AWS CLOUD PRACTITIONER

- CL-CO2 is the new AWS exam for cloud practitioner.
- Two types of questions:
  (1) Multiple Choice
  (2) Multiple Responses

- Tips: 1) eliminate answer
  2) set timer of each question

- Domains: 1) Cloud Concepts (24%)
  2) Security and Compliance (30%)
  3) Cloud Technology and Services (34%)
  4) Billing, Pricing, and Support (12%)

- 7's R for migration strategy:
  1) Rehost ("Lift & shift")
  2) Replatform ("[redacted] Lift and Reshape")
  3) Retain ("[redacted] Revisit")
  4) Retire
  5) Relocate ("Hypervisior-Level Lift & Shift")
  6) Refactor ("Re-architect")
  7) Repurchase ("Drop & Shop")

- Shared Responsibity Model (Read)

(Note)- Go through the out-of-scope AWS Services at high-level. If they appear in the exam eliminate that option.

- Domain 1: Cloud Concepts
  Task 1.1: Benefits of AWS Cloud

(i) Easy to Use	(iv) Reliable
(ii) Flexible	(v) Scalable and high-performance
(iii) Cost-Effective	(vi) Secure

- Cloud-Computing : on-demand of IT resources over the internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access the technology services, such as computing power, storage, and databases. And, AWS is the cloud-service provider.

Task 1.2 : Identify design principles of the AWS Cloud

(i) Operational Excellence
(ii) Security Pillar
(iii) Reliability Pillar
(iv) Performance Efficiency Pillar
(v) Cost Optimization Pillar
(vi) Sustainability Pillar

It helps cloud architects to build secure, high-performing, resilient and efficient infrastructure for a variety of applications and workloads.

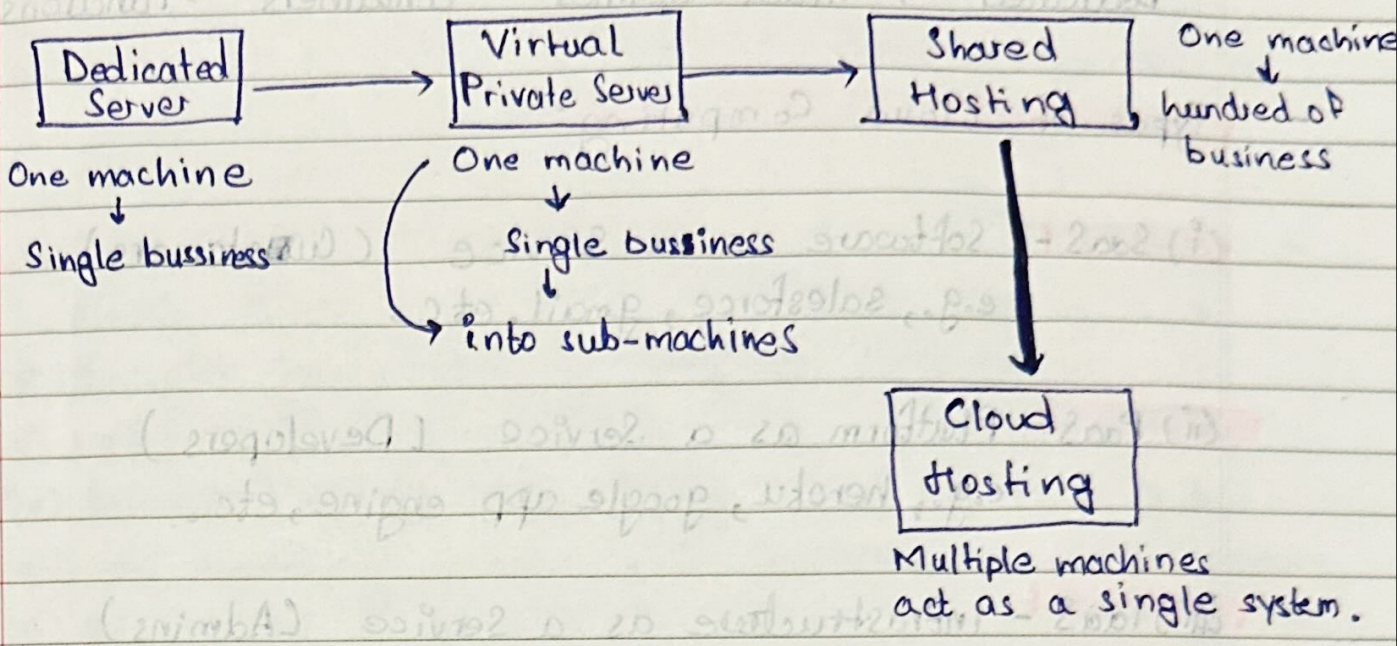
- 3-2-1 backup strategy: 3 copies, 2 mediums and 1 offsite

Task 1.3 : Understanding the benefits of and strategies for migration to the AWS Cloud.

