- **Amazon CloudWatch** - Amazon CloudWatch is a **monitoring** and **observability** service built for **DevOps** engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to **system-wide performance changes**, **optimize resource utilization**, and get a **unified view of operational health**. This is an excellent service for building Resilient systems. It also enables us to create **rules for events handling**.

- **AWS Systems Manager** – AWS Systems Manager gives you **visibility** and **control** of your infrastructure on AWS. Systems Manager provides a **unified user interface** so you can view **operational data** from multiple AWS services and allows you to automate operational tasks such as **running commands, managing patches** and **configuring servers** across your AWS resources **as well as on-premises infra**. With Systems Manager, you can **group resources**, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view **operational data for monitoring and troubleshooting**, and take action on your groups of resources. You can also use AWS Systems Manager to **apply patches to your EC2 instances** or **on-premises instances**. **You cannot use Systems Manager to apply patches to the underlying OS for AWS Aurora**.

- **AWS KMS** – AWS Key Management Service (KMS) makes it easy for you to **create and manage cryptographic keys** and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that **uses hardware security modules** that have been validated under **FIPS 140-2**, or are in the process of being validated, to protect your keys.

- **Configure the database in RDS Multi-AZ deployment with automatic failover to the standby :-**
  When you provision a Multi-AZ DB Instance, Amazon RDS automatically **creates a primary DB Instance** and **synchronously replicates the data to a standby instance** in a different Availability Zone (AZ). In case of an infrastructure failure, Amazon RDS(Relational DB service) performs an automatic failover to the standby (**or to a read replica in the case of Amazon Aurora**), so that you can resume database operations as soon as the failover is complete. Since the **endpoint for your DB Instance remains the same after a failover**, your application can resume database operation without the
- need for manual administrative intervention.

Another option which was incorrect– (**Configure the database in RDS read replica mode with automatic failover to the standby)** – For RDS, Read replicas allow you to create read-only copies that are synchronized with your master database. **There is no standby available while using read replicas.** In case of infrastructure failure, you have to manually promote the read replica to be its own standalone DB Instance, which means that the **database endpoint would change**.

- (If you can deploy database using beanstalk)**You cannot deploy only a database via Elastic Beanstalk** as its meant for **automatic application** deployment **when you upload your code**. Then Elastic Beanstalk automatically handles the deployment, from **capacity provisioning**, **load balancing**, **auto-scaling** to **application health monitoring**.
- **Deploy the database via CloudFormation** – You can deploy the database via CloudFormation for sure, however, **it does not provide any automatic recovery** in case of a disaster.
- **Amazon Aurora** is a **MySQL** and **PostgreSQL**-compatible relational database built for the cloud. Amazon Aurora is **fully managed** by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like **hardware provisioning, database setup, patching**, and **backups**. The **AWS Product team** is responsible for **applying patches to the underlying OS** for AWS Aurora.
- **(who can apply Patches to AWS Aurora) -** The AWS Support after receiving a request from the customer – AWS Support handles support tickets regarding AWS services. **AWS Support is not responsible** for applying patches to the underlying OS for AWS Aurora. **The AWS customer by SSHing on the instances** – **Answer is No**. AWS customers are only responsible for patching their own EC2 instances. So only **product Team can apply.**
- The **AWS Abuse team** can assist you when AWS resources are used to engage in abusive behavior. You need to contact the AWS Abuse team for **prohibited use of AWS services**. E.g. AWS owned IP-addresses are being used to carry out malicious attacks.
- **Amazon Route 53** is a highly available and scalable cloud **Domain Name System (DNS**) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names to IPs.

- **Weighted routing Policy** of Route 53 lets you **associate multiple resources with a single domain** name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software. To configure weighted routing, you **create records that have the same name and type for each of your resources**. You **assign each record a relative weight** that corresponds with how much traffic you want to send to each resource. Amazon Route 53 **sends traffic to a resource based on the weight** that you assign to the record as a proportion of the total weight for all records in the group.

- **Failover routing policy** – This routing policy is used when you want to configure **active-passive failover.**

- **Simple routing policy** – With simple routing, you typically route traffic to a **single resource**, for example, to a web server for your website.

- **Geolocation routing policy** – Use when you want to route traffic based on the **location of your users.**

- **Geoproximity routing policy** – Use when you want to route traffic based on the **location of your user and resources both** and, optionally, shift traffic from resources in one location to resources in another.

- **Latency routing policy** – This routing policy is used **when you have resources in multiple AWS Regions** and you want to route traffic to the region that provides the best latency.

<u>Support Plans in AWS</u> (Plans are subject to a 30 day minimum term. **)-**

- **Enterprise(***Recommended if you have business and/or mission critical workloads in AWS.***) –** Its main focus is helping the customer achieve their outcomes and find success in the cloud. You get **24×7 technical support from high-quality engineers**, **tools and technology to automatically manage the health of your environment**, **consultative architectural guidance delivered** in the context of your applications and use-cases, and a **designated Technical Account Manager (TAM)** to coordinate access to proactive/preventative programs and **AWS SMEs**. You get full access to **AWS Trusted Advisor** Best Practice Checks. You get access to **guidance**, **configuration**, and **troubleshooting** of AWS interoperability with many common operating systems, platforms, and application stack components. Unlimited cases / unlimited contacts and **Access to online self-paced labs**.

- **Business** – AWS recommends Business Support **if you have production workloads** on AWS and **want 24×7 phone, email and chat access** to Cloud Support Engineers and **architectural guidance in the context of your specific use-cases**. You get full access to **AWS Trusted Advisor** Best Practice Checks. You get access to **guidance**, **configuration**, and **troubleshooting** of AWS interoperability with many common operating systems, platforms, and application stack components. Unlimited cases / unlimited contacts

- **Basic** – The basic plan only provides access to the following:
  Customer Service & Communities – (i)**24×7 access to customer service**, **documentation**, **whitepapers**, and **support forums**. (ii)**AWS Trusted Advisor** – Access to the **7 core Trusted Advisor checks** and **guidance to provision your resources** following best practices to increase performance and improve security. (iii)**AWS Personal Health Dashboard** – A personalized view of the health of AWS services, and alerts when your resources are impacted.

- **Developer(***Recommended if you are experimenting or testing in AWS.***)** – AWS recommends Developer Support **plan if you are testing or doing early development on AWS** and want the ability to get **email-based technical support during business hours**. **AWS Trusted Advisor** – Access to the **7 core Trusted Advisor checks.** This plan also supports **general guidance** on how services can be used for various use cases, workloads, or applications. You do not get access to Infrastructure Event Management with this plan. Unlimited cases / 1 primary contact. This plan **does not support 24×7 phone based** technical support.

  Note : Both Basic and Developer plan do not support access to **guidance**, **configuration**, and **troubleshooting** of AWS interoperability with **third-party software**.

Amazon Macie - Amazon Macie is a fully managed **data security and data privacy** service that **uses machine learning and pattern matching** to discover and **protect your sensitive data** in AWS. Macie automatically **provides an inventory** of **Amazon S3 buckets** including a **list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside** those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and **alert you to sensitive data**, such as personally identifiable information (PII).

- **AWS Glue(ETL, Serverless)** – AWS Glue is a fully managed extract, transform, and load (**ETL**) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing. It is **Serverless.** ETL code that will be generated is **python Code**. Out-of-the Box integration with Amazon Athena, EMR and Redshift.

- **Amazon Polly** – Amazon Polly is a service that turns **text into speech**, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's **Text-to-Speech** (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. In addition to Standard TTS voices, Amazon Polly offers **Neural Text-to-Speech (NTTS)** voices that deliver advanced improvements in speech quality through a new machine learning approach. Polly's Neural TTS technology also **supports two speaking styles** that allow you to better match the delivery style of the speaker to the application.

- **AWS Secrets Manager** – AWS Secrets Manager helps you **protect secrets needed to access your applications, services, and IT resources**. The service enables you to easily rotate, manage, and retrieve **database credentials, API keys, and other secrets** throughout their lifecycle. Users and applications **retrieve secrets with a call to Secrets Manager APIs**, eliminating the need to hardcode sensitive information in plain text. You cannot use Secrets Manager for creating and using your own keys for encryption on AWS services.

- On-Demand pricing is always computed by the second (**with a minimum charge of 60 seconds**), even if the prices you see on the AWS site are per hour. Suppose I have launched an instance and terminated it within 30 sec then I will be charged with minimum of 60 seconds since it is a minimum time charge.

- **S3 Glacier Deep Archive** – S3 Glacier Deep Archive is Amazon S3's **lowest-storage class** and **supports long-term retention** and digital preservation for data that **may be accessed once or twice in a year**. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that **retain data sets for 7-10 years** or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. **It has a retrieval time (first byte latency) of 12 to 48 hours**. S3 Glacier Deep Archive takes the most time to retrieve data.

