① Characteristics of Cloud Computing:-

~~Elasticity~~ elasticity, on-demand, Agility, High-Availability

② Advantages of Cloud Computing:-

→ Trade fixed expense for variable expense.
→ Economies of ~~scale~~ scale.
→ Stop guessing capacity. → Because of on-demand usage model.
→ Increase speed and agility.
→ No more money spends on Data centers.
→ Go global in minutes.

③ AWS Global Infrastructure:-

Region → Physical locations spreaded across the globe to store your data.

Availability Zone → AZ is a combination of one or more datacenter in a region.

Edge Locations → An edge location is where an end user accesses services located at AWS.
→ Delivers contents close to the users.
→ Caches responses, so it reduces traffic on the origin server.
→ Cloudfront can be used.

④ Elastic Compute Cloud (EC2):-

EC2 = Servers

AMI (Amazon Machine Image) → OS image from which EC2 instance is launched. Eg:- Ubuntu, Windows etc.

EBS (Elastic Block Store) → Storage for EC2 instance.

EBS Snapshots → Back up the data on your Amazon EBS volumes by making point-in-time copies known as Amazon EBS snapshot.

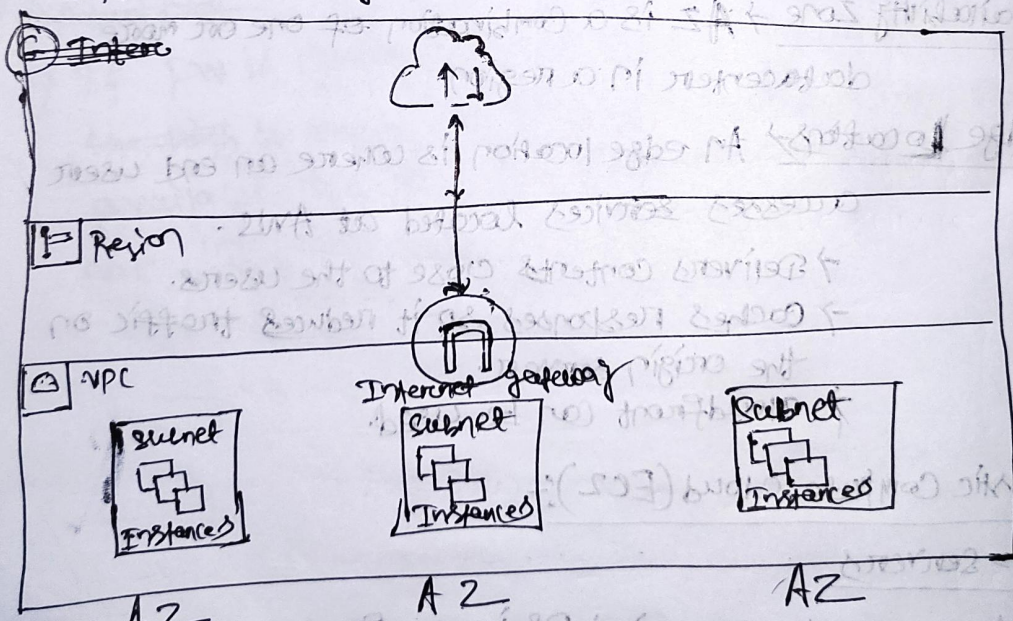
Instance Types → Each instance type comes with different CPU, memory, Network capacity.

⑤ VPC and Subnets

VPC → A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.

Subnets → A subnet, or subnetwork, is a segmented piece of a larger network. Specifically, subnets are ~~the~~ a logical partition of an Internet protocol (IP) network broken into multiple smaller-network segments.

→ EC2 instances must be created inside the VPC.
→ Each VPC has certain set of subnets. Each subnet has different IP ranges.



⑥ Internet Gateway

→ An internet gateway is a component that allows communication between the resources inside VPC and the internet.

→ It allows both inbound as well as outbound communication.

⑦ Types of Subnets

Public subnet → (i) Has internet gateway attached to it.
(ii) Users can directly connect to resources in public subnet from internet.

Private subnet → (i) No internet gateway attached to the subnet
(ii) No new connections from the internet can reach to the EC2 instances within the private subnet.

⑧ NAT Gateway → NAT Gateway allows the instances in the private subnet to initiate a new connection towards the internet. But no NEW internet connection will be allowed.

⑨ VPC peering →

→ By default, two VPC's cannot communicate with each other.

→ VPC peering is a network connection between two VPC that enables the communication between instances of both the VPC.

⑩ VPC Flow Logs → VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from ~~the~~ network interfaces in your VPC.

(11) Shared Responsibility Model :-

AWS responsibility "Security of the Cloud" AND Customer responsibility "Security in the Cloud".

Customer :- (i) Customer Data
(ii) Platform, Applications, Identity & Access Management
(iii) Operating System, Network & Firewall Configuration
(iv) Client Side data, Server-Side Encryption, Networking traffic protection.

AWS :-
- → **Software :-** Compute, Storage, Database, Networking
- → **Hardware/AWS Global Infrastructure :-** Regions, Availability Zones, Edge Locations.

(12) Managed vs. Unmanaged Services

Fully Managed → AWS takes care of the entire infrastructure and manages the required resources to deliver reliable service.

Eg :- Dynamo DB, SQS, SNS, Lex

Unmanaged → Customer is responsible for monitoring, provisioning, managing, securing, scaling the service based on requirement.

Eg: EC2

(13) Pricing Models of EC2

On-Demand → Pay for how much you use

Spot → Bid Spare Amazon EC2 Computing Capacity for upto 90% of the on-demand cost.
Suitable for stateless, interruptible workloads.

Reserved → Save upto ~72% on Amazon EC2 usage by committing to use a set level of compute power in $/hour for 1 or 3 years.

Savings Plan → Same as Reserved but in a specific AWS region and instance family.

Dedicated Hosts → A dedicated host is a physical EC2 server dedicated for your use.

