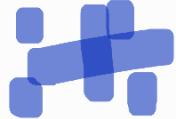
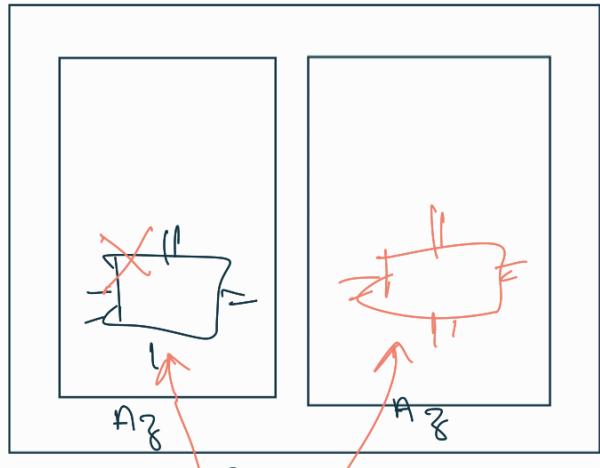


## Six Advantages of cloud Computing :-



- ① Trade capital expense (CAPEX) for operational expense (OPEX)
  - ↳ pay on-demand; don't own hardware.
  - ↳ Reduced Total Cost of ownership (TCO) & operational expense (OPEX).
- ② Benefit from massive economies of scale.
  - ↳ prices are reduced as AWS is more efficient due to large scale.
- ③ Stop guessing capacity.
  - ↳ Scale based on actual measured usage.
- ④ Increase speed and agility.
- ⑤ Stop spending money running and maintaining data centers.
- ⑥ Go global in minutes.
  - ↳ Leverage the AWS global Infrastructure.

Fault - Tolerance = multi AZ = High Availability.



multi-AZ = High Availability  
= Fault Tolerance

Even if resource is on AZ fails, then entire process will fail.  
To solve this we have deploy multi AZ.

Agility = Innovative, Speed & Decentralized.

Summary — IAM :-

- IAM user — mapped to a physical user has a password on AWS console.
- Groups — contains IAM users.
- Policies — JSON Document that outlines permissions for users and groups.
- Roles — for EC2 Instances @ AWS Services (To do some Action).
- Security — MFA + Password Policy.

- virtual MFA device (Software). → produce token.
  - universal 2nd Factor (U2F) Security Key. → USB port.
  - Hardware Key For MFA Device }  
 &  
Hardware Key For MFA Device }  
 for AWS Cloud (us)
- Hardware  
MFA

Robot (Password) + MFA = Successful Login

↓  
Non-decrypt

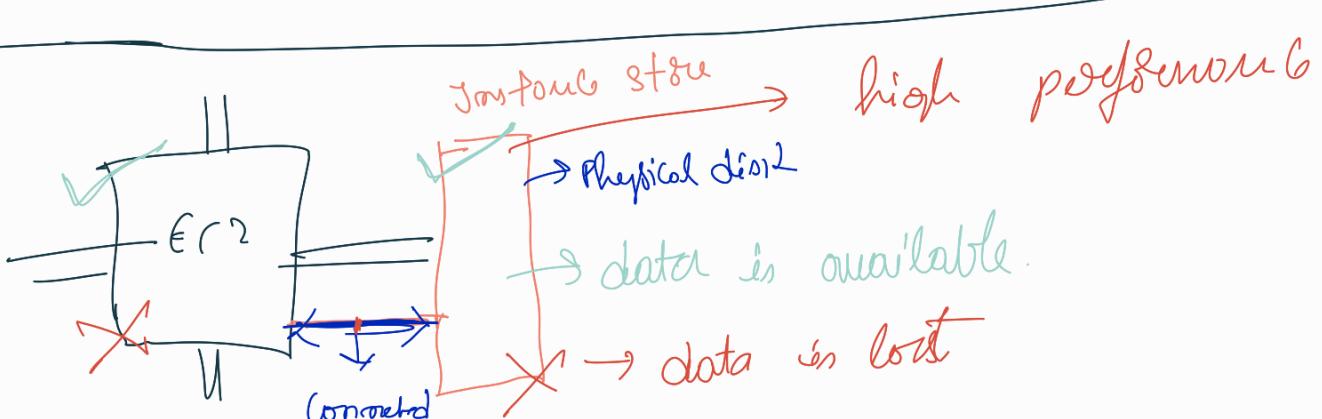
## EC2 → Summary :-

- EC2 instance = AMI (OS) + Instance Size (CPU + RAM) + storage + security groups + EC2 user Data.
- purchasing options :-

