AWS

CLOUD COMPUTING

Cloud Computing : The practice of using network of remote servers hosted on internet to store, manage and process data rather than a local server & personal computer.

on premises servers or **onsite servers** : A group of servers that are privately owned & controlled.

Cloud ⇒ The delivery of computing services like storage, database, Networking, Software, analytics intelligence & server.

Types of Cloud Models

① **Infrastructure as a Service ⇒ IAAS**

* IAAS is used by Network Architects
* IAAS gives access to resources like Virtual Machine and Virtual Storage

ex: Amazon web services (AWS), Microsoft Azure, Google Compute Engine (GCE) Rackspace, Digital ocean, Oracle Cloud, IBM Cloud.

EC-2 → By AWS

② **PAAS ⇒ Platform As A Service** :

* PAAS is used by developers
* PAAS gives access to run time Enviolmnet to deployment and development tools for Application.

ex: AWS Elastic Beanstalk, Windows Azure, Openshift, FB, Google Search Engine.

③ **SAAS ⇒ Software As A Service**:

* SAAS is used by END USERS
* SAAS gives access to the END USERS

ex: Microsoft office 365, G-mail, Google workspace

Resources. If we create anything underneath the services those are called Resources

AWS Region :

- AWS Region is a Seperate geographic area where we Cluster data Centres
- Each AWS Region is Completely Independent

Availability zones : Each AWS Region consist of multiple, isolated and physically Seperate AZ's within a geographical Area

* TO Avoid fault Tolerance Multiple AZ's are present & Scalability

Edge location : It is a data Centre, where end users access Services located at AWS Region to Reduce latency

latency : How much time it takes for data packet to travel Across.

IAM [Identity and Access Management]

* Provides access to Account Services where we can manage user, Roles, groups and password policy.
* It applies Globally to all Region.

Two ways to login as IAM user

1. using user name and password we can Access through Console
2. using Command line interface [CLI]
   * If we need to Install AWS CLI → then aws --version.
   * Then use command AWS Configure
   * Then it will giving Access Key & Secret Key which are present in user Credentials

→ Default Region → US-east-1 → North Virginia
→ Default output format → JSON.
→ To Change Region → --region ap-South-1 → use this in List of instance Command in CLI

To Change Region in order to list instance.

```
Command --region ap-South-1
```

How to Create User

→ Go to IAM
→ Click on Users → Click Add users
→ Enter name of User
→ Click the Box Auto Generate password
→ Click on reset password on login
→ Provide permission & Access
→ Click on Tags → Add Name
→ Review & Download CSV file
→ Click on Add user.

How to Create Group

→ Go to IAM
→ Click on Create Group → Give Group Name
→ Attach policies
→ Create Group
→ Select the Created Group
→ Attach the users required to Group

POLICY

A policy is a set of permission which is attached to a user, group and Role.

Q) In which format policy's are written?

JSON format

What is JSON Format ? Explain ?

1. Statement
2. EFFECT
3. ACTION
4. RESOURCE

POLICY STRUCTURE

1. EFFECT : Allow all the action Specified in the policy
   Deny all the action Specified in the policy
2. SID : unique name given for policy
3. PRINCIPAL : who is Assuming the policy
4. ACTIONS : Different Actions present in AWS is Specified
5. RESOURCES : on whoom are assuming the policy :

MANDATORY	Not Mandatory
1. Effect	1. SID
2. ACTION	2. Principal.
3. Resources	

Steps to Create Policy

→ Go to IAM
→ click on Policy → Create policy → Choose Service
→ Select the Actions & Resources → Click on Next
→ Enter Name of policy → Create Policy.

Steps to Attach policy to user

→ Click on created policy
→ Click on policy Usage
→ Select Attach → Select the required user
→ Click on Attach Policy.

Types of policy:

① Identity Based policy: Applicable on users, groups of users & Role
② Customer Managed → Accuracy of user
• AWS Managed policy → Accuracy of level.
• Inline policy or Session Based policy.

② Resource Based policy → Attach to a resource ex: EC2, S3
③ Session Based policy → Create a Temporary Session for a
of Inline Based policy.
Inline Policy → It is a embedded policy which is present while creating IAM user.

Two types of policy

① Identity Based policy: It can Attach to Iam user, Group user & Role.

ROLES: A Set of permission comes b/w the Services that grant access to action and Resources in AWS

Steps to Create Role:

→ Go to IAM
→ click on Role → Select AWS service → Click on EC2
→ provide the Access Required
→ Enter Role Name → Create a Role.

ASSUME ROLE

T S C (NOTES)

Assume Role Returns a set of temporary Security Credentials that you can use to access AWS resources that you might not normally have access to. These temporary credentials consist of an access key ID, a secret access key and a security token.