(14) EC2 Image Builder

EC2 Image Builder simplifies the building, testing and deployment of Virtual Machine and Container images for use on AWS or on-premises.

(15) AWS Compute Optimizer → recommends optimal AWS resources for your workloads to reduce cost and improve performance by analyzing historical utilization metrics using ML.

(16) Types of Firewalls →

Security Group → Gets attached at an instance level.

Network ACL (NACL) → Gets attached at a subnet level.

Web Application Firewall →

↳ To protect web applications against web based attacks.
↳ Attacks like: SQL injection, Cross site scripting (XSS) etc.
↳ Integrates with: - CloudFront, API Gateway, Application Load Balancer, AppSync

(17) Identity and Access Management

IAM is a framework of policies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.

(18) IAM Concepts

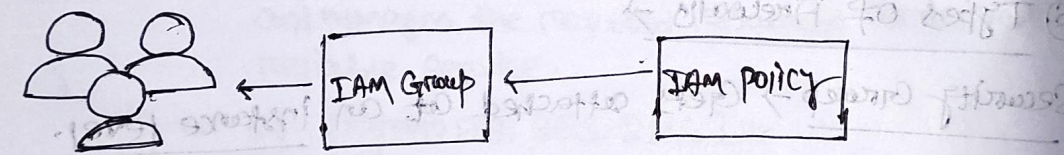
IAM User → Represents the human user or workload who uses the IAM user to interact with AWS.

IAM policy → IAM policies define permissions for an action to be allowed or denied in AWS.

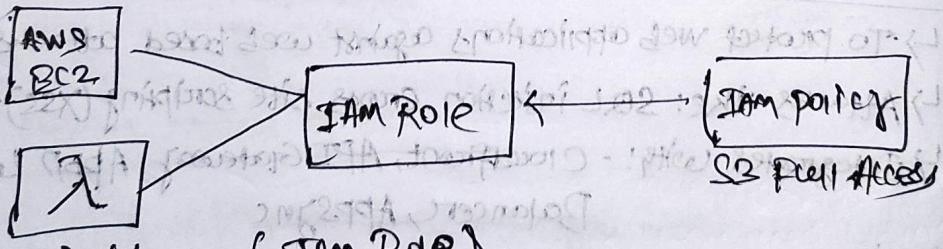
IAM groups → Collection of IAM users. IAM policies can be defined at group level.

IAM Role → Gets associated with AWS services.
(i) Cross account IAM role to provide users in one AWS account access to resource in other AWS account.

Credential Report → Lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices.



(IAM Group)



(IAM Role)

(19) Root users in AWS

→ Root user is a super-user in AWS.
→ It should be protected with MFA and should not be used unless required.

→ Create an IAM user ~~instead of root~~ with Administrator privilege and use that instead of ROOT.

→ For some account operations like changing account level settings or closing AWS account, you'll have to login with ROOT users.

(20) Imp. IAM Notes

→ If IAM user wants to access a specific AWS service, assign an IAM policy to it.

→ For EC2 service, to access other services like S3, Cloudwatch etc, you can make use of IAM role.

(21) IAM Access Analyzer

→ IAM access analyzer helps identify resources in your organization and accounts that are shared with an external entity.

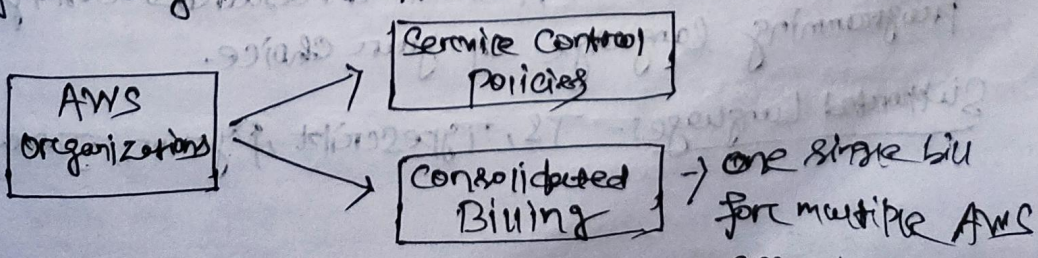
→ IAM access analyzer validates IAM policies against policy grammar and best practices.

→ IAM access analyzer generates IAM policies based on access activity in your AWS CloudTrail logs.

(22) AWS organizations

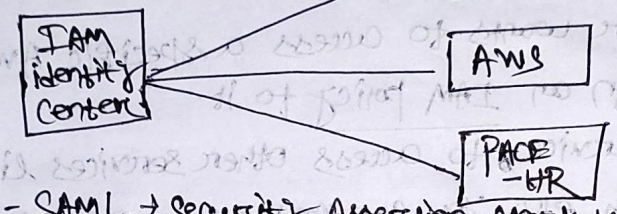
→ Account management service enables you to consolidate ~~multi~~ multiple AWS account into an organization that you ~~centrally~~ create and centrally manage.

→ Service Control policies (SCPs) are used to manage the security and permissions that are available to your organizations AWS accounts.



(23) IAM Identity Center (successor to AWS SSO) allows centralized access to multiple AWS accounts and provides users with single sign-on access to all their assigned accounts and applications from one place.

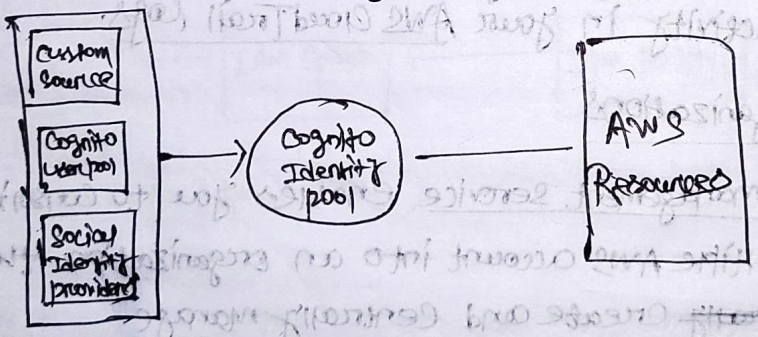
Keyword:-



Keyword:- SAML → Security Assertion Mark-up Language, or SAML, is a standardized way to tell external applications and services that a user is who they say they are.

