

Information for AWS cloud Practitioner Exam

Domain	Percentage of exam
Domain 1: Cloud Concepts	24%
Domain 2: Security and Compliance	30%
Domain 3: Technology	34%
Domain 4: Billing and Pricing	12%
Total	100%

In computing, a **client** can be a web browser or desktop application that a person interacts with to make requests to computer servers. A **server** can be services, such as Amazon Elastic Compute Cloud (Amazon EC2) – a type of virtual server.

The three cloud computing deployment models are -----
-----cloud-based, on-premises, and hybrid.

In a **cloud-based deployment** model, you can migrate existing applications to the cloud, or you can design and build new applications in the cloud. You can build those applications on low-level infrastructure that requires your IT staff to manage them.

On-premises deployment is also known as a *private cloud* deployment. In this model, resources are deployed on premises by using virtualization and resource management tools.

In a **hybrid deployment**, cloud-based resources are connected to on-premises infrastructure. You might want to use this approach in a number of situations. For example, you have legacy applications that are better maintained on premises, or government regulations require your business to keep certain records on premises.

Amazon EC2

Amazon Elastic Compute Cloud (EC2) is a web service that provides resizable compute capacity in the cloud. It allows users to launch virtual servers, known as instances, to run applications. EC2 offers flexibility in choosing instance types, operating systems, storage, and network configurations, making it suitable for a wide range of use cases, from hosting websites to running large-scale computational workloads. It provides features like scalability, on-demand pricing, and integrations with other AWS services to meet diverse computing needs.

Here are the key points about the Amazon EC2 instance types:

1. **General Purpose Instances**

- Balanced compute, memory, and networking resources.
- Suitable for application servers, gaming servers, enterprise backend servers, and small to medium databases.
- Best for workloads with roughly equivalent resource needs and no single resource optimization requirement.

2. **Compute Optimized Instances**

- Ideal for compute-bound applications needing high-performance processors.
- Use cases: high-performance web servers, compute-intensive application servers, dedicated gaming servers, and batch processing workloads.
- Focus on maximizing CPU performance.

3. **Memory Optimized Instances**

- Designed for workloads requiring large datasets processed in memory.
- Use cases: high-performance databases, real-time processing of large datasets, and memory-intensive applications.
- Focus on delivering high memory capacity and performance.

4. **Accelerated Computing Instances**

- Use hardware accelerators (coprocessors) for efficient processing of specific tasks.
- Use cases: graphics processing, game streaming, application streaming, and floating-point calculations.
- Accelerates specialized workloads not suited for standard CPUs.

5. **Storage Optimized Instances**

- Optimized for high sequential read/write access to large datasets.
- Use cases: distributed file systems, data warehousing, and high-frequency OLTP systems.
- Focus on delivering high IOPS for low-latency and high-performance storage needs.

Pricing of EC2 instances

Here are the key points about Amazon EC2 instance purchasing options:

1. On-Demand Instances

- Ideal for short-term, irregular workloads without interruptions.
- Pay for compute time with no upfront costs or contracts.
- Best for unpredictable usage patterns or development and testing.

2. Reserved Instances

- Offers a billing discount for steady-state workloads with a 1-year or 3-year commitment.
- Two types:
 - **Standard Reserved Instances:** Best for fixed needs with capacity reservation in specific Availability Zones.
 - **Convertible Reserved Instances:** Flexible for changes in instance types or zones with lower discounts.
- Requires specification of instance attributes like type, OS, and tenancy.

3. EC2 Instance Savings Plans

- Reduces costs with an hourly spend commitment for a 1-year or 3-year term.
- Provides flexibility across instance families, sizes, and operating systems in a Region.
- Savings up to 72% compared to On-Demand rates, without upfront instance specification.

4. Spot Instances

- Utilizes unused EC2 capacity with savings of up to 90% off On-Demand prices.
- Best for flexible, interruptible workloads like background jobs or data processing.
- Instances can be interrupted if capacity becomes unavailable.

5. Dedicated Hosts

- Physical servers exclusively allocated to you for license compliance and dedicated use.
- Supports On-Demand and Reserved options, but the cost is the highest among EC2 options.

Amazon EC2 Auto Scaling

Scalability involves beginning with only the resources you need and designing your architecture to automatically respond to changing demand by scaling out or in. As a result, you pay for only the resources you use.

Amazon EC2 Auto Scaling enables you to automatically add or remove Amazon EC2 instances in response to changing application demand. By automatically scaling your instances in and out as needed, you can maintain a greater sense of application availability.

Within Amazon EC2 Auto Scaling, you can use two approaches: dynamic scaling and predictive scaling.

- *Dynamic scaling* responds to changing demand.
- *Predictive scaling* automatically schedules the right number of Amazon EC2 instances based on predicted demand.

Key points about **Amazon EC2 Auto Scaling**:

1. Automatic Scaling

- Dynamically adds or removes EC2 instances based on application demand, optimizing resources.

2. Configuration Options

- **Minimum Capacity**: Ensures at least one EC2 instance is always running.
- **Desired Capacity**: The target number of instances to maintain (defaults to minimum capacity if unspecified).
- **Maximum Capacity**: Limits the maximum number of instances to scale out during high demand.

3. Cost Efficiency

- You only pay for the EC2 instances you use, ensuring a scalable yet cost-effective architecture.

Elastic Load Balancing

Key points about **Elastic Load Balancing (ELB)**:

1. Traffic Distribution

- Automatically distributes incoming application traffic across multiple resources, such as Amazon EC2 instances.

2. Single Point of Contact

- Acts as a single entry point for all incoming traffic, routing requests to multiple backend resources to prevent overloading any single instance.

3. Collaboration with Auto Scaling

- Works alongside Amazon EC2 Auto Scaling to maintain high performance and availability by balancing traffic as instances scale in or out.

4. Example Analogy

- Like a coffee shop employee directing customers to the least busy register, ELB evenly distributes workloads across available instances to optimize efficiency.

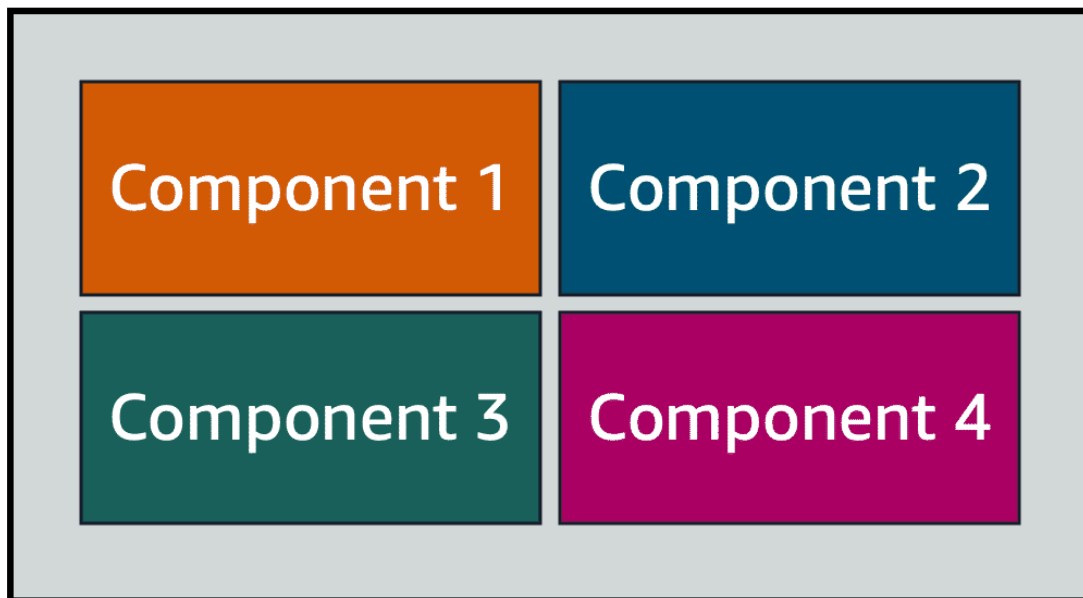
What is Amazon SNS and Amazon SQS

Key points about **Monolithic Applications and Microservices**:

1. Monolithic Applications

- **Tightly coupled components:** Components such as databases, servers, user interfaces, and business logic are closely interconnected.
- **Failure impact:** If one component fails, it can cascade, potentially causing the entire application to fail.

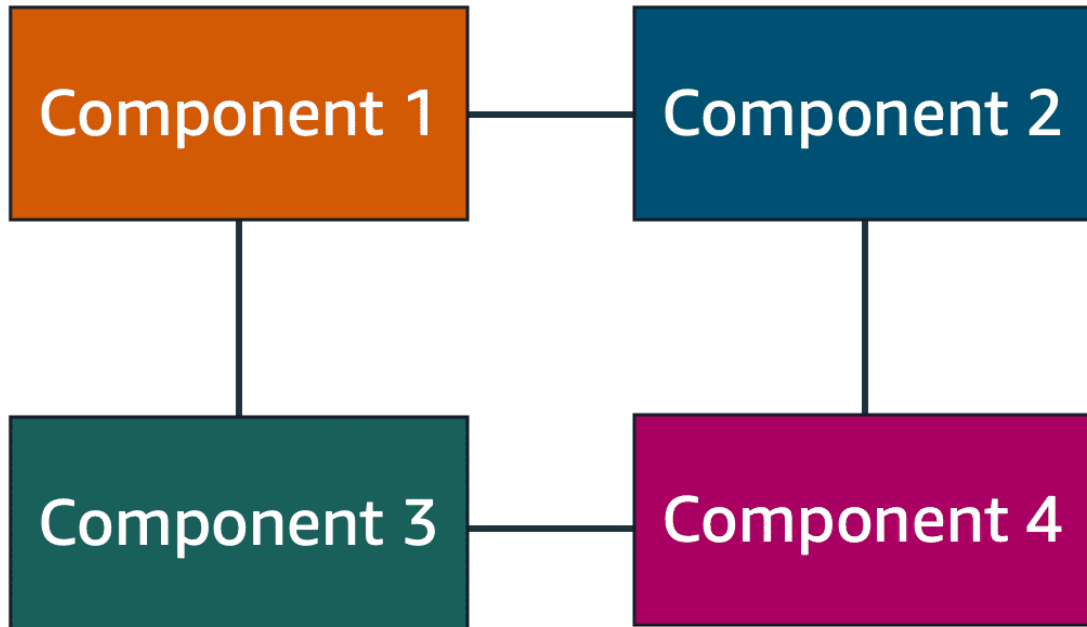
Monolithic application



1. Microservices Architecture

- **Loosely coupled components:** Each component operates independently, communicating with others.
- **Failure tolerance:** If one component fails, the rest of the application can continue functioning, enhancing availability.