Steps

→ Creat a user in IAM user
→ Creat a role → Provide S3 bucket full Access
→ Copy the arn of the user
→ Go to the role → Click on trust Relationship → Edit
Edit trust relationship
→ Replace "Servic" by "AWS" & "ec2---." by "ARN of user"
→ update policy.
→ open cmd
→ Type AWS configure
→ Enter all the Credential of user & login
→ Run Command aws sts assume-role --role-- arn <ARN of role>
- - -role -session -name -S3-fullaccess -Ecomple
-- duration-seconds 3600
→ Credentials will be displayed Copy all the Credentials
→ Run Set AWS_ACCESS_KEY_ID = <Enter ID>
→ Run Set AWS-SECRET_ACCESS_KEY = <Enter secret key>
→ Run Set AWS_SESSION-TOKEN = <Enter Token>
→ Run aws s3 api list-buckets
→ S3 bucket name will be printed

Switch Role / Cross Account

Switch Role / Cross Account ⇒ give access from one Account to Another Account

Steps

→ login As a root user
→ go to IAM Create user & Download .CSV file
→ Create STS policy and attach policy to user
→ Go to another browser
→ login as Another user
→ Create Role → Select AWS Account ⇒ Add Another Account
→ ENTER ID of the IAM user ⇒ click on Next
→ provide Admin Acces to Role → Give Role Name → Creat Role
→ Return to browser 1 → login as IAM user → click on Switch Role ⇒ paste privat ID of Another user
→ Enter Role name. Click on Switch.

STS POLICY : [Security Token Service]

It is a web Service that enables you to request temporary limited privilige Credentials for (IAM) user

JSON → Java script object Notation.

CLOUD WATCH

Amazon Cloud watch monitors your Amazon Web Service (AWS) Resource and Application you run on AWS in real time.

Metrics:

Metrics are data about performance of AWS Resources

Basic Monitoring : with AWS will polls / get data for every 5 minute → It is enabled default

Detailed Monitoring : AWS will poll / get data for every 1 minute
↳ we should enable this Manually while launching the Instance.

ALARM:

Cloud watch Alarm allows you to watch Cloud watch Metrics and to recieve notifications when the Metrics fall outside of the level that you Configured

Alarm State : If the CPU utilization goes beyond the Static Static threshold alarm goes to alarm State

Three States in Cloud watch Alarm

1. In Alarm : If CPU utilization goes beyond the Static threshold
2. OK State : If CPU utilization is less than Static threshold
3. Insufficient : when there is No Data to compare with threshold.

In Alarm we have:

1. Notification
2. Autoscaling Action
3. EC2 Action
4. System Manager Action.

Events: Events indicates Changes in AWS enviornment

Event Resource : which Resource you want to Monitor

Event Target : To Alert the event change through Notification

Cloud watch events is Now moved as Seperate Resource Called Event Bridge

Logs: Cloud watch logs enables you to centralize the logs from all your systems, application & AWS Services.

Cloud watch X-Ray Traces:

It is used to Analyse, Debug & optimise the Application performance.

It may consist of Service Maps & Traces, where you can create a Service Map for an Application & Trace the API for particular Application.

Different Types of Metrics in Cloud watch

1. Instance Metrics → CPU utilization.
2. CPU Credit Metrics
3. Status Check Metrics
4. EC2 usage Metrics
5. Traffic Mirroring Metrics
6. EBS Metrics.
7. Dedicated Host Metrics.
8. Network Metrics
9. Meta data Metrics

How to Create Alarm:

→ 1st Go to Alarm Section
→ Click on Create Alarm
→ Then we have to Select the Metric
→ Then Give the threshold value
→ Then Select the Threshold type ie [Static or Anomaly detection]
→ Then Select the Notification
in that Select the Alarm State
like In Alarm, or OK or Insufficient data
→ Then Select the SNS TOPIC, if SNS Topic is created then Select that Topic or create New SNS TOPIC by giving the End point to which Notification should be sent
→ Then SNS Topic will be created
→ Then View in SNS Console.
→ Then click on create Subscription.

→ Then select the protocol [protocol → end point where you want to post those Notifications]
like EMail, SMS, HTTP, HTTPS, AWS Lambda Amazon SQS
→ Then again give the end point
→ Then your Subscription will be Created
→ & then you will recive the Confirmation mail
→ After that you will recive the Alarms through notification as per your threshold limit

CLOUD TRAIL

It is mainly used to track user and API usage Activity

Different API activities

GET	LOCK
POST	UNLOCK
PUT	COPY
VIEW	DELETE.
LINK	
UNLINK	

ex: GET HTTP://flipkart.com/user.
To Get the user of flipkart.com.

Event History: Gives access to download and Record AWS Account Activity

* Cloud trail events are kept for 90 days in Event History
Saved in S3 - Bucket

Events: Records API activity & all resources & user Activity

Three types of Events

① Managment events: Tracks all the activity with respect to AWS resource.

② Data events: Mainly used to track the events of S3 buckets, lamda functions & Dynamo DB

NOTE
Data stored in S3 bucket is called as objects
object = data in S3 bucket.

③ Insight events: Mainly Tracks the unusual Activity Performed in AWS Account. (Which is Continously analysing Cloud Managment).

We can only only enable Cloud Trail Insights events on that log maygement events

Steps to create Cloud Trail

⇒ In Cloud Trail, we need to go to Trails
→ Then we need to click on create Trail
→ Then we need to give the Trail Name
→ Then It will ask for Storage location
① Create New S3 Bucket & ② use existing S3 Bucket
→ Then we Need to Select the events
Managent Event & Data event & Insights events
& ~~Management event Select~~
If we want to track all the Activity with respect to Resource we need to Select Managent Event
or
If we want to track the events of S3 Buckets, dynamo DB & Dynamo DB we need to Select Data event
or
If we need to track unusual Activity performed in AWS Account we need to Select Insights Activity
In order to enable this we need to enable Managent Activity also
→ Then Trail is created.

