AWS
(Amazon Web Services)

Course
name - Ultimate AWS Certified
Cloud Practitioner

instructor - Stephane Maarek

Platform - Udemy

duration - 15 hours

exam - CLF-C02

Total Service - 200+
Service Covered - 40+

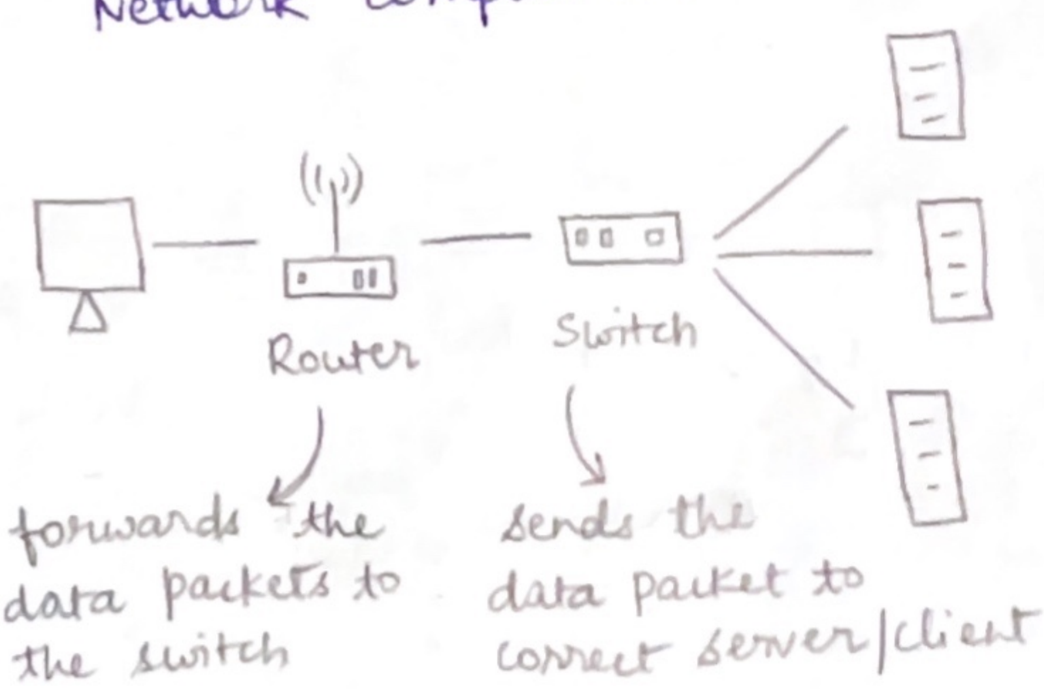
Todo
✓ 1. about
2. practice 6+1+1
3 exam
✓ 4. revision
✓ 5. list
✓ 6. pdf
7 ticket
8. register

Website Working

Server Composition

1 Compute - CPU
2 Memory - RAM
3. Storage - File
4. Database - Structured Data

Network Composition



Traditional Infrastructure

The servers were kept in a data center.

→ pay rent for data center
→ pay for power supply, cooling and maintaince for the servers
→ scaling up or down is difficult
→ data loss in disaster

Cloud Computing

It is the on demand delivery of the compute service, storage service and other IT services over the internet.

→ pay-as-you-go
→ auto scaling of resources

Application

Gmail
Google Photos
Netflix

Deployment Model

1. Private cloud → Rackspace
2. Public cloud → AWS, Azure, GCP
3. Hybrid cloud → on-primise + cloud

Characteristics

1. on demand delivery
2. pay-as-you-go
3. auto scaling of resource
4. broad network access and agile
5. resource pooling and multi-tenancy

Types of Services

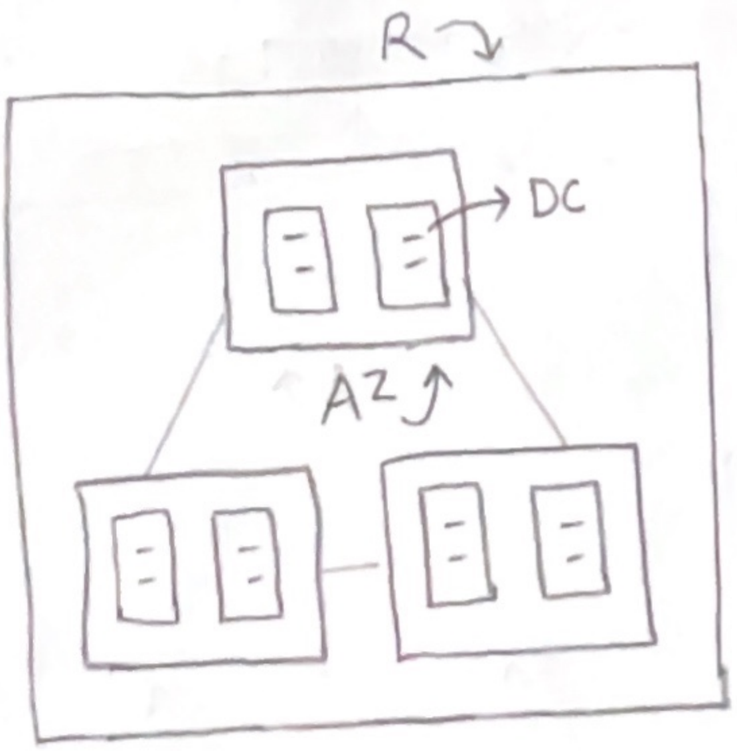
1. IaaS → EC2
2. PaaS → Elastic Beanstalk, Heroku
3. SaaS → Rekognition, Gmail

1 million = 10 lakh
1 billion = 100 crore

Pricing Model

Compute, Storage and Data Transfer out of the AWS cloud

AWS Infrastructure Global



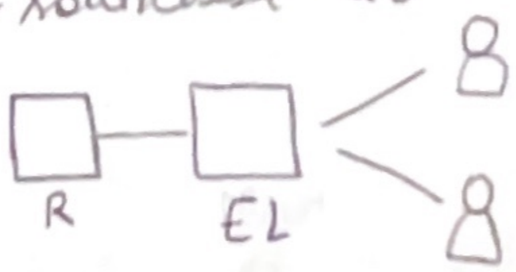
NASA - National Aeronautics and Space Adminstration

ISRO - Indian Space Research Organization

airbnb - Air Bed and Breakfast

R - Region → ap-southeast-2 (Sydney)
AZ - Availability Zone → ap-southeast-2a (The min is 3 and max is 6)
ap-southeast-2b
ap-southeast-2c
DC - Data Center

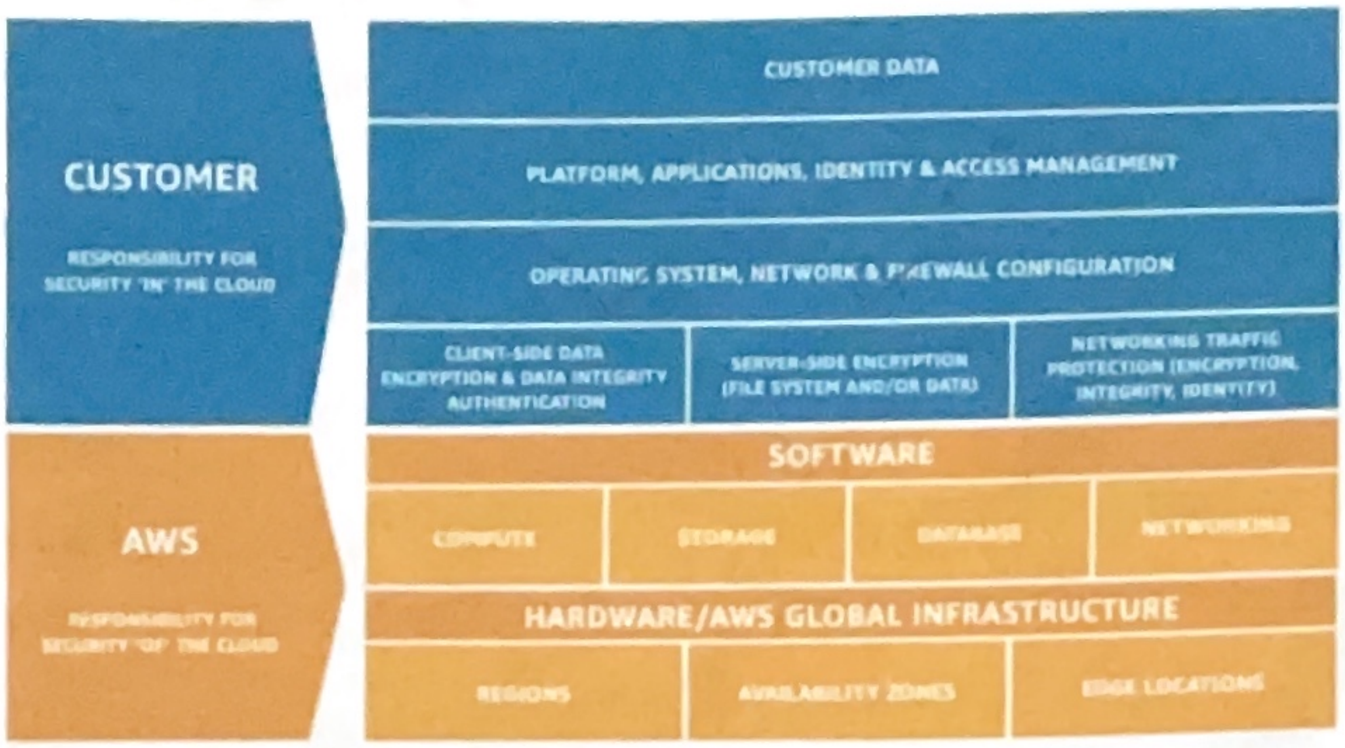
PoP or EL - Point of Presence or Edge Location