Microservices



Microservices on AWS

- **Amazon Simple Notification Service (SNS):** Enables a publish/subscribe model where messages are published to topics and delivered to various subscribers(a publisher publishes messages to subscribers), such as web servers, email addresses, or AWS Lambda functions. This is similar to the coffee shop; the cashier provides coffee orders to the barista who makes the drinks.
- **Amazon Simple Queue Service (SQS):** Used for decoupling application components by queuing messages between services, ensuring smooth communication. **Amazon Simple Queue Service (Amazon SQS)** is a message queuing service. Using Amazon SQS, you can send, store, and receive messages between software components, without losing messages or requiring other services to be available. In Amazon SQS, an application sends

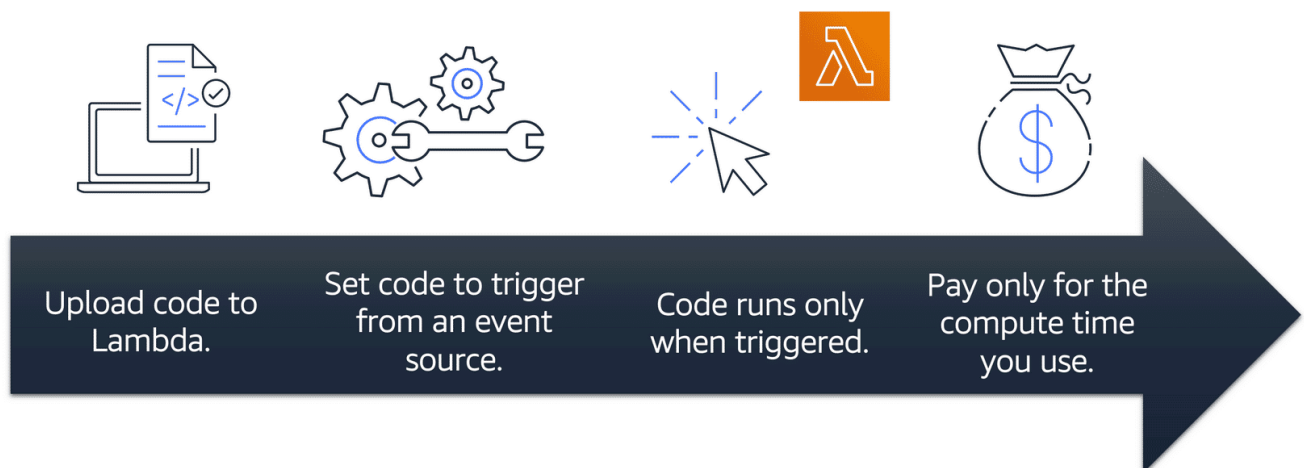
messages into a queue. A user or service retrieves a message from the queue, processes it, and then deletes it from the queue.

Amazon Lambda

[AWS Lambda](#)(opens in a new tab) is a service that lets you run code without needing to provision or manage servers.

While using AWS Lambda, you pay only for the compute time that you consume. Charges apply only when your code is running. You can also run code for virtually any type of application or backend service, all with zero administration.

For example, a simple Lambda function might involve automatically resizing uploaded images to the AWS Cloud. In this case, the function triggers when uploading a new image.



What is containers and container Orchestration

Here are the key points to remember about **containers** and **container orchestration**:

Containers:

1. **Standardized Packaging:** Containers package an application's code, dependencies, and runtime environment into one unit.
2. **Environment Consistency:** Containers ensure the application runs the same way across development, testing, and production environments.
3. **Efficiency:** Containers reduce debugging time by eliminating environmental discrepancies.

Scalability Challenges:

1. Managing a few containers on a single host is manageable manually.
2. At large scales (hundreds or thousands of containers across many hosts), manual management becomes inefficient and error-prone.
3. Critical tasks like monitoring memory usage, security, and logging require automation at scale.

Container Orchestration Services:

1. **Amazon ECS (Elastic Container Service):**
 - Fully managed.
 - Easy integration with other AWS services.
 - Ideal for simpler container orchestration needs.
2. **Amazon EKS (Elastic Kubernetes Service):**
 - Managed Kubernetes service.
 - Offers flexibility and scalability for complex containerized applications.
 - Supports Kubernetes workloads.

Why Use Container Orchestration?

1. Automates container deployment, scaling, and management.
2. Simplifies monitoring and resource allocation at scale.
3. Enhances reliability, security, and scalability for containerized applications.

These points will help you focus on the essentials of containerization and orchestration.

Amazon Elastic Container Service (Amazon ECS)

[Amazon Elastic Container Service \(Amazon ECS\)\(opens in a new tab\)](#) is a highly scalable, high-performance container management system that enables you to run and scale containerized applications on AWS.

Amazon ECS supports Docker containers. [Docker\(opens in a new tab\)](#) is a software platform that enables you to build, test, and deploy applications quickly. AWS supports the use of open-source Docker Community Edition and subscription-based Docker Enterprise Edition. With Amazon ECS, you can use API calls to launch and stop Docker-enabled applications.

Amazon Elastic Kubernetes Service (Amazon EKS)

[Amazon Elastic Kubernetes Service \(Amazon EKS\)](#)(opens in a new tab) is a fully managed service that you can use to run Kubernetes on AWS.

[Kubernetes](#)(opens in a new tab) is open-source software that enables you to deploy and manage containerized applications at scale. A large community of volunteers maintains Kubernetes, and AWS actively works together with the Kubernetes community. As new features and functionalities release for Kubernetes applications, you can easily apply these updates to your applications managed by Amazon EKS.

AWS Fargate

[AWS Fargate](#)(opens in a new tab) is a serverless compute engine for containers. It works with both Amazon ECS and Amazon EKS.

When using AWS Fargate, you do not need to provision or manage servers. AWS Fargate manages your server infrastructure for you. You can focus more on innovating and developing your applications, and you pay only for the resources that are required to run your containers.

Benefits of selecting a Region

- Compliance with data governance and legal requirements
- Proximity to your customers
- Available services within a Region
- Pricing

Availability Zones



An **Availability Zone** is a single data center or a group of data centers within a Region. Availability Zones are located tens of miles apart from each other. This is close enough to have low latency (the time between when content requested and received) between Availability Zones. However, if a disaster occurs in one part of the Region, they are distant enough to reduce the chance that multiple Availability Zones are affected.

A best practice is to run applications across at least two Availability Zones in a Region

Edge locations

An **edge location** is a site that Amazon CloudFront uses to store cached copies of your content closer to your customers for faster delivery.

Amazon CloudFront is a Content Delivery Network (CDN) service that delivers data, videos, applications, and APIs to users globally with low latency. It works by caching content at edge locations worldwide, improving the speed and reliability of content delivery.

AWS Management Console

AWS Management Console is a web-based interface for accessing and managing AWS services. You can quickly access recently used services and search for other services by name, keyword, or acronym. The console includes wizards and automated workflows that can simplify the process of completing tasks.

You can also use the AWS Console mobile application to perform tasks such as monitoring resources, viewing alarms, and accessing billing information. Multiple identities can stay logged into the AWS Console mobile app at the same time.

AWS Command Line Interface

To save time when making API requests, you can use the **AWS Command Line Interface (AWS CLI)**. AWS CLI enables you to control multiple AWS services directly from the command line within one tool. AWS CLI is available for users on Windows, macOS, and Linux.

By using AWS CLI, you can automate the actions that your services and applications perform through scripts. For example, you can use commands to launch an Amazon EC2 instance, connect an Amazon EC2 instance to a specific Auto Scaling group, and more.

AWS Elastic Beanstalk

With **AWS Elastic Beanstalk**, you provide code and configuration settings, and Elastic Beanstalk deploys the resources necessary to perform the following tasks:

- Adjust capacity
- Load balancing
- Automatic scaling
- Application health monitoring

AWS CloudFormation

With **AWS CloudFormation**, you can treat your infrastructure as code. This means that you can build an environment by writing lines of code instead of using the AWS Management Console to individually provision resources.

AWS CloudFormation provisions your resources in a safe, repeatable manner, enabling you to frequently build your infrastructure and applications without having to perform manual actions. It determines the right operations to perform when managing your stack and rolls back changes automatically if it detects errors.

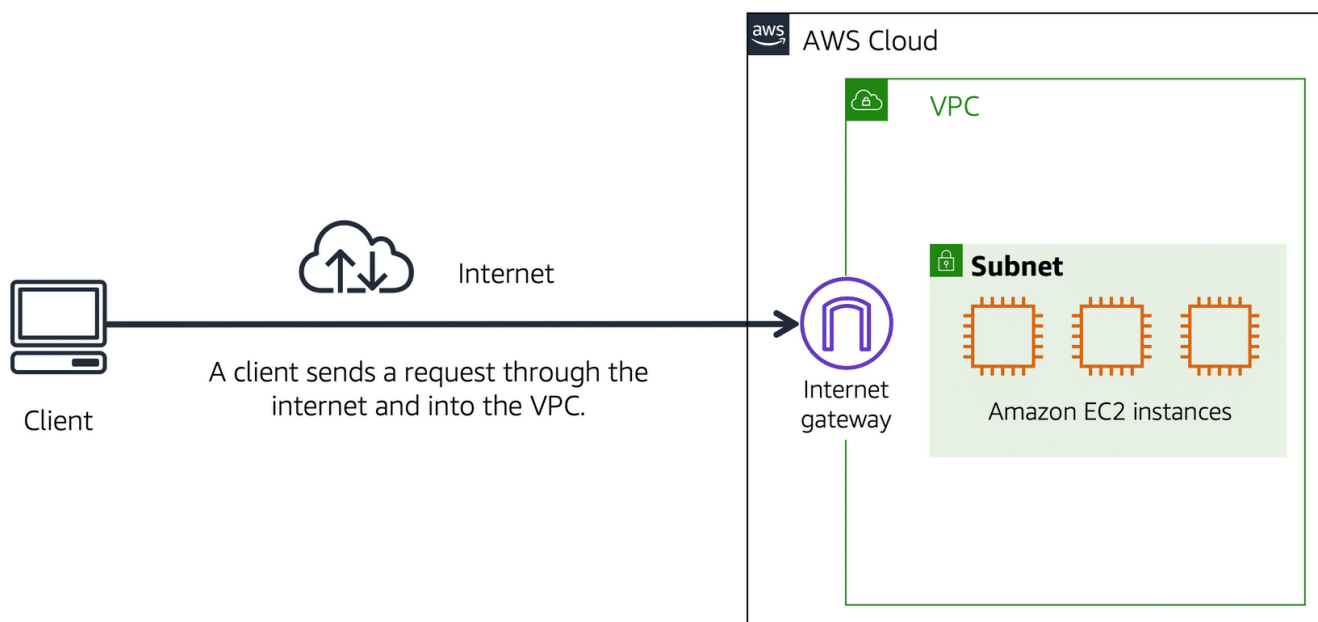
Amazon VPC

A networking service that you can use to establish boundaries around your AWS resources is [Amazon Virtual Private Cloud \(Amazon VPC\)](#)(opens in a new tab).

