Cloud services models

Cloud computing is on-demand delivery of computer power, database, storage, applications and other IT services

It has features like multi tenancy & resource pooling, Rapid elasticity & Scalability.

- IaaS - Infrastructure as service (EC2)
  Basic things like networking, virtualisation, storage is managed by vendor rest everything is manager by user

- PaaS - Platform as service (Elastic Beanstalk)
  Data & Application is manager by user

- SaaS - Software as a service (Rekognition)
  Only Data is managed by the user

Cloud deployment models

- Public Cloud
  Service provider who provides resources publicly and can be accessed by everyone, it is an in-expensive and less wastage of resources but there are security concerns

- Private Cloud
  Offers services to limited number of people behind the firewall & the security concerns are minimised here

- Hybrid Cloud
  It is a combination of on-premises & private cloud and third party public cloud services.

AWS History

- Launched in 2002 to internally on amazon.com
- 2004 they launched SQS
- 2006 they launched SQS, EC2, S3
- 2007 expanded globally

AWS Global Infrastructure

It is basically divided into 2 different parts and these are

- Regions
  - Regions is nothing but locations where their data centers are installed
  - Clusters of data centers
  - Choose regions on the following basis
    - Compliances
    - Proximity: If a application is developed for specific region then choose your aws region as that country or nearest country available this will reduced the latency

        - Availability of service: Check if necessary service for your application is available in the region you're choosing because not all regions have all the services
        - Pricing: Pricing varies from region to region

- Availability Zones
    - The data centers in the region can be one or many and these data centers are known as availability zones & users can access the services from anywhere in the world
    - Each region has 3 minimum availability zones and maximum 6

Domains of AWS

- Compute (Easy to)
    - Raw server to host a website or services and EC2 has storage options available for you
    - Elastic Beanstalk
        - Helps to deploy various application on AWS, no need to worry about the underlying architecture and it is similar to EC2 but the difference is that it has its own predefined libraries where EC2 is clean & blank slate

- Migration
    - As AWS has data centres across the global you can physically move the data from one centre to another
        - It has a storage service called as snowball which helps in migrating data securely
- Security & Compliance
    - It has IAM i.e. Identification & Authentication management tool
    - KMS which helps to create public and private keys and keep your system secure
- Storage
    - It also has storage services like S3, it works as bucket object like a thing where bucket is storage space and objects is nothing but your files
    - We also have a **cloudfront** which is also known as content delivery network
    - We have **Glacier** where we can store archives which is highly affordable
- Networking
    - It includes services like VPC, Direct connect, Route 53(DNS)
        - VPC is a virtual network that allows and launch your AWS resources
        - Direct connect is a least internet connection which can be used in AWS
- Messaging
    - It assures secure messaging and various applications takes care of it, for example cloud trail and opswork

- Databases
    - Similar to storage but databases has different purpose, storage is where you store executable files and database has a very likely SQL option called as Aurora which helps you to execute SQL commands at very faster rate which is 5x faster than your SQL
    - It also has Dynamo DB which an non-relational database which helps to deal with various unstructured data sources
- Management Tools
    - Cloud watch it helps you to set alarm and it is a cloud monitoring tool

Instance

It is a virtual server which runs applications on Amazon EC2, it can be treated as a small part of a large computer you have which owns it individual services like networking, os & etc. Each virtual environment is called as an individual instance

EC2 service

It is a resizable compute service which is also known as elastic compute service

Types of Instances

- General purpose instances
    - It is suited for the applications where you need it to be cost effective whilst maintaining the performance.
- Compute instances
    - These are for those who requires lot of computational power

- Memory instances
    - These types of instances are used when you need more memory i.e. more RAM, multi tasking system require such instances
- Storage instances
    - When you wish to store or execute big data type of application where you deal with huge amount of data then you're in need of such instance
- GPU instance
    - When you're working with applications or development which involves high level of graphics processing & rendering in such cases a GPU instance is opted in

EC2 Instance Pricing Models

- On Demand
  Made available to you as when it is need for example on hourly basis

- Dedicated
  When a company is dealing with high confidential data then there is need of isolation from other vendors those who are using the shared space so in this

case a dedicated instance will provide such services but it is costlier than your on-demand instance pricings