- **S3 Standard** – S3 Standard offers high durability, availability, and performance object storage for **frequently accessed data**. S3 Standard has a retrieval time (first byte latency) of **milliseconds**. Largest single upload size is **5 GB. Default 3 Replicas in AZs. Storage cost is higher than access cost.**

- **S3 Standard Infrequent Access** – when infrequent data (like for 30 days not accessed). S3 Standard IA has a retrieval time (first byte latency) of **milliseconds**. **3 Replicas in AZs. Accessing cost is higher than storage cost.** Data that is deleted within 30 days will be **charged f**
- **or whole 30 days**.

- **S3 Intelligent-Tiering** – The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically **moving data to the most cost-effective access tier**, without performance impact or operational overhead. It works by storing objects in two access tiers: **S3 Standard** and **S3 Standard IA.** S3 Intelligent-Tiering has a retrieval time (**first byte latency**) of **milliseconds**. No charges when data is moving between access tiers. Object size **of less than 128KB cannot** be moved to Intelligent tiering.

- **S3 Glacier** – Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class **for data archiving and long-term backup**. It is designed to deliver 99.999999999% durability. S3 Glacier has a retrieval time (first byte latency) of **minutes or a few hours**.

- **S3 One Zone Infrequent**: Data limited to only **one AZ and access less frequently but require quick access when required. Cheaper than S3 Standard Infrequent Access.** Although S3 One Zone-IA offers less availability than S3 Standard IA but that's not an issue for the given use-case(one of the question) since the thumbnails can be regenerated easily.

- **Layer 7 (Http/Https)- AWS WAF** is a web application firewall that lets you monitor the **HTTP** and **HTTPS** requests that are forwarded to an Amazon Gateway API, Amazon CloudFront or an Application Load Balancer. HTTP and HTTPS requests are part of the Application layer, which **is layer 7**.

- **Layer 3** – Layer 3 is the **Network layer** and this layer decides which physical path data will take when it moves on the network**. AWS Shield** offers protection at this layer.

- **Layer 4** (**TCP/UDP/TLS**)– Layer 4 is the **Transport layer** and this layer data transmission occurs using TCP or UDP protocols. **AWS Shield** offers protection at this layer.

- **Amazon Inspector** is an automated **security assessment** service that helps improve the **security and compliance of applications deployed on your Amazon EC2** instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

- **Amazon GuardDuty(Account related)** – Amazon GuardDuty is a **threat detection service** that monitors **malicious activity** and **unauthorized behavior** to protect your AWS account. GuardDuty **analyzes billions of events across your AWS accounts** from AWS **CloudTrail** (AWS user and API activity in your accounts), Amazon **VPC Flow Logs** (network traffic data), and **DNS Logs** (name query patterns). This service is for **AWS account level access**, **not for instance-level management** like an EC2.

- **AWS Shield** (**DDOS**)– AWS Shield is a managed **Distributed Denial of Service (DDoS)** protection service that **safeguards applications** running on AWS. AWS Shield provides **always-on detection and automatic inline mitigations** that minimize application downtime and latency, so there is **no need to engage AWS Support to benefit from DDoS protection**. Shield is general protection against DDos attacks for all resources in the AWS network, and **not an instance-level security assessment service**.

- **Dedicated instance** – Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. **Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.**

- **Lambda** – AWS Lambda **lets you run code without provisioning or managing servers**. You **pay only for the compute time you consume**. With Lambda, you can run code for virtually any type of application or backend service – all with **zero administration**. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability when triggered. Based on **Triggered** Functionality.

- **EMR** – Amazon EMR is the **industry-leading cloud big data platform** for processing vast amounts of data using open source tools such as Hadoop, Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. **Amazon EMR can be used to provision resources to run big data workloads on Hadoop clusters**. EMR provisions EC2 instances to manage its workload. **EMR is not a serverless service like lambda**.

- **Elastic Beanstalk** AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. **You simply upload your code** and Elastic Beanstalk automatically handles the deployment, from **capacity provisioning, load balancing, auto-scaling to application health monitoring**. Beanstalk provisions servers so it is not a **serverless service**.
  Since Amazon Elastic Beanstalk is a **PaaS layer**, **developers push the code along with the metadata.** The metadata contains the details of the AMI, language, framework, and runtime requirements along with connection information of databases or dependencies. Based on the metadata, AWS Elastic Beanstalk launches an appropriate AMI and configures it to run the code.

- **AWS Direct Connect** is a cloud service solution that makes it easy to establish a **dedicated network connection from your premises to AWS**. You can use AWS Direct Connect to establish a **private virtual interface from your on-premise network directly to your Amazon VPC**, providing you with a private, **high bandwidth network connection** between your network and your VPC. **This connection is private and does not go over the public internet.** *It takes at least a month to establish this physical connection.*

- **Amazon VPC Endpoint** – A VPC endpoint enables you to **privately connect your VPC to supported AWS services** and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC **do not require public IP addresses** to communicate with resources in the service. Traffic between your VPC and the other service **does not leave the Amazon network**. VPC Endpoint **cannot** be used to privately connect on-premises data center to AWS Cloud.

- **Internet Gateway** – An Internet Gateway is a **horizontally scaled**, redundant, and highly available **VPC component** that allows communication between your **VPC and the internet**. An internet gateway serves two purposes: **to provide a target in your VPC route tables for internet-routable traffic** and to **perform network address translation (NAT) for instances**. Internet Gateway **cannot** be used to privately connect on-premises data center to AWS Cloud.

- **Site-to-Site VPN** – AWS Site-to-Site VPN creates a secure connection **between your data center or branch office and your AWS cloud resources**. This connection **goes over the public internet** unlike **Direct Connect**.

- AWS Rekognition is an example of a SaaS service.

- **Instance Store** - An instance store provides **temporary block-level storage** for your instance. This storage is located on **hardware disks** that are physically attached to the host computer. This is a good option when you need **storage with very low latency**, but you **don't need the data to persist when the instance terminates**.

- **EFS** – Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic **NFS file system**. EFS is **not available as a hardware disk on the instance**.

- **EBS** – Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. EBS is **not available as a hardware disk on the instance.**

- **AWS Budgets** (**alerts, no forecasting**)gives you the ability to **set custom budgets that alert you when your costs or usage exceed** (or are forecasted to exceed) your budgeted amount.
  You can also use AWS Budgets to set reservation utilization or coverage targets and **receive alerts when your utilization drops below the threshold** you define. Reservation alerts are supported for **Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElasticCache**, and Amazon **Elasticsearch** reservations. AWS Budgets cannot forecast your AWS account cost and usage.

- **Simple Monthly Calculator** provides an estimate of usage charges for AWS services based on certain information you provide. It helps customers and prospects **estimate their monthly AWS bill more** efficiently. **You cannot use this service to receive alerts when the reservation utilization falls below the defined threshold**.

- **AWS CloudTrail** (**monitor account activity, also stores in S3**)– AWS CloudTrail is a service that enables **governance, compliance, operational auditing, and risk auditing of your AWS account**. With CloudTrail, **you can log, continuously monitor, and retain account activity** related to actions across your AWS infrastructure. **CloudTrail provides event history of your AWS account activity**, including actions taken through the **AWS Management Console**, **AWS SDKs**, **command-line tools**, and other AWS services. CloudTrail can be used to record AWS API calls and other activity for your AWS account and **save the recorded information to log files in an Amazon Simple Storage Service (Amazon S3)** bucket that you choose. By default, the log files delivered by CloudTrail to your S3 bucket are **encrypted using server-side encryption with Amazon S3–managed encryption keys** (SSE-S3).

- **AWS Trusted Advisor** – AWS Trusted Advisor is an **online tool** that **provides real-time guidance to help provision your resources** following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyzes your AWS environment **and provides best practice recommendations in five categories**:
  1. **Cost Optimization**
  2. **Performance**
  3. **Security**
  4. **Fault Tolerance**
  5. **Service Limits**.

  and 7 core checks are:
  1. S3 bucket Permissions
  2. Security Groups – Specific Ports Unrestricted
  3. IAM use
  4. MFA on root account
  5. EBS public snapshots
  6. RDS public snapshots
  7. Service Limits

- **Amazon Redshift** – Amazon Redshift is a fully-managed **petabyte-scale cloud-based** data **warehouse product** designed for **large scale data set storage and analysis**.