Amazon VPC enables you to provision an isolated section of the AWS Cloud. In this isolated section, you can launch resources in a virtual network that you define. Within a virtual private cloud (VPC), you can organize your resources into subnets. A **subnet** is a section of a VPC that can contain resources such as Amazon EC2 instances.

Internet gateway

To allow public traffic from the internet to access your VPC, you attach an **internet gateway** to the VPC.



Virtual Private Gateway

Important Points about Virtual Private Gateway:

1. **VPC Access:** Used to access private resources in a Virtual Private Cloud (VPC).
2. **VPN Connection:** Provides a secure VPN connection between a VPC and a private network (e.g., corporate network).

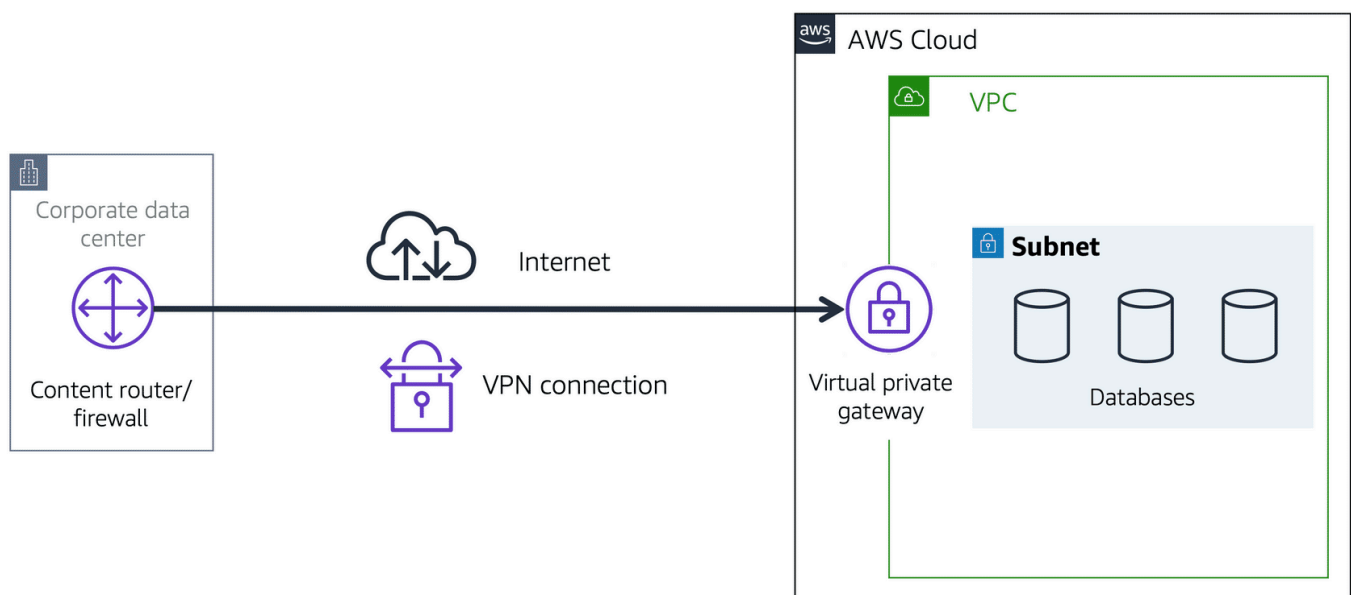
3. **Encryption:** Encrypts traffic to protect data while traveling over the internet.
4. **Traffic Control:** Ensures that only approved network traffic is allowed into the VPC.

Virtual Private Gateway:

A **Virtual Private Gateway (VGW)** is a component that allows secure, encrypted network connections between an AWS VPC and an external network, such as an on-premises data center. It acts as a "gateway" for traffic entering or leaving the VPC via VPN, ensuring data is transmitted securely.

Here's an example of how a virtual private gateway works. You can think of the internet as the road between your home and the coffee shop. Suppose that you are traveling on this road with a bodyguard to protect you. You are still using the same road as other customers, but with an extra layer of protection.

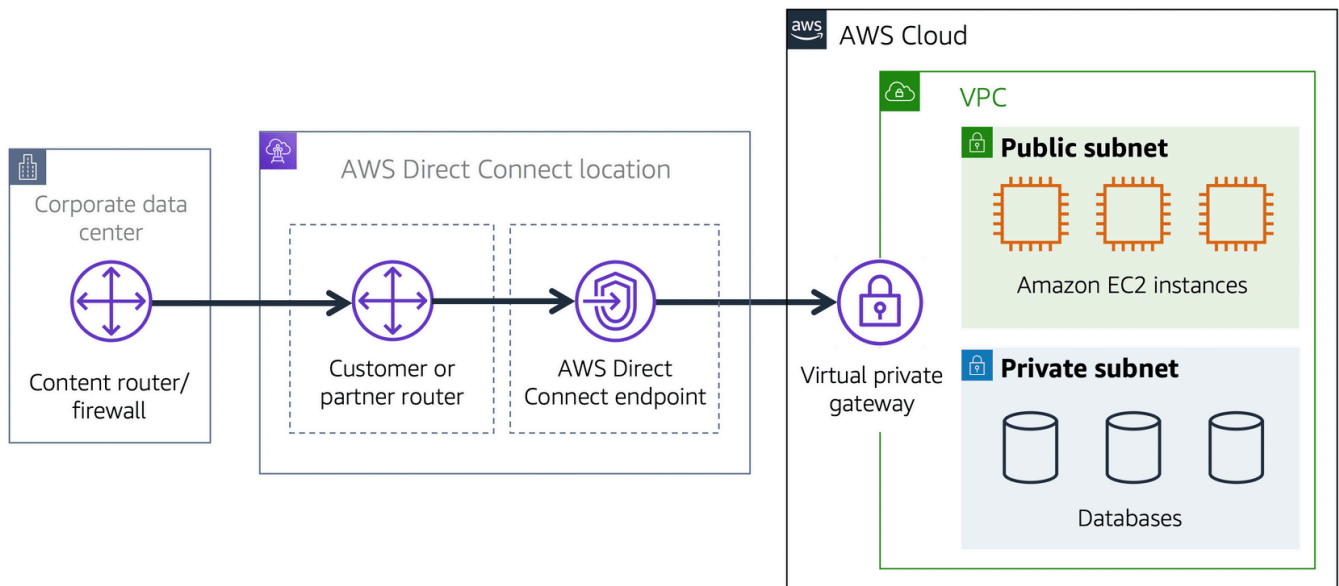
The bodyguard is like a virtual private network (VPN) connection that encrypts (or protects) your internet traffic from all the other requests around it.



AWS Direct Connect

[AWS Direct Connect](#) (opens in a new tab) is a service that lets you to establish a dedicated private connection between your data center and a VPC.

Suppose that there is an apartment building with a hallway directly linking the building to the coffee shop. Only the residents of the apartment building can travel through this hallway.



Thin explanation in points:

1. **VPC as Coffee Shop:** Think of a VPC as the entire coffee shop.
2. **Subnets as Workstations:** Subnets are like separate workstations (cashier and barista) within the coffee shop.
3. **Public and Private Subnets:**
 - Cashier's workstation (public) receives customer orders.
 - Barista's workstation (private) processes orders but cannot directly receive customer orders.
4. **Control Network Flow:** Subnets help control how network traffic flows, allowing certain traffic (like from the cashier) to enter the private area (barista's workstation) but blocking unauthorized access.
5. **Isolation of Resources:** Subnets provide isolation of resources by grouping them based on functionality or security. (In this case divided into groups or workstation of cashier and barista, so that customers don't directly order from barista and order from cashier so we need to isolate barista from the crowd of customers .)

Subnets

A subnet is a section of a VPC in which you can group resources based on security or operational needs. Subnets can be public or private.



Public subnets contain resources that need to be accessible by the public, such as an online store's website.

Private subnets contain resources that should be accessible only through your private network, such as a database that contains customers' personal information and order histories.

In a VPC, subnets can communicate with each other. For example, you might have an application that involves Amazon EC2 instances in a public subnet communicating with databases that are located in a private subnet.

Network traffic in a VPC

When a customer requests data from an application hosted in the AWS Cloud, this request is sent as a packet. **A packet is a unit of data sent over the internet or a network.**

It enters into a VPC through an internet gateway. Before a packet can enter into a subnet or exit from a subnet, it checks for permissions. These permissions indicate who sent the packet and how the packet is trying to communicate with the resources in a subnet.

The VPC component that checks packet permissions for subnets is a [network access control list \(ACL\)](#)(opens in a new tab).

Key Points to Understand About Network ACLs:

1. What is a Network ACL?

- A virtual firewall at the **subnet level** that controls **inbound and outbound traffic**.

2. How Does it Work?

- Similar to a **passport control officer** at an airport, checking and approving traffic (packets) both entering and exiting the subnet.
- Rules can allow or deny specific traffic based on criteria like IP addresses, ports, and protocols.

3. Default Network ACL vs. Custom Network ACL:

- **Default Network ACL:**
 - Allows **all inbound and outbound traffic** by default.
- **Custom Network ACL:**
 - Denies **all traffic by default** until rules are explicitly added.

4. Rule Structure in ACLs:

- **Rules are numbered:** Evaluated in ascending order.
- **Explicit Deny Rule:** If no rule matches the traffic, it's automatically denied.
- Both **allow** and **deny** rules can be configured.

5. Stateless Firewall:

- Network ACLs are stateless, meaning **inbound and outbound rules must be defined separately**. Allowing inbound traffic doesn't automatically allow a response outbound.

6. When to Use Network ACLs:

- Ideal for **controlling traffic at the subnet level** for public-facing or shared environments.
- Provides an **extra layer of security** for traffic in and out of subnets.

