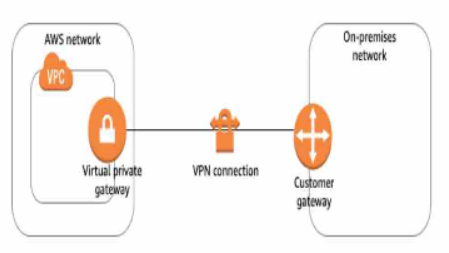
* **Fargate** is a serverless tool, good for running application on Docker containers with ECS or EKS but you do not have access to the underlying servers.   
  (ECS = Elastic Container Service; EKS = Elastic Kubernetes Service)
* **ECS** is a fully managed container service with access to the underlying servers. ECS is a scalable container management service that makes it easy to run, stop, and manage Docker containers on a cluster.
* **Trusted Advisor** help to provision resources following AWS best practices in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits and check if the EC2 instances are underutilized (under 10% of the CPU utilization). All customers have access to the 7 Core checks of Trusted Advisor that help increase the security and performance of the AWS environment: S3 Bucket permission, Security Groups for ports unrestricted, IAM use, MFA on root account, EBS public snapshots. RDS public snapshot and service limits.
* **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. Per the definitions above, Elastic Beanstalk falls under the Platform as a Service type (**PaaS**). At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time. There is **no additional charge** for Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.
* **CostExplorer** lets you visualize, understand, and manage your AWS costs and usage over time. Helps you identify cost-saving opportunities by downsizing or terminating EC2 instances. You can see all underutilized EC2 instances across member accounts in a single view.
* **CloudWatch** provides data and insights to monitor your application, respond to performance changes and optimize resource utilization. Think resource, performance monitoring, events and alerts, think CloudWatch. CloudWatch cannot be used to identify under-utilized EC2 instances. CloudWatch is a good service for building resilient (elastic, flexible, resistant) systems.
* **Personal Health Dashboard** provides alerts and remediation guidance when AWS is experiencing events that may impact you.
* Amazon **GuardDuty** is a threat detection service that monitors malicious activity to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (user and API activity in your account), VPC Flow Logs (network traffic data), and DNS Logs (name query pattern). All security findings are retained for 90 days. After 90 days you can enable CloudWatch events to automatically push findings in an S3 bucket in your account or another data store for long term retention.
* **Enterprise support plan**: Concierge-like service where the main focus is helping the customer achieve their outcomes and find success in the cloud, **24x7** technical support from high-quality engineers, (TAM) to coordinate access to proactive programs and AWS subject matter experts, 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases. When Business Critical System is Down you have a response from within 15 min. It allows unlimited contacts to open unlimited cases.
* **Business support plan** is recommended if you have production workloads on AWS and want 24x7 phone, email, and chat access to technical support and architectural guidance. You get full access to AWS Trusted Advisor Best Practice Checks. It allows unlimited contacts to open unlimited cases.
* **Developer Support plan** is recommended if you are testing or doing early development and want the ability to get email-based technical support during business hours. Can open an unlimited amount of cases for one preliminary contact. This plan also supports general guidance on how services can be used for various use cases, workloads, or applications. You get access to the 7 core Trusted Advisor checks. You have also the AWS Personal Health dashboard: a personal view of AWS services with alerts when your resources are impacted. It includes the help API for integration with your systems.
* **Basic support plan**: 24x7 access to customer service, documentation, whitepapers, and support forums. AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices. AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.
* **EC2 instance store** provides temporary block-level storage for your EC2 instance. Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data or data replicated between a fleet of instances, and other temporary content.
* **Amazon EFS** provides a simple, scalable, fully managed, elastic NFS file system. It is built to scale on-demand to petabytes, it provides massively parallel shared access to thousands of Amazon EC2 instances but not for caching info on EC2 instances. EFS is a regional service for storing data within and across multiple AZs for high availability and data durability. Amazon EC2 instance can access your EFS file system across multiple AZs, regions and VPCs while on-premise servers can access that EFS file system using AWS Direct Connect or AWS VPN.