Shared Responsibility Model diagram

CUSTOMER = RESPONSIBILITY FOR THE SECURITY **IN** THE CLOUD

AWS = RESPONSIBILITY FOR THE SECURITY **OF** THE CLOUD



How to choose an AWS region for your application?

1. compliance with data
2. proximity to user
3. avialability of service
4. appropriate price

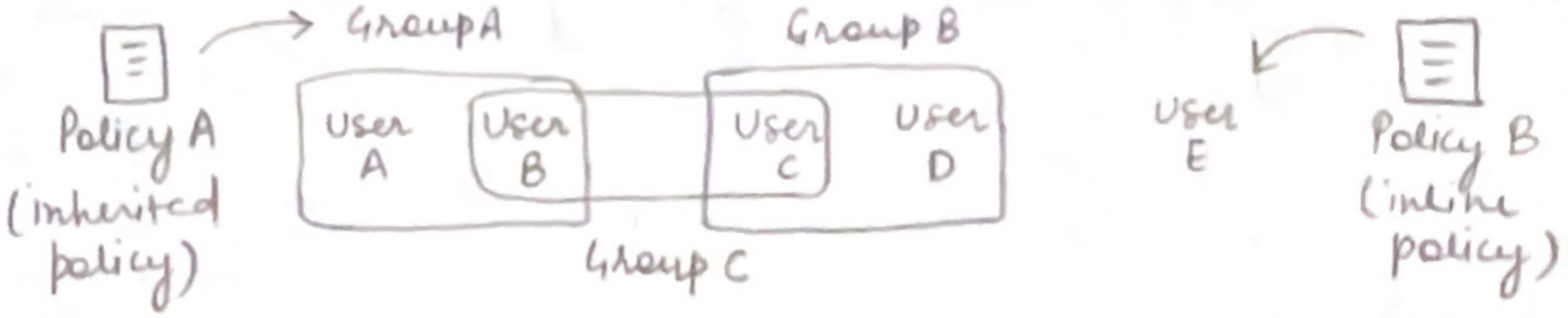
Note
ARN - Amazon Resource Name

Planning
✓ Section 1 to 3 : 10th May
✓ Section 4 : 11th May
✓ Section 5 : 12th May
✓ Section 6 to 8 : 16th May
✓ Section 9 to 15 : 22th May
✓ Section 16 to 23 : 23rd May

Command
echo "I am a new file." > notes.txt
cat notes.txt
ls
pwd

The cloudshell have features to download file and upload file.

SERVICE	SCOPE	FEATURES
1. IAM	Global	It stands for Identity and Access Management. We can create User, Group and Policy. There is a root user and IAM users.



The policy is the set of permissions written in a JSON document.

```
{ "Version": "2012-10-17",
  "Statement": [
        {
          "Effect": "Allow",
          "Action": "s3:GetObject",
          "Resource": ["arn:aws:s3:::myBucket/*"]
        },
        ...
  ]
}
```

Principal
Condition
EAR

→ You apply The Least Privilege Principle that states to not give more permissions than a user needs.

→ This service cannot be region specific.

→ There is a url to sign in for IAM users.

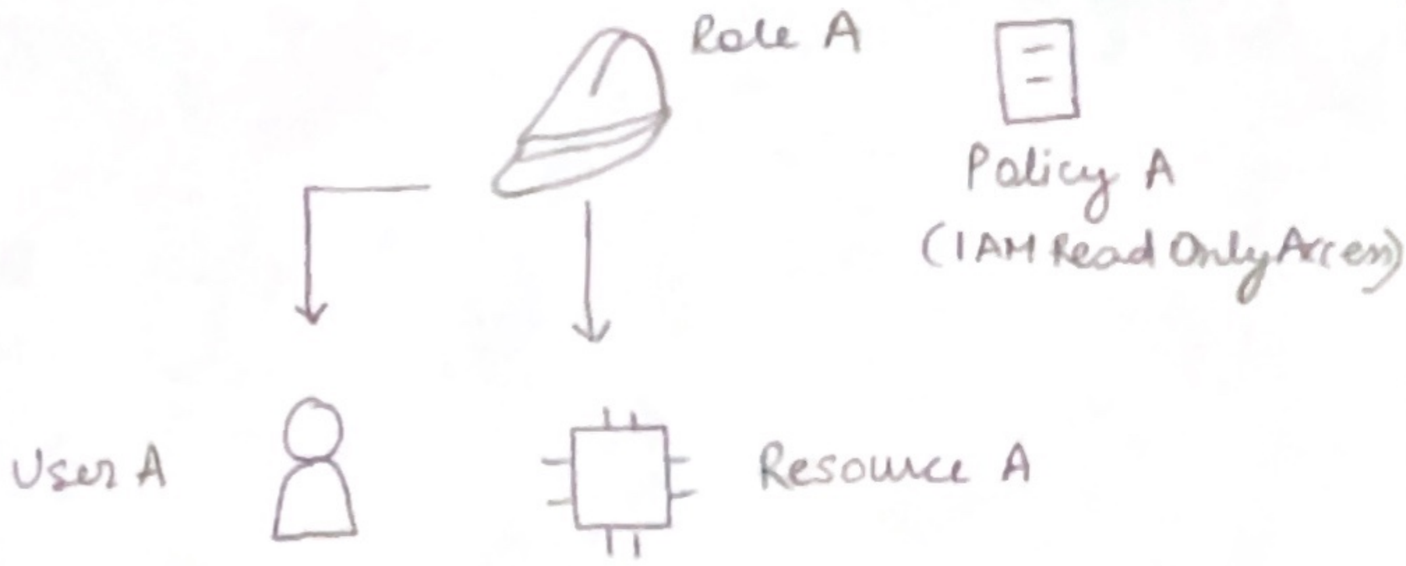
access AWS
1. Console
2. CLI - Command Line Interface → terminal / cloud shell
3. SDK - Software Development Kit

access key
1. Access Key ID
2. Secret Access Key

command
aws --version
aws configure
aws iam list-users

MFA - Multi Factor Authentication
MFA = password + security device
1. Virtual - Google Authenticator (single)
Authy (multi)
2. Physical - Universal 2nd Factor (YubiKey)
- Hardware Key Fob (Gemalto)
- Hardware Key Fob (SurePass ID)
for AWS GovCloud

Password Policy



We allow EC2 instance to access IAM.

Security Tool
1. Credential Report
AC 2. Access Adisor

2. EC2 Regional

It stands for Elastic Compute cloud.
It is a irtual server in the cloud.

Services
1. Instance (EC2)
2. Elastic Block store (EBS)
3. Elastic load Balancing (ELB) and
Auto Scaling Group (ASG)

In EC2 instance we can configure OS, CPU, RAM, Storage (EBS), Network Card, User Data and Security Group (Firewall).

The User Data is the bootstrap script which is configured for the first launch.