Understanding and properly configuring network ACLs ensures secure and efficient traffic flow within your AWS infrastructure.

Key Points About Stateless Packet Filtering:

1. What is Stateless Packet Filtering?

- Network ACLs perform **stateless filtering**, meaning they do not remember previous requests or responses.

2. How Does it Work?

- **Inbound and outbound traffic** is checked independently against the list of rules.
- Each packet is evaluated **without context** of previous packets.

3. Real-World Analogy:

- Similar to a **traveler** entering a country:
 - When sending a request (like traveling to a new country), it is checked.
 - When the response (or return trip) comes back, it is **checked again separately**.

4. Implications of Stateless Filtering:

- Inbound and outbound rules must be explicitly defined **individually** for bidirectional traffic.
- Ensures every packet complies with security rules at the subnet border.

This method ensures **rigorous security checks** for all network traffic, but it requires careful configuration of rules for seamless communication.

Key Points About Security Groups and Stateful Packet Filtering:

1. What is a Security Group?

- A **virtual firewall** that controls **inbound and outbound traffic** for Amazon EC2 instances.
- Operates at the **instance level**.

2. Default Behavior:

- **Inbound traffic:** Denied by default; custom rules must specify allowed traffic.
- **Outbound traffic:** Allowed by default; can be restricted by custom rules.

3. Analogy:

- Think of a **door attendant** in an apartment building:
 - They check a list to allow or deny entry (inbound traffic).
 - Guests leaving (outbound traffic) are not checked again.

4. Stateful Packet Filtering:

- Security groups remember **previous requests** and automatically allow matching responses.
- Example: If an EC2 instance sends a request to the internet, the response packet is automatically allowed, even if there are no inbound rules for it.

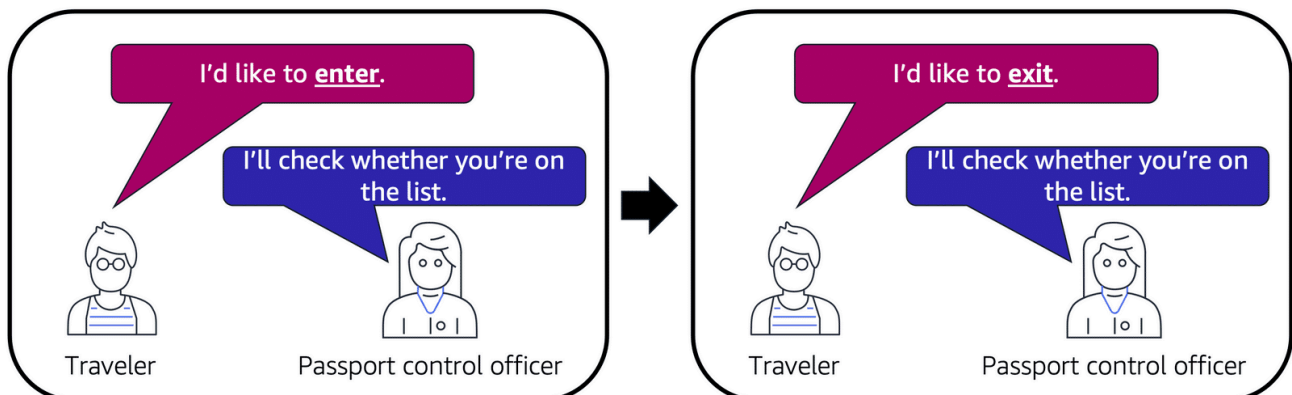
5. Association:

- Multiple EC2 instances can share a **single security group**, or each instance can have its own.

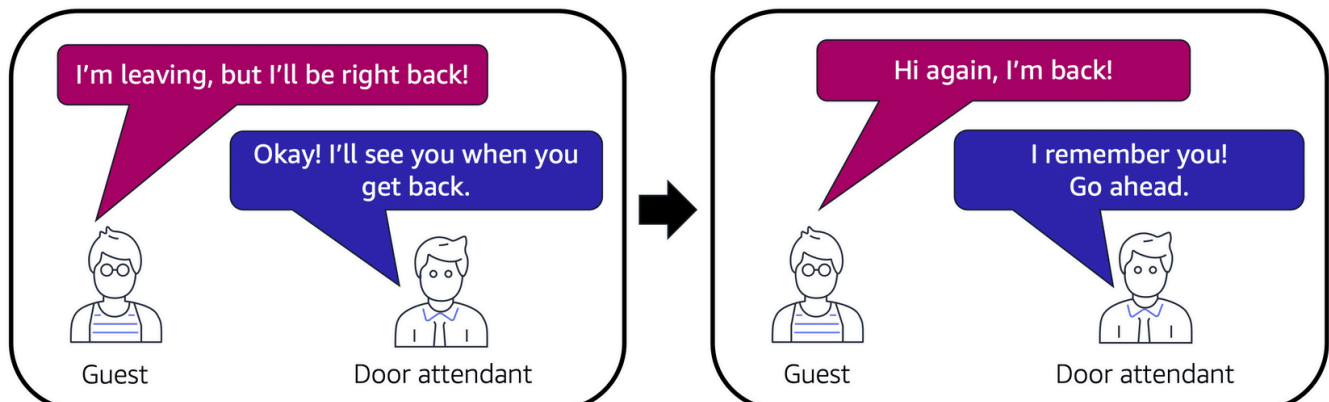
6. Difference from Network ACLs:

- **Security Groups:** Stateful filtering; remembers previous traffic.
- **Network ACLs:** Stateless filtering; checks traffic independently for each direction.

This ensures **fine-grained control** over traffic at the instance level while maintaining efficiency for bidirectional communication.



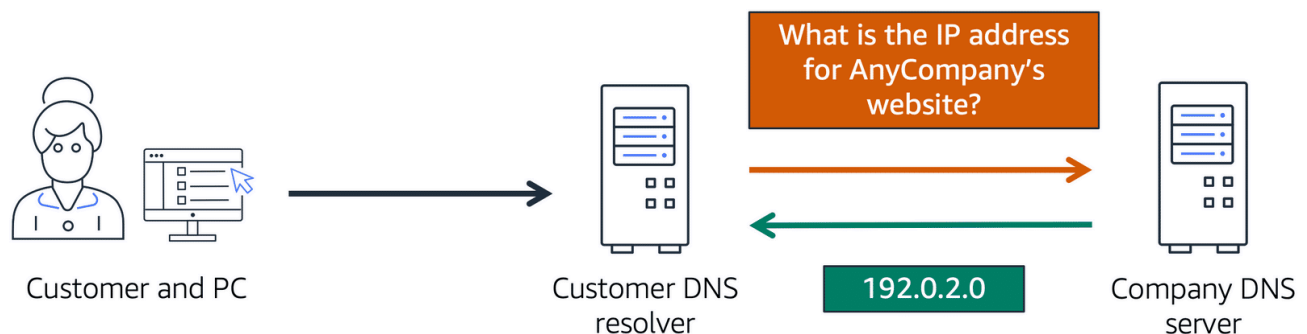
stateless packet filtering



What is a DNS?

A **Domain Name System (DNS)** is a system that translates **domain names** (like `example.com`) into **IP addresses** that computers use to identify each other on the internet. It acts as the "phone book" of the internet, enabling users to access websites by entering a human-readable name instead of a numeric IP address.

For example, when you type a web address into your browser, DNS resolution takes place to find the corresponding IP address so you can access the desired website.



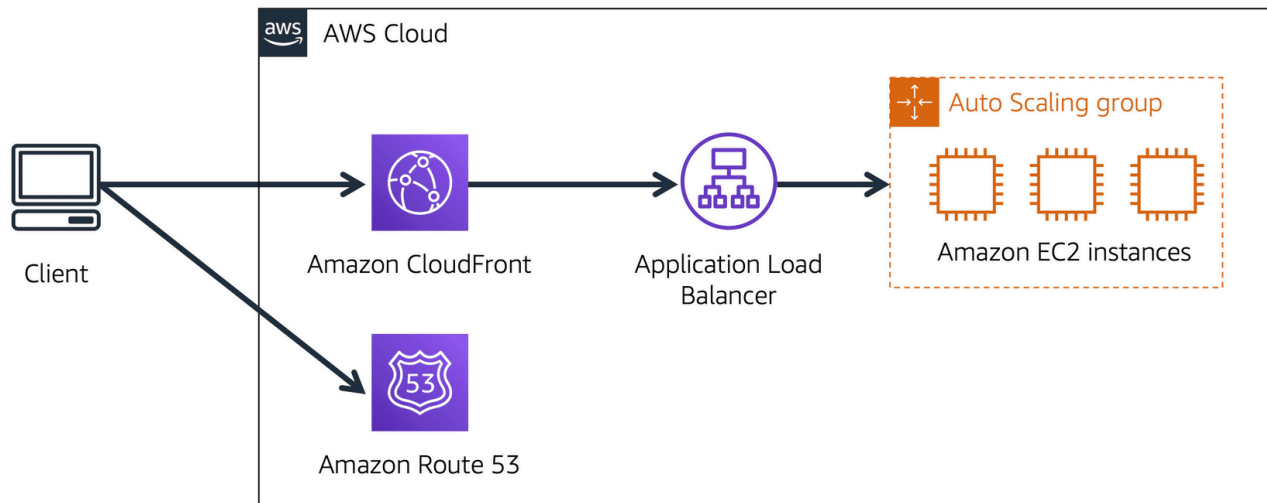
Key Points about Amazon Route 53:

- **What it is:** Amazon Route 53 is a DNS web service that provides a reliable way to route users to applications hosted on AWS or outside AWS.
- **Functions:**
 - Connects user requests to AWS resources like EC2 instances, load balancers, and more.
 - Allows domain name registration and management of DNS records.
 - Supports transferring DNS records from other registrars for centralized management.
- **Integration with Amazon CloudFront:**
 - Works together to deliver content efficiently from the nearest edge location to users.

Example of Route 53 and CloudFront in Action:

1. **User Request:** A customer visits a website like `AnyCompany.com`.
2. **DNS Resolution:** Route 53 resolves the domain to its IP address (e.g., `192.0.2.0`) and sends this information to the customer.

3. **Edge Location Routing:** The customer's request is routed to the nearest edge location using CloudFront.
4. **Content Delivery:** CloudFront connects to the Application Load Balancer, which directs the request to an appropriate EC2 instance in the backend.



Instance stores

Block-level storage volumes behave like physical hard drives.

