

AWS CCP

- * High availability → can be accessed from any type of devices, as long as it has internet connection.
- * Fault tolerant → when a device fails, the data can still be accessed by other devices because it has multiple backups on multiple devices.
- * Scalability → as user base grows, you have the ability to add more servers, quickly and easily.
- * Elasticity → you can grow, as well as shrink servers based on the demand.

* Six advantages of cloud computing:

- ① Trade capital expense for variable expense
- ② Benefit from massive economies of scale
- ③ Stop guessing capacity.
- ④ Increase speed and agility
- ⑤ Stop spending money running and maintaining data centers.
- ⑥ go global in minutes.

* Cloud computing models

- ① IaaS → Infrastructure as a service → provides hardware and software tools → online services that provide high level APIs using the underlying network infra like physical computing resources, location, security, etc → ex: EC2, S3, EBS, EMR, Redshift, etc --
- ② PaaS → Platform as a service → A third-party provider provides hardware and software tools → usually needed for developers. → ex: Elastic Beanstalk → provides a service to send users through a public network
- ③ SaaS → Software as a service → common delivery model for business applications → ex: AWS Marketplace

* Three ways to access AWS web services

- ① AWS Management console
- ② AWS command line interface
- ③ AWS SDK - Software development kit.

- * An AWS Region is a geographical location where one or many AZs reside(s).
- * An AWS Availability Zone (AZs) is a physical location that holds 1 or more AWS data center(s).

- * An AWS data center is where the AWS servers/resources are located and ready to serve the clients.

- * An AWS Edge location helps facilitate a global content delivery network. It serves content from location closest to users.

Analytics Services

- ① Amazon Athena → interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.
→ Athena is serverless, so there is no infra to manage, and you only pay for the queries that you run.
→ Athena is easy to use
→ Simply point to your data in S3, define the schema, and start querying using SQL.
- ② Amazon EMR → provides a managed Hadoop, Apache spark, Flink, etc --- frameworks and that makes it easy, fast and cost-effective to process vast amount of data across dynamically scalable EC2.
→ It interacts with data in other AWS data stores such as S3 and DynamoDB.
→ It is serverless / process and analyze large amounts of data.
- ③ Amazon CloudSearch → managed service in AWS that makes it simple and cost-effective to set up, manage and scale a search solution for your website or application.
→ It supports 34 languages.
- ④ Amazon ElasticSearch → fully managed service that makes it easy to deploy, secure and operate Elasticsearch to search, analyze and visualize data in real-time.
→ It also integrates with Amazon VPC, KMS, Lambda, IAM, cognito, CloudWatch and Kinesis's data firehose.
- ⑤ Amazon Kinesis → makes it easy to collect, process and analyze real-time data.
→ It is cost effective, flexible.
→ With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, IoT, ML, analytics, etc ---
→ Offers 4 services :
a) Amazon Kinesis data firehose
→ reliably load streaming data into data stores and analytics tools.
→ capture / transform / load streaming data into S3, Redshift, Elasticsearch
→ fully managed
b) Amazon Kinesis data analytics
→ analyze streaming data and respond to customer needs in real time.
c) Amazon Kinesis data streams
→ massively scalable and durable real-time data streaming service.
→ capture gigabytes of data per second of hundreds of thousands records.
d) Amazon Kinesis video streams
→ securely stream video from connected devices to AWS for ML / analytics
→ automatically provisions and elastically scales all the infra needed to ingest streaming video data from millions of devices.

- ⑥ Amazon Redshift → fully managed data warehouse
 → fast / scalable / simple / cost-effective to analyze data
 → stores petabytes of data
 → hosts a cluster of nodes that will be used to host the DW.
- ⑦ Amazon QuickSight → fast, cloud-powered BI service
 → create / publish interactive dashboards that can be accessed from browsers or mobile devices.
- ⑧ Amazon Data Pipeline → a web service that helps you move and process data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals.
 → with AWS Data Pipeline, you can regularly access your data where it is stored, transform and process it at scale, and efficiently transfer the results to S3, RDS, DynamoDB and EMR.
- ⑨ Amazon Glue → is a fully managed, extract, transform and load (ETL) service that makes it easy for customers to prepare and load data for analytics.
- ⑩ AWS Lake Formation → sets up a secure data lake in days
 → a data lake is a centralized, secured repo that stores all your data, both in its original form and prepared for analytics.
 → data lake enables you to break down data and combine different types of analytics to gain insights and guide better business decisions.
- ⑪ AWS Managed Streaming for Kafka (MSK) → build and run apps that use Apache Kafka to process streaming data
 → Apache Kafka is an open-source platform for building real-time streaming data pipelines and applications.

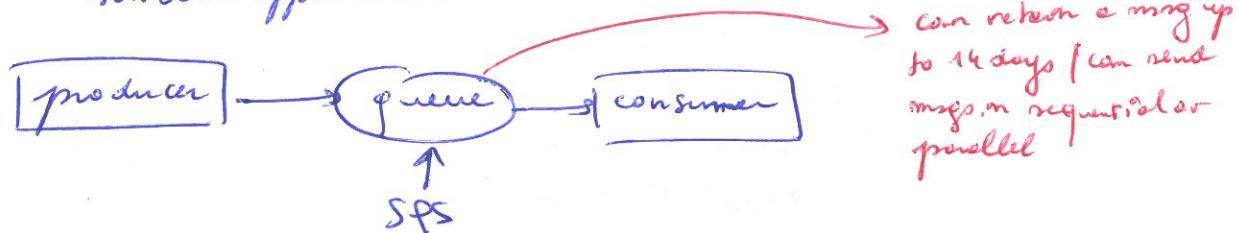
* Application Integration Services

- ① AWS Step Functions → lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.
 → Serverless orchestration for modern applications.
 → orchestration centrally manages a workflow by breaking it into multiple steps, adding flow logic and tracking inputs / outputs. As your application evolves, step functions maintain the application state.
 → Step functions frees your functions and containers from excess code, so your applications are faster to write, more resilient and easier to maintain.
 → Coordinates multiple AWS services such as ECS and Lambda

② Amazon MQ → a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud
→ it reduces your operational load by managing the provisioning, setup and maintenance of ActiveMQ, a popular open source msg broker.

③ Amazon SQS → Amazon Simple Queue Service

→ fully managed message queuing service that enables you to decouple and scale microservices, distributed systems and serverless applications.



→ two types of queues:

- a) Standard queues → offers maximum throughput
- b) FIFO queues

→ workflow:

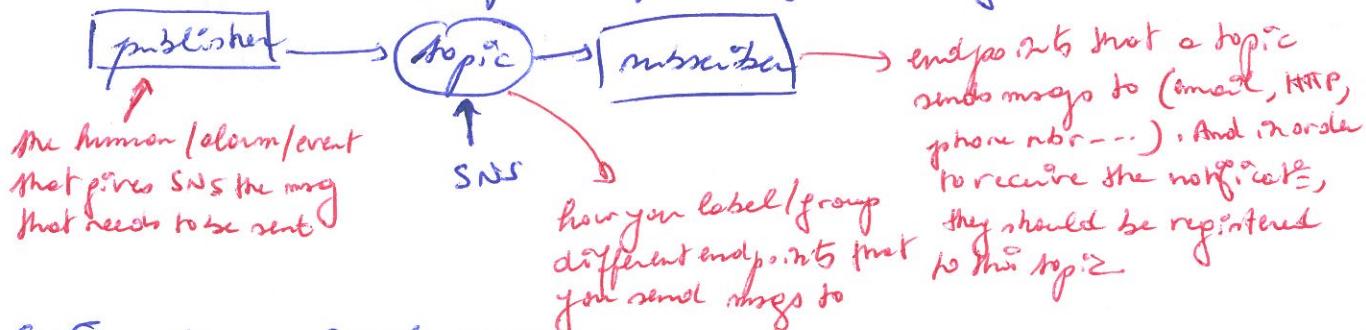
- Step 1: consumer reads a message from the queue (visibility timeout)
- Step 2: consumer processes the message read.
- Step 3: consumer deletes the message from the queue

④ Amazon SNS → Amazon Simple Notification Service

→ highly available, durable, secure, fully managed messaging service that enables you to decouple microservices, distributed systems and serverless apps.

→ Automate the sending of an email (txt msg notification) based on events that happen in AWS account.

→ Using SNS, your publisher systems can fan out msgs to a large # of subscribers for parallel processing, including SQS, Lambda, HTTPS



⑤ Amazon SWF → Amazon Simple Workflow

→ a fully managed state tracker and task coordinator.

→ If your application's steps takes more time than seems to be completed, you need to track the state of processing. If you need to recover or retry if a task fails, Amazon SWF can help you.