How do you set cloud watch Alarm: (Imp).

- In cloud watch we have something called as Metrics which stores the data about performance of System
- Like if you consider CPU Utilization of ec2 instance there data will be stored under Metrics tab under Cloud watch
- ~~If we need to~~ Then if we need to ~~Select~~ set Alarm then select an Alarm Select the corresponding Metrics
- Once the corresponding Metrics has selected we need to set the Threshold
- once after the threshold is set. we have different Actions ~~to Select~~ in order to set the Alarm

Last page

- ~~If~~ one is you can send out a Notification
- 2nd thing you can take EC2 Action like Stoping or Rebooting Instance if threshold is crossed
- 3rd one is Auto scaling option

SIMPLE NOTIFICATION SERVICE [SNS]

① TOPIC: SNS Topic is a logical access point that acts as a communication channel.

② Subscription: To receive messages published to a topic, you must subscribe an endpoint to the Topic

In Subscription we must select the end point like Mail, HTTP, SQS, HTTPS, SMS, AWS lambda

what are the protocol supported in TOPIC (Standard & fifo)

- In fifo TOPIC → only protocol supported is SQS
- In Standard TOPIC → SMS, Email, HTTP, HTTPS, AWS lambda

Protocol: It is an Endpoint where we need to post the Messages

Definition: SNS → Simple Notification Service is a Notification Service, provided as a part of AWS

* It provides a low cost infrastructure for the mass delivery of messages, predominantly to mobile users.

Producers/Publishers: Any Application Continously generating the messages.

Consumers: Any Application Continously receiving Messages.

---

what why do we use Standard Que instead of FIFO Que

Ex: In Some Application where message ordering is not an important factor & if there is no issue if we receive multiple copy of message in that case we use Standard que instead of FIFO que

FIFO	STANDARD
* Strictly preserved message order	* Best effort Messaging order
* Exactly one message delivery	* At least once message Delivery
* Subscription: SQS Protocol	* Subscription: SQS, lambda, HTTP, HTTPS, SMS, Email.

SIMPLE QUEUE SERVICE [SQS].

It is hosted que for storing messages as they travel between Applications or Micro Services. where particular Microservice is producing the Message to Queue & particular Microservice is Recving the Message.

It has two types

1) FIFO [First In First out] : These are designed to enhance messaging b/w Applications when the order of operations and events is critical. [Important]

2) Standard : Standard Ques Support at least once message delivery. Due to high Distributed Architecture more than one copy of Message might be delivered out of order.

Question : Interview

Have you Configured SQS Que & How to Configure SQS Que

- Yes i have Configured SQS Que. In my current project there was a requirement where we had Microservice Based Architecture
- One of the Microservice was generating the messages which need to be consumed by Multiple Microservices. During which i had Created a Que.
- So where Microservices will be publishing the message to the Que & the other Microservices would be Looking the particular messages out of the Que
- So There are Mainly two types of Queues
  ① FIFO & ② Standard Que
- Depending upon the requirement we can go with any one of the Que

Microservice Architecture : It is an Architectural development Style in which the applications is made up of Small Services that handle Small portion of the functionality & data by communicating with each other. directly

SQS Configuration :

① Visibility Timeout : It sets the length of the time that a message received from the queue by one consumer will not be visible to other consumer.

Assume we have 2 Consumers, if one Consumer is consuming a message from the Queue & if we have set the Visibility timeout for 30 sec so till 30 seconds that message will not visible for other Consumers

② Message Retention Period : It is the Amount of time that Amazon SQS retains the message that doesn't get deleted

Default Retention Period - 4 Days

Range → 60 sec – 14 Days

Max Retention Period – 14 Days

③ Delivery Delay : If Consumer needs additional time to process messages, we can delay each new message coming to the queue

Delivery Delay is the amount of time to delay each message added to queue.

Max delay time → 15 mins.

default → 0 seconds.

④ Maximum Message Size

→ Default Max Message size → 256 KB.

If it is more than 256 KB we can use Amazon SQS Java extend Client lib (JECL)

↳ Max - 2 GB

⑤ Receive message wait time → 0 to 20 seconds

Dead letter Queue : If a message can't be Consumed Successfully you can send it to a dead letter Queue

DLQ let you Isolate problematic message to debug why they are failed.

How do you Set Cloud watch Alarm

- In Cloud Watch we have something called as Metrics which stores data about performing of System
- Like If you Consider CPU utilization of EC2 instance those data will be stored under Metrics Tab under Cloud watch
- Then if we need to set Alarm, then we need to Select Alarm & Select the Corresponding Metrics
- Then Corresponding Metrics is Selected and Need to Set the Threshold.
- Once after the threshold is set we have different Actions in order to set the Alarm
- Like 1st one you can send out a Notification
- 2nd one you can take EC2 Action like Stoping or Rebooting Instance
- 3rd One is Autoscaling Action ⇒ in which New Instance is Launched Automatically to Phase the load
- 4th one is System Managed.