* **AmazonS3** is an object storage service not for caching info associated to EC2 instances. S3 can store for customers websites, mobile applications, backup and restore, archive, applications, IoT devices data, and big data analytics. You specify a global name space for your bucket but the bucket is regional. So **S3** is a regional service.
* **AWS Region** consists of **multiple**, isolated, and physically **separate AZ's** within a **geographic area**. **Each group of logical data centers** is called an **Availability Zone (AZ).**
* **Amazon VPC** is a logically isolated section of the AWS Cloud that you define where you can launch AWS resources. Selection of your IP address range, creation of subnets, and configuration of route tables and network gateways. A VPC spans all of the Availability Zones in the Region.
* A **subnet** is a range of IP addresses within your VPC. A **subnet** spans **only one** Availability Zone in the Region.
* Amazon **CloudWatch billing metric data** is stored in which AWS Region? **Us-east-1** *and it represents the worldwide charges.*
* **Route 53** is scalable cloud Domain Name System (**DNS**) web service.
* Failover routing policy is used when you want to configure active-passive failover. Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. This is called an active-passive configuration. You can use Route 53 Geolocation routing policy to block certain geographies. When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict the distribution of content to only the locations in which you have distribution rights.
* Geolocation routing policy is to route traffic based on the location of the user.
* Geoproximity routing policy is to route traffic based on the location of the resources.
* **Reserved Instances** provide you with significant savings on your Amazon EC2 costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for **a one-year or three-year** commitment, with the three-year commitment offering a bigger discount. You will be charged for the entire duration, irrespective of your usage, so this option is not correct for running weekly workloads.
* **Saving plans** are for **EC2 and Fargate** usage in exchange of a **1** year **or 3 years** commitment contract.
* **Dedicated hosts** can be purchased on demand **hourly**.
* **On-Demand Instances** is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you **pay only for the seconds** that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand **instances cannot be interrupted**.
* **RedShift** is a fully managed ***data warehouse*** for analyzing all your data using standard SQL and your existing BI tools.
* **RDS** is used primarily for On Line Transaction Processing (***OLTP***) while Redshift is used for analyzing and reporting. RDS is not an in-memory database.
* **DynamoDB** is a ***NoSQL database*** that supports key-value and document data models, petabytes of data and tens of millions of read and write requests per second. It is a fully managed, **multi-region**, multi-master, durable database with backup and restore, in memory caching for internet scale applications. All data is stored on SSD, **replicated on multi-AZs** in an AWS Region and provide **high availability** and data durability. With the key value model, DynamoDB has a flexible schema, so each row can have any number of columns at anypoint of time.
* **ElastiCache** is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing. it boosts the performance of your existing databases by retrieving data from high throughput and low latency ***in-memory data stores***.
* **Virtual MFA device** is a software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. Each virtual MFA device assigned to a user must be unique.
* **Hardware MFA device** is the hardware device corresponding to the Virtual MFA device.
* **U2F** security key - A device that you plug into a USB port on your computer to do a MFA access.
* **Read Replica** enhances primarily the database scalability. It is an example of horizontal scaling of resources.
* **Multi-AZ deployments**: Main purpose is ***high availability***. Always spans 2 AZ within a single region.
* **Multi-Region deployment**: Main purpose is ***disaster recovery*** *and* ***local performance***. Each region can have multi-AZ deployment.
* **Read Replicas**: Main purpose is ***scalability***. Can be within an AZ, cross-AZ or cross-Regions.
* **Cloud computing** is the *on-demand* *delivery of IT resources* over the Internet with *pay-as-you-go pricing*.
* **Agility** refers to the ability of the cloud to give you an easy access to a broad range of technologies so that you can innovate faster.
* **Elasticity**: means that you **provision** the number of **resources** that you **actually need**. You can **scale** these resources **up or down instantly**.
* **Cost savings**: you *trade capital expenses* (such as data centers and physical servers) *for variable expenses* (resources you pay for what you consume). And you can have lower expenses due to the ***economies of scale***.