Instance Type:
t2.micro
m5.8x large

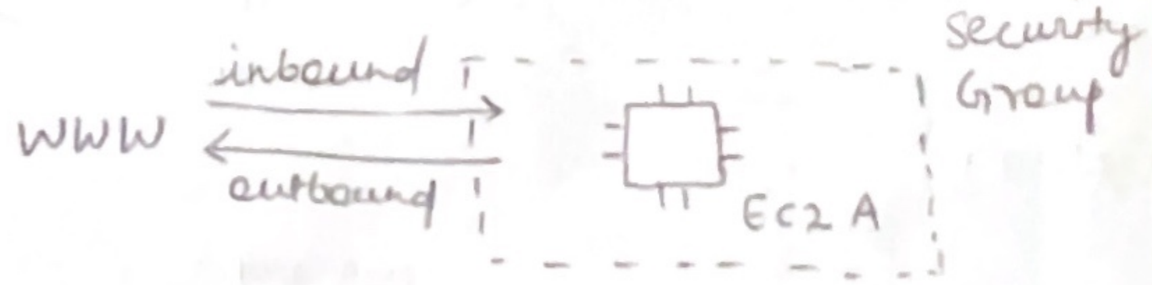
Key Pair:
Key Pair A

The instance have a public and a private IP address.

Inbound ↙ Port 80 HTTP
↘ Port 22 SSH

Outbound ↗ Any Port

The Security Group (Firewall) provides the network security. It monitors the in/out traffic of EC2 instance



Port 21 - FTP (File Transfer Protocol)
Port 22 - SFTP (Secure File Transfer Protocol)
Port 443 - HTTPS (Secure HTTP)
Port 3389 - RDP (Remote Desktop Protocol)

SSH / Putty / EC2 Instance Connect

It helps to control remote machines which means the ec2 instance.

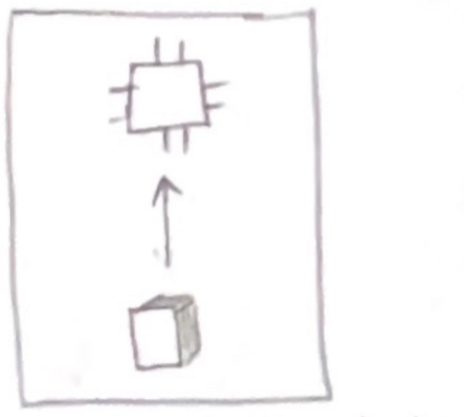
ssh -i '.\KeyPairA.pem' ec2-user@15.207.107.59

identity file

Purchasing Options
- → on demand
- → reserved (standard/convertible) (1 or 3 years)
- → saving plans (usage)
- → spot instance (less reliable)
- → dedicated host (server)
- → dedicated instance (hardware)

EBS Volume ①

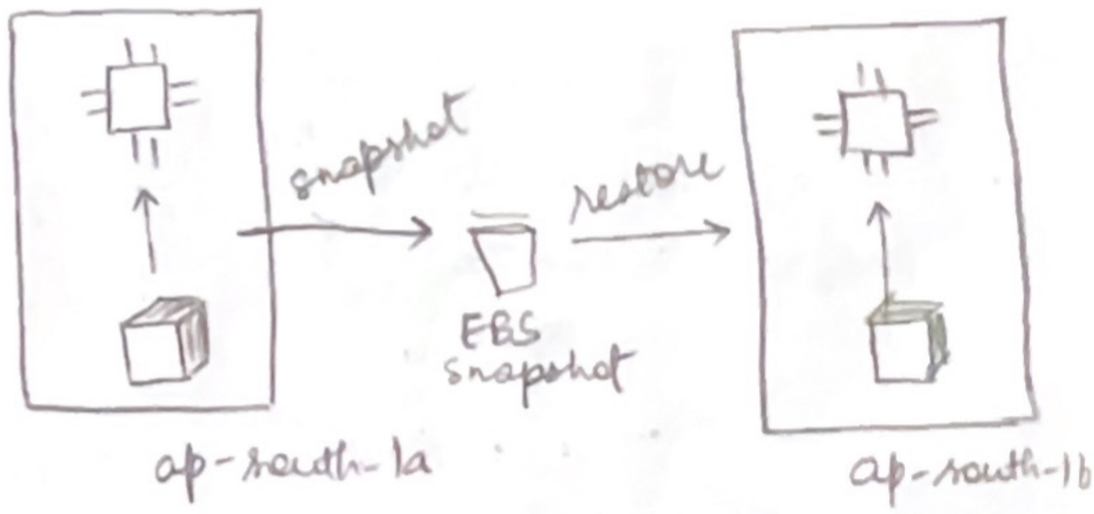
It stands for Elastic Block Store Volume.
It is a network storage drive.
It can persist data on instance termination.
It can be attach to one instance at a time.
It is bound to a specific AZ.



EBS Snapshot

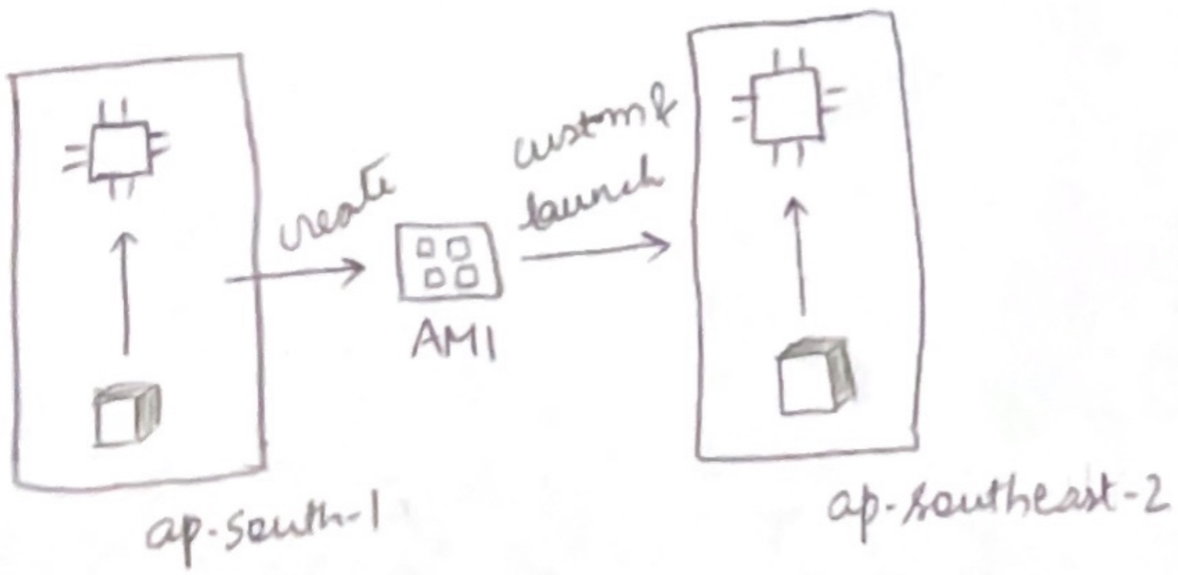
It stands for Elastic Block Store Snapshot.
It is used to create backup of EBS Volume
- → disaster
- → copy for AZ/R

It have EBS Snapshot Archive and EBS Snapshot Recycle Bin features.



AMI EC2

It stands for Amazon Machine Image EC2.
It is customization of EC2 instance.
It have faster boot time.
It is bound to a specific R.



EC2 Image Builder

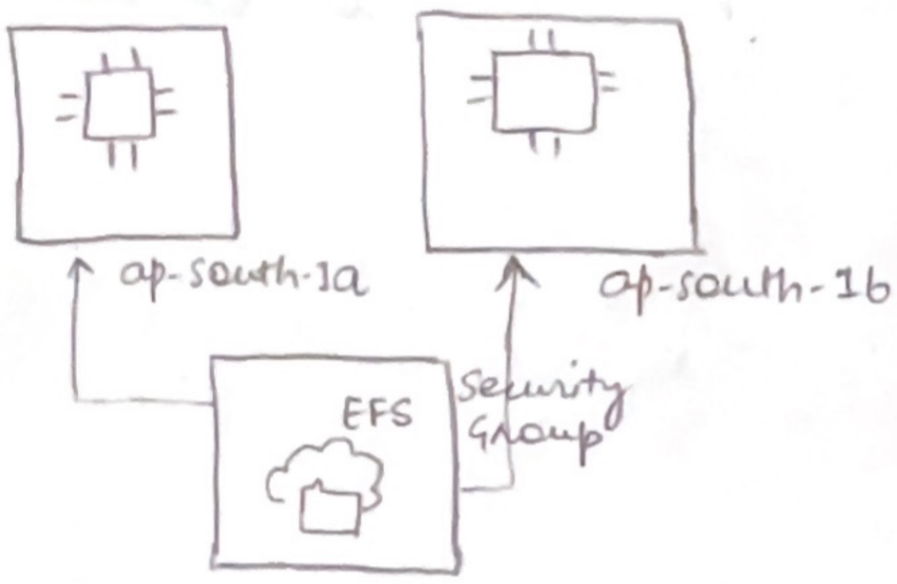
It automates the create, customize, test and deploy EC2 AMIs.
It can run on schedule.