Task 1.4 : Understand concepts of cloud economics.

- EC2 = Elastic Cloud Compute (Virtual Server in Cloud)

- Evolution of Cloud Computing:



- Cloud Service Provider:
  (i) provides multiple cloud services
  (ii) cloud services chained together to create cloud archi.
  (iii) accessible via single Unified API e.g., AWS API
  (iv) provides metered billing
  (v) rich monitoring built-in

- Cloud Provider: AWS, Azure, GCP

- 4 core (IaaS) would be: → [other services as well are also provided by cloud provider]
  (i) Storage (eg. EBS)
  (ii) Compute (eg. EC2)
  (iii) Networking (eg. VPC)
  (iv) Databases (eg. RDS)

- AWS has 200+ cloud services.

- **Evolution of Computing:**

  Dedicated → Virtual Machines → Containers → Functions

- **Types of Cloud Computing:**

  (i) SaaS - Software as a Service (Customers)
  e.g., salesforce, gmail, etc.

  (ii) PaaS - Platform as a Service (Developers)
  e.g., heroku, google app engine, etc.

  (iii) IaaS - Infrastructure as a Service (Admins)
  e.g., AWS, Azure, etc.

- **Cloud Computing Deployment Models:**

  (i) Public Cloud - everything build on CSP
  a.k.a cloud-native or cloud first

  (ii) Private Cloud - everything build on company's datacenters
  a.k.a on-premise

  (iii) hybrid - both on-premise and CSP
  CSP ↓ cloud-service provider

  (iv) Cross-Cloud - using multiple cloud providers

- Root User - sign-in through email
- IAM User - sign-in through Account ID

- Computing Power: throughput measured at which a computer can complete a computational task.

- Six Advantages of Cloud:
  (i) trade capital expenses for variable expense.
  (ii) benefit from massive economies of scale.
  (iii) stop guessing capacity.
  (iv) Increase speed and agility.
  (v) stop spending money and maintaining data centers.
  (vi) go global in minutes.

- AWS Global Infrastructure: globally distributed hardware and datacenters that are networked together to act as one large resource for the end customer.

- Regions are geographically distinct locations consisting of one or more availability zones.

- 4 factors needs to be considered when, choosing a region:
  (i) regulatory compliance in that region
  (ii) cost of service
  (iii) what services available
  (iv) distance or latency to end user

- Regional Services: where an AWS service will be launched and what will be seen within an AWS service's console.

- Global Services: some services operate across multiple regions and the region will be fixed to "Global".

- **Availability zone**: physical location made up of one or more datacenter.
  ↓
  hundreds of thousand of computers

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

- each AWS region is isolated from another region.

- AWS global network represents the interconnections betⁿ. global infrastructure.

- **Point of Presence (PoP)**: intermediate location betⁿ. an AWS Region and the end user, and this location could be a datacenter or collection of hardware.

- **PoP resources**: (i) edge location (cache of most popular Files)
  (ii) regional edge caches (much larger caches of less popular Files)

- Services uses PoPs for content delivery or expediated upload.

(i) AWS CloudFront - Content Delivery Network (CDN)
(ii) AWS S3 Transfer Acceleration - generate special URL that can be used by end user to upload Files to a nearby edge location.

(iii) AWS Global Accelerator ★ - Finds the optimal path from the end-user to your web-server.

- AWS Direct Connect : private / dedicated connection between your datacenter, office, co-location and AWS.

→ has very-fast network connection options :
(i) Lower Bandwidth - 50 MBps - 500 MBps
(ii) Higher " - 1 GBps or 10 GBps

- helps ↓ network costs and ↑ bandwidth throughput. (great for high traffic networks)
- more consistent network experience than typical internet-based connection. (reliable and secure)

- Direct Connect Locations are trusted partnered datacenters that you can establish a dedicated high speed, low-latency connection from your on-premise to AWS.