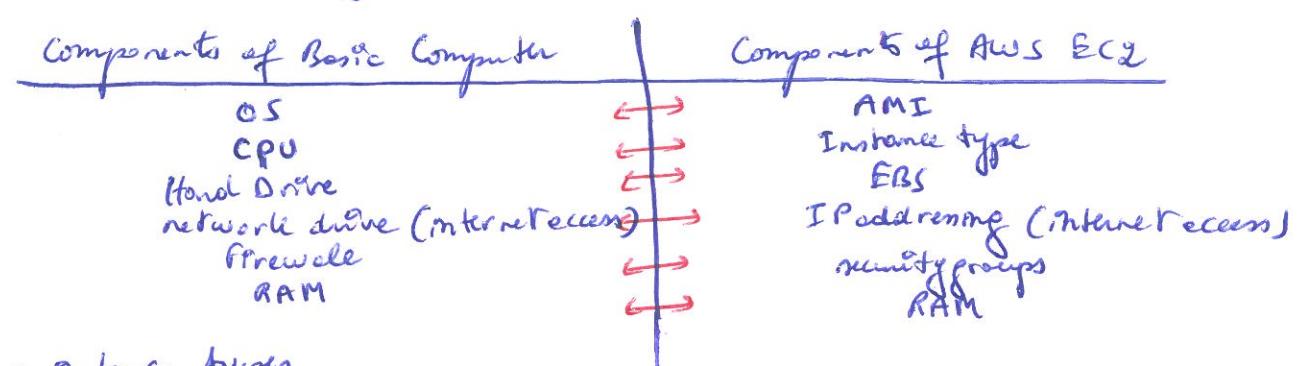
* AWS Cost Management

- ① AWS cost and usage report → a single location for accessing granular data about your AWS costs and usage
→ load these costs / usages into Athena, Redshift, quicksight.
- get lots of AWS usage for each service category by an account / IAM / tags.
- with AWS cost and usage report, you can &
- a) access comprehensive cost / usage information
 - b) track your EC2 RI usage
 - c) leverage strategic data integration using SPL queries
- ② AWS cost explorer → has an easy-to-use interface that lets you visualize, understand and manage your AWS cost and usage over time
→ no granular data
- can be generated or user-defined → cannot load into Athena, Redshift and quicksight
- Cost allocation tags, which is a key/value assigned by a user or by AWS to an AWS resource. It is used to organize resources and track costs on a detailed level.
- (a) → forecast your cost based on previous usage.
- cannot define any threshold, only visualize / understand / manage costs.
- ③ Budgets → set custom budgets that alert you when your costs or usage exceed your budget amount (Budget dashboard)
→ set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define.
→ Reservation alerts are supported by EC2, RDS, Redshift, Elastic Cache and Elasticsearch reservations.
→ Budget alerts can be sent via email or SNS.
- ④ AWS TCO calculator → calculate the total cost of ownership.
→ estimate the migration cost to AWS.
- ⑤ AWS Simple monthly Calculator → estimate per-service bills monthly.
→ use custom common examples.

* AWS Compute Services

① EC2 → a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.

Attached to AZ
(Zonal Service)



→ Instance types

① On demand

- * choose any instance type and provision / terminate at any time
- * most expensive / flexible
- * you pay for the compute capacity per hour/sec with no long-term commitments.
- * unpredictable workloads.

② Reserved (RI)

- * provides a significant discount (up to 75%) compared to on-demand instance
- * purchase for a set period of time (1 to 3 years)

* 4 types :-

a) Standard RI

- * 40% discount for 1 year / 60% discount for 3 years
- * can change AZ, instance type and network type
- * sellable in RI marketplace.

b) Convertible RI

- * 31% discount for 1 year / 54% discount for 3 years
- * can change AZ, instance type, network type
- * can change instance families, OS, tenancy and payment option
- * the exchange should be to an equal or better target.

c) Scheduled RI

- * purchased for 1 year.

* cannot be exchanged.

d) Zonal Standard RI

- * purchased for a specific AZ.

* cannot modify instance family.

③ On Spot

- * Bid on an instance type and only pay/use when the spot price = \leq your bid
- * Amazon sells unused instances for a discount of 90% for a short time
- * When you have an active bid, an instance is provisioned for you & you can use it if the spot price = \leq your bid.
- * It will be terminated automatically if spot price > your bid.
- * charged by minute.

④ Dedicated hosts

- * physical server dedicated to you
- * Appliance with specific compliance requirements

⑤ Savings plans

* RI + more flexibility

②

→ AMI (Amazon Machine Image)

* OS + software packages + settings

* It provides the needed information to launch an instance

* Components 8

- ① root volume template
- ② launch permissions
- ③ EBS

* categories

- ④ Community → free / just es
- ⑤ Market place → pay per use / OS + SP + licenses
- ⑥ My AMI → created by an AWS account

* One AMI can be used to launch multiple EC2 instances. (regional service)

Q6 AMI is considered as a backup for all of your EC2 instances including all of its EBS volumes

→ EBS (Elastic Block store) → storage service

* storage volume for EC2 instances (in the same AZ)

* persists independently from the life of an instance

* EBS volume is automatically replicated within its AZ to protect from component failure, offering high availability and durability.

A7 * EBS and EC2 are tied to AZ, however EC2 instance ID is regional
* EBS is durable, represents block-level storage volumes that you can attach/detach from your instance. (it contains only EC2 data, and not all infra)
* EBS can be used as primary storage device for data that requires frequent and granular updates.

A8 * Be aware that although EBS volumes are considered as local, the EBS snapshots are considered as regional since they are tied to an AZ.

* EBS snapshots are images of EBS used for duplicate/Backups. It is not active and you cannot attach/detach it. To restore a snapshot (make it active), you need to create a new EBS volume for the snapshot image.

* Backup the data on EBS to S3 is feasible by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved, each snapshot contains all of the information that is needed to restore your data to a new EBS volume. (you can run EBS backup while the EC2 instance is running)

* EBS is used for storing data that should be accessed frequently, because it takes into consideration the read/write latencies (same as EFS, DynamoDB, RDS on EC2)

* EBS volume types

a) throughput optimized HDD → provide low cost magnetic storage that defines performance in terms of throughput rather than IOPS. this volume type is a good fit for large sequential workloads such as EMR, ETL, data warehouses and log processing. they are similar to Cold HDD but supports frequently accessed data.

b) Cold HDD → it provides the lowest cost among all options and is suitable for less frequently accessed workloads.

c) Provisioned IOPS SSD → it is used for critical business applications that require sustained IOPS performance (not the most cost-effective)

d) General purpose SSD → it balances price and performance for a wide variety of workloads, but it is not suitable for frequently accessed, throughput-intensive workloads.

Features	SSD (solid state)	HDD (hard disk)
Best for workloads with small and random I/O	large and sequential I/O	
Can be used as a bootable volume	Yes	No
writable use cases	<ul style="list-style-type: none"> - Best for transactional workloads - critical business applications that require sustained IOPS performance - large DB workloads such as MongoDB, Oracle, SQL, ... 	<ul style="list-style-type: none"> - Best for large streaming workloads requiring consistent, fast throughput at low price. - Big data, data warehouses, log processing - throughput-oriented storage for volumes of data that is infrequently accessed.
Cost	moderate / high	low
dominate performance attribute	IOPS	throughput

→ Security groups

* Similar to NACL of VPC in behavior (deny / allow traffic)

* SG acts as a firewall at instance level

NACL // // // // subnet level

* for an instance, you can associate one or more security groups SG.

* by default, for inbound / outbound traffic, everything is denied.

→ IP addressing

* It is the public IP address of an EC2 instance (required for internet communication)

* by default, EC2 has a private IP address that allows it to communicate with other EC2 instances in the same VPC.

→ EC2 instance features/labels

a) instance tags

* tags enable you to categorize your AWS resources in different ways.

* useful when you have many resources, so you can differentiate them.

* assign your own metadata to each resource in the form of tags.

b) instance metadata

* It details the server and network information of the instance itself.

* automatically generated by AWS when you launch an instance.

* To add metadata of your own, use tags.

c) instance user data

* a custom script that you prepare if you want your instance to be initialized every time it is launched.

* cannot add metadata.

d) instance type

* not modifiable and cannot contain user-provided metadata.

* already fixed values provided by AWS.

② EC2 auto scaling

- helps maintain application availability by automatically adding/removing EC2 instances.
- scale up/down EC2 instances based on application traffic.
- Components:
 - a) launch configuration (scaling condition)
 - * this is the EC2 template used when auto-scaling needs to add an additional server to your auto-scaling group.
 - b) Auto Scaling group
 - * these are all the rules/settings that govern when an EC2 server is automatically added/removed. (It uses the EC2 health check and the ELB health check to determine whether the instance is healthy or not)
- Procedure:
 - a) define launch config.
 - b) define auto-scaling group.
 - c) perform the scaling group manually, by schedule, or by metrics.

