→ Cloud Concepts.

Cloud Computing :- the practice of using a network of remote servers hosted on the Internet to store, manage and process data, rather than a local server or a personal computer.

Evolution of Cloud Computing.

(1) Dedicated server : one machine for a single job.

(2) Virtual Private Networks.
Dedicated to single business but machine is divided into sub-machines.

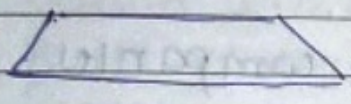
(3) Shared hosting.
eg. Godaddy.
one machine shared by hundreds of businesses.

(4) Cloud Hosting.
Multiple machines for multiple services.

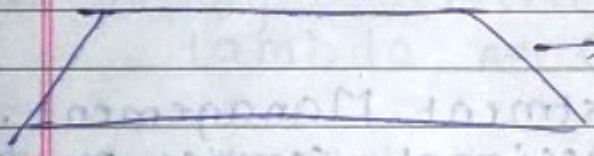
* HISTORY — Launched in 2002.

Types of Cloud Computing.

→ (Saas) Software as a Service.
→ A product run & managed by service provider.
→ Salesforce, Gmail, Office 365



→ (Paas) Platform as a Service.
→ Focus on deployment & management of your app.
→ EBS (elastic beanstalk)



→ (Iaas) Infrastructure as a service.
→ Basic building blocks for cloud IT
→ provide access to networking features, computers & data storage space.
→ Azure, GC, Aws.

→ Cloud Computing Deployment Models.

1. Public cloud - everything built on CSP.
2. Private Cloud - Everything built on company's data centers. 'Open-stack'
3. Hybrid : Using both On-Premises & A cloud service provider.
4. Cross Cloud : Multi cloud Providers.

Amazon Eks ←→ Azure Arc ←→ GCP Kubernetes engine.

5. Stop spending money on running & maintaining data centers.

6. Go global in minutes :- Deploy your app in multiple regions around the world in few clicks.

* Seven advantages to cloud.

1. Cost effective :- Pay as you go.
2. Global : launch workloads anywhere in the world. Just choose a region.
3. Secure :
4. Reliable :- Data backup, disaster recovery, data replication, fault tolerance.
5. Scalable
6. Elastic :- Automate scaling during spikes and drop in demand.
7. Current : The underlying hardware & managed software is patched, upgraded & replaced by cloud provider w/o interruption to you.

* AWS Global Infrastructure.

→ Globally distributed hardware & data centers that are physically networked together to act as one large resource for the end customer.

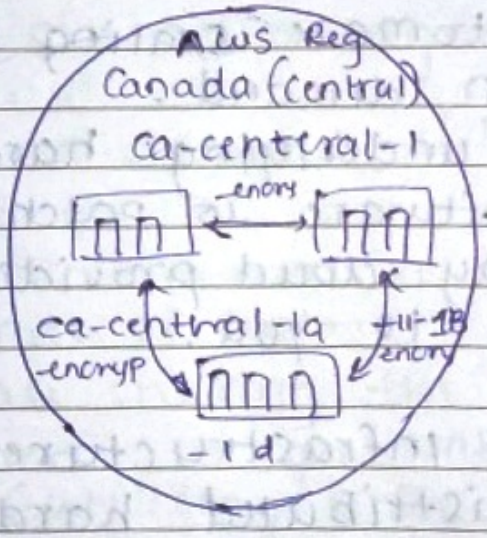
→ 25 Launched regions, 81 Availability zones, 108 Direct connection loc, 275+ points of presence, 11 local zone, 17 wavelength zone.

* Region vs Global services.

Regional services :-
if you want a service from canada you will set the region and this will lanch service there.

Global services :-
Some services are globally available everywhere.
S3, Cloudfront, Route53, IAM

* Availability zone (AZ) is physical loc made up of one or more datacenter.



* Selecting regions & AZ.

Fault tolerance

→ Fault domain is a section of a network that is vulnerable to damage if a critical device or system fails. The purpose of fault domain is that if a failure occurs it will not cascade outside that domain, limiting the damage possible.

Fault level - A fault level is a collection of fault domains.

The scope of a fault domain could be:

1. specific servers in a rack.
2. an entire rack in a datacenter.
3. an entire room in a datacenter.
4. the entire data center bu

It's upto the cloud service providers to define the boundaries of a domain.

Fault level
us-east-1 (Region)

Fault Domain	Fault Domain
us-east-1a (AZ)	us-east-1b (AZ)
↖	↗
This won't affect this	

Global Infrastructure.

* Amazon CloudFront : Content Delivery Service (CDN).
  → you point your website to CloudFront so that it will route requests to nearest Edge locations cache.
  → Allows you to choose an origin (such as a web-server or storage)

* Amazon S3 Transfer Acceleration -
  → Allows you to generate a special URL that can be used by end users to upload files to nearby edge locations. Once the file is uploaded to an edge location, it can move much faster within the aws network to reach S3.

* AWS Global Accelerator : can find optimal path from end user to your web-servers. They are deployed within Edge locations so you send user traffic to an edge location instead of directly to your web-application.

* AWS direct connect is a private / dedicated connection between your datacenter, office, co-location & AWS.

AWS Wavelength zones :- allows for edge-computing on 5G Networks. Applications will have ultra-low latency being as close as possible to the users.

→ Data Residency :- The physical or geographical location of where an organization or cloud resources reside.

→ Compliance Boundaries ?
→ where data or cloud resources are allowed to reside.

* AWS Outposts :- Physical rack of servers that you put in your data centr.

* AWS configs :- Policy as a code service You can create rules to continuous check AWS resources configuration.