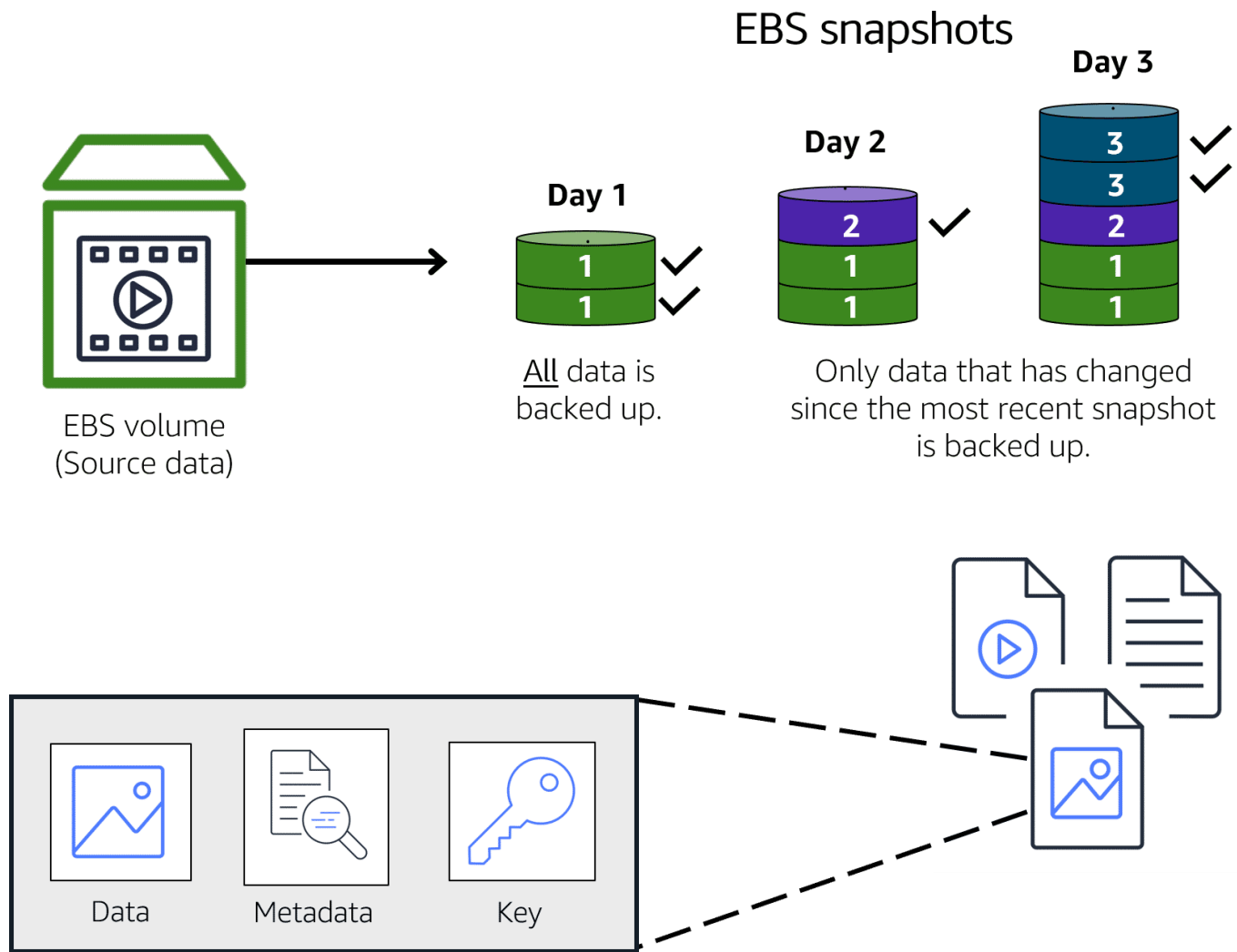
An [instance store](#) provides temporary block-level storage for an Amazon EC2 instance. An instance store is disk storage that is physically attached to the host computer for an EC2 instance, and therefore has the same lifespan as the instance. When the instance is terminated, you lose any data in the instance store.

Amazon Elastic Block Store

[Amazon Elastic Block Store \(Amazon EBS\)](#) is a service that provides block-level storage volumes that you can use with Amazon EC2 instances. If you stop or terminate an Amazon EC2 instance, all the data on the attached EBS volume remains available.

To create an EBS volume, you define the configuration (such as volume size and type) and provision it. After you create an EBS volume, it can attach to an Amazon EC2 instance.

Because EBS volumes are for data that needs to persist, it's important to back up the data. You can take incremental backups of EBS volumes by creating Amazon EBS snapshots.



In **object storage**, each object consists of data, metadata, and a key. The data might be an image, video, text document, or any other type of file. Metadata contains information about what the data is, how it is used, the object size, and so on. An object's key is its unique identifier.

Amazon Simple Storage Service (Amazon S3)

[Amazon Simple Storage Service \(Amazon S3\)](#)[\(opens in a new tab\)](#) is a service that provides object-level storage. Amazon S3 stores data as objects in buckets.

You can upload any type of file to Amazon S3, such as images, videos, text files, and so on. For example, you might use Amazon S3 to store backup files, media files for a website, or archived documents. Amazon S3 offers unlimited storage space. The maximum file size for an object in Amazon S3 is 5 TB.

When you upload a file to Amazon S3, you can set permissions to control visibility and access to it. You can also use the Amazon S3 versioning feature to track changes to your objects over time.

Amazon S3 Storage Classes (Key Points)

1. **S3 Standard:**

- For frequently accessed data.
- Stores data across at least three Availability Zones.
- High availability, suitable for websites, content distribution, and data analytics.

2. **S3 Standard-Infrequent Access (S3 Standard-IA):**

- For infrequently accessed data needing high availability.
- Lower storage price, higher retrieval price.
- Stores data in a minimum of three Availability Zones.

3. **S3 One Zone-Infrequent Access (S3 One Zone-IA):**

- Stores data in a single Availability Zone.
- Lower storage cost than S3 Standard-IA.
- Suitable if data can be easily reproduced during an AZ failure.

4. **S3 Intelligent-Tiering:**

- Automatically moves data between frequent and infrequent tiers based on access patterns.
- Small monitoring fee applies.
- Ideal for data with unpredictable access patterns.

5. **S3 Glacier Instant Retrieval:**

- For archived data requiring immediate access.
- Retrieval within milliseconds.

6. **S3 Glacier Flexible Retrieval:**

- Low-cost archiving for data accessible within 1 minute to 12 hours.
- Suitable for less frequent access, like archived records or media.

7. **S3 Glacier Deep Archive:**

- **Lowest-cost storage for long-term data retention. (Lowest for s3 deep archive)**
- Retrieval takes 12 to 48 hours.
- Ideal for data accessed rarely, e.g., once a year.

8. **S3 Outposts:**

- On-premises storage using AWS Outposts.
- Data stored redundantly across multiple devices.
- Suitable for local data residency requirements and high-performance needs.

Key Points on File Storage and Amazon EFS

1. **File Storage Overview:**

- Multiple clients (e.g., users, applications, servers) access shared file folders.

- A storage server organizes files using block storage with a local file system.
- Clients access data via file paths.

2. **Use Case:**

- Ideal for scenarios where multiple services and resources access the same data concurrently.

3. **Amazon Elastic File System (EFS):**

- A scalable file system for AWS Cloud services and on-premises resources.
- Automatically grows and shrinks as files are added or removed.
- Can scale on demand to petabytes without application disruption.

Difference between amazon EBS and amazon EFS

An Amazon EBS volume stores data in a **single** Availability Zone.

To attach an Amazon EC2 instance to an EBS volume, both the Amazon EC2 instance and the EBS volume must reside within the same Availability Zone.

Amazon EFS is a regional service. It stores data in and across **multiple** Availability Zones.

The duplicate storage enables you to access data concurrently from all the Availability Zones in the Region where a file system is located. Additionally, on-premises servers can access Amazon EFS using AWS Direct Connect.

Key Points on Relational Databases, Amazon RDS and amazon Aurora

1. **Relational Databases:**

- Data is stored in a structured format that relates to other pieces of data.
- Example: A coffee shop's inventory system, where each record has details like product name, size, and price.
- Uses **SQL** to store and query data, providing consistent, scalable storage.
- Allows querying for specific data relationships (e.g., identifying customers with frequent purchases).

2. **Amazon Relational Database Service (Amazon RDS):**

- Managed service for running relational databases in the AWS Cloud.
- Automates tasks like hardware provisioning, setup, patching, and backups.
- Integrates with other AWS services (e.g., AWS Lambda for querying databases in serverless applications).
- Provides **encryption options** for data at rest and in transit.

3. **Amazon RDS Database Engines:**

- Supports multiple database engines optimized for memory, performance, or I/O:
 - **Amazon Aurora**
 - PostgreSQL
 - MySQL
 - MariaDB
 - Oracle Database
 - Microsoft SQL Server

4. **Amazon Aurora:** AWS aurora

- Enterprise-class relational database compatible with MySQL and PostgreSQL.
- **Up to 5 times faster than MySQL** and **3 times faster than PostgreSQL**.
- Reduces **I/O operations** to lower costs while ensuring reliability.
- Supports **high availability** by replicating data across three Availability Zones.
- Continuously **backs up data** to Amazon S3.

Amazon DynamoDB

Key Points on Nonrelational Databases and Amazon DynamoDB

1. **Nonrelational Databases (NoSQL):**

- Data is stored and queried in tables but with structures beyond traditional rows and columns.
- **Key-Value Pairs:** A common structure where data is stored as items (keys) with associated attributes (values).
 - Example: Item 1 could store name, address, and favorite drink, while Item 2 stores name, address, and birthday.
- **Flexibility:** Items can have different attributes, and attributes can be added or removed at any time.

2. **Amazon DynamoDB:**

- A **key-value database service** that offers **single-digit millisecond performance** at any scale.
- **Serverless:** No need to provision, patch, or manage servers. You don't have to install or maintain software.
- **Automatic Scaling:** DynamoDB automatically adjusts capacity as your database size changes while maintaining consistent performance, making it suitable for high-performance, scalable use cases.

Amazon Redshift

[Amazon Redshift](#)(opens in a new tab) is a data warehousing service that you can use for big data analytics. It offers the ability to collect data from many sources and helps you to understand relationships and trends across your data.

AWS Database Migration Service (AWS DMS)

[AWS Database Migration Service \(AWS DMS\)](#)(opens in a new tab) enables you to migrate relational databases, nonrelational databases, and other types of data stores.