③ ECS (Elastic Container Service) - EKS (Elastic Kubernetes Service)

- highly scalable, high-performance container orchestration service that supports Docker containers and allows to easily scale containers in AWS.
- Elastic Container Registry (ECR) is a fully managed Docker container registry that makes it easy for developers to store, manage and deploy Docker container images. (Integrated with ECS)
- Elastic Container service for Kubernetes (EKS) makes it easy to deploy, manage and scale containerized applications using Kubernetes on AWS.

④ AWS Lightsail

- easiest way to launch and manage a virtual private server with AWS.
- lightsail plans include everything you need to jumpstart your project (VM, SSD, data transfer, DNS, static IP addresses) for a low predictable price.

⑤ AWS Batch

- Regional service (only on AWS and not on-premises)
- enables developers, scientists and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
- It dynamically provisions the optimal quantity and type of compute resources.

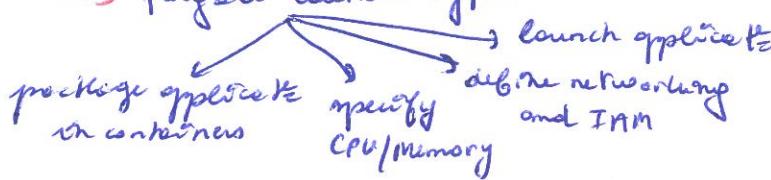
⑥ Elastic Beanstalk

- easy-to-use PaaS for deploying and scaling web apps and services developed with Java, .Net, PHP, Node.js, Python, Ruby, Docker, etc -- on familiar servers such as Apache, Nginx, IIS etc--.
- You can simply upload your code, and Elastic Beanstalk will handle the deployment, from capacity provisioning, load balancing, auto scaling to application health monitoring.
- You retain full control of the AWS resources powering your application.
- Only AWS level, not on-premise.

⑦ AWS fargate

- A compute engine for ECS that allows you to run containers without having to manage servers or clusters. With AWS Fargate, you no longer have to provision, configure, and scale clusters of VMs to run containers.
- Amazon ECS has two modes.

a) fargate launch type



b) EC2 launch type

- have server-level / granular control over before running your containers
- use ECS to manage a cluster of servers and schedule placement of containers on servers.

⑧ AWS Lambda

- Serverless computing that lets you run code without provisioning or managing servers.
- you only pay what you consume, there is no charge when your code is not running.
- supports Node.js, Ruby, C#, Python, etc.
- No access to infre / 3GB memory / 15 min timeout
- AWS Lambda Edge is a feature in CloudFront that lets you run your code closer to your application users, which improves performance and reduce latency.

⑨ AWS serverless application repository

- enables you to quickly deploy code samples, components and complete applications for common use cases such as mobile back-ends, events and data processing, logging, monitoring, IoT, etc. - . Serverless application model
- Each app is packaged with SAM template that defines the AWS resources used

⑩ AWS Outposts

- It brings native AWS services, infra and operating models to virtually any data center or on-premise facility.
- It comes in two variants:
 - a) VMware cloud → use same VMware control plane and APIs, in the cloud.
 - b) AWS native variant → use same APIs and control plane, on-premise.

⑪ VMware cloud on AWS

- Integrated cloud offering developed by VMware and AWS jointly
- highly scalable, secure, innovative service that helps migrate and extend on-premise VMware environments to AWS cloud ECG

VMware based

* Customer Engagement Services

- ① Amazon Connect → self-service, cloud-based contact center service that makes it easy for any business to deliver better customer service at low cost
- ② Amazon SES
→ cloud-based email sending service designed to help digital marketers and application developers send marketing, notification and transactional emails.

SNS	Via	SES
<ul style="list-style-type: none">- send notifications to subscribers of topics via multiple protocol like HTTP, email, SQS, SMS.- SNS is generally used for sending plain text emails which is triggered via other AWS services (ex: billing alarm)- A lot of AWS services can trigger SNS for notifications.		<ul style="list-style-type: none">- a cloud-based email (ex: SendGrid)- SES sends <u>HTML emails</u>, SNS cannot.- SES can receive inbound emails.- SES can create Email templates.- Custom domain name email.- Monitor your email reputation.

* Database services

→ Overview

Relational Database

- ① SQL
- ② RDS
- ③ Includes: Amazon Aurora, MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL
- ④ definition?
Web service that makes it easy to operate and scale a relational DB in the cloud. It is cost-efficient, resizable and manageable DB admin tools.
- ⑤ Structure?
* table format (vertical)
* columns and rows data
* used for any structured data such as contact list

Non-Relational database

- ① NoSQL
- ② DynamoDB
- ③ Can replace: MongoDB, Oracle NoSQL, CassandraDB.
- ④ definition?
fast and flexible NoSQL DB service that provides consistency and milliseconds latency to any application. It is flexible and make good fit for growing, IoT, -- applications.
- ⑤ Structure?
* json format (horizontal)
* json format data like name-value documents
* used for non-structured data such as cataloging documents

① Amazon Aurora

- MySQL and PostgreSQL compatible relational DB engine that combines the speed and availability of high-end commercial database with the simplicity and cost-effectiveness of open source databases.
- five times faster than MySQL and 3 times faster than PostgreSQL.
- fully managed RDS that automates time-consuming admin tasks.
- features:
 - a) distributed
 - b) fault-tolerant
 - c) self-healing
 - d) auto-scales up to 64 TB per database instance
 - e) high performance and availability with up to 15 low-latency read replicas
 - f) point-in-time recovery
 - g) continuous backup to S3.
 - h) replicates across 3 AZs.
- Aurora severless only runs when you need it (like Lambda)
- Aurora backttrack is a feature in Amazon Aurora that allows to restore a DB cluster at a time without restoring data from backups.

② Amazon RDS

- is a managed service that makes it easy to set up, operate and scale a relational database in the cloud. (time-consuming admin tasks)
- cost efficient / resizable capacity
- available on several DB instance types like Aurora, MySQL, Oracle, etc ---
- you can use AWS Data Migration service to easily migrate or replicate your existing databases to Amazon RDS.
- does not automatically scale / not fully managed
- RDS on VMware lets you deploy managed databases in on-premises VMware environments using RDS technology.

③ DynamoDB

- NoSQL Key/Value DB and document DB that delivers single-digit millisecond performance at any scale.
- fully managed / multi-region
- can handle more than 10 trillion requests per day / peaks more than 20 million requests per second
- Amazon DynamoDB Accelerator (DAX) is a caching feature only applicable for dynamoDB (NoSQL)

④ Document DB

- NoSQL document DB compatible with MongoDB.
- fully managed

⑤ Amazon ElastiCache

- a fully managed web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud.
- high throughput and low latency in-memory data stores
- improves application performance
- supports two open source in-memory caching engines:
 - a) Redis
 - b) Memcached

⑥ Amazon Neptune

- fast, reliable, fully managed graph database service that makes it easy to build and run applications that work with highly connected datasets.
- highly available with read replicas / point-in-time recovery / continuous backup to S3 / replication over AWS.

⑦ Amazon Quantum Ledger Database (QLDB)

- fully managed ledger DB that provides a transparent, immutable and cryptographically verifiable transaction log owned by a CA.
- QLDB tracks each and every application state change and maintains a complete and verifiable history of changes over time.

⑧ Amazon Pinpoint

- fast, scalable, fully managed time series database service for IoT and operational applications that makes it easy to store and analyze billions of events per day.

* Desktop and App streaming

① Amazon WorkSpaces

- is a fully managed DaaS solution in AWS which allows you to provision Windows / Linux desktop in few minutes and quickly scale to provide thousands of desktops across the globe
- cheaper than VDI.

② Amazon AppStream 2.0

- fully managed application streaming service which you can use to centrally manage your desktop applications on AppStream 2.0 and securely deliver them to your desktop.

8 Developer Tools

① AWS CodeCommit

- a fully managed source control service that makes it easy for companies to host secure and highly scalable private ~~git~~ repositories.
- It eliminates the need to operate your own source control or worry about scaling your infrastructure.
- It securely stores anything from source code to binaries, and work seamlessly with your existing ~~git~~ tools.
- It helps collaborate with colleagues via pull requests, branching and merging.

② AWS CodeBuild

- is a fully managed build service that compiles source code, run tests and produces software packages ready to be deployed.
- It scales continuously and processes multiple builds concurrently.

③ AWS CodeDeploy

- is used to automate code deployments to any instance including EC2 and on-premises, ECS, Lambda.
- helps you avoid downtime / handle complexity.

④ AWS CodePipeline

- is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.