High Availability.

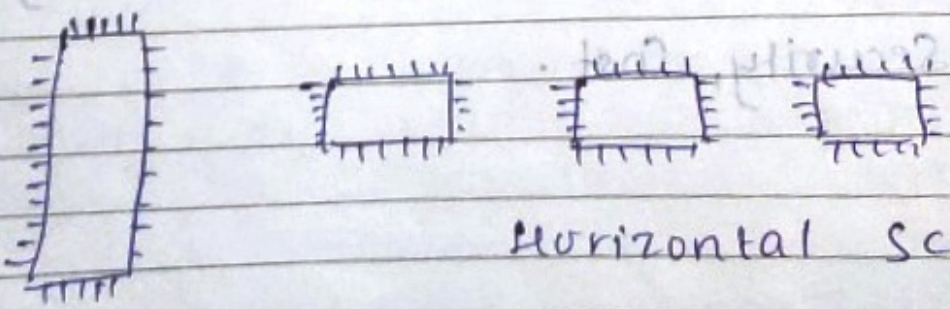
→ To ensure your service remain available by ensuring there is no single point of failure.

Running your workloads accross multiple AZ ensures that if 1 or 2 AZs become unavailable your service / application remains available.

* **Elastic load Balancer.**
allows you to evenly distribute traffic to multiple servers in one data center. If a data center becomes unavailable the load balancer will route the traffic to only available datacenters with servers.

High scalability → increase your capacity.

Vertical scaling



Horizontal Scaling

Upgrade to bigger server

server of same size.

High Elasticity.
→ automatically increase or decrease the capacity.

* [Auto scaling Groups (ASG)]: aws feature that will automatically add or remove servers based on scaling rules you define.

Fault Tolerance.
→ no single point of failure.
→ to have a copy of your database incase of fail over occurs

* [RDS Multi-AZ] is used.

High Durability:
→ to recover from disaster & to prevent loss of data

* [Cloud Endure]

→ Business Continuity Plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in services.

* Recovery Point Objective (RPO) → How much data are you willing to loose?
* Recovery Time Objective (RTO) → How much time are you willing to go down

Disaster Recovery Option.

(1) Backup and Restore.
RPO / RTO
Hrs.
You backup your newdata and restore it to new infrastructure.

(2) Pilot light.
RPO / RTO
10 minutes.
Data is replicated to another region with minimal servic running

(3) Warm Standby.
RPO / RTO
minutes.
Scaled down copy of your infra ready to scale up.

(4) Multi-site (Active/Active)
RPO / RTO
real time.
Scaled up copy of your infra in another region.

RTO :- Maximum acceptable delay between interruption of service and restoration of service.

RPO :- Maximum acceptable amount of time since the last data recovery point.

AWS API (application programming interface).

is

→ an API software that allows two applications or services to talk to each other. Most common → HTTP/s

* ARN - Amazon Resource Name.

* AWS CLI (command line interface). AWS CLI processes commands to a computer program in the form of lines of text.
  OS implement CLI in a shell.

* Terminal - is text only interface.

* console - physical computer to physically input information into a terminal.

* Shell - command line program that users interact with to input commands.
  * Bash * Zsh * Powershell.

EC2 - Virtual Server.

* Deployment models of Cloud Computing

1) Cloud based deployment.
→ Run all the parts of application in the cloud.
→ Migrate existing applications to the cloud
→ Design and build new applications in the cloud.

* 2) On-premises deployment.
→ Deploy resources using virtualization and resource management tools.
→ Increase resource utilization by using application management & virtualization technologies.
→ Also known as private cloud deployments

3) Hybrid deployment.
→ Connect cloud-based resources to on-premises infrastructure.
→ Integrate cloud-based resources with legacy IT infrastructure applications.

* Trade upfront expense :- refers to data centers, physical servers & other resources that you would need to invest in before using them.

Types of EC2:
General purpose → web servers, Code Rep
Compute optimized → Gaming, Sci Modell
Memory optimized → Memory (to load large amt of data before running an app)
Accelerated Computing → No. calculati
Storage Optimized → stored data.

Generdl Purpose instances.
→ provide a balance of compute, memory, and networking resources.
- eg. app servers, gaming, backend, small & medium databases

Storage optimized instances
→ IOPS req → input data → output

Accelerated computing instances
→ Graphic applications, game streaming, application streaming.

Amazon EC2 pricing.
→ On-demand. per hr / per sec.
→ Saving plan (72%) one yr / 3 yrs.
→ Reserved instances → predictable usage
→ 75% dis.

→ Spot instances - 90% off On-demand
- aws can reclaim

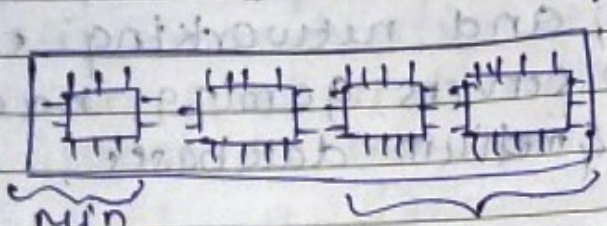
→ Dedicated hosts - nobody can share tendency of that host. Most expensive.

* Scaling Amazon EC2.

Amazon EC2 Auto scaling

(a) Dynamic scaling - Respond to changing demand.