- **Storage Gateway** – It is a **hybrid storage** that enable on-premises applications to seamlessly use AWS cloud storage. AWS Storage Gateway service provides three different types of gateways(**TVF**) – **Tape Gateway, File Gateway, and Volume Gateway** – that seamlessly connect on-premises applications to cloud storage, **caching data locally for low-latency access.**

- **Database Migration Service** – AWS Database Migration Service helps you **migrate databases** to AWS quickly and securely. **The source database remains fully operational during the migration**, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

- **SQS** – Amazon Simple Queue Service (SQS) is a fully managed **message queuing service** that enables you to **decouple and scale microservices, distributed systems, and serverless applications**. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

- **SNS** – Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed **pub/sub messaging service** that enables you to **decouple microservices, distributed systems, and serverless applications**. Using Amazon **SNS topics**, your **publisher systems can fan-out messages to a large number of subscriber endpoints** for parallel processing, **including Amazon SQS queues, AWS Lambda functions, and HTTP/S webhooks**. Additionally, **SNS can be used to fan out notifications to end users using mobile push, SMS, and email.**

- **Step Function** – AWS Step Function lets you **coordinate multiple AWS services into serverless workflows**. Use Step Functions to **combine multiple AWS Lambda functions** into responsive serverless applications and microservices, without having to write code for **workflow logic**, parallel processes, **error handling**, timeouts or **retries**.

- **Regions -** AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. **Each AWS Region consists of two(minimum two) or more Availability Zones**. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple AZ design of every AWS Region offers advantages for customers. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. Regions, including Regions in (**7 Regions**)North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East.

- An **Availability Zone (AZ)** is **one(minimum one) or more discrete data centers** with redundant power, networking, and connectivity in an AWS Region. **All traffic between AZs is encrypted.** AZs are physically separated by a meaningful distance, many kilometers, from any other AZ, although all are **within 100 km** (60 miles) of each other.

- **Amazon Transcribe - to add speech-to-text** capability to your applications. Amazon Transcribe uses a deep learning process called **automatic speech recognition** (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to **transcribe customer service calls**, to automate **closed captioning** and **subtitling**, and to generate metadata for media assets.

- The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations.
  You can remove an account from your organization only if the account has the information that is required for it to operate as a standalone account. For each account that you want to make standalone, you must accept the AWS Customer Agreement, choose a support plan, provide and verify the required contact information, and provide a current payment method.

  The **principals in the AWS account are no longer affected by any service control policies** (SCPs) that were defined in the organization. This means that restrictions imposed by those SCPs are gone, and the users and roles in the account might have more permissions than they had before.

- The **AWS Partner Network (APN)** is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

- **APN Consulting Partners** are **professional services firms** that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their migration to AWS cloud.
- **APN Technology Partner** – APN Technology Partners **provide hardware**, **connectivity services**, or **software solutions** that are either hosted on or integrated with, the AWS Cloud. **APN Technology Partners cannot help in migrating to AWS and managing applications on AWS Cloud.**

- **Concierge Support Team** (**billing and account experts**)– The Concierge Support Team are **AWS billing and account experts** that specialize in working with **enterprise accounts**. They will quickly and efficiently **assist you with your billing and account inquiries**. The Concierge Support Team is only available for the **Enterprise Support plan**. **Concierge Support Team cannot help in migrating to AWS and managing applications on AWS Cloud**.

- **Leverage AWS Professional Services and set up AWS Landing Zone to accelerate the infrastructure migration** :
  The **AWS Professional Services** organization is a **global team of experts** that can help you realize your desired business outcomes when using the AWS Cloud. AWS Professional Services **consultants can supplement your team** with specialized skills and experience that can help you achieve quick results.
  AWS Landing Zone is a solution that helps customers more **quickly set up** a secure, **multi-account** AWS environment and save time by automating the set-up of an environment for running secure and scalable workloads while implementing an initial security baseline through the creation of core accounts and resources.

- AWS Support cannot help with infrastructure migration.
- Trusted Advisor cannot automate the infrastructure migration.
- You may see use-cases asking you to select one of CloudWatch vs CloudTrail vs Config.
  Just remember this thumb rule –
  Think **resource performance monitoring**, **events**, and **alerts**; think CloudWatch.
  Think **account-specific activity** and **audit**; think CloudTrail.
  Think **resource-specific change history**, **audit**, and **compliance**; think Config.

- **Amazon DynamoDB** is a **key-value(NOSQL)** and **document** database that delivers **single-digit millisecond** performance at any scale. It's a fully managed, **multi-Region**, multi-master, durable database with built-in security, **backup and restore**, and **in-memory caching** for internet-scale applications.

- **Serverless Services on AWS (LADKAFASSESS)** -
    1. Lambda
    2. **API Gateway**
    3. DynamoDB
    4. S3
    5. **Kinesis**
    6. **Aurora**
    7. Fargate
    8. SNS
    9. SQS
    10. EFS
    11. RDS Proxy
    12. Step Functions
    13. **Athena**

- **Amazon Elasticsearch** – The term "Elasticsearch" is used to define a distributed, open source **search and analytics engine for all types of data**, including textual, numerical, geospatial, structured, and unstructured. Amazon Elasticsearch Service is a fully managed service that makes it easy to deploy, secure, and run Elasticsearch cost effectively at scale. It is a **search and analytics service** from Amazon.

- For the exam, there is no need to memorize these savings numbers. All you need to remember is that a **3 years term would always be more cost-effective than a 1-year term**. Then within a term, **"all upfront" is better than "partial upfront" which in turn is better than "no upfront"** from a cost savings perspective.

- **Fact** - AWS Shield Standard is activated for all AWS customers, by default. For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. With Shield Advanced, you also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. With the assistance of the **DRT (DDoS response team)**, AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: (**5**) Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

- **AWS Snowball** – AWS Snowball is a **data transport solution** that accelerates moving terabytes to petabytes of data into and out of AWS services using storage devices designed to be secure for **physical transport**.

- EFS file system can be mounted on instances across multiple Availability Zones. EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data. **EBS volume can be attached to a single instance in the same Availability Zone.**

- 5 Pillars of AWS well architected Framework:
    1. Operational Excellence
    2. **Security**
    3. Reliability
    4. **Performance** Efficiency
    5. **Cost Optimization**

- **Customer master keys (CMKs)** - Customer master keys are the primary resources in AWS KMS. A customer master key (CMK) is a **logical representation of a master key**. The CMK includes metadata, such as the **key ID**, **creation date**, **description**, and **key state**. The CMK also contains the key material used to encrypt and decrypt data. CMKs are created in **AWS KMS.**

  By default, **AWS KMS creates the key material for a CMK**. You **cannot extract, export, view, or manage** this key material. Also, you **cannot delete** this key material; you must delete the CMK. **However, you can import your own key material into a CMK or create the key material for a CMK** in the AWS CloudHSM cluster associated with an AWS KMS custom key store.

- AWS KMS supports three types of CMKs: customer managed CMKs, AWS managed CMKs, and AWS owned CMKs.

Type of CMK	Can we view CMK metadata	Can we manage CMK	Used only for my AWS account	**Automatic rotation**
Customer managed CMK	Yes	Yes	Yes	Optional. Every 365 days (1 year).
AWS managed CMK	Yes	No	Yes	Required. Every 1095 days (3 years).
AWS owned CMK	No	No	No	Varies

- **Customer managed CMKs** are CMKs in your AWS account that you create, own, and manage. You have **full control** over these CMKs, including establishing and maintaining their **key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases** that refer to the CMK, and **scheduling the CMKs for deletion**. Customer managed CMKs incur a monthly fee and a fee for use in excess of the free tier.

- **AWS managed CMKs** are CMKs in your account that are created, managed, and used **on your behalf by an AWS service** that is integrated with AWS KMS. Some AWS services support only AWS managed CMK. You can view the AWS managed CMKs in your account, view their key policies, and audit their use in AWS CloudTrail logs. However, you **cannot manage these CMKs, rotate them, or change their key policies**. And, you cannot use AWS managed CMKs in cryptographic operations directly; the service that creates them uses them on your behalf. You can also identify most AWS managed CMKs by their aliases, which have the format aws/service-name, such as aws/redshift. You do **not pay a monthly fee** for AWS managed CMKs. They can be subject to fees for use in excess of the free tier, but some AWS services cover these costs for you.

- **AWS owned CMKs** are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. Although **AWS owned CMKs are not in your AWS account**, an AWS service can use its AWS owned CMKs to protect the resources in your account. **You do not need to create or manage the AWS owned CMKs**. However, **you cannot view, use, track, or audit them**. **You are not charged a monthly fee or usage fee for AWS owned CMKs** and **they do not count against the AWS KMS quotas for your account.**

- The following AWS services support **reservations to optimize costs**:

i. **Amazon EC2 Reserved Instances** - You can use Amazon EC2 Reserved Instances to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances.

ii. **Amazon DynamoDB Reserved Capacity**- If you can predict your need for Amazon DynamoDB read-and-write throughput, Reserved Capacity offers significant savings over the normal price of DynamoDB provisioned throughput capacity.

iii. **Amazon ElastiCache Reserved Nodes** - Amazon ElastiCache Reserved Nodes give you the option to make a low, one-time payment for each cache node you want to reserve and, in turn, receive a significant discount on the hourly charge for that node.

iv. **Amazon RDS RIs** - Like Amazon EC2 RIs, Amazon RDS RIs can be purchased using No Upfront, Partial Upfront, or All Upfront terms. All Reserved Instance types are available for Aurora, MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines.

v. **Amazon Redshift Reserved Nodes** - **If you intend to keep an Amazon Redshift cluster running continuously for a prolonged period**, you should consider purchasing reserved-node offerings. These offerings provide significant savings over on-demand pricing, but they require you to reserve compute nodes and commit to paying for those nodes for either a **1- or 3-year duration**.