⑤ AWS CodeStar

- enables you to quickly develop, build and deploy applications in AWS.
- provides a unified user interface, enabling to easily manage your software development activities in one place.
- you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing your code faster.

⑥ Amazon Corretto

- no-cost, multiplatform, production-ready distribution of the Open JDK.
- Corretto is certified as compatible with Java SE standard.

⑦ AWS Cloud9

- cloud-based integrated development environment (IDE) that lets you write, run and debug your code with just a browser.
- It includes a code editor/debugger/terminal and supports Python, Ruby, JS, PHP, ...
- works with Lambda as well.

⑧ AWS X-Ray

- helps developers analyze and debug distributed applications in dev/prod.
- collects data about your app requests and provide in-line service map and average time spent for each request.
- you can use it with Lambda, but you have to enable it.
- by default, in Lambda, the invocation time is sent to X-Ray.

* Management and Governance Services

① AWS CloudWatch

- A monitoring and a management service (considered as a metrics repo)
- It monitors your applications, understand and respond to performance changes, optimize resource utilization and get a unified view of operational health.
- It collects monitoring and operational data in form of logs /metrics /events.
- CloudWatch is a collection of services:

a) CloudWatch logs - enables you to centralize your logs

* you can use logs to monitor /store /access log files from EC2, Route53 and cloud trail

* log retention

* archive log data

b) CloudWatch metrics - ex of memory usage

c) CloudWatch events - trigger an event based on a condition (ex take a snapshot

d) CloudWatch dashboards - create visualization based on metrics. of the server each hour

e) CloudWatch alarms - trigger notifications based on metrics

* can stop / terminate / reboot / resure EC2 instances

* can send notifications to the resources monitored based on rules you define

triggers SNS

EC2 / S3 / Billing

thresholds

② AWS Auto Scaling

- Monitors your applications and automatically adjusts capacity to maintain steady predictable performance at the lowest cost possible.
- Enables you to configure automatic auto-scaling for the AWS resources that are part of the application, in a minute.
- It provides a simple, powerful user interface that lets you build scaling plan for AWS resources, including EC2, ECS, DynamoDB indexes and tables, Amazon Aurora replicas.

③ AWS Control Tower

- automates the set-up of a baseline environment, or landing zone, that is secure, well-architected multi-account AWS environment.
- is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
- enables you to assess/audit/evaluate the configurations of your AWS resources.
- does not provide event history like CloudTrail
- with AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance, and dive into configuration details of a resource

⑤ AWS System Manager

- gives you the visibility and control of your infrastructure on AWS.
- provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.
- With System Manager, you can group resources like EC2, S3, or RDS, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.
- Tools &

a) Resource groups

b) Insight dashboard

* displays operational data for each resource group

* View API logs from AWS CloudTrail, and config changes from AWS Config

* Integrate with AWS CloudWatch dashboards

* " " " Personal health dashboard

* " " " Trusted advisor notifications

c) Run command → execute custom tools

d) State Manager → maintain consistent OS config (ex: firewall settings)

e) Inventory → collect/query config and inventory information

f) Maintenance window → run custom/maintenance tasks across resources

g) Patch Manager → select and deploy OS/patches automatically across resources

i) Parameter Store → provide encrypted location to store important admin info

j) Distribution → such as passwords (integrated with AWS KMS)

k) Session Manager → helps securely distribute and install software packages

* Browser based UI to manage controls/launch EC2 instances.

* IAM policies for administrative access.

⑥ CloudFormation

- gives developers and sys admins an easy way to create and manage a collection of related AWS resources, provisioning and updating them orderly and predictably
- create template to describe your AWS resources
- spin up infrastructure on AWS as template.
- control AWS infra by code.



→ you can use the same template to deploy multiple stacks.

* good / Yaml format

* has the resources + parameters + values needed

* has the output that can be stored for reuse

⑦ AWS CloudTrail

- is a web service used for governance / compliance / auditing of your account
- it records AWS API calls for your account and delivers log files to you.
- actions are taken from the console, CLI, API and SDK, and recorded.
- the recorded info includes the identity of the API caller, the time of the API call, the source IP of the API caller, the request parameters and the response.
- automatically created when the AWS account is created
- * event history
- * events are retained for 90 days
- * create a trail that can send events to S3 bucket for example.

⑧ AWS OpsWork

- is a configuration management service that helps customers configure and automate servers / applications, both on-premises and in the cloud.
- provides managed instances of Chef, puppet and Ansible that are automation platforms.

⑨ AWS Service Catalog

- allows organizations to create and manage catalogs of IT services approved for use on AWS.

⑩ AWS Trusted Advisor

- an online tool that provides real-time guidance to help provision resources following AWS best practices. (does not generate any PDF report)
 - a) cost optimization
 - b) security
 - c) performance
 - d) service limits
 - e) fault tolerance

⑪ Personal Health Dashboard

- provides alerts and remediation guidance when AWS is experiencing events that might affect you.
- while the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you personalized view into the performance and availability of the AWS services underlying your AWS resources.

⑫ AWS Managed Services

- provides ongoing management of your AWS infra so you can focus on your applications.
- helps reduce operational overhead and risk
- automates common activities such as CRs, monitoring, patch management, security, etc.

⑬ AWS console Mobile application

- View / manage a set of resources to support incident response
- monitor resources through the dedicated dashboard and view config. details, metrics and alarms for selected AWS services .

⑭ AWS License Manager

- manage licenses on AWS and on-premises servers from vendors like AWS, Oracle, IBM, etc --
- It lets admins create custom license rules , and then enforce them when an EC2 instance gets launched.

⑮ AWS well-architected tool

- helps review the state of your workloads and compares them to the latest AWS architectural best practices .
- It is based on the AWS well-architected framework , of which the below pillars :
 - a) operational excellence
 - b) security
 - c) reliability
 - d) performance efficiency
 - e) cost optimization

Media Services

① Amazon Elastic Transcoder

- ~~It is a media transcoding in the cloud that is designed to be a highly-scalable, easy-to-use, and cost-effective way for developers and businesses to convert/transcode media files from their source format into versions that will play back on devices like PCs, smartphones and tablets .~~

② AWS Elemental Media Connect

- ~~is a high-quality transport service for live video .~~
- ~~It enables you to build mission-critical live video workflows in the fraction of the time and cost of satellite or fiber services.~~

③ AWS Elemental Media Convert

- ~~is a file-based video transcoding service~~
- ~~Creates video-on-demand content for broadcast and multi-screen delivery & scale~~
- ~~Combines advanced video and audio capabilities with a simple web services interface~~

④ AWS Elemental MediaLive

- ~~is a broadcast live video processing service .~~
- ~~It lets you create high quality video streams for delivery to broadcast television and internet-connected multi-screen devices like connected TVs, tablets, smartphones, --.~~
- ~~The service works by encoding your live video-streams in real-time, taking a longer-sized live video source and compressing it into smaller versions for distribution to your viewers~~

- ⑤ AWS Elemental Media Package
→ it reliably prepares and protects your video for delivery over the internet
- ⑥ AWS Elemental Media Store
→ is an AWS storage service optimized for media.
→ it gives you the performance, consistency and low latency required to deliver live streaming video content.
- ⑦ AWS Elemental Media Player
→ lets video providers insert individually targeted advertising into their video streams without sacrificing broadcast-level quality-of-service.
- ### * Migration and Transfer Services
- ① AWS Migration Hub
→ provides a single location to track the progress of application migrations across multiple AWS and partner solutions.
→ it allows you to choose the AWS and partner migration tools that best fit your needs, while providing visibility into the status of migrations.
- ② AWS Application Discovery Service
→ it helps enterprise customers plan migration projects by gathering information about their on-premises data center.
→ it collects and presents config, usage and behavior data from your servers to help you better understand your workloads.
→ the collected data is returned in encrypted format in an AWS ADS data store.
→ you can export this data as CSV and use it in TCO, or plan your AWS migration.
- ③ AWS Database Migration Service
→ it helps migrate databases to AWS quickly and securely.
→ the source DB remains operational during the migration (minimizing downtime).
→ it supports homogenous migration such as Oracle to Oracle and heterogeneous migration such as Oracle/Microsoft SQL to Amazon Aurora.
→ it allows you to stream data into Amazon Redshift from Aurora, PostgreSQL, Oracle, ...
→ you can continuously replicate your data with high availability.
- ④ AWS Server Migration Service
→ it is an agentless service that makes it easier and faster for you to migrate thousands of on-premise workloads to AWS.
→ Not appropriate for migrating on-premises DBs.
- ⑤ AWS Schema Conversion Tool (SCT)
→ makes heterogeneous DB migration predictable by automatically converting the source DB schema and the majority of the DB code objects (views, functions, stored procedures) to a format compatible with the target DB. Any object that cannot be automatically converted will be marked to be done manually.
→ Once schema conversion is completed, SCT can help migrate data from a range of data warehouses to Amazon Redshift.
↳ Basically SCT migrate from one engine to another.
↳ e.g. PostgreSQL to MySQL or Oracle data warehouse to Amazon Redshift.