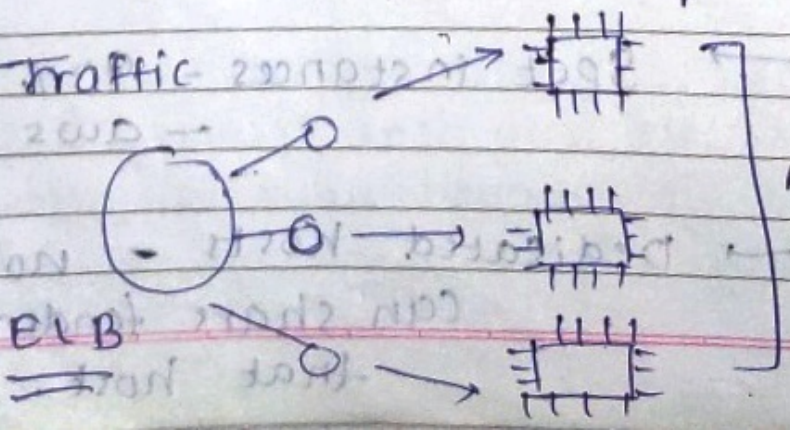
(b) Predictive scaling - schedule the right no. of EC2 instances based on predicted demand.



* Directing traffic with Elastic Load Balancer.
(causing uneven distribution).

Host → let's you know where to proceed.

ELB → Route Req → to process req.



* Messaging and ~~Queuing~~ Queuing.

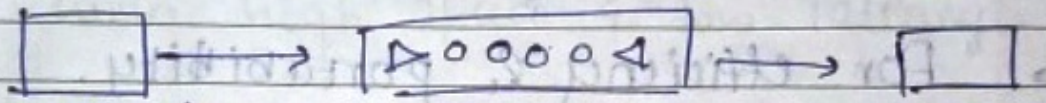
1) Tightly coupled Architecture.

A ——sends——→ B.

if

B fails, A fails.

2) loosely coupled Architecture.



* Amazon SQS (simple Queue Service)
* Amazon SNS (simple Notification Service).

→ Send, store, receive messages.
→ Send msgs as well as notifications

* Monolithic applications and Microservices

↓ Tightly coupled

↓ loosely coupled.

→ Additional Compute services.

(Serverless Applications)

AWS lambda : upload your code.
→ Triggered → Runs your code.

Auto scalable, Highly flexible, reliable.

Run time ≤ 15 mins.
Quick processing.

→ For efficiency & portability.

(i) ECS → Elastic Container Service.
EKS → Elastic kubernetes Service

Container : A package of your code.

* EC2 → Host traditional applications.
→ Full access to the OS.

AWS lambda → Host short running functions
→ Service-oriented applications.
→ Event-driven
→ Don't want to manage servers

Container based → AWS ECS or AWS AKS
↓
then choose EC2 that you manage or
Serverless AWS Fargate that manages for you.

Global Infrastructure & Reliability.

key factors to choose a region.
(i) Compliance.
(ii) Proximity.
(iii) Feature availability.
(iv) Pricing.

Edge locations:

Amazon CloudFront - Helps delivery of data, images, videos to customers with high speed & low latency.

An edge location is a site that amazon CloudFront uses to store cached copies of your content closer to your customers for faster delivery

* AWS Management Console.
  → Test environments.
  → View AWS bills.
  → View Monitoring.
  → Work with non-technical resources

* AWS Command Line Interface (CLI).
  → Allows you to make API calls using the terminal on your machine.

* AWS Software Development kits (SDKs).
  → Allows you to interact through various programming language.

* AWS Elastic Beanstalk.

→ You provide code & configuration settings, & elastic beanstalk deploys the resources necessary to perform following tasks.

- → Adjust capacity.
- → Load balancing.
- → Automatic scaling.
- → Application health monitoring.

* AWS Cloud Formation.

→ You can treat your IaaC. means you can build an env by writing lines of code instead of using the AWS Management Console.

Networking.

Amazon Virtual Private Cloud. (VPC).

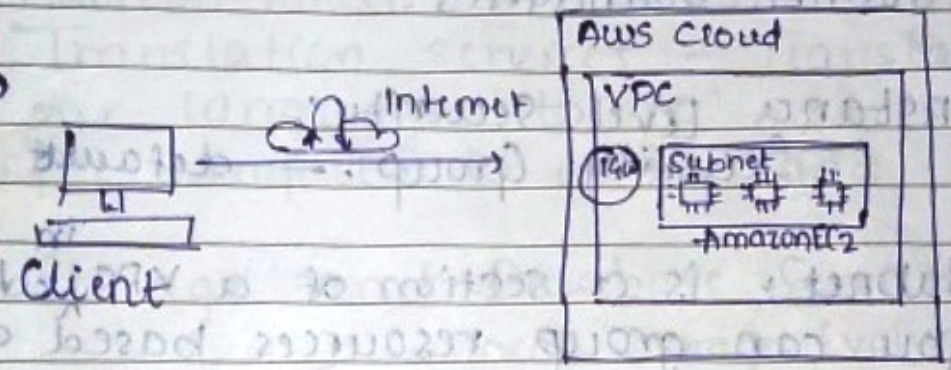
→ Let's you provision a logically isolated section of the aws cloud where you can launch aws resources in a virtual network that you define.