- on-Demand.
- Spot.
- Reserved (standard + Convertible + Scheduled)
  - ↳ no upfront (+).
  - ↳ partial upfront (++).
  - ↳ all upfront (+++).
    - ↳ you can change instance type.
    - ↳ 1yr & update to 3 yrs
    - ② change to on-demand

## EC2 Instance storage - Summary

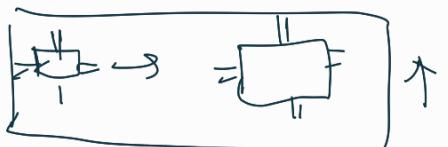
- EBS volumes -
  - m/w devices attached to one EC2 instance at a time.
  - within a AZ.
  - EBS Snapshots
    - ↓  
backups
    - ↓  
Transferring EBS volumes across AZ.
- AMI - Create ready-to-use EC2 with our customization.
- EC2 Instance store :
  - ↳ high performance n/w disk attached to our EC2 instance
  - ↳ lost our instance it will stop / terminate.
- EFS : N/w File System (NFS), can be attached to 100s of instances in a region.
  - EFS-IA : cost optimized storage class for infrequent accessed files.
  - FSx for windows : N/w File System for windows servers.
  - FSx for lustre : High Performance Computing Linux file system.



# High Availability & Scalability for EC2

- vertical scaling - increase instance size.

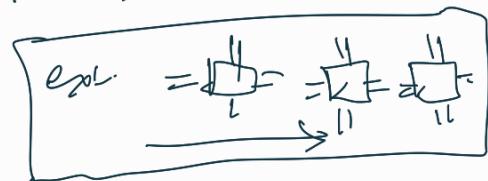
ex:-



from : t2.nano - 0.5GB of RAM, 1 CPU.  
to : t3.large - 8GB RAM, 4 CPU.

- Horizontal Scaling - increase no of instances.  
(= Scale out / Sm).

- Auto Scaling Group
- Load Balancer.



- High Availability - own instances for the same application across multi AZ.

- Auto Scale Group multi AZ
- Load Balancer multi AZ.

↓  
Fault Tolerant.

ELB - Distribute traffic across EC2 Instances, can be multi AZ.

- supports health checks.

- Application load Balancer - HTTP/HTTPS (layer 7).
- w/w load Balancer - TCP/UDP (layer 4).
- Gateway load Balancer - (layer 3).

ASG → Implement Elasticity for your applications across multiple AZ

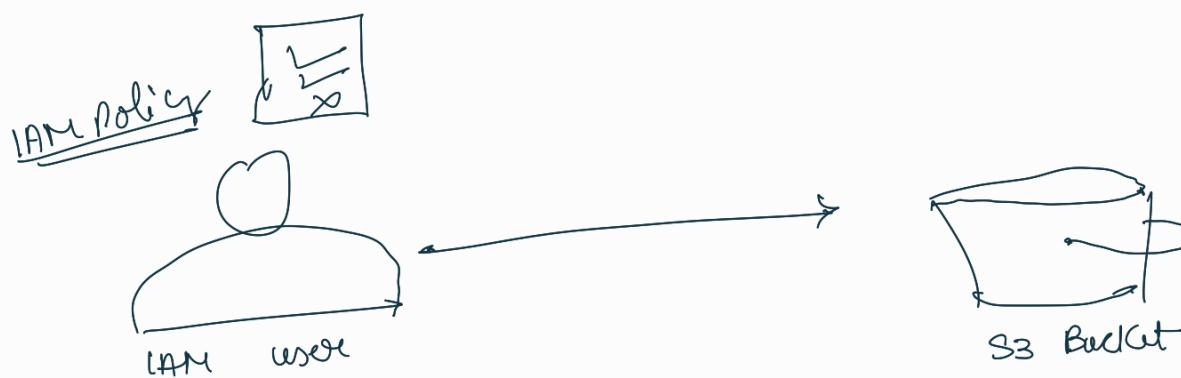
- Scale EC2 instance based on demand on your system, replace unhealthy.
- works with ELB.

