**[The 5 Pillars of the AWS Well-Architected Framework:](https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/)**

The AWS Well-Architected Framework describes the **key concepts, design principles, and architectural best practices** for designing and running workloads in the cloud.

**1- Operational Excellence**: The operational excellence pillar includes the **ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures**. **Key topics include** automating changes, responding to events, and defining standards to manage daily operations.

**2- Security:** The security pillar includes **the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies**. **Key topics include** confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

**3- Reliability:** The reliability pillar includes **the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as  misconfigurations or transient network issues.** **Key topics include** distributed system design, recovery planning, and how to handle change.

**4- Performance Efficiency:** The performance efficiency pillar includes the **ability to use computing resources efficiently to meet system requirements. Key topics 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.

**5- Cost Optimization:** The cost optimization pillar includes **the ability to avoid or eliminate unneeded cost or sub-optimal resources.**

**The performance efficiency pillar** includes **the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.**

**There are five design principles for PERFORMANCE EFFICIENCY in the cloud:**

– Democratize advanced technologies.

– Go global in minutes.

– Use serverless architectures.

– Experiment more often.

– Mechanical sympathy.

**The reliability pillar** includes **the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.**

**There are five design principles for RELIABILITY in the cloud:**

– Test recovery procedures.

– Automatically recover from failure.

– Scale horizontally to increase aggregate system availability.

– Stop guessing capacity.

– Manage change in automation.

**The cost optimization pillar** includes **the ability to avoid or eliminate unneeded cost or suboptimal resource.**

**There are five design principles for COST OPTIMIZATION in the cloud:**

– Adopt a consumption model.

– Measure overall efficiency.

– Stop spending money on data center operations.

– Analyze and attribute expenditure.

– Use managed services to reduce cost of ownership.

**The SECURITY pillar** includes the **ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.**

**There are six design principles for SECURITY in the cloud:**

– Implement a strong identity foundation

– Enable traceability.

– Apply security at all layers.

– Automate security best practices.

– Protect data in transit and at rest.

– Prepare for security events.

- Keep people away from data

**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**
3. **Automate to make architectural experimentation easier.**
4. **Allow for evolutionary architectures.**
5. **Drive architectures using data**
6. **Improve through game days.**

**1- Stop guessing your capacity needs:** Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you might end up sitting on expensive idle resources or dealing with the performance implications of limited capacity. With cloud computing, these problems can go away. You can use as much or as little capacity as you need, and scale up and down automatically.

**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. Because you only pay for the test environment when it's running, you can simulate your live environment for a fraction of the cost of testing on premises.

**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. You can track changes to your automation, audit the impact, and revert to previous parameters when necessary.

**4- Allow for evolutionary architectures:** Allow for evolutionary architectures. In a traditional environment, architectural decisions are often implemented as static, one-time events, with a few major versions of a system during its lifetime. As a business and its context continue to change, these initial decisions might hinder the system's ability to deliver changing business requirements. In the cloud, the capability to automate and test on demand lowers the risk of impact from design changes. This allows systems to evolve over time so that businesses can take advantage of innovations as a standard practice.

**5- Drive architectures using data:** In the cloud you can collect data on how your architectural choices affect the behavior of your workload. This lets you make fact-based decisions on how to improve your workload. Your cloud infrastructure is code, so you can use that data to inform your architecture choices and improvements over time.

**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.

**​ What are some key DESIGN PRINCIPLES for designing public cloud systems?**

 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.**

You can use the **consolidated billing** feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a *master (payer) account* that pays the charges of all the *member (linked) accounts*.

**Consolidated billing has the following benefits:**

• **One bill** – You get one bill for multiple accounts.

• **Easy tracking** – You can track the charges across multiple accounts and download the combined cost and usage data.

• **Combined usage** – You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

• **No extra fee** – Consolidated billing is offered at no additional cost.

**When using AWS Organizations with consolidated billing, best practices include:**

– Always **enable multi-factor authentication (MFA)** on the root account.

– Always use a **strong and complex password** on the root account.

– **The Paying account should be used for billing purposes only**. Do not deploy resources into the Paying account.

There is a **default limit of 20 linked accounts** but this can be extended and there is no reason why you should stick to a maximum of 20 accounts.

**AWS Direct Connect** is a network service that provides an **alternative to using the Internet to connect customers’ on premise sites to AWS.**

Data is transmitted through a **private network connection between AWS and a customer’s data center or corporate network.** Direct Connect is high bandwidth, and low latency.

**Benefits of AWS Direct Connect:**

– **Reduce cost** when using large volumes of traffic.

– **Increase reliability** (predictable performance).

– **Increase bandwidth** (predictable bandwidth).

– **Decrease latency**.

Using AWS Direct Connect, customers can establish private connectivity between AWS and their datacenter, office, or co-location environment, **which in many cases can reduce their network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.**

**IAM** is used to **securely control individual and group access to AWS resources**. **Groups** are collections of users and have policies attached to them. You can **use IAM to attach a policy to a group**. **AWS Identity and Access Management (IAM) is used for managing users, groups, and roles in AWS.**

When you create IAM policies, follow **the standard security advice of granting least privilege**—that is, **granting only the permissions required to perform a task**. Determine what users need to do and then craft policies for them that let the users perform only those tasks.

You can **manage AWS Identity and Access Management identities through** the **AWS Management Console, AWS Command Line Tools, AWS SDKs, and IAM HTTPS API.**

**To ensure the security of personal AWS account, best practices for managing ACCESS KEYS:**

– Don’t generate an access key for the root account user.

– Use Temporary Security Credentials (IAM Roles) Instead of Long-Term Access Keys.

– Manage IAM User Access Keys Properly.

**Access keys** are a **combination of an access key ID and a secret access key**. They are used to make **programmatic calls to AWS** using the API. They are associated with an **IAM user.**

**Access keys** are **long-term credentials** that can **be used to sign programmatic requests to AWS.**

**Security tokens** are **temporary credentials** that can also be **used to interact with AWS resources programmatically.**

**Console passwords** are used for signing users into the **AWS Management Console.**

**Server certificates** can be **used to authenticate to some AWS services using HTTPS.**

**Key pairs** are used **for authenticating to Amazon EC2 instances.**

With **Amazon Glacier** you **pay for**

* **storage on a per GB / month basis,**
* **retrieval requests and quantity (based on expedited, standard, or bulk),**
* **data transfer out of Glacier.**

**Amazon S3 Glacier** provides **three retrieval options** to fit your use case.

* **Expedited retrievals** typically return data in **1-5 minutes**, and are best used for **Active Archive use cases.**
* **Standard retrievals** typically complete between **3-5 hours work**, and **work well for less time-sensitive needs like backup data, media editing, or long-term analytics.**
* **Bulk retrievals** are the **lowest-cost retrieval option**, returning large amounts of data within **5-12 hours**.

**AWS Config** is a fully-managed service that provides you with an AWS **resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance**. It can be used to **manage configuration versions.**

**AWS Config** is a service that enables you to **assess, audit, and evaluate the configurations of your AWS resources.** Config continuously monitors and records your AWS resource configurations and allows you to **automate the evaluation of recorded configurations against desired configurations.**

**AWS Service Catalog** is used to create and manage **catalogs of IT services that you have approved for use on AWS**, including **virtual machine images, servers, software, and databases** to complete multi-tier application architectures.

**AWS Artifact** is **used for obtaining on-demand security and compliance reports and select online agreements.** This service provides access to **AWS security and compliance reports** such as **SOC and PCI**.

It is a central resource for **compliance-related information**. This service can be used to **get compliance information related to AWS’ certifications/attestations.**

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

**Reports available in AWS Artifact include:**

* **Service Organization Control (SOC) reports,**
* **Payment Card Industry (PCI) reports,**
* **Certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls**.

**Agreements available in AWS Artifact include:**

* **Business Associate Addendum (BAA)**
* **Nondisclosure Agreement (NDA).**

**Amazon Inspector** is an **automated security assessment service** that helps improve the **security and compliance of applications deployed on AWS.**

Amazon Inspector **automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.**

**Amazon Dynamo DB** is a fully managed **NoSQL database service** that provides fast and predictable performance with seamless scalability. **Push button scaling** means that you can scale the DB at any time without incurring downtime.

**Rekognition Image** is a **deep learning powered image recognition service** that detects objects, scenes, and faces; extracts text; recognizes celebrities; and identifies inappropriate content in images. It also allows you to search and compare faces.

**AWS Key Management Service** gives you **centralized control over the encryption keys used to protect your data.**

**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.

**AWS CloudHSM** is a **cloud-based hardware security module (HSM) that allows you to easily add secure key storage and high-performance crypto operations to your AWS applications**. It uses a highly secure hardware storage device to store encryption keys.

**AWS Snowmobile** can move **100PB per snowmobile**. AWS call this an **“Exabyte-scale data transfer service”.**

**AWS Snowball** you can **move up to 80TB per device**. AWS call this a “**petabyte-scale data transfer service”**. It is the best way for an organization **to transfer hundreds of terabytes of data** from their on-premise data center into Amazon S3 **with limited bandwidth available**. Using Snowball addresses common challenges with large-scale data transfers including **high network costs, long transfer times, and security concerns.**

**S3 Transfer Acceleration** is meant **speed up uploads to Amazon S3**. Amazon S3 Transfer Acceleration enables fast, easy, 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.** However, for these volumes of data Snowball is a better choice.

**S3 Cross-Region Replication** is used for **copying data between regions**. It is also unsuitable for moving such as huge amount of data.

**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 like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other**. Amazon Route 53 is **fully compliant with IPv6 as well.**

**Amazon Route 53** features include:

* domain registration,
* DNS,
* traffic flow,
* health checking,
* failover.

Amazon Route 53 helps AWS Customers **improve their application’s performance for a global audience**. Amazon Route 53 latency-based policy **routes user requests to the closest AWS Region, which reduces latency and improves application performance.**

**Auto Scaling** is a service for **distributing incoming connections** **between a fleet of registered EC2 instances.** Amazon EC2 Auto Scaling provides **elasticity** for your applications by automatically launching or terminating EC2 instances according to application load or schedules you define.  This helps with **resiliency and high availability** as it can also be set to ensure a minimum number of instances are always available.

Amazon EC2 Auto Scaling scales **horizontally by adding launching and terminating EC2 instances** based on actual demand for your application.

**AWS Lambda** lets you run **code as functions without provisioning or managing servers**. Lambda-based applications (also referred to as serverless applications) are **composed of functions triggered by events.** With serverless computing, your application still runs on servers, but all the server management is done by AWS.

**Amazon Elastic Container Service (ECS)** is a highly scalable, high performance **container management service** that supports **Docker containers** and allows you to **easily run applications on a managed cluster of Amazon EC2 instances.**

**AWS CodeDeploy** is a fully managed **deployment service that automates software deployments** to a variety of compute services such as **Amazon EC2, AWS Lambda, and your on-premises servers.**

**AWS CodeDeploy** is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises, and is not used for managing encryption keys.

**Amazon Cognito** lets you **add user sign-up, sign-in, and access control** to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and **supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.**

**Amazon Cognito** is **used for authentication using mobile apps**. This service is used for providing sign-in and sign-up services for mobile applications.

**AWS CloudFormation** provides a **common language for you to model and provision AWS and third party application resources in your cloud environment.** 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.** AWS CloudFormation **automates and simplifies the task of creating groups of related resources that power your applications.**

**AWS CloudFormation** is a service that gives developers and businesses **an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion**. AWS CloudFormation provides **a common language for you to describe and provision all the infrastructure resources in your cloud environment**. Think of CloudFormation as **deploying infrastructure as code**.

**The benefits of using AWS CloudFormation include:**

**1- CloudFormation allows you to model your entire infrastructure in a text file.** This template becomes the single source of truth for your infrastructure. This helps you to standardize infrastructure components used across your organization, enabling configuration compliance and faster troubleshooting.

**2- AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts.** CloudFormation takes care of determining the right operations to perform when managing your stack, and rolls back changes automatically if errors are detected.

**3- Codifying your infrastructure allows you to treat your infrastructure as just code.** You can author it with any code editor, check it into a version control system, and review the files with team members before deploying into production.

**4- CloudFormation allows you to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.**

**AWS OpsWorks** is **a configuration management service** that provides managed instances of **Chef and Puppet**. Chef and Puppet are automation platforms that **allow you to use code to automate the configurations of your servers**. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your [Amazon EC2](https://aws.amazon.com/ec2/) instances or on-premises compute environments. This service is involved with automation and configuration management.

**AWS Batch** enables developers, scientists, and engineers to **easily and efficiently run hundreds of thousands of batch computing jobs on AWS.** AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory-optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. With AWS Batch, there is no need to install and manage batch computing software or server clusters that you use to run your jobs, **allowing you to focus on analyzing results and solving problems**. **AWS Batch plans, schedules, and executes your batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances.**

**Amazon QuickSight** is a fast, cloud-powered **business intelligence service** that makes it easy **to deliver insights to everyone in your organization.**

**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 across your AWS resources.**

**Amazon Neptune** is a fast, reliable, fully-managed **graph database service** that makes it easy to build and run applications that work with highly connected datasets. With Amazon Neptune, you can create **sophisticated, interactive graph applications** that can **query billions of relationships in milliseconds**.