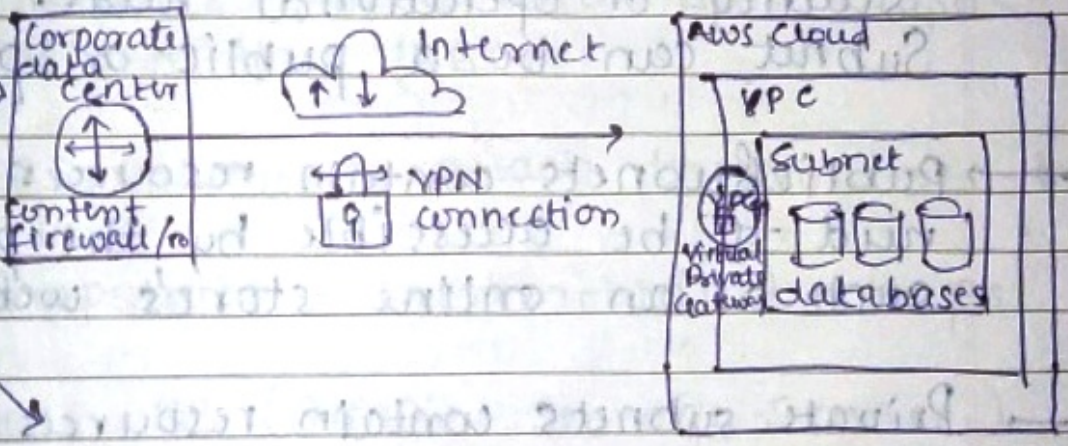
Subnets: Chunks of IP address in your VPC that allows you to grp VPC together.

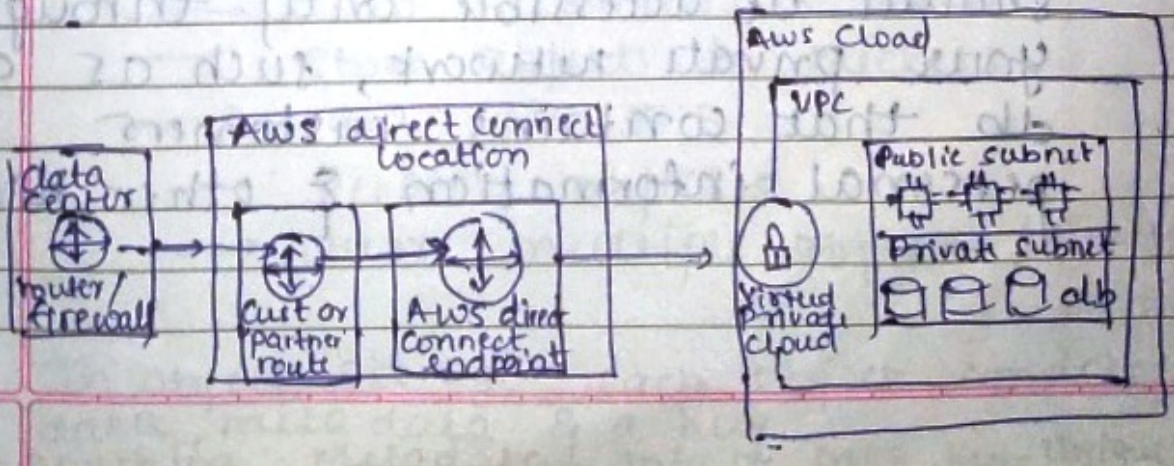
(Publicly) Internet Gateway (IGW) → Gateway to allow traffic to move on to your ~~networ~~ resources.

Virual Private Gateway (VPC) for Private (VPN) Door

→ AWS Direct Connect :- Completely private direct connection from your datacenter to aws.







Connectivity to aws -

* Subnets & network access control list.

Network hardening.

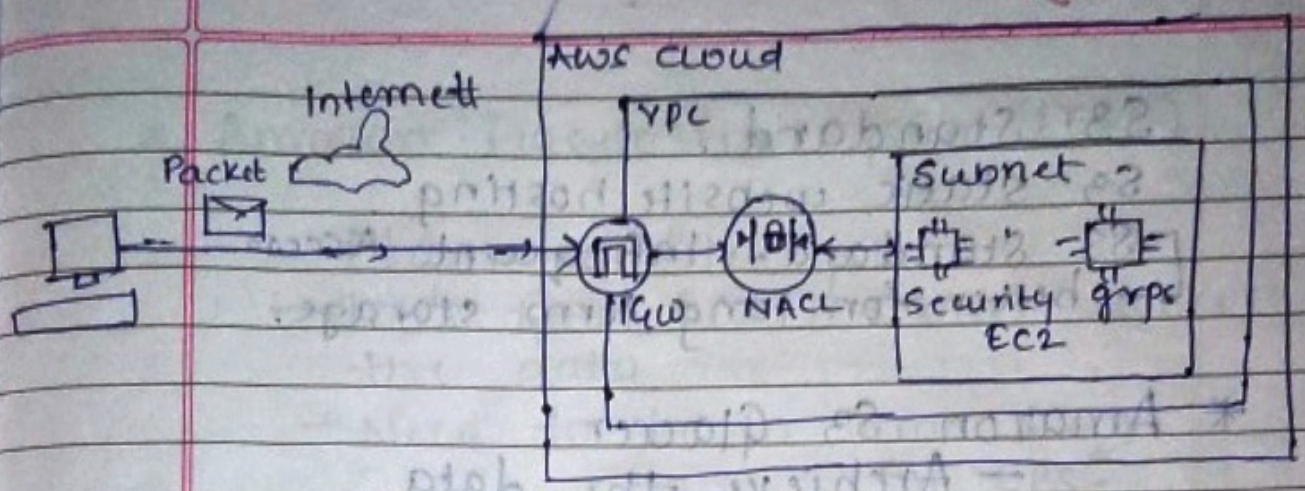
Network Access Control List (ACL) :-
- checks whatever is entering.
Validates a package only if it crossed subnet boundaries.

* Instance level security :-
Security Group :- default.