## Amazon S3 - Summary

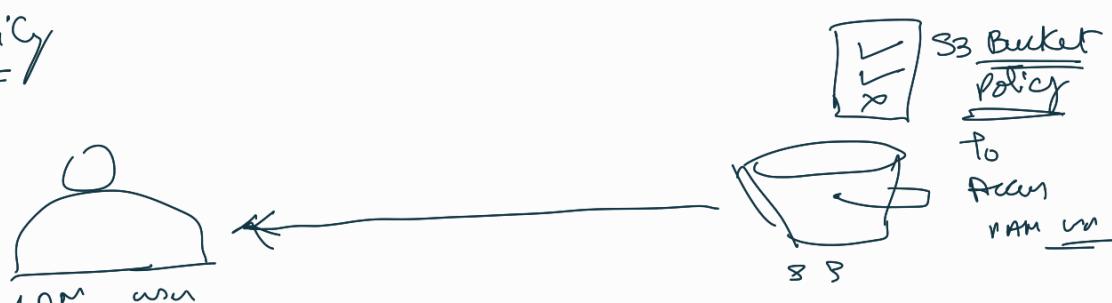
- Bucket - unlimited storage. } within a region.
    - ↓  
object - 5TB.
- ↳ if you are uploading more than 5GB into objects must use "multi-part upload"

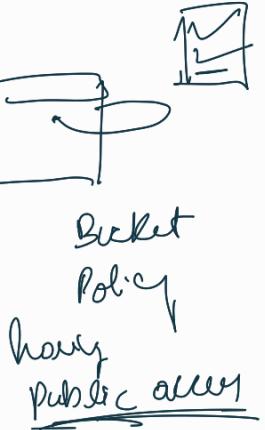
## S3 Security :-

### ① IAM policy



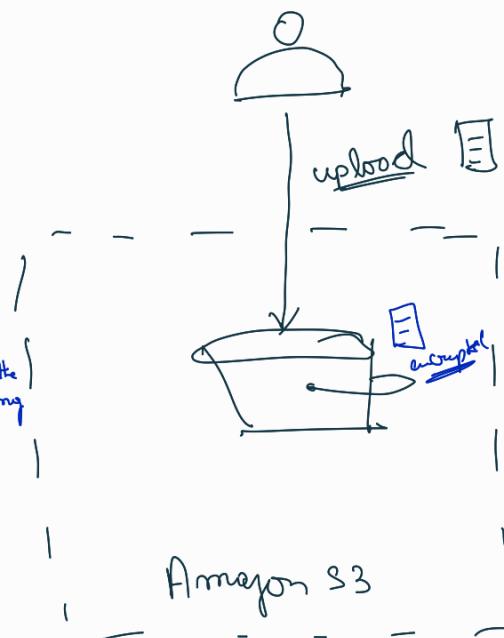
### ② Bucket Policy



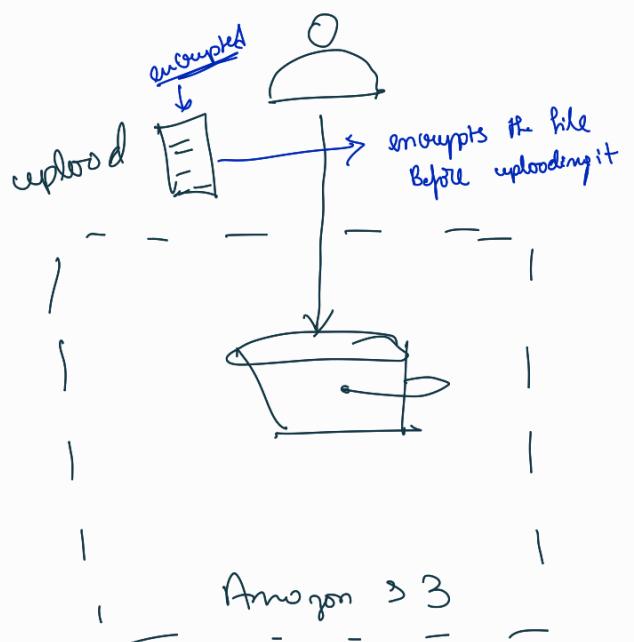


## → S3 Encryption :-

### Server-Side Encryption (Default)



### Client-Side Encryption



S3 - host static website on Amazon S3.

- S3 versioning - Prevent from accidental delete.
- S3 Replication - Same-region / Cross-region but for this versioning should enabled.