**Amazon Redshift** is a fast, scalable **data warehouse** that makes it simple and cost-effective to **analyze all your data across your data warehouse and data lake**. **Amazon Redshift** is a fully managed data **warehouse service** that allows you **to run complex analytic queries against petabytes of structured data using standard SQL and your existing Business Intelligence (BI) tools.**

Amazon Redshift is a fast, fully managed data warehouse service that is **specifically designed for online analytic processing (OLAP) and business intelligence (BI) applications, which require complex queries against large datasets.**

**Amazon Redshift** is a fully managed, **petabyte-scale data warehouse service** in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. **This enables you to use your data to acquire new insights for your business and customers.**

**AWS X-Ray** helps developers **analyze and debug production, distributed applications**, such as those built using a **microservices architecture**. With X-Ray, you can understand how your application and its underlying services are **performing to identify and troubleshoot the root cause of performance issues and errors.**

**AWS X-Ray** is a **service that collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization.**

**AWS X-Ray** is used to **analyze the behavior of your application by providing request tracing, exception collection, and profiling capabilities.**

**Benefits of AWS X-Ray include:**

1- Review request behavior

2- Discover application issues

3- Improve application performance

**Amazon Athena** is an **interactive query service** that makes it easy to analyze data **in Amazon S3 using standard SQL.**

Only the **Enterprise plan** comes with a TAM.

**AWS Elastic Beanstalk** is a platform service **that leverages the automation** capabilities of **CloudFormation** to build out application architectures.

AWS Elastic Beanstalk is an easy-to-use service for d**eploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.** You can simply **upload your code and Elastic Beanstalk automatically handles the deployment**, **from capacity provisioning, load balancing, auto-scaling to application health monitoring**. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

**You have just finished writing your application code. Which service can be used to automate the deployment and scaling of your application?**

**AWS Elastic Beanstalk** is considered a **Platform as a Service (PaaS).** It is an easy-to-use service for **deploying, scaling and updating web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.** You can simply **upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.** At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time

**Elastic Load Balancing (ELB)** is used for **distributing incoming connections** to Amazon EC2 instances.  Amazon Elastic Load Balancing is **used to spread load and introduce fault tolerance by distributing connections across multiple identically configured back-end EC2 instances.**

AWS Elastic Load Balancer (ELB) is **a service that distributes the incoming application traffic to multiple targets that you define.**

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as **Amazon EC2 instances, containers, and IP addresses.**

Elastic Load Balancing provides f**ault tolerance for applications by automatically balancing traffic across targets – Amazon EC2 instances, containers and IP addresses** – **and Availability Zones** while ensuring only healthy targets receive traffic.

**Elastic Load Balancing supports three types of load balancers.** You can select the appropriate load balancer **based on your application needs.**

* If you need to load balance **HTTP requests,** AWS recommends using the **Application Load Balancer**.
* For **network/transport protocols (layer4 – TCP, TLS, UDP) load balancing, and for extreme performance/low latency applications**, AWS recommends using **Network Load Balancer**.
* If your application is built within the **EC2 Classic network** then you should use **Classic Load Balancer.**

**AWS organizations** allow you to **consolidate multiple AWS accounts into an organization that you create and centrally manage**. Unused reserved instances (RIs) for EC2 are applied across the group so the organization can utilize their unused reserved instance instead of consuming on-demand instances which will lower their costs.

The **AWS Organizations API** can be used **to create AWS accounts and this can be automated through code.**

AWS Organizations helps you **centrally govern your environment as you grow and scale your workloads on AWS**. 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.**

**AWS Organizations has five main benefits:**

1) Centrally **manage access polices** across multiple AWS accounts.

2) **Automate** AWS account creation and management.

3) **Control access** to AWS services.

4) **Consolidate billing** across multiple AWS accounts.

5) **Configure** AWS services across multiple accounts.

**Which AWS service or feature helps restrict the AWS service, resources, and individual API actions the users and roles in each member account can access? AWS Organizations** offers the following policy types:

**Service control policies (SCPs)** offer central control over the maximum available permissions for all of the accounts in your organization.

**Tag policies** help you standardize tags across resources in your organization's accounts.

**SCPs** are used to restrict access within member accounts. For instance you can create an SCP that restricts a specific API action such as deploying a particular Amazon EC2 instance type. The policy would then prevent anyone, including administrators, from being able to launch EC2 instances using that instance type.

**Amazon Connect** is a self-service, **cloud-based contact center service** that makes it easy for businesses to **deliver better customer service at a lower cost.**

**Access keys** are a combination of an **access key ID and a secret access key**. They are used to make **programmatic calls to AWS using the API.**

Amazon EC2 instances running Linux are billed in one second increments, with a minimum of 60 seconds.

**AWS Elastic Beanstalk** can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. **Considered a Platform as a Service (PaaS) solution.** Supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications.

**Amazon EC2** is an **IaaS solution** that provides **unmanaged instances that you can deploy with a variety of operating systems**. With EC2 you are billed either by the second, for some Linux instances, or by the hour for all other instance types.

Amazon Elastic Compute Cloud (Amazon EC2) is a **server-based compute service**. Amazon EC2 is categorized as **Infrastructure as a Service (IaaS)** and, as such, requires the customer to perform all of the necessary configurations and management tasks.

**Elasticity** is the ability to **scale resources up or down and only pay for what you use**. A great example is **Auto Scaling** which launches and terminates EC2 instances based on the amount of load.

Elasticity is the ability to **dynamically adjust the capacity of a service or resource based on demand**. Scaling can be vertical (e.g. increase instance size) or horizontal (e.g. add more EC2 instances).

**With horizontal scaling** you **add more instances to a fleet of instances to service demand as it increases.** This can be achieved **automatically by using AWS Auto Scaling to add instances in response to CloudWatch performance metrics.**

**With vertical scaling** you are **adding CPU, RAM or storage to an existing instance**. This may involve **modifying the instance type which typically requires a restart**. With vertical scaling on AWS scalability is **limited by the maximum instance size.**

**Economy of scale** refers to **pricing benefits based on AWS purchasing large amounts of resources.**

**High availability** is an **example of resilience**.

**Fault Tolerance** is the **ability for a system to recover from the** **failure of a single component**.

**Agile Development** is a **flexible model of code development** that results in faster deployment times.

**Agility** is an example of **flexibility and speed of implementation.**

**Amazon CloudWatch** is a **monitoring service for AWS cloud resources and the applications** you run on AWS. You use CloudWatch for **performance monitoring**, not automating operational tasks. Amazon CloudWatch is a monitoring and management service built for **developers, system operators, site reliability engineers (SRE), and IT managers.**

You can monitor your estimated AWS charges by using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

The **alarm triggers when your account billing exceeds the threshold you specify**. It **triggers only when actual billing exceeds the threshold**. It doesn't use projections based on your usage so far in the month.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. CloudWatch is for performance monitoring (CloudTrail is for auditing).

It is **used to collect and track metrics, collect and monitor log files, and set alarms. Basic monitoring collects metrics every 5 minutes whereas detailed monitoring collects metrics every 1 minute.**

Amazon CloudWatch is a **monitoring service for AWS cloud resources** **and the applications you run on AWS.** CloudWatch performs **performance monitoring and can monitor custom metrics generated by applications and the operational health of your AWS resources.**

**You can use Amazon CloudWatch Logs** to **monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.** You can then retrieve the associated log data from CloudWatch Logs.

**AWS CloudTrail** is **a web service that records activity made on your account and delivers log files to an Amazon S3 bucket**. CloudTrail is for **auditing**, whereas CloudWatch is for performance monitoring. CloudTrail is **about logging and saves a history of API calls for your AWS account**

**Trusted Advisor** is an online resource to help you **reduce cost, increase performance, and improve security by optimizing your AWS environment**. Trusted Advisor provides **real time guidance** to help you **provision your resources following AWS best practices**. Offers a **Service Limits check** (in the Performance category) that displays your **usage and limits for some aspects of some services.** It can **assist with providing recommended actions on cost optimization.**

AWS Trusted Advisor offers a rich set of best practice **checks and recommendations across five categories:**

* **cost optimization;**
* **security;**
* **fault tolerance;**
* **performance;**
* **service limits.**

AWS Trusted Advisor improves the security of your application by closing gaps, enabling various AWS security features, and examining your permissions.

**The core security checks include: (Important)**

**1- Security Groups - Specific Ports Unrestricted.**

Checks security groups for rules that allow unrestricted access to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

**2- Amazon S3 Bucket Permissions.**

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. This check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.

**3- MFA on Root Account**

Checks the root account and warns if multi-factor authentication (MFA) is not enabled. For increased security, AWS recommends that you protect your account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device when interacting with the AWS console and associated websites.

**AWS Personal Health Dashboard** provides **alerts and remediation guidance** when AWS is experiencing **events that may impact you.**

**The benefits of the AWS personal health dashboard include:**

* A personalized View of Service Health
* Proactive Notifications
* Detailed Troubleshooting Guidance

**The AWS Service Health Dashboard** publishes AWS’ most up-to-the-minute information on service availability. The dashboard provides access to current status and historical data about every AWS Service. < ---- **What can you access by visiting the URL: http://status.aws.amazon.com?**

**4. test**

**AWS Budgets** 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**. It can be used to create alerts when the actual or forecasted cost of AWS services exceed a certain threshold.

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 ElastiCache, and Amazon Elasticsearch reservations.

**Cost Explorer** lets you visualize and understand your costs. AWS Cost Explorer – **enables you to visualize your usage patterns over time and to identify your underlying cost drivers.**

AWS Cost Explorer is **a free tool that you can use to view your costs and usage. You can view data up to the last 13 months, forecast how much you are likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase**. You can use AWS Cost Explorer to see patterns in how much you spend on AWS resources over time, identify areas that need further inquiry, and see trends that you can use to understand your costs. You can also specify time ranges for the data, and view time data by day or by month.

**The AWS support team** will direct you to use AWS Cost Explorer.

**AWS Cost and Usage report** is a tool that can be used to view usage for AWS services by category.

**The AWS Storage Gateway** AWS Storage Gateway is a **hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage.** **You can use the service** **for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration**. It seamlessly integrates on-premises enterprise applications and workflows with Amazon’s block and object cloud storage services through industry standard storage protocols. **AWS Storage Gateway** is **the service that enables your on-premises applications to seamlessly use AWS cloud storage.** The gateway connects to AWS storage services - such as Amazon S3 and Amazon EBS - and provides storage for files, volumes, snapshots, and virtual tapes in AWS.

It allows integration of on-premises IT environments with Cloud Storage. AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure.

**Amazon S3 Cross Region Replication (CRR)** is used for copying data from one S3 bucket to another S3 bucket in another region.

**Amazon CloudFront** is a content delivery network. It is used to get content closer to users.

**Amazon CloudFront** is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

**The use cases of Amazon CloudFront include:**

**1- Accelerate static website content delivery.**

CloudFront can speed up the delivery of your static content (for example, images, style sheets, JavaScript, and so on) to viewers across the globe. By using CloudFront, you can take advantage of the AWS backbone network and CloudFront edge servers to give your viewers a fast, safe, and reliable experience when they visit your website.

**2- Live & on-demand video streaming.**The Amazon CloudFront CDN offers multiple options for streaming your media – both pre-recorded files and live events – at sustained, high throughput required for 4K delivery to global viewers.

**3- Security.**

CloudFront integrates seamlessly with AWS Shield for Layer 3/4 DDoS mitigation and AWS WAF for Layer 7 protection.

**4- Customizable content delivery with Lambda@Edge.**

Lambda@Edge is a **feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency.**

**On-Demand EC2 billing option** gives you low cost, maximum flexibility, no upfront costs or commitment, and you only pay for what you use.

**Dedicated hosts** use physically **dedicated EC2 servers** to isolate your workloads and are expensive. **Dedicated hosts** are EC2 servers **dedicated to a single customer.**

Amazon 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 own licenses, but with the resiliency, simplicity and elasticity of AWS.** An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can **help address corporate compliance requirements**. It should be used to comply with per-core software license requirements.

**Which service allows an organization to bring their own licensing on host hardware that is physically isolated from other AWS accounts?**  **An Amazon EC2 Dedicated Host** is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts **allow you to use your existing per-socket, per-core, or per-VM software licenses, including Windows Server, Microsoft SQL Server, SUSE, Linux Enterprise Server, and so on.**

**Dedicated Instances** are Amazon **EC2 instances that run in a VPC on hardware** that’s dedicated to a single customer.

**Spot instances** are used for getting **a very low price** which you bid on. You lose some flexibility as you are constrained by market prices and your workloads can be terminated if the market price exceeds your bid price. Spot Instances allow you to purchase **spare computing capacity with no upfront commitment at discounted hourly rates. This is not used for long-term requirements.**

**Reserved instances** are based on a commitment to 1 or 3 years in exchange for a large discount. It provides significant discounts for fixed term contracts.

**Typical use cases for the pricing models listed are:**

**On-demand:**Good for users that want **the low cost and flexibility of EC2 without any up-front payment or long-term commitment. Applications with short term, spiky, or unpredictable workloads that cannot be interrupted.**

On Demand instances would help **provision any extra capacity that the application may need without any interruptions.**

**Reserved:** Applications with **steady state or predictable usage or that require reserved capacity. Using Reserved instances requires a contract of at least one year.**

**Spot:** Applications that have **flexible start and end times and that are only feasible at very low compute prices. May be terminated.** Spot Instances are well-suited for **data analysis, batch jobs, background processing, and optional tasks.**

**Dedicated hosts:**Useful for **regulatory requirements that may not support multi-tenant virtualization.** **Great for licensing which does not support multi-tenancy or cloud deployments.** **Dedicated instances are used when you want your instances to be isolated at the host hardware level from instances that belong to other customers (and also it has a greater cost).**

**A subnet** is a **range of IP addresses within a VPC.**

**Amazon EC2 Auto Scaling** is configured within the EC2 console and can launch instances within a VPC across multiple AZs (**Multiple AZs within a region**). It cannot launch resources into another AWS Region.

A user has an AWS account with **a Business-level AWS Support plan** and needs assistance with handling a production service disruption. The Business support plan provides a service level agreement (SLA) of < 1 hour for production system down support cases.

**The dedicated TAM** only comes with the Enterprise support plan.

The Technical Account Manager provides expert monitoring and optimization for your environment and coordinates access to other programs and experts.