- On Spot
  Such types of instances work on pricing bids we give to the aws, if the instance is available in particular pricing range than it is made available to use otherwise if the pricing increases then the sessions gets terminated in such scenarios you can work with volatile data if you have any

- Reserved
  If you are sure about the configuration you're looking for and the duration of time you wish to own such instance it becomes more affordable for you

Instances based on functioning

- Burstable
  This types of instances are good when you are aware about the cpu utilization limits for example if you think that only 40% cpu utilization is require then the instance will begin with it and if the later a lot more data comes in and requirement increases the processing power also increase of cpu to 100%

- EBS Optimised
  Such types of instances are chosen when quick response is needed, that means higher processing power. This instances provide high input & output processing power to meet your quick response needs
- Cluster Networking
  Instances are divided into clusters so that if first cluster needs to be performance optimized then second cluster can be storage optimized and third cluster can be gpu optimized and so on

- Dedicated
  Used when data security is very important to the company and requires isolations from sharing the instance space

AMI

AMI is a supported image of the maintained instances, for example if you need a multiple instance at a given point of time of same configurations then you can use this tool to launch multiple AMI of that instance.

Volume

Volumes are the storage attached to the instances which can be detached also and you can also add another volume to your instance if needed.

AWS Compute Domain

EC2

It is a raw server, like your personal computer that you are working remotely.

Elastic Beanstalk

It is an automated version of EC2 where you don't have the control over os but you have the control over the configurations. It is used basically to deploy the applications where you upload the code and your application is deployed to the AWS infrastructure.

AWS Lambda (Serverless computer service)

Again this is an automated version of EC2 but here you don't get control on os nor configurations, you just have to upload the code and you are done. No need to worry about the underlying architecture but the main hack is that you cannot deploy applications on lambda; it can be used only to execute background tasks.

AWS SDKs

These are the APIs which helps to developer for connecting to the desired service they want, these SDKs can be directly connected to the AWS

AWS S3

A **put event is a upload function**, Events is if something happening on S3 bucket you can configure the next actions or steps

IAM Policies Inheritance

- If you apply a policy at a group level then all the users in the group will inherit this policy
- Inline policy can be given to an individual user who is not attached to any group

IAM policy structure

- It consist of a version number of the policy which is basically the policy language date
- Id to identify the policy (optional)
- Statements: this can be one or multiple (mandatory)
    - We have a SID which is id of the statement (optional)
    - Effect: whether the policy allows or deny
    - Principal: It is account/user/role to which a policy will be applied
    - Actions: list of actions that are allowed or denied
    - Resource list: where to apply the action for eg, S3 bucket

How to access aws?

- AWS Management Console(protected by password & MFA)
- AWS Command Line Interface (CLI) protected by access keys
- AWS Software Development Kit (SDKs) protected by access keys

- Set of libraries which helps to manage AWS programmatically (language specific APIs)
- AWS CloudShell (it is available in very limited regions, if you create a file in cloudshell it remains even if the environment is restarted)

IAM roles for Services

Incase AWS Service wants to perform an action on behalf of your account then you need such roles

- Common IAM Roles
- EC2 Instance
- Lambda Functions
- CloudFormation

IAM Security Tools

- IAM credentials report (account level)
    - This is a report which has details about all the users and the status of their various credentials
- IAM Access Advisor (User level)
    - It shows the services permission granted to the user and when the the services was last time used
    - We can use this reports to revise our security policies

Bootstrapping

- Launching command when a machine starts, it is the only once run scripts
- EC2 bootstrap commands run with the root users, so they have sudo rights

Security Groups

- Controls how traffic is allowed into and out of your AWS Instance
- Security group has only **allow** rules
- Security group can be referenced by IP address or by Security Group
- Security group act as a firewall for the EC2 Instance
- Single security group can be attached to multiple instance
- Security groups are limited to the regions, if you change the region you need to add new security group

Classic Ports to Know

- 22 - SSH
- 21 - FTP
- 22 - SFTP
- 80 - HTTP
- 443 - HTTPS
- 3389 - RDP

Accessing EC2 Instance with SSH
Command: ssh -i <your pem file> <user name>@<public ip of ec2 instance>