- Local Zones : datacenters near densely populated area to provide single digit low latency performance for that area.

→ Purpose is to support high-demanding application sensitive to latencies :
- Media & Entertainment
- Electronic Design Automation
- Ad-Tech
- Machine Learning

- **Wavelength zones:** allows for edge-computing on 5G networks. Application will have low-latency being as close as possible to users.

- **Data-Residency:** physical or geographical locations of where an organisation or cloud resources reside.

- **Compliance Boundaries:** legal requirement by goverment or org. that describes where data and cloud resources reside.

- **Data Sovereignty:** jurisdictional control or legal authority that can be asserted over data because its physical location is within jurisdictional boundaries.

- **AWS Outpost** - physical rack of servers that you can put in your data center. Your data will reside whenever the Outpost physicall reside.

- **AWS Config** - policy as code service. You can create rules to continuous check AWS resources configuration. Deviated from expectations, you are alerted or in some-cases can auto-remediate.

- **IAM Policies** - can be written explicitly allowed to access to specific AWS regions.

- **Service Control Policy (SCP)** - are permissions applied organization wide.

- **AWS for goverment:**

(i) public sectors include public goods and government sectors / services. (e.g., military, public transit, etc.)

→ AWS can be ultisied to develope cloud workloads.
↳ achieves this by meeting regulatory compliance programs along with specific governance and security controls.

(i) HIPAA	(iii) CJIS
(ii) FedRAMP	(iv) FIPS

↳ special regions for US regulations called GovCloud.

(ii) GovCloud - CSP. provides isolated region to run FedRAMP workloads.

↙

Federal Risk and Authorization Management Program (standarized approach to security assessment, authorization, etc. for cloud products and services)

- **AWS Cloud's Sustainability:**
(i) Renewable Energy
(ii) Cloud Efficiency
(iii) Water Stewardship

- **AWS Ground Station:** - fully managed service that lets you control satellite communications, process data, and scale your operations without worrying about building or managing your own ground station infra.

- **High Availability**: no single-point-of failure.

- **AWS ELB** - load balancer allows you to evenly distribute traffic to multiple servers in one or more datacenter.

- **High Scalability**: increasing your capacity based on demand.

- **High Elasticity**: automatically ↑ or ↓ your capacity based on the current demand.

- **AWS ASG (Auto-Scaling Group)** - AWS feature that will add or remove servers based-on scaling rules you defined based on metrices.

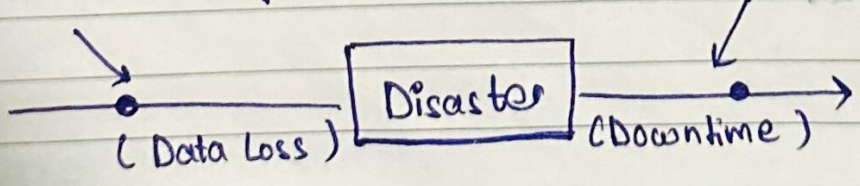
- **AWS RDS Multiple-AZ** - you run duplicate standby database in another Availability Zone. (Fault Tolerance)

- **High Durability**: recover from a disaster and to prevent loss of data. Solutions recover from a disaster is known as Disaster Recovery (DR).
  → **AWS Cloud Endure Disaster Recovery**

- **Bussiness Continuity Plan**: how business will operate during disruption in services.

RPO (how much data willing to lose)

RTO (how much time willing to go down)



- AWS ElasticBeanstalk - end-to-end web application management. It is an easy-to-use service for deploying and scaling web applications.

- API or Application Programming Interface: Software that allows two applications / services talk to each other. Most common type of API via HTTP/S requests.

- AWS SDK - Interact with the API using your favourite programming language.

- AWS CLI - It is a terminal / shell.

- AWS Management Console - Is a web-based unified console that build, manage, and monitor everything from simple web-apps to complex cloud deployments.

- point and click to manually launch and configure AWS resources with limited coding knowledge is known as "ClickOps".

- AWS Account ID - unique Account ID.
  It is used:
  (i) when logging in with non-root user account.
  (ii) cross-account roles
  (iii) support cases

- Powershell: task automation and configuration management framework. A command-line shell and a scripting language.

- Amazon Resource Names (ARNs): uniquely identifies AWS resources.