- Then If you want to send a Notification, we will go with Simple Notification Service (SNS) & while we need to configure the Topics & Subscriptions
- If you have already Topic existing we need not to Configure it ⇒ In Topic we have two options ie FIFO & Standard one → FIFO one supports SQS protocol But Standard one supports protocols like
- If you dont have Topic means we Need to Configure it
- Then you need to Select Subscription
- In Subscription you need to Select the protocol. If we need Text Notification we need to go for Standard one.
- like the endpoint where you want to post the Notification

Protocols (like Email, SMS, HTTP, HTTPS, AWS Lambda) & SQS

- Then you need to give the endpoint like whom the notifications should reach
- Like if you Select Email protocol then you need to give the Email id as Endpoint
- Like this we can create a Alarm
  ⇒ After this you will receive the notification Alarms through Notification as per your threshold limit

KEY MANAGEMENT SERVICE : KMS

Key mangened Servic [KMS] → AWS Key Management Servic is a manged Servic that makes it easy for you to create & manage cryptographic keys and control their use across wide range of Aws Servic & in your application.

It has two types of keys

1. Customer manged keys
2. Aws managed keys.

1. Customer Managed Keys : Managed completely by customers for encrypting the data

2. Aws managed keys : Completely managed by Aws for encrypting the data.

: Encryption: It mainly used to MASK (Secure) your data

1. Customer managed key : we have two type
   a. Symmetric Key b. Asymetric key

a. Symmetric Key : In this Single Master Key can be used for both Encryption and decryption

b. Asymetric Key : In this two Master Key Should be create for encryption and decryption.

Server Side Encryption → (SSE-S3) → All the Encryption Techinque handled by AWS. In their AWS will manage MasterKey for data encryption.
In this Encryption happens when Data is at Rest

Data → S3 → Encr
Save then

Client Side Encryption : (SSE-KMS) → In this Customer Should provided Master Key for data Encryption.
In this Encryption happens one the fly

Data → Encr → S3
then

* Have you used KMS Services?

Yes, I hoved used KMS Services, where ever the used data comes there we can configure the KMS

* Have you created any Keys?

No, there was no such requirement in our project, As we have using SSE which means AWS is mapping keys.

Then explain Customer managed keys & types of CMK → Symetric & Asymetric

Steps to Create Customes managed Keys

→ Go to KMS
→ Select Custom Managed Keys
→ Select Symetric & Asymtric
→ Add Name to Key
→ Select users who can use the Key
→

AWS SECRETS

AWS Secrets manager helps you to protect Secrets needed which are needed to Access your Application, Services & IT Resources This Service enables you to easily Rotate, Manage, Retrieve database Credentials, API Key

Steps to Create Secrets:

→ Go to Secret → Select Secret type → Select other type of Secret
→ Enter Value ie user name & password
→ Select Default encryption Key
→ Mention Secret Name
→ Disable Automatic Rotation.
→ under Sample code Select the Code → Click on Store.

* How were you managing Credentials in your project?

We were using Secrets manager in order to store the credentials of database. So that particular Secrets are fetched by developer.

* What is the issue if it comes like Access denied error:

ie Need to give permission to ie policy & Roles.

ex: Attach Role of EC2 - Select full Access to instance

VPC [VIRTUAL PRIVATE CLOUD]

Amazon Virtual private cloud enables you to launch AWS Resources into a virtual network that you have defined.

Network : Collection of IP Addresses.

CIDR [Classless Inter-Domain Routing]

Classless Inter-Domain Routing is a method for allocating IP addresses for IP routing

→ Formula to Configure IP Address

IPV4 = 2^32 - n
IPV6 = 2^128 - n

IPV4 = 2^32 - n

ex: If IP address = 10.0.0.0/24

n = 24 → No of IP address required

2^32 - 24 = 2^8 = 256 IP address can be allocated

→ SUBNET

A Subnet is a Range of IP address in your VPC. You can launch AWS Resources into a Specified Subnet

Two types of Subnet :

① PUBLIC SUBNET : Resources residing in the public Subnet has access over the internet

⑤ Private Subnet : Resources residing in the private Subnet doesn't have access over the internet

Some IP address are reserved they are

A) First Four IP address and last one IP Address are reserved

① 10.180.0.0 [Network address]
② 10.180.0.1 [VPC Router]
③ 10.180.0.2 [DNS Server]
DNS [Domain Name System] ⇒ The internet's System for converting Alphabetic Names into Numeric IP address.
④ 10.180.0.3 [Future use]
⑤ 10.180.0.255 [Network Broad Cast address].

Steps for VPC process

① Creation of VPC
② Creat of Subnet
③ Creation of Routing Table.
④ Internet Gateway ⇒ Then Attach VPC to IGW
⑤ Then You need to Associate the Subnet to Routing Table.
⑥ IGW in the RT.

---

① Steps to Create VPC

* Go to VPC ⇒ Select Your VPC ⇒ Create VPC
* Click on VPC only.
* Select Enter IPV4 CIDR [10.0.0.0/24] ⇒ 256 IP address
* Select Tenancy as default
* Click on Create VPC.

② Steps to Create Subnet

* Go to VPC ⇒ Select Subnet
* Click on Create Subnet
* Select your VPC (which is already Created).
* Give name to Subnet ⇒ Select Availability Zone
* Enter IPV4 CIDR Block.

1st Subnet ⇒ PUBLIC Subnet
IPV4 ⇒ 10.0.0.0/25

Private Subnet
IPV4 ⇒ 10.0.0.128/25

Then with Private & Public Subnet we Created
But still there are Just Subnet not Public & Private

RT [Routing Table]

It contains set of Rules that are used to determine where the Network Traffic from your Subnet or gateway is directed.