**The concierge support team** only comes with the Enterprise support plan.

Included as part of the Enterprise Support plan, **the Support Concierge Team** are AWS **billing and account experts** that specialize in working with enterprise accounts.

**The business-critical system down support** only comes with the Enterprise support plan.

**AWS Managed VPN** uses the Internet for network connections, so it is not creating a private connection. The AWS Managed VPN (which is a type of IPSec VPN) is fast to setup but uses the public Internet and therefore latency is not as good and is unpredictable.

**Client VPN**: A site-to-site VPN should be used rather than a client VPN to connect two sites together.

**AWS Virtual Private Network (AWS VPN)** is a service that lets you establish a secure and private tunnel from your on-premises network or device to the AWS global network.

**AWS VPN CloudHub** uses the Internet for network connections, so it is not creating a private connection.

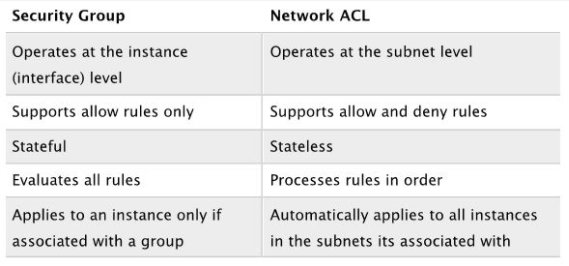
**An AWS VPC Endpoint** is a PrivateLink connection that connects an AWS public service to a VPC using a private connection. This does not connect on-premises environments to AWS.

VPC endpoint enable private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.

You can configure **subnets and endpoints** within the VPC section of AWS management console.

**EBS volumes and ELB** must be configured in the EC2 section of the AWS management console and **DNS records** must be configured in Amazon Route 53.

A **Network ACL** supports allow and deny rules. You can create a deny rule specifying a specific IP address that you would like to block.



**AWS Shield** is a managed **Distributed Denial of Service (DDoS) protection service**.

**AWS WAF** is a **web application firewall.** AWS WAF is a web application firewall that helps protect your web applications from common web exploits.

AWS WAF (Web Application Firewall) helps protect your web applications from **common web exploits** that could affect a**pplication availability, compromise security, or consume excessive resources**. **You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.**

**Amazon EC2** Compute service should be used for running a Linux operating system upon which you will install custom software. Amazon EC2 should be used when you need access to a full operating system instance that you can manage.

**Amazon Elastic Container Service (ECS) and Amazon Elastic Container Service for Kubernetes (EKS)** are used for running software containers, not full operating system instances.

**AWS Lambda** runs code as functions in response to events. With AWS Lambda you don’t have any servers to manage (serverless). Lambda functions scale out rather than up running multiple invocations of the function in parallel.

**AWS Directory Service** for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

**Amazon Cloud Directory** enables you to **build flexible cloud-native directories** for organizing hierarchies of data along multiple dimensions.

Amazon Cloud Directory allows the organization of hierarchies of data across multiple dimensions.

**‘Design for failure** is an architectural best practice recommended by AWS. This means always considering what would happen if a component of an application fails and ensuring there is resilience in the architecture.

A **virtual private cloud (VPC)** is a virtual network dedicated to your AWS account. A VPC spans all the Availability Zones in the region.

With **loose coupling** you reduce interdependencies between components of an application and often put a middle layer such as a message bus between components.

**Amazon ElastiCache** provides in-memory caching which improves performance for read requests when the data is cached in ElastiCache. ElastiCache can be placed in front of your database. Though it does improve read performance for database queries, **it is not a global service that is designed to improve performance for users around the world.** Amazon ElastiCache is an in-memory database cache and is **used to introduce improved performance rather than fault tolerance.**

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

**Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory data store, instead of relying entirely on slower disk-based databases.** Querying a database is always slower and more expensive than locating a copy of that data in a cache. **By caching (storing) common database query results, you can quickly retrieve the data multiple times without having to re-execute the query.**

**Amazon ElastiCache for Redis** is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Built on open-source Redis and compatible with the Redis APIs, ElastiCache for Redis works with your Redis clients and uses the open Redis data format to store your data. Your self-managed Redis applications can work seamlessly with ElastiCache for Redis without any code changes. ElastiCache for Redis combines the speed, simplicity, and versatility of open-source Redis with manageability, security, and scalability from Amazon to power the most demanding real-time applications in Gaming, Ad-Tech, E-Commerce, Healthcare, Financial Services, and IoT.

**The AWS Security Token Service (STS)** is **a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users).**

The **IAM console** provides information about when IAM users and roles last attempted to access AWS services. This information is called ***service last accessed data***. This data can help you identify unnecessary permissions so that you can refine your IAM policies to better adhere to **the principle of “least privilege.”** **That means granting the minimum permissions required to perform a specific task.**

**Penetrating Test:** Customers to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for selected services.

AWS customers are welcome to **carry out security assessments or penetration tests against their AWS infrastructure without prior approval for the following eight services:**

• Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.

• Amazon RDS.

• Amazon CloudFront.

• Amazon Aurora.

• Amazon API Gateways.

•  AWS Lambda and Lambda Edge functions.

• Amazon LightSail resources.

• Amazon Elastic Beanstalk environments.

**The 6 advantages of cloud computing are:**

– Trade capital expense for variable expense.

– Benefit from massive economies of scale.

– Stop guessing about capacity.

– Increase speed and agility.

– Stop spending money running and maintaining data centers.

– Go global in minutes.

**Amazon S3** is an object-based storage system that is accessed **using a RESTful API over HTTP(S).** It consists of buckets, which are root level folders, and objects, which are the files, images etc. that you upload. It **stores objects comprised of key, value pairs**

**LightSail** offers virtual servers (instances) that are easy to set up and backed by the power and reliability of AWS. AWS LightSail is a **compute service that offers a lower cost and easier to use alternative to Amazon EC2.**

Amazon LightSail provides an easy, low cost way to consume cloud services without needing the skill set for using VPC resources. **The product set includes virtual private servers (instances), managed MySQL databases, HA storage, and load balancing.** You can connect to other AWS services such as **S3, DynamoDB, and CloudFront, h**owever these are not part of the LightSail product range**.**

**Amazon Connect** is a **self-service, cloud-based contact center service that makes it easy for any business to deliver better customer service at lower cost.**

With Amazon RDS you are charged for:

* the type and size of database,
* the uptime,
* any additional storage of backup (above the DB size),
* requests,
* deployment type (e.g. you pay for multi AZ),
* data transfer outbound.

The **AWS Storage Gateway** service **enables hybrid storage** between on-premises environments and the AWS Cloud.

The **Gateway Virtual Tape Library** can be used with popular backup software such as NetBackup, Backup Exec and Veeam. Uses a virtual media changer and tape drives.

**File gateway** provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3.

The **volume gateway** represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes.

**Data stored within an AWS region is not replicated outside of that region automatically.** It is up to customers of AWS to determine whether they want to replicate their data to other regions. You must always **consider compliance and network latency when making this decision.**

**The AWS Simple Monthly Calculator** helps you to estimate the cost of using AWS services. It shows how much you would pay in AWS if you move your resources.

**The AWS Simple Monthly Calculator** helps you estimate your monthly AWS bill more efficiently. The calculator can be used to determine your best and worst case scenarios and identify areas of development to reduce your monthly costs. The AWS Simple Monthly Calculator is continuously updated with the latest pricing for all AWS services in all Regions.

**The AWS Cost & Usage Report** enables customers **to access detailed information** related to their AWS costs and usage. This information can **help them analyze their cost drivers and usage trends**.

**AWS Cost Explorer** is used to explore and analyze **your historical spend and usage.** AWS Cost Explorer allows you to have **visibility into your consumption patterns**, such as, mapping the most commonly used services, and identifying unexpected anomalies or expenses.

       AWS Cost Explorer can also be used to estimate AWS services costs, but it calculates these estimates based on your previous AWS consumption (meaning AWS Cost Explorer is suitable for **existing projects only**).

**AWS Cost Explorer Forecasting** provides an estimate of what your AWS bill will be, based on your past usage. AWS Cost Explorer segments your historical data based on distinct charge types (e.g., on-demand usage, reserved instance usage, and more) and **uses a combination of machine learning and rules-based models to predict spend across all of those charge types individually.**

**Amazon Instance Store** is a **type of ephemeral block-based volume** that can be **attached to a single EC2 instance at a time.**

**EBS volumes** can only be attached to a single EC2 instance at a time and are block devices (not NFS).

EBS-backed means the root volume is an **EBS volume** and storage is persistent.

Instance store-backed means the root volume is an **instance store volume** and storage is not persistent. Both EBS and Instance store volumes are block-based storage devices. EBS volumes can be used with all EC2 instance types whereas Instance store volumes are more limited in compatibility.

**EFS** is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS uses the **NFSv4.1 protocol.** Can concurrently connect 1 to 1000s of EC2 instances, from multiple AZs.

Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it.

Amazon EFS is **designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, with consistent low latencies.** As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones. **With these capabilities, Amazon EFS is well suited to support a broad spectrum of use cases, including web serving and content management, enterprise applications, media and entertainment processing workflows, home directories, database backups, developer tools, container storage, and big data analytics workloads**

**Amazon Elastic File System (Amazon EFS)** provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS Cloud services and on-premises resources.

Amazon Elastic File System (Amazon EFS) is a storage service that provides parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

**Elastic IP addresses** are for use in a specific region only and can therefore only be remapped between instances within that region. You can use Elastic IP addresses to **mask the failure of an instance in one Availability Zone by rapidly remapping the address to an instance in another Availability Zone**.

**Amazon Simple Notification Service (Amazon SNS)** is a web service that makes it easy to set up, operate, and send notifications from the cloud. SNS can be used to **send automated or manual notifications to email, mobile (SMS), SQS, and HTTP endpoints.**

**Amazon Simple Notification Service (SNS)** is a **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 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.

Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential step.

**Amazon Simple Workflow Service (SWF)** is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks. It **assist with coordinating tasks across distributed application components.**

**Amazon Simple Email Service (Amazon SES)** is a cloud-based email sending service designed to **help digital marketers and application developers send marketing, notification, and transactional emails.** It is limited to sending email.

**Amazon Elastic Container Registry (ECR)** is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy **Docker container images.**

Amazon ECR is integrated with Amazon Elastic Container Service (ECS). Amazon ECR eliminates the need to operate your own container repositories or worry about scaling the underlying infrastructure.

**APN Consulting Partners** are professional services firms that help customers of all sizes design, architect, build, migrate, and manage their workloads and applications on AWS. Consulting Partners include System Integrators (SIs), Strategic Consultancies, Agencies, Managed Service Providers (MSPs), and Value-Added Resellers (VARs).

**AWS IoT Core** is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.

**AWS Server Migration Service (SMS)** is an **agentless service** which makes it easier and faster for you to migrate thousands of on-premises **workloads** to AWS.

**Using IAM roles** instead of storing credentials within EC2 instances is more secure It is also easier to manage roles.

**Amazon SageMaker** is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes all the barriers that typically slow down developers who want to use machine learning.

**Amazon Rekognition** makes it easy to add image and video analysis to your applications.

**Amazon Comprehend** is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text.

**Amazon MQ** is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud.

With **the standard storage class** you pay a per GB/month storage fee, and data transfer out of S3. **Standard-IA and One Zone-IA** have a minimum capacity charge per object. **Standard-IA, One Zone-IA, and Glacier** also have a retrieval fee. **You don’t pay for data into S3 under any storage class.**

**Amazon Aurora Global Database** is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. This **is a way to have an SQL database across regions**, which is not a good use case for hosting media files.

**Amazon Aurora** is a MySQL and PostgreSQL-compatible relational database.

Amazon Aurora is a **MySQL and PostgreSQL compatible relational database built for the cloud, that combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases.** Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial-grade databases at 1/10th the cost. Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

           Amazon Aurora features "Amazon Aurora Serverless" which is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible and PostgreSQL-compatible editions), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs.

**Amazon ECS** is used for **running software containers** such as Docker containers.

**Amazon EKS** is used for **managing software containers** such as Docker containers.

**AWS CodeCommit** is a **fully-managed source control service** **that hosts secure Git-based repositories.**

**AWS CodeCommit** is a source code control service that hosts secure Git-based code repositories. AWS CodeCommit is designed for software developers who need a secure, reliable, and **scalable source control system to store and version their code.**

**CodeCommit is an AWS repository management system that allows for storing, versioning, and managing your application code.**

**You can store files on the Elastic Block Store (EBS), and Elastic File System (EFS).** EBS volumes are mounted as **block devices to EC2 instances** and EFS volumes are mounted to **the instance using the NFS protocol.**

**Amazon Simple Queue Service (SQS)** is a message bus for temporarily storing data that is being passed between application components. 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.**

Amazon SQS is a highly reliable, scalable message queuing service that enables asynchronous message-based communication between distributed components of an application. 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.**

**Amazon Simple Email Service (Amazon SES)** is a cloud-based email sending service designed to help **digital marketers and application developers send marketing, notification, and transactional emails.**

**Primary benefits of using AWS Elastic Load Balancing**

**High availability –** ELB automatically distributes traffic across multiple EC2 instances in different AZs within a region.

**Elasticity –** ELB is capable of handling rapid changes in network traffic patterns.

AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

You can upload code directly using a **ZIP or WAR file**. You can also **use a Git archive.**

**AWS Elastic Beanstalk** is an **application container on top  of Amazon Web Services**. Elastic Beanstalk makes it easy for developers to **quickly deploy and manage applications in the AWS Cloud.** Developers simply **upload their application code, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.**

It is a **PaaS solution to automate application deployment**.

