WHAT IS AWS?

Amazon launched AWS, a cloud computing platform to allow the different organizations to take advantage of reliable IT infrastructure like IAAS, PASS,SAAS.it also provides pay-as-you-go.

advantages of aws:

1.Flexiblity

2.Cost effectiveness

3.scalablity

4.security

IAM SERVICE

WHAT IS IAM?

- IAM stands for Identity Access Management.

- IAM allows you to manage users and their level of access to the aws console.

- It is used to set users, permissions and roles.

- It allows you to grant access to the different parts of the aws platform.

FEATURES:

- Centralised control of your AWS account

- Shared Access to your AWS account

- Granular permissions

- Identity Federation

- Multifactor Authentication

- Provide temporary access for users

- Permissions based on Organizational groups

WHAT IS A ROLE ?

- A role is a set of permissions that grant access to actions and resources in AWS.

- These permissions are attached to the role, not to an IAM User or a group.

WHAT IS INLINE-POLICY?

Inline policies are policies that you create and manage directly into a single user, group, or role and it is temporary.

what is custom trust policy?

You can create a custom trust policy to delegate access and allow others to perform actions in your AWS account. [cross-a/c replication]

what is identity provider?

With an identity provider (IdP), you can manage your user identities outside of AWS and give these external user identities permissions to use AWS resources in your account.

==============================================================================================================

S3 BUCKET

What is S3?

- S3 is a safe place to store the files.

- It is Object-based storage, i.e., you can store the images, word files, pdf files, etc.

- The files which are stored in S3 can be from 0 Bytes to 5 TB.

- It has unlimited storage means that you can store the data as much you want.

- Files are stored in Bucket. A bucket is like a folder available in S3 that stores the files.

- S3 is a universal namespace, i.e., the names must be unique globally. Bucket contains a DNS address. Therefore, the bucket must contain a unique name to generate a unique DNS address.

TYPES OF STORAGE CLASSES ?

1. S3 STANDARD

2. S3 STANDARD IA

3. S3 INTELLIGENT TIERING

4. S3 ONE-ZONE

5. S3 GLACIER INSTANT

6. S3 GLACIER FLEXIBLE RETRIVAL

7. S3 GALCIER DEEP-ARCHVIE

LIFECYCLE MANAGEMENT:

Assume a lot of data is updated in an S3 bucket regularly, and if all the data is maintained by standard storage it will cost you more(even if previous data is of no use after some time). So, to avoid extra expenses and to maintain data as per requirement only life cycle management is needed.

BUCKET VERSIONING: BUCKET VERSIONING IS MEANS TO KEEP MULTIPLE VARIETS OF AN OBJECT IN THE SAME BUCKET

OBJECT LOCK:

OBJECT LOCK CAN HELP YOU TO PROTECT YOUR OBJECT FROM BEING DELETED OR OVERWRITTEN FOR A FIXED AMOUNT OF TIME OR INDEFINATE.

STATIC WEB-HOSTING:

A static website consists of a series of HTML files, each one representing a physical page of a website. On static sites, each page is a separate HTML file.

DYNAMIC WEBSITE:

A dynamic website uses server technologies (such as PHP) to dynamically build a webpage right when a user visits the page.

After typing in a certain web address, the server will find a bunch of different pieces of information that it then writes into a single cohesive web page.

MULTI-REGION ACCESS POINTS:

S3 Multi-Region Access Points provide a single global endpoint to access a data set that spans multiple S3 buckets in different AWS Regions.

Multi-Region Access Points offer a global S3 hostname that provides access to multiple S3 buckets across AWS Regions with automatic routing and failover between buckets.

==============================================================================================================

EC2 SERVICE:

WHAT IS EC2 INSTANCE ?

- EC2 stands for Amazon Elastic Compute Cloud.

- Amazon EC2 is a web service that provides resizable compute capacity in the cloud.

- You can scale the compute capacity up and down as per the computing requirement changes.

- Amazon EC2 changes the economics of computing by allowing you to pay only for the resources that you actually use.

what is the types of ec2 instances?

1. general purpose [m-series and t-series]

2. compute optimized [c-series]

3. memory optimised [r-series and x-series]

4. accelerated computing [p-series and g-series]

5. storage optimised [i-series and d-series]

what is launched template ?

Launch Templates allow you to create a saved instance configuration that can be reused, shared and launched at a later time.

Templates can have multiple versions.

EC2 Pricing Options:

1. On Demand: It allows you to pay a fixed rate by the hour or even by the second with no commitment.

2. Reserved: It is a way of making a reservation with Amazon or we can say that we make a contract with Amazon.

The contract can be for 1 or 3 years in length.

3. Spot Instances: It allows you to bid for a price whatever price that you want for instance capacity.

Spot Instances are useful for those applications that have flexible start and end times.