* Public Routing Table
* Private Routing Table

① Steps to Create Route Table

→ Go to VPC → Create Route Table.
→ Enter Name & Route Table (PublicRT or PrivateRT)
→ Select VPC
→ Create Route Table.
→ Then ~~Select your Public Select~~

IGW [Internet Gate way]

Default Addr of IGW is 0.0.0.0

IGW is a logical connection between an Amazon VPC and the Internet.

IGW is Defined in Routing Table.

[* If we attach IGW to any of Subnet, that Subnet belongs Public Subnet].

② Steps to Create Internet Gate way

* Go to VPC → Create Internet Gateway
→ Enter Name
→ Click on Create internet gateway
→ Then Attach VPC to Internet Gateway in Actions
* Then VPC is Attached to IGW.

(5) Allocation of Subnet to Routing Table

* Go to RT
* Select Corresponding Subnet
* Then click on Subnet Association → edit Subnet Allocation
* Select Corresponding Subnet → Save Changes.
* Do ther for Two Subnets

(6) Add IGW in the RT

→ Go to Route Table → Select Rout which you want to make it as Public Subnet
→ Click on Corresponding Route ⇒ Edit Route
→ Add Route → Enter 0.0.0.0/0 ⇒ Enter IGW Name
→ Save Changes.

Then Public Subnet is Created.

VPC PEERING

It is a Networking Connection b/w two VPC's that enables you to route traffic b/w them.

Conditions of VPC Peering

1. CIDR block shouldn't overlap
2. Transitive peering relationships are not supported
3. If the VPC's are in different regions, inter region data transfer costs Apply
4. You cannot have more than one VPC peering connection between the same two VPC's at the same time

Steps to VPC Peering

→ Go to VPC → Select peering Connection
→ Enter name & → Select the VPC & Requestor
→ Select the Another Account → Enter AccountID & Acceptor
(or own Account)
→ Select the Region
→ Enter VPC & ID & Acceptors →
→ Then Accept the request
→ Create peering connection.

Acceptor: who is requested to VPC Peering

Requestor: who is requesting to VPC Peering.

NACL [Network Access Control list]

It is an optional layer of security that acts as a firewall for controlling traffic in and out of one & more Subnets

Steps of NACL

→ Go to VPC → Select Network ACL's → Select None
→ Select VPC → Create Network
→ Select Subnet → Subnet Association → Select Subnet → Overlap
→ Add Inbound and outbound Rules

SECURITY GROUP :

A Security group acts as virtual firewall for your instance to control inbound and outbound traffic.

Steps to Setup Security Group

→ Go to VPC → Security Group
→ Enter name → Select VPC
→ Add Inbound Rule
OutBound Rule will be always All traffic
→ Create Security group.

Q) If i need to restrict the usage of instance to specific user what will you do.

In Security groups & NACL in Inbound & outbound rule i will specify the IP & protocol used in Source Code in Source Code

---

Differnce b/w NACL & Security Group

NACL	SECURITY GROUP
* Firewall at Subnet Level	* Fire wall at Instance Level
* It is 1st layer	* It is 2nd layer.
* It is Stateless	* It is Statefull
* It only Allows	* It Both Allow & Deny

Stateless ⇒ Any Changes made in Inbound Rule will not be reflected in outbound Rule. It will add out Bound Rule seperately

Statefull ⇒ Any Changes made in Inbound Rules will be automatically reflected in outbound Rule.

Elastic IP:

It is on Reserved Public IP that you can assign to any EC2 instance in particular region.

EC2 [Elastic Cloud Compute]

AMI [Amazon Machine Image]

An AMI is a template that contain Software Configuration required to launch your Instance.

We can creat our own customised AMI images.
In my current project i have creato my own customised AMI Imge & will be using some AMI Imge for spinning up the Instance.

- What does your customised AMI Image made up of?

  My customised Image mainly consisting of Centos operating system & some Additional Application that need to be part of our Application.

- What role you Installing?

  Like we made some couple of Server where we need to install Docker, So instead of installing Docker again & again we would be customised AMI Image for spinning up of particular Instance.

- What was your Instance Configuration in your Company?

  We were using C5 family product where it has 16 core of CPU & 32 giga of RAM.

Types of Instances

① General purpose [T2, M5 & M4]
. T2 : Performance is more and can be used for many general purpose
M4/M5 : used for enterprise Application & Mid-Size database

② Compute optimised [C4 & C5]
→ used for High performance web Services & developing engineering Applications.

③ Memory optimized [X1 & R4]

It has high performance database in memory database

④ Accelerated computing [P3, P2, G3, F1]

G3 → used for 3D visualization & Rendering

F1 → used for security & financial analytics.

EC2 Purchasing options

① ON DEMAND → In these you can select the instance type & start, stop or Terminate the instance.

You are only charged if instance is running

② Reserved instance → In this we can purchase a instance for certain period of time.

③ SPOT instance → In this we "Bid" the instances type AWS will set the Bid price.

④ Dedicated Hosts → Here a separate physical machines will be allocated for you.

EBS (Elastic Block Storage)

* Amazon elastic block storage provides block level storage that can be attached to EC2 instances.