(24) Amazon Cognito provides authentication, authorization, and user management service for your web and mobile apps.

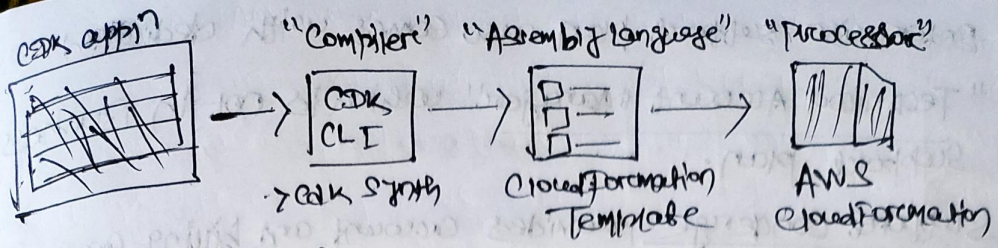
Keyword → social media logins



(25) AWS Cloud Development Kit

→ AWS CDK is an open-source framework that lets you model and provision AWS cloud resources using the programming language of your choice.

Supported Languages:- JS, Typescript, Python, Java, .NET



(26) Trusted Advisor

→ AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in 6 major categories:→ (i) Cost Optimization
(ii) Performance
(iii) Security
(iv) Fault tolerance
(v) Service limits
(vi) Operational excellence

(27) AWS CloudTrail → records the activities in your AWS account so that administrators can track on which user has performed which operation in AWS account.

Key Term: Record API Calls

(28) AWS Artifact → Central resource for compliance-related information.

(29) AWS Marketplace → is a catalog with thousand of software listings from software vendors which makes it easy for customers to deploy solutions in AWS.

(30) AWS support plans → Basic, Developer, Business, Enterprise

→ Chat support and AWS managed service is available from Business plan and higher.

→ AWS Infrastructure Event Management (IEM) offers architecture and scaling guidance and operational support during the preparation and execution of planned events such as shopping holidays etc.

↳ Available in enterprise for free and in business for additional fee.

→ Enterprise support plan also comes with dedicated "Technical Account Manager" which is not in Business Support plan.

→ Support Concierge provides account and billing analysis to help cut costs.
↳ Available in Enterprise plan.

(31) Amazon Partner Network (APN)

→ AWS partner Network (APN) is a group of external vendors (consultants) that have received endorsement from AWS regarding their expertise in building and maintaining implementing solutions for AWS.

→ The AWS professional services organization is a global team of experts that can help you realize your desired business outcome on AWS.

(32) AWS re:post includes AWS official knowledge center articles and videos covering the most frequent questions and requests that AWS receives from customers.

(33) AWS Budget gives you the ability to set custom budgets that alerts you when your cost or usage exceed (or are forecasted to exceed) your budgeted amount.

(34) With AWS Cost and Usage Report (CUR), you can retrieve, itemize, and organize the most comprehensive cost and usage data for your account.

(35) Amazon QuickSight allows building interactive business intelligence dashboard.
Can include ML insights.

(35) AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

(36) AWS Config allows customers to audit and monitor changes to AWS resources.

Key-words: - track, record, audit, evaluate

(37) AWS CloudFormation

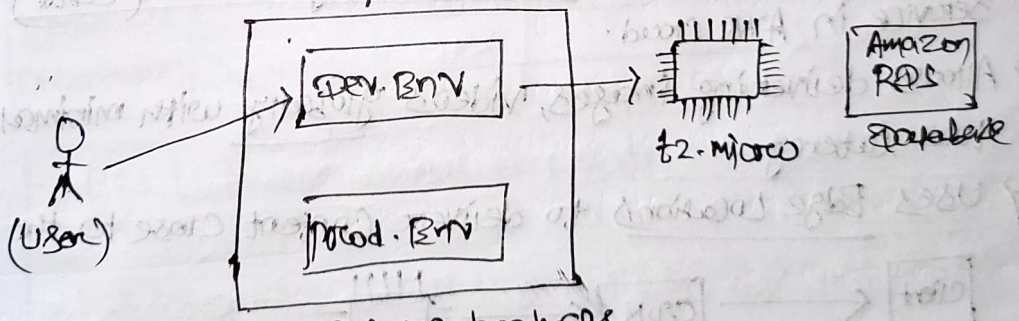
→ AWS CloudFormation is the Infrastructure as Code (IAC) solution in AWS.

→ Allows customers to create a reusable code template (repeatable version) to deploy resources across multiple accounts, regions.

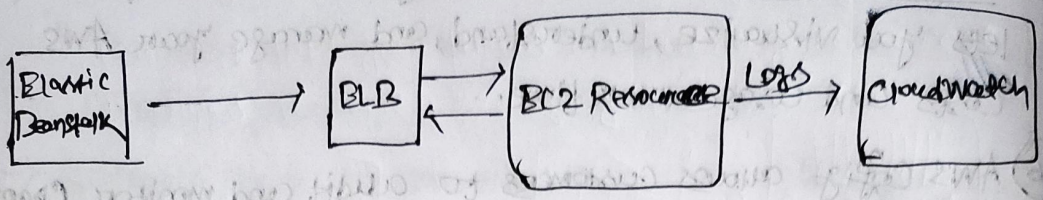
(38) AWS Service Catalog

→ AWS service catalog enables organization to create and manage catalogs of IT services approved for use on AWS.

→ Uses CloudFormation / Terraform IAC templates behind the scene.