EC2 Instance Store (II)

It is a hardware disk with high performance and less reliable.
It is not durable. It is preferred for temporary data.

EC2 EFS (III)

It stands for EC2 Elastic File System.
It manages file storage of EC2.
It can be attached to multiple instance at a time.
It is not bound to specific AZ



It have Infrequent Access and Lifecycle Policy feature.

Amazon FSx

It is a third party service.
It manges file storage with high performance and high reliable.

- FSx for windows - File system
- FSx for Lusture - High Performance Computing

Terminology

(i) Scalability

The application can handle greater load by adapting.

There are two types

- → Vertical — increase size of instance — up-down
- → Horizonal — increase no. of instance — out-in → ELB, ASG

(ii) High Availability

It goes hand in hand with horizontal scaling.
It means running application in atleast 2AZ.
It helps in disaster.

NV | India

(iii) Elasticity

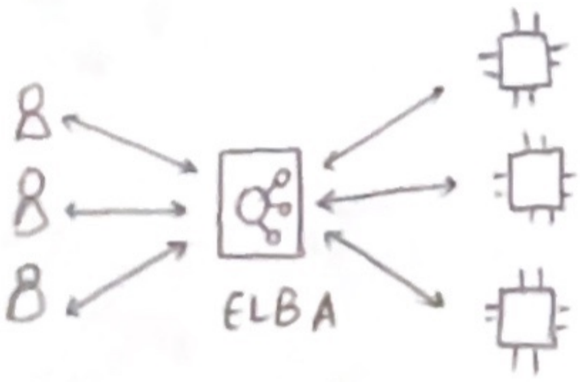
Once the system is scalable, there will be some 'auto scaling' based upon the load is called elasticity.

(iv) Agility

It means the IT resources are just a click away, which means it reduces the time to make those resources available to your developers.

ELB

It stands for Elastic Load Balancing.
It is a server that forwards internet traffic to multiple servers.



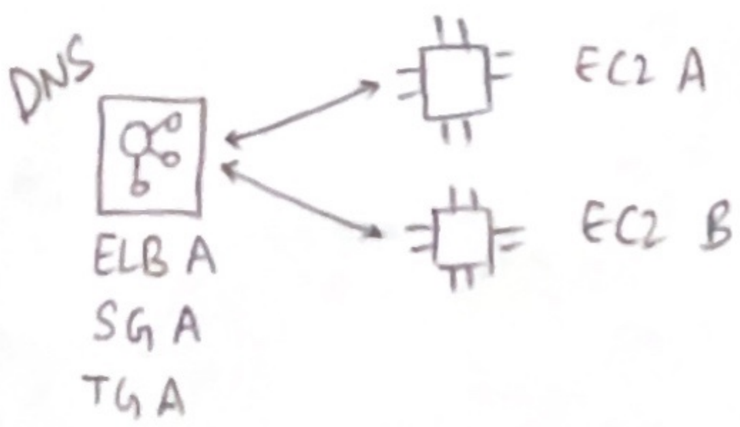
It can create single point of access (DNS)
It can handle failure of any instance.
It do regular health checkup of all instance.

There are three types

(i) ALB - Application Load Balancer
HTTP, HTTPS (Layer 7)

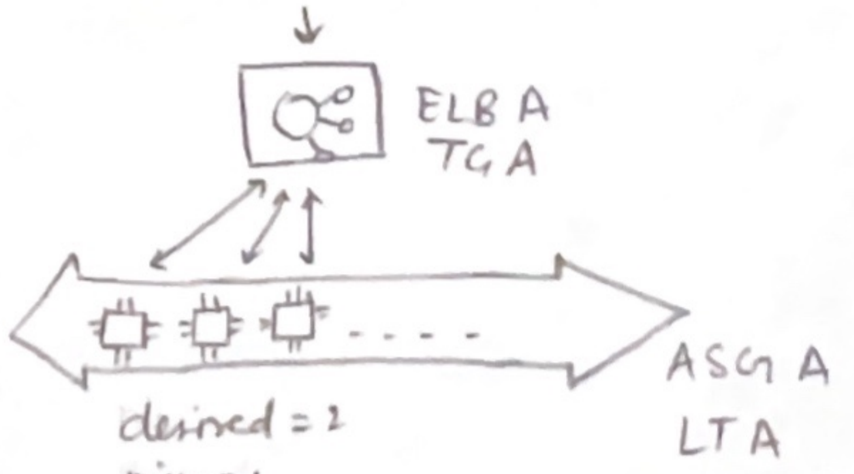
(ii) NLB - Network Load Balancer *
TCP, UDP (Layer 4)

(iii) GLB - Gateway Load Balancer
GENEVE, Firewall (Layer 3)



ASG

It stands for Auto Scaling Group.
In real life the load of the application can change.
It automatically increase/decreases the instance based on load.



Manual
dynamic (usage/schdule)
predictive (ML)

LT - Launch Template
SG - Security Group
TG - Target Group

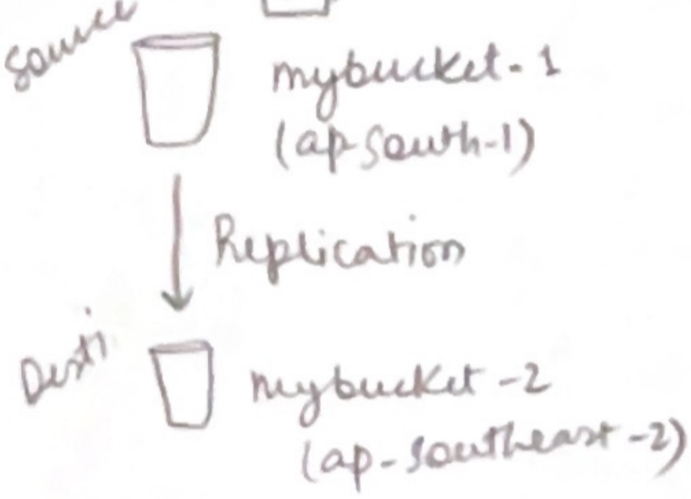
3. S3 Regional

It stands for Simple Storage Service.
It is a scalable storage in the cloud

→ Bucket (directory)
→ Object (file)
→ Key (s3://my-bucket/notes.txt)

- The pre-signed URL allow to access object without updating bucket policy.
- The Object URL allow to access object based on the bucket policy.

Security → User Based (IAM Policy)
→ Resource Based (Bucket Policy, Object ACL, Bucket ACL)
→ Encryption



- It can host a static website.
- You can enable Versioning at bucket level.
- It can create Replication i.e CRR and SRR.
The versioning needs to enabled and there should be a Replication Rule.

Storage class
→ Standard
→ Standard - Infrequent Access
→ One Zone - Infrequent Access
→ Glacier Instance Retrieval } archive
→ Glacier Flexible Retrieval
→ Glacier Deep Archive
→ Intelligent Tiering

Manual / Lifecycle
LR-A

Encryption

server-side (default)

client-side

IAM Access Analyzer

Snow Family

It is a highly secure portable device that helps in data migration and edge computing.

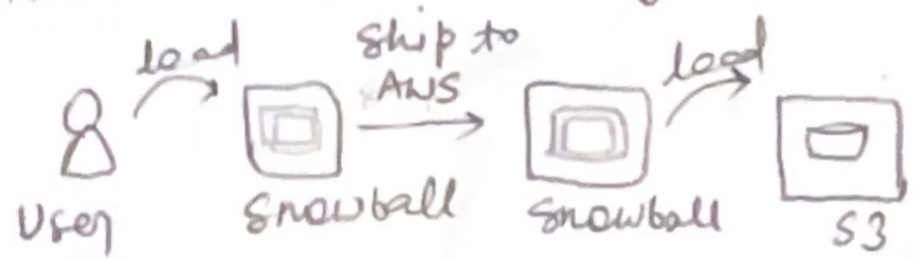
fast

↳ location with no internet

Devices

- → snowcone — TB
- → snowball edge — PB
- → snowmobile — EB

If it takes more than a week to transfer data then use snow family devices.



The AWS OpsHub is a software installed to handle snow family devices.

Storage Gateway

It bridge between on-premise data and cloud data.