EBS (Elastic Book Store)

- It is a network volume which you can attach to the instance while they run
- Only one EBS can be mounted at a time in CCP level
- EBS volumes are bound for availability in specific zones
- By default and Root EBS volume is deleted on instance termination, if you want to save some data then you have to untick the delete on termination option

EBS SnapShots

- It is used to make a backup of EBS volumes at any given point of time
- You can take a SnapShot of EBS volume even though if it is attached to the instance
- You can use the SnapShot of EBS volumes across different availability zones

EC2 Instance Store

- EBS volumes are network drive attached to your instance which has latency, If you need high performance then you can use EC2 Instance store
- It gives better I/O performance
- It is good for temporary storage like cache, temp memory because it gets terminated when you terminate an instance

EFS (Elastic File System)

- Managed NFS can be mounted on 100s of EC2 instances
- But it only works with the Linux EC2 instances
- It is highly scalable and expensive to use with per as you go structure

EFS IA (Infrequent Access)

It is for the files which are not accessed frequently but stored on your File System. If this option is enabled then it will automatically move the last accessed files to the IA storage based on the lifecycle policy

Elastic Load Balancing

High Scalability & Availability
There are two types of scalability

- Vertical Scaling
    - Increasing the size of the instance (eg. t2.micro -> t2.large)

- Horizontal (elasticity) Scaling
    - Instead of increasing the size of instance we increase the number of instances

Availability

It refers to running your application on AWS instances in 2 different AZ. The Goal of creating high availability zone is to survive data centers in disasters

Elastic load balancer (EBL)
will forward the internet traffic to multiple servers (EC2) instances downstream

4 different types of load balancers are offered by AWS

- Application load balancer(HTTP/HTTPS) layer 7
  - Http, https & gRPC traffic
- Network load balancer (Ultra high performance, allows for TCP) layer 4
  - Handles millions of request in a second
  - Manages tcp & udp traffic
- Gateway load balancer - Layer 3
  - GENEVE protocols
  - Used to route traffic to firewalls
  - Intrusion detection
- Classic load balancer - layer 4 & 7 (retire in 2023)

Amazon S3

- S3 stores the files in “buckets” which are top level directories and files under these directories are called as “objects”
- Bucket has a globally unique name across all the regions
- Objects in the buckets have a key which is the complete path of the object
- The maximum object size in S3 bucket is 5TB, if you want to upload anything above it, we have to use multi part upload.

Amazon S3 Replication
For S3 replication we must have versioning enabled
There are 2 variants of it

- CRR (Cross region replication) - Async in different region bucket
- SRR (Same region replication) - Async in same region bucket

S3 Durability

If you store 10M objects in S3 bucket then there are chances to lose a 1 object in every 10,000 years

S3 Availability

It has 99.99% availability i.e. it will be not available 53 minutes in a year when you’ll be accessing this service

S3 Storage classes

- These are different storage spaces where it is based on the use cases, for example instant retrieval, long term storage, secondary backup of a backup or very long term storage
- Objects can be move from one storage class to different storage classes by setting the life-cycle rules under the management options

S3 Encryption

By default there is a server side encryption, but a user can also make an encryption which is also called as client side encryption and both these models are available in aws

AWS Snow Family

It gives you actual physical devices to migrate data from in & out to AWS, the thumb rule is if you are taking more than a week of time to transfer some data then you are recommended to use AWS Snow devices

These are use for Data Migration (in & out from AWS) & Edge computing

Data Migration: Snowcone, Snowball Edge & Snowmobile

Edge Computing: Snowball Edge & Snowmobile

What is edge computing?