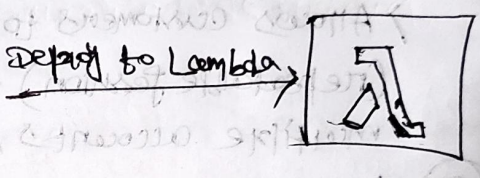
(39) AWS Elastic Beanstalk allows users to quickly deploy web applications on AWS without much knowledge of services so that customers can focus on your business.



(40) AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers.

```
export const handler =
async(event) => {
   const response = {
      statusCode: 200,
      body:
      JSON.stringify("Hello!");
      };
   return response;
};
```

Application Code

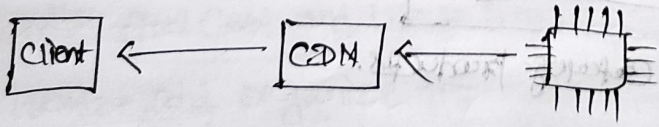


(41) Amazon CloudFront

→ Amazon CloudFront is a Content delivery network (CDN) service in AWS cloud.

→ Allows delivering images, videos globally with minimal / low latency.

→ Uses Edge Locations to deliver content close to the users



CDN → (i) Content delivery network (CDN) is a network of servers that caches content close to the end users, improving website performance, security and reliability.

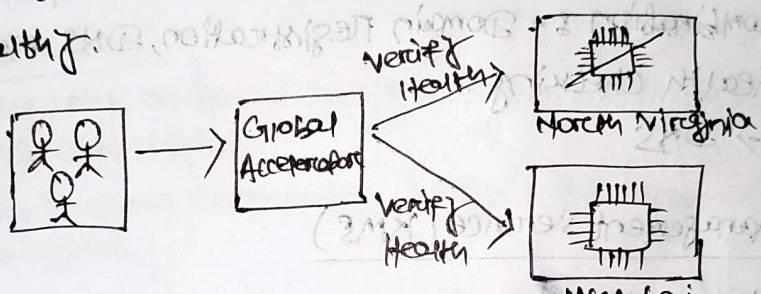
(ii) It reduces latency, bandwidth costs and DDOS attacks.

(42) Global Accelerator

→ Global accelerator improves performance by sending traffic through the AWS worldwide network infrastructure.

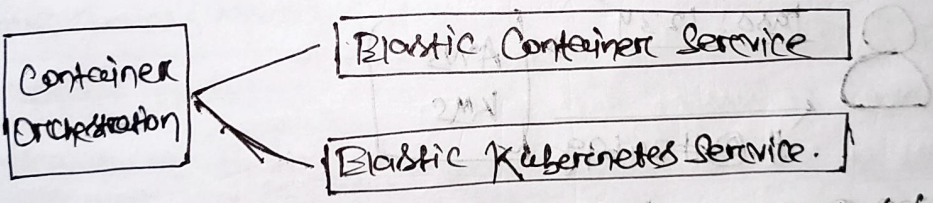
(43) Global Accelerator - Failover Capabilities

→ Global accelerator can also continuously monitor the health of all endpoints, and instantly begins directing traffic for all new connections to another available endpoint when it determines an active endpoint is unhealthy.



(44) Container Orchestration in AWS

Two primary services that are extensively used for container container orchestration use-cases.

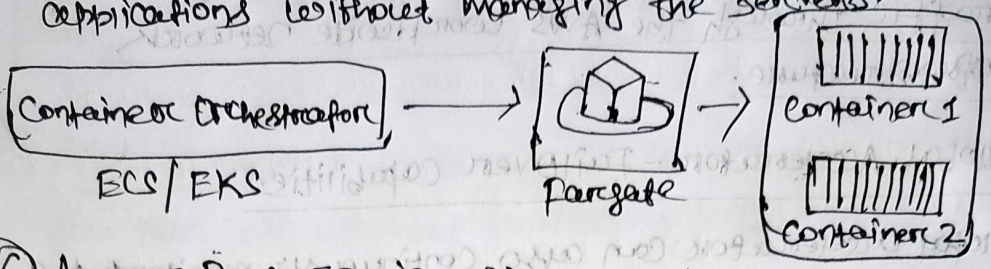


→ ECS is better suited for simple applications, while EKS is used for deploying Kubernetes clusters on AWS.

→ ECS integrates better with AWS ecosystem, where EKS offers more control.

→ EC2 relies on AWS-provided services like ALB, Route 53, etc., while EKS handles all these mechanisms internally, just as in any old Kubernetes cluster.

(45) AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building containers applications without managing the servers.



(46) Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service.

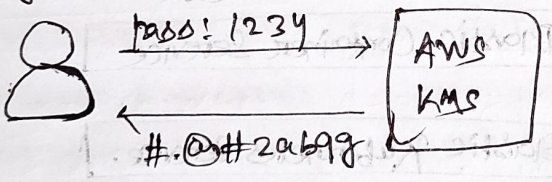
→ You can use Route 53 to perform 3 main functions in any combination :- Domain registration, DNS routing, and health checking.

Key-word → DNS

(47) Key Management Service (KMS)

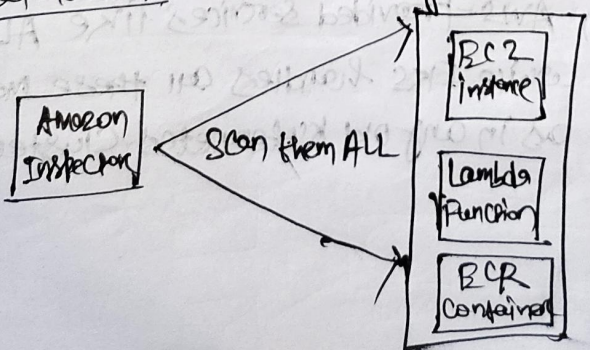
→ Provides encryption and decryption related functionality.

→ Integrates with wide variety of services like S3, EBS, DynamoDB etc.