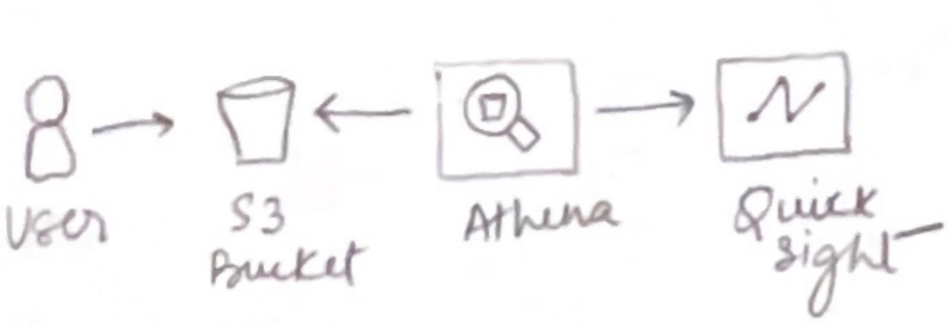
Databases

1. RDS (OLTP)	Regional SQL	It supports to create snapshot and restore snapshot. It stands for Relational Database Service. It does not support SSH.
2. Aurora	Regional SQL	It is not included in free-tier. It have better performance compared to RDS.
3. Aurora Serverless	Regional SQL	It provides autoscaling based on usage. It requires least management.
4. ElastiCache	Regional NoSQL	It is a in-memory database. It supports Redis and Memcached.
5. DynamoDB	Regional NoSQL	It supports read-write replication. It is a serverless database. It is a key-value database. Primary Key = Partition Key + Sort Key
6. DAX	Regional NoSQL	It stands for DynamoDB Accelerator. It is a 'in memory database.
7. RedShift (OLAP)	Regional SQL	It is used for data warehouse. It have a columnar storage.
8. RedShift Serverless	Regional SQL	It provides autoscaling based on usage.
9. EMR	X	It stands for Elastic Map Reduce. It is used in Big Data to create Hadoop cluster.

Deployment Options
1. Read Replica (load)
2. Multi AZ (failure)
3. Multi R (latency)

10. Athena

It is a serverless query service that perform analytics against S3 Object.

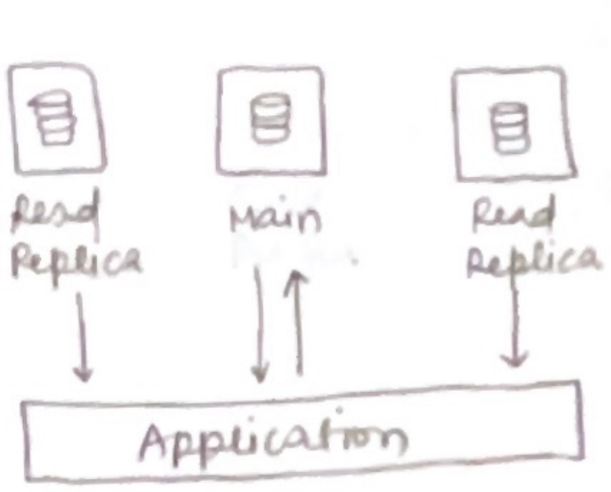


NOTE -

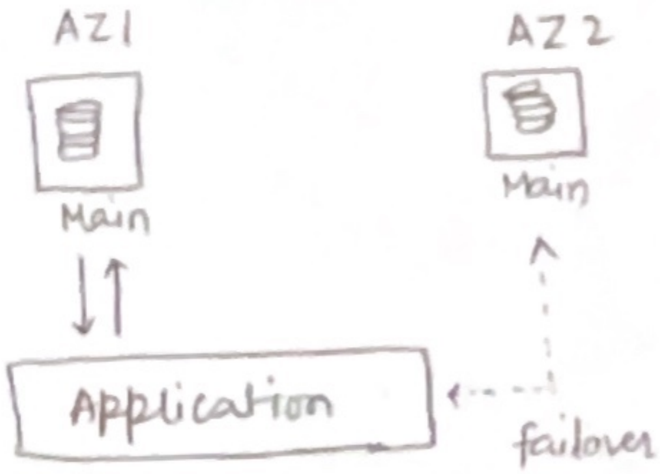
The advantages of using AWS Database Services are scalability, cost efficiency, disaster recovery and security.

→ The use case for NoSQL database are social network app and big data app. It is suitable for unstructured data and supports Horizontal Scaling.

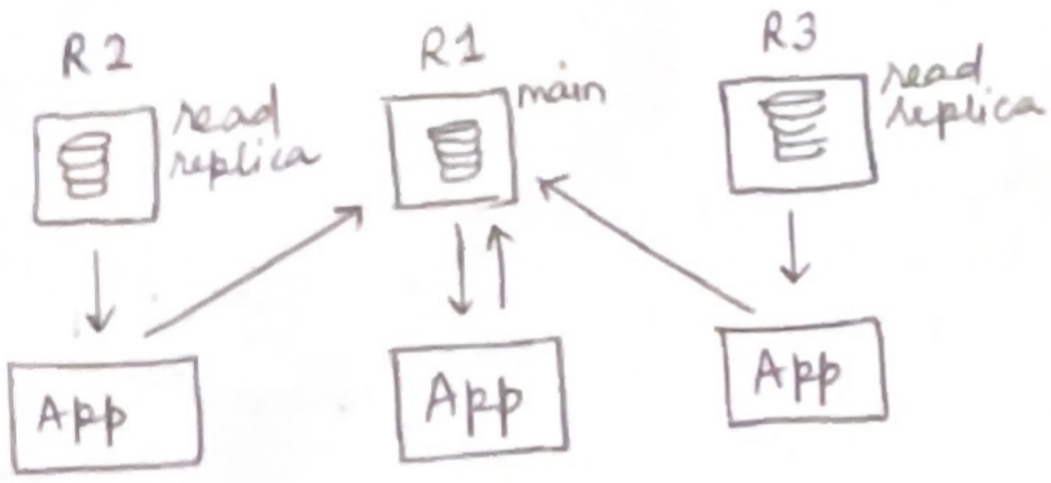
→ The use case for SQL database are financial system and CRM System. It is suitable for structured data and supports Veritical Scaling.



Read Replica



Multi AZ

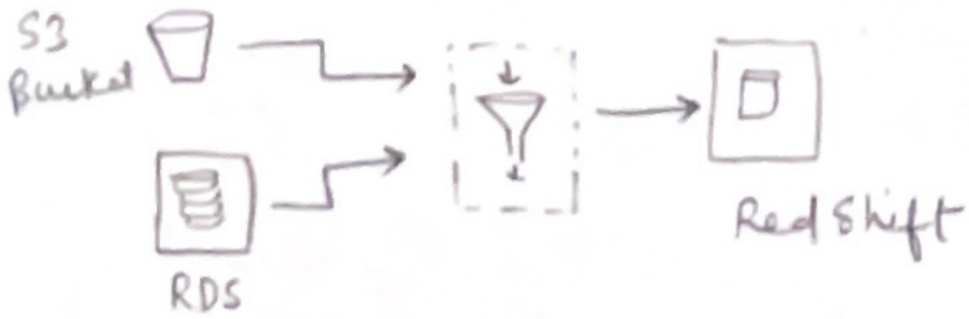


Multi R

1. DocumentDB	Regional NoSQL	It supports MongoDB.
2. Neptune	Regional NoSQL	It is graph database. It is used in social network and wikipedia.
3. Timestream	Regional SQL	It is time series database.
4. QLDB (Central)	Regional SQL	It stands for Quantum Ledger Database. It is used for recording financial transcation. It is a immutable system.
5. Managed Blockchain (Decentral)	Regional SQL	It supports finanial transcation without the need of central authority

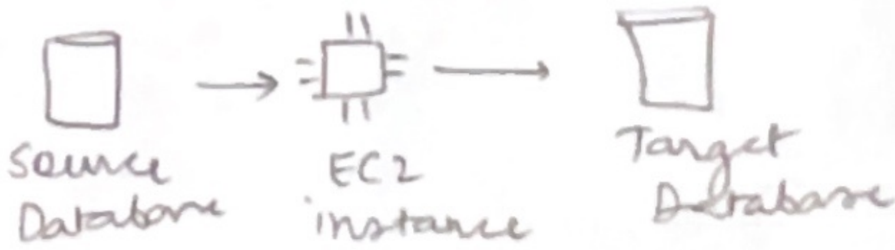
Glue

It is a ETL Service. It stands for Extract Transform and Load.
It is used for data processing to do data analytics.



DMS

It stands for Database Migration Service.