With AWS DMS, you move data between a source database and a target database. [The source and target databases](#)(opens in a new tab) can be of the same type or different types. During the migration, your source database remains operational, reducing downtime for any applications that rely on the database.

Other Use Cases for AWS DMS (Database Migration Service)

1. Development and Test Database Migrations:

- Enables developers to test applications against production data without impacting the production environment or users.

2. Database Consolidation:

- Combines multiple databases into a single database, streamlining data management and reducing complexity.

3. Continuous Replication:

- Facilitates sending ongoing copies of your data to other target sources, enabling real-time or near-real-time data replication instead of a one-time migration.

Amazon DocumentDB

[Amazon DocumentDB](#)(opens in a new tab) is a document database service that supports MongoDB workloads. (MongoDB is a document database program.)

Amazon Neptune

[Amazon Neptune](#)(opens in a new tab) is a graph database service.

You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as recommendation engines, fraud detection, and knowledge graphs.

Amazon Quantum Ledger Database (Amazon QLDB)

[Amazon Quantum Ledger Database \(Amazon QLDB\)](#)[\(opens in a new tab\)](#) is a ledger database service.

You can use Amazon QLDB to review a complete history of all the changes that have been made to your application data.

Amazon Managed Blockchain

[Amazon Managed Blockchain](#)[\(opens in a new tab\)](#) is a service that you can use to create and manage blockchain networks with open-source frameworks.

Blockchain is a distributed ledger system that lets multiple parties run transactions and share data without a central authority.

Amazon ElastiCache

[Amazon ElastiCache](#)[\(opens in a new tab\)](#) is a service that adds caching layers on top of your databases to help improve the read times of common requests.

It supports two types of data stores: Redis and Memcached.

Amazon DynamoDB Accelerator

[Amazon DynamoDB Accelerator \(DAX\)](#)[\(opens in a new tab\)](#) is an in-memory cache for DynamoDB.

It helps improve response times from single-digit milliseconds to microseconds.

Security

Here are the key points for the shared responsibility model of security in AWS:

1. Customer Responsibility (Security in the Cloud):

- Customers manage security for everything they create and store in AWS.
- Responsibilities include choosing AWS services, managing access, and securing content.
- Security steps depend on services, system complexity, and operational needs, such as configuring EC2 instances and security groups.

2. AWS Responsibility (Security of the Cloud):

- AWS is responsible for securing the underlying infrastructure of the cloud.
- Responsibilities include physical security of data centers, managing hardware/software infrastructure, and securing network and virtualization layers.
- AWS provides third-party audit reports to verify compliance with security standards.

Customers	Customer Data		
	Platform, Applications, Identity and Access Management		
	Operating Systems, Network and Firewall Configuration		
	Client-side Data Encryption	Server-side Encryption	Networking Traffic Protection

AWS	Software			
	Compute	Storage	Database	Networking
	Hardware/AWS Global Infrastructure			
	Regions	Availability Zones	Edge Locations	

141) Which IT controls do AWS and the customer share, according to the AWS shared responsibility model? (Choose two.)

- A. Physical and environmental controls
- B. Patch management
- C. Cloud awareness and training
- D. Zone security
- E. Application data encryption

Correct Answer: BC

Examples of shared controls include:

- **Patch Management** – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- **Configuration Management** – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- **Awareness & Training** – AWS trains AWS employees, but a customer must train their own employees.

Here is a concise summary of the key points for AWS Identity and Access Management (IAM):

IAM Overview

- **Purpose:** Securely manage access to AWS services and resources.
- **Features:** IAM users, groups, roles, policies, and multi-factor authentication (MFA).

[AWS Identity and Access Management \(IAM\)](#)[\(opens in a new tab\)](#) enables you to manage access to AWS services and resources securely. IAM gives you the flexibility to configure access based on your company's specific operational and security needs.

Key Components

1. Root User:

- Full access to the AWS account.
- **Best Practice:** Use only for specific tasks (e.g., changing email, support plans). Create an IAM user for daily tasks.

2. IAM Users:

- Represents an individual or application with specific credentials.
- **Default:** No permissions; permissions must be explicitly granted.
- **Best Practice:** Create individual users for everyone to enhance security.

3. IAM Policies:

- Documents that define permissions to AWS services/resources.
- **Best Practice:** Follow the **principle of least privilege** by granting only necessary permissions.

4. IAM Groups:

- Collection of IAM users with shared permissions.
- **Best Practice:** Use groups to manage permissions more efficiently (e.g., “Cashiers” or “Inventory Specialists”).

5. IAM Roles:

- Temporary permissions assigned to users, applications, or services.
- **Best Practice:** Use roles for tasks requiring temporary access (e.g., switching roles for different tasks).

6. Multi-Factor Authentication (MFA):

- Adds an extra layer of security by requiring a second verification method (e.g., a code sent to a device).

Best Practices Recap

- Minimize root user usage.
- Assign least privilege permissions.
- Use IAM groups for efficient management.
- Implement MFA for all sensitive operations.
- Use IAM roles for temporary or dynamic access needs.

This concise format ensures you cover all critical IAM information for your exam preparation.

AWS Organizations

AWS Organizations is a service that helps consolidate and manage multiple AWS accounts from a central location. It provides centralized control of account permissions, making it easier to govern access and implement policies across accounts.

Organizational Units (OUs)

Organizational Units (OUs) are logical groupings of AWS accounts within AWS Organizations. They enable the application of policies to groups of accounts with similar business or security requirements. Policies applied to an OU are automatically inherited by all accounts within that unit.

Key Points

- **Centralized Management:** AWS Organizations allows you to manage multiple AWS accounts from a central location.
- **Root:** The root is the parent container for all accounts in an organization.
- **Service Control Policies (SCPs):**
 - SCPs are used to enforce restrictions on AWS services, resources, and API actions for users and roles across accounts.
 - Policies can be applied at the organization, OU, or account level.

Security Control Policies (SCPs)

Security Control Policies (SCPs) are a feature of AWS Organizations that help manage permissions at the account level by defining guardrails for what actions IAM users and roles can perform across member accounts.

Key Points:

- SCPs do not grant permissions but restrict them, overriding even IAM policies.
- Applied at the organizational unit (OU), root, or account level to enforce governance.
- Used to prevent unintended privilege escalation or restrict specific services.
- Do not affect the management account of AWS Organizations.

* ***Organizational Units (OUs):***

- OUs group accounts with similar requirements for easier management.
- Policies applied to OUs automatically cascade to all member accounts.
- Useful for isolating workloads or accounts with specific security or compliance needs.

- **Consolidated Billing:** A feature of AWS Organizations that simplifies cost management by combining bills from multiple accounts into one.
- **Flexibility and Security:** AWS Organizations streamlines account management while enforcing consistent policies across all accounts.

AWS Artifact

[AWS Artifact](#) (opens in a new tab) is a service that provides on-demand access to AWS security and compliance reports and select online agreements. AWS Artifact consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports.



AWS Artifact Agreements

- Enables review, acceptance, and management of agreements for individual accounts or accounts under AWS Organizations.
- Offers agreements tailored to regulatory needs, e.g., HIPAA compliance.

AWS Artifact Reports

- Provides compliance reports from third-party auditors verifying AWS compliance with global, regional, and industry-specific standards.
- Includes access to documents like ISO certifications, PCI reports, and SOC reports.

- Reports are kept up-to-date for use as evidence of AWS security measures during audits.

Customer Compliance Center

The Customer Compliance Center is a resource hub designed to help organizations understand and meet their compliance needs on AWS. It provides educational materials, compliance documentation, and case studies to support regulated industries in addressing governance, audit, and compliance challenges.

Denial-of-service attacks

A **denial-of-service (DoS) attack** is a deliberate attempt to make a website or application unavailable to users.

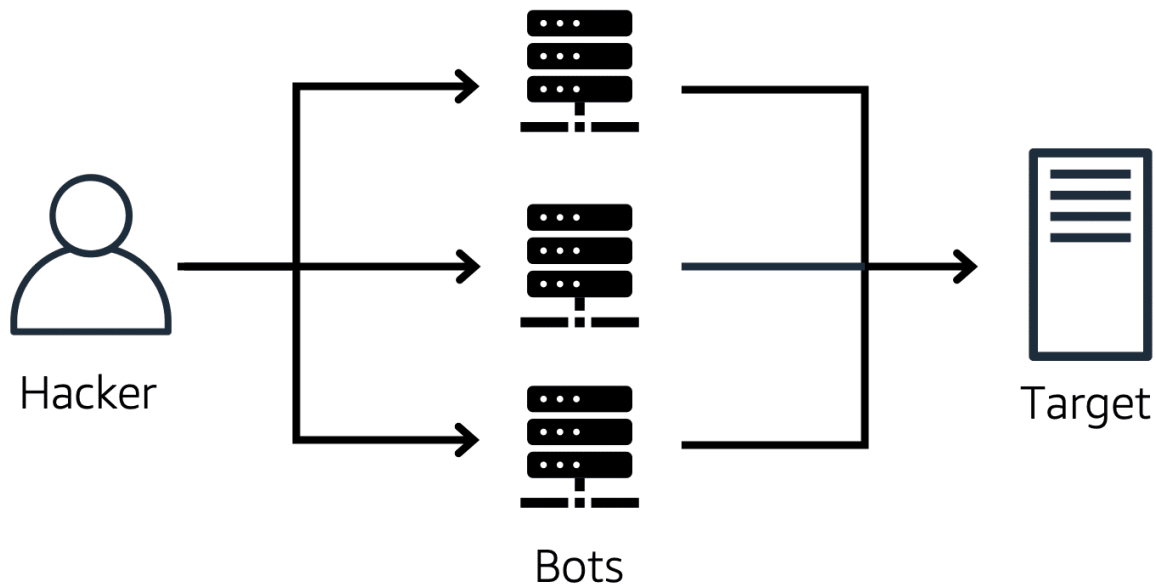


For example, an attacker might flood a website or application with excessive network traffic until the targeted website or application becomes overloaded and is no longer able to respond. If the website or application becomes unavailable, this denies service to users who are trying to make legitimate requests.

Distributed Denial-of-Service (DDoS) Attacks

A Distributed Denial-of-Service (DDoS) attack occurs when a website or application is overwhelmed with excessive traffic from multiple sources, making it unavailable to legitimate users. These attacks can be initiated by multiple attackers or a single attacker using a network of compromised computers (bots).

Distributed denial-of-service attack



The attack originates from **multiple** sources.

