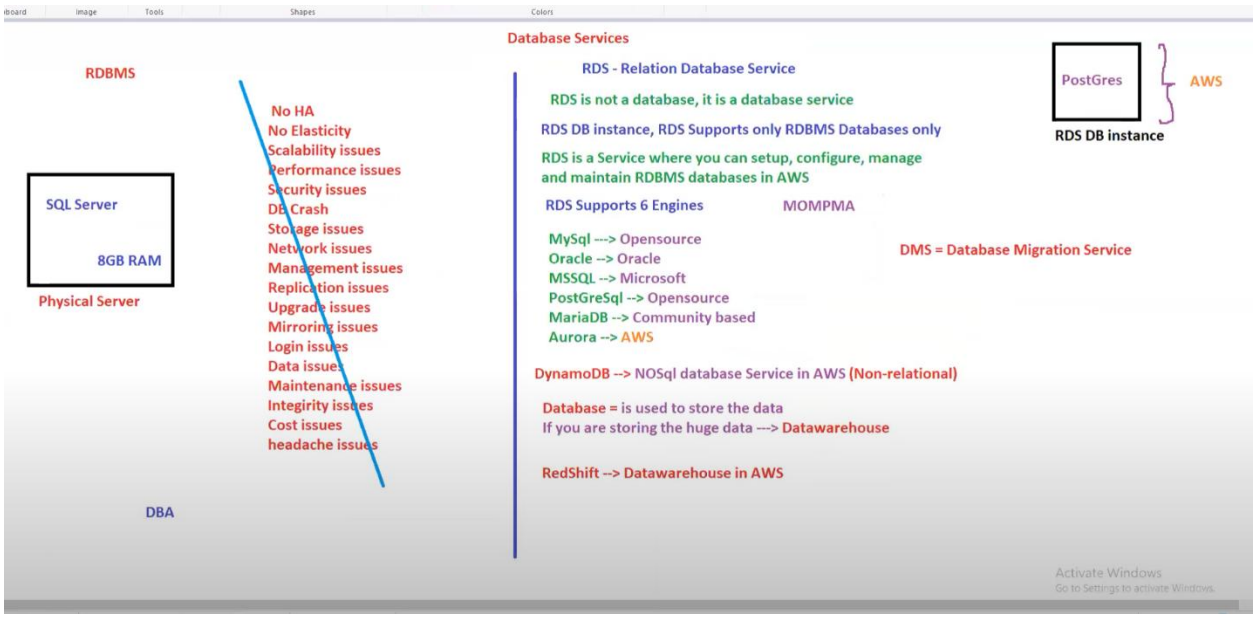


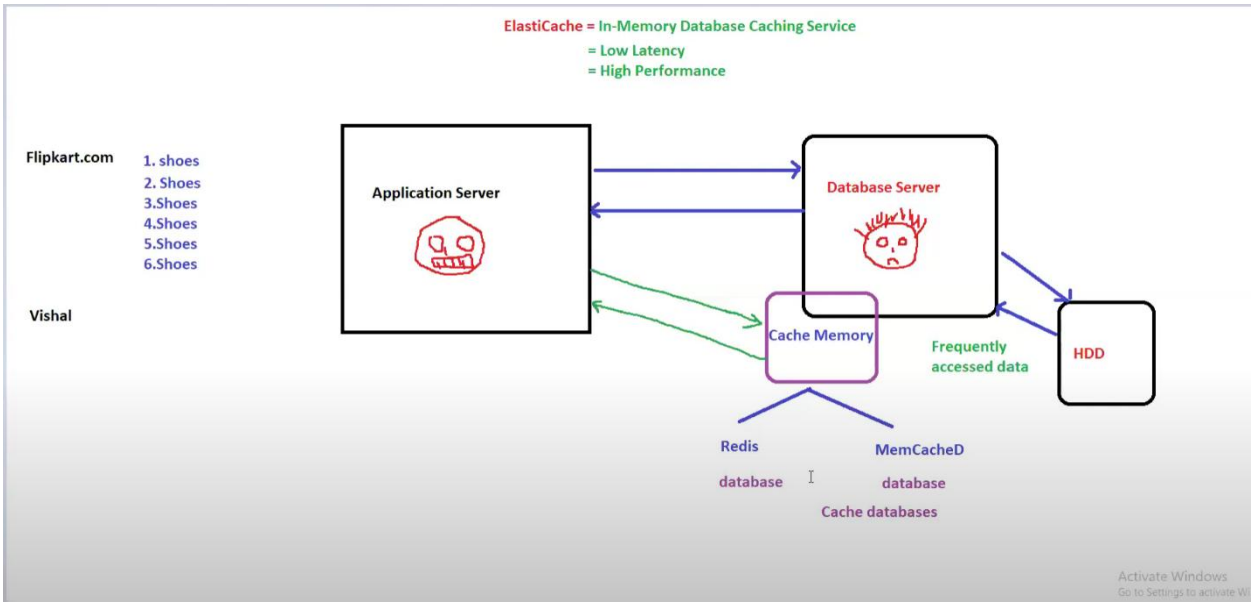


- It is best to host static website on s3(Simple Storage Service).
- S3 is object Based Storage.
- Elastic Block Storage (EBS): EBS is a Block based storage.
    - maximum volume = 16 TB
- Can we attach one volume with multiple ec2 instance (C.Q) = No
- Volume Size can be increase on FLY (i.e., while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

11TH SESSION AWS - EFS, DATA SERVICES

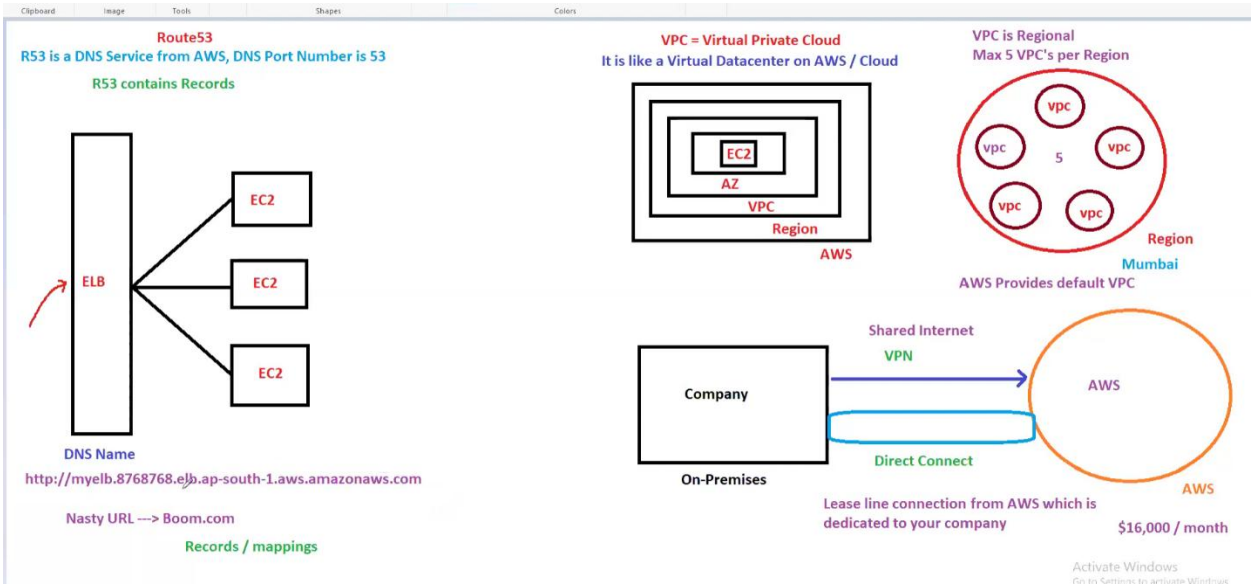


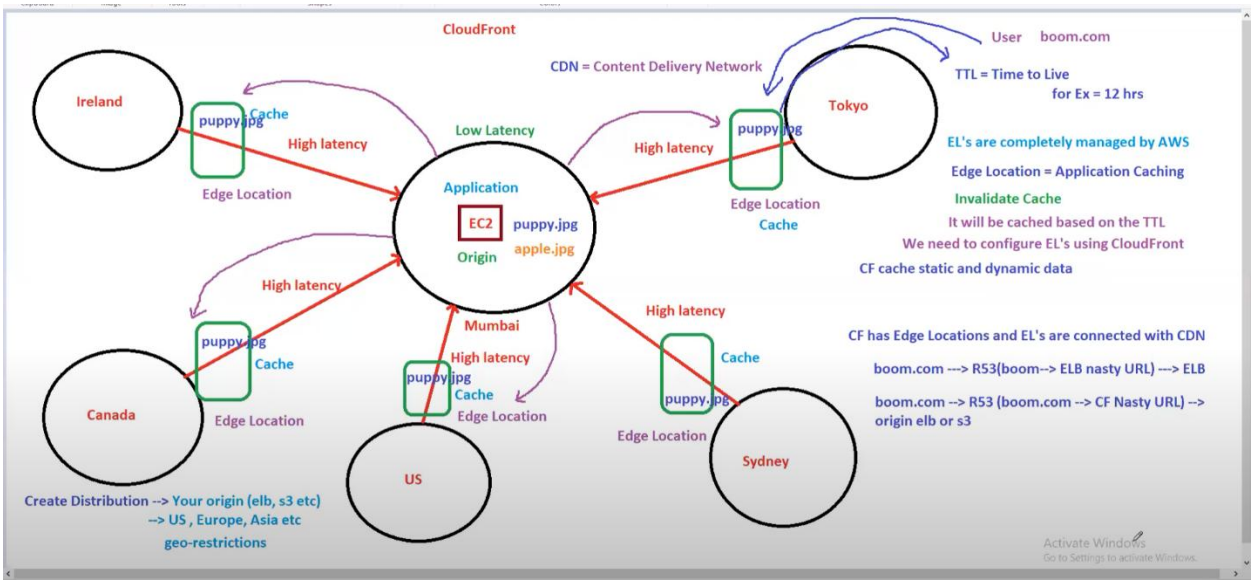




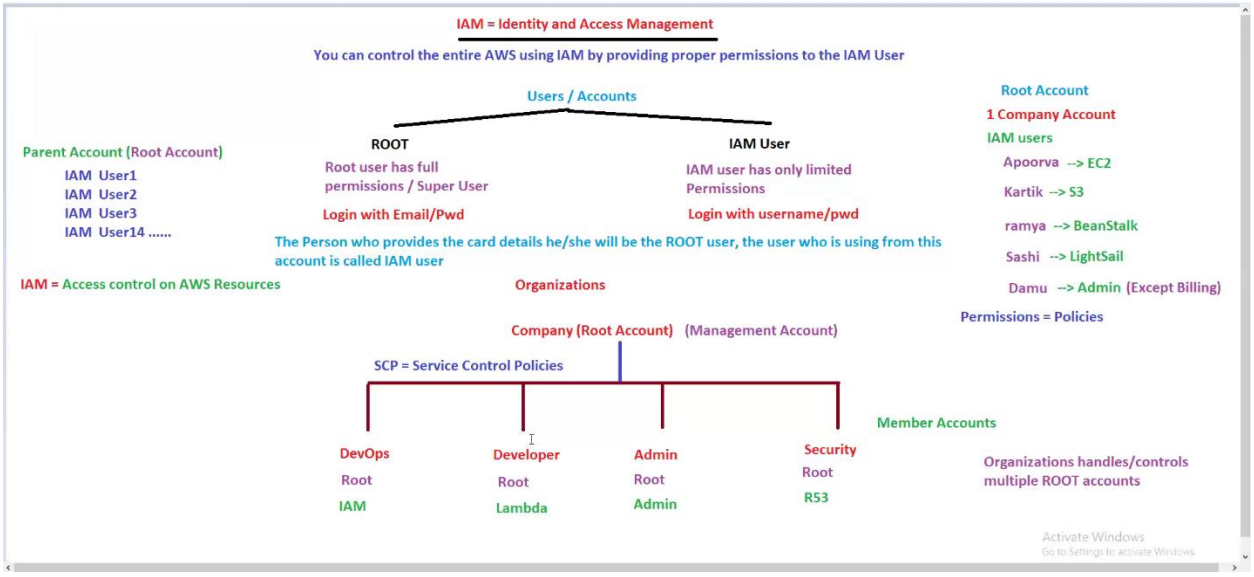
- NFS (Network File System) = EFS (Elastic File System in aws), and EFS is only for Linux System
- EFS is for Linux system and Fsx is for window system (C.Q)
- EFS can be mounted on multiple ec2 instance across different availability zone (C.Q)
- Which is the service in aws worked as hybrid storage = 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

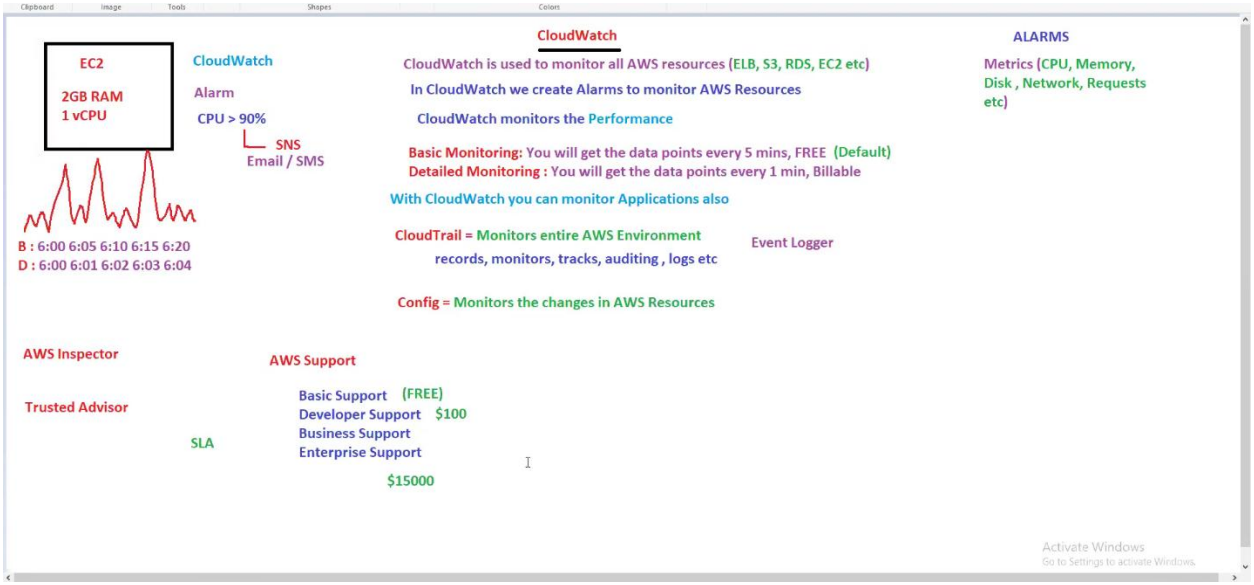
12 SESSION AWS - VPC, ROUTE53, CLOUD FRONT





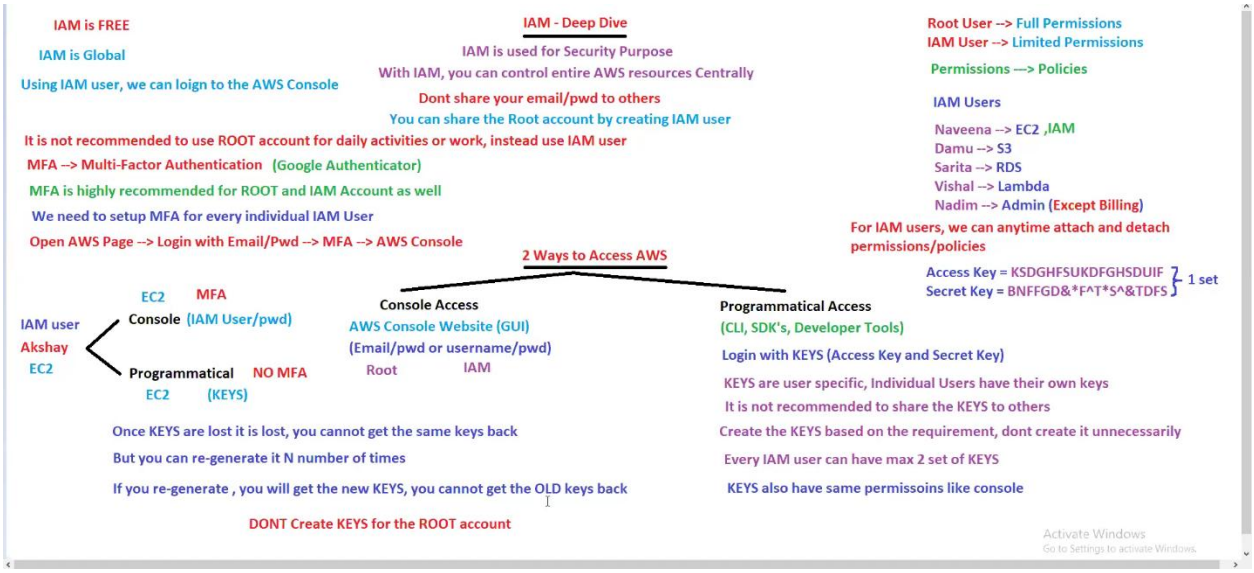
13TH SESSION AWS - IAM, CLOUD WATCH, CLOUD TRAIL





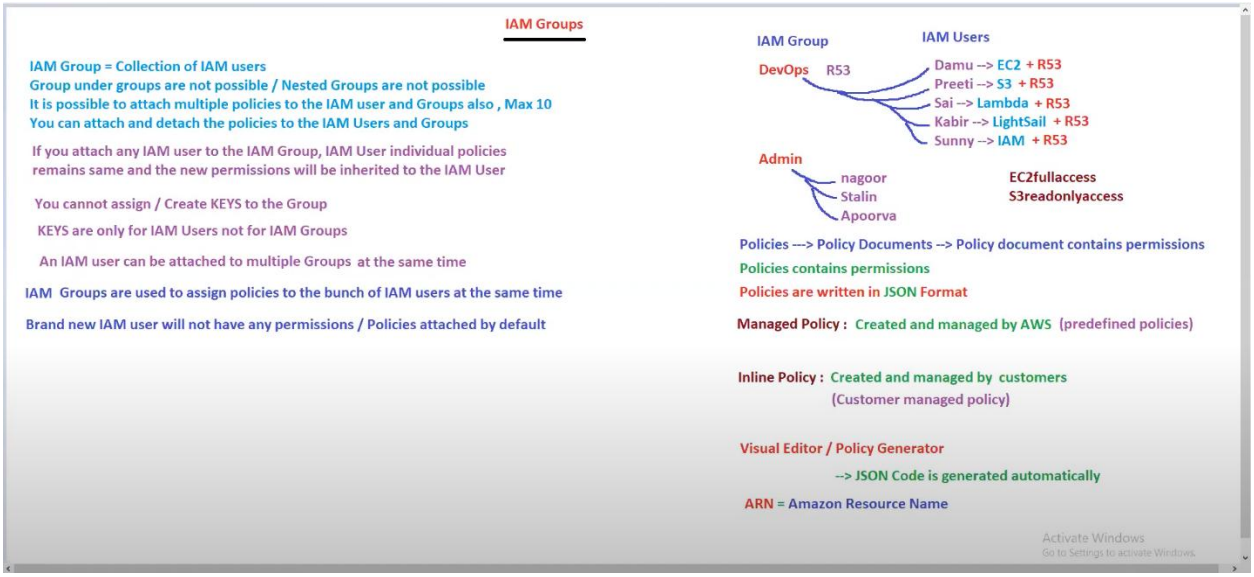
14TH SESSION AWS - REVISION TILL NOW & INTERVIEW QUESTIONS

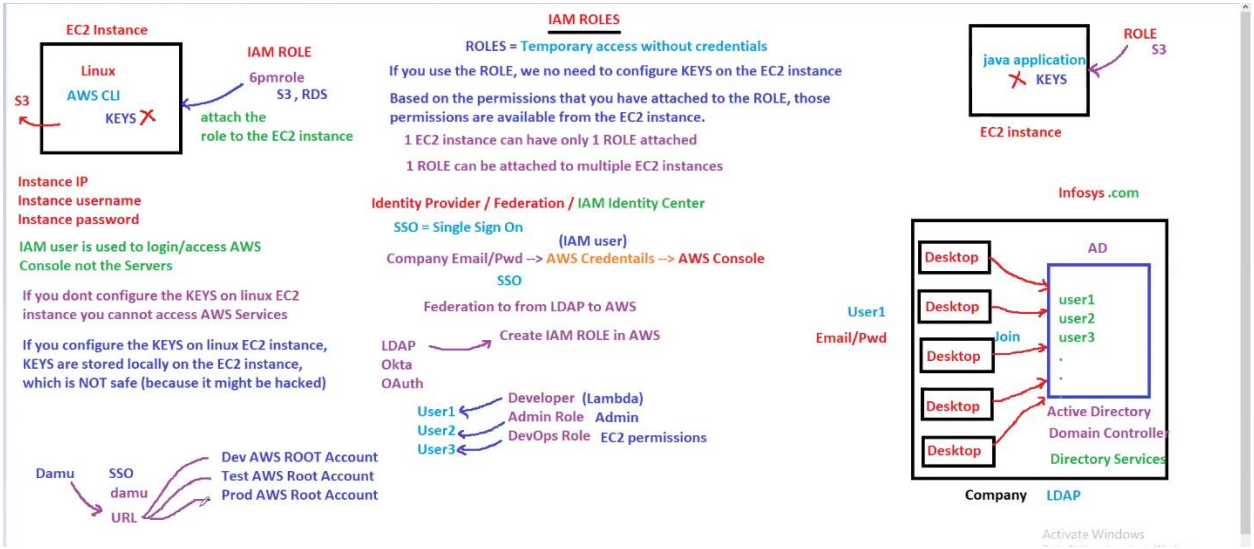
15TH SESSION AWS - IAM SERVICE



- 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)

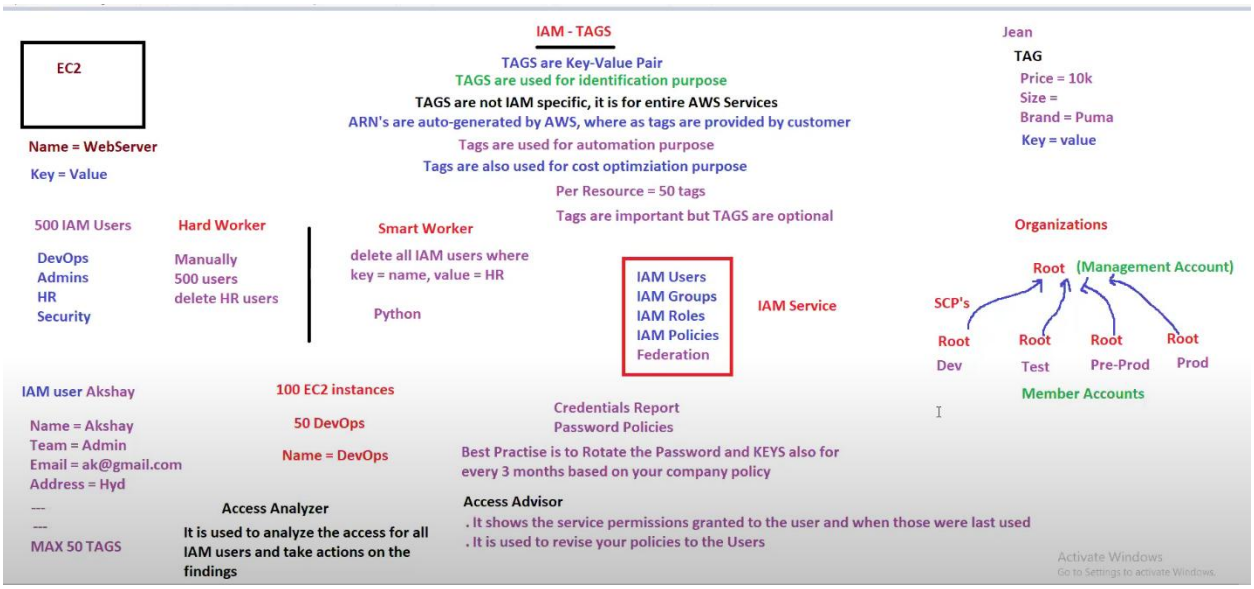
16TH SESSION AWS - IAM GROUPS IAM ROLES

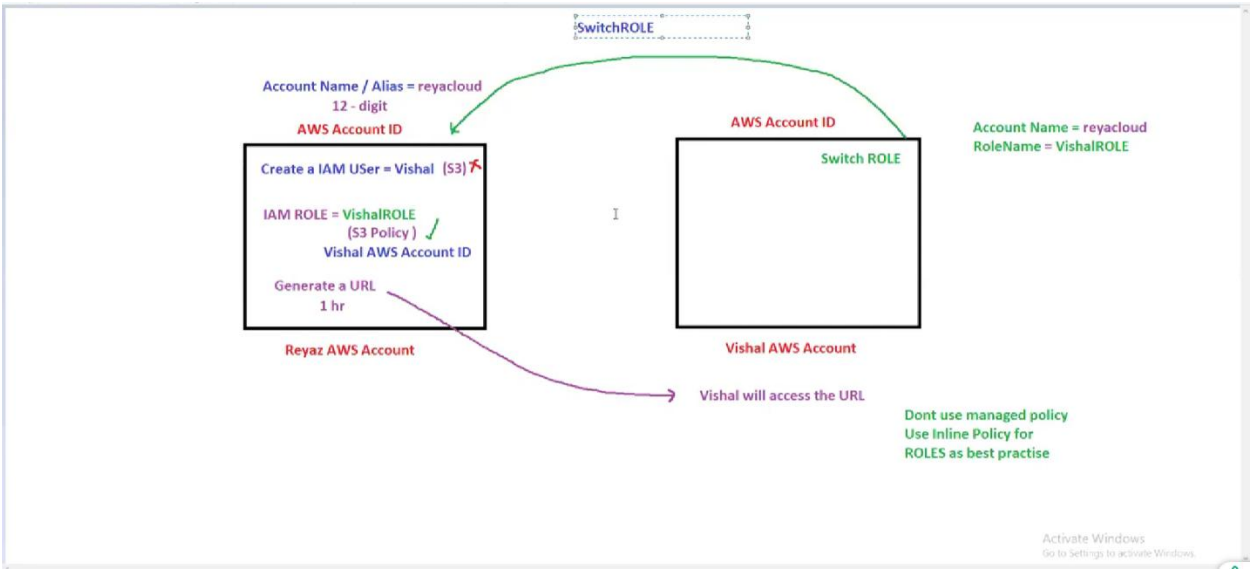




- we can attach policies to the group (C.Q)
- Policies are written in JSON Format (C.Q)
- ARN = Amazon Resource Name (not number) (C.Q).
- One Ec2 instance can have one role only, and one role have maximum 10 policies.
- one role can be attached to multiple ec2 instance.
- Identity Provider / Identity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

17TH SESSION.IAM TAG INSPECTOR TRUSTED ADVISOR





- 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

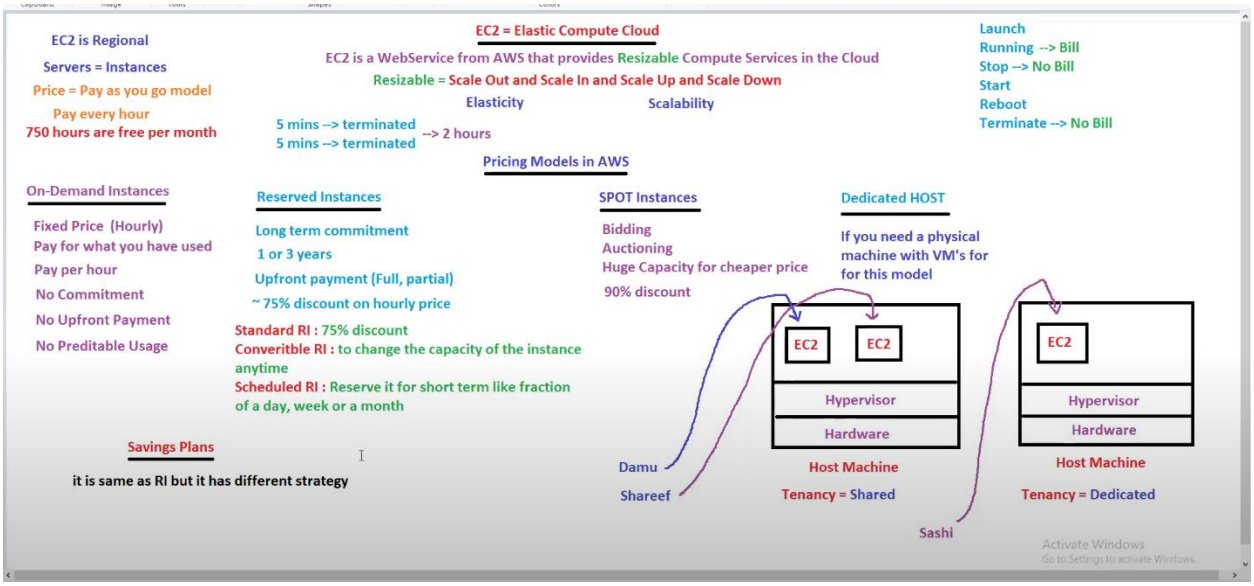
This user should able to only create users,list users,Get users, create group, list group
17. Create IAM Users(test3)
    --> Test3 custom policy(the one which you just created)

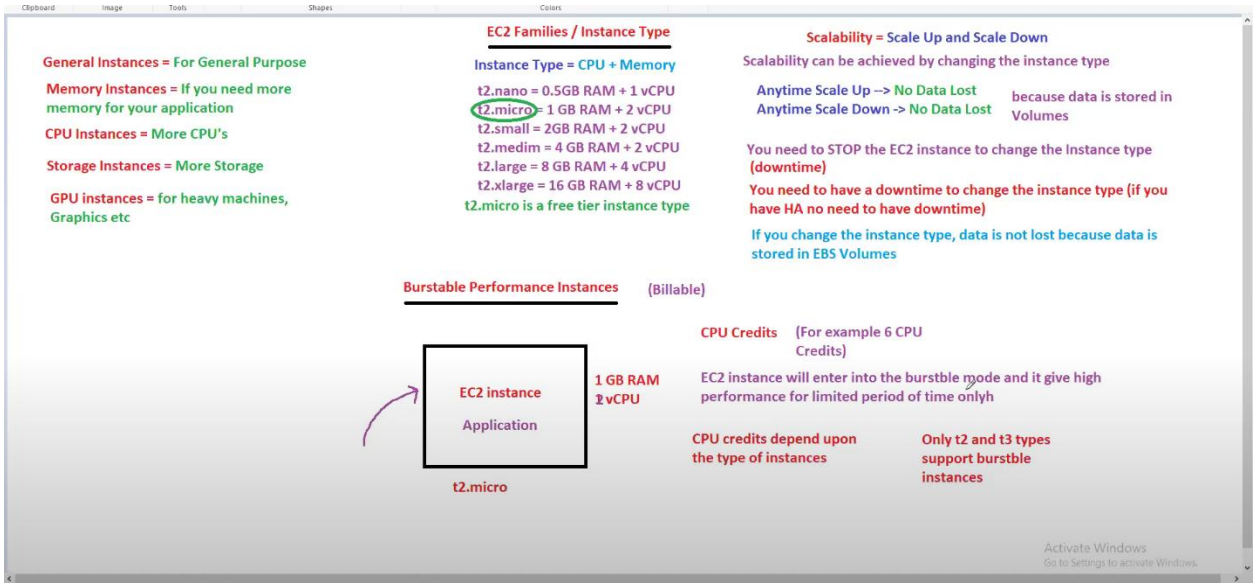
Logout and login with test3 and verify permissions what test3 can do or cannot do

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

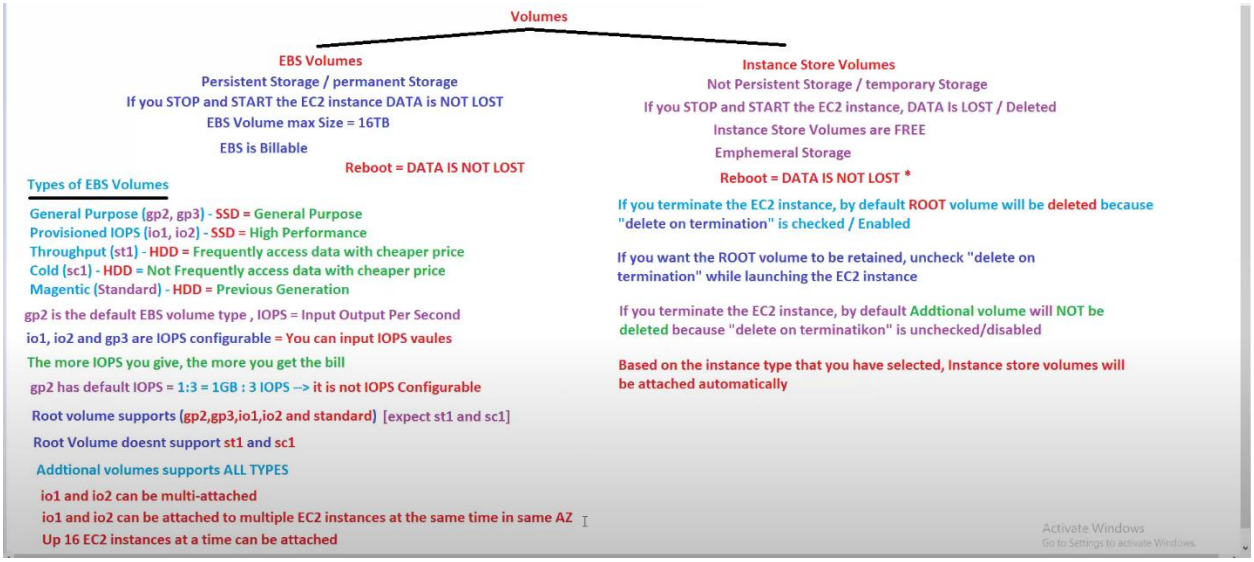
Optional: Federation: Create a free tier account in OKta and setup to AWS /
or AWS Identity Center

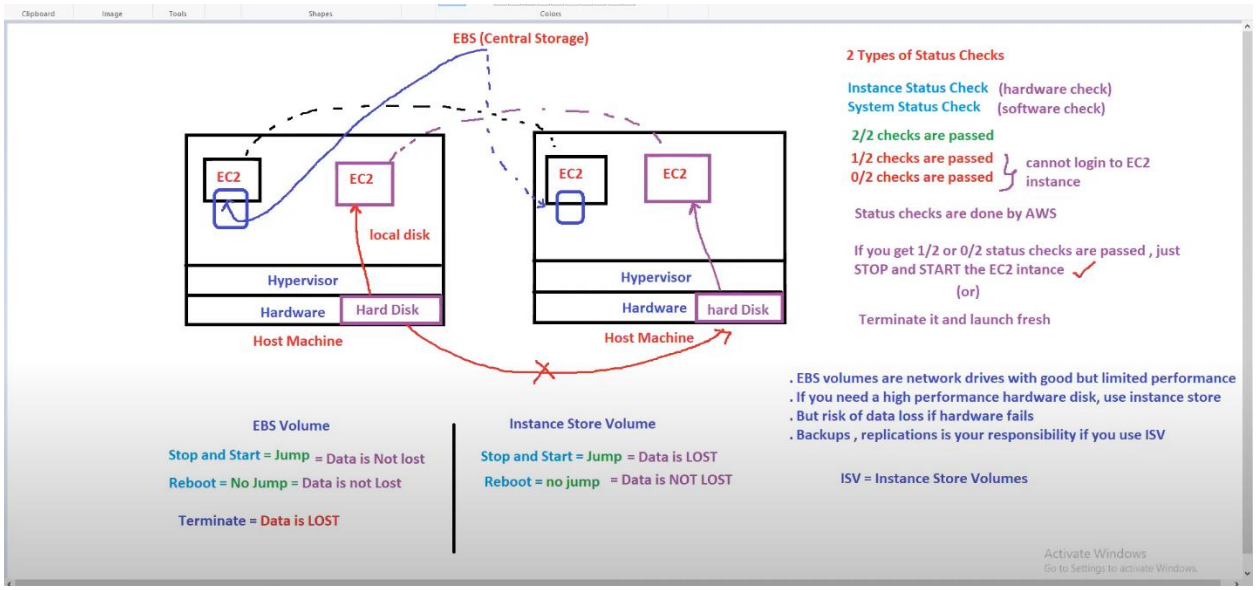
20TH SESSION AWS - EC2 SERVICE, EC2 FAMILIES INSTANCE TYPE



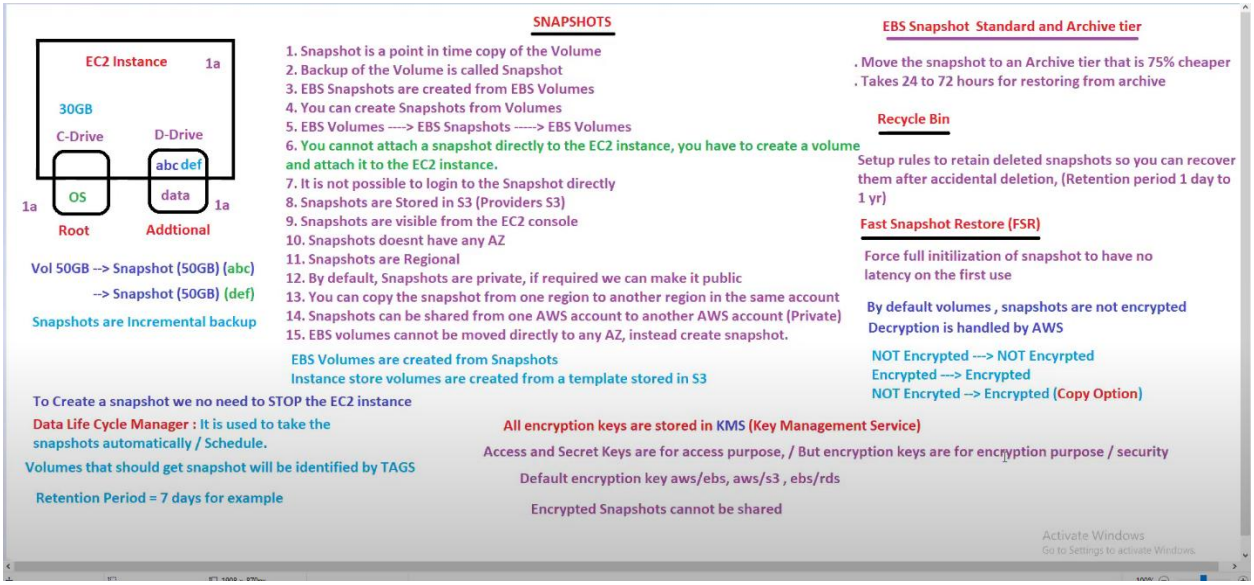


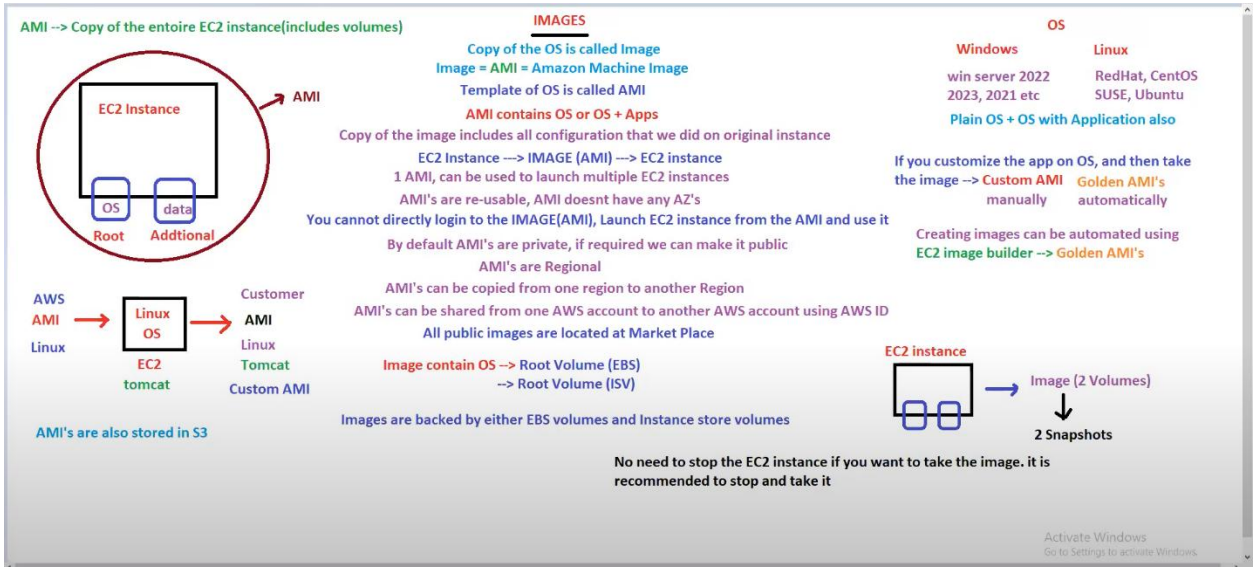
21ST SESSION AWS - EC2 VOLUMES, EBS VOLUMES, INSTANCE STORE VOLUME, EBS CENTRAL STORAGE

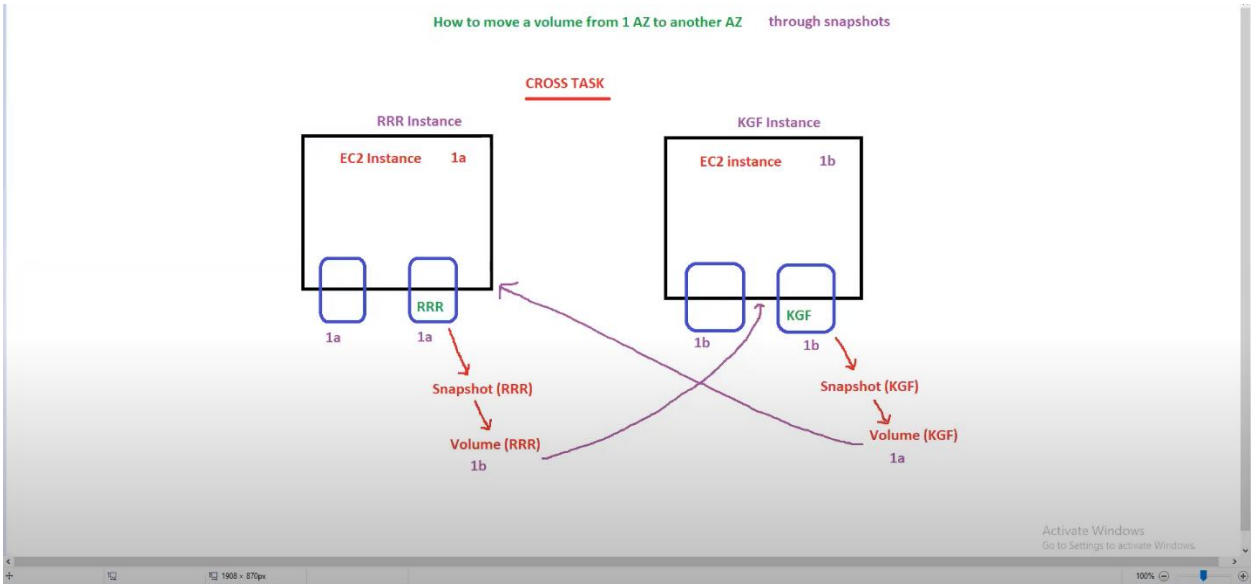




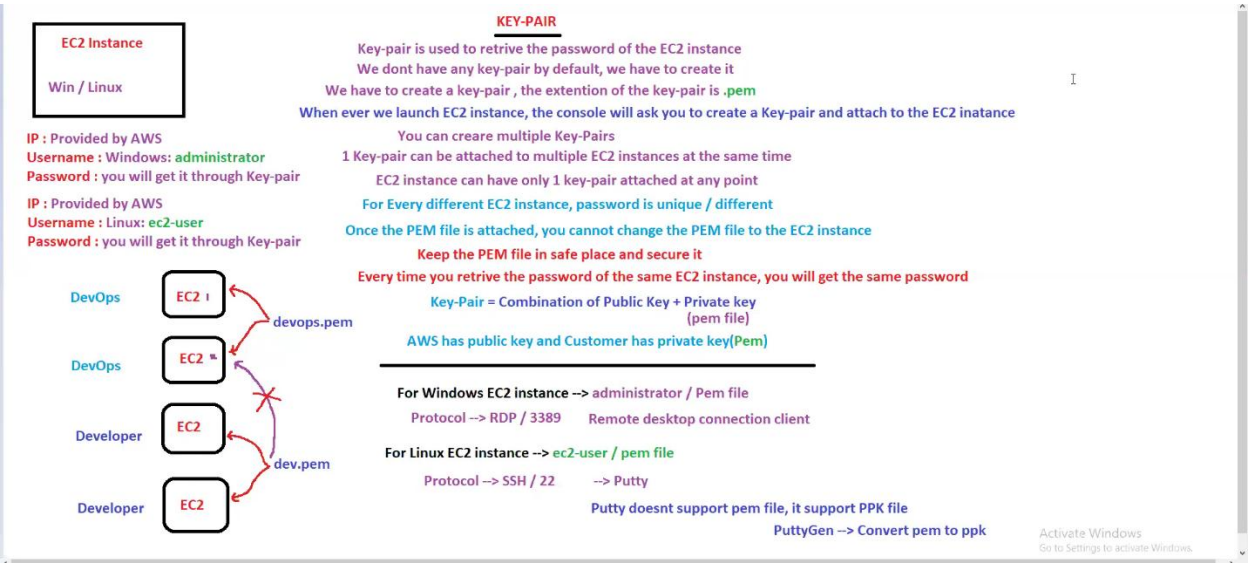
22ND SESSION AWS - EC2 INSTANCE, EBS SNAPSHOT STANDARD & ARCHIVE TIER, FSR (FAST SNAPSHOT RESTORE)

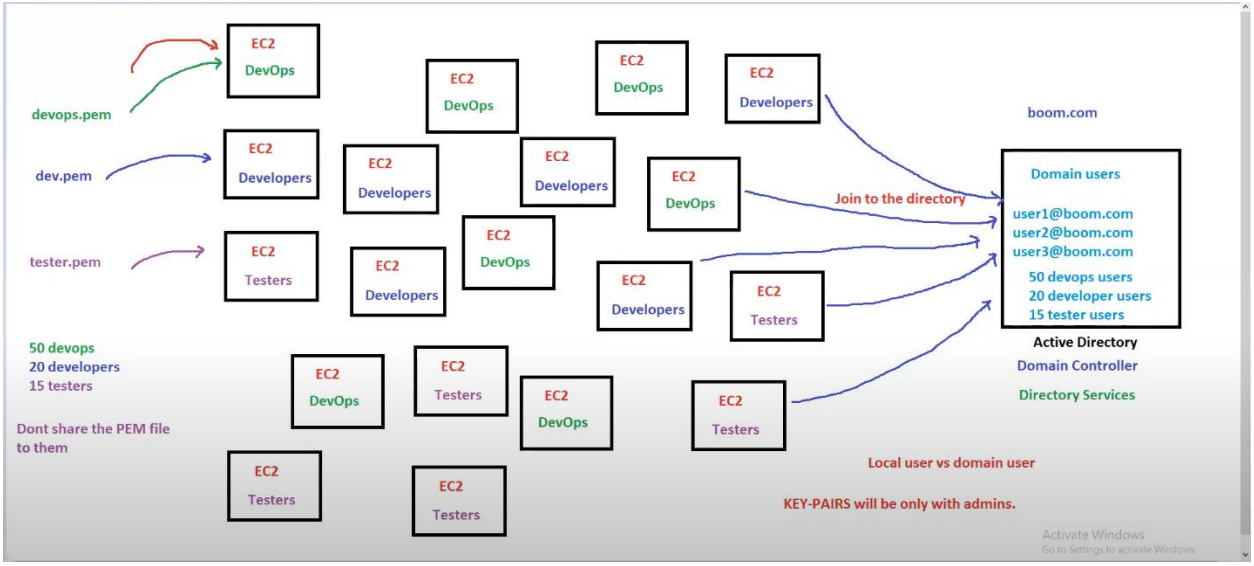





How to move a volume from 1 AZ to another AZ through snapshots
CROSS TASK
RRR Instance
EC2 Instance 1a
RRR
1a
1a
Snapshot (RRR)
Volume (RRR)
1b
KGF Instance
EC2 instance 1b
KGF
1b
1b
Snapshot (KGF)
Volume (KGF)
1a
Activate Windows
Go to Settings to activate Windows.

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

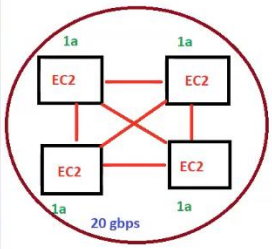




Cluster Networking Instances

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 hardwares



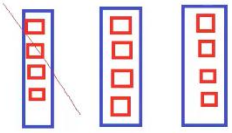
Cluster Placement Group : Grouping the instances in same rack same AZ , high performance, Low HA

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

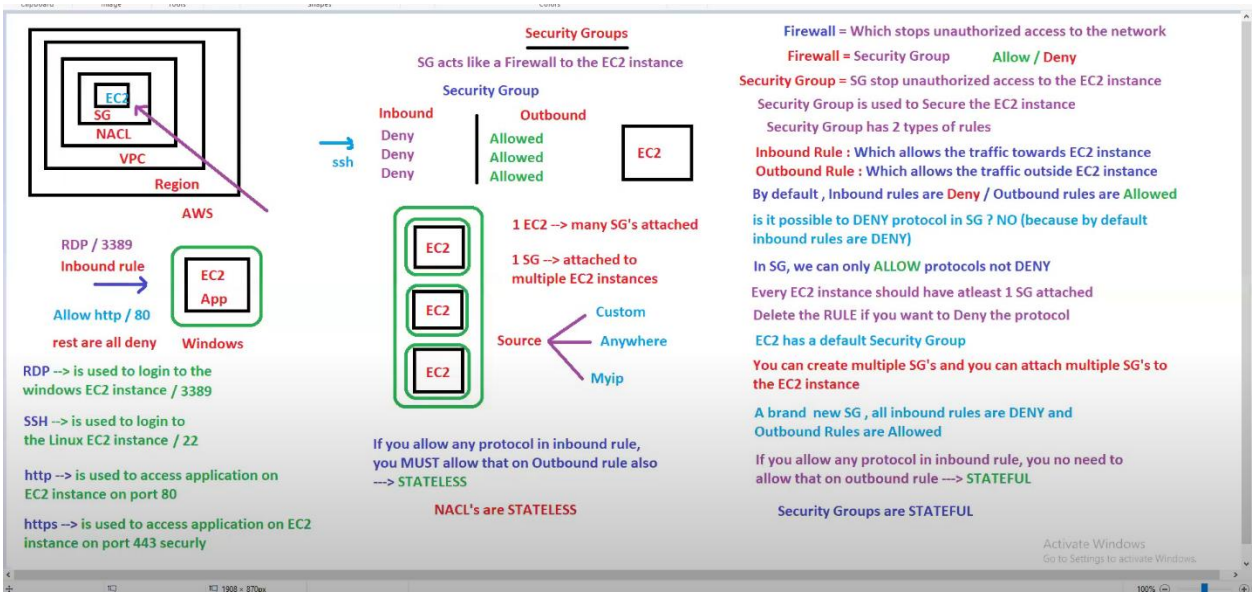
Each partition has 100's of EC2 instance.

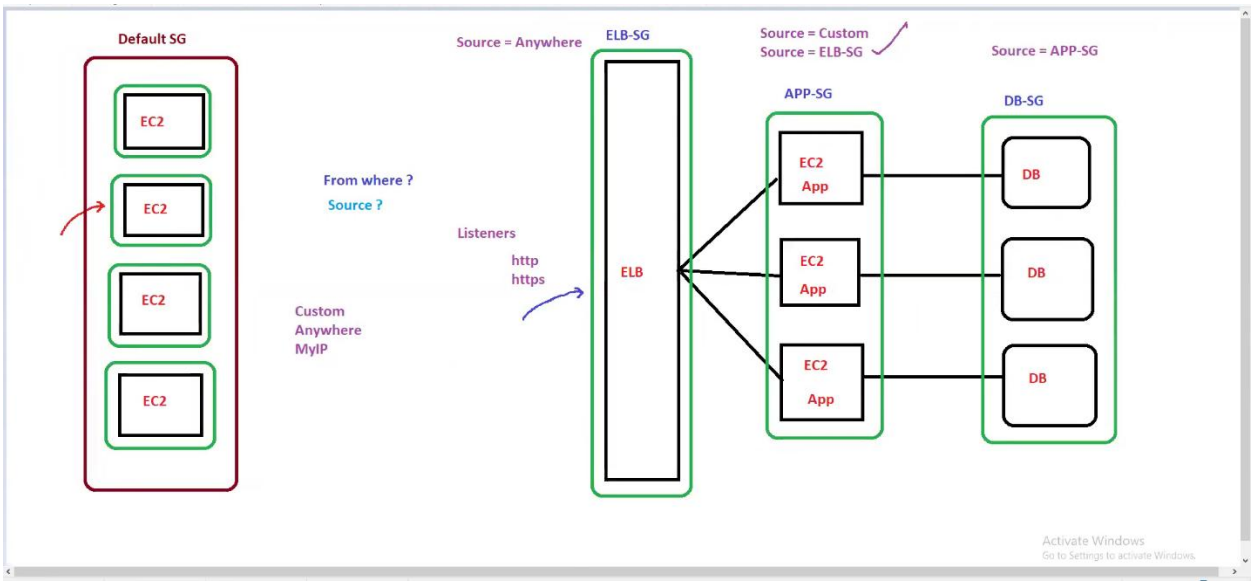


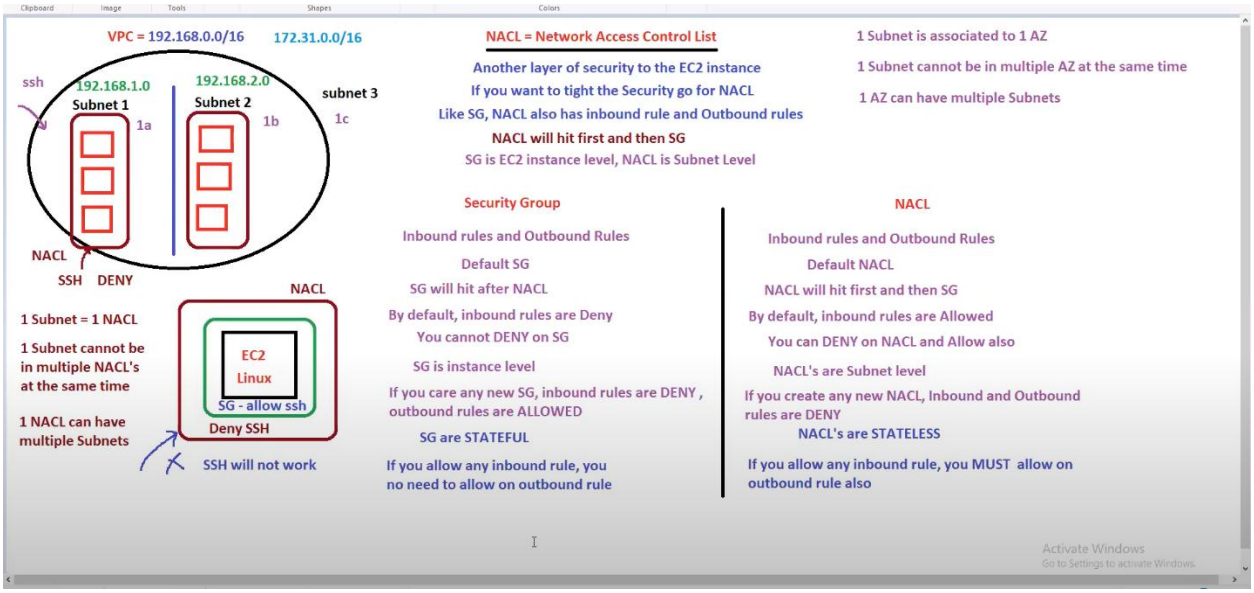
Placement Group recommended to have same homegenous instance type

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

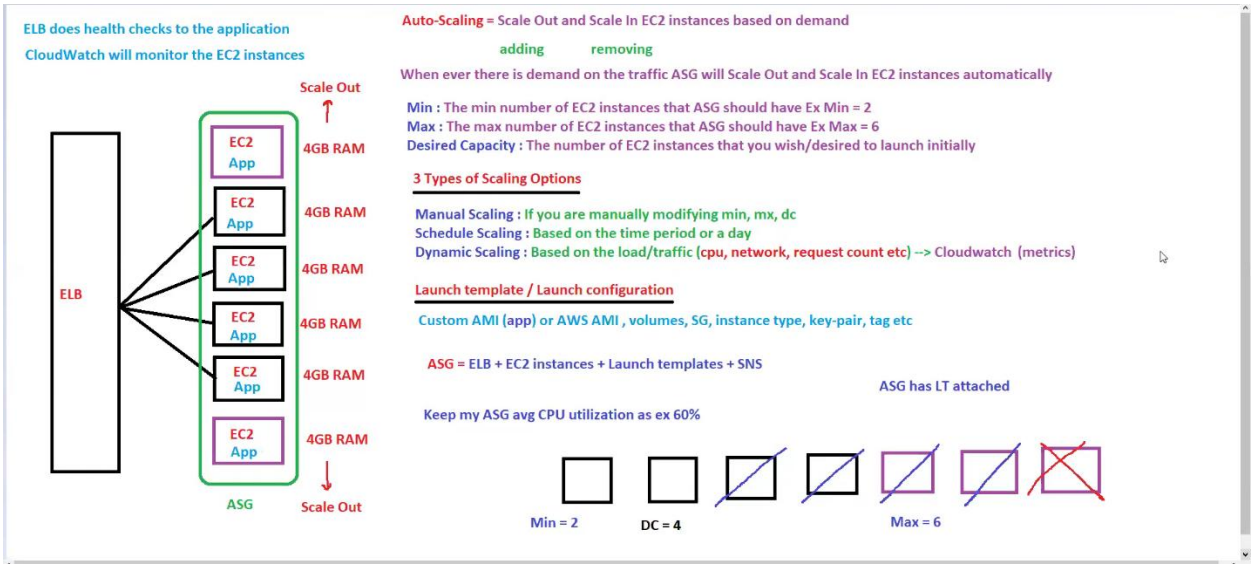
24TH SESSION AWS - EC2 SECURITY GROUPS, NACL

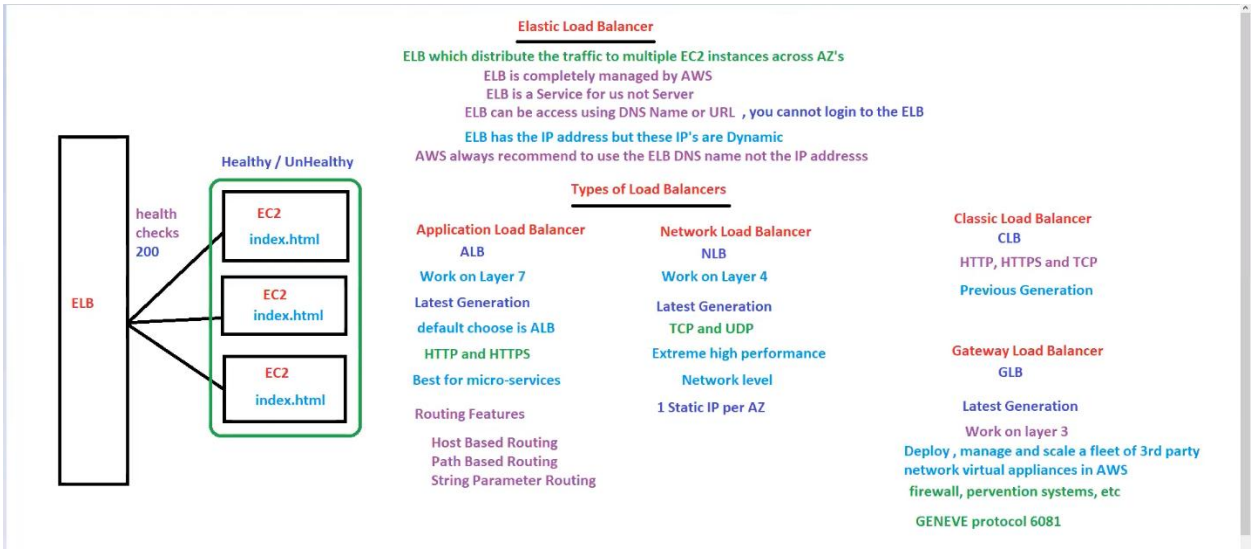


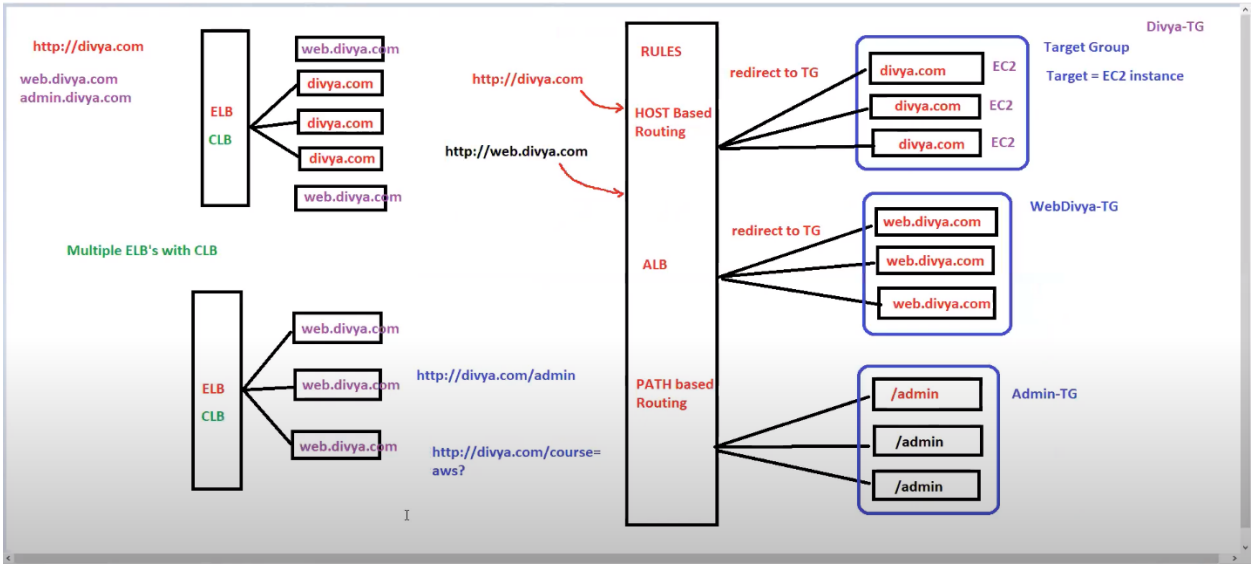


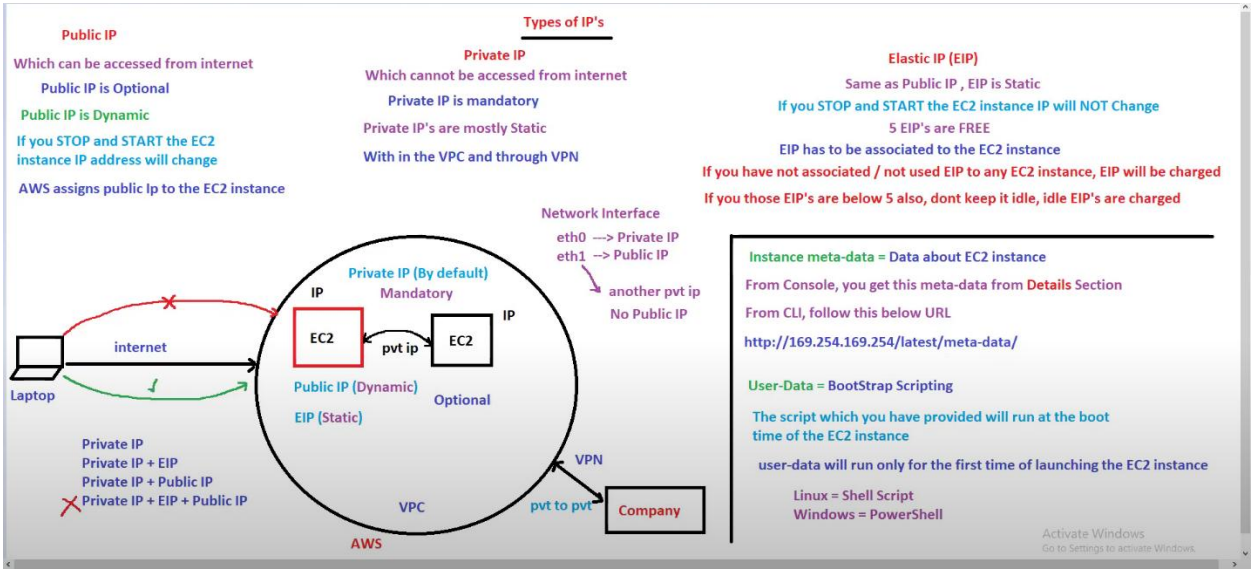

VPC = 192.168.0.0/16
172.31.0.0/16
ssh
192.168.1.0
Subnet 1
1a
192.168.2.0
Subnet 2
1b
subnet 3
1c
NACL
SSH DENY
1 Subnet = 1 NACL
1 Subnet cannot be in multiple NACL's at the same time
1 NACL can have multiple Subnets
NACL
EC2
Linux
SG - allow ssh
Deny SSH
SSH will not work
NACL = Network Access Control List
Another layer of security to the EC2 instance
If you want to tight the Security go for NACL
Like SG, NACL also has inbound rule and Outbound rules
NACL will hit first and then SG
SG is EC2 instance level, NACL is Subnet Level
1 Subnet is associated to 1 AZ
1 Subnet cannot be in multiple AZ at the same time
1 AZ can have multiple Subnets
Security Group
Inbound rules and Outbound Rules
Default SG
SG will hit after NACL
By default, inbound rules are Deny
You cannot DENY on SG
SG is instance level
If you care any new SG, inbound rules are DENY , outbound rules are ALLOWED
SG are STATEFUL
If you allow any inbound rule, you no need to allow on outbound rule
NACL
Inbound rules and Outbound Rules
Default NACL
NACL will hit first and then SG
By default, inbound rules are Allowed
You can DENY on NACL and Allow also
NACL's are Subnet level
If you create any new NACL, Inbound and Outbound rules are DENY
NACL's are STATELESS
If you allow any inbound rule, you MUST allow on outbound rule also
Activate Windows
Go to Settings to activate Windows.

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

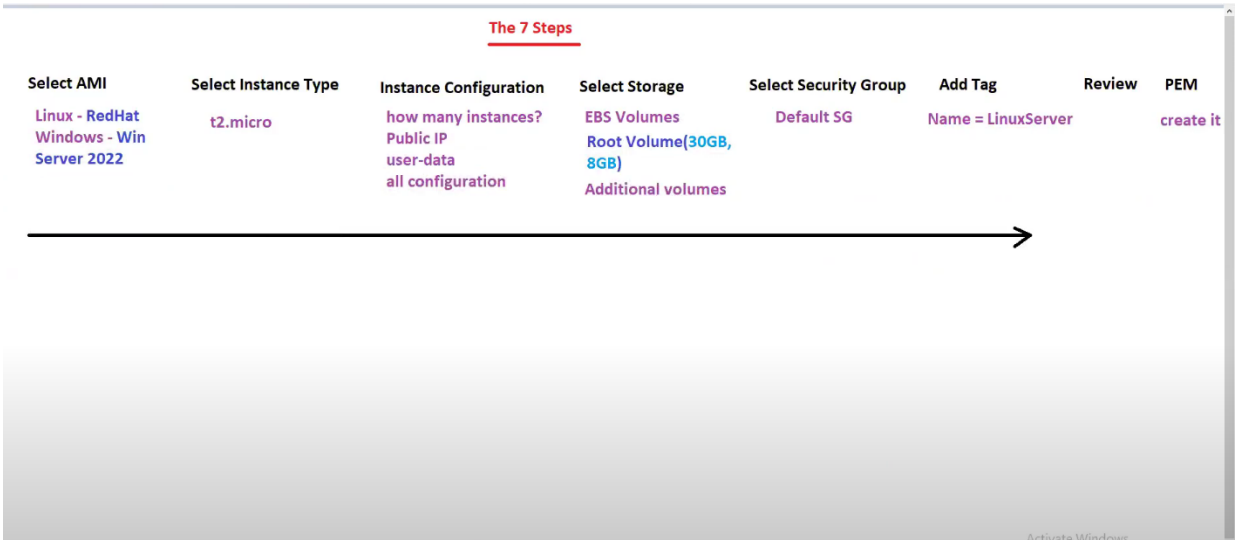


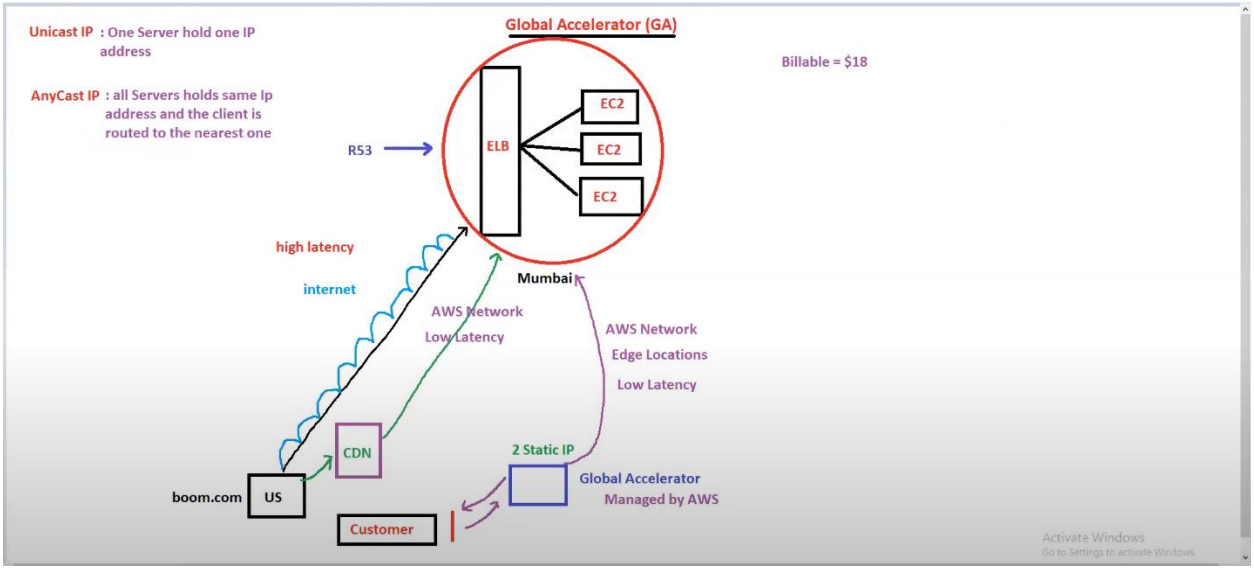



http://divya.com
web.divya.com
admin.divya.com
ELB
CLB
web.divya.com
divya.com
divya.com
divya.com
web.divya.com
Multiple ELB's with CLB
ELB
CLB
web.divya.com
web.divya.com
web.divya.com
http://divya.com
http://web.divya.com
RULES
HOST Based Routing
ALB
PATH based Routing
http://divya.com/admin
http://divya.com/course=aws?
redirect to TG
redirect to TG
divya.com
divya.com
divya.com
EC2
EC2
EC2
Divya-TG
Target Group
Target = EC2 instance
web.divya.com
web.divya.com
web.divya.com
WebDivya-TG
/admin
/admin
/admin
Admin-TG



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




Unicast IP : One Server hold one IP address
AnyCast IP : all Servers holds same Ip address and the client is routed to the nearest one
Global Accelerator (GA)
Billable = $18
R53
ELB
EC2
EC2
EC2
high latency
internet
Mumbai
AWS Network
Low Latency
AWS Network
Edge Locations
Low Latency
CDN
2 Static IP
Global Accelerator
Managed by AWS
boom.com
US
Customer
Activate Windows
Go to Settings to activate Windows.

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 protocal to the Security Group (dont do any changes to the default rule)
   use remote desktop protocal 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 protocal 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. Disssociate 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

9. Terminate EC2 instances.(if you have protection enabled --> disable that first from instance settings --> change termiantion 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 availble

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

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.

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 (addtional volumes + Root Volumes) - different AZ's
2. Increase the root volume size

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 availble

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.

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)

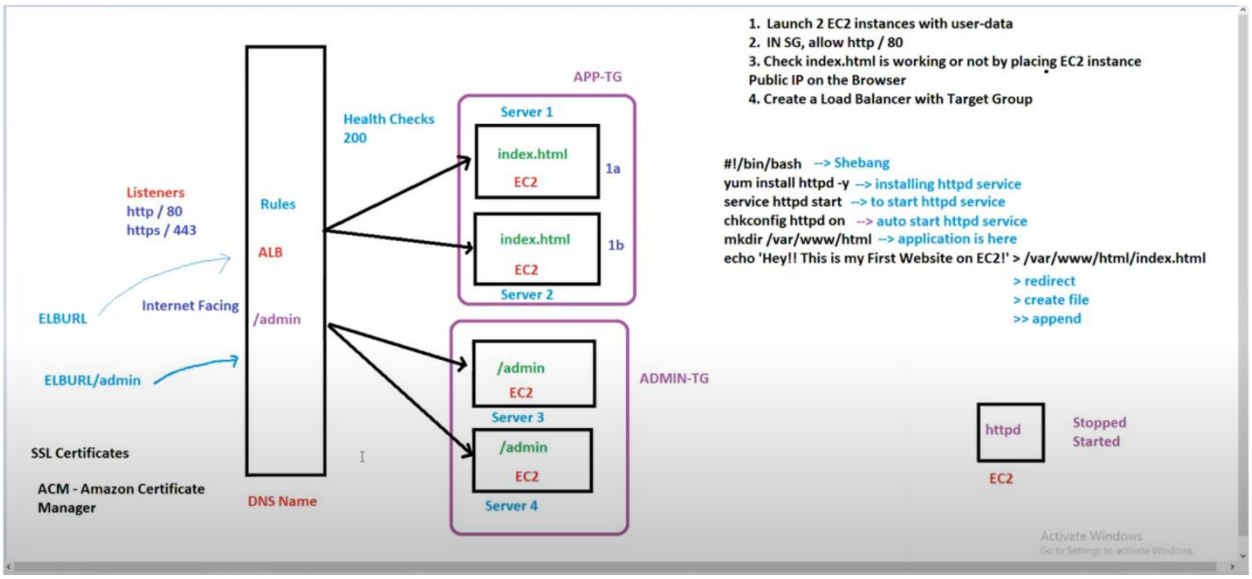
Terminate EC2 instances, Delete images, Delete snapshots

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 (addtional volumes + Root Volumes) - different AZ's
2. Increase the root volume size
3. Add addtional volume and make it available to the user.
4. Play with attach and detach volume for Root and Addtional 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 addtional 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 addtional 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

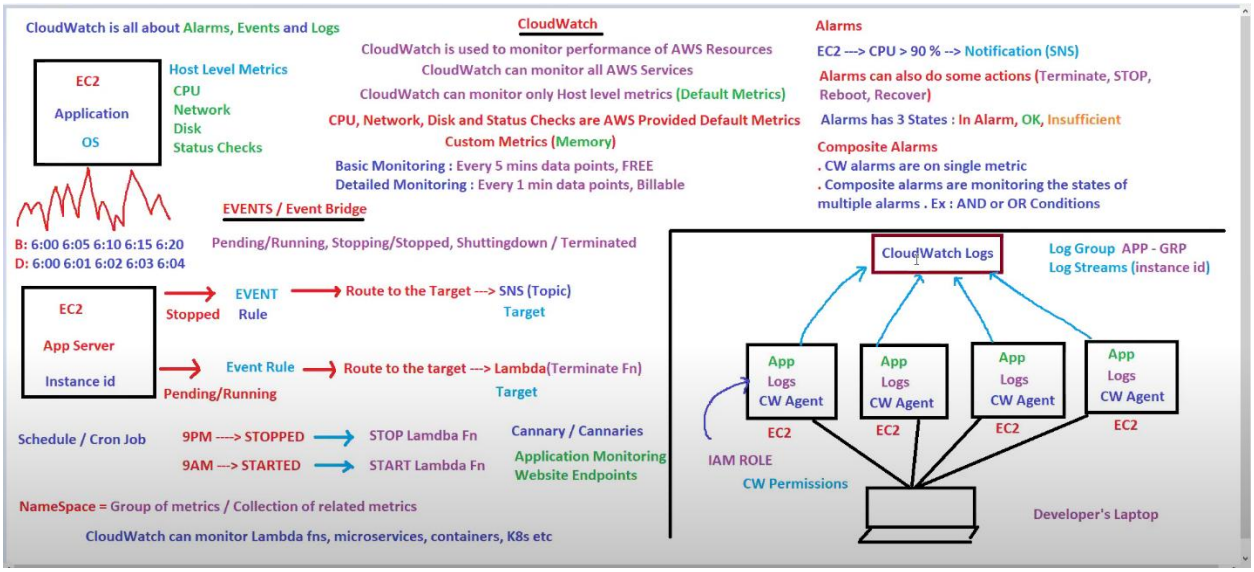
32ND SESSION AWS - EC2 INSTANCE LOAD BALANCER



33RD SESSION AWS - EC2 PRACTICAL 5 LOAD BALANCER

34TH SESSION AWS - EC2 PRACTICALS 6 = AUTO SCALING

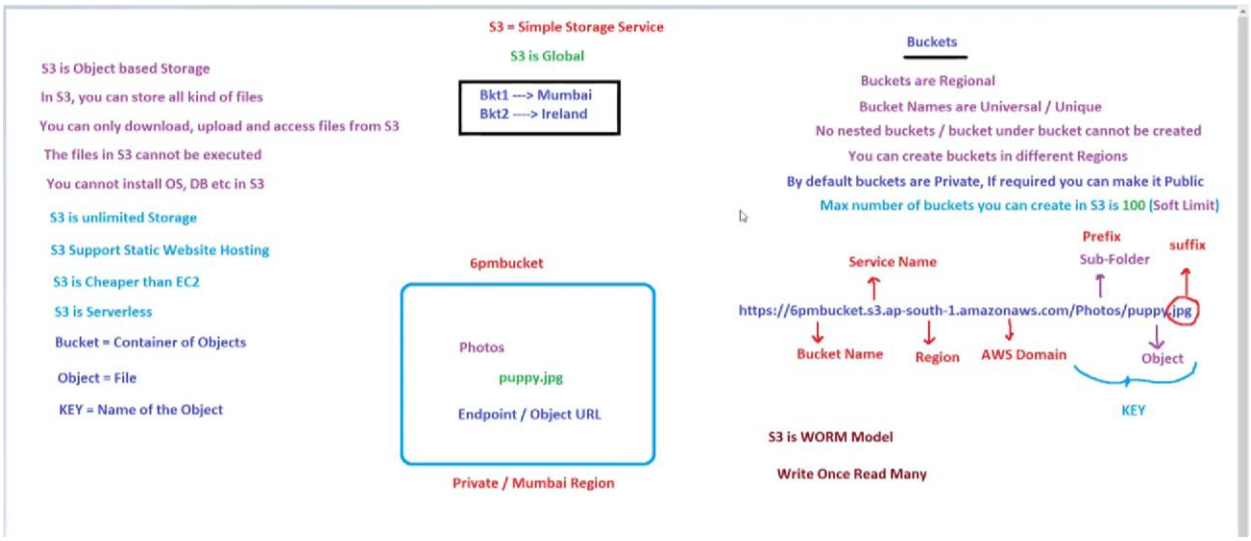
35TH SESSION AWS - CLOUDWATCH ALARMS EVENTS & LOGS

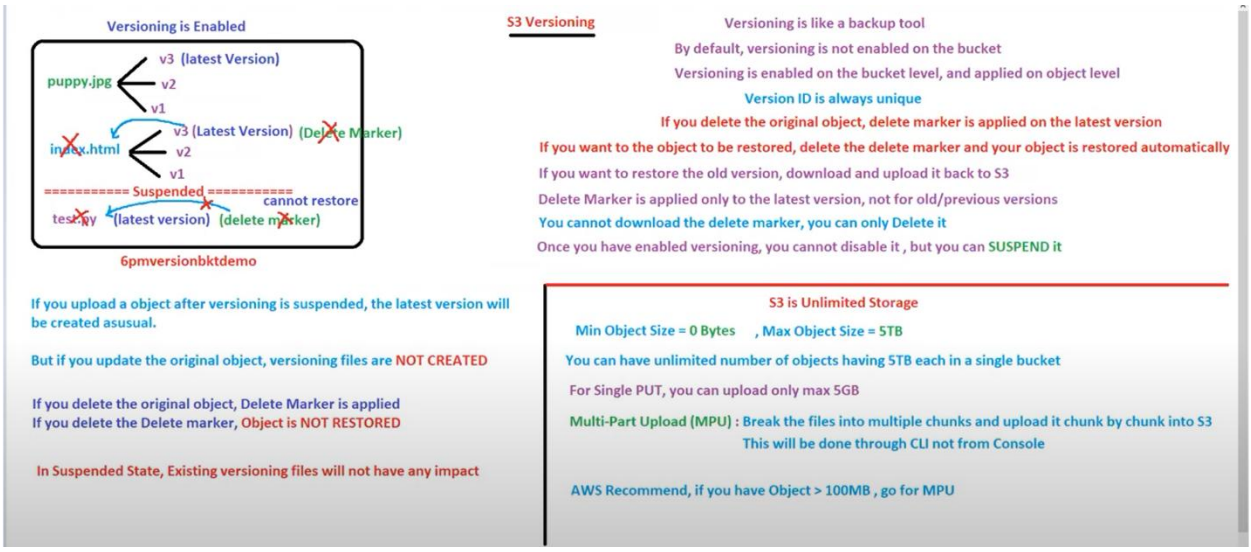


36TH SESSION AWS - CLOUDWATCH PRACTICALS ALARMS EVENTS & LAMBDA AWS CONSOLE

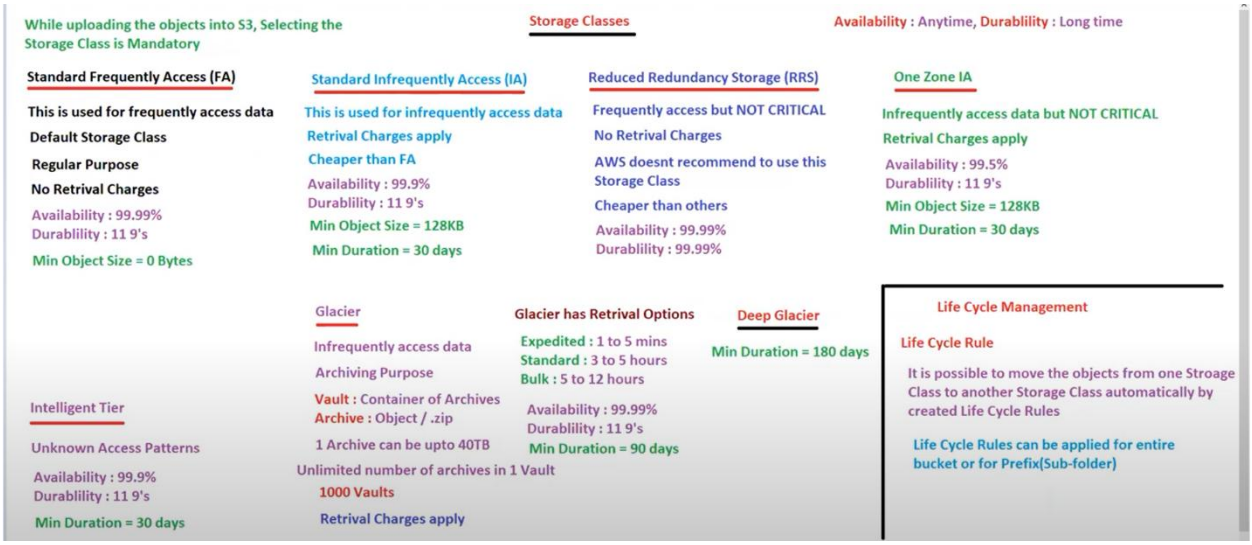
38TH SESSION AWS - ELASTIC BEANSTALK, ELASTIC BEANSTALK ARCHITECTURE, BLUE GREEN DEPLOYMENT

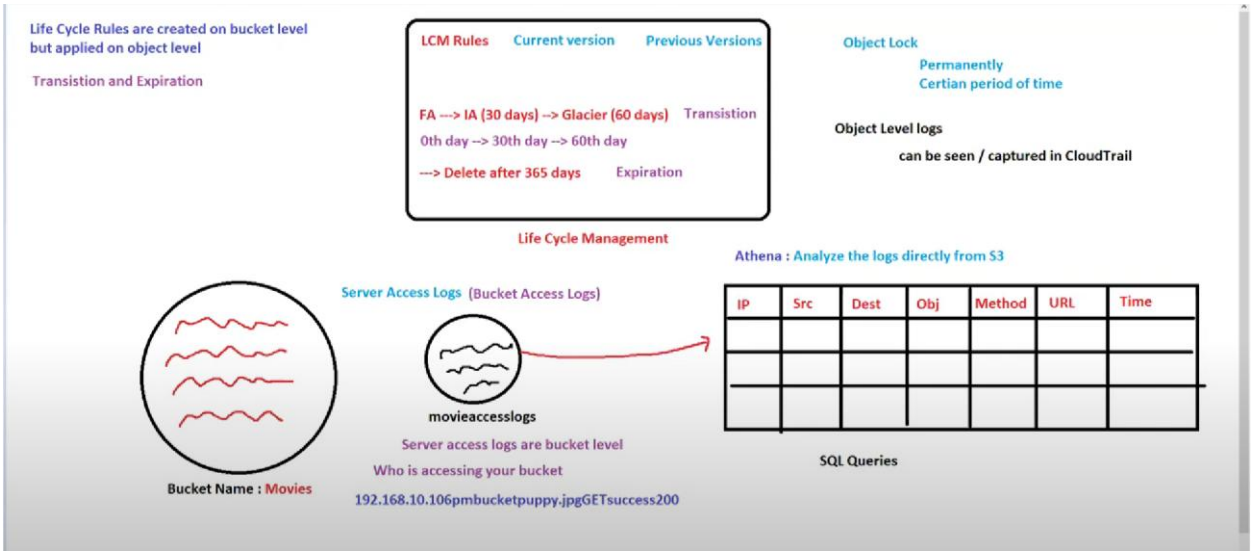
39TH SESSION AWS - S3 = SIMPLE STORAGE SERVICE, S3 VERSIONING

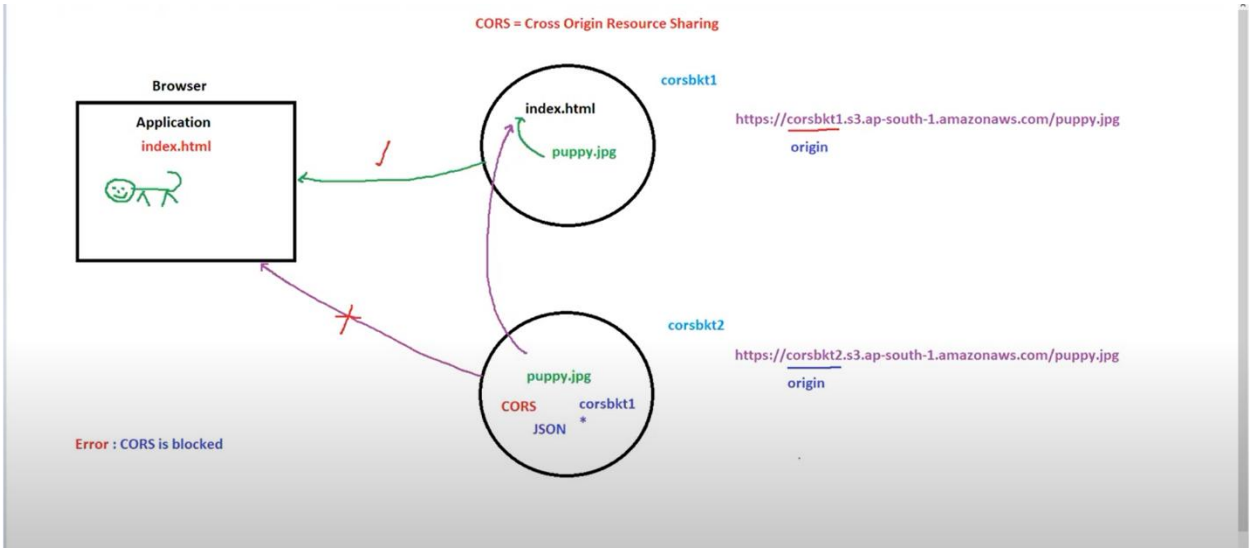


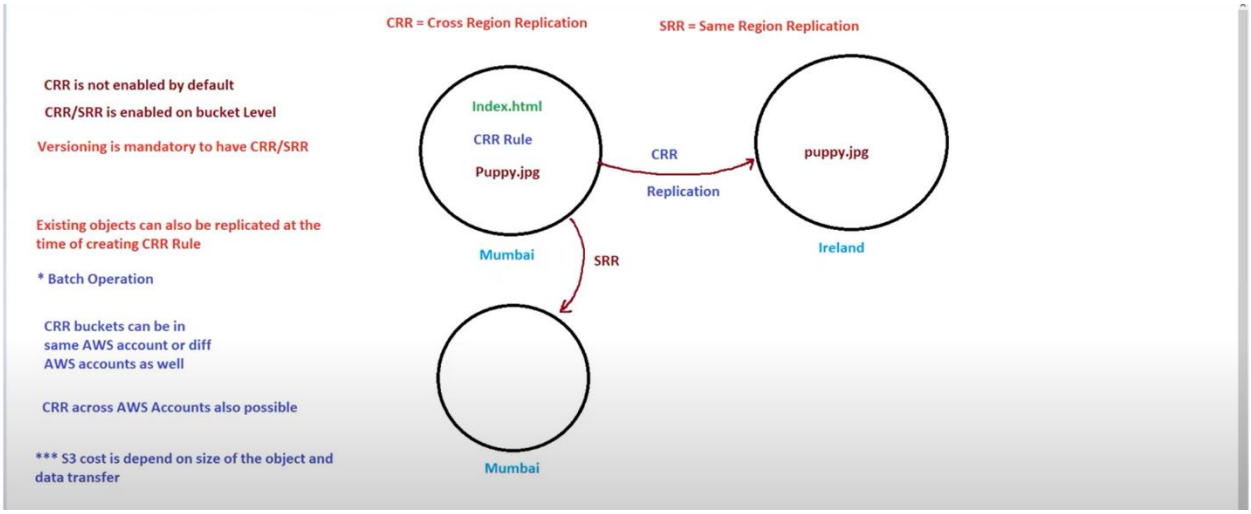


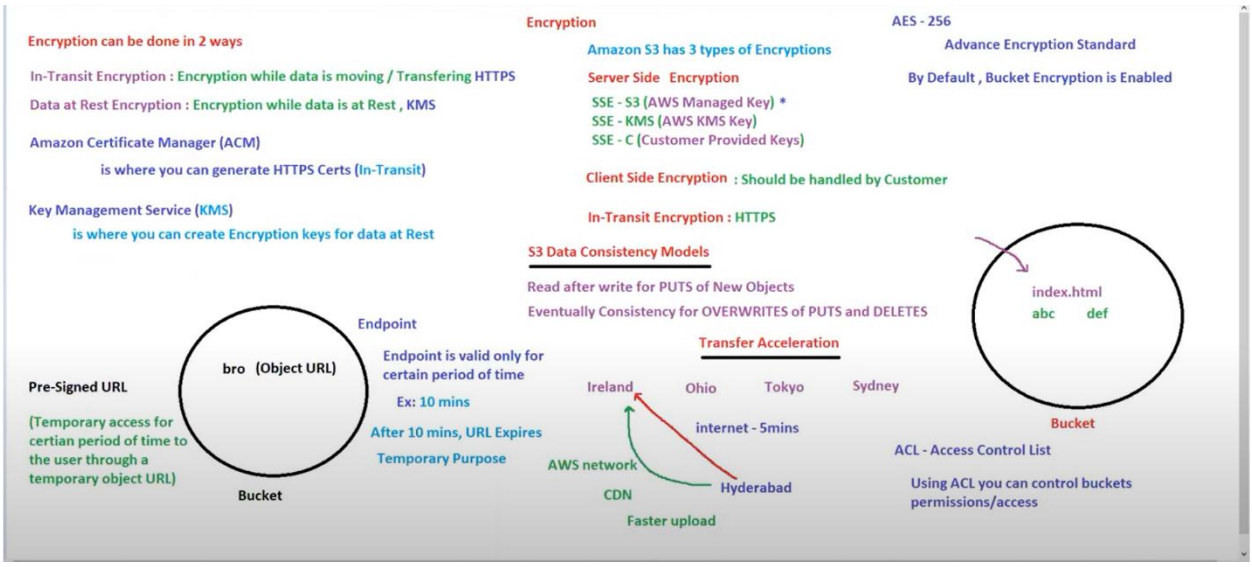
40TH SESSION AWS - S3 STORAGE CLASSES, GLACIER, LCM RULES, CORS, CRR, SRR, ENCRYPTION



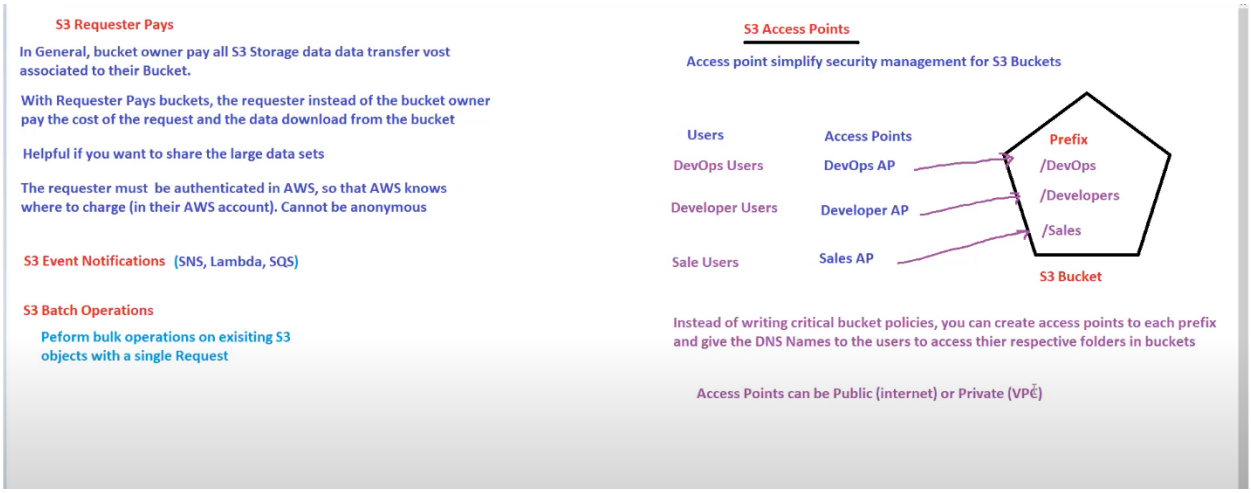



CORS = Cross Origin Resource Sharing
Browser
Application
index.html
corsbkt1
index.html
puppy.jpg
https://corsbkt1.s3.ap-south-1.amazonaws.com/puppy.jpg
origin
corsbkt2
puppy.jpg
CORS
corsbkt1
*
JSON
https://corsbkt2.s3.ap-south-1.amazonaws.com/puppy.jpg
origin
Error : CORS is blocked


CRR = Cross Region Replication
SRR = Same Region Replication
CRR is not enabled by default
CRR/SRR is enabled on bucket Level
Versioning is mandatory to have CRR/SRR
Existing objects can also be replicated at the time of creating CRR Rule
* Batch Operation
CRR buckets can be in same AWS account or diff AWS accounts as well
CRR across AWS Accounts also possible
*** S3 cost is depend on size of the object and data transfer
Index.html
CRR Rule
Puppy.jpg
Mumbai
CRR
Replication
puppy.jpg
Ireland
SRR
Mumbai


Encryption can be done in 2 ways
In-Transit Encryption : Encryption while data is moving / Transfering HTTPS
Data at Rest Encryption : Encryption while data is at Rest , KMS
Amazon Certificate Manager (ACM)
is where you can generate HTTPS Certs (In-Transit)
Key Management Service (KMS)
is where you can create Encryption keys for data at Rest
Encryption
Amazon S3 has 3 types of Encryptions
Server Side Encryption
SSE - S3 (AWS Managed Key) *
SSE - KMS (AWS KMS Key)
SSE - C (Customer Provided Keys)
Client Side Encryption : Should be handled by Customer
In-Transit Encryption : HTTPS
AES - 256
Advance Encryption Standard
By Default , Bucket Encryption is Enabled
S3 Data Consistency Models
Read after write for PUTS of New Objects
Eventually Consistency for OVERWRITES of PUTS and DELETES
index.html
abc def
Bucket
Endpoint
Endpoint is valid only for certain period of time
Ex: 10 mins
After 10 mins, URL Expires
Temporary Purpose
Pre-Signed URL
(Temporary access for certian period of time to the user through a temporary object URL)
bro (Object URL)
Bucket
Transfer Acceleration
Ireland
Ohio
Tokyo
Sydney
internet - 5mins
AWS network
CDN
Hyderabad
Faster upload
ACL - Access Control List
Using ACL you can control buckets permissions/access

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



--> Delete the Application
Upload you 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 webite 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 acheive it
2. Try with bucket policy also

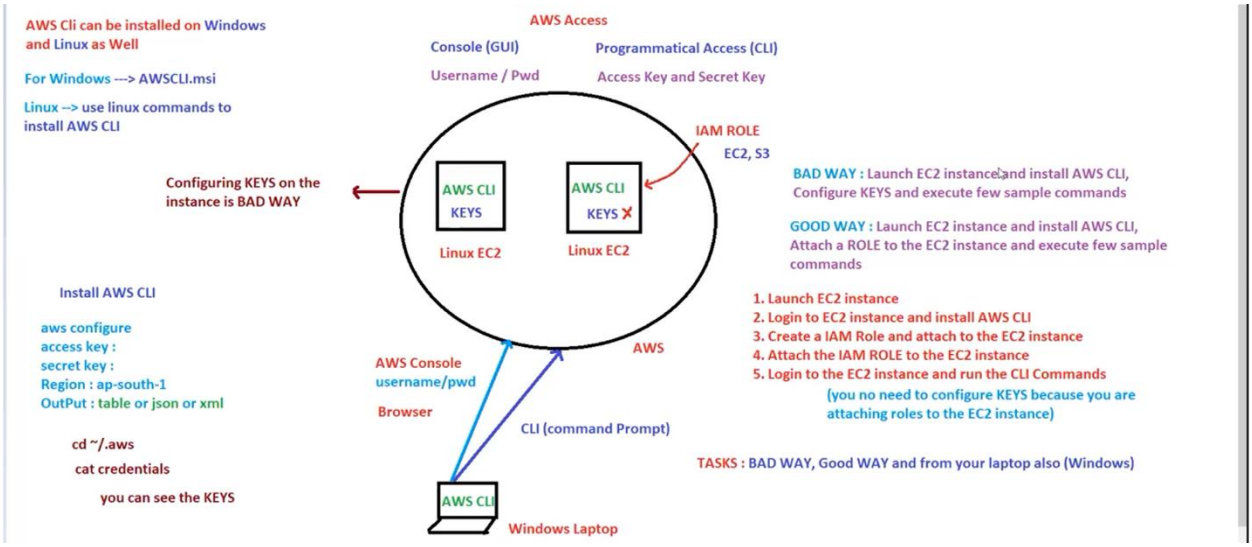
logout from your account
login as user1 and access user1bkt (should be access) , access user2bkt(should not access)
logout user1
login as user2 and access user2bkt (should be access) , access user1bkt(should not access)

S3 Acces Point setup

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

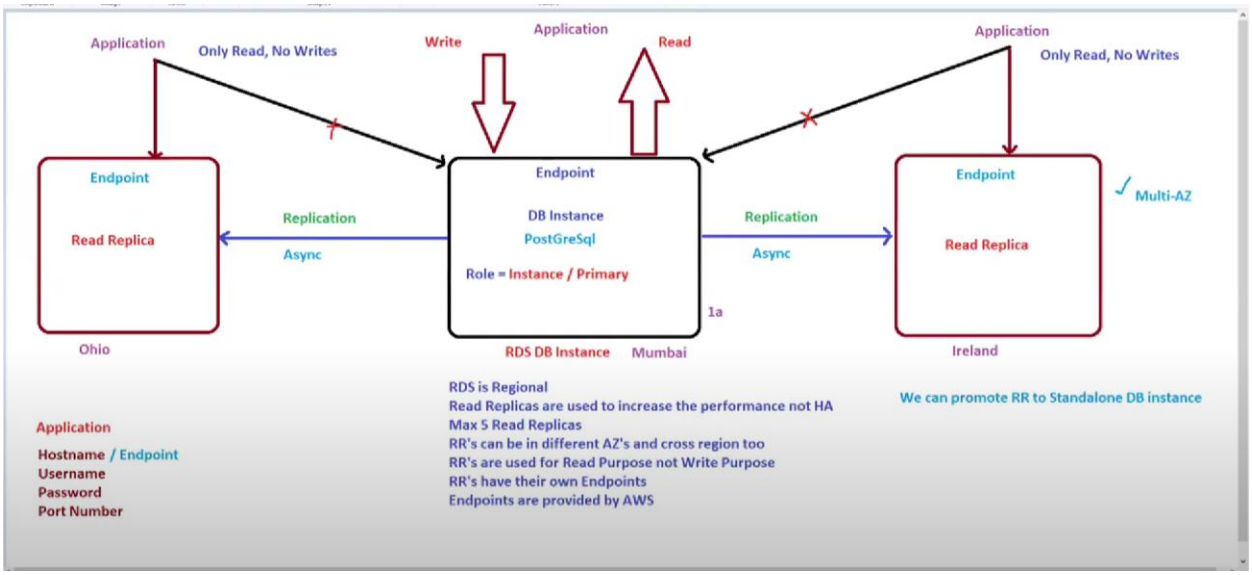
43RD SESSION AWS - EFS SERVICE DEMO & PRACTICALS AWS CONSOLE

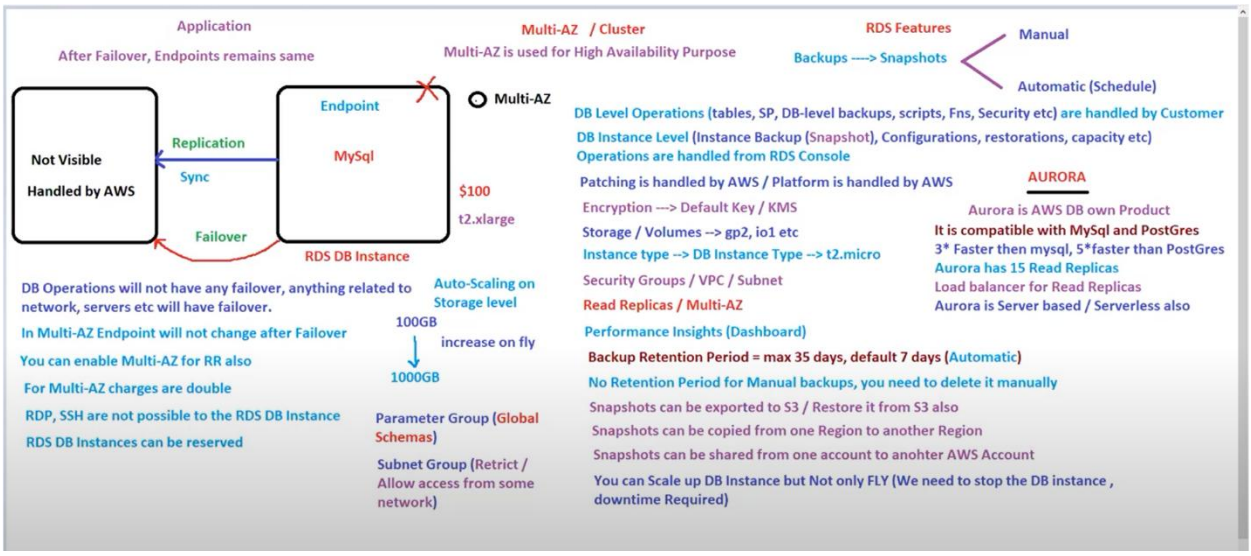
44TH SESSION AWS - CLI TUTORIAL & PRACTICAL IN AWS CONSOLE



46TH SESSION AWS - STORAGE GATEWAY SERVICE TUTORIAL & PRACTICALS

47TH SESSION AWS - RDS, RDS PROXY

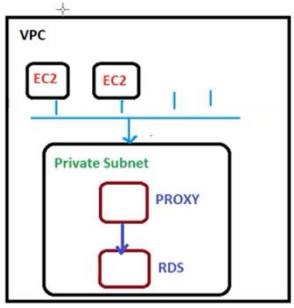




AWS RDS PROXY

. Fully managed database proxy for RDS
. Allows apps to pool and share the DB Connections establised 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 credentails
. 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

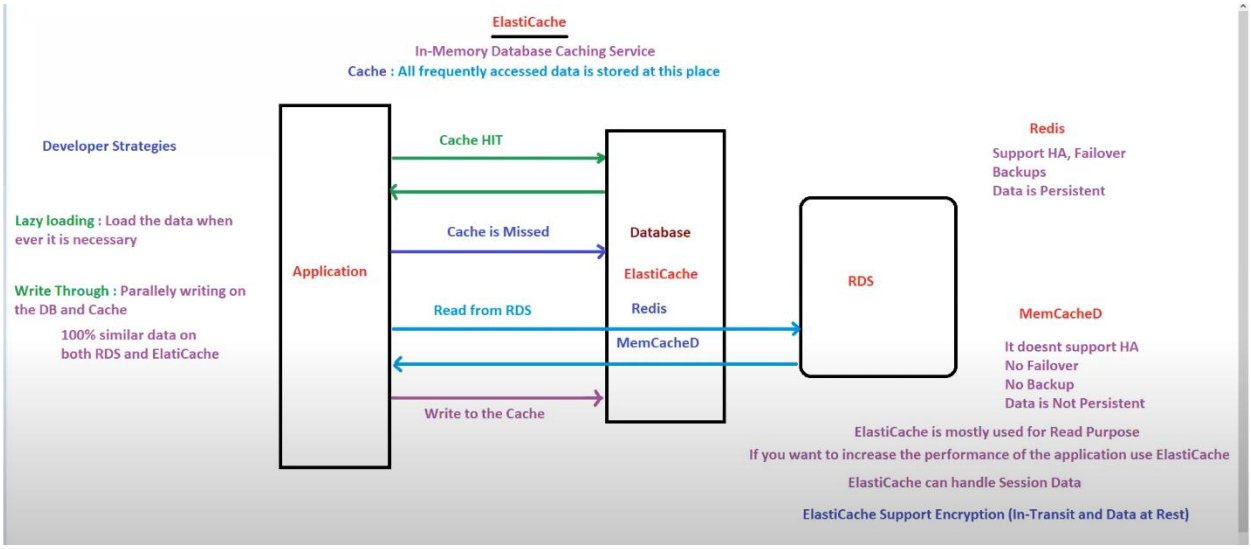


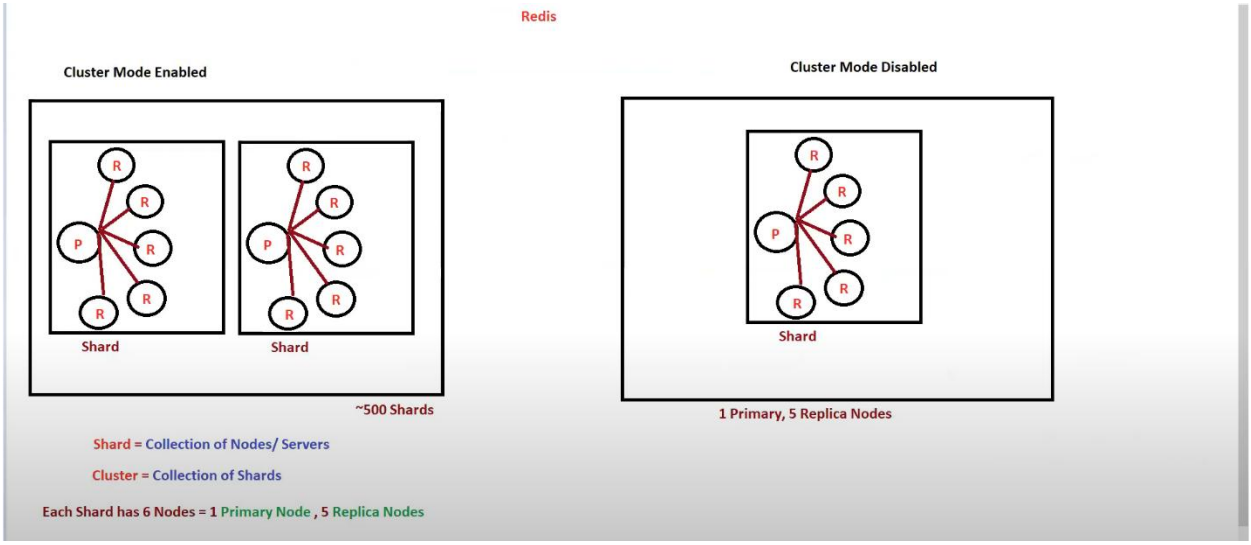
48TH SESSION AWS - RDS PRACTICAL

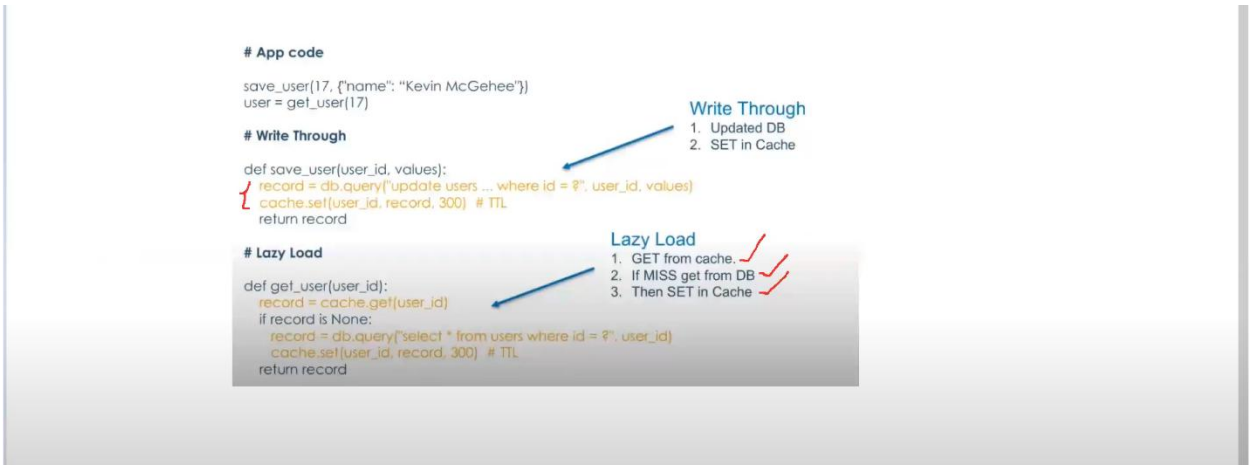
```
sudo yum install nfs-utils -y
mount -t nfs -o nolock,hard 172.31.29.167:/filegateway730am filegateway/
cd filegateway
mkdir filegateway


**********
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 ireland(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 intance, 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)
```

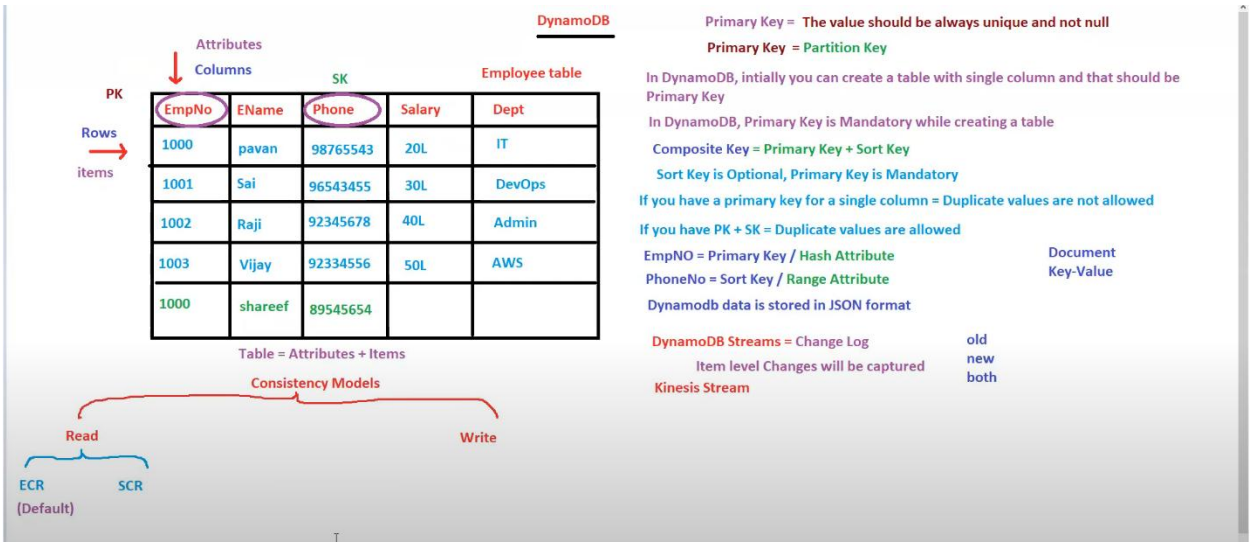
49TH SESSION AWS - ELASTIC CACHE SERVICE, REDIS TUTORIAL & PRACTICAL

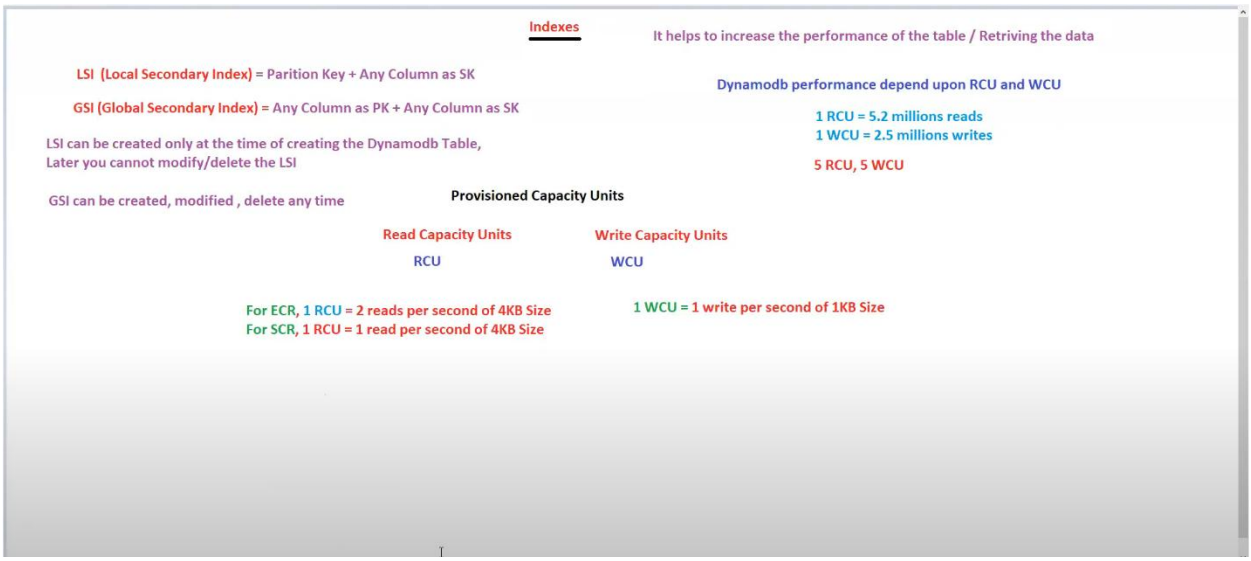





# App code
save_user(17, {"name": "Kevin McGehee"})
user = get_user(17)
# Write Through
def save_user(user_id, values):
record = db.query("update users ... where id = ?", user_id, values)
cache.set(user_id, record, 300) # TTL
return record
Write Through
1. Updated DB
2. SET in Cache
# Lazy Load
def get_user(user_id):
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
Lazy Load
1. GET from cache.
2. If MISS get from DB
3. Then SET in Cache

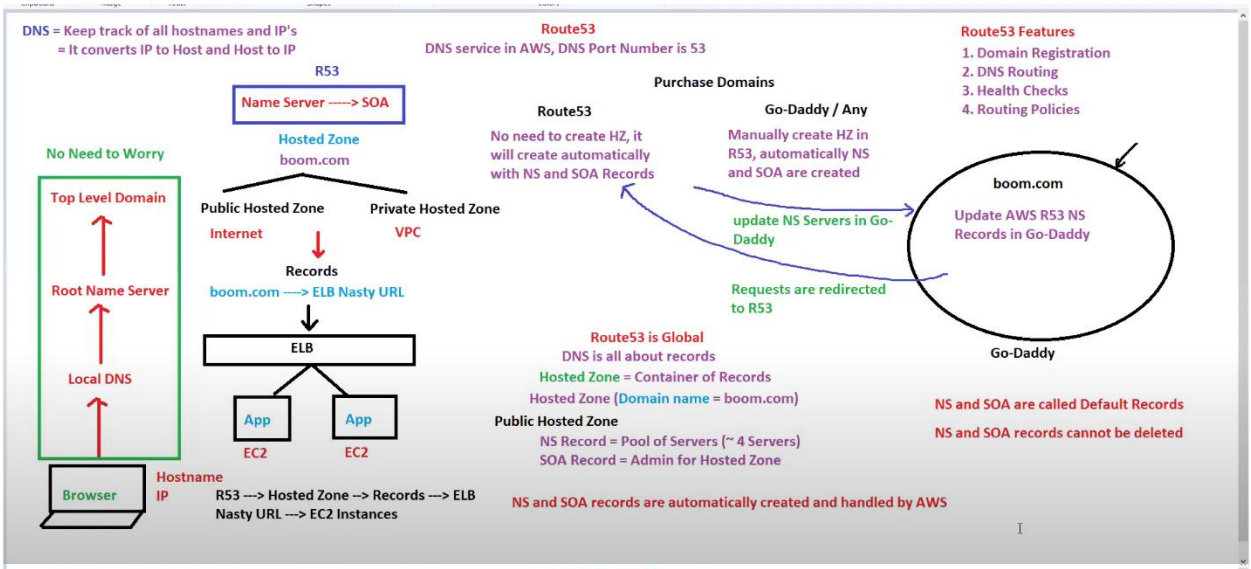
50TH SESSION AWS - DYNAMODB, INDEXES

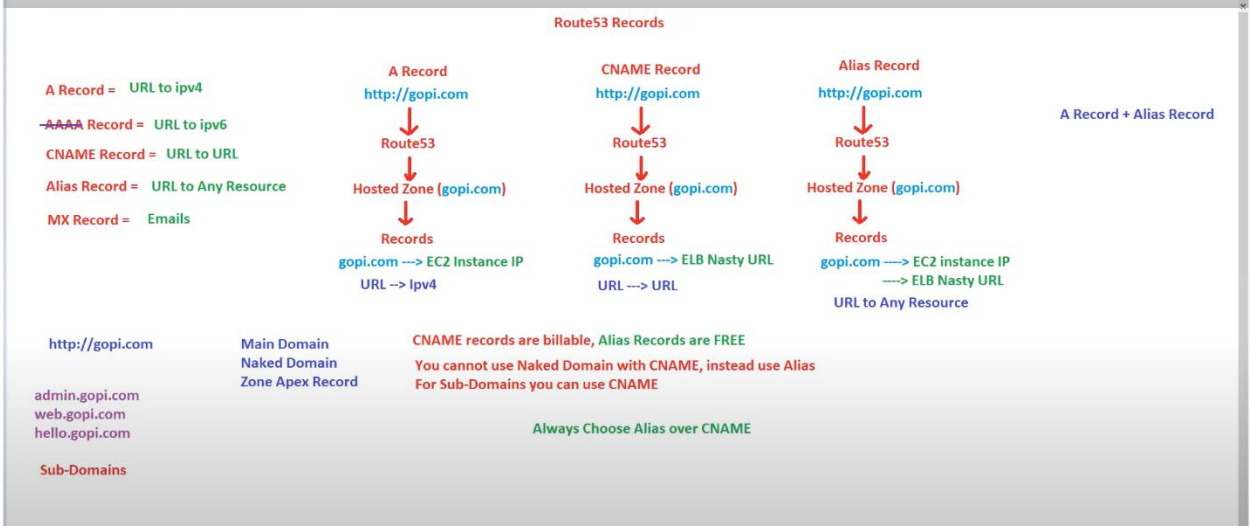


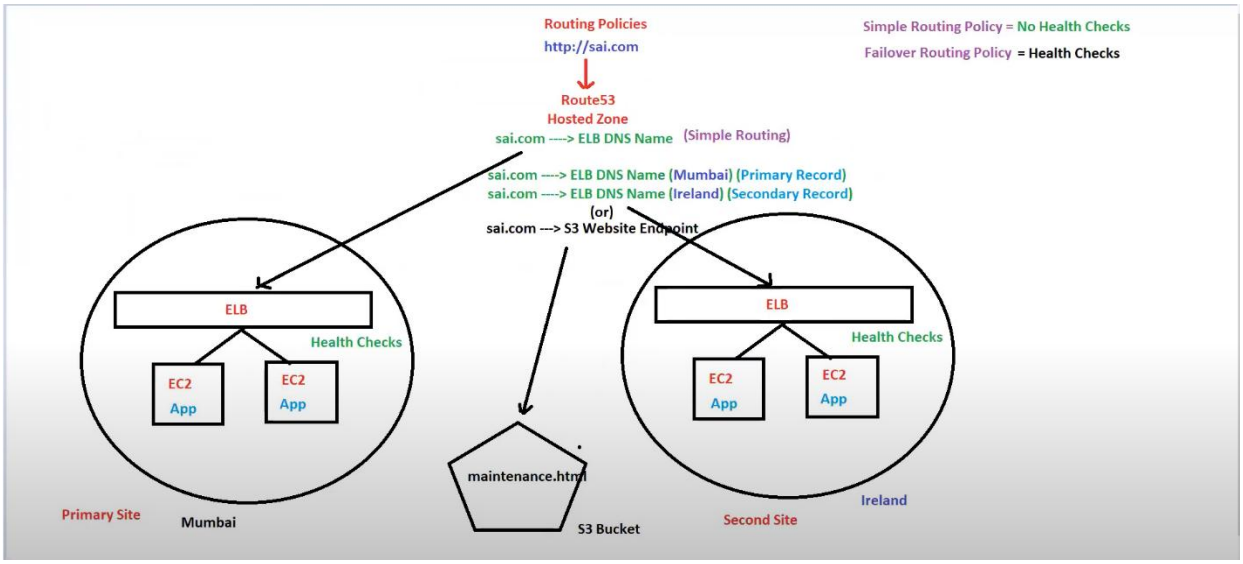


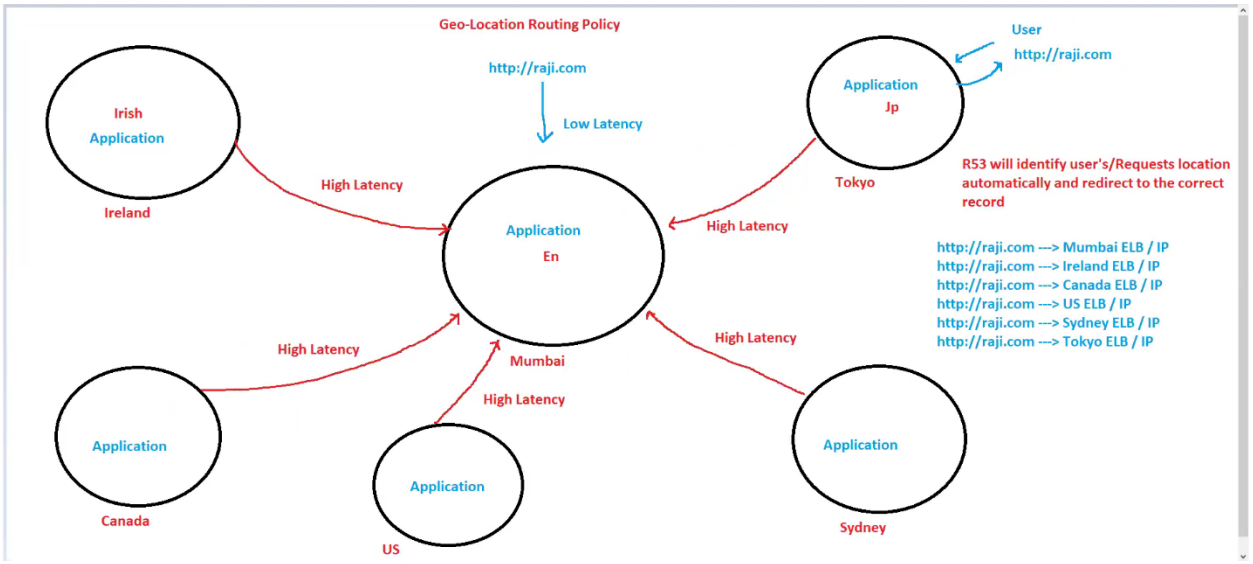
51ST SESSION AWS - DYNAMODB PROVISIONING CAPACITY PRACTICAL IN CONSOLE

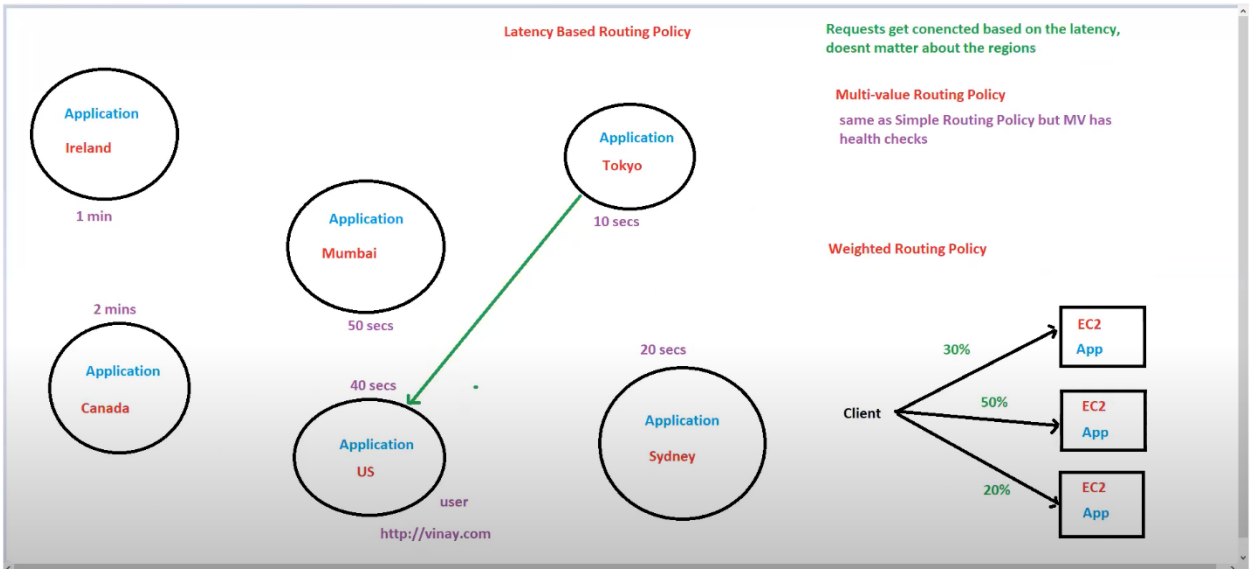
52ND SESSION AWS - ROUTE53 INTRODUCTION TUTORIAL



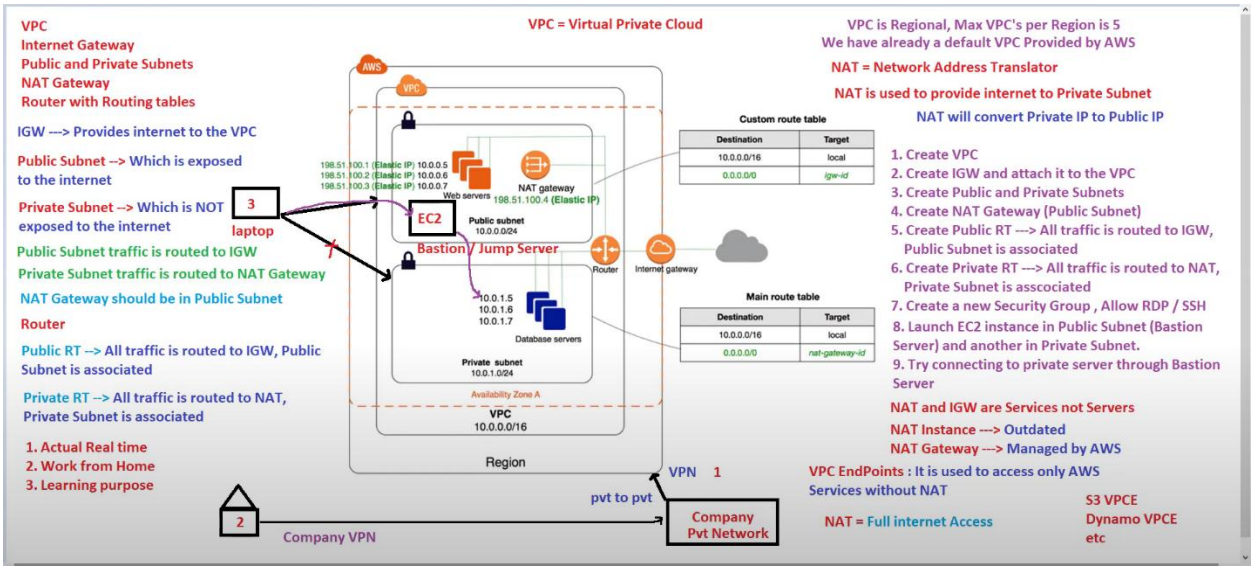


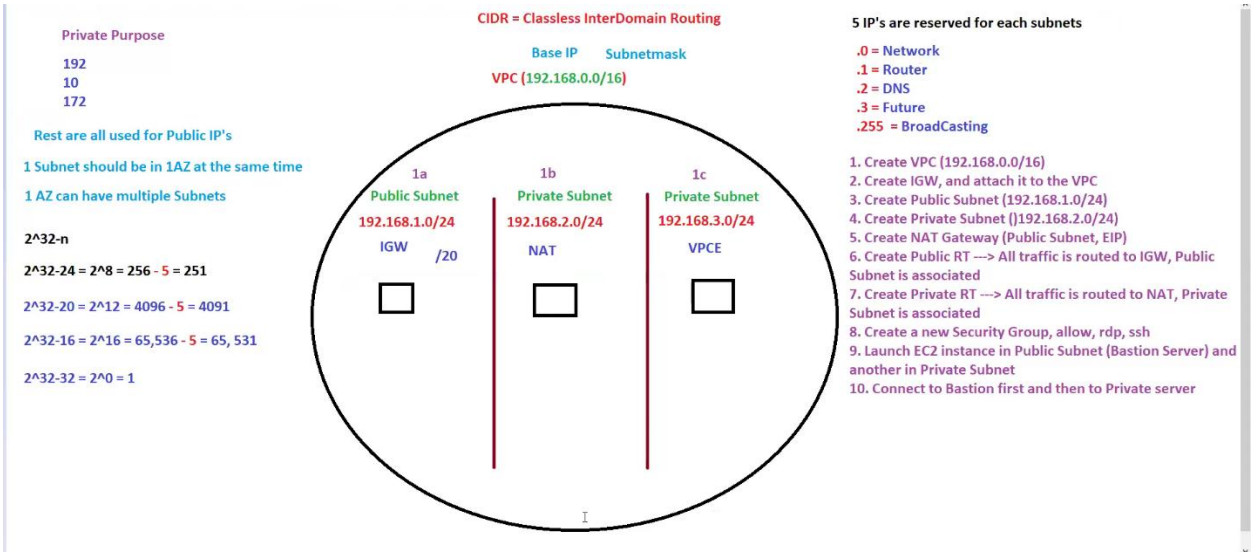

Routing Policies
http://sai.com
Route53
Hosted Zone
sai.com ----> ELB DNS Name (Simple Routing)
Simple Routing Policy = No Health Checks
Failover Routing Policy = Health Checks
sai.com -----> ELB DNS Name (Mumbai) (Primary Record)
sai.com -----> ELB DNS Name (Ireland) (Secondary Record)
(or)
sai.com ---> S3 Website Endpoint
ELB
Health Checks
EC2
App
EC2
App
ELB
Health Checks
EC2
App
EC2
App
maintenance.html
Primary Site
Mumbai
S3 Bucket
Second Site
Ireland


Geo-Location Routing Policy
http://raji.com
Low Latency
User
http://raji.com
Irish
Application
Ireland
High Latency
Application
En
Application
Jp
Tokyo
High Latency
R53 will identify user's/Requests location automatically and redirect to the correct record
http://raji.com ---> Mumbai ELB / IP
http://raji.com ---> Ireland ELB / IP
http://raji.com ---> Canada ELB / IP
http://raji.com ---> US ELB / IP
http://raji.com ---> Sydney ELB / IP
http://raji.com ---> Tokyo ELB / IP
High Latency
Mumbai
High Latency
High Latency
Application
Canada
Application
US
Application
Sydney


Latency Based Routing Policy
Requests get conencted based on the latency, doesnt matter about the regions
Application
Ireland
1 min
Application
Tokyo
10 secs
Application
Mumbai
50 secs
Multi-value Routing Policy
same as Simple Routing Policy but MV has health checks
Weighted Routing Policy
2 mins
Application
Canada
20 secs
40 secs
Application
US
user
http://vinay.com
Application
Sydney
Client
30%
50%
20%
EC2
App
EC2
App
EC2
App

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