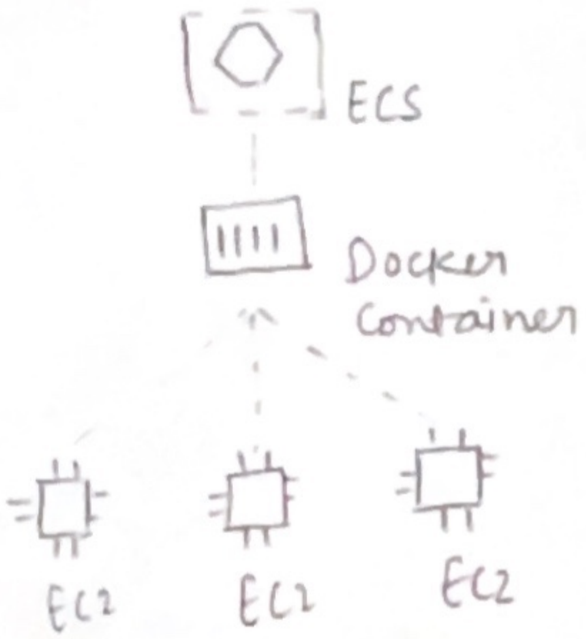


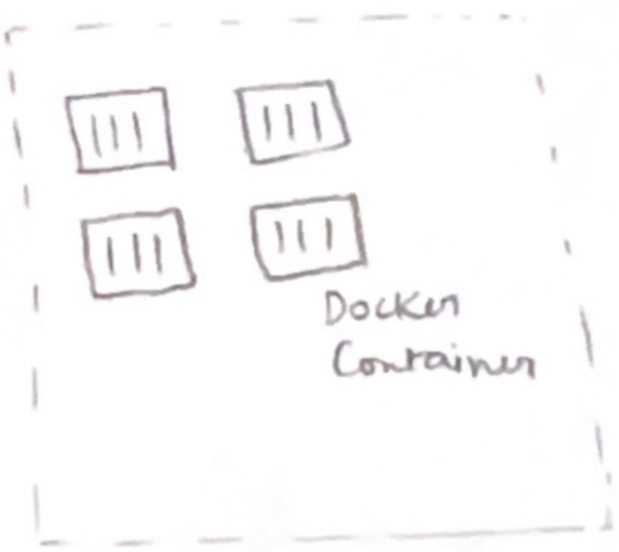
Compute

1. ECS — Regional
   It stands for Elastic Container Service.
   It runs docker container over the cloud
   We need to create EC2 instance.

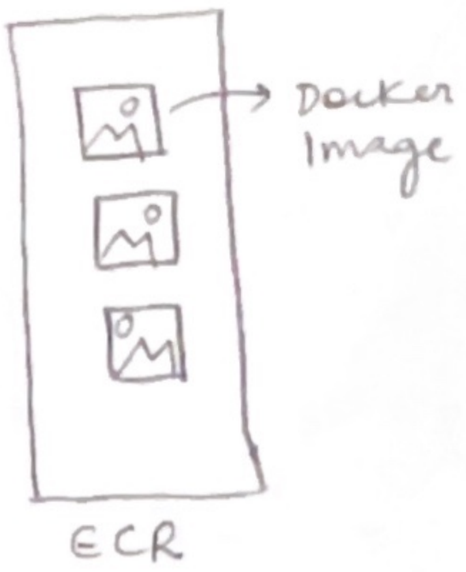
2. Fargate — Regional
   It runs docker container over the cloud.
   It creates the EC2 instance.
   It is serverless

3. ECR — Regional
   It stands for Elastic Container Registery
   It is used to store docker images.





Fargate



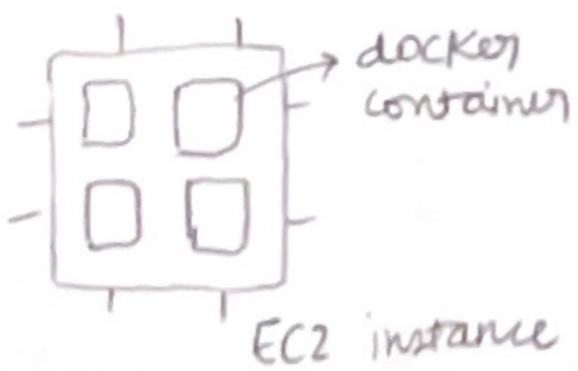
4. Lamda — Regional
   It is a virtual function in the cloud.
   It is a FaaS. It is event driven.
   The pricing is based on calls and duration.
   duration - 15 min
   memory - 128 mb to 10240 mb
   emphemral storage - 512 mb to 10240 mb

5. API Gateway — Regional
   It is a serverless API service over the cloud.

6. Batch — Regional
   It is a batch processing service over the cloud.
   It is a docker image that runs on ECS.

7. Light Sail — Regional
   It supports virtual server, storage, database and network
   It is for people with little cloud experience.

Docker
It is use for application deployment.
The application is packed in a container
and can be run in any OS.



Docker Image
Docker Repository

Serverless
The servers are taken care by the cloud.

LIST

The IAM is global and the rest are all regional.

1. IAM
2. EC2 (EBS Volume, EBS Snapshot,
   AMI, Image Builder, ELB, ASG)

   Instance Store

   EFS

   FSx

3. S3

   Snow Family

   Storage Gateway

4. RDS, Aurora, Aurora Serverless, ElastiCache

   DynamoDB, DAX, DocumentDB

   Redshift, Redshift serverless

   Neptune, Timestream

   QLDB, Managed Blockchain

   EMR, Athena

   Glue, DMS

5. ECS, Fargate, ECR

   Lambda, API Gateway

   Batch, Light sail

   Docker

   serverless

Deployment and Managing Infrastructure

1. CloudFormation
   It is use to create and manage aws resources with a code template.
   It is a IaaC. It stands for Infrastructure as a Code.
   → It can destroy and recreate the aws resources over the cloud.
   → It can automate the diagram generation aws resources over the clould
   It is known as Application Composer

CDK
It stands for Cloud Development Kit
It is use to define the code templat in the familiar programming language
It compile code templat in to the YAML/JSON file.

2. Beanstalk Elastic → EBS
   It is use for deployment of application.
   It is a PaaS. It stands for Platform as a Service.
   It also provides health monitoring
   It uses cloud formation under the hood

3. Code Deploy
   It deploy the application automatically.
   It is a hybrid service that works with EC2 instance and on premise server

4. Code Commit
   It is a code repository.
   It is alternate to GitHub.

5. Code Build
   It is a service for code development

6. Code Pipeline
   It is use to create pipeline for all the steps to automatically deploy code to production

7. Code Artifact → artifact management
8. Code Star → Unified UI for managing software development activities at one place.
9. cloud 9 → IDE

10. Systems Manager → SSM
    It is use to manage EC2 instance and on prenise system.
    → It runs automatic patches and configure.
    → It runs commands across system

1. Session Manager → secure shell on EC2
2. Parameter Store → store configuration

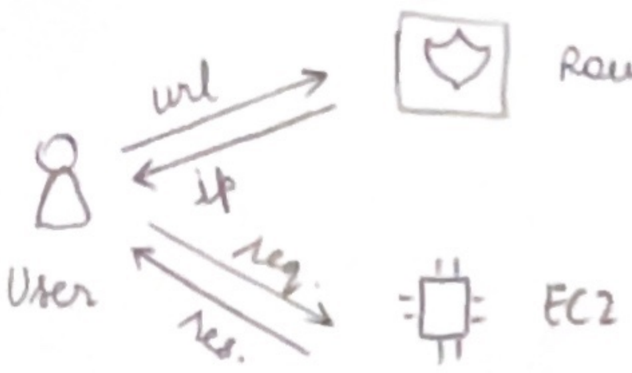
Global Infrastructure

NOTE : First Four are the global service.

1. Route 53

It is a DNS. It stands for Domain Name System.

It route user to the closest deployment to decrease latency.