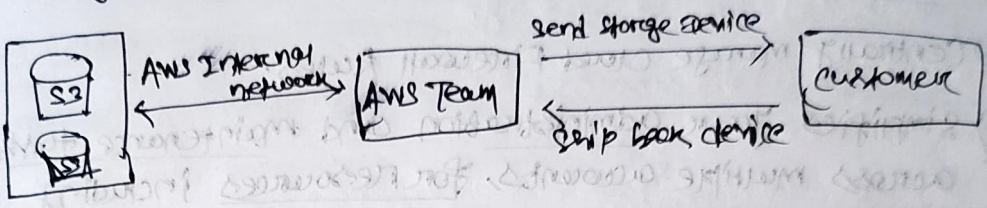
(48) Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerability and unintended network exposure.

Catchword! - Vulnerability



(49) AWS Shield is a managed Distributed Denial of Service (DDoS) service that safeguards the workloads running on AWS against DDoS attacks.

(50) AWS Snowball family allows customers to accelerate moving offline data or remote storage to the cloud.



Devices:-

(1) Snowball Edge

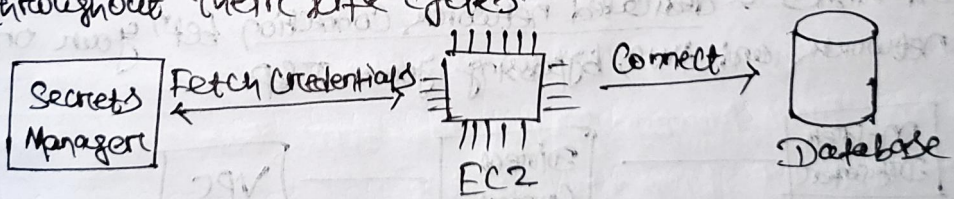
↳ Device with on-board storage and compute power for select AWS capabilities.

↳ Can perform computation, analysis in areas without internet connectivity.

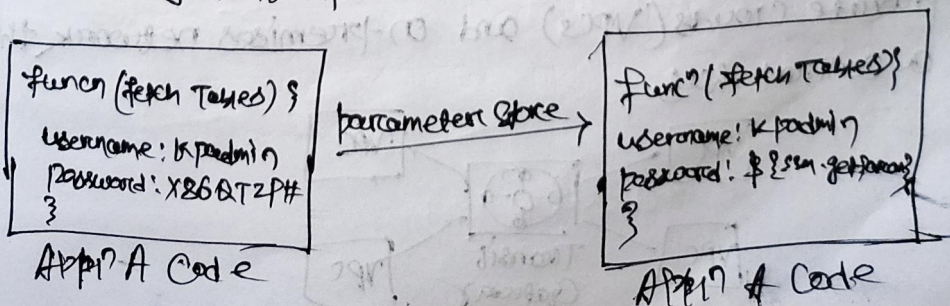
(2) Snowmobile

↳ Quickly and securely transfer up to 100 petabytes of data in as little as a few weeks.

(50) AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their life cycles.



(51) Systems Manager Parameter Store provides secure storage and management of secrets.



Secrets Manager Vs. Parameter Store

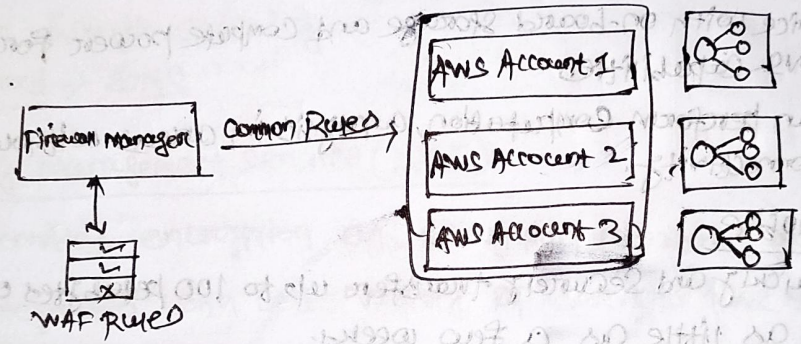
→ MOST Cost-Effective for Secrets Storage = Parameter Store

→ If you need automatic credentials rotation = Secrets Manager

(52) Firewall Manager

→ Centrally manage cloud Firewall Rules.

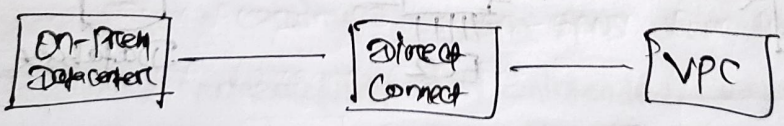
→ Simplifies your administration and maintenance tasks across multiple accounts, for resources including AWS WAF, AWS Shield Advanced, Amazon VPC security groups, AWS Network Firewall.



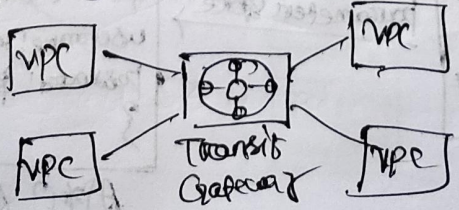
(53) AWS Direct Connect links your internal network to AWS services over a fiber optic cable. It

→ Delivers consistent, low-latency performance.

→ Establishes a dedicated network connection b/t your on-premises network and AWS, bypassing your ISP.



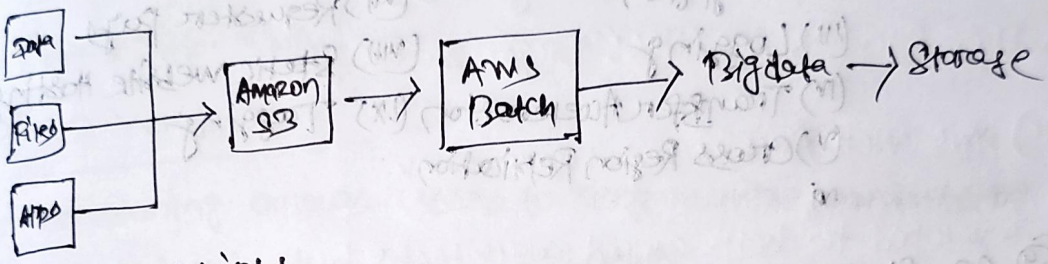
(54) AWS Transit Gateway connects your Amazon Virtual private clouds (VPCs) and on-premises network through a central hub.