* **Deploy globally in minutes**: you can expand to new geographic regions and deploy globally in minutes in a few clicks and you can put those applications in a closer proximity to end users to reduce latency and improves their experience.
* **Site-to-Site VPN** enables you to securely ***connect your on-premises network to your Amazon VPC***. This connection goes over the internet. ***Virtual Private Gateway (or a Transit Gateway***) and ***Customer Gateway*** are the components of a VPN Connection. You must configure routing to pass traffic through the VPN connection.
* **Storage Gateway** is a hybrid cloud storage service that connects your on-premises environments with AWS Cloud.
* A **NAT** **Gateway** (Network Address Translation) or NAT Instance can be used in a private subnet in your VPC to enable instances in the private subnet to initiate outbound traffic to the Internet. NAT Gateway is managed by AWS but NAT Instance is managed by you.
* **Internet gateway** is VPC component that allows communication between VPC instances and the internet.
* **Well-Architected Framework** is based on five pillars: — ***Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization***.
* **Performance efficiency pillar** focuses on using IT and computing resources efficiently. Key topics are: select the right resource types and sizes based on workload need, monitor your architecture performance.
* **Reliability pillar focuses** on the ability to ***prevent, and quickly recover from failures*** to meet business and customer demand. Key topics are: cross projects requirements, recovery planning and how we handle changes.
* **Operational Excellence pillar** includes the *ability to run and monitor systems to deliver business value and to continually improve supporting processes* and procedures. For that your entire workload (applications and infrastructure) *is defend as code (application as code and infrastructure as code)* and you update it with code. Operations procedure are defined as code and automated through a trigger in response to an event.
* **Security pillar** focuses on ***protecting information & systems***. Key topics are: integrity of data and confidentiality, identify and manage who can do what, establishing controls to detect security events.
* **Cost Optimization pillar** focuses on avoiding un-needed costs. Key topics are: control where the money is spent., select the right number of resources type, scaling to meet business needs without overspending.
* **CloudFormation** allows you to program a simple ***text file*** (example: in a JSON format) for the provisioning of all resources needed for your applications across all regions and accounts. Think ***infrastructure as code***; think CloudFormation. (This is very different from Beanstalk where you just upload your application code and Beanstalk automatically figures out what resources are required to deploy that application. In CloudFormation, you have to explicitly specify which resources you want to provision.)

CloudFormation cannot help with the moving of data and applications into another Region.

* **CodePipeline** is a continuous delivery service that enables you to automate the steps required to release your software. It integrates AWS ***CodeCommit***, Amazon ***S3***, AWS ***CodeBuild***, AWS ***CodeDeploy***, AWS ***Elastic Beanstalk***, AWS ***CloudFormation***, AWS ***OpsWorks***, Amazon ***ECS***, and AWS ***Lambda***.
* **Amazon S3** bucket for a static website: When you configure a bucket as a static website, you must enable website hosting, set permissions, and create and add an index document. And of course, you must disable the block public access for that bucket or the account level block public access.
* Use **CloudFront** and its edge location to ***improve the performance*** of your website.
* **S3 Transfer Acceleration** enables fast and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.
* S**ecurity Group** acts as a virtual firewall for your instance to control inbound and outbound traffic. A Security Group evaluates all rules before deciding whether to allow traffic and act *at instance level*. A Security Group is **stateful**, that is, it automatically allows the return traffic.
* A **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**: it works at **subnet** level. A NACL contains a numbered list of rules and evaluates the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the NACL. By default, a NACL allows all traffic. If you put a custom NACL, it is to deny some traffic. A NACL is **stateless** which means all traffic inbound or out bound must evaluate the rules to pass.
* **AWS Config** includes how the resources are related to one another and the ***configurations and relationships historic change over time***. It can deliver historic changes as a snapshot file to your S3 bucket for analysis.
* **Amazon Macie** is a fully managed ***data security and data privacy service*** that uses machine learning (**ML**) and pattern matching to discover and protect your sensitive data in AWS.