AWS Shield

AWS Shield is a service designed to protect applications against Distributed Denial-of-Service (DDoS) attacks. It offers two levels of protection: Shield Standard and Shield Advanced.

AWS Shield Standard

- **Cost:** Free for all AWS customers.
- **Protection:** Protects AWS resources from common and frequently occurring DDoS attacks.
- **Real-Time Detection:** Uses various analysis techniques to detect malicious traffic and automatically mitigates it.

AWS Shield Advanced

- **Cost:** Paid service for advanced protection.
- **Protection:** Offers detailed diagnostics and protection against more sophisticated DDoS attacks.

- **Integration:** Works with Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing.
- **Customization:** Can be integrated with AWS WAF to write custom rules for mitigating complex DDoS attacks.

AWS Key Management Service

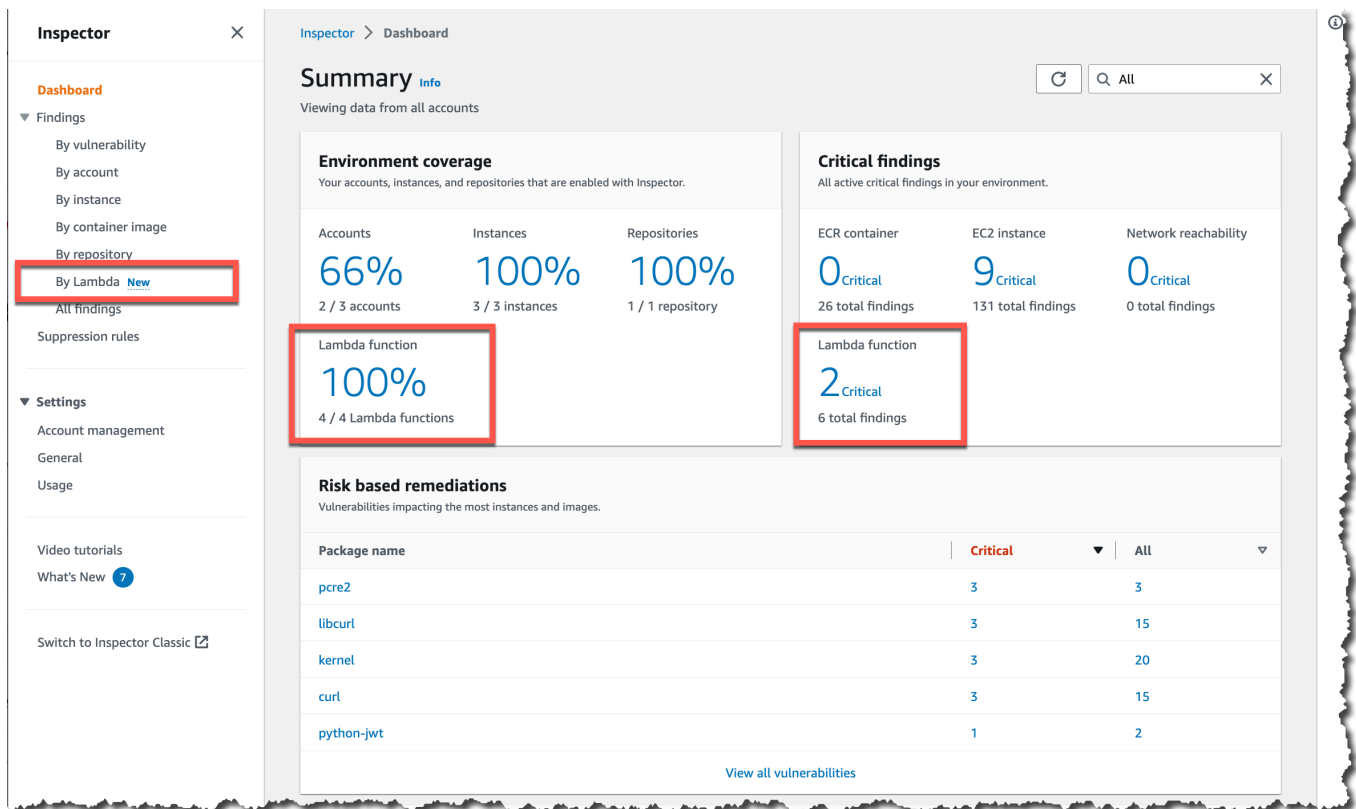
[AWS Key Management Service \(AWS KMS\)](#)[\(opens in a new tab\)](#) enables you to perform encryption operations through the use of **cryptographic keys**. A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data. You can use AWS KMS to create, manage, and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.

AWS WAF

[AWS WAF](#)[\(opens in a new tab\)](#) is a web application firewall that lets you monitor network requests that come into your **web applications**.

AWS WAF works together with **Amazon CloudFront and an Application Load Balancer**. Recall the network access control lists that you learned about in an earlier module. AWS WAF works in a similar way to block or allow traffic. However, it does this by using a **[web access control list \(ACL\)](#)**[\(opens in a new tab\)](#) to protect your AWS resources.

Amazon Inspector



Amazon Inspector is a service that helps improve the security and compliance of applications by performing automated security assessments. It scans for vulnerabilities and deviations from security best practices.

- Automated Security Assessments
- Security Findings
- Vulnerability Checks
- Recommendations for Fixes
- Shared Responsibility Model

Amazon GuardDuty

[Amazon GuardDuty\(opens in a new tab\)](#) is a service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment.

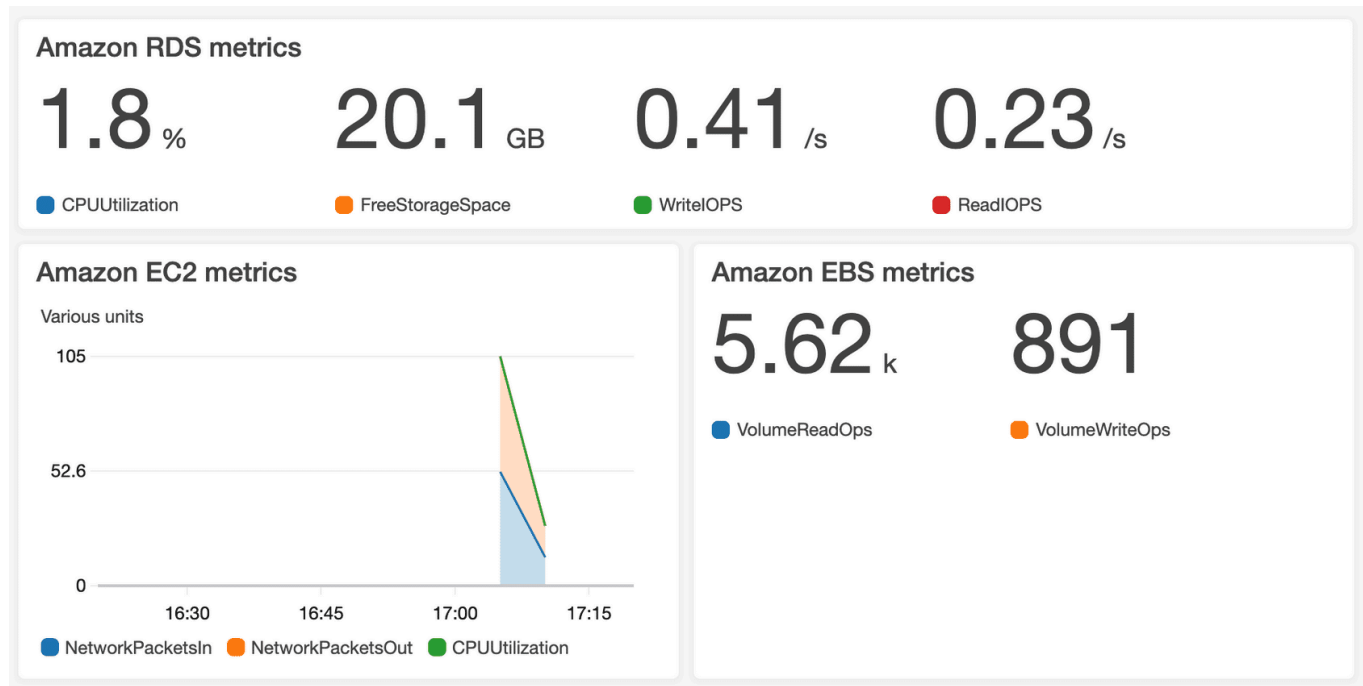
Amazon CloudWatch

[Amazon CloudWatch\(opens in a new tab\)](#) is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.

CloudWatch uses [metrics\(opens in a new tab\)](#) to represent the data points for your resources. AWS services send metrics to CloudWatch. CloudWatch then uses these metrics to create graphs automatically that show how performance has changed over time.

CloudWatch alarms





With CloudWatch, you can create [alarms\(opens in a new tab\)](#) that automatically perform actions if the value of your metric has gone above or below a predefined threshold.



The CloudWatch [dashboard\(opens in a new tab\)](#) feature enables you to access all the metrics for your resources from a single location.

AWS CloudTrail

[AWS CloudTrail\(opens in a new tab\)](#) records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more. You can think of CloudTrail as a “trail” of breadcrumbs (or a log of actions) that someone has left behind them.

<u>What</u> happened?	A new IAM user (Mary) was created.	
<u>Who</u> made the request?	IAM user John	
<u>When</u> did this occur?	January 1, 2020 at 9:00 AM	
<u>How</u> was the request made?	Through the AWS Management Console	

CloudTrail Insights

Within CloudTrail, you can also enable [loglog](#). This optional feature allows CloudTrail to automatically detect unusual API activities in your AWS account.

AWS Trusted Advisor

[AWS Trusted Advisor](#)([opens in a new tab](#)) is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.

Trusted Advisor compares its findings to AWS best practices in five categories: cost optimization, performance, security, fault tolerance, and service limits. For the checks in each category, Trusted Advisor offers a list of recommended actions and additional resources to learn more about AWS best practices.



For each category:

- The green check indicates the number of items for which it detected **no problems**.
- The orange triangle represents the number of recommended **investigations**.
- The red circle represents the number of recommended **actions**.

Pricing

AWS Free Tier

The [AWS Free Tier](#)(opens in a new tab) enables you to begin using certain services without having to worry about incurring costs for the specified period.

Three types of offers are available:

- Always Free
- 12 Months Free
- Trials

For each free tier offer, make sure to review the specific details about exactly which resource types are included.

Always Free

These offers do not expire and are available to all AWS customers.