(55) Amazon Macie makes use of machine learning to identify sensitive data stored in AWS.

Amazon Macie → Continually Evaluate Amazon S3 Storage → Automated Sensitive data discovery → Full discovery scans → Take action

(56) AWS Batch enables developers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.



Catch-word : Jobs

(57) AWS Tags

→ A Tag is a label that you assign to an AWS resource.

→ Each tag consist of a key and an optional value.

* Cost Allocation Tags can be used to track bill associated with tagged resources.

Miscellaneous Pointers

→ For use-cases where you want to achieve high-availability with enabling failover across regions, you can use services like Route 53, Global Accelerator.

→ If you want to gain full control of patch management for OS, you should choose EC2 over other managed services.

→ Temporary, Limited Time credentials = AWS STS (Simple Token Service).

(58) Amazon S3

→ AWS Simple Storage Service (S3) is an Object storage designed to store and retrieve any amount of data from anywhere.

Catch-words: Object Storage

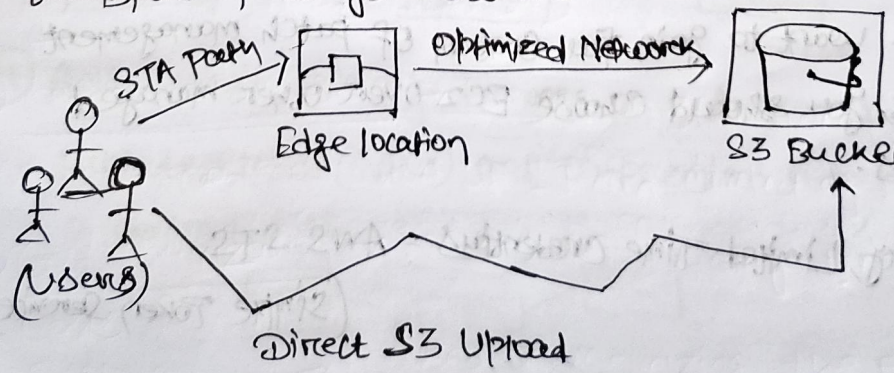
Features :- (i) Versioning
(ii) Encryption
(iii) Logging
(iv) Transfer Acceleration
(v) Cross Region Replication
(vi) Events
(vii) Requester pays
(viii) Static website Hosting
(ix) Tagging

(59) S3 - Storage classes

- → S3 Standard
- → S3 Standard - Infrequent Access
- → S3 one zone - Infrequent Access
- → Intelligent Tiering
- → Amazon S3 Glacier

(60) S3 - Transfer Acceleration

S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by 50 - 500%. for long-distance transfer of larger objects.



(61) S3 Encryption

→ All Amazon S3 buckets have encryption configured by default, and objects are automatically encrypted.

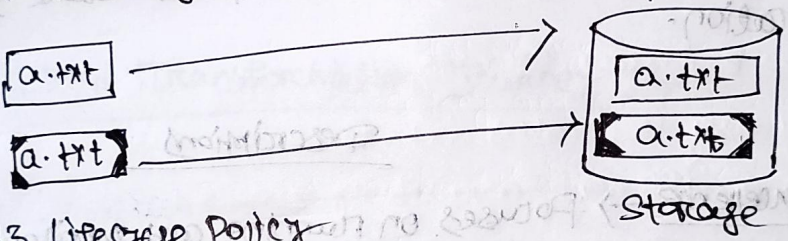
Two major encryption schemes to protect objects:

1. Server-side encryption with Amazon S3 managed keys (SSE-S3) – default
2. Server-side encryption with AWS KMS managed keys (~~AWS~~ SSE-KSM)

(62) S3 versioning

→ Versioning allows users to keep multiple variants of an object in the same S3 bucket.

→ Protects against accidental deletion/overwrites.



(64) S3 Lifecycle Policy

→ An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.

Type of Actions	Description
Transition actions	Define when objects transition to another storage class: Eg: After 30 days, move objects to Glacier.
Expiration actions	define when objects expire. S3 deletes expired objects on your behalf.