### S3 Storage classes :-

↳ Standard S3

↳ Amazon S3 Standard - Infrequent Access (S3 Standard - IA)

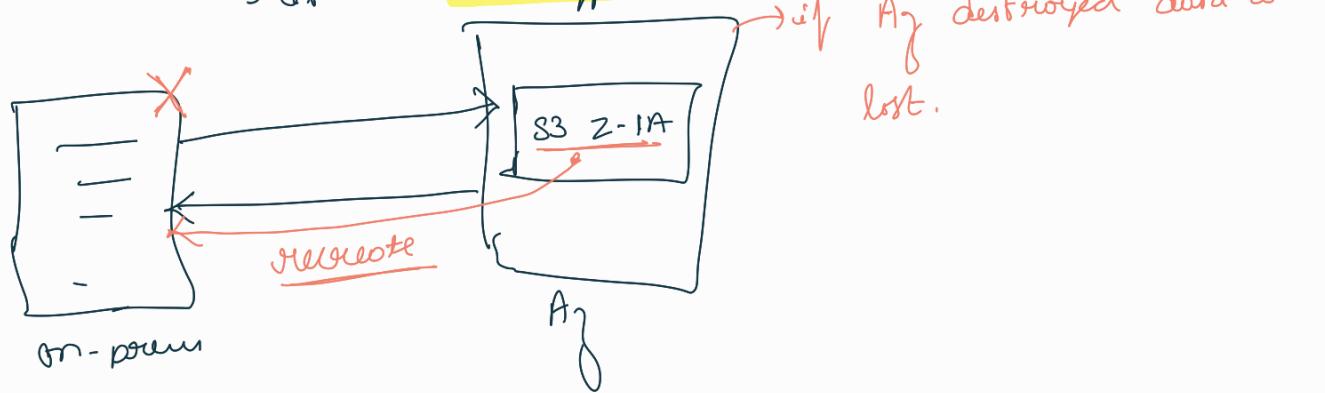
- deployed multi AZ - (High Available).
- use cases : Disaster Recovery, backups.

↳ Amazon S3 One-zone - infrequent Access (S3 one zone - IA)

- Single AZ. (data lost when AZ is destroyed).

- use cases : Storing secondary backup copies of on-premises data, data can recreate.

→ it is cost-effective compare to standard - IA.



### Amazon S3 Glacier Storage Classes -

S3 Glacier - data archive / backup

↓ pricing : price for storage + object retrieval cost.

S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
<ul style="list-style-type: none"> <li>• <u>Milli second</u> retrieval.</li> </ul>	<ul style="list-style-type: none"> <li>• <u>Expedited</u> : 1 to 5 mins.</li> <li>• <u>Standard</u> : 3 to 5 hrs.</li> <li>• <u>Bulk</u> : 5 to 12 hrs.</li> </ul>	<ul style="list-style-type: none"> <li>• Standard - 12 hrs.</li> <li>• Bulk - 48 hrs.</li> </ul>
Min storage duration is <u>90</u> days.	Min storage duration is <u>90</u> days.	Min storage duration is <u>180</u> days.

## S3 Intelligent - Tweeping

↳ More objects automatically b/w Access tiers based on usage.

exp: Standard - Glacier (your usage go long time)  
↳ cost-efficient

Snow Family: Import data onto S3 through physical device, edge computing. (also for very large amount of data).

Storage Gateway :- hybrid solution to extend

Bridges b/w on-prem on-prem storage to S3.  
data and cloud  
data in S3.

# Databases & Analytics - Summary

→ Relational Databases → RDS  
→ Aurora (MySQL & PostgreSQL).

- Multi AZ = High Availability.
- Read Replicas = Read only copy.

→ in-memory Database : ElastiCache.

→ DynamoDB - LowLatency, NoSQL, Seamless Database,  
Key/Value.

↳ Dynamo Accelerator (DAX) = Cache for DynamoDB.  
↳ in-memory.  
↳ Wx performance.

→ Redshift :- Data warehouse.

→ EMR :- Hadoop Cluster, Big Data,  
made of hundreds of EC2 Instances.

→ Athena :- Query data on S3 (SQL).

→ Quick Sight :- dashboards on your data,  
visualize.

→ Document DB - MongoDB (NoSQL Database).

Amazon QLDB - Financial Transactions Ledger.  
↳ Immutable Journal (can't change).  
↳ Cryptographically unforgeable Protections.

Amazon Glue :- Managed ETL  
( Extract Transform Load )  
Data Catalog Service.

OMS :- Database Migration.

Neptune :- graph database.

Docker : Container Technology to run applications.

↳ ECS - run Docker Containers on EC2 Instances.  
we have to manage our infrastructure

Fargate (serverless).  
↳ Run Docker Containers without provisioning  
the Infrastructure  
→ no need to manage.

→ ECR : private Docker Image Repository  
↳ storage in Docker containers.