* **CloudTrail** is a service that enables ***auditing, and risk auditing*** of your AWS account. CloudTrail provides an event ***history*** of your AWS ***account activity (events, API calls,…)***. (Config is focused on the configuration of your AWS resources whereas CloudTrail focuses on the events or API calls, that drive those changes). Think Account activity and audit, think CloudTrail,
* **Snowball** is a *data transport solution* that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport. AWS snowball is a data migration and edge computing device.
* **Database Migration Service** helps you ***migrate databases*** from on-premises to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. Homogeneous (Oracle to Oracle) and heterogeneous (Mysql to Aurora) database migration can be done using Database Migration Service (Step 1: schema migration, step 2: database migration).
* **Direct Connect** creates a ***private connection*** from your ***on-premise network (a remote network) to your VPC*** which does not use the public internet. It takes **one month** to establish that connection.
* **Transit Gateway** *connects VPCs and on-premises* networks through a **central hub**. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. As you expand globally, inter-Region peering connects AWS Transit Gateways using the AWS global network. Your data is automatically encrypted and never travels over the public internet.
* **Lambda** lets you ***run code without provisioning*** or managing servers. (***serverless***) You pay only for the compute time you consume. With Lambda, you can run code for any application or backend service. You can use Amazon S3 to trigger AWS Lambda to process data immediately after an upload. Lambda is a ***regional service***. 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. The lambda has a maximum execution time of 15 minutes. A solution to run a log backup process every day at 2 AM is 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.
* **EC2 instance** provides ***compute capacity*** in the AWS cloud with support for ***per second billing***. You can use EC2 to provision virtual servers on AWS Cloud and access the underlying OS. Maintaining the server and its software has to be done by the customer.
* **Amazon ECS** is a scalable, container management service that makes it easy to run, stop, and manage Docker containers on a cluster of EC2 instances.
* **SQS** is a fully managed ***message queuing service*** that enables you to decouple and scale microservices, distributed systems, and serverless applications.
* **AMI** provides the information required to launch an instance. You must specify an AMI when you launch an instance. The AMI must be in the same region as that of the EC2 instance to be launched. The region of AMI has no bearing on the performance of the EC2 instance.
* **Cost Allocation Tag** is a ***label*** that you or AWS ***assigns to an*** AWS ***resource***. Each tag consists of a key and a value. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. AWS provides two types of cost allocation tags, an AWS generated tags and user-defined tags. AWS defines, creates, and applies the AWS generated tags for you, and you define, create, and apply user-defined tags. You **must** activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report. But tags are not mandatory.
* **Cost Explorer** has an interface that lets you manage your AWS ***costs and usage over time***. At the top of the Cost Explorer page are the Month-to-date costs and Forecasted month end costs. The Forecasted month end costs show how much Cost Explorer estimates that you will owe at the end of the month and compares your estimates costs to your actual costs of the previous month. So, you can forecast your cost and usage in the future so that you can plan ahead. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top 5 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.
* **Simple Monthly Calculator** provides an ***estimate the monthly cost*** for a AWS service based on certain information you provide: the expected usage of the service. It helps customers estimate their monthly bill efficiently.
* **TCO calculator** helps to compare the cost of your applications in an **on-premises** environment **to AWS**. Once you describe your on-premises environment configuration, TCO calculator produces a detailed cost comparison with AWS.
* **AWS Billing and Cost Management** is the service that you use to pay your AWS bill and analyze and control your costs. It is the billing department for AWS services.
* **AWS shared responsibility model**: AWS is responsible for protecting the infrastructure that runs all of the services offered in the Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Cloud security and compliance are the responsibilities of AWS. **AWS is responsible of the security OF the cloud**.
* **Customer shared responsibility model**: Customer's responsibility is determined by the AWS Cloud services that a customer selects. For abstracted services, as S3 and DynamoDB, AWS operates the infrastructure layer, the OS and platforms and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to set the appropriate permissions. For example: the customer is responsible for maintaining the versions of a Lambda function. **Security IN the Cloud** is the responsibility of the customer. With Amazon EC2 which is categorized as IaaS, the customer is responsible for Guest OS update ad patching, application software installed, configuring security group (configuring firewall) and AWS is responsible for the infrastructure layer only.