Points to Note

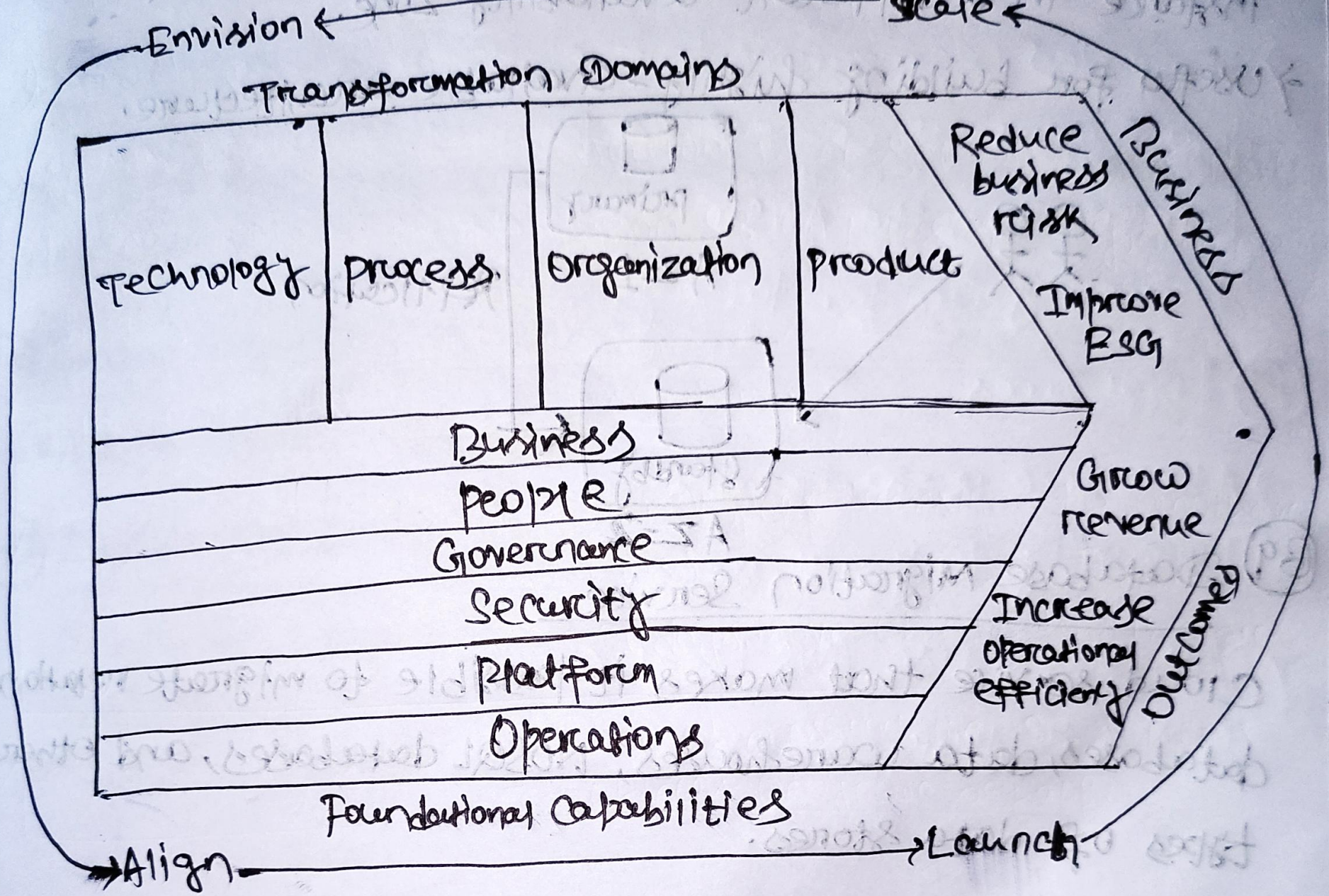
1. Object Storage = S3
2. Block Storage = EBS
3. File Storage = EFS (NFS)
4. Most Cost effective storage = S3
5. Free services in AWS: Organization, IAM

(65) AWS Well-Architected Framework

developed to help cloud architects build secure, high-performing, resilient and efficient infrastructure for their application.

Pillars	Descriptions
① Operational Excellence	→ Focuses on running and monitoring systems, and continually improving processes and procedures.
② Security	→ Focuses on protecting information and systems.
③ Reliability	→ Focuses on workloads performing their intended functions, and how to recover quickly from failure to meet demands.
④ Performance Efficiency	→ Focuses on structured and streamlined allocation of IT and computing resources.
⑤ Cost Optimization	→ Focuses on avoiding unnecessary costs.
⑥ Sustainability	→ Focuses on minimizing the environmental impacts of running cloud workloads.

(66) Cloud Transformation Journey Phases



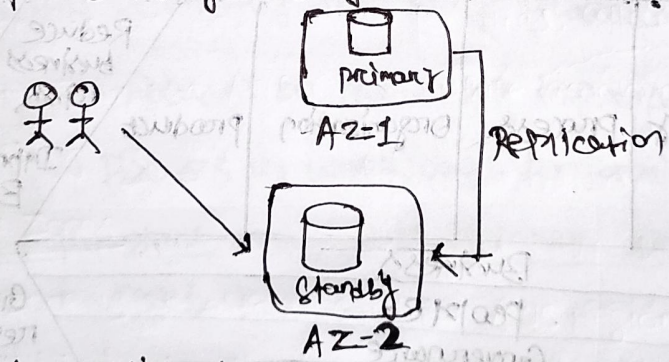
(67) Database Primer

Database Types/compatibility	Services
Relational Database(MySQL)(OLTP)	RDS, Aurora
postgreSQL	Aurora, RDS
NoSQL, key-value DB, Non-Relational DB	DynamoDB
Time Series Database	TimeStream
In-Memory database, Caching	Redis, Memcached
Extract, Transform, Load (ETL)	Glue
Graph Database	Neptune

(68) RDS Multi-AZ Architecture

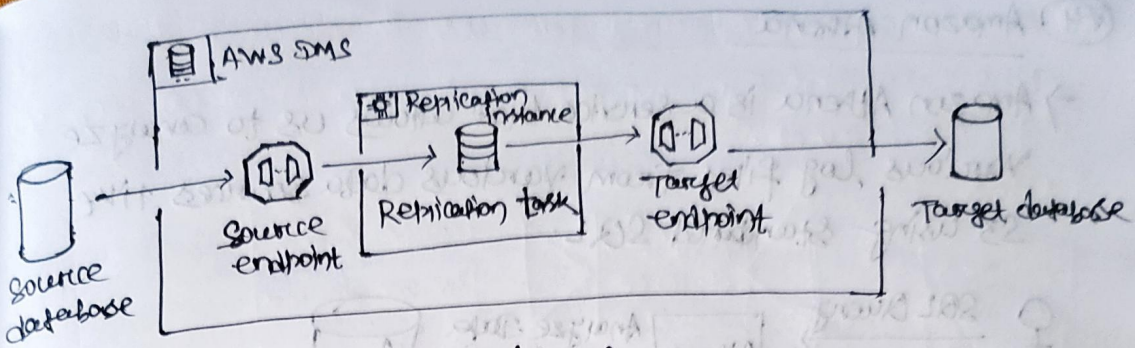
→ In this approach, Amazon creates a standby DB instance and synchronously replicates data from the primary DB instance in a different availability zone.