A place where a system is generating data but there is no internet connectivity, no computing power but you still want to do the computing without sending the data to the cloud and use all the aws services this can be possible with the help of AWS IoT GreenGrass

AWS Storage Gateway

It bridges the solution for on-premises and S3 storage because there might be demands for hybrid cloud

Databases

- Storing data on disks (EBS, NFS, EC2 & etc) can have some limits
- To structure the data & help in easy retrieval + storing data with help of unique indexes
- You can also define the relationships between databases
- Relational Databases - simple sql databases (RDS - Relational Database Service)
- Cannot SSH into RDS service
- Supports PostGres, MySQL, MariaDB, SSMS

Amazon Aurora (Non Open Source DB)

- Supports PostGres & MySQL
- Objective is more efficient & faster, scale up & down automatically by 1TB steps
- Read Replicas are made to handle the extensive read load which comes from application. There can be upto 15 read replicas of a Amazon RDS Service
- Amazon ElasticCache - In memory dataset
- No SQL Databases - non relational databases
- Vertical & Horizontal scaling is possible

Dynamo DB

- Fully managed available in 3AZ database
- NoSQL DB

- It is serverless db
- Absolutely single digit low latency
- It has no schema & everything is within one table

Dynamo DB Accelerator (DAX) - cache in between Dynamo DB for faster access
It gives microseconds low latency

Redshift
- this is based on PostGres and cannot be used for OLTP but good for OLAP (Data warehousing and analytics)
- Data is stored in columns instead of rows so it is columnar database
- It has a Massively Parallel Query Execution

Amazon EMR (Elastic MapReduce)
- This is not actually a database but it helps to make hadoop clusters to analyze and process huge amount of data
- A cluster can be made of more than 100 of EC2 instances
- It helps in configuring the ec2 instances to works smoothly with hadoop

Amazon Athena
- Serverless query service to perform analytics with s3 objects
- It uses SQL for processing the data
- You can use amazon quick sight for dashboarding and visualization of data if the analytics is done with the help of amazon athena

Document DB
It is a type of no sql db which is based on MongoDB

Amazon Neptune
- It is fully managed graph database
- Graph db is basically a social network

Amazon QLDB
- Quantum Ledger Database
- A ledger book is recording financial transactions
- Fully managed, Highly available
- Immutable System
- No Decentralized component
- Can be managed using SQL

Amazon Managed BlockChain - It can be Decentralised
- It is a service to join a public block chain network
- Create a private blockchain network
- Compatible with Hyperledger fabric & ethereum

Amazon Glue

- It is a tool for ETL process
- Fully serverless service

Docker

- It is a software development platform which allows developer to package their applications in container and deploy them easily on any os
- In docker containers can scale up and down very easily within seconds

ECS (Elastic Container Service)

- It helps of launch docker container on EC2 instance
- You have to maintain the infrastructure of ec2 instances
- AWS will only take care of starting and stopping the container

Fargate

- It helps of launch docker container on AWS
- You don't have to maintain the infrastructure of ec2 instances
- It is a serverless solution no need to launch any ec2 instances

ECR (Elastic Container Registry)

- Private docker registry for AWS
- Store docker images and they can be run on ECS or Fargate

Serverless

Anything which a developer doesn't takes care about the infrastructure and AWS is responsible for smooth execution of the codes & functions deployed by the developer
Main serverless services we saw till now are

- S3
- Dynamo DB
- Fargate
- Lambda (Pioneer of All)

Lambda

- You can deploy functions to this serveless service without worrying about scaling
- It is a run-on-demand facility
- Scaling is automated in lambda
- It is an Event Driver services - it invoke the function if some event is triggered
- Lambda pricing is based on calls and duration
- Time limit for lambda is 15 minutes

Amazon API Gateway

- It can be used to created serverless API
- It allows developer to create, publish, maintain, monitor & secure API's
- This service can be used because your lambda function is not publically accessible so to make it use for any clients you can create a proxy request to amazon lambda functions through amazon api gateway
- It supports REST & Websocket(Web streaming) APIs

Amazon Batch

- It is a fully managed Batch Processing service at any scale
- Batch service will automatically launch the EC2 or spot instances to execute the batch jobs based on the load
- No time limit for batch job as it is dependent on instances
- It is not a serverless service

Amazon LightSail

- It provides you with virtual servers, networking, databases, storage & etc without worrying about their internal functioning
- It doesn't has auto scaling
- It has less aws services integrations
- It is good for an individual for someone with no cloud experience