- AWS CLI - allows users to programmatically interact with the AWS API via entering single or multi-line commands into a shell or terminal.

- AWS SDK - collection of software development tools in one installable package.
  → used to programmatically create, modify or delete or interact with AWS resources.

- AWS Cloud9 - cloud IDE for writing, running, and debugging code.

- AWS Cloudshell - browser-based shell built into the AWS Management Cloud.

- Infrastructure as Code (IaC) - you write configuration script to automate creating, updating or destroying cloud infrastructure.

- AWS has two offerings for IaC:
  (i) AWS CloudFormation (CFN) - declarative IaC Tool
  (ii) AWS Cloud Development Kit (CDK) - imperative IaC Tool

Declarative	Imperative
- what you see is what you get. (Explicit)	- you say what you want and, rest filled in. (Implicit)
- more verbose & zero-chance of mis-configuration	- vice-versa.
- Uses scripting language e.g., JSON, YAML, XML	- Uses programming language.

- AWS Toolkit - an open-source plug-in for vscode to create, debug, deploy AWS resources.

- Access Keys : a secret key required to have programmatic access to AWS resources when interacting with AWS API outside of AWS Management Console.
  - commonly referred to AWS credentials.
  - are to be stored in ~/.aws/credentials

- AWS S3 - (Simple storage service) is an object storage service that offers industry-leading scalability, data availability, security and performance.

- Shared Responsibility Model: a cloud-security framework that defines the security obligations of the customer versa the CSP e.g. AWS.

  Customer Responsibity in Data / Configuration.

  AWS Responsibity of Hardware / Operation of Managed Services / Global Infrastructure.

- Types of Cloud Computing Responsibity:
  (i) On-Premise (Customer)
  (ii) Infrastructure as Service (Customer + CSP)
  (iii) Platform as a Service (Mostly CSP)
  (iv) Software as a Service (CSP)

- AWS WorkDocs - Content Collaboratin

- Function as a Service (FaaS):
  (i) AWS Lambda - serverless backend (customer just upload the code and AWS takes care of everything rest)

- AWS Amplify - Serverless Framework
- AWS Lambda - Serverless Architecture
- AWS Fargate - Serverless Containers orchestration service
- ECS / EKS - Containers

- Computing Services:
  - AWS EC2 - Elastic Compute Cloud allows you to launch Virtual Machines.
    - ↳ emulation of physical computer using software.
  - AWS LightSail - managed virtual server service. (friendly verison of EC2)
  - AWS ECS - container orchestration service.
  - AWS ECR - repository for container images.
  - AWS EKS - a fully managed Kubernetes service.

- Higher Performance Computing services:
  - Nitro System: combination of dedicated hardware and lightweight hypervisor enabling faster innovation and enhanced security. All new EC2 instances types uses the Nitro System.
    e.g., Nitro Cards, Nitro Security Chips, Nitro Hypervisor
  - Bare Metal Instance: launch EC2 instance that have no supervisor so you can run workloads directly on the hardware for maximum performance and control. The M5 and R5 EC2 instances run on bare metal.

- AWS Bottlerock - linux-based OS, purposly built by AWS for running containers on VMs or bare metal hosts

- **AWS Parallel Cluster** - AWS-supported open source cluster management tool that makes it easy for you to deploy and manage High Performance Computing (HPC) clusters on AWS.

- **Edge Computing**: pushing your computing workloads outside of your networks to run close to the destination location.

- **Hybrid Computing**: run workloads on both on-premise data center and AWS virtual Private Cloud.

- **AWS Outposts** - physical rack of servers that you can put in your datacenter. Allows you to use AWS API and services such as EC2 right in your datacenter.

- **AWS Wavelength** - to build and launch your application in a telecom datacenter. (application will have low latency and, will be as closest as possible to end-user)

- **VMWare Cloud** - manage on-premise virtual machines using VMWare.

- **AWS Local Zones** - edge datacenters located outside of an AWS regions.

- **Storage**:

  - **Types of Storage Services**:
    (i) Elastic Block Storage (EBS) - Block
    (ii) AWS Elastic File Storage (EFS) - File
    (iii) AWS Simple Storage Service (S3) - Object

→ provides unlimited storage

- S3 - It is an object storage service.
- S3 Object - Object contains your data.
- S3 Bucket - Buckets hold objects. Buckets can also have folders which in turn hold objects. And, buckets name should be unique.