* **EBS** is a ***block storage service*** designed for use with Amazon EC2. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems and media workflows are widely deployed on EBS.
* **EC2 Instance store** provides ***temporary block-level storage*** for your EC2 instance. This storage is located on disks. Ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance is terminated. EC2 instance store cannot be used for file sharing between instances.
* **SaaS** provides you with a complete product that is run and managed by the service provider. You don’t have to think about how the service is maintained or how the underlying infrastructure is managed. You only need to think how you will use that particular software. Examples: ***Rekognition****,* ***Gmail***. ***DropBox*** or ***Zoom*** are examples of SaaS services.
* **IaaS** (Infrastructure as a Service) contains the basic building blocks for cloud IT. It typically ***provides access to networking features, computers (virtual or on dedicated hardware), and data storage space***. IaaS gives the *highest level of flexibility and management control over IT resources*. ***EC2*** is an example of an IaaS service on AWS, ***GCP, RackSpace, Limode***.
* **PaaS** (Platform as a Service) removes the need to manage underlying infrastructure (usually hardware and OS), and allows you to ***focus on the deployment and management of your applications***. You don’t need to worry about resource provisioning, capacity planning, software maintenance, patching, or any other heavy lifting involved in running your application. ***Beanstalk*** on AWS, ***Google App Engine*** are examples of a PaaS service.
* **FaaS** (Function as a Service) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage application functionalities without the building and maintaining of the infrastructure associated with developing and launching an app. ***Lambda*** is an example of a FaaS service.
* You will **pay a fee** each time you **read** from or **write data** stored on the **EFS - Infrequent Access storage class** - Data stored on the Infrequent Access storage class costs less than Standard and because you access to those files less frequently. So, you will pay a fee each time you read from or write to a file.
* Amazon **EBS Snapshots** are a point in time copy of your block data. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. But EBS Snapshots are stored incrementally, which means you are ***billed only for the changed blocks*** stored.
* When using **EBS direct APIs** for Snapshots, additional EC2 data transfer charges will apply only when you use external data transfer or cross-region data transfers.
* **AWS Backup** is a fully managed service to back up your Amazon EFS file data. With AWS Backup, you ***pay only for the amount of backup storage*** you use and the ***amount of backup data you restore*** in the month.
* **EBS** - Snapshot storage is based on the amount of space your data consumes in Amazon S3. Because Amazon EBS does not save empty blocks, it is likely that the snapshot size will be considerably less than your volume size. ***Copying EBS snapshots is charged for the data transferred across regions***. After the snapshot is copied, ***standard EBS snapshot charges apply for storage in the destination region***.
* Amazon **Athena** is an interactive query service that makes it easy to analyze data in Amazon S3 using standard **SQL**. Athena is ***serverless*** and you ***pay only for the queries that you run***. Athena cannot be used for in-memory database.
* **AWS Budgets** enable you to ***plan your service usage, service costs and instance reservations***. AWS Budgets information is updated up to three times a day. Budgets track your costs, subscriptions, refunds and RIs. There are four different budget types you can create under AWS Budgets - ***Cost budget*** (how much you want to spent on a service), ***Usage budget*** (how much you want to use on one or more services), ***Reservation budget*** (track the usage of Reserved Instances) and ***Savings Plans budget***.

AWS Budgets gives 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. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others.

* **Recognition**: you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Recognition is a *regional service* and a SaaS model of service.
* **Global Scope services**: Most of the services that AWS offers are Region specific. But few services, by definition, need to be in a global scope because of the underlying service they offer: AWS **IAM**, Amazon **CloudFront**, **Route 53** and **WAF** are some of the global services.
* **Regional Scope services**: ***Lambda*** is a regional service. ***Recognition*** is a regional service and Amazon ***S3*** is also a regional service.
* **IAM** enables you to ***manage access to AWS services and resources***. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is a global scope service.
* **CloudFront** is a fast content delivery network (***CDN***) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront is a global service.
