AWS Cloud Practitioner

⇒ free practice exam. www.~~example~~ exampro.co/clf-c01

26% – Cloud concepts
25% – Security & compliance
33% – Technology
16% – Billing & Pricing

700/1000 for passing

65 questions (15 unscored, 50 scored)
Exam time 90 minutes
- Questions can be multiple choice or single choice

x —— x —— x

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

Evolution of cloud hosting

- Dedicated server
- Virtual Private Server
- shared hosting
- cloud hosting

AWS — amazon's cloud service solution

Simple Queue Service (SQS) — 2004
Simple Storage Service (S3) — 2006
Elastic Compute Cloud (EC2) — 2006
In 2010, all amazon's retail sites had migrated to aws

A CSP is a company which:-
- provides multiple cloud services
- services can be chained together to create Cloud architectures
- cloud services are accessible via a Single Unified API
- metered billing
- rich monitoring built-in like AWS cloud Trail
- have IaaS offering
- offer automation via IaC (infrastructure as code)

CSPs landscape

Tier 01 AWS, GCP, Azure

Tier 02 IBM, Oracle Cloud, Rackspace

Tier 03 Vultr, Digital Ocean, Linode

Common Cloud services:

CSPs can have 100s of services but most common services are
1) Compute (EC2) 2) Networking (VPC) 3) Storage (EBS)
4) Databases (RDS)
aws has 200+ Cloud services

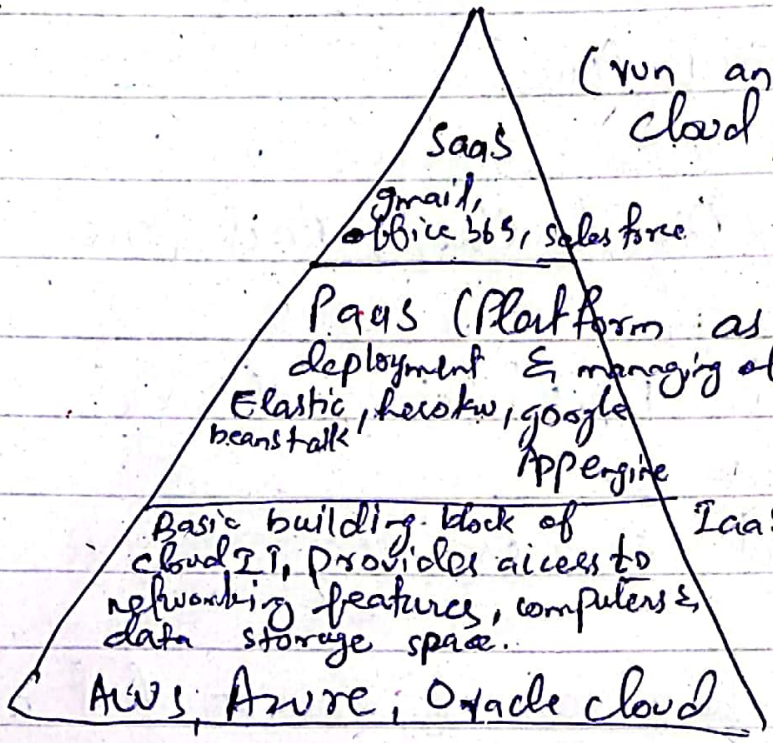
Analytics, AR/VR, containers and a lot more.

Evolution of computing

→ Dedicated → VMs (hypervisor)
→ Containers (VMs running containers + VM itself running on hypervisor)

→ Functions (Serverless, even more versatile than containers, you only pay for the time you've spent on compute)

Types of Cloud Computing:-



(run and managed by the cloud provider)

IaaS (Infrastructure as a service)

Cloud computing deployment models:-

→ Public Cloud (Cloud native / Cloud first)
→ Private cloud (On premise / could be openstack)
→ hybrid (On premise + CSP
→ Cross-cloud (Amazon EKS ↔ Azure Arc ↔ GCP Kubernetes Engine)

Regions

- uscast-1 is the original region & some services (billing etc) only show up in North Virginia.
  - Some services are global services like cloudfront, S3 etc.