- S3 Storage Classes: (ADR = Avail., Durability, Replication)
  (i) S3 Standard (Default) - Fast, ADR
  (ii) S3 Intelligent Tiering - Uses ML to analyse & determine app. of S3
  (iii) S3 Standard - IA (Infrequent Access) of files
  (iv) S3 One-Zone-IA - Only exist in one AZ
  (v) S3 Glacier - long-term cold storage & data retrieval time (mins-hrs)
  (vi) S3 Glacier Deep Archive - lowest cost & data retrival 12 hrs

- AWS Snow Family - storage and compute devices used to physically move data in or out the cloud.
  (i) AWS Snowcone - 8 TB (HHD) or 14 TB (SSD)
  (ii) AWS Snowball Edge - Storage Optimized - 80 TB.
  Compute Optimized - 39.5 TB
  (iii) AWS Snowmobile - 100 PB of Storage

- AWS Storage Gateway - hybrid cloud storage service that extends your on-premise storage to cloud.
  → Three types:
- File Gateway - extends your local storage to AWS S3
- Volume Gateway - chaces your local drives to S3. So, you have a continuous backup of local files in the cloud.
- Tape Gateway - stores files onto virtual tapes for backing up your files on very cost effective long term storage.

- AWS Backup - Managed Back-up service
- CloudEndure Disaster Recovery - continuously replicates your machines into low-staging area in your target AWS account and preferred region.
- Amazon FSx - Feature rich and highly-performant file system.

- Database:

- data-store that stores semi-structured and structured data.
- Types: (i) Relational
  (ii) Non-Relational

- A relational datastore designed for analytic workload which is generally column-oriented data-store.

- A document store is a NOSQL database that stores documents as its primary data structure.
  ↓
  A document could be an XML but more commonly is JSON or JSON-like document stores.

- NoSQL Database Service:
  (i) AWS Dynamo DB - NoSQL key/value and document database. (use when we want a massavily scalable database)

  (ii) AWS DocumentDB - NoSQL document that is "MongoDB" compatible. (when we want a MongoDB database)

  (iii) Amazon Keyspaces - Fully managed Apache Cassandra database.

- **Relational Database Services:**
(i) RDS - relational database service, synonymous with SQL and OLTP and most commonly used.
RDS supports: MySQL
MariaDB
Postgres (SQL)
Oracle
Microsoft SQL Server
Aurora

(ii) **AWS Aurora** - Fully managed database of either MQSQL and PSQL database.

(iii) **Aurora Serverless** - on-demand version of Aurora. (used when want most benefits of Aurora but, can trade to have cold starts or don't have lots of traffic demand)

(iv) **RDS on VMWare** - When you want database managed by RDS on your own datacenter.

- **AWS Redshift** - petabyte-size data-warehouse. (used when you want to quickly generate analytical reports from a large amount of data)

- **Elastic Cache** - managed database of in-memory and caching open-source databases Redis or Memcached.

- **Neptune** - managed graph database.

- **Amazon Timestreams** - Fully managed time-series database.

- Database Migration Service (DMS) - you can migrate from:
  (i) on-premise database to AWS
  (ii) From two-database in diff. or same AWS account using diff. SQL engines
  (iii) From an SQL to [redacted] noSQL database

- Networking:

- AWS Virtual Private Network (VPN) - a secure connection between on-premise, remote offices, mobile employees.

- AWS Direct Connect - dedicate gigabit connection from on-premise data-center to AWS (a very fast connection)

- AWS PrivateLinks - (VPC Interface Endpoints) keeps traffic within the AWS Network (keeps secure)

- EC2:

- EC2 Tenancy:
  (i) Dedicate Host -
  (ii) Dedicate Instance -
  (iii) Default -

- Pricing Models:
  (i) On-Demand - Least Commitment - Pay-As-You-Go
  (ii) Spot - Biggest Savings
  (iii) Reserved - Best Long-term
  (iv) Dedicated - Most Expensive
  (v) AWS Savings Plan

- RI Attributes :-
  (i) Instance type
  (ii) Region
  (iii) Tenancy
  (iv) Platform

- Identity :

- Zero-Trust Model : operates on principal of "trust no one, verify everything."
  Identity becomes primary security parameter.