Subnet : is a section of a VPC in which you can group resources based on security or operational needs.
Subnet can be a public or private one.

→ Public subnets contain resources that need to be accessible by the public, such as an online store's website.

→ Private subnets contain resources that should be accessible only through your private network, such as a db that contains customers personal information & other histories



GLOBAL NETWORKING.

Amazon Route 53 - Domain Name Service - Translation services - Translating our languages to ip addresses for computer to understand

* Storage and Database Services.
  1. Instance stores and Aws Elastic Block Store (EBS) → local storage (volume).

     EBS volumes - attach the volumes to EC2
     ↓
     Snapshots - incremental backups

  2. AWS S3 (Simple storage Service).
     → data is stored as objects.
     → store objects in buckets.
     → max size 5TB.
     → version objects
     → create multiple ~~objects~~ buckets.

In object storage, each object consists of data, metadata & a key
* Data - Anything, metadata - info of data, key - Unique Identifi

S3 standard.
S3 static website hosting.
S3 standard - Infrequent Access
↳ better for long term storage.

* Amazon S3 Glacier:
  - Archieve the data.

* Amazon S3 Lifecycle Policy:
  Moves data automatically between tiers.

AWS EBS vs S3

1. EBS - sizes upto 16TiB.
   - Survive termination of the EC2 instance
   - Solid state by default
   - HDD Options
2. S3 - Unlimited Storage.
   - Individual objects upto 5 TBs.
   - Write once / read many.
   - 99.999999999 % durable.
   - web enabled

* Amazon Elastic File system (EFS).

- Managed file system.
- Let's ~~you~~ EC2 instances access the data.
- Need to be in same AZ for EBS.
- Regional resource.

* Amazon RDS. (Relational Db Service)
  - → Automated patching.
  - → Backups.
  - → Redundancy.
  - → Failover.
  - → Disaster Recovery.

Amazon Aurora.
PostgreSQL
MySQL
Maria DB
Oracle DB
Microsoft SQL Server.

} Amazon RDS database engines.

* Amazon Dynamo DB.
  - serverless.
  - A non relational db - NOSQL.
  - Purpose built.
  - Fully managed.
  - Highly scalable.

RDS VS DynamoDb.

1) RDS
- Automatic high availability
- recovery provided.
- A customer owner of data.
- customer owner of schema.
- customer owner of network.

2) Dynamo DB
- Key-value pair.
- Massive throughput capabilities.
- PB size potential.
- Granular API access.

* Amazon Redshift.
- Data warehousing as a service.
- Massively scalable.
- Used for Big Data Analytics.

* Aws Data Migration Service (DMS).
- Migrate existing db to cloud.

* Amazon Document DB
  - document db service that supports MongoDb workloads.

* Amazon Neptune.
  - Graph based Db service.
  - build & run apps that work with highly connected datasets, such as recommendation engines, fraud detection, & knowledge graphs.

* Aws Quantum ledger Db (QLDB)
  - review a complete history of all the changes that have been made to your application data.

SECURITY

* Shared responsibility model.
  Aws → Security of the cloud
  Aws → Protect the cloud
  Customer → Protect what is in the cloud

* User permissions and access.

  (IAM) → Identity Access Management.

AWS Organizations.

- centralized management.
- consolidated billing.
- hierarchial groupings of accounts.
- AWS services & API actions access control.

* Compliance.

AWS Artifact - gain access to compliance reports documented by third party.
Provides on-duman access to AWS security & compliance report distributed

* DDOS (Denial of Service ~~Attacks~~).

For low level network attacks
→ like UDP flood attacks - Security groups.

→ Slow loris attack - Elastic load Balancer.

→ for sharpest attacks - AWS shield with AWS WAF.

Amazon Inspector.
→ Helps improve security.
→ exposure of EC2 instances.

Amazon Guard duty.
→ Threat detector.

→ runs automated security assessments
→ checks vulnerabilities

MONITORING AND ANALYSIS

* Monitoring - Observing systems, collecting metrics, & then using data to make decisions.

Amazon Cloudwatch.
→ Monitor aws infrastructure & applications you run on aws.
→ Health checks.
→ Integrated by SNS.

Benefits :- (i) access to all your access.
(ii) visibility across your applications
(iii) drive insights to optimize applications.

Amazon CloudTrail:
→ Every req made to aws gets logged in CloudTrail engine.
→ records api calls for your account.

* AWS Trusted advisors.
→ Cost Optimization.
→ Performance.
→ Security.
→ Fault Tolerance.
→ Service limits.

PRICING AND SUPPORT.

AWS Free Tier.

Aws pricing Calculator.
→ Let's you explore AWS services & create an estimate for the cost of your use cases on Aws.

Cost Explorer.
→ Explore where are you spending money!
→ Enables you to visualize, understand & manage your AWS costs & usage over time.

Five pillars of the well-Architected framework.

→ Operational Excellence.
→ Security.
→ Reliability.
→ Performance Efficiency.
→ Cost Optimization.
→ Sustainability.

Migration & Innovation.

* AWS Cloud Adoption framework (CAF).

→ Business, People & Governance perspectives focus on business capabilities.

→ Platform, Security & Operations perspectives focus on technical capabilities.

Migration Strategies.

(i) Rehosting - lift & shift. ← few cloud optimizati
(ii) Replatforming - lift tinker & shift.
(iii) Retire - removing apps no longer needed
(iv) Retain - keeping apps that are critical for business in source env.
(v) Repurchasing - moving to brand new
(vi) Refactoring - reimagining how an application is architected

AWS Snow Family.

~~AWS Snowcone~~. Snow Family - collection of physical devices that help to physically transport upto exabytes of data into & out of aws.