Metered Billing

- Being charged by the hour / compute.
- If you are overbilled, you get a single free pass

1:02:40

AWS Budget:

- you can setup AWS Budget to stop any misspending on AWS.
- you can setup email alerts to get info when you've exhausted your free aws quota

Burning Platform when a company abandons old technology for new technology

AWS Computing Offering

- EC2 (general computing)
- AWS Inferentia (2nd) (GPU offering) for AI/ML workloads.
- AWS Bracket (Quantum computing via CalTech)

Benefits of Cloud:

- Agility
- Pay as you go
- Economy of scale
- Global Reach
- Security
- Reliablity
- High Availablity
- Scalablity
- Elasticity

Six Advantages of Cloud.

1) Trade capital expense for variable expense
2) Benefit from massive economies of scale
3) Stop guessing capacity.
4) Increase speed & agility
5) Stop spending money on running & maintaing data servers
6) Go global in minutes

7) Current: The underlying hardware is managed & software is patch by the CSP without any cost to the customer.

AWS Regions:

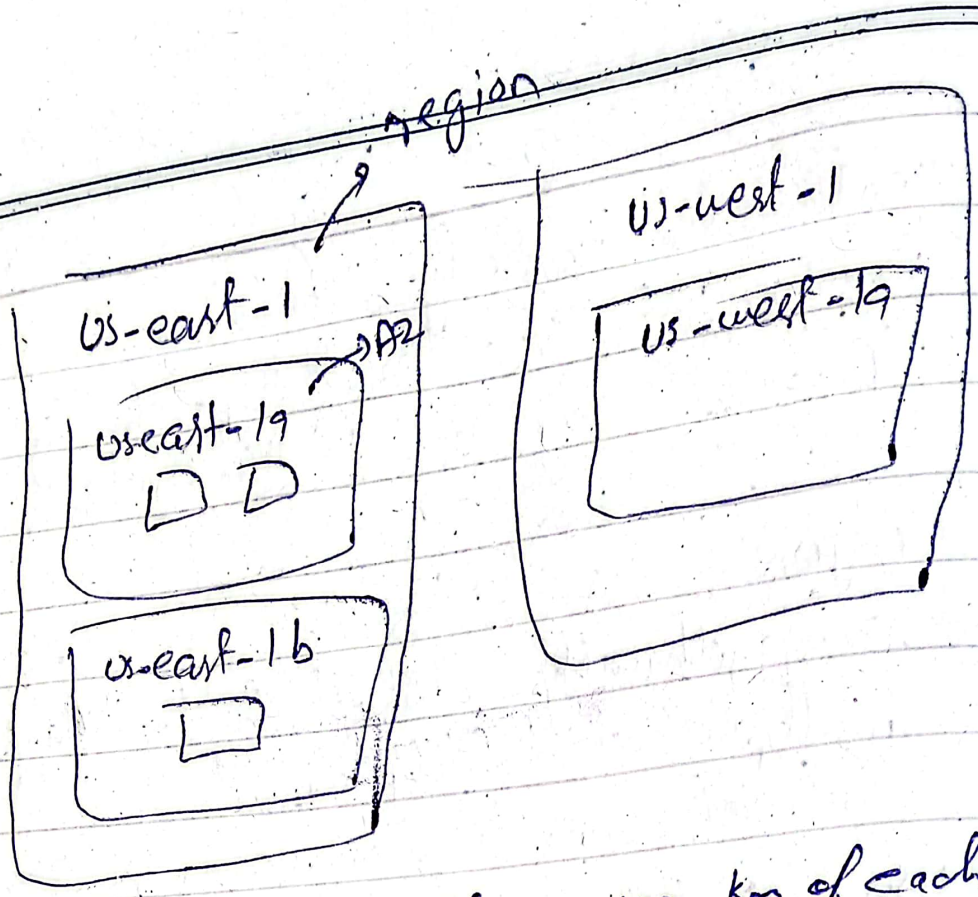
- Geographically distinct locations having multiple availablity zones.
- Cost of aws services varies per region.
- Some services are available in specific regions.
- Some aws services are fixed to global (S3, Cloudfront, IAM etc)