**Object lifecycle management** can be used with objects so that they are **stored cost effectively throughout their lifecycle.** Objects can be transitioned to another storage class or expired. It **enables you to set rules to automatically transfer objects between different storage classes at defined time intervals.**

**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.

You can point **AWS Glue to data stored on AWS, and AWS Glue discovers the data and stores the associated metadata (e.g. table definition and schema) in the** **AWS Glue Data Catalog**. **Once cataloged, the data is immediately searchable, queryable, and available for ETL.**

AWS Glue is a **fully-managed, pay-as-you-go, extract, transform, and load (ETL) service that automates the time-consuming steps of data preparation for analytics.**

**Amazon Elastic Map Reduce (EMR)** provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process **vast amounts of data** across dynamically scalable Amazon EC2 instances

**Amazon DynamoDB Accelerator (DAX)** is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second.

DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management.

**Where possible, you should replace EC2 workloads with AWS managed services that don’t require you to take any capacity decisions.** AWS Lambda is a serverless services and you only pay for actual processing time. Other examples of services that you don’t need to make capacity decisions with include: ELB, CloudFront, SQS, Kinesis Firehose, SES, and CloudSearch.

**A cloud practitioner needs to decrease application latency and increase performance for globally distributed users.**

Amazon S3 is an object-based storage system. It can be used to store data such as files and images that need to be served. Optionally, an S3 bucket can be configured as a static website. Amazon CloudFront is a content delivery network (CDN) that caches content at Edge Locations around the world.

These two services can work together with an S3 bucket configured as an origin for the CloudFront distribution. Users around the world will then be able to pull the content from the local Edge Location with lower latency and better performance.

**Amazon AppStream** 2.0 is an application streaming service for streaming applications to computers

**Assuming you have configured them correctly, which AWS services can scale automatically without intervention** : Both **S3 and DynamoDB** automatically scale as demand dictates. In the case of DynamoDB you can either configure the on-demand or provisioned capacity mode. With on-demand capacity mode DynamoDB automatically adjusts the read and write throughput for you.

**Amazon Kinesis** is a set of services used for collecting, processing and analyzing **streaming data**.

**Amazon Route 53** health checks monitor the health and performance of your web applications, web servers, and other resources.

**Point-in-time- recovery:** You can restore an Amazon RDS database instance to a specific point in time with a granularity of 5 minutes. Amazon RDS uses transaction logs which it uploads to Amazon S3 to do this.

**The TCO calculator** asks for the number of servers (Physical or VMs) you are running on-premises. You also need to supply the resource information (CPU, RAM) and specify whether the server is a DB or non-DB.

Use this new calculator to compare the cost of your applications in an on-premises or traditional hosting environment to AWS. Describe your on-premises or hosting environment configuration to produce a detailed cost comparison with AWS.

**Amazon CloudWatch Events** delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources.

**AWS Direct Connect gateway:** a company connect from their on-premises network to VPCs in multiple regions using private connections. You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different Regions.

**An internet gateway** is a horizontally scaled, redundant, and highly available VPC component that **allows communication between instances in your VPC and the internet**. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

**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 that have been assigned public IPv4 addresses.

**Cross-Region replication (CRR)** is used to copy objects across Amazon S3 buckets in different AWS Regions. The only option here that will help is to use CRR to copy the data to another region. This will provide disaster recovery.

**AWS LightSail** is a service that is used for running virtual instances and databases using a simplified user interface for users who are less experienced with AWS (also at a much lower cost than EC2).

**A Cloud Practitioner needs to rapidly deploy a popular IT solution and start using it immediately: Quick Starts** are built by AWS solutions architects and partners to help you **deploy popular technologies** on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Each Quick Start includes **AWS CloudFormation templates** that automate the deployment and **a guide** that discusses the architecture and provides step-by-step deployment instructions.

**The well architected framework** is documentation that provides guidance on design best practices.

**An Amazon Machine Image (AMI)** provides the **information required to launch an instance.** You can use an AMI to launch identical instances from a standard template. This is also known as a Golden Image (though no such feature exists in AWS with this name). **An AMI is created from** **an EBS snapshot and also includes launch permissions and a block device mapping**. **It allows an administrator to create a standardized image that can be used for launching new instances**.

**In your on-premises environment, you can create as many virtual servers as you need from a single template. What can you use to perform the same in AWS? -** An **Amazon Machine Image (AMI)** is a template that contains a software configuration (for example, an operating system, an application server, and applications). This pre-configured template save time and avoid errors when configuring settings to create new instances. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

**Which AWS components aid in the construction of fault-tolerant applications?**

**Elastic IP addresses** can be easily remapped between EC2 instances in the event of a failure. **Amazon Machine Images (AMIs)** can be used to quickly launch replacement instances when there is a failure.

**A company needs protection from distributed denial of service (DDoS) attacks on its website and assistance from AWS experts during such events: AWS Shield Advanced** provides **enhanced detection and includes a specialized support team for customers on Enterprise or Business support plans. The AWS DDoS Response Team (DRT) are available 24/7 and can be engaged before, during, or after a DDoS attack.**

**AWS Firewall Manager** is used to simplify management of AWS WAF, AWS Shield Advanced, and Amazon VPC security groups.

**AWS WAF** is used for **protecting web applications and APIs against** **malicious attacks**. This is not a DDoS prevention service.

**Amazon EBS encryption** offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. It uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and snapshots.

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

All volumes can now be encrypted at launch time and it’s possible to set this as the default setting.

**Both non-root and root volumes of EBS can be encrypted.**

**What should be done to keep the data on EBS volumes safe?**

**1) Ensure that EBS data is encrypted at rest.**

**2) Create EBS Snapshots.**

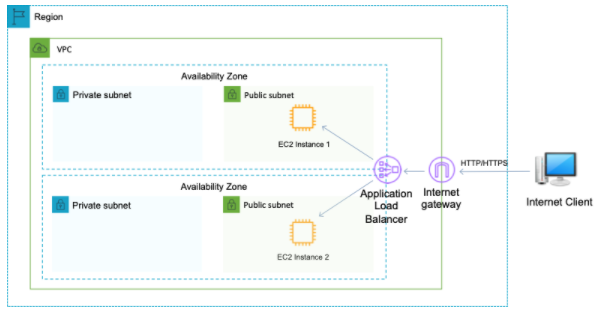
**EBS Snapshots** are incremental backups, which means that only the blocks on the device that have changed after your last snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.

**Which support plan is the lowest cost option that allows unlimited cases to be open?**

**With the Developer plan you can open unlimited cases**. You can also open unlimited cases with the **Business and Enterprise plans but these are more expensive**. You cannot open any support cases with the basic support plan.

**When you deploy an application across multiple Availability Zones the application can be considered to be highly available.** You must also have a way of directing traffic to the application in each AZ such as **an Elastic Load Balancer.**

The diagram below depicts an example of a highly available application deployed on EC2 instances in multiple AZs and using an ELB to direct traffic:



**Amazon S3 cross-region replication**: 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.

Both source and destination buckets must have versioning enabled. The source bucket owner must have the source and destination AWS Regions enabled for their account. The destination bucket owner must have the destination Region-enabled for their account. **S3 buckets configured for cross-region replication can be owned by a single AWS account or by different accounts.**

Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying hardware, underlying operating system (OS), or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.

Required patching is automatically scheduled only for patches that are related to security and instance reliability. Such patching occurs infrequently (typically once every few months) and seldom requires more than a fraction of your maintenance window.

All you need to do to get enable patching is specify the maintenance window in which the patching will take place. This can be done at instance creation time or at any time afterwards.

Enable automatic patching for the instances using the Amazon RDS console.

AWS Key Management Service (KMS) makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications. AWS KMS provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.

**Amazon KMS is used when encrypting EBS volumes.** AWS Key Management Service is also integrated with other AWS services including **Amazon S3**, and **Amazon Redshift**, to make it simple to encrypt and decrypt your data.

**AWS Lambda and Amazon API Gateway** are both app-facing components of the AWS Serverless infrastructure.

**AWS Step Functions** is an orchestration service. **AWS Step Functions** lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. AWS Step Functions lets you build visual workflows that enable fast translation of business requirements into technical requirements. It **makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow.**

You can use **resource groups** to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at one time. Resource groups make it easy to group resources using the tags that are assigned to them. You can group resources that share one or more tags. **It** **enables you to group resources that share one or more tags.**

**Resource Groups** help you organize **multiple AWS resources in groups**. 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.

**Amazon DynamoDB** is a **fully managed NoSQL database service** that provides fast and predictable performance with seamless scalability. **Push button** **scaling** means that you can scale the DB at any time **without incurring downtime**. DynamoDB is **schema-less.**

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity, makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

DynamoDB **enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS** so that they do not have to worry about hardware provisioning, setup and configuration, throughput capacity planning, replication, software patching, or cluster scaling.

**Which feature of Amazon S3 enables you to create rules to control the transfer of objects between different storage classes?** : **Lifecycle Management.** To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their ***Amazon S3 Lifecycle***. **An *S3 Lifecycle configuration* is a set of rules that define actions that Amazon S3 applies to a group of objects.** There are two types of actions:

• **Transition actions**—**Define when objects transition to another storage class.** For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

• **Expiration actions**—Define when objects expire. Amazon S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

**Object sharing** refers to the ability to make any object publicly available via a URL.

**Versioning** enabled you to automatically keep multiple versions of an object (when enabled).

**Bucket policies** are used for controlling access to buckets, they can’t be used to move data between storage classes.

AWS has a set of solutions to help you with **cost management** and optimization. This includes services, tools, and resources to organize and track cost and usage data, enhance control through consolidated billing and access permission, enable better planning through budgeting and forecasts, and further lower cost with resources and pricing optimizations.

**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 Amazon S3.** **Macie applies machine learning and pattern matching techniques to the Amazon S3 buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.**

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data stored in Amazon S3. Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with other AWS accounts. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data. Amazon Macie can also be used in combination with other AWS services, such as AWS Step Functions to take automated remediation actions. This can help you meet regulations, such as the General Data Privacy Regulation (GDPR).

**Amazon GuardDuty** is a service that analyzes your resources using anomaly detection and machine learning. It does not detect personally identifiable information.

**Amazon GuardDuty** offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

**Amazon GuardDuty** offers **threat detection that enables you to continuously monitor and protect your AWS accounts and workloads.** GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

**Amazon Inspector** automatically **assesses applications for exposure, vulnerabilities, and deviations from best practices.**

**AWS Shield** is involved with protecting your resources of **distributed denial of service (DDoS) attacks.**

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers and provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

**Amazon ElastiCache and Amazon Redshift** both support reserved nodes. Reservations can be used to gain a large discount from the on-demand rate in exchange for the commitment to a contract for 1 or 3 years.

**The advantages of using Amazon RDS** include being able to **easily scale by increasing your instance type without having to go through a long procurement cycle for getting new hardware or worrying about whether capacity exists on your existing private cloud infrastructure**. You can also **implement fault tolerance and scalability features through multi-AZ and read replicas easily**

With Amazon RDS **you do not have control of the operating system and you cannot use any database software you like as you are restricted to a list of several engines. There are costs for replicating data between AZs and regions so this must be taken into account in any cost analysis**

**An Amazon Elastic Block Store (EBS) volume** is often described as a **“virtual hard disk in the cloud”.** EBS volumes are block-level storage volumes that are attached to EC2 instances much as you would attach a virtual hard disk to a virtual machine in a virtual infrastructure.

**Which AWS service can be used to run Docker containers?: AWS Fargate** is a serverless compute engine for containers that 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.

AWS Fargate is a **compute engine for Amazon ECS** that allows you **to run containers** without having to manage servers or clusters.

**According to the AWS Well-Architected Framework, what change management steps should be taken to achieve reliability in the AWS Cloud?**

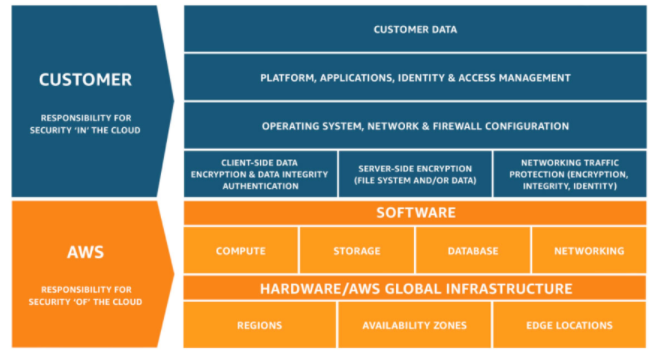
**AWS Config** can be **used to track the configuration state of your resources** **and how the state has changed over time.** With **CloudTrail** you can **audit who made what API calls on what resources at what time.** This can help with identifying changes that cause reliability issues.

**A *virtual private gateway*** is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection. **A customer gateway** is a physical device or software application on corporate data center side of the VPN connection.

**You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots.** Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

**Shared Controls** are controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include **patch management, configuration management, and awareness and training.**

**The Business Associate Addendum (BAA)** is an agreement you can choose to accept within AWS Artifact Agreements.



**Which of the authentication options below can be used to authenticate using AWS APIs?** Access keys are long-term credentials for an IAM user or the AWS account root user. You can **use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).** Server certificates are SSL/TLS certificates that you can **use to** **authenticate with some AWS services.**

**Amazon RDS** is a **managed database service that supports MySQL**. The DBA can reduce operational overhead by moving to RDS and having less work to do to manage the database.

**A VPC peering connection** helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

**A VPC peering connection** is a networking connection between **two** VPCs that enables customers to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. Using VPC peering to connect hundreds of VPCs is very complex and time consuming because customers need to peer each Amazon VPC to each other manually.

**AWS Security Token Service (STS)** is **used for requesting temporary credentials.**

**Amazon Simple Queue Service (SQS)** is **a message queue used for decoupling application components.**

**Amazon Simple Notification Service (SNS)** is a web service that makes it easy to set up, operate, and send notifications from the cloud. SNS supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS.