Note

① For one volume only one instance can be attached.

Snapshot EBS

We can take backup of EBS volume and store it to Amazon S3 Bucket by taking snapshots.

Data life cycle Manager.

You can use Amazon data life cycle manager to automate the creation, retention and deletion of snapshots.

Difference b/w snapshot & AMI:

An EBS snapshot is a backup of single EBS volume.

An AMI image is backup of an entire EC2 instance.

Steps to attach EBS volume & take snapshot.

* Launch two instances in different AZ's.
* Create EBS Volume & attach it to instance 1
* log in Instance 1 using putty & run 'lsblk' to verify volume attached to instance. But it will not be mounted.
* Format the disk "Mkfs -t ext4 /dev/ xvdf"
* Create directory mkdir /mnt/mydisk.
* Mount the disk "mount /dev/xvdf/ mnt/mydisk.
* Then df -TH to verify
* Create files in mydisk.
* Take snapshot of that EBS volume
* unmount disk : unmount /mnt/mydisk.
* Detach the volume from instance.

* Create a new volume from that snapshot
* Attach the volume to Instance 2.
  * Then create directory cd / then mkdir /mnt /my disk.
  * mount /dev/xvdf /mnt /my disk.
  * Then cd to mydisk.
  * Then ls → the files created in that volume will be present here also.

How to resize EBS volume.

→ Go to EBS volume.
→ Click on Modify → under allocated storage, increase the size.
→ In CLI enter resize2fs /dev/xvdf
→ Click on df -TH to check.

EFS (Elastic file system)

→ Amazon elastic file system is a regional service storing data within & across multiple availability zone.

EBS	EFS
* Cannot be shared across multiple instances	* Can be shared across multiple instances
* Hardly scalable.	* Scalable storage
* Block storage.	* Object storage.

EFS (Elastic File System)

Amazon Elastic file System is a regional service storing data within and across multiple Availability Zone.

EBS	EFS
* Cannot be shared across multiple Instance * Hardly Scalable * Block storage	* Can be shared across multiple Instance * Scalable Storage * Object Storage.

AUTO SCALING

Auto Scaling: Aws Auto Scaling Monitors your Application and Automatically adjust the capacity to maintain steady.

Horizontal Scaling: In Horizontal Scaling you add more EC2 Machines into your VPC.

Vertical Scaling: In Vertical Scaling you add more CPU and RAM to an existing EC2

Launch Template: Launch Template captures all the para required to launch an EC2 instance within one resource.

Steps for Auto Scaling:

1. Go to Auto Scaling
2. Enter Launch Template.

ELASTIC LOAD BALANCER

It will Manage and Control the flow of Inbound request to group of targets by distributing evenly across the targets.
The Targets may be EC2 instances, Lambda or Containers.

① Have you created the load Balancer? what is the type of load balancer created.
Yes i have created Application load Balancer in order to handel http & https requests.

Types of load Balancer:

① Application load Balancer: It is mainly used for Web Application running HTTP & HTTPS protocols.
* operates at request level.

② Network load Balancer: It mainly operates at Connection Level, whenever we require High performance at very low latency. It mainly route traffic to targets within VPC. It can handle millions of request per second.

③ Gateway load Balancer: It helps you to easily deploy, scale and manage your third party Virtual Appliances.

④ Classic load Balancer: It operates at both Connection Level & request Level & used for Applications that were built in existing EC2 [Discontinued on 15 AUG 2021].

Load Balancer Setup.

1. Go to Load Balancer in EC2
2. Create Load Balancer
3. Click Application Load Balancer & Create
4. Enter the name of load balancer.
5. Select Internet facing & Internal.

Internet facing: Load balancer can be accessed by outside world over the Internet ie users & customers.

Internal: Load Balancer can be Accessed only by your ~~Project~~ Organisation & Internal Members.

6. Select IPV4
7. Select the VPC & Subnets - web mapping has to be done
8. Then Create a Security → In Inbound rules add HTTP & HTTPS
   → Select the VPC & then add inbound rules.
9. Enter listners & Routing
10. Create Load Balancer.

Load Balancers Set up for HTTPS

1. Enter the name of load balancer
2. Select VPC & Subnets
3. Select the Security group
4. under Configure Security Setting [HTTPS asks for Security Certificate we have to take Certificate from trusted Organisation]

* IP address has to be mapped to domain name, for we can use Route 53 in AWS for mapping IP address to domain name
* After maping is done, Certificate should be taken from trusted Organisation
* They will provide all the required details.

(5) Configure Health Check

* Here we have to set response timeout, default time is 2-60 sec instances have to response to load balancer within response time given, then it is considered as Healthy.

* Then Interval has to be mentioned, default is 5-300 sec. Interval means Health check performs.

* Set unhealthy threshold: Attempts of response will be defined.
  for ex: 2 or 3

* Set Healthy response → Here also we are setting threshold to check response.

(6) Then select the backend instances

(7) Review & Create.

Target Groups / Listeners

Target groups are used to route request to one or more registered Targets when using a load balancer.

→ what are listners in ELB?
Listeners are nothing, by target groups which recieves the incoming request & route to the registerd Target.

→ what is Health check in AWS Elastic Load Balancer?
It is used for AWS monitoring to determine the availability of registered EC2 instances & their readiness to recieve traffic.