(i) AWS Snowcone - small, rugged & secure edged computing & data transfer device.
Features 2 CPUs, 4GB of memory, 8 TB of usable storage.

(ii) AWS Snowball : offer two types of devices.
(a) Snaball Edge Storage Optimized
- large scale data migration

(b) Snowball Edge Compute Optimized
- Provides powerful computing resources for use case such as ML, full motion video analysis & local computing stacks.

Innovation with AWS.

→ Amazon SageMaker - Quickly build, train & scale ML moduls or build custom moduls

→ Amazon Augmented AI (Amazon 2AI)
ML platform.

→ Amazon Lex.
Heart of Alexa
Helps build interactive chatbots

→ Amazon Textract.
Extracting text & data.

→ Amazon DeepRacer.
Reinforcement Learning

→ AWS Ground station.
Access Satellite.

→ AWS Transcribe.
Convert Speech to text.

→ AWS Fraud Detector.
Fradulent activities.

Well-Architected Framework:

→ 5 Pillars.

(i) Operational Excellence.
- focuses on running & monitoring systems.

(ii) Security.
- checks integratity of data & protecting systems by encryption.

(iii) Reliability.
- recovery planning.

(iv) Performance Efficiency.
- using resources efficiently.

(v) Cost Optimization.
- Optimizing forecost.

Six advantages of cloud computing :

→ Trade upfront expense for variable expense
→ Benefit from massive economies scale
→ Stop guessing capacity.
→ Increase speed & agility.
→ Stop spending money running & maintaining data centers.
→ Go global in minutes.

* AMAZON CLOUDFRONT.

→ is a web service that speeds up the distribution of your static & dynamic web content, such as .html, .css, .js & image files to your users. cloudfront delivers your content through a www network of data centers called edge locations.

* AMI (Amazon Machine Image).

→ Provides the information required to launch an instance, which is a virtual server in the cloud.
→ You specify an AMI when you launch an instance, & you can launch as many instances from the AMI as you need.

* AWS (DMS) – Data Migration Service

* AWS Trusted Advisor.

(i) Cost Optimization.
(ii) Performance.
(iii) Security.
(iv) Fault Tolerance.
(v) Service limits.

* Adv that Enterprise Support cust receive
→ Access to a Technical ~~Service~~ Account Manager.

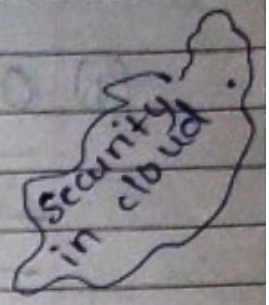
* Components of Total Cost for Technology
→ Hardware acquisition
→ Software acquisition
→ Infrastructure.
→ Downtime.
→ Installation.
→ Maintenance.
→ Training
→ Support
→ Space
→ Electricity.

* Cost Management tools
→ Billing Dashboard
→ Cost Explorer.
→ Cost Usage and Report.

Shared Responsibility Model.

Customer Responsibility

Customer Data
Platform, Apps, IAM
OS, Network and Firewall Configuration



Client side Data Encryption & Data Integrity Auth

Server Side Encryption (File Sys and data)

Network traffic Protection

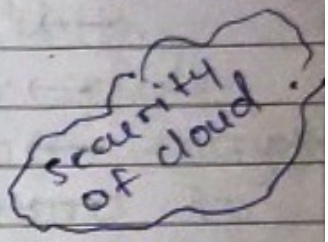
AWS Responsibility

AWS Foundation Services

Compute Storage Database Network

AWS Global Infrastructure

Regions AVZ Edge locations



→ All new buckets are Private.
→ logging per req can be turned on a buc
→ Log files are generated & stored in different bucket.
→ Access controls is configured using Bucket Policies & ACL's.

S3 Encryption.

In transit → SSL/TLS.

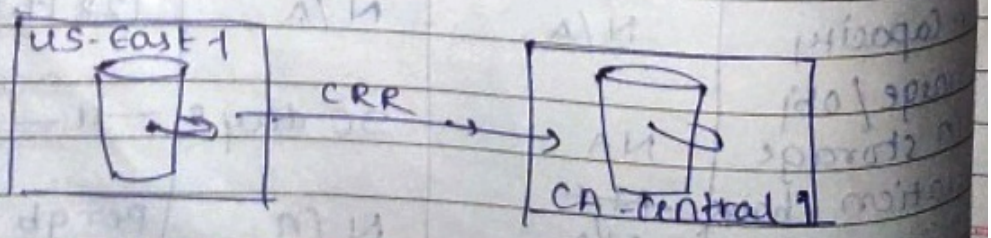
Server side Encryption (SSE)- Encryption at Rest.

amazon manage all keys
- SSE - AES → algo
- SSE - KMS → key management servi
- SSE - C → customer provide key.

Client side encryption (CSE):
→ You encrypt your own files before uploading them to S3.

S3 Cross Region

When disaster takes place, we can turn on CRR of source region to destination region to save our data.



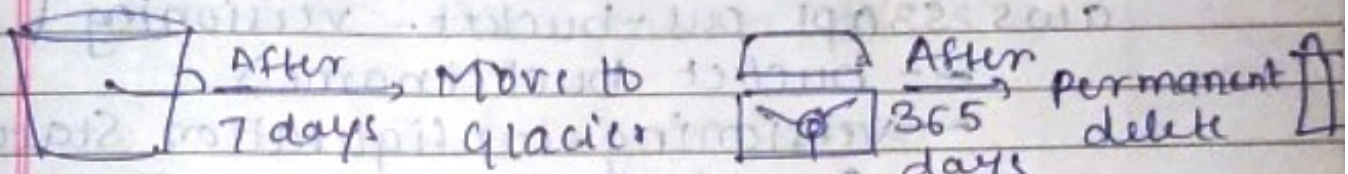
Turn on Versioning.