- Use **AWS Organizations** to manage **AWS accounts** of all units and then share the reserved EC2 instances amongst all units. AWS Organizations helps you to **centrally manage billing**; **control access**, **compliance**, and **security**; and **share resources across your AWS accounts**. Using AWS Organizations, you can **automate account creation**, **create groups of accounts to reflect your business needs**, and **apply policies for these groups for governance**. You can also simplify billing by **setting up a single payment method** for all of your AWS accounts. **AWS Organizations is available to all AWS customers at no additional charge**.

- **AWS Cost Explorer** (**forecast, filtering dimensions**, **adjust range, monthly/daily granularity**)lets you explore your **AWS costs and usage** at both a **high level** and at a **detailed level** of analysis, and empowering you to dive deeper using several **filtering dimensions** (e.g., **AWS Service**, **Region**, **Linked Account**). AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you **visualize the costs and usage associated with your top five cost-accruing AWS services**, and **gives you a detailed breakdown of all services in the table view.** The reports let you **adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends.**

- **AWS Cost and Usage Reports** – The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to **publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3)** bucket that you own. You can **receive reports that break down your costs by the hour or month**, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in a comma-separated value (**CSV**) format. **AWS Cost and Usage Reports cannot forecast your AWS account cost and usage.**

- **AWS CloudFormation** – AWS CloudFormation allows you to **use programming languages or a simple text file to model and provision**, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think **infrastructure as code**; think CloudFormation.

- **AWS Artifact** is your go-to, **central resource for compliance-related information that matters to your organization**. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact

include our **Service Organization Control (SOC) reports, Payment Card Industry (PCI)** reports, and certifications from accreditation bodies across geographies.
Different types of agreements are available in AWS Artifact Agreements to address the needs of customers subject to specific regulations. For example, the **Business Associate Addendum (BAA)** is available for customers that need to comply with the **Health Insurance Portability and Accountability Act (HIPAA)**. **It is not a service**, **it's a no-cost**, self-service portal for on-demand access to AWS' compliance reports.

- S3 is object storage and it **does not support file append operations.**

- There are two types of VPC endpoints**: interface endpoints** and **gateway endpoints**.
  An interface endpoint is an **elastic network interface** with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered **by AWS PrivateLink**, a **technology that enables you to privately access services by using private IP addresses**.
  A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. You may see a question around this concept in the exam. Just remember that **only S3 and DynamoDB support VPC Endpoint Gateway**. **All other services that support VPC Endpoints use a VPC Endpoint Interface**.

- **AWS Total Cost of Ownership (TCO) Calculator**
  TCO calculator helps to **compare the cost of your applications in an on-premises or traditional hosting environment to AWS**. AWS helps reduce Total Cost of Ownership (TCO) by reducing the need to invest in large capital expenditures and providing a pay-as-you-go model that empowers to invest in the capacity you need and use it only when the business requires it. Once you describe your on-premises or hosting environment configuration, it produces a **detailed cost comparison with AWS. TCO Calculator cannot provide the estimate of the monthly AWS bill based on the list of AWS services**.

- A **security group** acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the instance level, not at the subnet level. You **can specify allow rules, but not deny rules**. You can specify separate rules for inbound and outbound traffic.

- A **Network Access Control List (NACL)** is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at subnet level). A network ACL has separate inbound and outbound rules, and each rule **can either allow or deny traffic**.

- You can use a **network address translation (NAT)** gateway or a NAT Instance to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. **NAT Gateway is managed by AWS** but **NAT Instance is managed by you**.

- AWS Support plans provides **access to Infrastructure Event Management** for an **additional fee for Business Plan**.

- **Service Catalog** – AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

- **AWS Personal Health Dashboard** (**personalized view**) provides alerts and remediation guidance when AWS is experiencing events that may impact you. With Personal Health Dashboard, **alerts are triggered by changes in the health of your AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues**. It gives a **personalized view of the status of the AWS services** that are part of your Cloud architecture so that you can quickly assess the impact on your business when AWS service(s) are experiencing issues.

- **AWS Service Health Dashboard** – AWS Service Health Dashboard publishes most **up-to-the-minute information on the status and availability of all AWS services in tabular form for all Regions that AWS** is present in. You can check on this page (https://status.aws.amazon.com/) any time to get current status information or subscribe to an RSS feed to be notified of interruptions to each service.

Exam Alert:

While the **Service Health Dashboard** displays the **general status of AWS services**, **Personal Health Dashboard** gives you a **personalized view of the performance and availability of the AWS services** underlying your AWS resources.

- With **Amazon Rekognition**, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate **facial analysis** and **facial search** capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases. It can **Identify person in a photo, Detect text in a photo, Label objects in a photo**. You **cannot use Rekognition to resize photos to create thumbnails.**

- **AWS Fargate** is a **serverless compute engine for containers**. It works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate **removes the need to provision and manage servers**, lets you specify and pay for resources per application, and improves security through application isolation by design. Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no over-provisioning and paying for additional servers. Fargate runs each task or pod in its kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design.

- Think **account-specific activity** and **audit**; think **CloudTrail**. CloudTrail **cannot be used to monitor CPU utilization for EC2 instances or send emails**.

- **Amazon Athena** is an **interactive query service** that makes it easy to **analyze data in Amazon S3 using standard SQL**. Athena is **serverless**, so there is no infrastructure to manage, and you pay only for the queries that you run. Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

- **AWS CloudHSM** is a **cloud-based hardware security module** (HSM) that **enables you to easily generate and use your own encryption keys on the AWS Cloud**. With CloudHSM, you can **manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs**. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is standards-compliant and **enables you to export all of your keys to most other commercially-available HSMs**, subject to your configurations. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. **CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.**

- **Amazon API Gateway** is a fully managed service that makes it easy for **developers to create, publish, maintain, monitor, and secure APIs** at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out.

- **Lightsail** is an easy-to-use **virtual private server** (VPS) that offers you everything needed to build an application or website, plus a cost-effective, monthly plan.

- Since RDS is a managed service, So applying patches to underlying OS, underlying database, underlying hardware is sole responsibility of AWS. Though Database encryption is customer's responsibility.

  Q. **An IT company wants to run a log backup process every Monday at 2 AM. The usual runtime of the process is 5 minutes. As a Cloud Practitioner, which AWS services would you recommend to build a serverless solution for this use-case? (Select two)**

  ANS. To build the solution for the given use-case, you can create **a CloudWatch Events** rule that triggers on a schedule via a cron expression. You can then set the **Lambda** as the target for this rule.

- **IAM** and **Auto Scaling** is free of cost in aws.

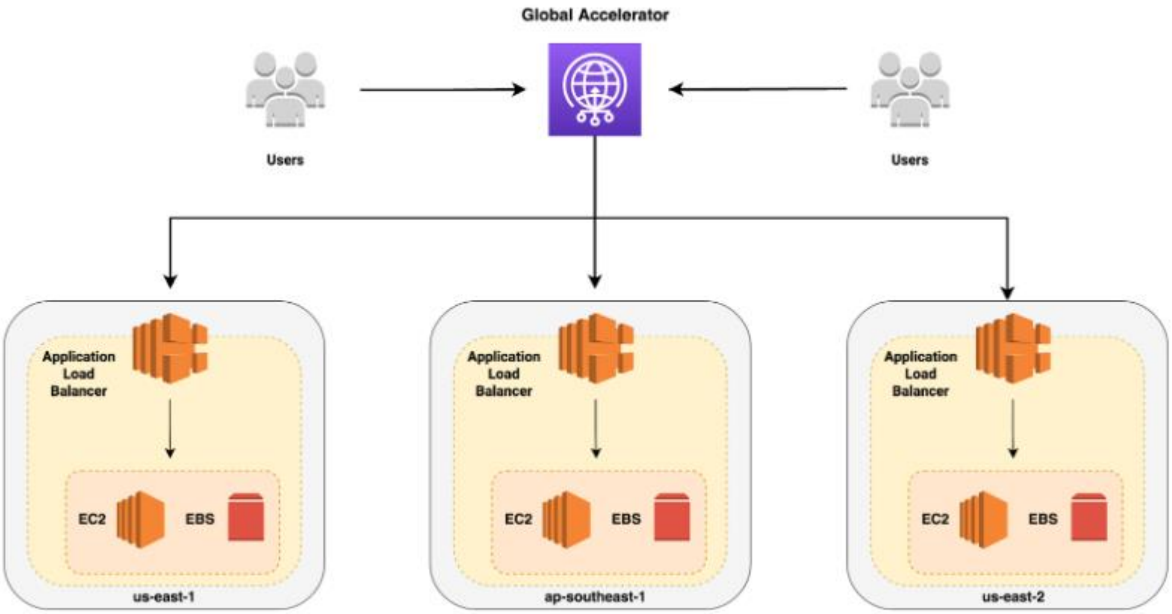
- Business and Enterprise plans support **programmatic access** to AWS support center.