**AWS Transit Gateway** is a service that enables customers **to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.** With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway into each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway **acts as a hub that controls how traffic is routed among all the connected networks which act like spokes.**

**AWS Transit Gateway** is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks. AWS transit gateway simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks.

AWS Direct Connect connects you to a single Amazon VPC, not multiple VPCs in different Regions.

AWS VPN is a point-to-point connection between an on-premises location and a single Amazon VPC.

AWS Client VPN allows end users to connect to AWS using a VPN client.

**When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.**

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. User data is data that is supplied by the user at instance launch in the form of a script. User data is limited to 16KB. User data and meta data are not encrypted.

**Benefits of using IAM groups** : Groups are collections of users and have policies attached to them. This enables you to organize groups of users by job function or role and apply relevant policies to the group.

You can use groups to assign permissions to users and should follow the principal of least privilege when assigning permissions.

**Which HTTP code indicates a successful upload of an object to Amazon S3**; HTTP response status codes indicate whether a specific HTTP request has been successfully completed.

- A HTTP 200 codes indicates a successful upload.

- A HTTP 300 code indicates a redirection.

- A HTTP 400 code indicates a client error.

- A HTTP 500 code indicates a server error.

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. NLBs direct connections **based on information at the TCP connection level.**

**Amazon Elasticsearch Service** is **involved with operational analytics such as application monitoring, log analytics and clickstream analytics.** Amazon Elasticsearch Service allows you to search, explore, filter, aggregate, and visualize your data in **near real-time.**

**Amazon EMR** is **for big data processing using the Spark and Hadoop frameworks**, Amazon EMR provides a managed service for processing vast amounts data.

**Amazon Athena** is used to **analyze data directly in S3 and Glacier using standard SQL queries.**

**Amazon QuickSight** **provides a fast, cloud-powered business analytics service, that that makes it easy to build stunning visualizations and rich dashboards that can be accessed from any browser or mobile device.**

AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow 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.

**You have AWS Basic support, and you have discovered that some AWS resources are being used maliciously, and those resources could potentially compromise your data. What should you do? ---- > The AWS Abuse team** can assist you when AWS resources are being used to engage in the following types of abusive behavior:

**I. Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are being used to spam websites or forums.

**II. Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.

**III. Denial of service attacks (DOS):** Your logs show that one or more AWS-owned IP addresses are being used to flood ports on your resources with packets, and you believe this is an attempt to overwhelm or crash your server or software running on your server.

**IV. Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are being used to attempt to log in to your resources.

**V. Hosting objectionable or copyrighted content:** You have evidence that AWS resources are being used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.

**VI. Distributing malware:** You have evidence that AWS resources are being used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

**Amazon Relational Database Service (Amazon RDS)** makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity while automating time-consuming administration tasks such as hardware provisioning, operating system maintenance, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

        Amazon RDS can be used to host Amazon Aurora, PostgreSQL, **MySQL**, MariaDB, Oracle, and SQL Server databases.

**AWS Marketplace** is **a digital catalog with thousands of software listings from independent software vendors** that make it easy to find, test, buy, and deploy software that runs on AWS. AWS Marketplace includes software listings from categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps.

The AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. Customers can quickly launch pre-configured software with just a few clicks, and choose software solutions in AMI and SaaS formats, as well as other formats. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL.

**The AWS Marketplace provides value to buyers in several ways:**

1- It simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL.

2- Customers can quickly launch pre-configured software with just a few clicks, and choose software solutions in AMI and SaaS formats, as well as other formats.

3- It ensures that products are scanned periodically for known vulnerabilities, malware, default passwords, and other security-related concerns.

**The principle of least privilege** is one of the most important security practices and it means granting users the required permissions to perform the tasks entrusted to them and nothing more. The security administrator determines what tasks users need to perform and then attaches the policies that allow them to perform only those tasks. You should start with a minimum set of permissions and grant additional permissions when necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them down.

**S3** - Companies today need the ability to simply and securely collect, store, and analyze their data at a massive scale. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices.  It’s a simple storage service that offers highly available, and infinitely scalable data storage infrastructure at very low costs. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry. S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements. It gives customers flexibility in the way they manage data for cost optimization, access control, and compliance. S3 provides query-in-place functionality, allowing you to run powerful analytics directly on your data at rest in S3. And Amazon S3 is the most supported cloud storage service available, with integration from the largest community of third-party solutions, systems integrator partners, and other AWS services. Amazon S3 stores any number of objects, but each object does have a size limitation. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

**Common use cases of Amazon S3 include:**

**Media Hosting** – Build a redundant, scalable, and highly available infrastructure that hosts video, photo, or music uploads and downloads.

**Backup and Storage** – Provide data backup and storage services for others.

**Hosting** **static websites**– Host and manage static websites quickly and easily.

**Deliver content globally** - Use S3 in conjunction with CloudFront to distribute content globally with low latency.

**Hybrid cloud storage**- Create a seamless connection between on-premises applications and Amazon S3 with **AWS Storage Gateway** in order to reduce your data center footprint, and leverage the scale, reliability, and durability of AWS.

**There are three Cloud Computing Models:**

**1) Infrastructure as a Service (IaaS)** - Infrastructure as a Service (IaaS) contains **the basic building blocks for cloud IT** and typically **provide access to networking features, computers (virtual or on dedicated hardware), and data storage space.** IaaS provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.  **EC2**

**2) Platform as a Service (PaaS)** - Platform as a Service (PaaS) removes the need for your organization to manage the underlying infrastructure (usually hardware and operating systems) and allows you to **focus on the deployment and management of your applications**. This helps you be more efficient as you don’t need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.   **AWS Elastic Beanstalk service.**

**3) Software as a Service (SaaS) -** Software as a Service (SaaS) provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software. **A common example of a SaaS application is web-based email which you can use to send and receive email without having to manage feature additions to the email product or maintain the servers and operating systems that the email program is running on.**

**Amazon EBS** volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans.

EBS is **a block level storage that provides storage volumes for use with Amazon EC2 and Amazon RDS**.

**Standard RIs** provide the most significant discount **(up to 75% off On-Demand**) and are best suited for steady-state usage. Standard Reserved Instances are not modifiable. Standard RIs are best suited for **steady-state usage.**

**Convertible RIs** provide a discount (**up to 54% off On-Demand**) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. These attributes include instance family, instance type, platform, scope, and tenancy. **An organization has decided to reserve EC2 compute capacity for three years in order to reduce costs. It is possible that the application workloads could change during the reservation time period. Convertible RIs is the EC2 Reserved Instance (RI) type that will allow the company to modify the reservation if they need to.**

Like Standard RIs, **Convertible RIs are best suited for steady-state usage.** But this option allows you to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value.

**Scheduled RIs** are available to launch within the time windows you reserve. This option allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month. Scheduled Reserved Instances are not modifiable

**The AWS Finance Team** provides data driven analysis, strategic decision support, financial planning, and controllership to teams that plan and build data centers, design and source servers, and develop and sell cloud services at massive scale to developers and businesses all over the world.

You can use the **Amazon Virtual Private Cloud console** (VPC) to launch AWS resources, such as Amazon EC2 instances. You can use it to specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

**S3 Intelligent-Tiering** is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers - frequent access and infrequent access - when access patterns change.

**Amazon Kinesis Video Streams** enables you to securely stream video from connected devices (IoT devices) to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales all the infrastructure needed to ingest streaming video data from millions of devices. It durably stores, encrypts, and indexes video data in your streams, and allows you to access your data through easy-to-use APIs.

**Amazon Simple Queue Service (SQS)** is a **fully managed message queuing service that enables you to send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available**. SQS lets you decouple application components so that they run independently, increasing the overall fault tolerance of the system. Multiple copies of every message are stored redundantly across multiple availability zones so that they are available whenever needed.

**Amazon SES (Amazon Simple Email Service)** is a flexible, affordable, and highly-scalable email messaging platform for businesses and developers.

**Amazon Connect** is a cloud-based **contact center service** that makes it easy for businesses to deliver customer service at low cost.

**AWS Virtual Private Network (AWS VPN)** allows you to establish a secure and private tunnel from your network or device to the AWS global network.

**In CloudWatch**, you can set up a billing alarm that triggers if your costs exceed a threshold that you set. This CloudWatch alarm can also be configured to trigger an SNS notification to your email address.

**AWS Budgets** is another AWS service that can be used in this scenario. AWS Budgets 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. **The difference between AWS Budgets and Amazon CloudWatch billing alarms** is that Amazon CloudWatch billing alarms alert you when your **actual** cost exceeds a certain threshold, while AWS Budgets can be configured to alert you when the **actual** or **forecasted** cost exceeds a certain threshold.

**AWS Pricing Calculator** is a web service that you can use **to estimate the cost for your AWS** **monthly bill based on your expected usage.**

**What does AWS provide to deploy popular technologies - such as IBM MQ - on AWS with the least amount of effort and time?: AWS Quick Start Reference Deployments** outline the architectures **for popular enterprise solutions on AWS and provide AWS CloudFormation templates to automate their deployment.** Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices. These accelerators reduce hundreds of manual installation and configuration procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

**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.

AWS Infrastructure Event Management is a short-term engagement with AWS Support, included in the Enterprise-level Support product offering, and available for additional purchase for Business-level Support subscribers. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS.

**Per-second billing is available for instances launched in:**

- On-Demand, Reserved and Spot forms

- All regions and Availability Zones

- Amazon Linux and Ubuntu

**The AWS Management Console** allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on the go.

**The AWS Command Line Interface (CLI)** is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

**The AWS SDK (Software Development Kit)** allows you to interact with AWS services using your preferred programming language.

**AWS API** refers to the AWS application programming interface.

**You should attempt to build as much automation as possible in both detecting and reacting to failure.** You can use services like **ELB and Amazon Route53** to configure health checks and mask failure by only routing traffic to healthy endpoints. In addition, **Auto Scaling** can be configured to automatically replace unhealthy nodes. You can also replace unhealthy nodes using the **Amazon EC2 auto-recovery feature or services such as AWS OpsWorks and AWS Elastic Beanstalk**. It won’t be possible to predict every possible failure scenario on day one. Make sure you collect enough logs and metrics to understand normal system behavior. After you understand that, you will be able to set up alarms that trigger automated response or manual intervention.

**AWS Certificate Manager** (ACM) is a service that lets you **easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.**

**AWS Database Migration Service (DMS)** helps you migrate databases to AWS easily 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 most widely used commercial and open-source databases. The service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora or Microsoft SQL Server to MySQL. It also allows you to stream data to Amazon Redshift from any of the supported sources including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, SAP ASE, and SQL Server, enabling consolidation and easy analysis of data in the petabyte-scale data warehouse. AWS Database Migration Service can also be used for continuous data replication with high availability.

**AWS Server Migration Service (SMS)** is used to migrate your on-premises workloads to AWS.

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

**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: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering, and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier. There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers. It is the ideal storage class for long-lived data with access patterns that are unknown or unpredictable.

**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.

**Under the Shared Responsibility Model, which of the following controls do customers fully inherit from AWS? Environmental Controls and Physical Controls**

<https://aws.amazon.com/compliance/shared-responsibility-model/>

**Amazon EC2 Instance Store** provides temporary block-level storage for your instance. Instance store is ideal for 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.

**Amazon EBS** is not a cost-effective solution for storing images or videos (compared to Amazon S3). Amazon EBS is a block level storage that can be used as a drive for Amazon EC2 or Amazon RDS instances. Amazon EBS is designed for application workloads that benefit from fine tuning for performance and capacity. Typical use cases include Big Data analytics engines (like the Hadoop/HDFS ecosystem and Amazon EMR clusters), relational and NoSQL databases (like Microsoft SQL Server and MySQL or Cassandra and MongoDB), stream and log processing applications (like Kafka and Splunk), and data warehousing applications (like Vertica and Teradata).

**Which of the following is equivalent to a user name and password and is used to authenticate your programmatic access to AWS services and APIs?**

Access keys consist of two parts: an access key ID and a secret access key. You use access keys to sign programmatic requests that you make to AWS if you use AWS CLI commands (using the SDKs) or using AWS API operations. Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests.

**Global Reach -** With AWS, you can deploy your application in multiple regions around the world. The user will be redirected to the Region that provides the lowest possible latency and the highest performance. You can also use the CloudFront service that uses edge locations (which are located in most of the major cities across the world) to deliver content with low latency and high performance to your global users.

**High Availability -** High Availability can be achieved by deploying your application in multiple Availability Zones within a single Region. If one Availability Zone goes down, the others can handle user requests. This may not reduce latency to your international users. In other words, the application will be available for them all the time, but with high latency.

**Elasticity** refers to the ability of a system to scale the underlying resources up when demand increases (to maintain performance), or scale down when demand decreases (to reduce costs).

**Durability** refers to the ability of a system to assure data is stored and data remains consistent in the system as long as it is not changed by legitimate access. This means that data should not become corrupted or disappear due to a system malfunction. Durability is used to measure the likelihood of data loss. For example, assume you have confidential data stored in your Laptop. If you make a copy of it and store it in a secure place, you have just improved the durability of that data. It is much less likely that all copies will be simultaneously destroyed.

Data durability can be achieved by replicating data across multiple Availability Zones within a single Region. For example, the S3 Standard Tier is designed for 99.999999999% durability. This means that if you store 100 billion objects in S3, you will lose one object at most.

**VPC Flow logs** only **capture** **information** about the IP traffic going to and from network interfaces in your VPC. This information can help you **monitor the traffic** that is reaching your instances and diagnose overly restrictive or overly permissive security group and network ACL rules.

**ElastiCache** is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution, while removing the complexity associated with deploying and managing a distributed cache environment. The in-memory caching provided by Amazon ElastiCache can be used to significantly improve latency and throughput for many read-heavy applications (such as social networking, gaming, media sharing and Q&A portals) or compute-intensive workloads (such as a recommendation engine).