* **WAF** allows you to configure web access control lists (***Web ACLs***) on your CloudFront distributions or Application Load Balancers to filter and block requests based on request signatures. WAF is a global service.

WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that ***allow, block, or monitor (count) web requests*** based on conditions that you define. These conditions include ***IP addresses, HTTP headers, HTTP body, URI strings, SQL injection, and cross-site scripting***. You can use the IP address-based match rule to block specific geographies.

* **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. AWS Shield cannot be used to block users from certain geographies.
* **AWS Shield Advanced** offers cost protection against spikes in your AWS bill that could result from a DDoS attack. This cost protection is provided for your *Elastic Load Balancing load balancers, Amazon CloudFront distributions, Amazon Route 53 hosted zones, Amazon Elastic Compute Cloud instances, and your AWS Global Accelerator accelerators*. AWS Shield Advanced is a ***paid service*** for all customers.
* **Elastic Load Balancing (ELB)** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a ***single AZ or across multiple AZ’s*** *(Availability Zones)*.
* **ECR** (Elastic Container Registry) can be used to store, manage, and deploy ***Docker container images***. Amazon ECR eliminates the need to operate your container repositories. You can then pull your docker images from ECR and ***run*** those ***on*** Amazon ***Elastic Container Service (ECS).***
* **Global Accelerator** is a service that *improves the availability and performance* of your applications with local or global users. It provides ***static IP addresses*** that act as a fixed entry point to your application ***endpoints*** ***in a single or multiple AWS Regions***, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances. AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, up to ***60% improving the performance*** of your traffic.

Global Accelerator improves performance for a wide range of applications over ***TCP or UDP by proxying*** packets ***at the edge*** to applications running in one or more AWS Regions. Global Accelerator is a ***good fit for non-HTTP use cases***, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or *deterministic, fast regional failover*.

* **CloudFront *and* Global Accelerator** use the global network and its edge locations distributed all around the world. **CloudFront** improve the performance for *cacheable content* (such as images and videos) and *dynamic content* (dynamic site delivery). **Global Accelerator** *improves performance* for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. ***Both services integrate with AWS Shield for DDoS protection***.
* **Spot Instance** is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at ***up to 90% of discounts***, you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for ***data analysis, batch jobs, background processing, and other tasks that can be interrupted within a short notice***. So, spot instance are not suitable for critical workloads that need to run at a specific point in time.
* **On-Demand Instance** is an instance that you use on-demand. You have full control over its lifecycle — you decide when to launch, stop, hibernate, start, reboot, or terminate it. There is no long-term commitment required when you purchase On-Demand Instances. There is no upfront payment and you **pay only for the seconds** that your On-Demand Instances are running. The price per second for running an On-Demand Instance is fixed. On-demand instances **cannot be interrupted**.
* **Reserved Instances** provide you with significant **savings (up to 75%)** costs compared to On-Demand Instance pricing. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account. You can purchase a Reserved Instance for a **one-year or three-year** commitment, with the three-year commitment offering a bigger discount. Reserved instances **cannot be interrupted**.
* **EC2 Dedicated Hosts** allow you to use your eligible **software licenses** from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your licenses, but with the simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use. Dedicated host are not cost-efficient comparted to the On-Demand price.
* **VPC peering** connection is a networking **connection between two VPCs** that enables you to route traffic between them privately. VPC peering is not transitive, a separate VPC peering connection has to be made between two VPCs that need to talk to each other. With growing VPCs, this gets difficult to manage.
* **Enable MFA** for all users in your account is a recommendation from AWS.
* **Rotate credential regularly** is recommended by AWS. You must change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. You can apply a password policy to your account to require all your IAM users must rotate their passwords.
* **IAM best practices**: Lock away your Root user access keys, create individual IAM users, use groups to assign permission to IAM users, grant least privilege, configure a strong password policy for your users, enable MFA, use roles for applications that run on EC2 instances, user roles to delegate permissions, do not share access keys, rotate credentials regularly, remove unnecessary credentials, monitor activity in your AWS account. You must know that you cannot reduce the permissions associated with your root user. So never share these root user access keys with any other users, even the administrators.