AWS CloudFormation

- It is a declarative way of outlining your AWS infrastructure
- The code which we write to create the infrastructure is called as stack
- You specify the requirements to it and it will basically create everything for you in the right order
- CloudFormation is used when it is a Infrastructure as a Code
- The template can be saved and reused anytime and anywhere on the AWS

AWS CDK (Cloud Development Kit)

- It is basically a infrastructure as code in your own desired language
- Use CDK CLI for transforming the code to CloudFormation template

AWS Elastic BeanStalk (PaaS)

- It is a developer point of view for deploying an application on AWS
- Beanstalk from a cloud perspective is a platform as a service model
- It is fully managed by AWS
- Health monitoring is also done by beanstalk
- It uses a cloudformation for provisioning infrastructure for our application

AWS CodeDeploy

- It is again used for deploying the applications automatically
- It can be used for versioning of the code, basically V1 to V2 upgrades
- It can also used to migrate on premises servers to AWS
- It is basically a hybrid service

AWS CodeCommit

- Before publishing code live on internet you need to store it somewhere, here this solution helps you to version your code automatically
- It is a competitive product to GitHub

AWS CodeBuild

- It helps to build the code, run & test to get ready for deployment of the final product
- It is fully managed and serverless

- It comes with pay-as-you-go pricing model

AWS CodePipeline

- Used for orchestrate the process of fetching, building, Test & Deployment
- It ensures that the CodeCommit, CodeBuild & CodeDeploy service works hand in hand to deploy the code in final products like Elastic Beanstalk
- It is a core part of CICD services (Continuous Integration & Continuous deployment)

AWS CodeArtifact

- If your software package has dependencies then its build is dependent until we retrieve and execute them
- Traditionally we have to make our own artifcat management systems but nowadays aws offers the one with more secure, reliable & cost effective solution
- It works with build tools like maven, gradle, npm, yarn, twin, pip & NuGet
- Development can use CodeBuild and then can retrieve the dependencies from CodeArtifact

AWS CodeStar

- It is a tool to manage the software development activities at one place
- It quickly allows you to set-up with CodeCommit, CodeBuild, CodeDeploy, Elastic BeanStalk & etc

AWS Cloud9

- IDE for writing, running & testing the code in the cloud itself
- Works in your web browser
- It allows for code collaboration
- Its basically a Cloud IDE

AWS SSM

- It allows to manage the EC2 & fleet of server on premises
- Allows to patch the systems
- Runs the commands simultaneously across the server fleet
- It works with all major os like linux, windows, mac os & raspbian
- It also gives the operational statistics of the machine

SSM Session Manager

- Allows to start secure shell on EC2 & on premises servers
- It doesn’t requires port 22 to be opened
- It doesn’t requires ssh or bastion host

Global Applications

- It is a application which is deployed in multiple geographies i.e regions or Edge Locations
- It helps to decrease the latency
- It has also help in disaster recovery if a region goes down
- Attack Protection

Amazon Route53
Its is a managed DNS
A DNS is a collection of address with allows users to find the server with the help of URLs
Routing Policy

- Simple - doesn't has health check
    - One to One http request
- Weighted
    - Weights are assigned to the servers and load balancing is done
- Latency
    - Used to minimize latency where user is redirected the nearest server
- Failover routing policy
    - If the primary server is dead because of some reasons, request are redirected to the failover servers

CloudFront (Content Delivery Network)
- Improve read performance, content is cached at edge location
- Improves user experience
- 216 edge locations
- Prevents DDOS protection

AWS Outpost
- These are the server racks which will allow for on premises development of your applications
- It comes with pre-installed aws services

AWS Wavelength
- Wavelengths are infrastructure deployments embedded with telecommunications providers data center at the Edge of 5G networks
- Ultra low latency to applications with 5G network

AWS Local Zones
It is used when the VPC needs to extend the services and user needs low latency access

Cloud Integration
- Synchronous
    - application-application
- Asynchronous
    - application-queue-application

Amazon SQS (Simple Queue Service)
- Oldest offering of AWS (10+ year olds)
- Fully managed service
- It is use to decouple the applications
- Default retention is 4 days, max retention is 14 days