        In-memory caching improves application performance by storing critical pieces of data in memory for low-latency access. Cached information may include the results of common database queries or the results of computationally-intensive calculations.

     The primary purpose of an in-memory data store is to provide ultrafast (submillisecond latency) and inexpensive access to copies of data. Querying a database is always slower and more expensive than locating a copy of that data in a cache. Some database queries are especially expensive to perform. An example is queries that involve joins across multiple tables or queries with intensive calculations. By caching (storing) such query results, you pay the price of the query only once. Then you can quickly retrieve the data multiple times without having to re-execute the query.

**These are things that traditional web hosting cannot provide:**

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

**Which of the following services will help businesses ensure compliance in AWS?: AWS CloudTrail** is designed to log all actions taken in your AWS account. This provides a great resource for governance, compliance, and risk auditing.

**CloudEndure Migration** simplifies the process of migrating applications from physical, virtual, and cloud-based infrastructure, ensuring that they are fully operational in any AWS Region without compatibility issues.

**EC2 instance pricing varies depending on many variables:**

- The buying option (On-demand, Reserved, Spot, Dedicated)

- Selected AMI

- Selected instance type

- Region

- Data Transfer in/out

- Storage capacity.

Note: The number of allocated Elastic IPs is the factor that may affect Amazon EC2 charges. You can have only one Elastic IP (EIP) address associated with a running instance at no charge.

**Amazon EC2** provides you **the highest level of control over your virtual instances**, including root access and the ability to interact with them as you would any machine.

**What are the connectivity options that can be used to build hybrid cloud architectures?**

* AWS VPN
* AWS Direct Connect

**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.

**An internet gateway** is a VPC component that allows communication between your VPC and the internet.

**Change management** is defined as **“the Process responsible for controlling the Lifecycle of all Changes.** The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services.

        Despite all of the investments in software and hardware, an erroneous configuration or misstep in a process can frequently undo these efforts and lead to failure.

**AWS Config and AWS CloudTrail** are **change management tools** that help AWS customers audit and monitor all resource and configuration changes in their AWS environment

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**.

          AWS maintains service limits for each account to help guarantee the availability of AWS resources, as well as to minimize billing risks for new customers. Some service limits are raised automatically over time as you use AWS, though most AWS services require that you request limit increases manually. Most service limit increases can be requested through the **AWS Support Center** by choosing Create Case and then choosing Service Limit Increase.

**What is the primary storage service used by Amazon RDS database instances?**

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.

**Which of the following AWS services is designed with native Multi-AZ fault tolerance in mind? Amazon Simple Storage Service and Amazon DynamoDB**

**Amazon EBS volume data** is replicated across multiple servers within the same Availability Zone. **Amazon EFS data** is redundantly stored across multiple Availability Zones providing better durability compared to EBS volumes.

**Per-second billing is available for instances launched in:**

- On-Demand, Reserved and Spot forms

- All regions and Availability Zones

- Amazon Linux and Ubuntu

**What are the Amazon RDS features that can be used to improve the availability of your database?**

* Multi-AZ Deployment
* Read Replicas

**Where can you store files in AWS?**

* Amazon EBS
* Amazon EFS

**AWS CodePipeline** is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.

**Which of the following services allows you to run containerized applications on a cluster of EC2 instances? Amazon ECS**

**AWS Data Pipeline** is a web service that makes it easy to schedule regular data movement and data processing activities in the AWS cloud.

**AWS Identity and Access Management (IAM)** is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

**A company has created a solution that helps AWS customers improve their architectures on AWS. Which AWS program may support this company?**

**APN Consulting Partners** are professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on AWS. Consulting Partners include System Integrators, Strategic Consultancies, Agencies, Managed Service Providers, and Value-Added Resellers. AWS supports the APN Consulting Partners by providing a wide range of resources and training to support their customers.

**APN Technology Partners** provide software solutions that are either hosted on, or integrated with, the AWS platform. APN Technology Partners include Independent Software Vendors (ISVs), SaaS, PaaS, Developer Tools, Management and Security Vendors.

**AWS Professional Services** shares a collection of offerings to help you achieve specific outcomes related to enterprise cloud adoption. AWS Professional Services also trains your team with specialized skills and provides global specialty practices to support your efforts in focused areas of enterprise cloud computing. **AWS Professional Services** **assists customers in achieving their desired business outcomes.**

**A Technical Account Manager (TAM)** is your designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices and proactively keep your AWS environment operationally healthy. TAM is available only for the Enterprise support plan.

**Which of the following can help protect your EC2 instances from DDoS attacks?**

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. A Network Access Control List (NACL) acts as a firewall for controlling traffic in and out of one or more subnets. Therefore, if they are configured properly, they can protect your instances from DDoS attacks.

**Security Groups** are an **Amazon VPC networking feature that allows customers to control instance traffic.**

       AWS does not configure security groups or NACLs to protect you from DDoS attacks. It is the responsibility of the customer to set the appropriate NACL and security group rules to protect from these attacks and secure their network.

       In addition to Security Groups and NACLs, AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow 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.

**AWS automation tools that help them deploy their applications faster:**

**AWS Elastic Beanstalk** makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

**AWS CloudFormation** automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. Creating and interconnecting all resources your application needs to run is now as simple as creating a single EC2 or RDS instance.

**AWS Migration Hub** is used to track the progress of application migrations to AWS.

**AWS will charge the user once the AWS resource is allocated (even if it is not used). Thus, it is advised that once the user's work is completed he should:**

1- Delete all Elastic Load Balancers.

2- Terminate all unused EC2 instances.

3- Delete the attached EBS volumes that he doesn’t need.

4- Release any unused Elastic IPs.

**What is the most cost-effective purchasing option for running a set of EC2 instances that must always be available for a period of two months? On-Demand Instances**

**AWS Spot instances** can be interrupted at any time by AWS. You should only choose Spot instances if the question clearly stated that the application can handle interruptions or if continuous processing is not required. Usually Spot instances are used for batch processing jobs or for non-production applications, such as development and test servers, where occasional downtime is acceptable.

**Access keys** are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

**The AWS Key pair cryptography** enables you to securely access your Amazon EC2instances using a private key instead of a password.

**AWS SDKs** are used to simplify using AWS services in your applications with an API tailored to your programming language or platform. AWS SDKs in AWS include Java SDK, .NET SDK, Node.js SDK and many others.

AWS ACCOUNT ROOT USER and IAM USER requires an access key ID and a secret access key to get long-lived programmatic access to AWS resources.

**An AWS IAM** user might need **to make API calls** or **use the AWS CLI**. In that case, you need to create an access key (access key ID and a secret access key) for that user. You can **create IAM user access keys with the IAM console, AWS CLI, or AWS API**. To create access keys **for your AWS account root user, you must use the AWS Management Console.**

**Note:**Having access keys for your root user is not considered best practice. Anyone who has root user access keys for your AWS account has unrestricted access to all the resources in your account, including billing information. If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to.

**The following tasks can only be performed if you have root user credentials:**

1- Change your account settings. This includes the account name, root user password, and email address.

2- View certain tax invoices.

3- Close your AWS account.

4- Change your AWS Support plan or Cancel your AWS Support plan.

5- Register as a seller in the Reserved Instance Marketplace.

**To estimate the costs of Amazon EBS consider the following:**

1- Volume type.

2- Input/output operations per second(IOPS).

3- Snapshots.

4- Data Transfer.

**To estimate the costs of an Amazon CloudFront distribution consider the following:**

- Data Transfer Out.

- Traffic distribution.

- Number of requests.

**To protect your AWS infrastructure in this situation you should lock down your root user account and all IAM user accounts that the administrator had access to. To protect your AWS infrastructure you should:**

1- Change the email address and the password of the root user account

2- Enable MFA on the root user account

3- Rotate (change) all access keys for all accounts

4- Change the user name and password of all IAM users

5- Enable MFA on all IAM user accounts

**The fault tolerance of an application** is its ability to recover gracefully from failures. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.

**Amazon Elastic Transcoder** is a media transcoding service. It is designed to be a highly scalable, easy-to-use, and cost-effective way to convert (or transcode) media files from their source format into versions that will play back on devices like smartphones, tablets, and PCs.

**Amazon Pinpoint** is used by marketers to engage their customers by sending targeted email, SMS, push notifications, and voice messages.

**AWS customers have two options to host their databases on AWS:**

1- Using a managed database:

AWS Customers can use managed databases such as Amazon RDS to host their databases. In this case, **AWS is responsible** for performing all database management tasks such as hardware provisioning, patching, setup, configuration, backups, or recovery.

2- Installing a database software on Amazon EC2:

Instead of using a managed database, AWS customers can install any database software they want on Amazon EC2 and host their databases. In this case, **Customers are responsible** for performing all of the necessary configuration and management tasks.

**Note:** For Amazon RDS, all security patches and updates are applied automatically to the database software once they are released. But for databases installed on Amazon EC2, customers are required to apply the security patches and the updates manually or use the AWS Systems Manager service to apply them on a scheduled basis (every week, for example).

For Technical Support, each of the **Business and the Enterprise support plans** provides 24x7 phone, email, and chat access to Support Engineers.

**When you want to reduce the costs of Amazon EBS consider the following:**

1- Delete Unattached Amazon EBS Volumes:

An easy way to reduce wasted spend is to find and delete unattached volumes. However, when EC2 instances are stopped or terminated, attached EBS volumes are not automatically deleted and will continue to accrue charges since they are still operating.

2- Resize or Change the EBS Volume Type:

Another way to optimize storage costs is to identify volumes that are underutilized and downsize them or change the volume type.

3- Delete Stale Amazon EBS Snapshots:

If you have a backup policy that takes EBS volume snapshots daily or weekly, you will quickly accumulate snapshots. Check for stale snapshots that are over 30 days old and delete them to reduce storage costs.

**Since you are targeting a global audience, you should leverage AWS global regions to serve content to your users. The deployment option that gives you the highest redundancy** is to deploy the application in multiple Availability Zones within multiple AWS regions. This redundancy will also increase the fault tolerance of the application because if there is an outage in a single Availability Zone, the other Availability Zones can handle requests.

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

**S3 One Zone-IA** has **the lowest availability rating**: 99.5%. S3 One Zone IA only stores data in one Availability Zone instead of multiple Availability Zones that the other storage classes utilize.

**AWS provides three pricing models:**

1- Pay-as-you-go

2- Save when you reserve

3- Pay less by using more

**Amazon CloudSearch** is used to set up, manage, and scale a search solution for your website or application.

**For some services, AWS automatically replicates data across multiple Availability Zones to provide fault tolerance in the event of a server failure or Availability Zone outage.**

**For S3 Standard, S3 Standard-IA, and S3 Glacier storage classes**, your objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each on different power grids within an AWS Region. This means your data is available when needed and protected against AZ failures.

**All of your data in DynamoDB** is stored on solid state disks (SSDs) and is automatically replicated across multiple Availability Zones within an AWS region, providing built-in high availability and data durability.

An **instance store** provides temporary block-level storage for EC2 instances. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content.

**With AWS Lambda**, you pay only for what you use. You are charged based on the number of requests for your functions and the time it takes for your code to execute.

**Placement Groups** are logical groupings or clusters of EC2 instances within a single Availability Zone.

**AWS is responsible** for physical controls and environmental controls. Customers inherit these controls from AWS.

**Loose Coupling** - As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components. It allows individual application components or services to be modified without affecting other components.

**Cross-Region Replication (CRR)** is an Amazon S3 feature that enables customers to replicate data across different AWS Regions; to minimize latency for global users and\or meet compliance requirements.

**Change Management** is the process responsible for controlling the Lifecycle of all Changes made in an AWS account. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services. An erroneous configuration or misstep in a process can frequently lead to infrastructure or service disruptions. Creating and implementing a change management strategy will help reduce the risk of failure by monitoring all changes and rolling back failed changes.

AWS Config and AWS CloudTrail are change management tools that help AWS customers audit and monitor all resource and configuration changes in their AWS environment. AWS Config provides information about the changes made to a resource, and AWS CloudTrail provides information about who made those changes. These capabilities enable customers to discover any misconfigurations, fix them, and protect their workloads from failures.

**Basic and Developer support plans provide access to only 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security**. Business and Enterprise level Support Plans provide access to a full set of Trusted Advisor checks.

AWS recommend Business Support if you have production workloads on AWS and want 24x7 access to technical support and architectural guidance in the context of your specific use-cases.

In addition to what is available with Basic Support, Business Support provides:

1- AWS Trusted Advisor - Access to the full set of Trusted Advisor checks and guidance to provision your resources following best practices to help reduce costs, increase performance and fault tolerance, and improve security.

2- AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted. Also includes the Health API for integration with your existing management systems.

3- Enhanced Technical Support – 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.

Response times are as follows:

- General Guidance - < 24 hours

- System Impaired - < 12 hours

- Production System Impaired - < 4 hours

- Production System Down - < 1 hour

4- Architecture Support – Contextual guidance on how services fit together to meet your specific use-case, workload, or application.

5- AWS Support API - Programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

6- Third-Party Software Support - Guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

7- Access to Proactive Support Programs – Ability to purchase Infrastructure Event Management for an additional fee. This provides Architecture and scaling guidance, and real-time operational support during the preparation and execution of planned events, product launches, and migrations.

**The AWS free security resources** include the

* AWS Security Blog,
* Whitepapers,
* Developer Documents,
* Articles and Tutorials,
* Training,
* Security Bulletins,
* Compliance Resources and
* Testimonials.

With **Federation**, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.

**Federation** is an AWS feature that enables users to access and use AWS resources using their existing corporate credentials.

**AWS offers multiple options for federating your identities in AWS:**

**1- AWS Identity and Access Management (IAM):** You can use AWS Identity and Access Management (IAM) to enable users to sign in to their AWS accounts with their existing corporate credentials.