AWS Availablity zones:

- AZ is a physical location made up of one or more datacenter
- A region will have generally 3 availablity zones
- Common practice to run workloads in atleast 3 AZs

us-east-1a, us-east-1b, us-east-1c

availablity zones



All AZs are within a 100 kms of each other
When launching EC2 you select AZs of where your instance will be launched.

AWS Fault Tolerence:

- fault domain is a section of a network that is vulnerable to damage if a critical device or system fails.
  Purpose of fault domain is that if a failure occurs it will not cascade outside that domain

- A fault level is a collection of fault domains

fault domain could be
- specific servers in a rack
- entire rack in a data center

AWS Region would be a fault level
And AWS AZs within the regions would be a fault domain.

You want to run in multiple AZs to minize availability risks

AWS cloudfront (CDN) is aws content distribution network.

Point of Presence (PoP)
A data center owned by AWS or a trusted partner i.e utilized for content delivery or expediated workload

Edge location contain copies of most popular files (webpages, images, videos)

Regional edge location are datacenters which hold much larger caches of less popular files.

AWS Services Using PoP

1) AWS CloudFront
2) Amazon S3 Transfer Acceleration
3) AWS Global Accelerator - can find optimized path from end user to the web server

AWS Direct Connect

is a private/dedicated connection between your datacenter, office, co-location & AWS. (Imagine a fiberoptic from your VM directly to AWS)

1) Lower Bandwidth (50Mbps - 500 MBps)
2) Higher Bandwidth (1GBps - 10GBps)

AWS Direct Connect Location are trusted partnered datacenters that you can establish a dedicated highspeed low latency connection from your on-premise AWS.

AWS local zones

datacenters located very closely to densely populated areas to provide a single digit milisecond low latency performance
- available for specific services.
  - EC2, VPC, FSL etc.

AWS wavelength zones allows for edge computing on 5G Networks.
You create a subnet tied to a wavelength zone & then you can launch VMs to the edge of the targeted 5G Networks

Data Residency:

The physical or geographic location of where an organization or cloud resources reside.

- AWS Outpost physical rack of servers you can put in your datacenter, Your data will reside wherever your outpost physically reside.

- AWS Config Policy as Code, thus if you deviate from your expectations you are alerted.

IAM Policies can be written explicitly to deny access to specific Aws Regions. A service Control policy (SCP) are permissions which are applied organization wide.

AWS GovCloud
for working & completing compliance requirements for ~~Aws~~ working with US Govt.

AWS China
- has a aws chinese version with domain: amazonaws.cn
- benefit is that you won't have to traverse the great firewall
- you need to have a local chinese business license for using it.

Aws Ground Station
fully managed service that lets you control satellite communications, process data & scale your operations without having to worry about infrastructure
- weather forecasting
- surface imaging etc

Aws Outposts
a rack of servers running Aws infrastructure on your physical location. Aws Outposts comes with 42U, 1U, 2U

2:14:49

Solutions Architect: architecting solutions using multiple services

Cloud Architecture a solutions architect, architecting technical solutions using cloud services.
have to keep in mind:
- Availability - Scalability - Elasticity
- Fault tolerance - Disaster Recovery
- Security + cost

High availability

- no single point of failure
- multiple AZs
- implemented using (Elastic loadbalancer)