- Low latency

Amazon Kinesis
- It is used for real time big data streaming
- Fully managed service
- It can handle traffic from multiple sources with low latency (Kinesis Streams)
- Analytics can be done with the help of (Kinesis Analytics)
- To send output to S3 or redshift we use (Kinesis Firehose)

Amazon SNS (Simple notification service)
Send one message to multiple receivers

Amazon MQ
- If using traditional protocol from sending message no need to re-engineer the application just install amazon mq on premises to it integrates two technologies
- It should be used if company is migration from traditional on premises server to cloud but want to use the open message protocols

Amazon CloudWatch Metrics
- Provides metrics of every amazon aws services
- Metrics have timestamps
- EC2 Instances: utilisation, Status check, network traffic (No RAM Metrics)
    - By default it is refreshed at 5 minutes
    - Optional detailed monitoring per minute available at a cost
- EBS Volus: Disk Read & writes
- And many more

Amazon CloudWatch Alarm
- It is used to trigger notification for any metrics
- Alarm Actions can be
- Auto Scaling groups (Extend or Shrink)
    - EC2 Actions
    - SNS Notifications
    - Can create a billing alarm

Amazon CloudWatch Logs
- CloudWatch Logs collects logs from
    - Elastic Beanstalk
    - ECS
    - AWS Lambda
    - CloudTrail
    - Route53
    - EC2: On-Premises

Amazon EventBridge (CloudWatch Events)

- React to events happening on AWS Services
- Schedule: Cron Jobs
- It can also react to event outside the event bus for example SaaS partners or Outside events

Amazon CloudTrail

- Services which provides compliance, governance & audit for aws account
- It is enabled by Default
- Anything that happens are logged in CloudTrail
- Can push this logs to Amazon S3 or CloudWatch

Amazon X-Ray

- Tracing & visual analysis of your application
- Helps understanding dependencies, tracing, troubleshooting
- Helps to monitor the pacing of the application development progress
- Identify the exception impacts

Amazon CodeGuru

Automated code reviews and recommendations for application performances

2 services

- CodeGuru Reviewer
    - Gives actionables insights if deployed in any repository
    - It supports java & python

- CodeGuru Profiler
    - If deployed then it analysis the expensive line of codes
    - Identify & remove code inefficiency
    - Basically optimize the code

AWS Health Dashboard

- It shows the health of all the services
- It shows the historical information of all the data

VPC (Virtual Private Cloud)

- Public Ip address are random (changes on start or stop & reboot)
- Private IP address are Static (doesn't changes on start or stop & reboot)
- VPC are restricted to regions
- Subnets are the partitions of the vpc
- Public subnet are accessible from internet
- Private subnet aren't accessible from internet
- To define the access between the internet and subnets we use Route Tables
- Internet Gateway helps EC2 instance in public subnet to connect with the internet

- NAT Gateways helps EC2 instance in private subnet to connect with internet while being private

Network ACL & Security Group

- NACL is a firewall which controls traffic at the subnet level
- Can allow and deny rules
- Rules will be only IP Address
- Security groups are the firewalls which are controlling traffic to and from ENI or EC2 Instance
- Security Groups only have allow rules
- It can have IP address or other security groups

VPC Flow Logs

- Log of all the traffic going through your interfaces
- It can be sent to S3, CloudWatch, FireHose

VPC Peering

- Connect 2 VPC privately using AWS network
- IP address should not overlap
- VPC should not be transitive

VPC Endpoints

- Endpoints allows you to connect AWS services using private network instead of public network
- Low latency
- With the help of endpoints we can connect to amazon S3 & DynamoDB
- Use VPC Endpoint interface to connect any other services

AWS PrivateLink

- It is more secure so that a vendor can expose their aws services to more than 1000's of VPC without peering, igw, NAT or route table
- It requires a network load balance & a Elastic Network Interface

AWS TransitGateway

Allows to connect VPC, VPN Connect & Direct Connect Gateway

AWS Web Application Firewall

- Protect your web application from common web exploits (layer 7)
- Layer 7 is HTTP and Layer 4 is TCP
- It is deployed on AWS load balancer, API GateWay & CloudFront

AWS KMS (Key Management Service)

KMS managers encryption of keys for us

CloudHSM

Gives us encryption hardware and we have to manage the encryption keys

AWS ACM (Amazon certificate manager)