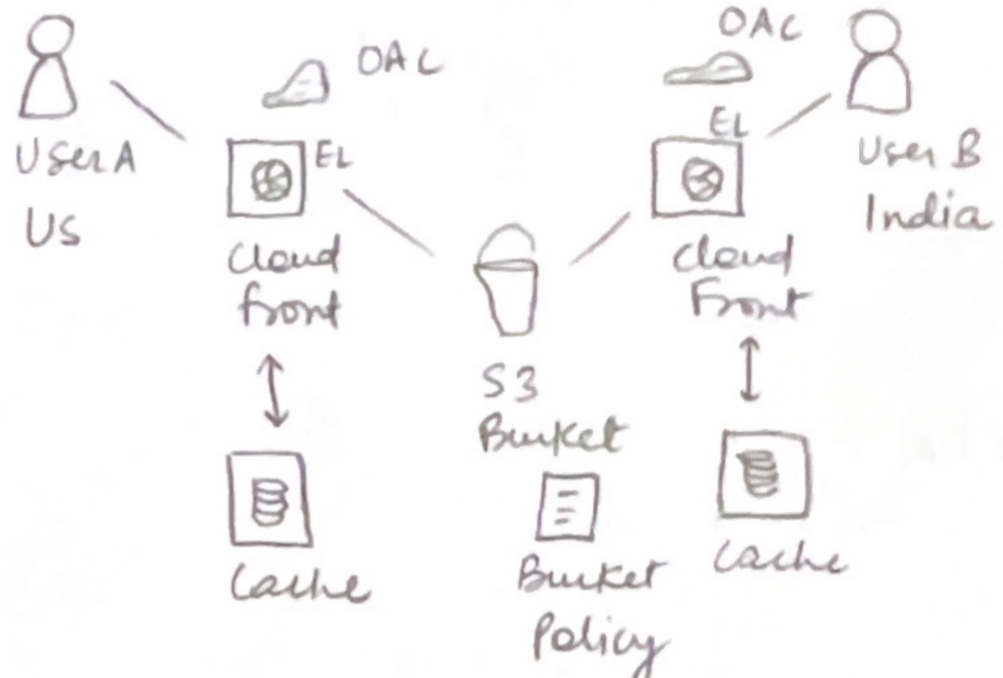
It have several routing policy

1. Simple RP
2. Weighted RP
3. Latency RP
4. failover RP

2. Cloud Front

It is a CDN. It stands for Content Delivery Network.

It replicates part of application to the edge location to decrease latency.



It provides DDoS protection, WAF, OAC and shield.

- Distributed Denial of Service
- web App Firewall
- Origin Access Control

3. S3 Transfer Acceleration

It accelerate upload and download in S3 It uses cloud front

4. Global Accelerator

It accelerate performance of the global application. It uses edge location.

1. Outpost → It is use to manage on-premise server, It provides extension to AWS service.
2. WaveLength Zone → telecommunication provider 5G Network
3. Local Zone → There are multiple local zones under the region.

Architecturing and Ecosystem

Well Architecture Framework → White Paper
Scalability, Disposable Resource, Automation, Loose Coupling, Serices

1. Operational Excellence → perform operation as code
   make frequent, small and reversible change
   manage failure
2. Security
3. Reliability
4. Performance Efficiency
5. Cost Optimization
6. Sustainability

Well Architecture Tool → workload

Customer Carbon Footprint Tool

Cloud Adoption Framework → White Paper
Business, People, Governance, → Business
Platform, Security, Operation → Technology

APN → AWS Patner Network
- Technology
- Training
- Consultancy

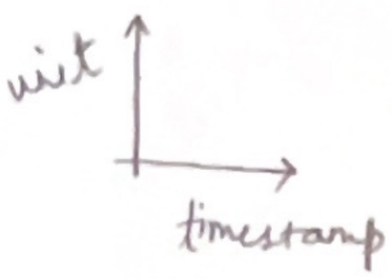
IQ → profession help

re:Post → community forum
knowledge center

Manage Services → support

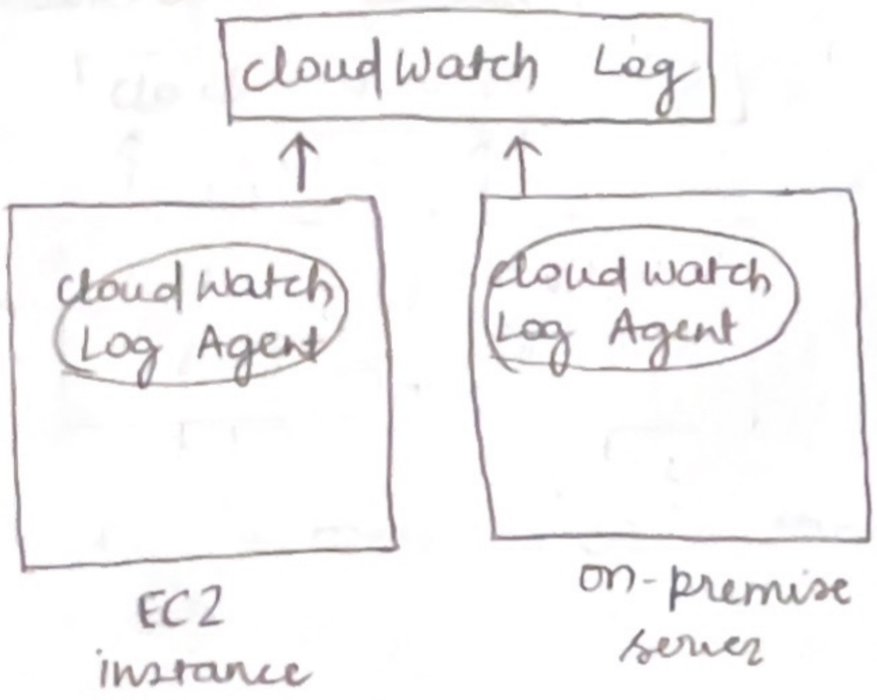
Cloud Monitoring

1. CloudWatch Metrics
   It is a graph representation use for monitoring.



2. CloudWatch Alarm
   It is use to trigger alarm for any cloudWatch Metric.
   The Billing Alarm is only available in North Virgina (us-east-1)

3. CloudWatch Log
   It is use to list the logs of the resources at real time.



4. Event Bridge
   It is a serverless service use to create rules for event driven application.
   → Schudule
   → Event Pattern
   → Rule
   → Event Bridge Scheduler

5 Cloud Trail
   It is use to track user activity.
   It provides governance, compliance and audit for AWS account.
   It is enabled by default.

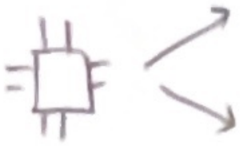
6. X-Ray CloudWatch
   It is use to analyze and debug your applications.
   It provides the visual analysis of applications.

7. ~~Cloud~~ Guru
   It is a Machine Learning powered service that provides
   → automated code review → code Guru Reviewer
   → application performance recommendation → code Guru Profiler

8. Health Dashboard
   It provides the health of aws resources.
   → service history → all resources all regions
   → account health → personal used resources

VPC and Networking

IP Address



- Public IPv4 Address
- Private IPv4 Address

Elastic IP

Default VPC

VPC
It stands for Virtual Private Cloud.
It is a private network to deploy resources.

Subnet
It allow to portion VPC network into public and private.

Internet Gateway
It helps VPC to connect public subnet with internet.

NAT Gateway
It helps VPC to connect private subnet with internet via public subnet.

Endpoint Gateway
It helps VPC to connect private subnet with S3 and DynamoDB.

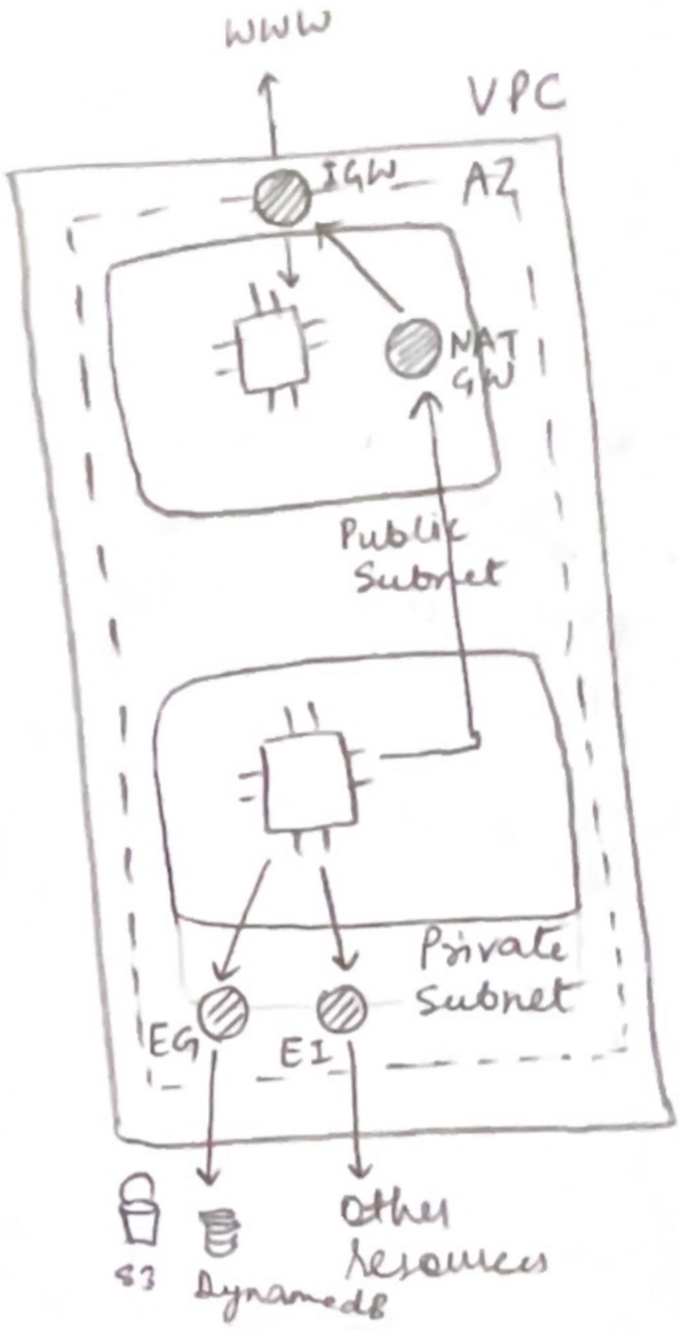
Endpoint Interface
It helps VPC to connect private subnet with other resources.