- To access **EFS** file systems from **on-premises**, you must have an **AWS Direct Connect or AWS VPN connection** between your on-premises datacenter and your Amazon VPC.

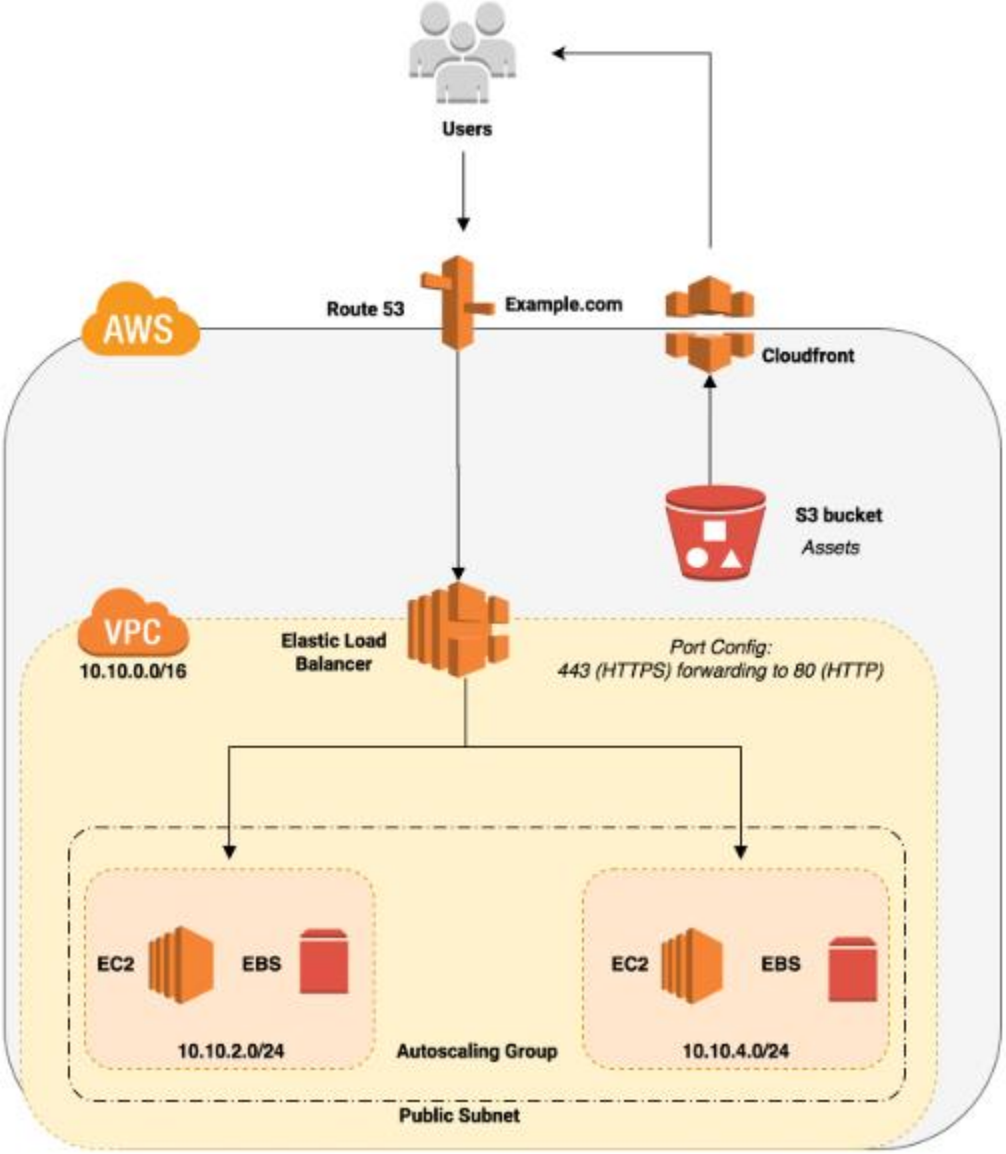
- Amazon **S3** can be accessed from **on-premises** only via **AWS Storage Gateway.**

- AWS service can help you analyze your infrastructure to identify unattached or underutilized EBS volumes – **AWS Trusted Advisor.**

- **AWS Global Accelerator** is a networking service that sends your user's traffic through Amazon Web Service's global network infrastructure, improving your internet user **performance by up to 60%.** When the **internet is congested**, Global Accelerator's automatic routing optimizations will help keep your packet loss, jitter, and latency consistently low. With Global Accelerator, you are **provided two global static customer facing IPs** to simplify traffic management. On the back end, add or remove your AWS application origins, such as Network Load Balancers, Application Load Balancers, Elastic IPs, and EC2 Instances, **without making user facing changes**. To mitigate endpoint failure, Global Accelerator automatically re-routes your traffic to your nearest healthy available endpoint.
  AWS Global Accelerator is a service that **uses edge locations** to look for the optimal pathway from your users to your applications. For example, you have a banking application that is scattered through **multiple AWS regions** and low latency is a must. Global Accelerator will route the user to the nearest edge location then route it to the nearest regional endpoint where your applications are hosted.



- **Amazon CloudFront** is a Content Delivery Network (CDN) like Cloudflare and Akamai. CloudFront is used to **deliver static assets** (such as videos, images, and files) securely to various devices around the globe with low latency.
  Let us say you have a streaming website with thousands of videos in your repository. It is inefficient to serve these videos uniquely whenever a user requests for it as this will lead to high bandwidth requirements and high CPU/Memory/disk utilization, which in turn results in frequent downtimes, endless video buffering, and irritated users who are trying to load their favorite shows. Speeding up the website is as simple as **offloading the videos, thumbnails, and any static assets from your server to Amazon S3**, and **using CloudFront to serve and cache these assets.**



- **Edge locations** serve requests for **CloudFront** and **Route 53**. CloudFront is a content delivery network, while Route 53 is a DNS service. Requests going to either one of these services will be routed to the nearest edge location automatically. This allows for low latency no matter where the end user is located. Edge Locations is a not a service, it is a APN.

Difference Between Global Accelerator and CloudFront –

- (**IPs**)CloudFront uses multiple sets of **dynamically** changing **IP addresses** while Global Accelerator will provide you a set of **static** IP addresses as a fixed entry point to your applications.
- (**PRICE**)CloudFront **pricing** is mainly based on data transfer out and HTTP requests while Global Accelerator charges a **fixed hourly fee** and an incremental charge over your standard Data Transfer rates, also called a Data Transfer-Premium fee (DT-Premium).
- CloudFront uses **Edge Locations to cache content** while Global Accelerator uses **Edge Locations to find an optimal pathway** to the nearest regional endpoint.
- (**PROTOCOL**)CloudFront is designed to handle **HTTP protocol** meanwhile Global Accelerator is best used for both **HTTP and non-HTTP protocols** such as **TCP** and **UDP**.

- The common denominator with these two(Cloud Front and Accelerator) services is that they use **Edge Locations.**

- **AWS Cloud9** is a **cloud-based integrated development environment (IDE)** that lets you write, run, and debug your code **with just a browser**. It includes a code editor, debugger, and terminal. Cloud9 comes prepackaged with essential tools for popular programming languages, including JavaScript, Python, PHP, and more, so you don’t need to install files or configure your development machine to start new projects.

- **AWS Amplify** if for developers for fastest and easiest way to build mobile and web apps that scale.

- **AWS AppSync** is used to accelerate application development with scalable **GraphQL APIs.**

- **The AWS Acceptable User Policy** provides **information regarding prohibited actions on the AWS infrastructure.**

- **S3 Data Consistency Model -**
  - **Read after Write consistency** for PUTS of new objects
    - If you read a file as soon as you upload it, you'll be able to read the file
  - **Eventual consistency for overwrite** PUTS and DELETES (can take some time to propogate)
    - If you update a file and overwrite the old version, you may get the old file or the new file. It will eventually show up.
    - You may be updating to one availability zone, may take time to propagate to other availability zones.