⑥ AWS SnowBall

- is a petabyte-scale data transport solution that uses secure appliances to transfer large amount of data into and out of AWS.
- the client will encrypt and transfer the files to the appliance at high speed.
- you can track the job status using Amazon SNS, text messages, or console.

⑦ → AWS SnowBall edge

is a data migration and edge computing device that comes in two options

a) Storage optimized

- * provides 100 TB of capacity
- * 24 vCPUs
- * well suited for local storage
- * well suited for large scale data transfer

b) Compute optimized

- * 52 vCPUs
- * optional GPU for ML and video analysis
- * block/object storage

=) AWS SnowBall edge supports specific EC2 instance types as well as Lambda, so customers may develop, test and then deploy applications on devices in remote locations to collect, process and return the data.

⑧ AWS SnowMobile

- is an exabyte-scale data transfer service used to move extremely large amounts of data to AWS. (transfer up to 100 PB per SnowMobile)
- it uses multiple layers of security designed to protect your data including dedicated security personnel, GPS tracking, alarm monitoring, 24/7 video surveillance.
- All data is encrypted with 256-bit encryption keys managed through AWS KMS and designed to ensure both security and full chain of custody of your data.

⑨ AWS DataSync

- a data transfer service that makes it easy for you to automate moving data between on-premises storage and Amazon S3 or EFS.
- it automatically handles many of the tasks related to data transfer including running instances, handling encryption, network optimization, etc --.
- You can use it to transfer data at speeds up to 10 times faster than open-source tools.

⑩ AWS Transfer for SFTP

- fully managed service that enables the transfer of files directly into and out of AWS S3 using SFTP, also known as S3FTT.

⑪ AWS Transfer Accelerator

- uses AWS edge locators in order to migrate smaller amount of data such as gigabytes or terabytes into AWS.

AWS Mobile Services

① AWS Amplify

- makes it easy to create, configure and implement scalable mobile applications powered by AWS.
- it seamlessly provisions and manages your mobile backend and provides a simple framework to easily integrate your backend with your iOS, Android, --

② Amazon Cognito

- lets you add user sign up, sign in, and access control to your web/mobile apps quickly and easily. authentication authorization
- you can authenticate users through social media identity providers like facebook, twitter, --.
- identity pools / user pools

③ Amazon Pinpoint

- makes it easy to send targeted messages to your customers through multiple engagement channels.
- email, SMS, push notifications
- promotional alerts, transactional messages, customer retention campaigns.

④ AWS Device Farm

- it is an app testing service that lets you test and interact with your android, iOS and web apps on many devices at once, or reproduce issues on a device in real-time.

⑤ AWS AppSync

- Serverless backend for mobile, web and enterprise applications.
- it makes it easy to build data driven mobile and web applications by handling nearly all the application data management.
- it uses GraphQL

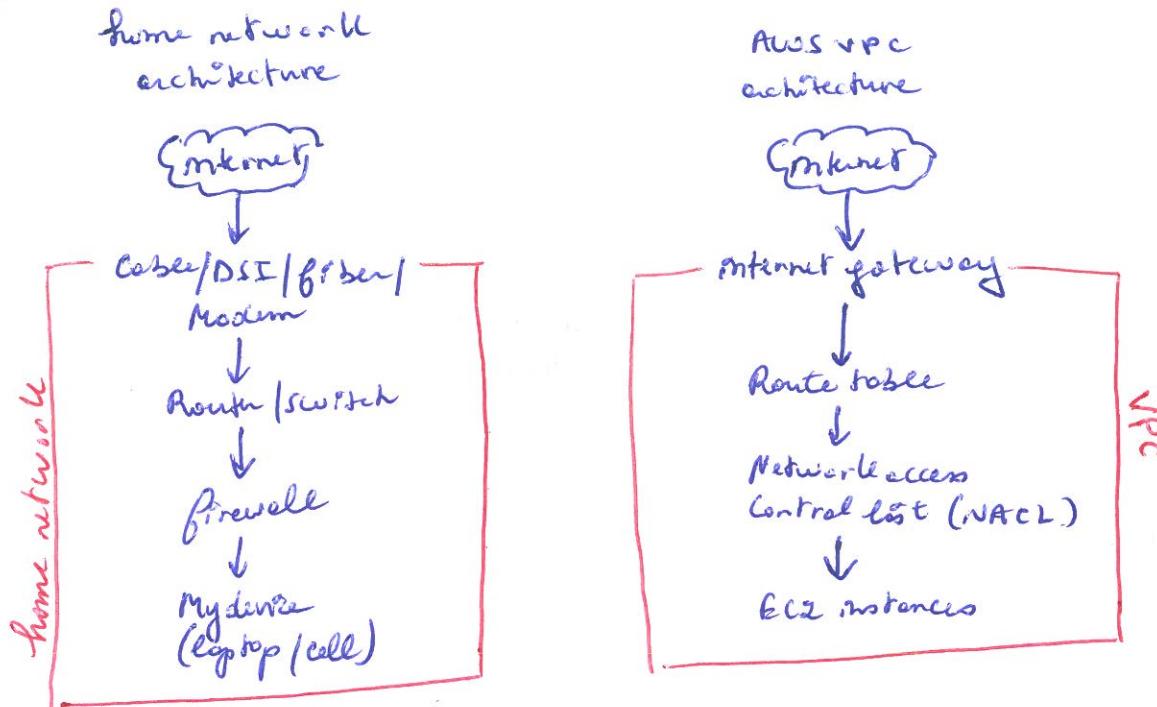
AWS Shared Responsibility Model

- customer is responsible for the security on the cloud
- AWS is responsible for the security off the cloud

Responsibilities	Customer	AWS	Both
Controls	<ul style="list-style-type: none"> - customer data - platform, app, IAM, - OS / network / firewall configuration - client / server side data encryption and firewall protection <p>- route and communications protection or zone security (e.g. customer should route, zone data securely)</p>	<ul style="list-style-type: none"> - Compute - Storage - Database - Networking - AWS Global Infra <p>AWS Regions AWS Edge Locations</p>	<ul style="list-style-type: none"> - patch mgmt - config mgmt - Awareness and Threat hunting

& Networking and Content Delivery

① Amazon VPC (virtual private cloud)



→ Route table

- * set of rules used to determine the direction of the network traffic.
- * the default VPC has already a main route table
- * once we access through the internet gateway and we are inside the VPC, we need something to tell the data where to go. It is the route table.
- * the route table provides the connection between various resources (like EC2) inside VPC
- * In a VPC, you can have multiple active route tables.
- * In a VPC, you cannot delete a route table that has dependencies (associated subnets)

→ Network access control list (NACL)

- * optional layer of security that acts as a firewall for controlling traffic in and out of one or more subnets.
- * the default VPC has an NACL and is associated with the default subnet.
- * when traffic goes through the internet, internet gateway then route table, it will hit the NACL before reaching EC2.
- * NACL has inbound/outbound rules (for the default NACL, all traffic is allowed)
 - evaluation based on the rule # from lowest to highest
 - the first rule evaluated that applies to the traffic type will be immediately applied/rejected, regardless of the rule that comes after.
- * when you create an NACL, all the traffic is initially denied.
- * a subnet can only be associated with one NACL at a time.
- * An NACL allows/denies traffic from entering a subnet. But once traffic is inside the subnet, the AWS resource (like EC2) may have additional security layer such as security groups
 - subnet level
 - you create allow/deny rules
 - instance level
 - you create allow rules

→ Elastic Network interface

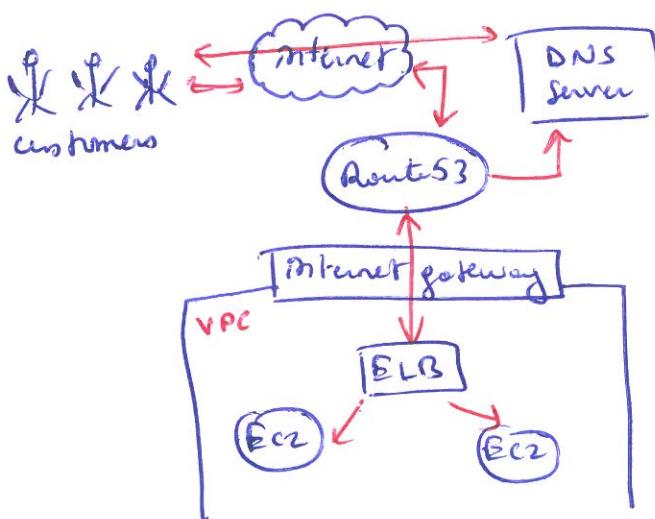
- * a logical networking component in VPC that represents a virtual network card.