* **VPC endpoint Gateway** enables you to privately ***connect*** your ***VPC*** *to* supported AWS ***services*** powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. There are **two types of VPC endpoints**: **interface endpoints** and **gateway endpoints**. For 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**.
* **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.
* **Every AWS account provides its own invoice** at the end of the month. You can get separate invoices for development and production environments by setting up separate AWS accounts for each environment.
* **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 and apply policies for these groups. You can 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.
* You cannot create separate invoices based on tags.
* **Amazon EC2** is categorized as Infrastructure as a Service (**IaaS**) and, as such, requires the customer to perform all the necessary security configuration and management tasks. Customers are responsible for the management of the guest operating system (including updates and security patches), of any application software or utilities installed by the customer on the instances and the configuration of the AWS-provided firewall (called a security group) on each instance.
* **Configuration management is a shared responsibility**. AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
* **Awareness & Training** is also a shared responsibility. AWS trains AWS employees, but a customer must train their own employees.
* **S3 Versioning** is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. If you overwrite an object, it becomes a new object version in the bucket and you can restore always the previous version.
* **S3 lifecycle configuration** - To manage your S3 objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. With S3 Lifecycle configuration rules, you can tell Amazon S3 to ***transition objects to less expensive storage classes, or archive or delete them***. Lifecycle configuration will do the hard lifting of moving your data into cost-effective storage classes without user intervention.
* **S3 Storage Classes** - Amazon S3 offers a range of storage classes designed for different use cases. These include **S3 Standard** for general-purpose storage of **frequently accessed data**; **S3 Intelligent-Tiering** for data with unknown or changing access patterns; **S3 Standard-Infrequent Access** (S3 Standard-**IA**) and **S3 One Zone-Infrequent Access** (S3 One **Zone-IA**) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (**S3 Glacier**) and Amazon S3 Glacier Deep Archive (**S3 Glacier Deep Archive**) for long-term archive and digital preservation.
* **S3 One Zone-IA** is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and offers the lowest availability.
* **S3 Standard** offers high durability, availability, and performance object storage for frequently accessed data.
* **S3 Intelligent-Tiering** storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.
* **S3 Glacier** is a secure, durable, and extremely low-cost S3 cloud storage for data archiving and long-term backup.
* **CRR**: **Amazon S3** is an object storage service that offers scalability, data availability, security, and performance. ***Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets***. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region.
* Although Amazon **S3** stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. **Cross-Region Replication (CRR)** allows you to replicate data between distant AWS Regions to satisfy these requirements. CRR can be used for compliance requirements, to minimize latency or increase operational efficiency (For example : 2 compute clusters in 2 different regions want to analyse the same set of objects).
* **SRR** is used to copy objects across Amazon S3 buckets in the same AWS Region. SRR can be used for aggregate logs into a single bucket, configure live replication of data between production and test accounts or abide data sovereignty laws (duplicate data in separate accents within a same region).
* **S3 Glacier encryption** always done is a storage service optimized for infrequently used data, or "cold data”. Data at rest stored in S3 Glacier is automatically server-side encrypted with keys maintained by AWS.
* **Storage Gateway** **encryption** always done - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data ***transferred between the gateway and AWS storage is encrypted*** using SSL (Secure Socket Layer) for all ***three types of gateways*** - **File**, **Volume** and **Tape** Gateways.
* **EBS volume encryption** not done by default: not encrypted by default. You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create.
* **Redshift encryption** not done by default - Encryption is an optional setting in Amazon Redshift. When you enable encryption for a cluster, the data-blocks and system metadata are encrypted for the cluster and its snapshots.
* Amazon **EFS drives** encryption not done by default - Encryption is not a default setting, but an optional configuration for EFS drives. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest.
* **CloudWatch** **Logs** can be used to monitor, store, and access your log files from Amazon *EC2 instances*, *AWS CloudTrail*, *Route 53*, and other sources such as *on-premises servers* and you can archive them for future analysis.
* **Penetration testing**: AWS ***customers can carry out security assessments or penetration tests*** ***against their AWS infrastructure*** ***without prior approval*** for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.