High Scalability

- increase your capacity
- Scaling Up
- Scaling Out

High Elasticity

automatically increasing & decreasing capacity

implemented using autoscaling groups

- generally referred for horizontal scaling

Fault Tolerance

no-single point of failure, preventing the chance of failure

Fail-over, secondary system becomes primary when primary system fails

Implemented RDS multiAZ

High Durability

ability to recover from a disaster

Cloud "Endure disaster Recovery" service by AWS

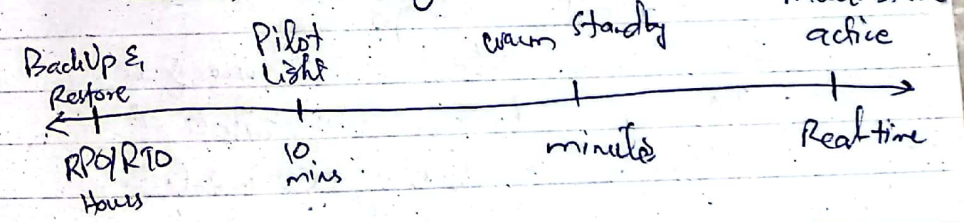
Business continuity plan (BCP)

a document that outline how a business will continue operating during an unplanned disruption in services.

- RPO (Recovery Point Objective) max acceptable amount of data loss.

RTO (Recovery Time Objective) max downtime your business can tolerate.

Disaster Recovery Options:-



AWS API

AWS API is an http API which you can send request to using HTTP requests with softwares like Postman.

Each AWS service has its own service endpoint
- you need a signed request for authentication
- we rarely directly make requests to AWS API, but clients do use it

AWS Management Console :-

- basic MC when you login
- deploying resources via clicks is called ClickOps.
- If you select a service from there it will open the console of the service for eg EC2 console

Service Console

each service has their own console which you can access by typing in the the name of AWS service & accessing it.

The UI of each service varies a lot

AWS Account ID

- every account has a 12 digit account ID
- it is also shown in IAM service console.
- used in creating policies

AWS Tools for Powershell

- Powershell is a task automation & configuration management framework
- AWS Tools for powershell lets you interact with the AWS API via Powershell Cmdlets
- type pwsh in cloudshell to switch to Powershell

Amazon Resource Names (ARN)

Uniquely identifies AWS resources. ARNs are required to specify a resource unambiguously across all of AWS.

ec2/s3 etc.

arn:partition:service:region:account-id:

aws/aws-cn/aws-us-gov

us-east-1

→ resource-type/resource-id

Can also include (*) when making IAM policies etc.

AWS CLI

Terminal: Text only interface (input + output)

Console: A physical computer to physically input information in terminal.

Shell A command line program that users interact with to input commands

- Bash
- Powershell

28.59+2.5 = 31.09

AWS cli allows users to programatically interact with AWS API via entery style or multi line comments.

- requires python
- can be installed on windows/ Mac & Linux

AWS SDK

a collection of software development tools in one installable package.

AWS SDK is provided in all famous languages.

Cloud9 is the default AWS IDE

AWS Cloud Shell

A browser based shell that is built into the AWS Management Console

- 1 GB free storage per AWS region

Infrastructure as Code (IaC)

Configuration script to automate, creating, updating or destroying cloud infrastructure.

Two offering by aws
- AWS cloud formation → (Declarative)
- AWS cloud development Kit (CDK) → (Imperative)

Cloud Formation

- write using json or yaml
- simple but can lead to large files & limited in creating dynamic infrastructure

CDK (Cloud development Kit)

- allows you to use a programming language to write IaC
- Typescript was the first & is generally the most updated

SDK & CDK may look similar but CDK ensures ~~independent~~ idempotent of your infrastructure.

AWS Toolkit for VSCode:-

Opename plugin for VSCode to create, debug, deploy AWS resources

Access Key

is a key (duh!) & secret required to have programmatic access to AWS resources when interacting with AWS API. also referred as AWS credentials

- you can have 2 access keys
- root user can generate keys for other users.

AWS Shared Responsiblity Model

Shared Responsiblity model is a Cloud security framework that defines the security obligations for customers versa the Cloud service Provider (csp)
eg AWS

IN	Data Configuration	customer
aws OF	Hardware Operation of Managed Services Global infrastructure	

customer for in the cloud
aws for OF the cloud

Shared Responsibility for Compute:

~~Function as a Service (FaaS)~~

Containers:-

Customer: - configuration of containers
- Deployment of Containers
- storage of containers.