- ② Amazon Cloudfront
- is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and higher transfer speeds.
 - Cloudfront is integrated with both physical servers (AWS global infra) and other AWS services.
 - Cloudfront is a global service and you can distribute it in front of your EC2 instances in order to make your application, that resides in a specific location, responsive in the same ideal time for all users in different locations.
 - Cloudfront can be directly connected to EC2 / S3 / ELB / Lambda Edge.
 - Cloudfront works seamlessly with AWS Shield.
 - when you deploy a Cloudfront distribution, it creates a cached copy of your website and copies to servers located near people trying to access it. Which means you are connecting your EC2 into edge locations.
- has a cache

③ Route53

- is a highly available and scalable Domain Name System (DNS) web service.
- it is designed to give developers a reliable and cost-effective way to route end-users to internet applications by translating human readable names, such as `www.example.com` to IP addresses, that computers use to connect to each other.
- Route53 effectively connects end-users requests to EC2 / ELB / S3 or outside AWS.
- it is a global service.
- three main functions.
 - a) domain registration
 - b) DNS service
 - c) health checking
- A DNS Server is a database of website domains and their corresponding IP addresses.

- five routing policy types
 - a) simple
 - b) fail over
 - c) geolocation
 - d) weighted
 - e) latency



→ when you register a domain using route53, we need to send this information to the DNS server so that it has the domain name as well as the corresponding IP address. So when a customer types the website needed, the request across the internet will be forwarded to the DNS server. The latter is going to send back the IP address. The user will go through the internet then, down to route53 into the internet gateway, and the IP address given to the DNS server will then be the IP of the ELB which will distribute the traffic between EC2.

- Amazon route53 can help create a hybrid architecture using Amazon route53 Resolver which provides recursive DNS for AWS vPC and on-premises network over AWS direct connect or AWS managed VPN.

④ Elastic load balancer (ELB)

→ AWS ELB distributes automatically incoming traffic across multiple targets such as EC2, ECS, Lambda, IP endpoints, etc --- and across one or more AZs

→ three types

a) Application load balancer

* Best suited for HTTP / HTTPS load balancing

* advanced request routing at the delivery of modern technologies like containers and microservices.

* traffic is routed to targets within the VPC based on the request context.

* performs at layer 7 (request level)

* Support path-based routing, host-based routing, websockets and

containerized applications.

b) Network load balancer

* Best suited for TCP / UDP / TLS load balancing

* performs at layer 4 (connection level)

* handles millions of requests per second

* handles sudden and volatile traffic

c) Classic load balancing

* Basic load balancing across EC2

* performs at layer 4 and 7

* intended for applications built within EC2 classic network.

(fiber option)

⑤ AWS Direct Connect

→ is a cloud service solution that makes it easy to establish a dedicated network connection (not through internet) from your on-premises data center to AWS.

⑥ AWS PrivateLink

→ simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public internet.

→ provides private connectivity between VPCs, AWS services and on-premises applications securely on the Amazon network.

⑦ AWS API gateway

→ a fully managed service for testing, publishing, maintaining, monitoring and securing APIs at any scale.

⑧ AWS transit gateway

→ a service that enables customers to connect their VPCs and on-premises networks to a single gateway

⑨ AWS global accelerator

→ a networking service that improves availability and performance of your application

→ uses the highly available congestion free AWS network to direct internet traffic from users to your application on AWS making it a better user experience.

⑩ AWS App Mesh

→ makes it easy to monitor and control microservices running on AWS.

→ you can use it with ECS and EKS as it uses open source Envoy proxy.

⑪ AWS Cloud Map

→ resource discovery service

→ with Cloud Map, you can define custom names for your application resources, and it maintains the updated locate of these dynamically changing resources.

→ increases availability.

⑫ AWS VPN

- lets you establish a secure and private tunnel from your network (device) to AWS global network.
- a) Site-to-site VPN → securely connect on-premises network site to VPC.
- b) AWS client VPN → securely connect users to AWS or on-premises networks.

⑬ Amazon VPC VPN connection

- can link your data center (network) to your VPC on AWS. There are two sides of the connection &
- a) customer gateway (customer side)
- b) VPNGate private gateway (AWS side)

⑭ NAT gateway

- enables EC2 instances in a private subnet to connect to the Internet or other AWS services, but prevent the internet to initiate a connection with them.

⑮ Egress-only Internet gateway

- same as NAT gateway, but for IPv6 traffic only.

⑯ VPC peering

- a networking connection between VPCs only.

⑰ VPN connection / AWS VPN cloud hub

- internet based connection (slow traffic between on-premises and AWS)

• Security, Identity and compliance Services

① AWS Security Hub

- it is a single place that aggregates, organizes and prioritizes your security alerts, from AWS services such as Amazon GuardDuty, Inspector, Macie, as well as Partner Solutions.

② AWS Cloud Directory

- enables you to build flexible, cloud-native directories for organizing hierarchies of data along multiple dimensions.
- fully managed, eliminates time-consuming schema tasks

③ AWS Directory Service

- provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory with other AWS services

④ AWS Cloud HSM

- a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS cloud.

⑤ AWS Certificate Manager

- lets you easily provision, manage and deploy public / private SSL/TLS certificates for AWS usage.

- It does not store any certificate or compliance related document

⑥ AWS IAM (Identity access management)

- enables you to securely control access to AWS services and resources for your users.
- In order to access AWS resources and services, a user should be assigned a certain policy, because by default he has no permissions to access anything (we call it attach a policy)
- a policy cannot be full access, read only, write only, etc --
- If we want to attach a certain policy to multiple users, we create a group, attach a policy to it and then add users to it.
- Because only policies are assigned to users/groups, if we want to grant an AWS service (like EC2) access to another service (like S3), we need to attach a role to EC2 and then a policy to this role, in order to access S3 with the necessary permissions.
- The role gives permissions to AWS services to almost act like a user.
- IAM is a global service with the below characteristics:
 - a) a group can contain many users, and users can belong to multiple groups
 - b) there is a limit to the nb of groups you can belong as a user, and to how many groups there is in nb.
 - c) groups can't be nested; they can contain only users, not groups
 - d) There is no default group that automatically includes all AWS users. If you want to have a group like that, you need to create it and then add all users to it.
- IAM Best practices:
 - a) lock away your AWS account root user access keys.
 - b) do not share access keys
 - c) create individual IAM users
 - d) use groups to assign permissions to IAM users
 - e) grant least privilege
 - f) use access levels to review IAM permissions
 - g) use roles to delegate permissions
 - h) use roles for applications that run on EC2
 - i) use permissions with AWS Managed policies
 - j) use customer Managed policies instead of inline policies.
 - k) enable MFA
 - l) Configure strong password policies for users.
 - m) rotate credentials regularly / remove unused credentials
 - n) use policy conditions for extra security
 - o) Monitor activity in your AWS account.
- IAM policy simulator
 - enables you to test and troubleshoot IAM and resource-based policies.
 - testing policies to AWS resources includes S3 buckets, SES queues, SNS topics, S3 glacier vaults

⑦ Penetration tests

- permitted services for security assessment and penetrate tests without approvals against AWS infrastructure
 - * EC2, NAT gateways, ELB
 - * RDS
 - * Cloudfront
 - * Aurora
 - * API gateways
 - * Lambda
 - * Lambda edge functions
 - * Lightsail
 - * Elastic Beanstalk
- prohibited services
 - * DNS zone walking via route 53 hosted zones
 - * DDOS, DDoS, SDDoS, SDDoS
 - * Port flooding
 - * Protocol flooding
 - * Request flooding (login, API, --)

⑧ Amazon GuardDuty

- A threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.
- intelligent and cost-effective
- uses ML, anomaly detection, and integrated threat intelligence
- Analyzes tons of billions of AWS events across data sources like AWS CloudTrail, VPC flow logs and DNS logs
- Can be integrated with AWS CloudWatch.

⑨ Amazon Inspector

- an automated security assessment service that helps improve security and compliance of applications deployed on AWS EC2.
- It automatically assesses applications for exposure, vulnerabilities and deviations
- generates a PDF report telling you which security checks passed
- an audit tool for security of EC2 instances.

⑩ AWS Artifact

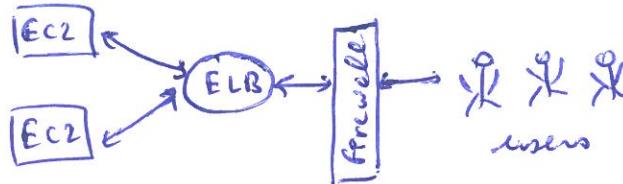
- a central resource for compliance-related information.
- generates a security report based on global compliance frameworks such as SOC, PCI etc --
- submit docs to auditors in order to prove security and compliance of your app.