4. Dedicated Hosts: A dedicated host is a physical server with EC2 instance capacity which is fully dedicated to your use.

AMAZON MACHINE IMAGE:

An AMI contains the software configuration (for example, an operating system, an application server, and applications) required for the creation of EC2 instances.

WHAT IS EBS VOLUME ?

An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances.

types of ebs-volume:

1. ssd backed volume [BOOTABLE]: general purpose ssd [gp2]

provisional iops ssd [io1]

2. hdd backed volume: throughput optimised hdd

cold hdd

3. magnetic standard [BOOTABLE]

\* IOPS: READ AND WRITE OPEATION COUNT

\* THROUGHPUT ACTUAL MEASUREMENT OF READ AND WRITE BITS PER SECOND THAT TRANSFERED OVER A NETWORK.

SNAPSHORT: EBS SNAPSHORT ARE POINT IN TIME IMAGES/COPIES OF YOUR EBS VOLUME.

ITS RECOMMEDED TO STOP THE INSTANCE AND THEN CREATE SNAPSHORT TO AVOID DATA-LOSSES.

LIFECYCLE MANAGER: YOU CAN USE AMAZON DATA LIFECYCLE MANAGER TO AUTOMATE THE CREATION, RETENTION AND DELETION OF EBS SNAPSHORT AND EBS-BACKED AMI'S.

SECURITY GROUP: AN AWS SECURITY GRP ACTS AS AN VIRTUAL FIREWALL FOR YOUR EC2 INSTANCES TO CONTROL INCOMING AND OUTGOING TRAFFIC

SECURITY GROUP IS STATELESS [IN STATELESS YOU ONLY SET THE INBOUND TRAFFIC AND OUTBOUND TRAFFIC IS ALREADY SET.]

ELASTIC IP: IF YOU NEED AN FIXEDM IP ADDRESS FOR YOUR INSTANCE THEN YOU NEED AN ELASTIC IP.

YOU CAN ONLY HAVE 5 ELASTIC IP IN YOUR ACCOUNT.

NETWORK INTERFACE: An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

PLACEMENT GROUP: Placement group are way of a logical grouping for a independent instances together in a selected region.

where group members are able to a communicate with one another in a way that provides low latency and high avalibility

KEY PAIRS: A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance.

LOAD BALANCER: - Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones.

- Load balancer handles fault torlenace and high avalibility.

TYPES OF LOAD-BALANCER:

1. APPLICATION LOAD BALANCER: - Application load balancers are intelligent, sending specific requests to specific web servers.

- It is operated at Layer 7 of the OSI Model.

- it handles the request of HTTP AND HTTPS.

2. NETWORK LOAD BALANCER: - It is operated at the Layer 4 of the OSI model.

- It handles millions or requests per second

- It is best suited for load balancing the TCP traffic when high performance is required.

3. GATEWAY LOAD BALANCER: A Gateway Load Balancer operates at the third layer of the Open Systems Interconnection (OSI) model, It listens for all IP packets across all ports and forwards traffic to the target group that's specified in the listener rule.

TARGET GROUPS: A target group tells a load balancer where to direct the traffic to ec2 instance or fixed ip addresses [cidr].

LISTENER: A listner is a proccess that checks for connect requests using the protocol and port that you configure.

HEALTH CHECK: 300 SECONDS [5 MINS] ITS CHECK THE HEALTH STATUS OF YOUR TARGETED INSTANCES. IT PROCESS,SENSE AND MONITOR THE INSTANCES

IF TARGET GROUP IS NOT HEALTHLY IT GIVE UPDATE TO LOAD BALANCER.

AUTO-SCALING: It helps to maintain the avalibility of your applications.

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling

These features help you maintain the health and availability of your applications.

TYPES OF AUTO-SCALING:

1. MANUAL: [keep scaling policy same as it is ; desired= 4, max= 4, min=4]

2. DYNAMIC: [ increase and decrease] This is yet another type of Auto Scaling in which the number of EC2 instances is changed automatically depending on the signals received. Dynamic Scaling is a good choice when there is a high volume of unpredictable traffic.

3. PREDICTIVE: Predictive scaling analyzes each resource’s past workload and predicts the anticipated load for the following two days using machine learning.

4. Scheduled: Users may choose the time range based on which additional resources will be added. Scheduled autoscaling is a hybrid approach that operates in real-time, predicts known changes in traffic loads, and responds to such changes at predetermined intervals.

Tenancy: Tenancy defines how EC2 instances are distributed across physical hardware and affects pricing.

There are three tenancy options available:

Shared (default) — Multiple AWS accounts may share the same physical hardware.

Dedicated Instance (dedicated) — Your instance runs on single-tenant hardware.

Dedicated Host (host) — Your instance runs on a physical server with EC2 instance capacity fully dedicated to your use, an isolated server with configurations that you can control.