→ Batch : run batch jobs on AWS owned  
managed EC2 instances.

batch jobs → fixed job start @ 9:00 AM  
and end @ 11:00 AM

→ Lambda : predictable & low pricing for  
Simple applications & DB tasks.

## handler - Summary

↓  
serverless Function as a Service.

Billing - no of request your function made & duration it takes for your code to execute.

max time - up to 15 minutes.

## Deployment - Summary

managing & provisioning our infrastructure by code/script instead of manual procedure.

→ CloudFormation - <sup>↑</sup> Infrastructure or code, almost all AWS services supports.  
• Repeat across Regions & Accounts



→ Fc2

SG

ALB

Route 53

①

we have to  
create each  
& everything.

②

using CloudFormation

↳ **Template**

↳ you can work  
a **code** such

Launches Fc2,  
ALB, SG, Route 53

why this  
template you can  
dependably launch  
your infrastructure  
in any Region ③ Accounts.

## → Elastic Beanstalk (Paas) :-

you can quickly deploy and manage applications in the AWS without having to learn about the infrastructure that you use.

It reduces the management complexity .. automatically handles the details of capacity, LB, scaling & health monitoring.

→ you can use any type languages / custom lang.

Ops works : managed chef & puppet in AWS

— please go through code commit, deploys pipeline, Build —

refer      notes.

Aws FleetPro :- provides on-demand downloads of Aws security and compliance documents such as

→ AWS ISO certifications.

→ Payment card industry (PCI) reports.

→ Service Organization Control (SOC) reports.

Point 53 :- Managed DNS (Domain Name System)  
↳ Monitors health.  
↳ Domain registration

## Routing Policies

- \* Simple Routing Policy - routing traffic to **single resource**.
- \* weighted Routing Policy - traffic to **multiple resources**.
- \* Latency routing policy - routing traffic to get **better performance / low-latency**.
- \* Failover Routing Policy - routing traffic to **active-active / resource primary - failover**.

CloudFront :- Content Delivery Network (CDN),  
(cache) - **Improve user experience (low-latency)**

S3 Transfer Acceleration :- **increase transfer speed by transferring file to an AWS edge location. (Global destination).**

## AWS Global Accelerator :-

Improves global application availability & performance using the AWS global network.

SQS :- Queue service is used to decouple app in AWS.

SNS :- Notification service sends messages through email, Lambda, SQS, SMS.

Kinesis :- real-time data streaming.

Amazon MQ :- Managed message broker.

CloudWatch :- monitor the performance of AWS services.

↳ Alarms : automate notification, perform EC2 action.

↳ logs : collect log files from AWS services.

CloudTrail :- audit API calls made within your AWS account.

X-Ray :- trace requests made through your applications.

Aws Health Dashboard :- Status of all Aws services across all regions.

Aws Account Health Dashboard ; personalized view, view impact on your Infrastructure.

Amazon Code Review → review & Improve your code Quality.

~~Review~~  
vPC, Subnet, Iaas NAT Gateways,  
NACL, SG, VPC, Global IP  
from prev - not us

Aws Shared Responsibility Model

- Aws responsibility security of the cloud
- ↳ protect cloud infrastructure  
h/w s/w, facilities & networking on Aws.
  - ↳ managed service like DynamoDB, RDS etc.
  - ↳ configuration using your S3 bucket
    - ↓  
server-side encryption  
→ data privacy etc.

Customer — Security in the cloud.

→ EC2 Instances (guest OS's configuration)  
hands over code.

Both — Patch management, Awareness & training of  
AWS & configuration management.  
Custom.

AWS Shield Standard

↳ protect against DDoS attack for your website &  
applications, for all customers, no additional cost.

AWS Shield Advanced (Additional protection)

- 24/7 access to AWS DDoS response team.
- protect against higher fees during  
unusual spikes due to DDoS

↳ additional cost

AWS WAF

protects your web application from  
common web exploits (Chaper 7)

Web ACL  
↓ ↳ protects SQL Injection, Cross-site scripting (XSS)  
AWS Content  
↳ block user / country.

- KMS — Encryption keys managed by AWS.
- Cloud HSM — H/w encryption, customer managed encryption keys.
- Guard Duty — malicious / unauthorized activity.
- Inspector — vulnerability.
- Macie — protects sensitive data.
- Amazon Detective — security issues ⚡ suspicious activities.
- AWS Abuse — Report AWS resources used for abusive ⚡ illegal purposes.
- Config — track config changes.