⑪ Amazon Macie

- a security service that uses ML to automatically discover, classify and protect sensitive data on AWS (like personally identifiable information 'PII')
- a fully managed service that continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized or risks in data
- Can be integrated with AWS CloudWatch.
- Macie is capable to protect data in S3.

⑫ AWS Firewall Manager
→ a security management service that makes it easier to centrally configure and manage AWS WAF rules across your accounts and applications.

⑬ AWS CloudFront
→ web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.



- Integration with ELB, CloudFront or API gateway.
- Create web access control lists in order to filter traffic ~~http requests~~
- Block users to stop traffic from including IP addresses / request header values.
- Use a ruleset from a trusted AWS security partner in the AWS WAF rules marketplace

→ protect web application from 10 most dangerous attacks :

- a) injection
- b) broken authentication
- c) sensitive data exposure
- d) XML External Entities (XXE)
- e) broken access control
- f) security misconfigurations
- g) cross-site scripting (XSS)
- h) insecure Deserialization
- i) using components with known vulnerabilities
- j) insufficient logging and monitoring

⑭ AWS Shield
→ a managed distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS.

→ a DDoS attack is a malicious attempt to disrupt normal traffic by flooding a website a large amount of fake traffic.

→ All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.

→ two tiers of AWS shield :

- a) Standard → protects you against layer 3 (network), 4 (transport) and 7 (application) attacks
 - protection against most common DDoS attacks and access to tools and best practices to build a DDoS resilient architecture.
- b) Advanced → 3000 USD/year
 - for additional protection against larger and more sophisticated attacks, visibility into attacks, and 24x7 access to DDoS experts for complex cases
 - available on : route 53, cloudfront, ELB, AWS global accelerator, Elastic IP.

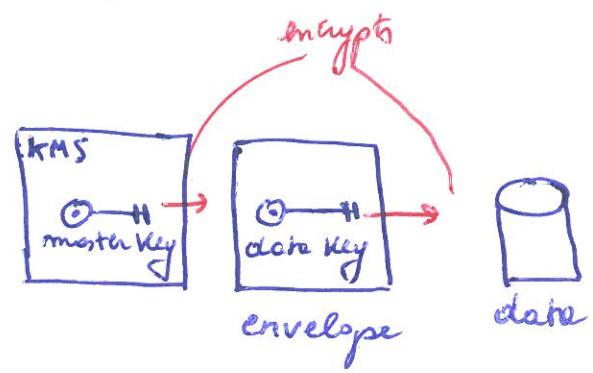
⑮ AWS Key Management Service (KMS)
→ makes it easy to create and manage keys and control the use of encryption across a wide range of AWS services and in your application.

→ it is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

→ KMS is a multi-tenant HSM (Hardware Security Module)

→ KMS uses Envelope Encryption

When you encrypt your data, it is protected, but you have to protect your encryption keys. When you encrypt your data key with a master key, it is an additional layer of security.



16 AWS Organizations

→ policy-based management for multiple AWS accounts

→ easy tracking for the combined costs of all of your AWS accounts (consolidated bills)

→ Share volume pricing and RI discounts by combining usage of all accounts.

→ No granular data

→ Create service control policies (SCP) that centrally control AWS service use across multiple AWS accounts.

17 AWS Secret Manager

→ helps you protect secrets needed to access your applications, services and IT resources

→ enables you to easily rotate, manage and retrieve DB credentials, API Keys and other secrets throughout their lifecycle

→ integrates with RDS for MySQL, PostgreSQL and Aurora

18 AWS Single Sign-On (SSO)

→ a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

→ manage SSO access and user permissions to all of your accounts in AWS organizations

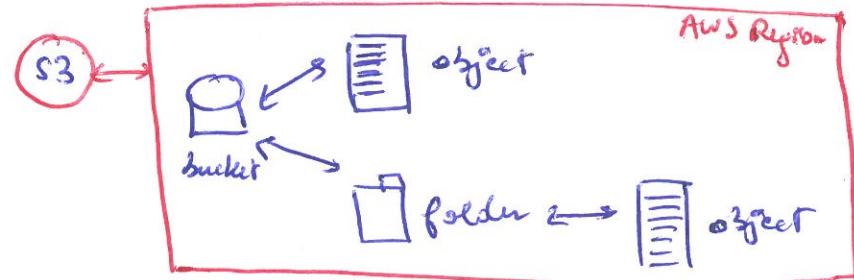
* Storage Services

① Amazon Simple Storage Service S3

- object storage service that offers industry-leading scalability, durability, security, and performance
- store/retrieve any amount of data, at anytime from anywhere on the web
- Buckets are root level folders you create in S3.
- objects are files stored in the bucket
- When you create a bucket, you choose the specific region in which this bucket will reside physically.

→ you get charged for
a) Storage cost

- storage class
- date at rest
- per GB



b) Request pricing → put, copy, post
list, get, data retrieval,
data archive, data restore.

→ Bucket names

- must be unique across all AWS
- 3-15 length 563 characters
- contains only lowercase, numbers and hyphens
- must not be formatted as IP addresses.

→ Storage class

* Represents the classification assigned to each object in S3
* Each storage class has attributes that dictate things like

- Storage cost
- Object durability
- Object availability
- Frequency of access

* Each object must be assigned to a storage class.

* You can change the storage class at anytime (for the most parts)

* Classes are 6

a) Standard

- * default storage, designed for all purpose general storage.
- * 99.999999999% object durability (99.999999999%)
- * 99.99% object availability.
- * the most expensive.

b) Reduced Redundancy Storage (RRS)

- * designed for non-critical reproducible objects
- * 99.99% object durability
- * 99.99% object availability
- * less expensive than the standard

c) Infrequent Access (S3-IA)

- * designed for objects that you do not access frequently, but must be immediately accessed
- * eleven nines for object durability and availability for 99.99%
- * less expensive than standard and RRS.

d) Glacier

- * a secure, durable and extremely low-cost storage service for date archiving and long-term backup.
- * eleven durability
- * you can store data for as little as 0.004 \$ per gigabyte per month
- * it provides 3 options for access to archives, from few minutes to several hours.
- * Glacier deep archive provides two access options ranging from 12 to 48 hours

The percent over a year that a file stored in S3 will not be lost

The percent over a year that a file stored in S3 will be accessible

* How to change a storage class

By default, all objects uploaded in S3 are set to standard. To change the storage class it should be done prior / during the upload process, either:

- a) set details : select another class during the upload process
- b) lifecycle policies :

→ for classes Standard, RRS and S3-IA, you can manually, and at any time change the class in the object 'properties', but to move an object to Glacier, you need the object lifecycle and it will take up to 1-2 days to take effect.

→ Object lifecycle

- * a set of rules that automate the migration from a class to another based on time intervals.

* lifecycle management : the functionality is located on the bucket level,

can be deleted
or rolled back

and the policy can be applied to a

→ the bucket

→ one specific folder in the bucket

→ one specific object within the bucket.

→ S3 permission functionality can be found on bucket and object level

* on the bucket level (internal access), you can view permissions, edit permissions.

* on the object level (external access), you can control who opens, downloads and views permissions, edit permissions.

→ Versioning (it is either ON or OFF)

- * a feature that keeps track of all objects versions (old/new)
- * once is ON, you can suspend it, but can fully turn it OFF.
- * suspending versioning will prevent any in the future, but the old versions will remain.
- * versioning can only be set on bucket level, and applies to all objects within the bucket.

② Amazon Elastic Block Store (EBS)

→ Developed in EC2 part (page 4)

③ Amazon Elastic File System (EFS)

- is a fully managed service that provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS cloud services and on-premises.
- up to petabytes of scale
- EFS is a regional service storing data within and across multiple AZs for high availability and durability.
- you share EFS across thousands of EC2 instances at the same time.
- cannot be connected to CloudFront
- not suitable for static content

④ Amazon FSx for Lustre

- fully managed file system that is optimized for compute-intensive workloads, such as T performance, ML, media data processing etc --
- it is integrated with S3
- it enables you to burst your CIO from on-premises to AWS by allowing you to access your FSx file system over Amazon Direct Connect or VPN.
- cheap and performant non-replicated storage durable in S3.

⑤ Amazon FSx for Windows File Server

- fully managed native Microsoft Windows file system on which you can easily move your Windows-based applications that require file storage to AWS.

⑥ AWS Storage Gateway

- a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage.
- you can use it for archiving, DR, cloud data processing, migration, etc --
- it has local caching.
- includes file gateway, volume gateway and tape gateway.