AWS
- OS, hypervisor, runtime.

FaaS (Function as a Service)

Lambda functions

Computing Services

- EC2 - main service (VMs)
- LightSail (managed virtual server service). used when you are not much familiar with aws, can host wordpress etc.
- Containers:
  - ECS (elastic container Service)
  - ECR (elastic container registry) (repository for container images)

ECS Fargate serverless orchestration container service.

EKS (elastic Kubernetes service) fully managed Kubernetes service

EC2 highly configurable server
AM2 - options such as no. of CPUs

AM2 - predefined configuration for a VM.

- Ability to store multiple hard drives EBS (elastic block store)
- Considered backbone for AWS

Amazon lightsail managed virtual server service, friendly version for EC2

ECS is a container orchestration service
ECR (elastic container register which holds images of containers)

ECS Fargate is a serverless container orchestration service i.e. you don't need to keep your EC2 server running

EKS (elastic kubernetes service)

AWS Lambda serverless function service, you are ~~round~~ charged about your usage rounded to 100 ms

x ——— x ———

Higher Performance Computing

Nitro system dedicated hardware & lightweight hypervisor

Bare metal instances: EC2 instances that have no hypervisor (M5 & R5)

Bottlerocket: → linux based opensource OS for running containers on bare metal VMs.

Usage 100s or 1000s of PCs for huge workloads used in HPC

AWS Parallel clusters. AWS supported opensource cluster management tools

Generally HPC is used for ML or other high demanding tasks.

Edge Computing: when you push your computing workload outside of your network & run close to destination location.

Eg computing on phones, IOT devices or external servers

Hybrid computing Run workload on both on premise datacenter & AWS VPC (virtual Private cloud)

AWS Outposts A physical rack of servers that you can put in your own data centers. (AWS APIs & use EC2 right in your datacenter).

AWS Wavelength :- build & launch application in your own datacenter, ultra low latency applications pushed on 5G network

VMWare cloud on aws manage on premise VMs using VMWare as EC2 instances.

AWS Local Zones: edge datacenters located outside of an AWS region so you can use AWS closer to end destination

CloudFront also has functions called edge functions which are executed to aws edge locations to decrease response time, the benefit over AWS Lambda is less time for cold start.

Cost & Capacity Management

Cost Management: How do we save money?

Capacity Management: Manage demand of traffic by adding / upgrading servers

EC2 spot instances:-

You bid on unused AWS compute capacity & get a lower rate, but it doesn't have high availability & you can get outbid on 2 min notic period but you get upto 90% discount.

EC2 reserved instances:-

You can reserve EC2 instances for a time period of 1/3 years & get upto 72% discount

AWS Batch plan/execute batch workloads across full range of AWS compute services can utilize spot instances to save money.

AWS Comput Optimizer: reduce cost & improve performance using ML to analyze your previous usage history

EC2 ASG (Autoscaling groups)
Add or remove EC2 servers to meet current demand of traffic.

Elastic Load Balancers -
Distributes traffic, re-route traffic from unhealthy to healthy instance.

AWS Elastic Beanstalk easy to deploying web applications without developers having to worry about setting up AWS services

Types of Storage Services

EBS (Elastic block store)

Data split into evenly split blocks, directly accessed by OS. (virtual HD attached to VM)

EFS (elastic file storage)

when multipe users/VMs need to access the same drive / file share

Amazon storage service (S3):

when you just want to upload files, not intended for High IOPs

Introduction to S3

- unlimited storage
- S3 buckets hold S3 object
- object can be 0B to 5TB

S3 Storage classes

- S3 Standard (default)
- S3 Intelligent Tiering
- S3 Standard IA
  (fast but for less accessed files, 50% less than standard)

- S3 One-Zone-IA
- S3 Glacier
  long term cold storage but recovery can take mins to hrs
- S3 Glacier deeparchive.
  very cheap; 12 hr retrieval time.