- **S3 Transfer Acceleration -**
  a. Users upload to an **edge location instead of directly to S3 bucket**
  b. Once it goes to an edge location, it automatically gets distributed to the S3 bucket
  c. File goes across Amazon's backbone to transfer much faster

- **S3 Cross Region Replication**
  a. Management > Replication
  b. Allows you to replicate bucket in one region to bucket in another region in the world
  c. Useful for disaster recovery
  d. Any object upload to first bucket is automatically replicated to second bucket

FACTS FROM PRACTICE SET 3 :

- There are four cost components to consider for S3 pricing –
  storage pricing; request and data retrieval pricing; data transfer and transfer acceleration pricing; and data management features pricing.
  Under "Data Transfer", **You pay for all bandwidth into and out of Amazon S3**, **except** for the following: (1) Data transferred in from the internet, (2) Data transferred out to an Amazon Elastic Compute Cloud (Amazon EC2) instance, when the instance is in the same AWS Region as the S3 bucket, (3) Data transferred out to Amazon CloudFront (CloudFront).

- CloudFormation is the AWS service which you use to provision the same AWS infrastructure across multiple AWS accounts and regions.

- AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during application deployment.

- **AWS Credentials Report** is service where you can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

- **Amazon EC2 Instance Connect** provides a simple and secure way to connect to your instances using Secure Shell (SSH). With EC2 Instance Connect, you use AWS Identity and Access Management (IAM) policies and principals to control SSH access to your instances, removing the need to share and manage SSH keys. All connection requests using EC2 Instance Connect are logged to AWS CloudTrail so that you can audit connection requests. EC2 Instance Connect can be used to connect to an EC2 instance from a Mac OS, Windows or Linux based computer.

- AZs are the collection of one or more data centers in **same location**.

- **CloudWatch Billing Alarms**: Sends an alarm when the actual cost exceeds a certain threshold.
  Budgets: Sends an alarm when the actual cost exceeds the budgeted amount or even when the cost forecast exceeds the budgeted amount.

- AWS WAF lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. It does not cover Amazon Route 53.

- WAF can **block all requests except the ones that you specify**. This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.

- S3 storage classes do not charge any data retrieval fee – Standard, Intelligent Tiering.

- S3 storage classes has NO constraint of a minimum storage duration charge for objects:

  S3 Standard

- S3 storage classes has constraint of a minimum storage duration charge for objects:

S3 Intelligent Tiering (30 days)

S3 One Zone IA (30 days)

S3 Glacier (90 days)

- A Reserved Instance is a reservation that provides a discounted hourly rate in exchange for an upfront fee and term contract. Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) use this approach to sell reserved capacity for hourly use of Reserved Instances. It is not a virtual machine. It is a commitment to pay in advance for specific Amazon EC2 or Amazon RDS instances.

- S3 stores data in a **flat non-hierarchical structure**. All objects are stored in S3 buckets and can be organized with shared names called prefixes. You can also append up to 10 key-value pairs called S3 object tags to each object, which can be created, updated, and deleted throughout an object's lifecycle.

- **U2F security key** – Universal 2nd Factor (U2F) Security Key is a device that you can plug into a USB port on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.

- **Amazon S3 Replication** where in we can copy objects between different AWS Regions or within the same Region. You can use replication to **make copies of your objects that retain all metadata, such as the original object creation time and version IDs**. Amazon S3 supports two types of replication: Cross Region Replication vs Same Region Replication.

- AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running **on-premises**.

- <u>Performance Efficiency</u> –include **selecting the right resource types and sizes based on workload requirements**, **monitoring performance**, and **making informed decisions** to maintain efficiency as business needs evolve.
  <u>The Operational Excellence</u>(IaaC) pillar includes **define your entire workload (applications, infrastructure) as code** and update it with code. You can **implement your operations procedures as code** and **automate their execution by triggering them in response to events**.

Cost Optimization – include understanding and controlling where the money is being spent, **selecting the most appropriate and right number of resource types**, analyzing spend over time, and scaling to meet business needs without overspending.

- Lambda does not support running container applications.

- IAM, Route53, CloudFront, WAF are global in scope.

- Customers use Amazon RDS databases primarily for online-transaction processing (**OLTP**) workload while Redshift is used primarily for reporting and analytics(**OLAP**).

- Data encryption is automatically enabled at rest for which of the following AWS services – S3 Glacier, Storage Gateway.

- If you have large quantities of data you need to migrate into AWS, offline data transfer with **AWS Snowball** can overcome the challenge of limited bandwidth, and avoid the need to lease additional bandwidth. Snowball moves terabytes of data in about a week. You can use it to move things like databases, backups, archives, healthcare records, analytics datasets, IoT sensor data and media content, especially when network conditions prevent realistic timelines for transferring large amounts of data both into and out of AWS.

- You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance. The AMI must be in the same region as that of the EC2 instance to be launched. If the AMI exists in a different region, you can copy that AMI to the region where you want to launch the EC2 instance.

- With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute. Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms.

- AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.

- AWS Personal Health Dashboard provides **alerts and remediation guidance when AWS is experiencing events that may impact you**. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources.

- AWS Shield Advanced is a paid service for all customers, irrespective of the Support plan.

- AWS services support High Availability by default – DynamoDB and EFS.
  DynamoDB is a fully managed, multi-Region, multi-master, durable database. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability.
  Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.

- Amazon Redshift only supports Single-AZ deployments. EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data.

- Amazon Rekognition does not do image processing tasks such as converting images to greyscale or resizing images. Human pose detection is not available in Amazon Rekognition.

- Lambda does not support running container applications.

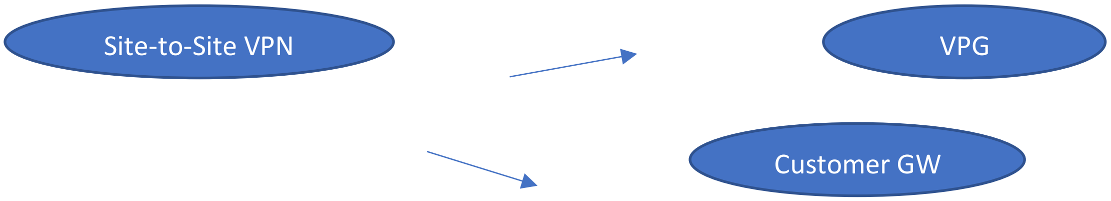
- Every AWS account provides its own invoice end of the month. You can get separate invoices for development and production environments by setting up separate AWS accounts for each environment.

- CloudWatch can be used to centralize the server logs for both EC2 instances and on-premises servers as well.

- AWS Config includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

- Components of an AWS Site-to-Site VPN – Virtual Private Gateway & Customer Gateway. A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. A customer gateway is a resource in AWS that provides at the customer end.

- AWS customers can carry out security assessments using penetration tests against their AWS infrastructure without prior approval for few common AWS services.



Facts from Practice Set4 :

- Read Replicas allow you to create read-only copies that are synchronized with your master database. Read Replicas are used for improved read performance. You can also place your read replica in a different AWS Region closer to your users for better performance. **Read Replicas are an example of horizontal scaling of resources**.

- (**While selecting multiple options for DDOS**)AWS Best Practices for DDoS Resiliency. These include services such as Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to control and absorb traffic, and deflect unwanted requests. These services integrate with AWS Shield, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

- The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud:
  1- **Stop** guessing your capacity needs
  2- **Test** systems at production scale: In the cloud, you can create a production-scale test environment on demand, complete your testing, and then decommission the resources.
  3- **Automate** to make architectural experimentation easier: Automation allows you to create and replicate your systems at low cost and avoid the expense of manual effort.
  4- **Allow** for evolutionary architectures
  5- **Drive** architectures using data This lets you make fact-based decisions on how to improve your workload.
  6- **Improve** through game days: Test how your architecture and processes perform by regularly scheduling game days to simulate events in production. This will help you understand where improvements can be made and can help develop organizational experience in dealing with events.

- AWS customers are welcome to carry out security assessments and penetration tests against their AWS infrastructure without prior approval for 8 services:

1- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.
2- Amazon RDS.
3- Amazon CloudFront.
4- Amazon Aurora.
5- Amazon API Gateways.
6- AWS Lambda and Lambda Edge functions.
7- Amazon Lightsail resources.
8- Amazon Elastic Beanstalk environments.

- AWS **consolidated billing** enables an organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have **volume pricing** tiers across certain usage dimensions that give the user lower prices when they use the service more. For example for 3 accounts, 1 master 2 other accounts, if you use 50 TB in each account you would normally be charged $23 *50*3 (because they are 3 different accounts), But with consolidated billing you would be charged $23*50+$22*50*2 (because they are treated as one account) which means that you would save $100.

- The Amazon Elastic MapReduce and DynamoDB are managed services that you **don't need to manage their underlying infrastructure**. Other managed services include: Amazon S3, Amazon RDS, Amazon Redshift, Amazon **WorkSpaces**, Amazon CloudFront, Amazon **CloudSearch** and several other services.

- For Enterprise-level customers, a **TAM** (Technical Account Manager) provides technical expertise for the full range of AWS services and obtains a detailed understanding of your use case and technology architecture. TAMs work with AWS Solution Architects to help you launch new projects and give best practices recommendations throughout the implementation life cycle. Your TAM is the **primary point of contact** for ongoing support needs, and you have a direct telephone line to your TAM.