- Services to manage SSL & TLS certificates
- Supports for both public & private TLS certificate
- It is free for public TLS certificate

AWS Secret Manager

- New service for managing the secrets
- Capability of force rotating secrets every “X” days
- Secrets are encrypted using KMS
- It is a paid service

AWS Artifact

- It is not really a service
- It provides customers with the documents on the go for amazon compliances and aws agreements
- Artifacts reports include aws iso certificates, payment card industry, system and org control reports
- Artifacts agreements allows you to track and manage the BBA, HIPPA agreements for individuals in a org
- This can also be used for internal audit & compliance purpose

AWS GaurdDuty

- It helps you to do Intelligent Threat discovery to protect aws account
- Its is helpful to protect CryptoCurrency Attacks

Amazon Inspector

Service to run automatic security assessments on aws services

AWS Config

- Helps in auditing and recording compliance of your aws resources
- Helps to record configurations and changes over the time
- Can be store data in amazon S3 and later can be analyzed by athena

Amazon Macie

Fully manage data security and privacy service which uses machine learning to protect your data

AWS Security Hub

- Central security tool for managing the security across various aws accounts and automate security checks
- It integrate the reports of GaurdDuty, Macie, Inspector, IAM Access manager, system manager & partner network solutions
- For security hub to work you should have config enabled

AWS Abuse
If suspected unusual access or unusual activity with resources then you can report to aws abuse team

Amazon Rekognition
- It is used to recognise the text, people, objects, scenes in the images or videos
- It is used for labeling, Content Moderation, Text Detection, Face Detection & analysis

Amazon Transcribe
- Automatically convert speech to text
- It uses deep learning process called as ASR (Automatic Speech Recognition)
- Remove automatically PII information
- Automatically language identification

Amazon Polly
It is opposite of Transcribe

Amazon Translate
- Natural & accurate language translator
- Allows you to localize content

Amazon Lex+ & Connect
- Same technology that powers Alexa
- It understand the intent of the caller by using natural language understanding
- Amazon connect helps to make virtual contact center

Amazon Comprehend
- It is used for NLP
- Fully manager & serverless service
- It is used to find learnings & insights, relationships from the text

Amazon SageMaker
Fully managed service for developers to make machine learning models

Amazon Forecast
Fully managed service to deliver high quality of forecasting based on the ML

Amazon Kendra
- Fully managed document search service by ML
- Extract answers within a document

Amazon Personalize
- Fully manager ml service to built fully personalized app based on personalisation
- Same technology used by amazon.com

Amazon Textract
Used to extract text in writing from any scanned documents

AWS Organisation

- It is a Global Service
- Allows to manage multiple aws accounts
- Main account is master account
- API is available for account creation
- Restrict account privileges

SCP Service control policies

- Allows you to blacklist or allow the IAM policies
- It is not applied to root account

AWS Control Tower

- It is easy to secure & governance multi account aws environments
- It runs on top on organization

AWS service catalog

- It is set of predefined services which a new user can use instead of allowing them all services of aws
- So that the user doesn't do anything non complaint unintentionally

AWS pricing model

- Pay-as-you-go
- Save when you reserve (long term commitments)
- Pay less by using more
- Pay less as AWS Grows

AWS Compute Optimiser

It helps to reduce cost by optimizing the workloads on ec2 instances, ebs volumes & etc

Pricing Calculator

It is used to estimate the cost of the cloud architecture

AWS Cost Explorer

- It is used to visualize and track the cost
- It allow to forecast usage upto 12 months

AWS Budget

- Send alarms when cost exceeds the budget
- Using sns service
- Cost, Reservation, Usage & savings plan

AWS Trusted Advisor

- It is service which gives you high level assessment of your aws account
- And provide recommendation
    - Cost optimisation
    - Performance
    - Security
    - Fault tolerance
    - Service Limits
- 7 core check support plan on basic & developer plan

AWS STS (Security Token Service)

- It allows to create a temporary access keys to the aws services
- You can configure the expiration period

AWS Cognito

It provides identity for your web & mobile applications

AWS IAM Identity center

Single sign in for all your AWS account in organization