→ Useful for building highly-available architecture.



(69) Database Migration Service

Cloud service that makes it possible to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores.



#10 Simple Queue Service (SQS)

-> Fully managed message queuing service.
-> Supports First-In-First-Out messaging (FIFO).
-> Useful for architecture design of loosely coupled systems.

-> Loosely Coupled System, Microservice Architecture = Important Design Principle (SQS, Step Function)
-> Tightly couple system, Monolithic Architecture = Bad Design

#11 Simple Notification Service (SNS)

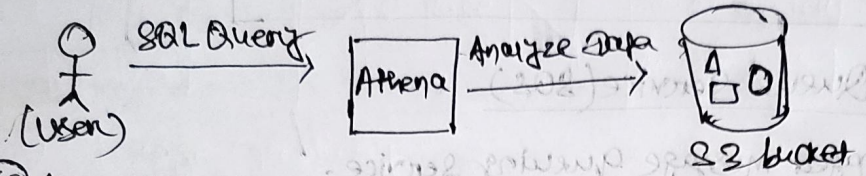
-> SNS is a fully managed messaging and mobile notification service for delivering messages to the subscribed endpoints.
-> Can send text messages (SMS), emails etc. from distributed applications.

#12 Amazon Workspace is a fully managed, secure, reliable virtual desktop solutions.

#13 Amazon Appstream is a secure, reliable, and scalable application streaming and low-cost virtual desktop service.

#4 Amazon Athena

→ Amazon Athena is a service that allows us to analyze various log files from various data sources like S3 using standard SQL.



#5 AWS-CloudShell

→ A browser-based shell which allows you to quickly run CLI commands, scripts with the AWS Command Line Interface (CLI), experiment with services using the CLI, and use other tools to increase your productivity.

#6 AWS Outposts

→ AWS outposts is a fully managed service by AWS that extends AWS infrastructure, services, and APIs to your on-premises environment.

→ It enables organizations to run AWS applications in their own data centers or on-premises facilities, allowing them to benefit from the AWS cloud while maintaining local data processing and low latency.

#7 Local Zones

→ A local zone is an extension of an AWS Region in geographic proximity to your users.

→ You should use AWS Local Zones to deploy workloads closer to your end-users for low-latency requirements.

#8 Developer Tools

(i) CodeCommit :- Git repository for storing central code. [version control]

(ii) CodeBuild :- Build and Test code

(iii) CodeDeploy :- To deploy application

(iv) CodePipeline :- Connects CodeCommit, CodeBuild, CodeDeploy

(v) CodeStar :- Setup continuous delivery pipeline easily.

(vi) CodeGuru :- Improving code Quality.

(vii) X-Ray :- Capability to view end-to-end performance metrics and troubleshoot distributed applications

(viii) Cloud9 :- IDE that lets you write, run and debug your code with just a browser.

(ix) ECR :- Store and manage Docker Container images.

(x) Redshift :- Data Warehouse

(xi) API Gateway :- Rest APIs

#9 AWS Health :-

→ AWS Health events are notifications that AWS health sends on behalf of other AWS services.

→ You can use these events to learn about upcoming or scheduled changes that might affect your account.

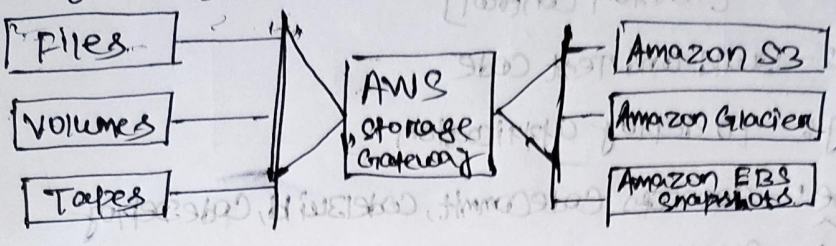
#10 Amazon FSx

→ Amazon FSx makes it easy and cost-effective to launch and run popular file systems.

Eg :- Requirement of a fully managed Windows File server can be achieved using Amazon FSx.

- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File server
- Amazon FSx for Lustre

(81) Amazon S3 File Gateway provides an interface via NFS, SMB for synchronization of data from on-premise to S3 bucket.



(82) Storage Gateway

→ AWS storage Gateway allows both your on-premises applications and your cloud based applications to access storage that is available in the AWS cloud.

Catch-word!- Tape Gateway (Library), Volume Gateway, Cached Volumes

(83) Machine Learning Services

(i) Comprehend:- NLP service that use machine-learning to uncover valuable insights and connections in text.

(ii) Translate:- Neural machine translation service that delivers fast, high-quality, affordable, and customizable language translation.

(iii) Textract:- Automatically extracts text, handwriting, and data from scanned documents.

(iv) Lex:- Build, test and deploy conversational interfaces in applications

(v) Transcribe:- automatic speech recognition service to convert audio to text.

(vi) Kendra:- enables your users to search structured and unstructured data.

(84) Application Discovery Service

-> AWS Application Discovery Service helps enterprise customers plan migration projects by gathering information about their on-premises data centers.

-> Can gather information like Hostname, Mac Address, IP Address etc.

(85) AWS Codestar is a cloud service designed to make it easier to develop, build, and deploy applications on AWS by simplifying the setup of your entire development project.

(86) AWS CDK is a software development framework that enables developers to define Infrastructure as Code (IaC) using familiar programming languages like Typescript, Python, Java, C#, and more.

(87) An Amazon Machine Image (AMI) is a special type of virtual appliance used to create virtual machine within Amazon EC2.

↳ It serves as the basic unit of deployment for services delivered using EC2.

↳ An AMI includes necessary information to launch an instance, such as Operating System, application server, and applications.

(88) AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregate alerts, and enables automated remediation.

Ashish