**2- AWS Directory Service:**AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS Command Line Interface (CLI), and Windows applications running on AWS using their existing corporate Microsoft Active Directory credentials.

**3- AWS Single-Sign-On (AWS SSO) Service:**You can use the AWS SSO service to federate your identities into your AWS environment.

**The AWS Acceptable Use Policy** describes prohibited uses of the web services offered by AWS. For example, any activities that are illegal, that violate the rights of others, or that may be harmful to others are prohibited. If a customer violates the policy or authorizes or helps others to do so, AWS may suspend or terminate their use of the services.

  Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of **tags**. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria.

**To view your AWS bill,** open the “Bills” pane of the **Billing and Cost Management console**, and then choose the month you want to view from the drop-down menu.

**What is the maximum amount of data that can be stored in S3 in a single AWS account?**

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

   If your database’s schema cannot be denormalized, and **your application requires joins or complex transactions,** consider using a relational database such as Amazon RDS.

**What are the services that AWS provides to protect against network and application layer DDoS attacks?**

**Amazon CloudFront, AWS Shield, AWS Web Application Firewall (WAF), and Amazon Route 53** work seamlessly together to create a flexible, layered security perimeter against multiple types of attacks including network and application layer DDoS attacks. These services are co-resident at the AWS edge location and provide a scalable, reliable, and high-performance security perimeter for your applications and content.

Additional information:

**AWS Shield** provides always-on DDoS 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. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

**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.

**How does AWS help customers achieve compliance in the cloud?**

       AWS environments are continuously audited, and its infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries, including PCI DSS, ISO 2700, ISO 9001, and HIPAA. You can use these certifications to validate the implementation and effectiveness of AWS security controls. For example, AWS companies that use AWS products and services to handle credit card information can rely on AWS technology infrastructure as they manage their PCI DSS compliance certification.

**What is the recommended storage option when hosting an often-changing database on an Amazon EC2 instance?**

**Amazon EBS** provides durable, block-level storage volumes that you can attach to a running EC2 instance. **You can use Amazon EBS as a primary storage device for data that requires frequent and granular updates**. Amazon EBS is the recommended **storage option when you run a database on an EC2 instance.**

**Durability** refers to the ability of a system to assure data is stored and data remains consistent in the system as long as it is not changed by legitimate access. This means that data should not become corrupted or disappear due to a system malfunction.

         Durability is used to measure the likelihood of data loss. For example, assume you have confidential data stored in your Laptop. If you make a copy of it and store it in a secure place, you have just improved the durability of that data. It is much less likely that all copies will be simultaneously destroyed.

        Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component. The replication of data makes EBS volumes 20 times more durable than typical commodity disk drives, which fail with an AFR (annual failure rate) of around 4%. For example, if you have 1,000 EBS volumes running for 1 year, you should expect 1 to 2 will have a failure.

**Traceability** is related to the tracking of changes made throughout a system.

**Security Groups and NACLs** are the two parts of the VPC Security Layer. Security Groups are a firewall at the instance layer, and NACLs are a firewall at the subnet layer.

**Amazon Lightsail** is designed to be the easiest way to launch and manage a virtual private server (VPS) with AWS. Lightsail plans include everything you need to jumpstart your project –a virtual machine, SSD-based storage, data transfer, DNS management, and a static IPaddress–for a low, predictable price.

**What is the main benefit of attaching security groups to an Amazon RDS instance?**

In Amazon RDS, security groups are used to control which IP address ranges can connect to your databases on a DB instance. When you initially create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.

**AWS File Transfer Acceleration** is an S3 feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.

**AWS Application Discovery Service** is used to discover on-premises server inventory and behavior. This service is very useful when creating a migration plan to AWS.

**AWS Database Migration Service** is used to migrate your data to and from most of the widely used commercial and open source databases.

**Which of the following compute resources are serverless?**

* **AWS Fargate**
* **AWS Lambda**

**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.

**What is the most cost-effective storage option that provides immediate retrieval of your backups? Amazon S3**

**Which of the following would you use to manage your encryption keys in the AWS Cloud? AWS KMS and CloudHSM**

**Which of the following is a feature of Amazon RDS that performs automatic failover when the primary database fails to respond? RDS Multi-AZ**

Amazon RDS can be configured to use **Read Replicas** to scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

**Which of the following S3 storage classes is most appropriate to host static assets for a popular e-commerce website with stable access patterns?**

S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

**AWS Virtual Private Network (AWS VPN)** provides an **internet-based connection** that enables customers to connect their on-premises network or branch office site to AWS. Internet-based connectivity can have **unpredictable performance** and despite being encrypted, can present security concerns.

VPN Connections can be configured in **minutes** and are a good solution if customers have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

**Amazon Relational Database Service (Amazon RDS)** is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including **Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.**

**There are three types of EC2 Reserved Instances(RIs) that you can choose from based on your applications needs:**

**1- Standard RIs:** These provide **the most significant discount** (up to 75% off On-Demand) and are best suited for **steady-state usage.**

**2- Convertible RIs:** These provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. Like Standard RIs, Convertible RIs are best suited for steady-state usage.

**3- Scheduled RIs:** These are available to launch within the time windows you reserve. This option allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month.

**A policy** is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied.

**Each policy consists of:**

**1- Principal:**

Who needs access.

**2- Action:**

What action to allow or deny.

**3- Resource:**

Which resource to allow or deny the action on.

**4- Effect:**

What will be the effect when the user requests access - either allow or deny.

**5- Condition:**

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 relation to Amazon RDS databases:**

**AWS is responsible for:**

1- Managing the underlying infrastructure and foundation services.

2- Managing the operating system.

3- Database setup.

4- Patching and backups.

**The customer is still responsible for:**

1- Protecting the data stored in databases (through encryption and IAM access control).

2- Managing the database settings that are specific to the application.

3- Building the relational schema.

4- Network traffic protection.

Services like **AWS Config, Amazon Inspector, and AWS Trusted Advisor**continually monitor for compliance or vulnerabilities in your AWS environment which gives you a clear overview of which resources are in compliance, and which are not. With AWS Config rules you can also see if a component was out of compliance even for a brief period of time in the past, making both point-in-time and period-in-time audits very effective.

**Amazon MQ** is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud.

**An organization uses a hybrid cloud architecture to run their business. Which AWS service enables them to deploy their applications to any AWS or on-premises server? AWS CodeDeploy**

**AWS CodeDeploy** is a service that automates application deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.

             You can also use **AWS OpsWorks** to automate application deployments to any instance, including Amazon EC2 instances and instances running on-premises. OpsWorks is a service that helps you automate operational tasks like code deployment, software configurations, package installations, database setups, and server scaling using Chef and Puppet.

**Amazon Athena** is an **analytics** service that makes it easy **to query data in Amazon S3** using standard SQL commands.

**Amazon Kinesis** is an **analytics** service that allows you to easily **collect, process, and analyze video and data streams in real time.**

**Amazon QuickSight** is a very fast, easy-to-use, cloud-powered business **analytics** service that makes it easy for all employees within an organization **to build visualizations, perform ad-hoc analysis, and quickly get business insights from their data, anytime, on any device.**

**Economies of scale: It means that AWS will continuously lower costs as it grows.**

**Elastic Load Balancing (ELB)** is used to distribute traffic automatically across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

**Amazon Elastic Container Service** is used to run containerized applications in AWS.

**AWS Data Pipeline** is a **web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals.** AWS Data Pipeline helps you easily create complex data processing workloads that are fault tolerant, repeatable, and highly available. With AWS Data Pipeline, you can regularly access your data where it’s stored, transform and process it at scale, and efficiently transfer the results to AWS services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR.

**Which service can you use to route traffic to the endpoint that provides the best application performance for your users worldwide? AWS Global Accelerator**

**With the Server-based Architectures, compute resources continue to run all the time but with serverless architecture, compute resources are only used when code is being executed.**

Serverless architectures can reduce costs because you do not have to manage or pay for underutilized servers, or provision redundant infrastructure to implement high availability. For example, you can upload your code to the AWS Lambda compute service, and the service can run the code on your behalf using AWS infrastructure. With AWS Lambda, you are charged for every 100ms your code executes and the number of times your code is triggered.

**Amazon RDS** is a fully-managed relational database service. It is a highly available and highly consistent **database that supports ACID transactions.**

**Server-based services include**: Amazon EC2, Amazon RDS, Amazon Redshift and Amazon EMR.

**AWS Serverless Services include:**

**Compute:** AWS Lambda, AWS Fargate

**Messaging:**Amazon SNS, Amazon SQS

**Database:**Amazon DynamoDB**,**Amazon Aurora Serverless

**Orchestration:**AWS Step Functions

AWS doesn't charge usage for a stopped instance, or data transfer fees. For a stopped instance AWS will only charge you for EBS storage volumes attached to the instances.

**Which of the following services allows you to install and run custom relational database software?**

        If an AWS customer needs full control over a database, AWS provides a wide range of Amazon EC2 instances - with different hardware characteristics - on which they can install and run their custom relational database software.

        If **EC2** is used instead of RDS to run a relational database, the customer is responsible for managing everything related to this database.

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

**An Amazon EBS volume is a durable, block-level storage device that can be attached to a single EC2 instance.** You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for database software.

**AWS Identity and Access Management (IAM)** is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to access and use AWS resources.

**Amazon EBS pricing has two factors:**

**1- Volumes:** Volume storage for all EBS volume types is charged by the amount of GB you provision per month, until you release the storage.

**2- Snapshots:** 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 based on the volume of data transferred across regions. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. For each incremental snapshot, only the changed part of your Amazon EBS volume is saved. After the snapshot is copied, standard EBS snapshot charges apply for storage in the destination region.

**S3 pricing is based on four factors:**

1) Total amount of data (in GB) stored on S3

2) Storage class (S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access, S3 One Zone-IA, S3 Glacier, or S3 Glacier Deep Archive)

3) Amount of data transferred out of AWS from S3

4) Number of requests to S3

**AWS CloudFormation** **allows customers to create a template that programmatically defines policies and configurations of all AWS resources as code and so that the same template can be reused among multiple projects**

**DynamoDB global tables** are ideal for massively scaled applications with globally dispersed users. Global tables provide automatic replication to AWS Regions world-wide. They enable you to deliver low-latency data access to your users no matter where they are located. It **is the name of the DynamoDB replication capability that provides fast read \ write performance for globally deployed applications.**

**DynamoDB Accelerator (DynamoDB DAX)** is an in-memory cache for DynamoDB that reduces response times from milliseconds to microseconds.

**DynamoDB point-in-time recovery (PITR)** is used to back up your data with per-second granularity and restore to any single second from the time it was enabled up to the prior 35 days. DynamoDB PITR works as additional insurance against accidental loss of data.

**Use code to provision and operate your AWS infrastructure will help you eliminate human error and automate the process of creating and updating your AWS environment.**

**AWS supports several MFA device options including** **Virtual MFA devices, Universal 2nd Factor**(**U2F) security key, and Hardware MFA devices.**

**Access keys** are long-term credentials for an IAM user or the AWS account root user. Customers can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

**The AWS Key pair** cryptography enables customers to securely access their Amazon EC2 instances using a private key instead of a password.

**What is the AWS Support feature that allows customers to manage support cases programmatically?**

The AWS Support API provides programmatic access to AWS Support Center features to create, manage, and close support cases, and operationally manage Trusted Advisor check requests and status. AWS Support API is available only for AWS  customers who have a **Business or Enterprise** support plan.

The service currently provides two different groups of operations:

1- Support Case Management operations to manage the entire life cycle of AWS support cases, from creating a case to resolving it.

2- Trusted Advisor operations to access the checks provided by AWS Trusted Advisor.

Included with the Enterprise support plan, **Operations Support** provides consultative reviews of your AWS operations and advice for optimization.

**The customer is responsible for protecting their data in the following ways:**

1- Data encryption (at rest and in transit)

2- Setting up access control

3- Monitoring user activity

4- Applying MFA

5- Using advanced managed security services such as Amazon Macie.

**When you begin to estimate the cost of using Amazon EC2, consider the following:**

1- Clock hours of server time: The amount of time that the instances will be running has a direct bearing on the overall price, as EC2 instances are charged either by the hour or by the second, depending on which AMI is used.

2- Instance type: Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity.

3- Pricing model: On-Demand, Reserved, Spot and Dedicated

4- Number of instances: You can provision multiple instances of your Amazon EC2 and Amazon EBS resources to handle peak loads.

5- Load balancing: The number of hours the Elastic Load Balancer runs and the amount of data it processes contribute to the EC2 monthly cost.

6- Elastic IP addresses: You can have one Elastic IP (EIP) address associated with a running instance at no charge. Additional Elastic IPs are not free.

7- Operating systems and software packages: Operating system prices are included in instance prices, unless you choose to bring your own licenses.

**Which of the following factors should be considered when determining the region in which AWS Resources will be deployed?**

Per AWS Best Practices,

* **proximity to your end users,**
* **regulatory compliance,**
* **data residency constraints(Data Sovereignty), and**
* **cost** are **all factors you have to consider when choosing the most suitable AWS Region.**

**AWS IAM and Elastic Beanstalk is FREE.**

**Amazon SQS can be used to decouple the components of the application.**

**Running EC2 instances in parallel is best suited for processing a large number of binary files.**

**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:**

1- Change your AWS root account password and the passwords of any IAM users.

2- Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.

3- Delete any potentially compromised IAM users.

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

5- Respond to any notifications you received from AWS Support through the AWS Support Center.

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

**Amazon Chime** is a communications service for online meetings.

**AWS CloudFormation** allows you to use programming languages or a simple text file (template) to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

**AWS Elastic Beanstalk** is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

**Which of the following are examples of the customer’s responsibility to implement “security IN the cloud”?**

Security **IN** the Cloud” refers to the Customer’s responsibility in the Shared Responsibility Model. Customers are responsible for items such as building application schema, monitoring server and application performance, configuring security groups and network ACLs, and encrypting their data.