* Additional Services (essential)

→ AWS Support

	Developer	Business	Enterprise
use case (recommendation)	Testing in AWS	prod workloads in AWS	Business / critical workloads in AWS
AWS trusted advisor	flare checks	full set of checks	full set of checks
architectural guidance	general	contextual to your use cases	consultative review / customized app guidance
Technical account management	X	X	✓
training	X	X	✓
account assistance	X	X	concierge support account
Enhanced technical support	Business hours / email access to cloud support/unlimited cases	24x7 email/chat / phone to cloud support channels + unlimited cases	24x7 email/chat / phone to cloud support channels + unlimited cases
Programmatic Case management	X	AWS Support API	AWS Support API
Third party Software Support	X	Interoperability and config. guidance and troubleshooting	Interoperability and config. guidance and troubleshooting
Proactive Programs	X	access to rare event mgmt for extra fee	rare event mgmt / TAM operate and orchestrated reviews
Cost	>= 29 \$	>= 100 \$	>= 15k \$
Case Response Time	general guidance	< 24 business hours	< 24 h
	System impaired	< 12 business hours	< 12 h
	production system impaired	X	< 4 h
	production system down	X	< 1 h
	Business - critical system down	X	< 15 min
Case Severity			

* AWS Basic is free, offers account support, billing questions, service limits and access to documentation.

→ AWS Partner Network APN

helps partners to build successful AWS Business

① APN Consulting partners & helps to design / architect / migrate / build new applications on AWS. It includes system integrators, resellers, MSPs, digital agencies, etc --

② APN Technology partners & helps to provide software solutions that are hosted on / integrated with AWS. It includes, SaaS, PaaS, management and security vendors, independent software vendors (ISVs)

→ AWS Marketplace

* Service that provides a sales channel for APN consulting Partners and ISVs to sell their solution to AWS customers

* Online software store / digital catalog that include thousands of software listings, such as AMI-based, container-based, ML, SaaS, desktop application products.

→ Service oriented architecture principles (SOA)

⇒ Decouple your components

- 1) use SQS to isolate components
- 2) use SQS as buffers between components
- 3) design each component to be self-reliable and interact asynchronously with others
- 4) Bundle logical contract of a component into AMI (to be deployed more often)
- 5) make your application stateless.

→ AWS GovCloud

- * an isolated AWS region which is designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements.

→ AWS Multipart upload API

- * allows to upload a single object as a set of parts.
- * each part is a portion of the object's data.
- * you can upload parts independently and in any order, and if any fails, you can retransmit it without affecting the others.
- * after the upload process finishes, S3 assembles these parts and creates the object. (useful for objects >100 MB). It provides
 - 1) improved throughput (parallel upload of parts)
 - 2) quick recovery from any network issue
 - 3) pause and resume object uploads
 - 4) begin an upload without knowing the final object size.

→ AWS BatchWriteItem API is a dynamoDB API for upload.

- Cross-origin Resource sharing (CORS) is only applicable for client-side applications that are loaded in one domain to interact with resources in a different domain.

→ AWS acceptable use policy ⇒ defines what you can do on the platform as an AWS user

- AWS Infrastructure event management is a structured program available to enterprise/business support that helps planning to large-scale events such as infrastructure migration, marketing events, etc.

→ AWS documentation is available in two formats

- 1) HTML
- 2) Kindle

- * To make sure that the information you are reading is up-to-date, the page URL will include the word latest

* Blockchain Services

① Amazon Managed Blockchain

- a fully managed service that makes it easy to create and manage scalable blockchain networks using open source frameworks such as Hyperledger Fabric and Ethereum

* Business Applications

① Alexa for Business

- a service that enables organizations and employees to use Alexa to get more work done
- Employees can use Alexa as their intelligent assistant to be more productive in meeting rooms, at their desks and even with Alexa devices at home.

* AR and VR

① Amazon Sumerian

- lets you create and run virtual reality (VR), augmented reality (AR), and 3D applications quickly and easily without requiring any specialized programming or 3D graphics expertise

* Game Tech

① Amazon GameLift

- a managed service for deploying, operating and scaling dedicated game servers for session-based multiplayer games.
- can defend from DDoS attacks.

② Amazon Lumberyard

- a free, cross-platform, 3D game engine for you to create the highest-fidelity games, connect your games to the rest compute and storage of the AWS cloud, and engage fans on Twitch.

* IoT Services

① AWS IoT Core

- managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices.
- makes it easy to use Lambda, Kinesis, S3, SageMaker, DynamoDB, CloudWatch, CloudTrail, QuickSight to build IoT applications that gather, process, analyze and act on data generated by connected devices without having to manage infrastructure.

② Amazon FreeRTOS

- OS for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect and manage.
- makes it easy to connect devices to AWS IoT Core and AWS IoT Greengrass.

③ AWS IoT Greengrass

→ a software that lets you run local compute, messaging, data processing, ML, sync on connected devices securely.

④ AWS IoT 1-Click

→ a service that enables simple devices to trigger AWS Lambda functions that can execute an action

⑤ AWS Analytics

→ fully-managed service that makes it easy to run sophisticated analytics on massive volumes of IoT data without having to worry about the cost / complexity of building an IoT analytics platform.

⑥ AWS IoT Button

→ programmable button / WiFi device easy to configure and designed for developers to help them get started with AWS IoT Core, Lambda, DynamoDB, SNS

⑦ AWS IoT Device Defender

→ fully managed service that helps you secure your fleet of IoT devices.
→ it continuously audits your IoT configurations

⑧ AWS IoT Device Management

→ makes it easy to securely onboard, organize, monitor and remotely manage IoT devices at scale.

⑨ AWS IoT Events

→ fully managed IoT service that makes it easy to detect and respond to events from IoT sensors and applications

⑩ AWS IoT SiteWise

→ makes it easy to collect and organize data from industrial equipment at scale.
→ easily monitor equipment across your facilities

⑪ AWS IoT Things Graph

→ makes it easy to visually connect different devices and web services to build IoT applications. (drag and drop interface)

⑫ AWS Partner Service Catalog

→ helps you find devices and hardware to help you explore, build and go to market with your IoT solutions.

* Machine Learning (ML)

① Amazon SageMaker

- is a fully managed platform that provides every developer / data scientist the ability to build, train and deploy ML models quickly on AWS.
- Amazon SageMaker Ground truth helps you build highly accurate training datasets for ML quickly.

② Amazon Comprehend

- is a natural language processing (NLP) service that uses ML to find insights and relationships in text.
- No ML experience is required.

③ Amazon Lex

- Build conversational interfaces to any application using voice and text.
- provides advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text.

④ Amazon Polly

- turns text into lifelike speech
- lets you create apps that talk.
- AI service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice.

⑤ Amazon Rekognition

- add analysis to your application
- detect objects, scenes and faces in images.
- search and compare faces.

⑥ Amazon Translate

- Neural machine translation service that delivers fast, high quality and affordable language translation.

⑦ Amazon Transcribe

- Automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications.
- Using Transcribe API, you can analyze audio files stored in S3 and have the service return a text file of the transcribed speech.

⑧ Amazon Elastic Inference

- allows you to attach low-cost GPU powered acceleration to EC2 and SageMaker instances to reduce the cost of running deep learning inference by 75%.

⑨ Amazon forecast

→ a fully managed service that uses ML to deliver highly accurate forecasts of data.

→ it combines time series data and additional variables to build forecasts.

⑩ Amazon Textract

→ it automatically extracts text and data from scanned documents.

⑪ Amazon Personalize

→ a ML service that makes it easy for developers with no prior ML knowledge, to create individualized recommendations for customers using their applications.

⑫ Amazon Deep Learning AMIs

→ provides ML practitioners and researchers with the infrastructure and tools to accelerate deep learning in the cloud, at any scale.

⑬ AWS DeepLens

→ helps put deep learning in the hand of developers with a fully programmable video camera, tutorials, code, and pre-trained models.

⑭ AWS DeepRacer

→ helps to get started with reinforcement learning (RL).

→ RL is an advanced ML

⑮ Apache MXNet on AWS

→ fast and scalable training and inference framework, that includes Gluon interface which allows developers to get started with deep learning on the cloud, edge devices and mobile apps.

⑯ TensorFlow on AWS

→ enables developers to easily and quickly get started with deep learning in areas such as computer vision, natural language understanding and speech translation.

⑰ AWS Inferentia

→ ML inference chip designed to deliver high performance at low cost

* Robotics

⑱ AWS RoboMaker

→ makes it easy to develop, test and deploy intelligent robotics apps at scale.

* Satellite

⑲ AWS Ground Station

→ fully managed service that lets you control satellite communications, downlink, and process satellite data.

→ lets you scale your satellite operations quickly, easily and cost-effectively without having to worry about building or managing your own ground station infrastructure.