AWS Snow family

storage & compute devices used to physically move data in or out of the cloud when moving data over the internet or private connection is too slow difficult or costly.

- Snow Cone (8TB hdd, 14TB SSD)
- Snowball edge (80TB (storage optimized), 39.5TB (compute optimized))
- Snowmobile. 100PB of storage

→ all data is delivered to S3

Storage Services

- S3
- S3 Glacier
- EBS (elastic block store
- Elast file storage (EFS)
- Storage gateway
  hybrid cloud storage extending onprem storage to cloud.
- File gateway (local storage extension to S3)
- Volume gateway
  cache local drives to S3 for continuous backup of local files
- Tape Gateway
  store file on virtual tapes for very cheap long term storage

AWS Backup Backup plans for multipe aws services

Amazon Fsx feature rich, highly performant file system for windows & linux (lustre)

- serverside encryption in S3
- S3 lifecycle rules
- you can have 100 buckets in aws you can increase limit to 1000 by getting a service level increase.

- To mount EFS to an EC2 instance you have to run linux commands on the cloudshell
  with EFS you can connect multiple EC2 instances with 1 EFS volume

Database: structure / semi-structured

Datawarehouse: relational datastore designed for analytic workloads, which is generally columnoriented data-store
- optimized around aggregating columns

Keyvalue store is a noSQL db
- dumb & fast
- lack relationships, indexes, aggregation
- they scale really well

DynamoDB

AWS flagship NoSQL Database, very cost effective & very fast
- AWS flagship database service.

DocumentDB NoSQL document that is MongoDB compatible

Amazon Keyspaces variation for Casandra.

RDS

relational database service
supports - MySQL - MariaDB, PostgreSQL

AWS Aurora is a fully managed database of either MySQL or PSQL
very highly available, durable & scalable

Aurora serverless when you want Aurora benefits, but can trade cold starts

RDS on VMWare allows you to deploy RDS supported engines on an on-premise data center

Redshift a petabyte sized datawarehouse, for OLAP, can be expensive.

Elasticache managed db for in memory dbs such as Redis or Memcached

Neptune is a graph database.

Amazon Time ~~series~~ streams for timeseries data.

Amazon Quantum Ledger Service for financial transactions logs.

Database Migration service:-
from on-premis to AWS
from SQL to NoSQL

Cloud Native Networking Services

- VPC: logically isolated section of AWS cloud.
- AZ: aws data center
- subnet: logical partion of IP Network.
- Route Table: determine where network traffic from subnets are directed to.
- NACL: act as a firewall on subnet level
- Security group:- act as a firewall on instance level.

Enterprise / Hybrid Networking

Direct connect: dedicated gigabit connection from onpremise datacenter to VPC endpoints

AWS VPN: source to connect btw onpremise, remote offices, mobile employees

Private links keeps traffic within the AWS network when working within aws.

Security Groups v/s NACLs

Security Groups	NACLs.
- At instance level	- at subnet level
- implicity block everything	- You create allow & deny rules
- only create allow rules	- can block a single IP address
- cannot block a single IP address	

You can add a security group 10.0.0.0/16, a subnet should be less than that

- you create a subnet & add it to a internet gateway & rdp route table.
- inbound (incoming traffic) or outbound (outgoing)

AWS CloudFront

an aws CDN which caches your static files, it also has edge functions, you can block certain locations, you have to choose a source.

x —— x —— x

7:08:55

EC2

highly configurable virtual server.
Anything/everything on aws uses ec2 underneath

EC2 Tenancy

1) Dedicated Host 2) Dedicated Instance
3) Default (you'll be moved around)

Dedicated hosts
- per host billing (expensive)
- sockets, cores, host ID

- AMI id is region based (same config may have different id in a different region)

General purpose (T series)
Compute optimized (C-series)
Memory optimized (R-series)
Accelerator optimized (P-series)
storage optimized (I series)