- AWS Infrastructure Event Management(IEM) is a structured program available to Enterprise Support customers (and Business Support customers for an additional fee) that helps you plan for large-scale events such as product or application launches, infrastructure migrations, and marketing events. With Infrastructure Event Management, you get strategic planning assistance before your event, as well as real-time support during these moments that matter most for your business. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS.

- ADVANTAGES OF CLOUD COMPUTING OVER TRADITIONAL HOSTING

  High-availability (eliminating SPOFs**: single points of failure)
  **Distributed infrastructure
  **On-demand infrastructure for scaling applications or tasks
  **Cost savings

- You can use the **AWS Organizations APIs** to automate the creation and management of new AWS accounts. The Organizations APIs enable you to create new accounts programmatically, and to add the new accounts to a group. The policies attached to the group are automatically applied to the new accounts. For example, you can automate the creation of sandbox accounts for developers and grant entities in those accounts access only to the necessary AWS services.

- VMware Cloud on AWS is an integrated cloud offering jointly developed by AWS and VMware delivering a highly scalable service that allows organizations to seamlessly migrate and extend their on-premises VMware vSphere-based environments to AWS.

- Using Amazon RDS falls under the shared responsibility model, following are customer responsibilities - **Managing the database settings** & **Building the relational database schema.**

- Creating **RDS Read Replicas** across regions improves your disaster recovery capabilities and allows you to scale out globally. The **RDS Multi-AZ feature** always spans two Availability Zones within a single Region.

- **AWS Security scales with your AWS Cloud usage.** No matter the size of your business, the AWS infrastructure is designed to keep your data safe. **AWS Security doesn't start automatically**, you have to go on and set up how your data will be accessed and decide whether this data will be encrypted or not and so on.

- The number of servers, the server type, the number of processors is required to calculate the Total Cost of Ownership for the AWS Cloud.

- Amazon EMR helps you analyze and process vast amounts of data by distributing the computational work across a cluster of virtual servers running in the AWS Cloud. The cluster is managed using an open-source framework called Hadoop.

- Amazon Inspector allows you to create assessment templates to automate security vulnerability assessments throughout your development and deployment pipelines or for static production systems.

- EC2 instance pricing varies depending on many variables:
  – The buying option (On-demand, Reserved, Spot, Dedicated)
  – Selected AMI
  – Selected instance type(t2,t3)
  – Region
  – Data Transfer in/out
  – Storage capacity.

- When you begin to estimate the cost of using Amazon EC2, consider the following:
  **Clock hours of server time
  **Instance type
  **Pricing model
  **Number of instances
  **Load balancing
  **Detailed monitoring
  **Elastic IP addresses
  **Operating systems and software packages

- Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly-scalable hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.

- Understanding your service limits (and how close you are to them) is an important part of managing your AWS deployments – continuous monitoring allows you to request limit increases or shut down resources before the limit is reached. One of the easiest ways to do this is via **AWS Trusted Advisor’s Service Limit Dashboard**, which currently covers 39 limits across 10 services. Most service limit increases can be requested through the **AWS Support Center** by choosing Create Case and then choosing Service Limit Increase.

- DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon **EBS**) volumes for database and log storage.

- Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. Server-Side Encryption is an option of protecting data at rest in Amazon S3. Server-Side Encryption involves requesting Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

- As an S3 user, there is virtually no limit on the amount of data you can store in S3.

- When creating a **tagging strategy** for AWS resources, make sure that it accurately represents organizationally relevant dimensions and adheres to the following tagging best practices:
  1- Always use a standardized, **case-sensitive** format for tags, and implement it consistently across all resource types.
  2- Consider tag dimensions that support the ability to manage resource access control, cost tracking, automation, and organization.
  3- Implement **automated tools** to help manage resource tags.
  4- Err on the side of using too many tags rather than too few tags.
  5- Remember that **it is easy to modify tags** to accommodate changing business requirements, however consider the ramifications of future changes, especially in relation to tag-based access control, automation, or upstream billing reports.

- Amazon **SWF(Simple Workflow**) helps developers build, run, and scale background jobs that have parallel or sequential steps. You can think of Amazon SWF as a fully-managed **state tracker** and **task coordinator** in the Cloud. If your app's steps take more than 500 milliseconds to complete, you need to track the state of processing, and you need to recover or retry if a task fails, Amazon SWF can help you.

- AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS. AWS CodeStar provides a **unified user interface**, enabling you to easily manage your software development activities in one place. With AWS CodeStar, you can set up your entire **continuous delivery toolchain** in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your whole team to work together securely, allowing you to easily manage access and add owners, contributors, and viewers to your projects. Each AWS CodeStar project comes with a **project management dashboard**, including an integrated **issue tracking capability powered by Atlassian JIRA Software**. With the AWS CodeStar project dashboard, you can easily track progress across your entire software development process, from your backlog of work items to teams' recent code deployments.

- CodeGuru helps to find your most expensive lines of code and improve code quality.

- AWS Lightsail is an **inexpensive, easy-to-use, novice friendly** and interactive platform to configure and launch web applications quickly.

- Why does it takes between 24 to 48 hours for changes made to a hosted zone in Amazon Route 53 to reflect globally?

  Because, **DNS Resolvers** around the world can only reflect the changes in their cache after the TTL has expired, it is 24 hours by default.

- VPC Peering between 2 VPCs in different regions and under separate AWS Accounts can share traffic between each other. VPC Peering can be used to replicate data to geographically distinct locations for fault-tolerance, disaster recovery and redundancy.

- RDS doesn't support AutoScaling like EC2 instances, but **it does support manual horizontal scaling (by adding read replicas)** and manual vertical scaling (by upgrading/downgrading an existing instance). RDS doesn't scales automatically.

- There are five design principles for performance efficiency in the cloud:
  1- **Democratize advanced technologies**: Rather than having your IT team learns how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.
  2- **Go global in minutes**: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.
  3- **Use serverless architectures**: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.
  4- **Experiment more often**: With virtual and automatable resources, you can quickly

carry out comparative testing using different types of instances, storage, or configurations.
5- **Mechanical sympathy**: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.

- ** AWS has a Built-in firewall that can be used to control traffic to your network.
  ** You can secure your network by encrypting your data in transit with TLS across all services.

- The AWS SDK can simplify using AWS services in your applications with an API tailored to your programming language or platform. Programming languages supported include Java, .NET, Node.js, PHP, Python, Ruby, Go, and C++.
  AWS CLI allows you to control multiple AWS services from the command line and automate them through scripts NOT from programming languages.

- The amount of security configuration work you have to do varies depending on which services you select and how sensitive your data is. However, there are certain security features—such as **individual user accounts and credentials**, **SSL/TLS for data transmissions**, and **user activity logging**—that you should configure no matter which AWS service you use.

- Just upload your code and Lambda takes care of everything required to run and scale your code with high availability.

- You can back up data stored in Amazon S3 manually NOT automatically. Amazon S3 supports data replication and versioning instead of automatic backups.

- AWS recommends that you delete your root access keys because you can’t restrict permissions for the root user credentials. If you want to manage services that require administrative access create an IAM user, grant administrator access to that user, then use those credentials to interact with AWS.

- The Application Programming Interface (API) allows developers to easily work with various AWS services programmatically. There is no difference in performance when you provision resources using the console or using the AWS API. In fact, if you access AWS through the AWS Management Console or through the command line tools, you are actually using tools that make calls to the AWS API.

- When a storage device has reached the end of its useful life, AWS procedures include a **decommissioning process** that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

- You can use ACM or IAM to store and deploy server certificates.

- AWS Professional Services created the AWS Cloud Adoption Framework (AWS CAF) to help organizations design and travel an accelerated path to successful cloud adoption.

- AWS Service Catalog allows organizations to create and manage catalogs of IT services that are **approved for use on AWS**. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to **centrally manage commonly deployed IT services**, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

- Global Tables builds upon DynamoDB's global footprint to provide you with a fully managed, multi-region, and multi-master database that provides fast, local, read and write performance for massively scaled, global applications. **Global Tables replicates your Amazon DynamoDB tables automatically across your choice of AWS regions.** Multi-master replication ensures that updates performed in any region are propagated to other regions, and that data in all regions are eventually consistent.

- You have bought 4 Amazon EC2 reserved instances for a 1 year term. After 7 months you decide to sell 2 of your instances on the Amazon EC2 Reserved Instance Marketplace. Which of the following is true regarding this scenario? When selling a reserved instance on the Amazon EC2 Reserved Instance Marketplace, you only have the option to set an upfront price for the instance. The usage price and other configuration (e.g., instance type, Availability Zone, platform) will remain the same as when the Reserved Instance was initially purchased. Each Reserved Instance sold on the Amazon EC2 Reserved Instance Marketplace will be charged a service fee of 12% on the total upfront price NOT monthly.