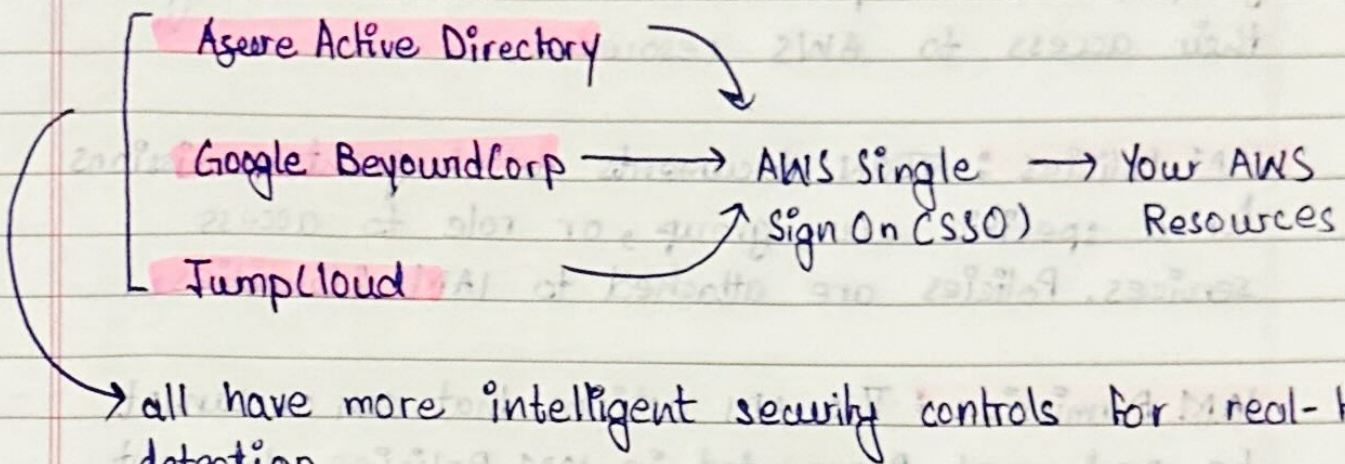
- AWS Identity and Access Management (IAM) - IAM Policies, Permission Boundaries, Service Control Policies, IAM Policies Conditions (Restrict IP Address, Restrict on Region, etc.)

- AWS does not have a ready-to-use identity controls are intelligent, which is why AWS is considered to not have a true zero trust offering for customers, and third-party services needs to be used.

- A collection of services can be setup to overcome above issue but, requires expert knowledge.

(i) AWS CloudTrail - Tracks All API calls
↓
(ii) AWS GuardDuty - Detects suspicious or malicious activity based on CloudTrail and other logs
↓
(iii) Amazon Detective - used to analyze, investigate and quickly identify security issues (can ingest findings From GuardDuty)

- **Zero Trust on AWS with third-parties:**



- **Directory Service:** maps the names of network resources to their network addresses. It is a shared information infrastructure for locating, managing, administering and organizing resources.

- **Active Directory:** gives organizations the ability to manage multiple on-premise infrastructure components and systems using a single identity per user.

- **Single sign-on (SSO):** an authentication scheme that allows a user to log-in with a single ID and password to diff. systems and software.
allows IT dept. to administrator a single identity that can access many machines and cloud services.

- **Lightweight Directory Access Protocol (LDAP):** application protocol for accessing and maintaining distributed directory information services.

- **AWS IAM** - can create and manage AWS users and groups, and use permission to allow and deny their access to AWS resources.

- **IAM Policies** : JSON documents which grant permissions for a specific user, group, or role to access services. Policies are attached to IAM identities.

- **IAM Permission** : The API actions that can or cannot be performed. Represented in IAM Policies document.

- **IAM Identities** :
  (i) **Users** : end users who can interact with AWS resources programatically or via interface.

  (ii) **Groups** : eg., Administrators, Developers, Auditors

  (iii) **Roles** : grants AWS resources permission to specific AWS API action. Associate policies to a Role and then, assign it to an AWS resource.

- **Principle of Least Privilege** (PLOP) - is a computer security concept of providing a user, role or application the least amount of permissions to perform a operation or action.

  (i) **Just-Enough-Access (JEA)** : permitting only exact actions for the identity to perform a task.

  (ii) **Just-In-Time (JIT)** : smallest length of duration an identity can use permissions.