Elastic IP

allows to reserve an IP address
- when an ec2 instance starts after stopping its public IP gets changed.
- we use elastic load balancer to overcome this issue & direct it to the ec2 instance & look it to the private IP address

elastic IP doesn't automatically release the private IP of a deleted EC2 server

Application load Balancer :(ALB)

distribute traffic among EC2 servers

EC2 Pricing Model

- On demand (pay per hr (second accuracy))
- reserved (upto 75% off) (1 or 3 yr, can resell unused server instances)
- Spot (upto 90% saving) (can stop at any time)
- Dedicated (when you need guarantee for enterprise requirement (most expensive))

RI formula:- Term × Class offering × RI attributes × Payment option

1/3 yr

Regional RI	Zonal RI
- Regional RI doesnt reserve capacity	Zonal RI reserve capacity
- discount applies to instances in the region	- applies to instances in the specific zone.
- 20 RI allowed per region	- 20 zonal RI allowed per AZ

x ——— x ———

Capacity Reservation You can reserve capacity, you will be charged on demand rate, doesnt matter if the server is running or not.

Standard R2	Convertible R2
- can be modified, but can't be exchanged - can be bought or sold in the marketplace	- can't be modified, but can be exchanged - can't be bought/sold

AWS Batch used for running batch jobs.
SageMaker is an aws service which uses MC EC2 instances.

Zero Trust Model

Primary Security Parimeter: 1st line of defense & its security control that protects a company's cloud resources.

Old way (Network centric)
New way (Network security control)

Aws CloudTrail: tracks api calls

AWS Guard Duty Detects suspicious or malicious activity based on cloudTrail & other logs

Amazon Detective used to analyze, investigate & quickly identify security issues.

3rd party services
- Azure Active directory
- Google BeyondCorp
- Jumpcloud

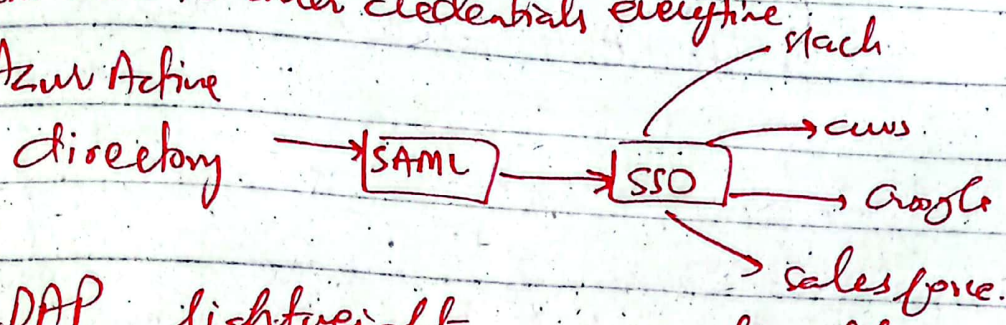
Directory service: shared information infrastructure for locating, managing administering & organizing resources.

Identity Providers (IPDs)
a service which maintains identity information & also provides authentication services to applications
Fb, Twitter, Amazon, Github, Linkedin

OpenID able to login to diff platforms using google or facebook.

OAuth 2.0 doesn't use usernames or passwords but uses authentication tokens.

SAML Single Sing-On via browser using a single ID & password to different systems
dont have to enter credentials everytime



LDAP lightweight access directly, same as SAML but have to enter credentials everytime

Security key a secondary device used as second step in authetication process to gain access to device.

IAM Policies:-
JSON docs granting permission to specific user, group or role to access services policies are attached to IAM identities

IAM identities
IAM Users - interact with AWS
IAM Groups share same level of permissions level of the group

IAM Roles grant AWS resources permissions to specific AWS API actions. Associate policies to a Role & then assign it to AWS resource.

x —— x —— x

AWS well architected Framework:

01) Operational Excellence
02) Security
03) Reliability
04) Performance Efficiency
05) Cost optimization

DONE!!!