==============================================================================================================

VPC [Virtual Private Cloud] :

Vpc is a Virtual Network or data center inside aws for one client.

it is logically isolated from other virtual n/w in the aws cloud.

advanatages:

- maximum 5 vpc created in a region and 200 subnets in a vpc

- we can allocate max. 5 elastic ip

disadvantages:

- you cannot create same cidr in two vpc

- if you want to pair to another vpc then that should be in different aws region.

- same subnet cannot be created in different avaliabilty zones.

- once you created vpc with a cidr you cannot change

- you can use secondary cidr to extend the cidr limit.

vpc types :

1. default vpc - created in aws region when an aws account is created.

- it has default cidr [172.31.0.0/16] , security group , NACL and route table settings.

- has an internet gateway by default.

2. custom vpc - created by aws account root / iam user.

- aws user create custom vpc, subnet , internet gateway and route table.

public subnet: if a subnet's traffic is routed to an internet gateway, the subnet is called public subnet.

private subnet: if a subnet does not have route to the internet gateway, the subnet is called private subnet.

IP reserved:

1. 10.0.0.0 - network address.

2. 10.0.0.1 - reserved by aws for vpc route.

3. 10.0.0.2 - reserved for dns server.

4. 10.0.0.3 - reserved for future use.

5. 10.0.0.255 - Broadcast address.

Note : aws doesnt support broadcast address in vpc but reserve the address.

impiled router [logical router] : it is central routing function.

- it is connects the different az together and connect the vpc to the internet gateway

- you can have upto 200 route tables per vpc.

- you can have upto 50 routes entries per route table.

internet gateway: an internet gateway is a virtual router that connects with to the internet gateway.

- default vpc is already attached with a internet gateway.

- it supports ipv4 and ipv6.

nat gateway : In Nat gateway we can use public ip and private ip as well. whereas in nat gateway we only use elastic ip.

- For security updates and patches update of private ip instance we use Nat gateway.

- your charged nat gateway in hourly bases.

security group:

- it is virtual firewall work at network interface level.

- upto 5 security group per ec2 instance can be applied.

- can have permit rule , cannot have deny rule.

- stateful

- applies to an instance only.

NACL [network access control list] :

- Nacl is optional layer of security for your vpc that acts on a firewall for controlling traffic in and out of one or more subnet.

- stateless

- you can attach NACL with multiple subnet however a subnet can be associated with only one NACL.

- applies to all instances in the subnet.

VPC Peering: A vpc peering connection is a networking connection between two vpc that enables you to route traffic between them using ipv4 address and ipv6 address.

you can create vpc peering connection between your own vpc, or with a vpc in another aws account , the vpc mustbe in different region.

vpc endpoint: A vpc endpoint is privately connect your vpc to supported aws services. Endpoint are virtual device

Elastic File System [efs] :

AWS EFS is serverless , simple , elastic , set and forget file system that automatically grows and shrinks as you add and remove files with no need for management or provisioning.

Relational Database Service :

- Relational Databases are the databases that what most of us are all used to.

- Relational Database is like a spreadsheet such as Excel, etc.

- A Database consists of tables. For example, Excel is a spreadsheet that consists of a workbook, and inside the workbook, you have different sheets, and these sheets are made up of rows and columns.

Limitations of RDS :

- You can have upto 40 aws rds DB instance.

DB instance:

- Each DB instance has a Db instance identifier.

- The DB instance identifier must be unique for that customer in an AWS Region.

- DB instance Create a Master user. It has permissions to create databases and to perform create , delete , select , update and insert operations on the tables the master user creates.

Virtual Private Network :

Vpn connection refers to the connection between your vpc and your own on premises network.

site to site vpn support internet protocol security (ipsec) vpn connection.

the followings are the key concept of site-to-site vpn

- vpn connection

- vpc tunnel

- customer gateway

- customer gateway devices

- target gateway

- virtual private gateway

- transit gateway

Route53 :

Amazon route 53 is a highly available and scable cloud domain name system (dns) web service.

Route53 continous monitor your application ablilty to recover from failure and control application recovery with Route 53 application controller.

Features of Route 53 :

- easy to register your domain

- highly reliable

- scable

- can be used with other services

- health check

- cost effective

types of routing policy:

- simple routing policy

- weighted routing policy

- failover routing policy

- geolocation routing policy

- geoproximity routing policy

- latency routing policy

- ip based routing policy

- multivalue answer routing policy

Dns :

- dns stand for domain name system.

- dns is used when you use aninternet.

- dns is used to convert human-friendly domain name into an ip address.

- ip address are used by computers to identify each other on the network.

Domain Register:

Domain register is an authority that assigns the domain names so that is cannot be duplicated.

RECORD TYPE :

1. State Of Authority (S.O.A)

2. Name Server (N.S)

3. A Record [Address]

4. TTL [time-to-live]

5. C NAMES []

6. Alias Record