1. NACL → It stands for Network Access Control List. It is a firewall in Subnet.
2. Security Group → It is a firewall in EC2.

1. VPC Flow Logs → It is use to log information about network traffic.
2. VPC Peering → It is use to connect two VPC. It is non transitive.

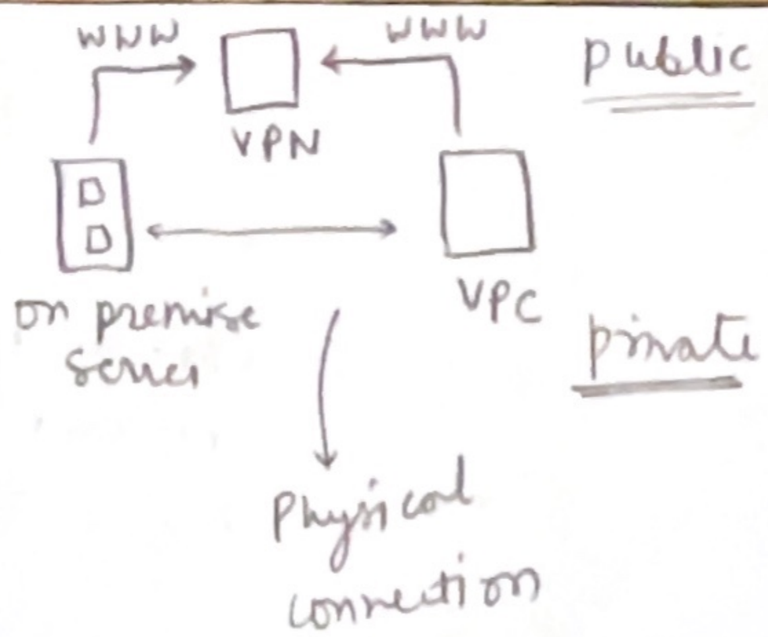
Transitive Gateway
→ It provides peering between 1000s of VPC and on premise in a star connection

Elastic IP
It allow to attach a fixed public IPv4 address to EC2 instance.



Private Link
It is use to connect VPC to 3rd party VPC.

1. Site to Site
2. Direct Connect
3. Client VPN



1. Cloud Formation, CDK, Elastic Beanstalk
   Code Deploy, Code Commit, Code Build, Code Pipeline
   Code Artifact, Code Star, Cloud 9
   System Manager (Session Manager / parameter store)
2. Route 53, Cloudfront
   S3 Transfer Acceleration, Global Accelerator
   Outpost, Wavelength Zone, Local Zone
3. SQS, Kinesis, SNS, MQ
4. cloud Watch (Metric, Alarm, Log)
   Event Bridge
   Cloud Trail, cloudWatch X-Ray
   Code Guru, Health Dashboard
5. IP Address
   VPC, Subnet, Internet Gateway, NAT Gateway
   Endpoint Gateway, Endpoint Interface
   NACL, Security Group,
   Private Link
   VPC flow logs, VPC peering
   Transitive Gateway

Security and Compliance

1. DDoS Protection → It stands for Distributed Denial of Service.
   It can be done by Shield, WAF, CloudFront and Route53
   - Standard
   - advanced

   The WAF stands for Web Application Firewall
   It provide protection in layer 7 of HTTP.
2. Network Firewall → It protects VPC.
3. Firewall Manager → It manages all the security rules.
4. Penetration Testing → It is to attack your own infra
5. Encryption
   - Data at Rest
   - Data at Transit

   KMS → Key Management Service (encryption key)
   - a. customer manged key
   - b. aws managed key
   - c. aws owned key
   - d. cloud HSM key

   CloudHSM → Hardware Security Module (encryption hardware)
6. Certificate Manager → It manages SSL and TLS certificate
   It is known as ACM
7. Secret Manager → It manages secret by rotation.
   It is mostly used in RDS.
8. Artifact → It stores compliance documents
9. Gaurd Duty → It checks data from cloudTrail logs and other logs
   It protects from crypto currency attack.
10. Inspector → It provides automatic security
    It is mostly used for EC2, ECR and Lambda.
11. Config → It records configurations and changes over time.
12. Macie → It alert for sensitive data in cloud.
    It uses ML. The PII stands for Personal Identifiable Information
11. Security Hub → It is a central tool to manage security tools.
12. Detective → It quickly identify the root cause of security issue.
13. Abuse → It is use to report abusive/illegal stuffs.

Machine Learning

1. Rekognition → It is use to recognise using image/vedio
2. Transcibe → It converts audio into text.
   It can automatically remove PII.
   It supports multi-lingual
3. Polly → It converts text into audio
4. Translate → It is use for language translation.
5. Lex and Connect → It is the technology that power Alexa.
   It convert audio to text
   → It is a virtual contact center
6. Comprehend → It is a NLP that stands for Natural Language Processing
7. Sage Maker → It is use to build ML models
8. Forecast → It provides forecast based on historical data
9. Kendra → It can search data from documents
10. Personalize → It is a recommendation tool.
11. Textract → It scan text from image.

Advanced Identity.

1. STS → security Token Service
2. Cognito → It is identity for web and mobile application's user.
3. Microsoft Active Directory → It is a database of object on premise.
4. IAM Identity Center → It is also known as Single Signon.

Architecturing and Ecosystem

Well Architecture Framework → White Paper
Scalability, Disposable Resource, Automation, Loose Coupling, Serices

1. Operational Excellence → perform operation as code
   make frequent, small and reversible change
   manage failure
2. Security
3. Reliability
4. Performance Efficiency
5. Cost Optimization
6. Sustainability

Well Architecture Tool → workload

Customer Carbon Footprint Tool

Cloud Adoption Framework → White Paper
Business, People, Governance, → Business
Platform, Security, Operation → Technology

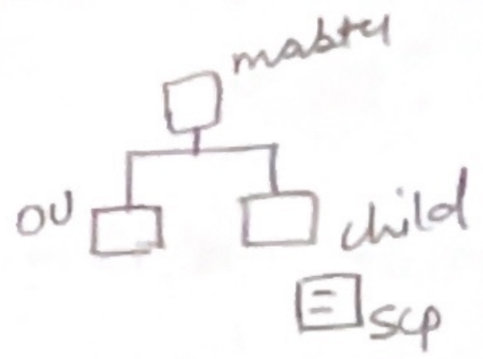
APN → AWS Patner Network
- Technology
- Training
- Consultancy

IQ → profession help

re:Post → community forum
knowledge center

Manage Services → support

Account Management, Billing and Support



account

1. Organization → global service
   manage aws accounts
   Consolidated bills
   aggregated usage
   The scp i.e Service Control Policy helps to restrict account privilege. It does not apply on master account.
   pooling of resources
   automate aws account creation
   multi account strategy

2. Control Tower → secure
   multi account creation
   automated

3. Resource Access Manager → share resources in multi account

4. Service Catalog → It is a self service portal
   It is a list of products.

Pricing

1. Pricing Model → Pay as you go
   save when you reserve
   pay less by using more
   pay less as aws grow
   The private IP cost less as compared to public IP.

2. Saving Plan → long term commitment on resources

3. Compute Optimizer → recommendation based on analysis using ML

Billing

1. Pricing Calculator → estimate
2. Billing Dashboard
   Cost Allocation Tag
   Cost and Usage Report
   Cost Explorer → saving plan / forecast
   } track
   Resource Group
   Tag Editor ←
3. Billing Alarm
   Budget
   } monitor
4. Cost Anomaly Detection → detect unusual spends using ML
5. Service Quotas → notify on exceed of threshold
6. Trusted Advisor → recommendation based on analysis
7. Support Plan → Developer, Business, Enterprise on Ramp, Enterprise, Basic
   29 100 5500 15,000 0
   1 hour 30 min 15 min 4.