S3 Versioning

→ Store all versions of an object in S3.
→ Once enabled, cannot be disabled only suspended on the bucket.
→ Get any version of file you want.

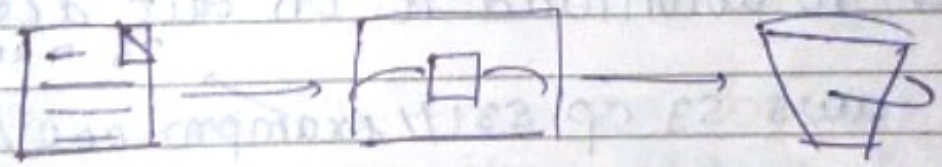
S3 Lifecycle Management.

* Automates the process of moving objects to different storage classes.
* Can be used with versioning.



S3 Transfer Acceleration.

As data arrives at the Edge location it is automatically routed to S3 over a specially optimized path.



S3 - MFA Delete

→ MFA delete ensures users cannot delete objects from bucket unless they provide their MFA code.

* AWS CLI must be used to turn on MFA
* Bucket must have versioning turned on.
* Only Bucket owner logged in as Root user can Delete objects from bucket.

```
aws s3api put-bucket-versioning \
--bucket bucketname \
--versioning-configuration Status=
    Enabled, MFADelete = Enabled \
--mfa "your_mfa_serial-number
      mfa-code" \
```

* For accessing private files :-

→ To download it on our desktop.

```
aws s3 cp s3://exampro-000/enterprise-d
                ↑ s3 name of bucket      ↓ name of folder
/barclay.jpg ~/Desktop/barclay.jpg
↓ name of image
```

S3 Bucket Policies

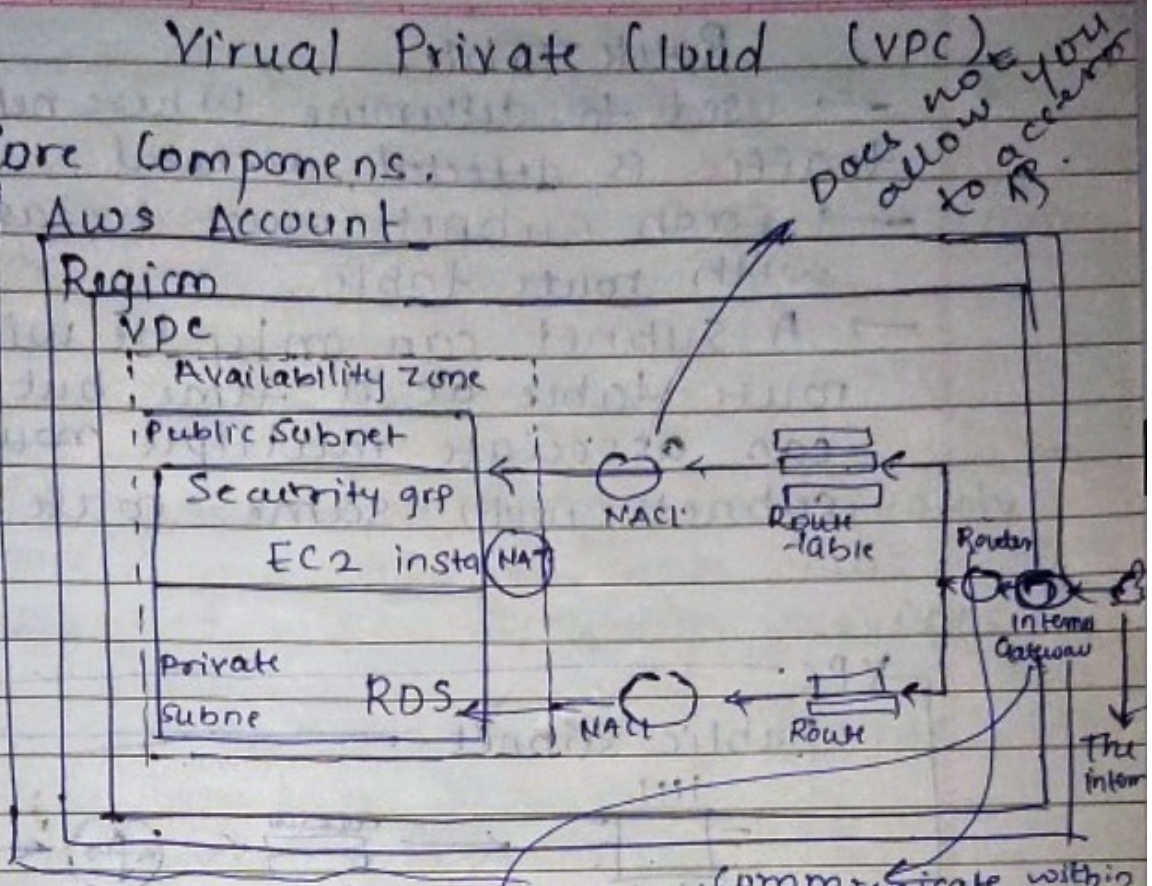
>> Bucket >> Permission >> Policies
>> Policy Generator

→ S3 has 6 Storage classes.
* Standard
* Intelligent Tiering.
* IA
* One Zone IA.
* Glacier
* Glacier Deep Archieve.