          “Security **OF** the Cloud” refers to the AWS’ responsibility in the Shared Responsibility Model. AWS is responsible for items such as the physical security of the DC (data center), creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

NOTE:

For "Patch Management",  AWS is responsible for patching the underlying hosts and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

**Amazon Cognito** lets customers add user sign-up, sign-in, and access control to their web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

**Availability Zones within a Region are connected over low-latency links in order to make synchronous replication of your data possible.**

**The AWS Well-Architected Tool** helps customers review the state of their workloads and compares them to the latest AWS architectural best practices. The tool is based on the [AWS Well-Architected Framework](https://aws.amazon.com/architecture/well-architected/), developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure.

**Customers can work with AWS Identity and Access Management in any of the following ways:**

**1- AWS Management Console:** The console is a browser-based interface that can be used to manage IAM and AWS resources.

**2- AWS Command Line Tools:**  Customers can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks. Using the command line can be faster and more convenient than the console. The command line tools are also useful if you want to build scripts that perform AWS tasks.  AWS provides two sets of command line tools: **the AWS Command Line Interface (AWS CLI) and the AWS Tools for Windows PowerShell.**

**3- AWS SDKs:**  AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically.

**Amazon EC2 Auto Scaling offers the following benefits:**

1. Better fault tolerance.
2. Better availability
3. Better cost management

**AWS WAF** is a web application firewall that **lets customers monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer**. AWS WAF also lets customers control access to their content by defining customizable web security rules.

**Amazon RDS READ REPLICAS feature facilitates offloading of database read activity.**  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.

**The automated backup feature of Amazon RDS** enables point-in-time recovery for your database instance. This allows you to restore your database instance to any second during the retention period.

Additional information: You can also use the RDS Snapshots feature to manually back up your DB instances.

**Multi-AZ Deployments** are used to increase the fault tolerance of your application by automatically failing over to the standby DB instance which located in a separate AZ within the same region.

**Database snapshots** are user-initiated backups of your RDS instance stored in Amazon S3 that are kept until you explicitly delete them.

**AWS Data Pipeline** is a web service that helps customers reliably process and move data between different AWS compute and storage services, as well as on-premises data sources.

 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 permissions.

**AWS Application Load Balancer (ALB)** is part of the AWS Elastic Load Balancing family that is specifically designed to handle HTTP and HTTPS traffic. An ALB automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. Once you register the Amazon EC2 instances with the ALB, it automatically distributes the incoming traffic across those instances. The Load Balancer also performs health checks on the instances and routes traffic only to the healthy ones.

**A transit Virtual Private Cloud (VPC)** is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center. Transit VPCs help organizations transfer data from one Amazon VPC to another, simplifying operations and eliminating the latency issues by peering between resources.

**AWS-managed databases** are a database as a service offering from AWS where AWS manages the underlying hardware, storage, networking, backups, and patching. Users of AWS-managed databases simply connect to the database endpoint, and do not have to concern themselves with any aspects of managing the database. **Examples of AWS-managed databases include:**

**-Amazon RDS ( Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server),**

**- Amazon DocumentDB,**

**- Amazon Redshift, and**

**- Amazon DynamoDB.**

**Fault Tolerance -** A system that is designed to be fault tolerant can recover gracefully from EC2 instance failures. Amazon Web Services gives customers access to a vast amount of IT infrastructure–compute, storage, and communications–that they can allocate automatically (or nearly automatically) to account for almost any kind of failure.

**The principle of least privilege** means granting users the required permissions to perform the tasks entrusted to them and nothing more.

**A pilot light** scenario is a disaster recover / business continuity scenario wherein a minimal amount of services are kept running in a failover location to enable the business to meet their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the event of a disaster. By nature, a pilot light scenario will take some time to spin up and promote to production (as opposed to an active-active DR scenario) and will therefore not mitigate the per-minute losses that will be experienced by the company in the event of an outage.

Additional information: Recovery time objective (RTO) and recovery point objective (RPO) are two key metrics to consider when developing a disaster recover (DR) plan. RTO represents how many hours it takes customers to return to a working state after a disaster. RPO, which is also expressed in hours, represents how much data customers could lose when a disaster happens. For example, an RPO of 1 hour means that customers could lose up to 1 hour’s worth of data when a disaster occurs.

**Multi-threading** is the ability of a central processing unit (CPU) to provide multiple threads of execution concurrently, which may lead to faster overall execution. Amazon EC2 instances support multi-threading, For example, an m5.xlarge instance type has two CPU cores and two threads per core by default—four threads in total. While multi-threading leads to maximum utilization of the CPU and improves the overall perfomance of EC2 instances, multi-threading has nothing to do with recovering EC2 instances from failures.

**Enterprise Support Plan gives customers access to a ‘Well-Architected Review’ for business critical workloads.**

 You can use either the **AWS IAM console or the AWS CLI** to enable a virtual MFA device for an IAM user in your account.

Free AWS services include: AECIAOC

* Amazon VPC.
* Elastic Beanstalk (but not the resources created).
* CloudFormation (but not the resources created).
* Identity Access Management (IAM).
* Auto Scaling (but not the resources created).
* OpsWorks.
* Consolidated Billing.

Amazon Workspaces is incorrect. This service is used for running managed desktops in the cloud.

**reducing application latency and increasing performance for end users**

* **Amazon ElastiCache**
* **Amazon CloudFront**

S3 Event Notifications is a feature that notifies you when certain events happen in your S3 bucket.

Amazon CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files.

Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech-to-text capability to their applications.

Comprehend identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech; and automatically organizes a collection of text files by topic.

AWS Artifact is a resource for compliance-related information. It provides on-demand access to AWS’ security and compliance reports and select online agreements.

**Connect the AWS Cloud and on-premises resources**

An AWS Managed VPN is a virtual private network connection over the public Internet. This creates an encrypted link between the on-premises network and your AWS VPC. Another way to achieve this outcome is to provision an AWS Direct Connection which connects on-premises networks to AWS using private network links.

AWS Managed Services is a managed service for lowering operational overhead and risk.

Amazon Elastic File System allows you to connect hundreds or thousands of EC2 instances concurrently and is accessed using the file-level NFS protocol.

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed.

Amazon S3 Standard provides higher durability and availability but costs more.

Amazon S3 Glacier Deep Archive is used for archiving so data cannot be immediately accessed.

Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud. Amazon SNS is used for building and integrating loosely-coupled, distributed applications.

Amazon Elastic Block Storage (EBS) provides storage volumes for EC2 instances.

Amazon Elastic File System (EFS) provides an NFS filesystem for usage by EC2 instances.

Amazon Relational Database Service (RDS) provides a managed relational database service.

AWS allows customers to assign metadata to their AWS resources in the form of *tags*. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. AWS Cost Explorer and detailed billing reports support the ability to break down AWS costs by tag.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users).

Amazon EC2 is used for running operating systems instances in the cloud.

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS filesystems are mounted using the NFS protocol (which is a file-level protocol).

Access to EFS file systems from on-premises servers can be enabled via **Direct Connect or AWS VPN.**

You mount an EFS file system on your on-premises Linux server using the **standard Linux mount command for mounting a file system** via the **NFSv4.1 or NFSv5 protocol.**

Amazon Elastic Block Storage (EBS) is block-level storage that can only be accessed by EC2 instances from the same AZ as the EBS volume.

Amazon Glacier is an archiving solution that is accessed through S3.

**For maximum redundancy and fault tolerance** the application should be deployed in multiple AWS Regions and multiple Availability Zones within each of those regions. This architecture may use Amazon Elastic Load Balancers and Amazon Route 53 records to direct traffic to instances. Alternatively, it could use AWS Global Accelerator.

**The Amazon Relational Database Service (RDS)** is a managed service where AWS manage administration tasks including hardware provisioning, database setup, patching and backups. The customer is responsible for configuring security groups to control access to the database.

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. With Chef, you use code templates, or cookbooks, to describe the desired configuration of instances or on-premises server.

**asynchronous integration between application components:**

* AWS Step Functions
* Amazon SQS

Amazon EC2 Auto Scaling helps with horizontal scaling of your EC2 instances.

AWS CloudFormation automates the deployment of infrastructure based on templates.

AWS DataSync is used for migrating data from network attached storage (NAS) devices to AWS. It is not used for databases.

**An AWS managed VPN** can be used to quickly connect from an office to an Amazon VPC.

**A Route Table** is part of a VPC and is used to control how traffic is routed within the VPC.

An Internet Gateway is used to connect a public subnet to the Internet.

AWS Direct Connect provides high-bandwidth, low-latency connectivity but takes weeks to months to setup (and is much more expensive).

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.

AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

An EBS volume is a block storage device that is most similar to a virtual hard disk in the cloud as when attached to an instance it appears as a local disk that can have an operating system installed on or be formatted and used for any other local storage purpose.

Amazon Route 53 supports the resolution of public domain names to IP addresses or AWS resources. Amazon Route 53 is a highly available and scalable Domain Name System (DNS) service using hosted zones. It can also be used for domain registration, health checks, and traffic flow.

A hosted zone is a collection of records for a specified domain in Route 53.

AWS Trusted Advisor provides real-time guidance to help customers provision resources following AWS best practices. The service offers guidance for;

* cost optimization,
* performance,
* security,
* fault tolerance,
* service limits.

You may choose a region to reduce latency, minimize costs, or address regulatory requirements.

CloudFormation is used for automated provisioning of infrastructure.

AWS CodeCommit is primarily used for software version control.

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.

**AWS Cloud9** is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions.

CloudFront is a content delivery network (CDN) that allows you to store (cache) your content at “edge locations” located around the world. This allows customers to access content more quickly and provides security against DDoS attacks. CloudFront can be used for data, videos, applications, and APIs.

Benefits include:

– Cache content at Edge Location for fast distribution to customers.

– Built-in Distributed Denial of Service (DDoS) attack protection.

– Integrates with many AWS services (S3, EC2, ELB, Route 53, Lambda).

**Take a snapshot to capture the point-in-time state of the instance** is to take a backup of an Amazon EC2 instance using AWS tools.

Identity and access management (IAM) Policies are documents that define permissions and can be applied to users, groups and roles. IAM policies can be written to grant access to Amazon S3 buckets.

IAM Roles are created and then “assumed” by trusted entities and define a set of permissions for making AWS service requests.

IAM Groups are collections of users and have policies attached to them.

An IAM user is an entity that represents a person or service.

AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. It is considered a PaaS service. However, you do still need to deploy within a VPC so more AWS expertise is required.

**Which AWS service can you use to install a third-party database? Amazon EC2**

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users.

It provides static IP addresses that act as a fixed entry point to application endpoints in a single or multiple AWS Regions, such as Application Load Balancers, Network Load Balancers or EC2 instances.

Uses the AWS global network to optimize the path from users to applications, improving the performance of TCP and UDP traffic.

**Fault tolerance** is a mechanism used for ensuring the availability or recoverability of your application in the of a hardware or software fault.

**Disposable resources** is an architectural principle in which servers and other components are treated as temporary resources and are replaced rather than updated.

**High availability** is a mechanism used for ensuring the availability of your application and protecting against the failure of hardware or software components.

**What AWS services can be used that don’t require you to make any capacity decisions upfront?**

* AWS Lambda
* S3

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

AWS Service Health Dashboard shows the current status of services across regions. However, it does not provide proactive notifications of scheduled activities or guidance of any kind.

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

Amazon CloudWatch dashboard is used for monitoring performance related information for your infrastructure and resources, not the underlying AWS resources.

**A user has limited knowledge of AWS services, but wants to quickly deploy a scalable Node.js application in an Amazon VPC. Which service should be used to deploy the application? AWS Elastic Beanstalk**

Global Services:

* AWS IAM
* AWS Direct Connect
* Amazon Route 53
* Amazon CloudFront
* Amazon WAF & Shield
* Amazon Artifact
* AWS Trusted Advisor
* AWS Personal Health Dashboard

AWS Virtual Private Network solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network.

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS CloudHSM enables you to easily generate and use your own encryption keys on the AWS Cloud.

AWS Secrets Manager enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

KMS is involved with creating and managing encryption keys

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

AWS Trusted Advisor checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

CloudWatch is used for performance monitoring.

VPC Flow Logs are used to capture network traffic information, they will not easily identify unrestricted security groups.

AWS Managed Services manages the daily operations of your AWS infrastructure in alignment with ITIL processes. AWS Managed Services provides a baseline integration with IT Service Management (ITSM) tools such as the ServiceNow platform.

AWS Managed Services provides ongoing **management of your AWS infrastructure so you can focus on your applications**. By implementing best practices to maintain your infrastructure, AWS Managed Services helps to reduce your operational overhead and risk.

AWS Managed Services currently supports the 20+ services most critical for Enterprises, and will continue to expand our list of integrated AWS services.

AWS Managed Services is **designed to meet the needs of Enterprises** that require stringent SLAs, adherence to corporate compliance, and integration with their systems and ITIL®-based processes.

Amazon DynamoDB is fully managed and can be scaled without incurring downtime. DynamoDB scales horizontally and it does so seamlessly.

Both RDS and ElastiCache use EC2 instances and therefore scaling (vertically) requires downtime.

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.

Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. Using Amazon SNS topics, your publisher systems can fan out messages to a large number of subscriber endpoints for parallel processing, including [Amazon SQS](https://aws.amazon.com/sqs/) queues, [AWS Lambda](https://aws.amazon.com/lambda/) functions, and HTTP/S webhooks.

Amazon Simple Workflow Service (Amazon SWF) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services.

Amazon Machine Images (AMI) store configuration information for Amazon EC2 instances.

Amazon Elastic Container Registry (ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images.