---

what: Cache: Cache is High speed data storage layer which stores a subset of data, so that future request for that data are served up faster.

ALIAS: Mapping of Hostname & IP Address to AWS Service

ROUTE-53

Route 53 is a Domain Name Server web we can map IP Address to Domain Name & HostName to Another Hostname.

DNS PORT Number - 53

→ Where do you register the Domain Name?
Route 53 is the service which we can use to register Domain Name.

- **A-RECORD** : A Record means mapping of domain Name to IP Address.
- **C-NAME RECORD** : Mapping of Hostname to Another Hostname.

C - Means → Ceronical

- **TTL [Time to live]** : DNS TTL is a setting that tells DNS resolver How long to cache a query before requesting a New one.

→ ROUTING POLICY

① Latency Routing Policy : we use this policy when we have resources in Multiple Aws regions & you want to route the traffic that provides least latency

② Weighted Routing Policy : we use this policy to route traffic to Multiple Resource in Proportions (%) that you Specify.

What are advantages of Route 53

- It is flexible, means Amazon Route 53 traffic flow provides flexibility in Choosing Traffic
- It a cost effective
- It is Secure
- It is Scalable, it mean it is designed to handle large amount of queries.

LAMBDA FUNCTION

Aws lambda lets you to run code without provisioning & managing servers.

Aws lambda languages:

Node JS, PYTHON, JAVA, GO, PYTHON3

Aws lambda integration:

Kinesis, API gateway, dynamo DB, AWS S3, Cloudwatch Events, Cloudwatch watch logs, SNS

① Have you written lambda function? & why do we use lambda

Yes, i have written lambda function in order to take snapshot of an EBS volume

② what is Trigger functionality :

I have configured trigger functionality where in it we were taking the backup every two weeks.

③ what a destination?

Also i have configured the destination where once the back up is success i would getting a notification in the mail.

SIMPLE STORAGE SERVICE - S3

Amazon S3 is a simple web service which can be used to store and retrive any amount of data

NOTE : S3 cannot be attached to instance

Buckets: It is a resource in S3 where we store data

Two types of Buckets:

① PUBLIC BUCKET : Data present in these Bucket have access over the internet.

② Private Bucket : Data present in these Bucket don't have accss over the internet.

→ In projects we use private Buckets.

→ Buckets can also be used to Host Static web pages.

Static web pages/website : web page which be common for every user is called as static webpage.

Applications of usage of Buckets :

→ It is used to store Application data.

→ It can be used to Host static webpages.

* Rules for Bucket Naming :

① Bucket Name should be unique

② Bucket name must be between 3 & 63 Charactors long.

③ Bucket name should only contains lowercase

④ Bucket name should only end with letters & numbers it should not have any special charaterists at end.

⑤ IP Address Cannot be given has bucket name

⑥ Bucket names can't begin with xn---

* Limitations of S3 Buckets :

① only 100 Buckets can be created per Account.

② Can hold unlimited objects.

S3 Storage Classes:

① STANDARD: * It is designed for general & All Purpose Storage
* It is very expensive
* Durability of object is more
* Availability of object is more

② Reduced Redundancy STORAGE:
* Designed for non-Critical objects
* Durability is more
* Availability is more
* Less expensive than Standard.

③ Infrequent Access:
* Designed for objects which are access less frequently
* Object durability is more
* Object Availability is more
* Less expensive than Reduced Redundancy Storage

④ Glacier:
* Designed for long term Archival Storage
* It will take long time to retrive objects from this Storage
* Cheapest of all S3 Storage Class.

S3 LIFE CYCLE POLICY:

S3 life cycle policy is a set of rules that automate the migration of the object Storage Class to different Storage Class

Steps to Create S3 Bucket

1. Go to S3 Bucket → Click on Create bucket
2. Enter the Name of Bucket
3. Select the AWS region
4. Choose the ownership.

ACL's Disabled - All the objects in the bucket can only Accessed by this Account

ACL's Enabled - All the objects in the bucket can be Accessed by other AWS Account.

5. Check the box block all public Accss
6. Bucket Versiong enable or disable.

Bucket Versioning:

Versioning means keeping of multiple variants of an object in the same bucket. We can use this feature to preserve, retrive & restore every version of object stored in buckets.

7. Select encryption key → [SSE-S3]
8. Create Bucket.

(1) Have you used encryption key on S3 Bucket?
⇒ Yes we have used [SSE S3] Key will be managed by AWS

(2) What is the Maximum size of S3 Bucket?
⇒ we can upload 5GB of data at single time, size of S3 is unlimited.

(3) What kind of encryption are in S3 Bucket
SSE - S3 ⇒ AWS managed
SSE - KMS ⇒ customer managed.

(4) Replication in S3 or S3 RTC? Cross Region Replication.
⇒ It is designed to replicate 99.99% of objects within 15 min after upload. we can replicate the data in same region or in different region.

(5) How to recover deleted files in S3 Bucket?
In list of Buckets ⇒ open the Bucket of delted object
⇒ Go to folder of delted object ⇒ Turn on list versions
⇒ Then enter Name of delted object
⇒ Then select the previous version and then click download.

RDB [Relational Data Base]

Amazon Relational Database Service make easy to setup, operate and scale a relational Database in the cloud.