VPC is a logically isolated section of Aws where you can launch your own resources & network

Virual Private Cloud (VPC)

Core Components:



Communicate outside of AWS to the internet

Communicate within subnets

- Internet Gateway
- Nat Gateway
- VPN
- Customer Gateway
- Routing tables etc.
- VPC endpoints.
- VPC Peering.

* VPC Peering:

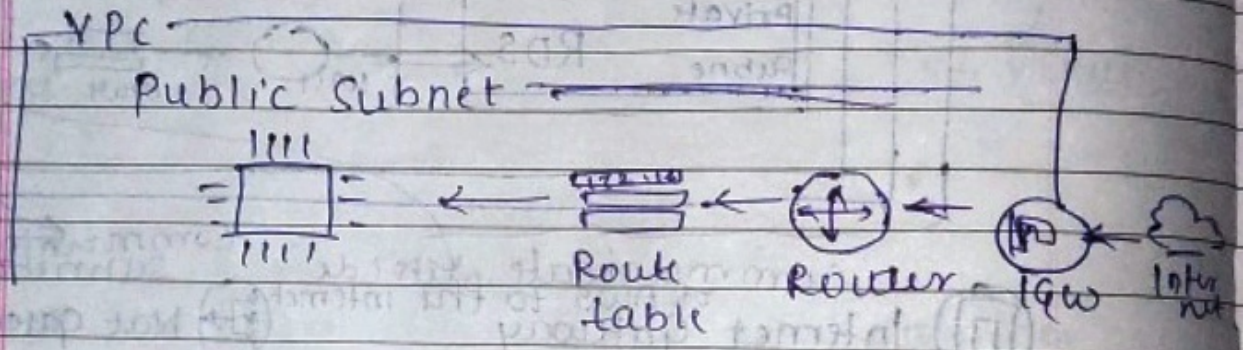
→ Allows you to connect one VPC with another over a direct network route using private IP addresses.

→ Star connection.

1 central VPC - 4 other VPC's.

Route Table.

→ used to determine where network traffic is ~~directed~~ directed.
→ Each subnet must be associated with route table.
→ A subnet can only be with one route table at a time but you can associate multiple ~~route tables~~ subnets with same route table.



* Bastions / Jumpbox

→ Bastions are EC2 instances which are security harden. They are designed to help you gain access to your EC2 instances via SSH or RCP. That are in a privat subnet.
→ Also known as Jumpboxes.

Direct Connect.

→ Dedicated network connection from on-premises location to AWS

VPC Endpoints.

VPC Endpoints allow you to privately connect your VPC to other AWS services, VPC endpoint services.

There are 2 types of VPC Endpoints.
1. Interface Endpoint.
2. Gateway Endpoint.

→ Helps you keep traffic within AWS network.

VPC Flowlogs.

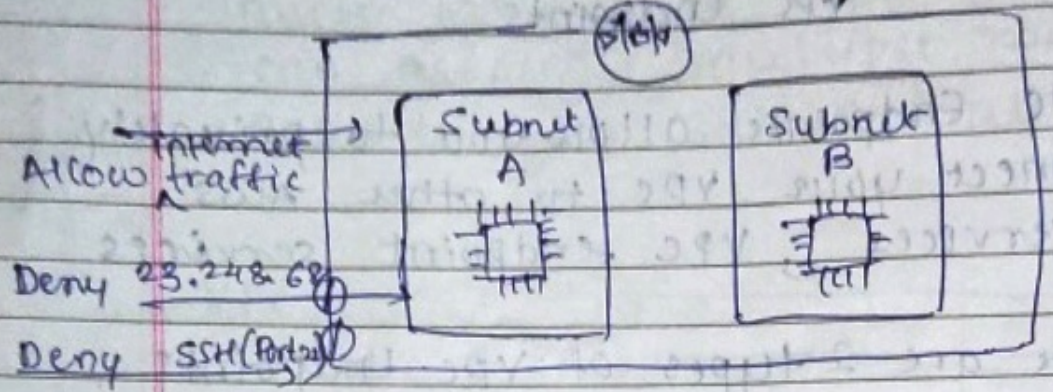
→ Allow you to capture IP traffic information in-and-out of Network Interfaces within your VPC.

Flow logs
VPC can be created for
(i) VPC (ii) Subnets (iii) Network Interface.

→ All log data is stored using Amazon Cloudwatch logs.
→ After a flow log is created it can be viewed in detail within Cloudwatch logs.

* Network Access Control List. (NACL's)

An (optional) layer of security that acts as a firewall for controlling traffic in & out of subnets.



SECURITY GROUPS:

A virtual firewall that controls the traffic to & from EC2 instances.

Type: SSH, Protocol: TCP, Port = 22, Source: My ip:

→ You can have 10,000 security grps in a region (default is 2,500).
→ You can have 60 inbound rules & 60 outbound rules per security grp.

* NAT (Network Address Translation)
(NAT) method of re mapping one IP address space into another.

→ Nat instances vs NAT Gateways.

NAT instances (legacy) are individual EC2 instances.

NAT Gateways is a manage service which launches redundant instances within the selected AZ.

* IAM (Identity Access Management)

Manages access of AWS users & resources.

→ Core components :-

1. Users :- End users who log in
2. Groups :- group of users
3. Roles :- Associate permissions to a Role & then assign this to an user or grp.
4. Policies :- JSON document which grant permission for specific users, groups, or role to access services.

Types of policies.

1) Managed Policy -
Created by AWS
You cannot edit

2) Customer Managed Policies -
Created by Customer
Editable.

3) Inline Policy -
Policy which is directly attached to the user.