- Whether you are deploying a new environment for testing, or increasing capacity of an existing system to cope with extra load, you will not want to manually set up new resources with their configuration and code. It is important that you make this an automated and repeatable process that avoids long lead times and is not prone to human error. The following approaches can be used to achieve this:

  **__Bootstrapping__: When you launch an AWS resource like an Amazon EC2 instance or Amazon Relational Database (Amazon RDS)DB instance, you start with a default configuration. You can then execute automated bootstrapping actions. That is, scripts that install software or copy data to bring that resource to a particular state. You can __parameterize configuration__ details that vary between different environments (e.g.,production, test, etc.) so that the same scripts can be reused without modifications.

  **__Golden Images__: Certain AWS resource types like Amazon EC2instances, Amazon RDS DB instances, Amazon Elastic Block Store (Amazon EBS) volumes, etc., can be launched from a golden image: a snapshot of a particular state of that resource. When compared to the bootstrapping approach, a golden image results in faster start times and removes dependencies to configuration services or third-party repositories. This is important in auto-scaled environments where you want to be able to quickly and reliably launch additional resources as a response to demand changes.

- If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:

  **__Change__ your AWS root account password and the passwords of any IAM users.

  **__Delete or rotate__ all root and AWS Identity and Access Management (IAM) access keys.

  **__Delete__ any resources on your account you didn’t create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.

  **__Respond__ to any notifications you received from AWS Support through the AWS Support Center.

- Placement Groups are logical groupings or clusters of instances within a single Availability Zone.

- Benefits of AWS X-Ray include:

  1- **Review request behavior**:

  AWS X-Ray traces user requests as they travel through your entire application. It aggregates the data generated by the individual services and resources that make up your application, providing you an end-to-end view of how your application is

performing.
2- **Discover application issues**:
With AWS X-Ray, you can glean insights into how your application is performing and discover root causes. With X-Ray's tracing features, you can follow request paths to pinpoint where in your application and what is causing performance issues.

- With Cloud Directory, you can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries. While traditional directory solutions limit you to a single hierarchy, Cloud Directory offers you the flexibility to create directories with hierarchies that span multiple dimensions. For example, you can create an organizational chart that can be navigated through separate hierarchies for reporting structure, location, and cost center. Amazon Cloud Directory automatically scales to hundreds of millions of objects and provides an extensible schema that can be shared with multiple applications.

- Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
  Uploading encrypted files to Amazon S3 is called "Client-Side Encryption".

- Proximity to your end users, compliance, data residency constraints, and cost are factors you have to consider when choosing the most suitable AWS region.

- AWS publishes security bulletins about the latest security and privacy events with AWS services on the **Security Bulletins** page.

- The AWS **Serverless Application Repository** is a managed repository for serverless applications. It enables teams, organizations, and individual developers to store and share reusable applications, and easily assemble and deploy serverless architectures in powerful new ways. Using the Serverless Application Repository, you don't need to clone, build, package, or publish source code to AWS before deploying it. Instead, you can use pre-built applications from the Serverless Application Repository in your serverless architectures, helping you and your teams reduce duplicated work. Integration with AWS Identity and Access Management (IAM) provides resource-level control of each application, enabling you to publicly share applications with everyone or privately share them with specific AWS accounts.

- With Storage Gateway you can backup and archiving, disaster recovery, cloud data processing, storage tiring, and migration.

- Amazon CloudFront charges are based on the data transfer out of AWS and requests used to deliver content to your customers. There are no upfront payments or fixed platform fees, no long-term commitments, no premiums for dynamic content, and no requirements for professional services to get started. **There is no charge for data transferred from AWS services such as Amazon S3 or Elastic Load Balancing.**

  When you begin to estimate the cost of Amazon CloudFront, consider the following:
  – **Traffic distribution**: Data transfer and request pricing varies across geographic regions, and pricing is based on the **edge location** through which your content is served.
  – **Requests**: The number and type of requests (HTTP or HTTPS) made and the geographic region in which the requests are made.
  – **Data transfer out**: The amount of data transferred out of your Amazon CloudFront edge locations.

- The AWS Cloud includes many design patterns and architectural options that you can apply to a wide variety of use cases. Some key design principles of the AWS Cloud include scalability, disposable resources, automation, loose coupling, managed services instead of servers, and flexible data storage options.

- Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon data centers). You can protect data in transit by using SSL or by using client-side encryption.
  Also, You have the following options of protecting data at rest in Amazon S3.
  1- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
  2- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

- The factors that have the greatest impact on cost include: Compute, Storage and Data Transfer Out. Their pricing differs according to the service you use.

- **Tags are key-value pairs** that allow you to organize your AWS resources into groups.
  You can use tags to:
  1- Visualize information about tagged resources in one place, in conjunction with Resource Groups.
  2- View billing information using Cost Explorer and the AWS Cost and Usage report.

3- Send notifications about spending limits using AWS Budgets.

It is recommended to use logical groupings of your resources that make sense for your infrastructure or business. You could organize your resources by: Project, Cost center, Development environment, Application or Department. For example, if you tag resources with an application name, you can track the total cost of a single application that runs on those resources.

- Each S3 storage class is rated on its availability and durability.

- The Benefits of AWS Security include :
  1- Keep Your Data Safe: The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.
  2- Meet Compliance Requirements: AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
  3- Save Money: Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility.
  4- Scale Quickly: Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

- Amazon EMR is not serverless. Amazon EMR uses Amazon EC2 to process to process data at any scale. **1)**EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

- Database backup is an important operation to consider for any database system. Taking backups not only allows the possibility to restore upon database failure but also enables recovery from data corruption. Amazon S3 provides highly durable and reliable storage for database backups while reducing costs. Data stored in Amazon S3 can be retrieved immediately when needed.

- For S3 storage and data transfer OUT from EC2, AWS follows a tiered pricing model. Tiered pricing means that you pay less per unit when you use more. For example the more GBs you use in S3, the more you save.

- You can reduce the load on your source DB Instance by routing read queries from your applications to one or more read replicas. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

- AWS Lambda natively supports Java, Go, PowerShell, Node.js, C#, Python, and Ruby code, and provides a Runtime API which allows you to use any additional programming languages to author your functions.

- When a new IAM user is created, that user has NO access to any AWS service. This is called a non-explicit deny. For that user, access must be explicitly allowed via IAM permission and access policies.

- AWS Certificate Manager can be used to secure network communications and establish the identity of websites over the Internet.

- **AWS continues to lower the cost of cloud computing for its customers,** making everything from web apps to big data on AWS even more cost-effective and widening the TCO (Total Cost of Ownership) gap with traditional infrastructure.

- Route 53 offers health checks to monitor the health and performance of your application as well as your web servers and other resources. Route 53 can be configured to route traffic only to the healthy endpoints to achieve greater levels of fault tolerance in your applications.
  Note: You can also monitor the health of your web servers using the Elastic Load Balancing health checks.

- WorkMail gives users the ability to seamlessly access their email, contacts, and calendars using the client application of their choice, including Microsoft Outlook, native iOS and Android email applications, any client application supporting the IMAP protocol, or directly through a web browser.

- Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit.

- **The more time passes using AWS, the less you pay for its services**”. This corrected statement now describes “**Economies of scale**”.

- If you work with multiple resources in multiple stages, you might find it useful to manage all the resources in each stage as a group rather than move from one AWS service to another for each task. **Resource Groups** help you do just that. By default, the AWS Management Console is organized by AWS service. But with the Resource Groups tool, you can create a **custom console** that organizes and consolidates information based on your project and the resources that you use.

- Chat access to AWS Support Engineers is available at the Business and Enterprise level plans only.

- Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers performance improvements from **milliseconds to microseconds** – even at millions of requests per second. DAX adds **in-memory acceleration** to your DynamoDB tables without requiring you to manage cache invalidation, data population, or cluster management.

- S3 pricing is based on four factors:
  1- The storage class you have chosen.
  2- The total amount of data (in GB) you've stored.
  3- Data Transfer Out.
  4- Number of Requests.

- The policy is a JSON document that consists of:
  >> **Actions**: what actions you will allow. Each AWS service has its own set of actions.
  >> **Resources**: which resources you allow the action on.
  >> **Effect**: what will be the effect when the user requests access—either allow or deny.
  >> **Conditions** – which conditions must be present for the policy to take effect. For example, you might allow access only to the specific S3 buckets if the user is connecting from a specific IP range or has used multi-factor authentication at login.

- In the US regions, Snowball appliances come in two sizes: 50 TB and 80 TB. All other regions have 80 TB Snowballs only.
  In either case, it is better (cost-effective) to use 3 or 4 snowball devices to transfer 200 TB.
  3 snowballs * 80TB = 240 TB
  4 snowballs * 50 TB = 200 TB

- You can transfer up to 100 Petabytes (100,000 Terabytes) per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck.