

Cloud

<u>Public Cloud</u>	<u>Private Cloud</u>	<u>Hybrid Cloud</u>
* Public cloud is owned by cloud service provider like Azure, AWS.	* Private cloud is dedicated to one organization.	Hybrid cloud is combination of private cloud and public cloud.

VPC DISSETO

As per definition VPC is Virtual private cloud the VPC is enables to launch the AWS resources into a virtual network that we have defined.

A virtual private cloud is secure, isolated private cloud hosted within a public cloud. It is logically isolated from the other virtual network in the AWS cloud.

VPC is virtual our logical datacenter.

Subnets:-

Subnet is collection of datacenter or group of data center.

We can launch the AWS resources in Subnets such as EC2 instances.

③ How to secure the EC2 instance?

→ Controlling the network access for example through the configuring VPC & security groups

* Managing the credentials used to connect the instance

④ What is

→ EC2

that

in

in

A

⑤ What

→ *

*

*

*

*

④ Procedure for launch EC2 instance?

→ ① Open the Amazon EC2 console

② Choose the AMI (Amazon machine image) Example windows or linux etc.

③ Choose the instance type

④ Configure the instance details, we have to provide the some information based on the requirements

~~Processing information~~

⑤ Add the storage details and Add the Tags

~~click on the~~

~~Review and launch~~

~~Select on the cloud~~.

⑥ Configure the security groups

⑦ Finally click on the Review and launch.

~~the~~ ~~Review~~ for launching EC2 instance.

Q) What is EC2 instance?

→ EC2 instance is virtual server, is a web service that provides secure, resizable compute capacity in the cloud.

In the EC2 instance we can run the application on the AWS infrastructure.

Q) Why Amazon EC2?

→ * Auto scaling

* Pay-as-you-go

* Increased Reliability

* Elasticity.

* Auto scaling :-

is basically providing resources according to the demand. They either scale up or scale down corresponding to the increase or decrease demand.

* Pay-as-you-go :-

We have to pay only for what we have used, based on the time.

* Increased Reliability :-

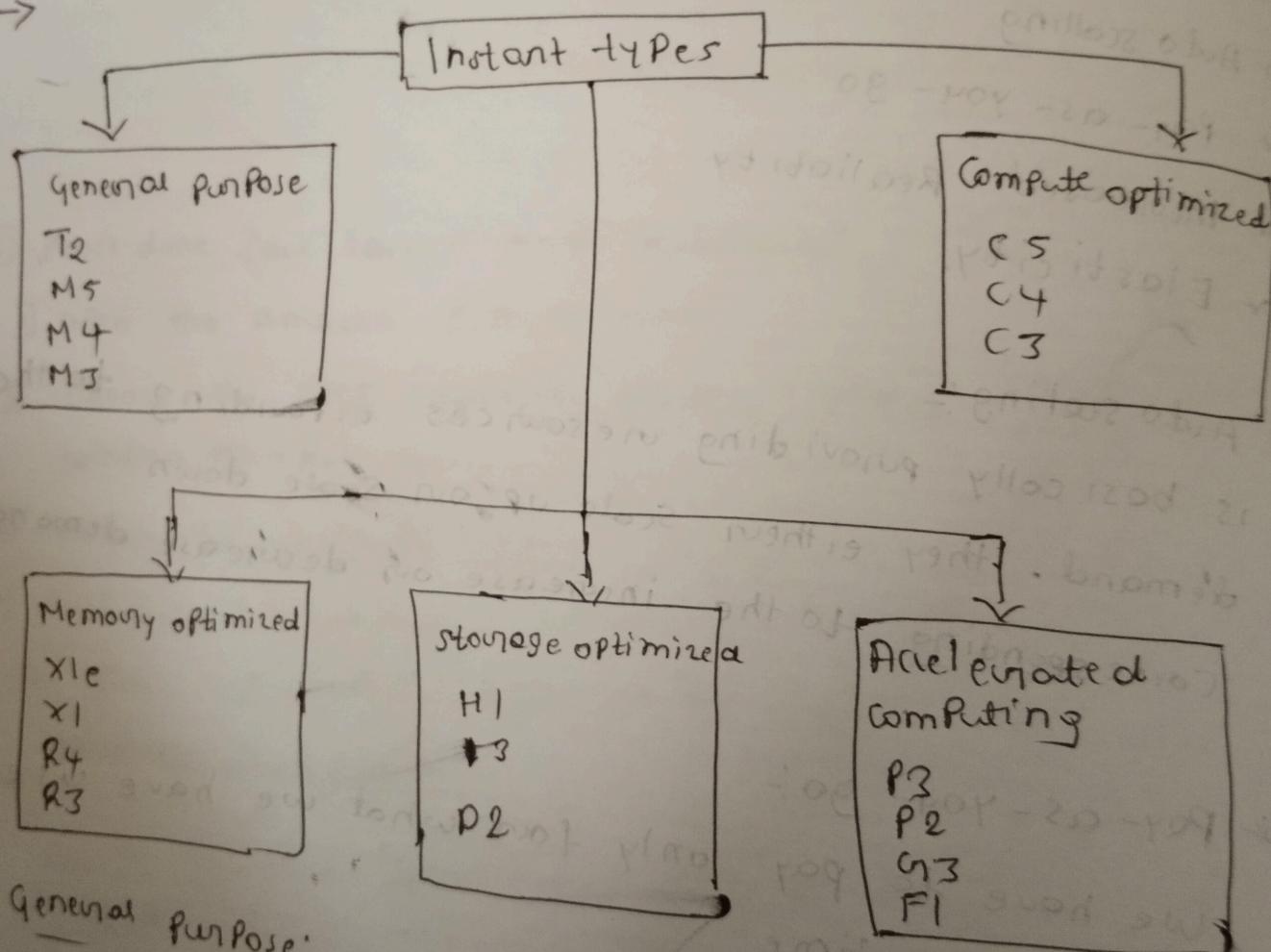
AWS is spread across 20 world regions with 61 availability zones. So we can run our application in multiple zones. So that when one datacenter fails or lose data, our application is running on another datacenter.

Elasticity

instead of 10-low-configuration machine, we can buy the single-high-configuration with user basis in the cloud based on the requirement, we can edit the configuration.

③ AWS EC2 Instance types?

→



* General purpose:

General purpose instance provide a balance among compute, memory, and networking resources. One they can be used for variety of workloads.

Compute instance:

* Compute optimized instance:

these instances are useful for compute dependent application that need high performance processors

they are well suited for the following application like

* batch processing workloads

* High performance web servers

* High performance computing

* Scientific modeling

* gaming servers

C5, C4 and C5N are the instances under this category

* Memory optimized instance

these instances are for delivering fast performance for processing large data sets in memory.

R5, R4, R5Q and R5D instances are memory optimized

* Accelerated computing instances:-

these instances are the latest gen-purpose instances

and they provide a accelerated performance

when the CPU clock rate increases

P3, P2, H3 and F1 are accelerated computing

P3 & P2 are general purpose instances

H3 is graphic intensive application

Storage optimized:

Storage optimized instances are designed for workloads that contain very large data sets

which has to be written in memory and requires high sequential read and write access.

Amazon EC2 instance Features

Many features of Amazon EC2 instance features

are customizable such as storage, virtual processors, memory available to instance

Elastic IP address:

it is a static public IPv4 address.

Operating System:

EC2 supports many OSes including Linux, Microsoft Windows Server, CentOS and Debian.

Amazon CloudWatch:

it is monitoring the AWS cloud services and application deployed on AWS.

Automated Scaling

Automated Scaling: Adding and removing capacity
EC2 Servers in response to application demand.
Based on the demand it will adding & removing
Capacity of EC2 Servers.

① How to Create an AWS EC2 Instance from scratch

→ open the AWS Management console and click the EC2

② Creation of an instance
click on Launch instance

③ choose the AMI section

④ Configure the instant details like

number of instances

Networks VPC details

subnet

Public IP enable or not

IAM Role

those things we have to configure

⑤ Next adding storage details

⑥ Add the tags

for identifies the particular instance while it is running.

⑦ Create the new security group then click on review and launch.