What are the RDB supported in AWS

1. Amazon Aurora
2. MY SQL
3. Mario DB
4. Postgresql [POSTgres SQL]
5. Oracle
6. Microsoft SQL Server

Relation dataBase and Non Relational Database.

Relation Database or SQL: These database store data in rows & columns like a spread sheet

Non Relation data base or No SQL: These database doesn't use tabular schema of rows & column instead it use storage model.

Ex: MongoDB, DynomoDB.

Relation DataBase/SQL	Non-Relation Database /No SQL.
→ It is Rational Database	→ It is Non-Rational, Distributed Data Base
→ Vertically Scalable	→ Horizontally Scalable.
→ Pre-define Schema	→ Dynamic Schema.

CLOUD FORMATION

Cloud formation is a service in which you can set up your AWS resources by using or creating Template in which we will describe all the AWS resources we want

Template: It is a file where we declare AWS resources you want to create and configure. Template file will be written in JSON or YAML format

STACKS: Stack is a collection of AWS resources that you can manage as a single unit.

Basic Template

```
Resources:
  VPC:
  Type: AWS::EC2::VPC
  Properties:
  CIDR BLOCK: 10.0.0.0/16
```

There are 3 Sections in Cloudformation Template:

1. Parameters
2. Resources [Mandatory]
3. outputs

we have to specify parameters & outputs in Template to reuse the Template.

→ Have you written cloud formation Template?

Yes, I have written Cloud formation Template, it mainly consist of Parameters, Resources & output

Parameter: This section is mainly used to define the inputs to resource section.

Resource: This section is mainly used to define the properties of Resources that you are going to Create.

Output: In this section we can output some values depending on the requirement.

The codes can be written in two format
① JSON ② YAML

Where were you maintaing Template ?
We were maintaing in S3 Bucket.

Example:

```
Parameters:
VPC CIDR:
Description:
 Type : String
 Default : 10.192.0.0/16
Resources:
 VPC:
Type : AWS::EC2::VPC
properties
CIDR BLOCK : !Ref VPCCIDR

outputs:
 VPC:
 Description:
 Value: Ref VPC.
```

RollBack: RollBack enables your to AWS cloud formation to monitor the state of your Application during Stack creation and updating & to RollBack that operation if the Application breached the threshold.

Drifting: If any manual changes occurs AWS will detect & revert it. This is known as drifting in cloud formation.

COGNITO

* It mainly provides authentication, authorization & user management for your application

authentication → validating credentials
authorization → giving authority to access.

Cognito provides user flows
- Sign up
- Sign in
- forgot & change password
- Multifactor authentication.
- Email & phone verification

social identity can also be integrated to apps & web application using cognito
for ex:
1) facebook
2) google
3) Amazon
4) SAML → one authentication for many apps like Amazon, Prime, shopping, music etc.

AWS Cognito User Pools

AWS cognito user pools, which will manage user sign-up sign-in, password policies for the application.
→ It is there to authenticate users for our application

AWS Cognito identity pool

This is a service which was designed to authorize your users to use the various AWS services.
→ When you exchange the authentication token to get temporary AWS credentials which you can use to access the resources directly from the app

difference b/w user pool & identity pool.

* user pool acts as mediator b/w your app & external social identity providers.
* you can add multiple identity providers as you need.

* Identity pool provides access to AWS services directly from app.

diff b/w IAM & Cognito

IAM	Cognito
* Gives secure Access to AWS service & resources to your users	* It mainly provides authentication authorization & user management for your application.

ELASTIC BEANSTALK:

Elastic Bean Stalk is a AWS service that is used for deploying & scaling web applications.

diffrence b/w EBS & lambda.

EBS :- It acts as platform as a servic [PAAS] were you can manage some Aspects of the infrastructure. Developers can create test & deploy the application on the platform.

Lambda : In this you cannot make any changes to code once it is uploaded. It is a serverless servic. Lambda doesn't store data but it allows to acess the other data storage servic.

VPN.

It is mainly used to establish a secure & private tunnel from your network or device to AWS network.

two types of VPN

① **AWS site to site VPN**: It enables you to securely connect your on-premises network or office site to your Amazon VPC.

② **AWS client VPN**: Enables you to securely connect users to AWS network.

⇒ What are different ways to connect to private network
* Bastion host * VPN Connection
→ VPN connection is a best practise to connect to pvt network.

Have you configured or create a VPN client?

⇒ * First we need to spin up a VPN server in public subnet.
* Then download the VPN software.
* Install the software & enter all required credential
* Using those credentials we can access to AWS network, then we can connect to private subnet.

CLOUD FRONT (DNS)

Cloud front is fast delivery network service that securly delivers data, videos & applications to customers globally with low latency & high transfer speed.

Edge location:- It is the area where the contents will be cached, so when a user is trying to access my content, the content will automatically be searched in the edge location.

" A site that cloudfront uses to cache copies of your content for the delivery to users at any location.

① where the data will be cached after creating cloudfront distribution?
→ edge location.

Create distribution
↓
Origin domain → S3
↓ → ELB
S3 Bucket- acces.
↓
Public acces
↓
default cache behavion.
↓
Compress objects automatically ->.
↓
Viewer
· HTTP & HTTPS.
↓
allowed HTTP methods.

GET HEAD, PATCH
↓
Function allowlist
↓
Create distribution