* **Network Stress Testing** - AWS considers "network stress test" to be when a test sends a large volume of test traffic to a specific target application. The endpoint and infrastructure are expected to be able to handle this traffic.
* **Amazon Inspector** is an ***automated, security assessment service*** that helps you check for unintended network accessibility and for vulnerabilities on those EC2 instances to improve the security and compliance of applications deployed in AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. ***Think deviation from*** ***security best practices, think Amazon inspector***.
* **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.
* **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 across your AWS resources. 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. System Manager cannot be used to run a process on a schedule.
* **AWS Cost and Usage Reports** **(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 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 comma-separated value (CSV) format.
* **Hybrid Cloud**: The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to the internal system.
* **Public Cloud**: A public cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing.
* **Private Cloud**: All is private or on-premise. Unlike a Public cloud, a Private cloud enables businesses to avail IT services that are provisioned and customized according to their precise needs. The business can further avail the IT services in a secure and reliable way over a private IT infrastructure.
* **On Premise**: This is not a cloud deployment model. When an enterprise opts for on-premises, it needs to create, upgrade, and scale the on-premise IT infrastructure by investing in sophisticated hardware, compatible software, and robust services. Also, the business needs to deploy dedicated IT staff to upkeep, scale, and manage the on-premise infrastructure continuously.
* To **improve** the **availability** of a fleet of EC2 instances, **Deploy** the **EC2 instances across different Availability Zones** in the same AWS Region.
* **Amazon Macie** is used with Amazon S3. 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).***
* 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. Amazon Rekognition does not do image processing tasks such as converting images to greyscale or resizing images.
* The company needs to create resources in the new AWS Region and then move the relevant data and applications into the new AWS Region. There is no off-the-shelf solution or service that the company can use to facilitate this transition.
* **S3 Glacier Deep Archive** is Amazon S3’s *lowest-cost 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**.
* **Auto Scaling group scales out** and adds a greater number of EC2 instances to match an increase in demand
* **Auto Scaling group scales in** and reduces the number of EC2 instances to match a decrease in demand
* AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain the performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas.
* You can use **scaling policies** to increase or decrease the number of instances in your group dynamically to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group, between the minimum and maximum capacity values that you specify, and launches or terminates the instances as needed. You can also scale on a schedule.
* **MQ is a managed message broker** service for Apache ActiveMQ and RabbitMQ that makes it easy to set up and operate message brokers on AWS. Amazon MQ reduces your operational responsibilities by managing the provisioning, setup, and maintenance of message brokers for you. Because Amazon MQ connects to your current applications with APIs and protocols, you can easily migrate to AWS without having to rewrite code.
* If you're using messaging with existing applications, and want to move the messaging functionality to the cloud quickly and easily, AWS recommends you consider Amazon MQ. It supports APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications. If you are ***building brand new applications in the cloud, AWS recommends you consider Amazon SQS and Amazon SNS***.
* Amazon **SNS** is a fully managed messaging service for both ***application-to-application (A2A) and application-to-person (A2P) communication***. The A2A pub/sub functionality provides topics for **push-based**, many-to-many messaging between distributed systems, microservices, **and event-driven** serverless applications. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push”
* **Amazon Kinesis** data stream enables you to build applications that ***process or analyze streaming data*** for specialized needs. You can continuously add various types of data such as clickstreams, application logs and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.
* **CloudHSM** is a ***cloud-based hardware security module (HSM)*** that enables you to easily generate and use your encryption keys on the AWS Cloud. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.
* **Step Function** lets you ***coordinate multiple AWS services into serverless workflows***. You can design and run workflows that stitch together (coudre ensemble) services such as AWS ***Lambda*** *(serverless functions)*, AWS ***Glue*** (ETL service) and Amazon ***SageMaker*** (ML=machine learning service).
* AWS **Management Console** is a simple web interface for accessing AWS services.
* **CLI** can access AWS services from the command line and automate service management with scripts.
* **SDK** can also **access via APIs** the AWS services.