⑧ then Review your instant details and then launch it

⑨ Creating a new key pair.

Choose the a new key pair. and give a name for key pair. download key pair then proceed the launch instance.

→ keep downloaded key pair in safe location for accessing the virtual machine.

if it is a window server we can use the RDP. for accessing server using this key pair if it is linux we can use the git bash for accessing the server using this key pair.

VPC

Q) What is actual definition on the term VPC?

→ VPC - Virtual private cloud is a private space within the Amazon cloud that enables to launch the AWS resources.

Up to 5 VPC we can create in one region
200 subnets

VPC are fully customizable. we can create a subnets, set up route table, configure the network gateway, set up network access control lists, choose the IP addresses range and many more in virtual private cloud.

Q) What are the components of Amazon VPC?

* Virtual Private cloud:

A logically isolated virtual network in the AWS cloud.

* Subnet:

A segment of a VPC's IP address range, where we can place groups of isolated resources.

* Internet gateway:

It allows communication between your VPC and the internet.

* NAT gateway:

It makes easy to connect the Internet from the instances with in a private subnet.

* Hardware VPN Connection:

It is connection between your Amazon VPC and your data center.

* Virtual Private gateway:

Amazon VPC side of a VPN connection

* Peering Connection:

VPC to VPC private connection

* VPC End point:

We can access for S3 from our VPC without using internet gateway or NAT

③ What are Security Groups in VPC?

- > it is the manager traffic for the instance.
- > it acts as a virtual firewall that can control inbound and outbound traffic for different EC2 instances.

④ What is Network ACLs in VPC?

- > It is controlling the ~~inbound~~ inbound and outbound traffic in VPC.

Swami Komanagatta, Om bhumihalingeshwara, Gai Amareya

1) What is EC2?

→ EC2 instance is Virtual Server, is web service that provides Secure, resizable compute capacity in the cloud.

in the EC2 instance we can run our application on the AWS infrastructure

2) how to launch in EC2? selecting network, ami, security groups, subnets, key and user scripts?

→ 1) open the AWS management console and click on EC2.

~~① choose the AMI section~~

② click on launch instance

③ choose the AMI section

(its including linux, microsoft windows server, centos and debian)

④ configure the instant details like

Number of instance

Net work VPC details

Subnet

public IP Enable or not

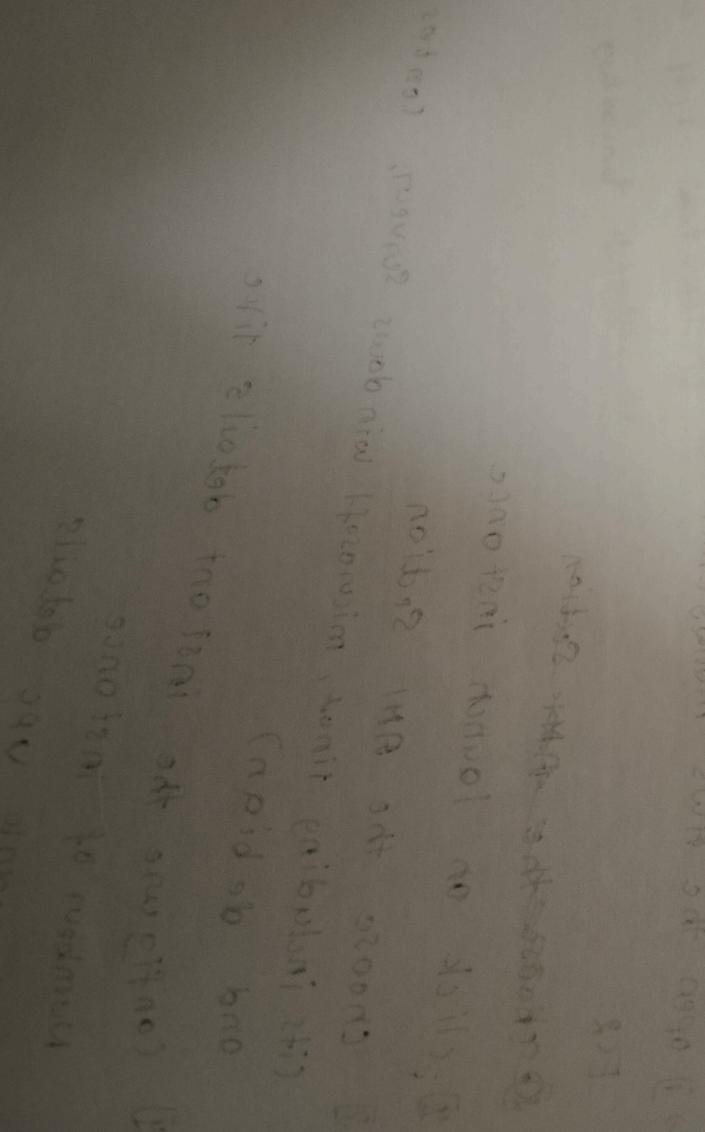
IAM Role

these we have to configure in this section.

~~DISCRETE~~ adding storage details

5) Next

- ⑤ Add the tags for previous host instance onto host for identify the particular instance and set the security group and set the key pair
- ⑥ Create the new security group and inbound and outbound rules
- ⑦ Click on review and launch
- ⑧ Creating the new key pair give the key pair name & download the key pair then launch the instance.



3) What are Scripts in EC2? How you can

find EC2 Advance Setting?

→ AWS user data is the set of commands /data we can provide the commands to a instance launch time.

For Example if I want launch the instance want to have docker, Then we can ~~set~~ provide set of bash commands in the user data.

then we can the instance with docker

using this user data scripts we can set the downloaded software or packages after launching time

- * go to EC2 → click on launch instance → give the instance name → select the AMI → select instance family → create the key pair
- configure the network setting → configure the storage → then click on the Advance details scroll down the details then down side we can get the user data ^{thing} / ~~thing~~ here we can write the script

Q) how to attach and detach role to ec2
-> Open AWS console
-> Open the EC2 console

② Choose the instance

③ Click ~~Create~~ action and click on Security and

Select Modify IAM role and choose

Q) Here we can attach and detach IAM role to our EC2 instance

Q) Why you attach IAM role to EC2 and what advantage of it?

-> To protect the instance against unauthorized access

Quesstion
Using IAM role we can grant access to the specific AWS service and resources

and assignments should restrict access to certain resources and services to certain accounts and regions

Q What happens if you stop/stand EC2 instance
→ When you stop the instance, data is stored
in the Amazon EBS volumes.

→ we don't change usage from stopped instance but
we do change from the storage Amazon EBS

Volumes will still know about the data stored

when you start the EC2 instance, it starts to
do the servicing. Amazon EC2 assigns a
new IP address to the instance.
IPV4 address will never change.

Q What EC2 lifecycle
→ EC2 instance life cycle determines how
on EC2 instance transitions through
different states from the moment it is
launched to its termination life
existing ~~existing~~ Pending, running,
shutting-down, terminated.

③ different ways to ssh into EC2

- > connect using the Amazon EC2 console.
- > connect using your key pair & ssh client

Q) what is the default user name of EC2 to ssh?

→ ec2-user on most

10) What is key based authentication?

→ key based authentication is more secure and allows encrypted method of authentication that allows the user to gain the access to target resources.

Q) What is security groups?

→ it can act as a virtual firewall for EC2 instances.

it can manage the inbound and outbound traffic from different EC2 instances.

inbound rule is applied for incoming traffic

outbound rule is (usually) for outgoing traffic.

QUESTION

Q1) how to attach a security group to ec2 instance.

- 1) open the AWS management console
- 2) click on EC2
- 3) then click on security groups & click on the Create security group.
- 4) Enter the basic details Security group name, description, ~~Open details select~~ VPC. and save
- 5) Edit inbound & outbound rules.
- 6) Edit inbound & outbound rules once we created security group
- 7) go to instance, select the instance, go to action and click on the Security then click on change security group
- 8) select the associated security groups the Add security group & click on save

the security group is attached to the EC2

13) can i attach multiple security group to EC2?

→ Yes, we can assign multiple security groups to EC2 instance and then attach multiple security groups to EC2 instance.

14) Point number:

SSH = 22

HTTP = 80

HTTPS = 443

dns = 53

NDP = 3389

MySQL = 1433

PostgreSQL = 5432

Ques 10) How to create custom security group?

→ 1) open the AWS console and choose EC2.

2) then click on the create security group and click on the create security group

3) Enter the basic details

Security group name, description

select the VPC, save it

④ then edit the in-bound

4) then we can edit the in-bound & out-bound rules.

VPC

Q) What is VPC?

→ VPC is Virtual private cloud, is virtual network dedicated to your AWS account. It is logically isolated from the other virtual networks. It enables you to launch AWS resources into a virtual network.

Q) What is Subnet?

→ Subnet is a range of IP addresses in our VPC. We attach AWS resources such as EC2 instances and RDS DB instances to subnets. We can create subnets to group of instances together according to operational needs.

Q) How to subnet calculation?

- Go to route table & select the route table
- ② On the Subnet association tab choose the Edit
- ③ Select Subnet Associated with Route table
- ④ Choose the Save option.

Q7 How to create subnet?

- Open the AWS console
- Go to VPC
- Click on the subnet & click on create subnet
- Choose the VPC & Availability zone for a subnet & create it.

Q8 What is Internet gateway?

- Internet gateway allows communication between VPC and Internet. It supports IPv4 & IPv6 address.

Q9 How to attach internet gateway to VPC?

- Go to VPC section

- Click on the internet gateway
(First we need to create internet gateway → Create internet gateway)

- Select gateway then go to action

- Select the attach VPC & choose Our VPC

- Attach the internet gateway to VPC

:3506 / / :3506

- ④ How to attach Internet gateway to Routetable?
- ① Goto VPC
- ② Go to RouteTable
- ③ Go to edit routes
- ④ In edit routes we can attach the Internet gateway, transmission of both incoming & outgoing traffic.

⑤ What is Routetable?

→ Routetable is enables the you can create private connection between VPC and another AWS services. it determined the where network traffic from our VPC is directed.

- ⑥ how to associate the Route table to Subnet?
- ① Go to Subnet & select the Subnet
- ② click on the route table
- Here we can attach the route table of subnet A.

~~What is routing table~~

→ What is subnet?

→ Subnet is the range of IP address within the VPC. It comes under the VPC. We can connect multiple subnet in VPC.

For example instance need to talk internet we keep it in a public subnet where internet gateway is attached.

on any other critical server we don't want expose to the internet we can keep it in private subnet because there's no internet gateway attached.

→ What is Routing table?

Whenever we create a subnet the routing table is automatically created.

A route table contains set of rules, basically it's going to have rules it determines where network traffic from VPC is directed.

Zone 1 / 25DG

- How to attach internet gateway to vpc
- Go to VPC & click on your table
- ① Select the vpc table
- ② Go to routes & edit the routes. Add another route.
destination IP as 0.0.0.0/0. & save it.

What is NAT Gateway? Why and How it is used?

- A NAT Gateway NATWORK Address Translation
- We can use the NAT gateway for private subnets
- Connect the internet on outside of the network.

QUESTION: What is VPC Peering & how to do it?

→ What VPC Peering is technique for securely

→ VPC Peering is connecting two or more virtual private cloud.

How to do it:

1) go to VPC

2) click on Peering Connection & click Peering Connection.

Config like Peering Connection like give the name.

Select the VPC requester &

select another VPC to peer with

My Account

Another Account

Region Other Region

Another Region

Save it

3) Once they

the Peering connection is established
they will receive accept Peering connection

DISSE70
1 Creating on S3 bucket and setting IAM Permissions
Object

→ Add

→
1 go to Amazon S3 → click on create bucket

→ Set

2 Give the general configuration.

GD

give the bucket name → select the AWS region

GP

3 object ownership.

ACLs disabled

— if bucket owned by the this Account, FOU Access
to bucket and its object is specified using only
Policies

ACLs Enabled.

— if the bucket is owned by the other AWS Account.

Access to bucket and Objects can be specified using
ACLs

→ Select the bucket versioning

- Disable
- Enable

Versioning means keeping multiple variants of an
object in the same bucket

we can use the versioning to preserve, retrieve and
restore Every version of Every object stored in S3

: 35DG

- Add the Tags
 - Server side Encryption
 - ① Disable
 - ② Enable

(Automatically encrypt new object stored in this bucket)
 - ~~the bucket~~ (we can create the key)
 - Then create the bucket.
- Once create the bucket we need to create IAM user.
- Go to IAM user.
 - Give ~~Read~~ the username.
 - Select the AWS Credential type
 - Access key
 - Password
 - Set Permission.
 - Give the Tags
 - Create the user.

DISSE70

→ once we created user; then we need to create the Access Policy

→ click on Policies



Add inline Policies



click on JSON tab



Here we can paste the Policies



once Review policies



then creat the Policies.



Policies is created,

How to create load balancer

- click on Ece instance
- Go to load balancer → click on create load balancer
- Then select the load balancer type
 - ① Application load balancer
 - ② Network load balancer
 - ③ classic load balancer
- create load balancer → select the IP address type
- give the load balancer name → select the availability zones
- Listener protocol
 - HTTP
 - BD
- select the VP
- select only one Availability zone (not both)
- give the tags (e.g. app for the load balancer)
- Create the security groups → Add rule
 - A
- click on config we mounting
 - Edit target group details
 - Health check Path
- Register the target groups
- Review and create

Q1 What is CloudFront?

CloudFront is

→ Content delivery network that retrieves data stored in the Amazon S3 bucket and distributes to its numerous edge locations across the world.

→ Cloud

Edge locations are the network of data centers

distributed worldwide through which content is delivered.

a sim
of
ups

Q2 CloudFormation

→ CloudFormation is service that helps

you model and set up your AWS resources

so that we can spend the less time

managing those resources.

Federations are

→ Cloud Formation is provider the user to with a simple way to create and manage a collection of AWS resources by provisioning and updating them in an orderly and predictable way.

We can simply create a template for any EC2 instances or for an RDS instances, and uploaded in the Cloud formation portal, and Cloud formation will provision and configure those resources based on the template we define.

⇒ Route 53;
Amazon Route 53 is highly available and
scalable domain system web service.
it helps to connect the user request to internet

application running AWS on on-premise

to distribute the requests and no need to consider
no separate tools for testing, monitoring, tool etc.
Amazon Route 53 provides the monitoring like
CPU usage, memory usage, latency, etc. No need

Cloud watch

→ Cloud watch is a monitoring & observability
service.

→ Collect and track metrics collect and monitor
log files, and set Alarms to help you
troubleshoot and respond quickly.

Main function of Amazon Cloudwatch.

1) Metrics:-
it provides the way to collect, store and monitor
metrics.

③ Alarms:

it allows you to set threshold from your metrics and we can receive the notification when the threshold is breached.

④ Logs:

it provides the way to monitor instance and analyze the logs from our AWS resources and application.

→ Metric monitoring with AWS CloudWatch.

→ collect & monitor the metrics from your AWS resources.

→ metrics is describe the behaviour on performance

of your resources , memory utilization etc.
like CPU utilization , memory utilization etc.

⑤ Setting Cloud Watch Alarms

→ can be set up the notify you when certain alarms can be set up the notify you when certain alarms can be set up the notify you when certain conditions are met.

conditions are met.

For example CPU utilization gone high that too time some time some auto scaling plans would be generated so that Auto scaling

plans would be generated so that Auto scaling
can happen for CPU utilization can be balanced.

~~DISADV~~
We could create an Alarm that should notify you when CPU utilization, on EC2 instance, will be set in threshold.

Notification can be sent by mail or SMS.

* Analyzing the logs with CloudWatch

→ CloudWatch Logs allows you to collect and analyze the logs from your AWS resources.

Cloud Watch:

It is a service monitor the resources in AWS.

- Go to Cloud Watch
- Click Alarms → click Create Alarm
 - Select the metrics
 - Auto Scaling
 - EC2
 - Network ELB
 - SNS
 - Select the metrics
 - Select the threshold type
 - Static
 - Anomaly detection
 - Define the alarm condition
 - Create threshold
 - Condition: Create/Equal
 - Comparison Operator: Less Than or Equal To
 - Threshold value: 200
 - Time Period: 5 minutes
 - Define the threshold value.
 - Configure the actions
 - Like Alarm state trigger
 - SNS topic → we can provide our Email ID (we need subscribe the topic in mail).
 - Add the name & description
 - Create the alarm.

Lambda: 29.556.70

What is Lambda?

→

Load balancer stores details about instances

→ open the EC2 console → click on the Loadbalancer

→ choose the load balancer type

→ define the load balancer rule

→ load balancer name

→ select VPC

→ Listener configuration

→ Assign the security group for load balancer

→ Configure the health check for the EC2 instance

→ Add EC2 instance with load balancer

→ then give the Tags

→ then create & verify the load balancer

(Lambda was triggered when given a request from a mobile device -
Lambda will trigger off whenever there is a change in the bucket)

:3500 / / :3500

Auto scaling:

- Open the EC2 console
- Choose Auto Scaling group
- Choose Launch configuration →
 - * Give the name for Auto Scaling
 - * Select the instances
 - * Instance type
 - * Add the volumes
 - * Edit the Groups (where we are running application)
 - ~~The request is taken~~
where the requests are coming)
- Create the launch configuration
- Go to Auto Scaling.
- Select the launch configuration
(in the launch configuration) (which we mentioned)
- Configure the setting → Network settings
 - Select VPC & Subnet
- Add the load balancer
(or else add the target groups)
-
- Configuring the group size & scaling policy
 - Group size . Desired capacity Maximum capacity
 - Minimum capacity
- Scaling policy → set target value → 50.

Lambda:

→ Lambda is a SaaS Service.
it is a compute service using this we can run our code without provisioning managing service.

Q) what is the difference b/w Lambda & EC2

→

the provisioned resources like no. of vCPU, memory etc. are managed by AWS.
Lambda - off loaded (no need to manage)
EC2 - self managed (need to manage)

→ Lambda has no cost for idle time & smaller footprint

additional cost for cold start

costly off load for initial execution & scaling

EBS

Elastic block store
it provides the block level storage volume
for the instance.

Types of volumes:

SSD, HOD, Previous generation volumes

Q How to attach EBS volumes to instances?

→ open the ECE console

→ select the volumes

→ click on create volume

* select volume type

* add the size

* select availability zone

* create the volume

→ select volume → click on action

→ click select attach volume

→ select the instance

→ then attach the volume

we can attach the multiple volume to
one instance

Q how do increase the EBS volume size?

- open the EC2 console
- go to volumes → find selected volume
- right click on the volume ⇒ click the modify, volume
- choose configuration of volume like size, type
etc.
(we can only increase the volume)
- click on modify,
- login the EC2 instance putty or ssh tool
- type the command df -h
- block device name
→ the type XFS - shows /dev/xvdf
- size of -h
- increase the dev size

RDS:

What RDS is → RDS is a relational database service is a fully managed open source cloud database service

RDS:

Amazon Relational Database is managed SQL database service provided by AWS. RDS supports an array of database engines to store and organize the data. It also helps relational database management tasks such as data migration, backup, recovery, and patching.

MySQL is a relational database management system it is based on the Structured Query language.

It also helps database tasks such as data migration, backup, recovery and patching

Q What is Load balancing?

→ Load balancer is it will balancing load.

it will distributes the incoming traffic across the multiple targets.

3 types

1)

load balancer it will also noticeable incoming

new job

balancing between shadow

of

signs

shadow job to know no unique job

2) ~~dedicative~~ Auto scaling?

→ Autoscaling it monitors the application and automatically adjust the capacity of the instance

accordingly based on the monitoring job to maintain

on demand

multiple function

multiple worker

multiple target

if no load left

return job

idle

multiple worker

53:

object storage service.
that provides data availability, scalability,
Security & Performance,
we can store & retrieve any amount of data
any time, anywhere.

Route 53:

Route 53 is highly available & scalable domain
name system.
we can use route 53 to perform 3 main function
domain Registration, dns Routing, health checking.