For example, AWS Lambda allows 1 million free requests and up to 3.2 million seconds of compute time per month. Amazon DynamoDB allows 25 GB of free storage per month.

12 Months Free

These offers are free for 12 months following your initial sign-up date to AWS.

Examples include specific amounts of Amazon S3 Standard Storage, thresholds for monthly hours of Amazon EC2 compute time, and amounts of Amazon CloudFront data transfer out.

Trials

Short-term free trial offers start from the date you activate a particular service. The length of each trial might vary by number of days or the amount of usage in the service.

For example, Amazon Inspector offers a 90-day free trial. Amazon Lightsail (a service that enables you to run virtual private servers) offers 750 free hours of usage over a 30-day period.

How AWS Pricing concepts work

AWS pricing works in the following ways:

1. **Pay for what you use:** You pay only for the resources you actually use, with no long-term contracts or complex licensing requirements.

2. **Pay less when you reserve:** Some services offer reservation options, allowing you to save significantly compared to On-Demand pricing by reserving capacity in advance.
3. **Pay less with volume-based discounts:** Certain services offer tiered pricing, where the per-unit cost decreases as your usage increases.

AWS Pricing Calculator

The [AWS Pricing Calculator](#)(opens in a new tab) lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can organize your AWS estimates by groups that you define. A group can reflect how your company is organized, such as providing estimates by cost center.

Pricing example if you wanna read it for understanding of logic

AWS pricing for different services is structured based on usage and specific components. Here are the main points for each service:

AWS Lambda Pricing

- **Charges based on requests and compute time:** You pay for the number of requests and the duration your function runs.
- **Free Tier:** 1 million requests and 3.2 million seconds of compute time per month.
- **Compute Savings Plan:** Allows for cost savings by committing to consistent usage over 1 or 3 years.

Amazon EC2 Pricing

- **Charges based on compute time:** You pay only for the compute time used by running instances.
- **Spot Instances:** Offers up to 90% cost savings for workloads that can tolerate interruptions.
- **Additional savings:** Available through Savings Plans and Reserved Instances.

Amazon S3 Pricing

- **Storage:** You pay for the storage used based on object size, storage classes, and the duration objects are stored.
- **Requests and Data Retrievals:** You pay for the number of requests made to your S3 objects and buckets.
- **Data Transfer:** No cost for data transfers within the same region; charges apply for data transferred into and out of S3, with some exceptions.

- **Management and Replication:** Charges apply for storage management features like inventory, analytics, and object tagging.

[AWS Billing & Cost Management dashboard](#)

Use the [AWS Billing & Cost Management dashboard](#)(opens in a new tab) to pay your AWS bill, monitor your usage, and analyze and control your costs.

AWS Consolidated billing

AWS Organizations also provides the option for [consolidated billing](#)(opens in a new tab).

The consolidated billing feature of AWS Organizations enables you to receive a single bill for all AWS accounts in your organization. By consolidating, you can easily track the combined costs of all the linked accounts in your organization.

AWS Budgets

In [AWS Budgets](#)(opens in a new tab), you can create budgets to plan your service usage, service costs, and instance reservations.

The information in AWS Budgets updates three times a day. This helps you to accurately determine how close your usage is to your budgeted amounts or to the AWS Free Tier limits.

AWS Cost Explorer

[AWS Cost Explorer](#)(opens in a new tab) is a tool that lets you visualize, understand, and manage your AWS costs and usage over time.

AWS Cost Explorer includes a default report of the costs and usage for your top five cost-accruing AWS services. You can apply custom filters and groups to analyze your data. For example, you can view resource usage at the hourly level.

AWS Support plans:

Basic Support

- Free for all AWS customers
- Access to whitepapers, documentation, and support communities
- Limited AWS Trusted Advisor checks
- AWS Personal Health Dashboard access

Developer Support

- Best practice guidance
- Client-side diagnostic tools
- Building-block architecture support

Business Support

- Use-case guidance for AWS offerings and services
- All AWS Trusted Advisor checks
- Limited third-party software support
- It also contains the phone support that enterprise support has

Enterprise On-Ramp Support

- Pool of Technical Account Managers for proactive guidance
- Cost Optimization workshop (**one per year**)
- 30-minute response time for business-critical issues
- Concierge support team for billing/account assistance
- Tools for monitoring costs and performance

Enterprise Support

- Designated Technical Account Manager (TAM)
- Operations Reviews and innovation-driving tools
- 15-minute response time for business-critical issues
- Full access to proactive services and support automation workflows

6/20

What is the MINIMUM AWS Support plan that provides technical support through phone calls?

Report Content Errors

A Enterprise ✕

Incorrect. The Enterprise Support plan provides phone support, but it is not the minimum plan to do so.

B Business ✓

Correct. You can call or chat with technical support by using the Business Support plan or the Enterprise Support plan. The Business Support plan is the minimum plan that provides this feature.

Learn more about [AWS Support plans](#).

C Developer

Incorrect. The Developer Support plan allows only email creation of support tickets and does not provide phone support.

D Basic

Incorrect. The Basic Support plan provides customer support for non-technical issues, such as increases in service quotas. However, the Basic Support plan does not provide technical support.

✕ Incorrect Your Answer: **A** Correct Answer: **B** Continue

TAMs

A **Technical Account Manager (TAM)** is a dedicated AWS expert assigned to customers who subscribe to the **Enterprise On-Ramp** and **Enterprise Support** plans. The TAM acts as the primary point of contact between AWS and the customer, providing proactive guidance and helping to optimize cloud usage.

AWS Marketplace

[AWS Marketplace](#) is a digital catalog that includes thousands of software listings from independent software vendors. You can use AWS Marketplace to find, test, and buy software that runs on AWS.

Six core perspectives of the Cloud Adoption Framework

At the highest level, the [AWS Cloud Adoption Framework \(AWS CAF\)](#)[\(opens in a new tab\)](#) organizes guidance into six areas of focus, called **Perspectives**. Each Perspective addresses distinct responsibilities. The planning process helps the right people across the organization prepare for the changes ahead.

AWS Cloud Adoption Framework (AWS CAF) - Six Core Perspectives

1. Business Perspective

- **Definition:** Aligns IT with business needs and ensures IT investments link to business outcomes.
- **Main Points:**
 - Create a business case for cloud adoption.
 - Align business strategies and IT strategies.
 - Involves business managers, finance managers, and strategy stakeholders.

2. People Perspective

- **Definition:** Focuses on change management strategies for successful cloud adoption across the organization.
- **Main Points:**
 - Evaluate organizational structures, roles, and skills.
 - Identify gaps in skills and processes for cloud adoption.
 - Involves human resources, staffing, and people managers.

3. Governance Perspective

- **Definition:** Ensures IT strategy aligns with business strategy to maximize value and minimize risks.
- **Main Points:**
 - Update staff skills and processes for business governance in the cloud.
 - Manage and measure cloud investments.
 - Involves CIO, program managers, and enterprise architects.

4. Platform Perspective

- **Definition:** Focuses on implementing solutions on the cloud and migrating workloads from on-premises.
- **Main Points:**
 - Use architectural models for IT systems structure.
 - Define the architecture of the target cloud environment.
 - Involves CTO, IT managers, and solutions architects.

5. Security Perspective

- **Definition:** Ensures visibility, auditability, control, and agility in security for cloud adoption.
- **Main Points:**
 - Structure security controls for the organization's needs.
 - Ensure security objectives are met in the cloud.
 - Involves CISO, IT security managers, and analysts.

6. Operations Perspective

- **Definition:** Focuses on enabling, operating, and recovering IT workloads to meet business expectations.
- **Main Points:**
 - Define day-to-day and long-term operational procedures.
 - Align operations with business requirements.
 - Involves IT operations and support managers.

1. Business Perspective

- ◆ **Focus:** Aligning IT with business goals and value creation.
- ◆ **Key Actions:**
 - Justifies cloud adoption with a strong business case.
 - Ensures IT investments align with business outcomes.
 - Involves business managers, finance teams, and executives.

✅ **Exam Tip:** If a question asks about **business growth, cost optimization, or IT strategy alignment with company goals**, choose **Business Perspective**.

2. People Perspective

- ◆ **Focus:** Workforce readiness and change management.
- ◆ **Key Actions:**

- Identifies required cloud skills and closes gaps.
- Manages organizational change during cloud adoption.
- Involves HR, training teams, and leadership.

✅ **Exam Tip:** If a question involves **training employees, reskilling, or managing cloud adoption resistance**, pick **People Perspective**.

3. Governance Perspective

- ◆ **Focus:** Risk management, compliance, and cloud financial controls.
- ◆ **Key Actions:**

- Ensures IT governance aligns with business policies.
- Implements compliance and security frameworks.
- Involves CIOs, compliance teams, and finance managers.

✅ **Exam Tip:** If a question mentions **compliance, cloud policies, security governance, or financial accountability**, select **Governance Perspective**.

4. Platform Perspective

- ◆ **Focus:** Cloud infrastructure, applications, and migrations.
- ◆ **Key Actions:**

- Designs scalable, cloud-native architectures.
- Manages infrastructure as code (IaC).
- Involves cloud architects, DevOps, and IT engineers.

✅ **Exam Tip:** If a question is about **migrating applications, cloud architecture, or infrastructure planning**, pick **Platform Perspective**.

5. Security Perspective

- ◆ **Focus:** Protecting cloud data, workloads, and compliance.
- ◆ **Key Actions:**

- Implements security controls across cloud resources.
- Ensures encryption, identity management, and monitoring.
- Involves CISOs, security analysts, and IT compliance teams.

✅ **Exam Tip:** If a question mentions **data security, encryption, compliance, or risk mitigation**, select **Security Perspective**.

6. Operations Perspective

- ◆ **Focus:** Monitoring, maintenance, and operational excellence.
- ◆ **Key Actions:**

- Defines cloud operations and incident management.
- Ensures performance monitoring and reliability.
- Involves IT support teams, DevOps, and SREs.

✅ **Exam Tip:** If a question is about **cloud monitoring, troubleshooting, automation, or operational efficiency**, pick **Operations Perspective**.

How This Helps in Exam Questions

- **Example Question Pattern:**

"A company wants to ensure that its cloud adoption aligns with compliance regulations while managing financial risk. Which AWS CAF perspective should they focus on?"

- ✅ **Correct Answer:** Governance Perspective (because it deals with compliance and financial risk).

- **Another Example:**

"A firm is struggling with employee resistance to cloud adoption and lacks cloud-skilled staff. What AWS CAF perspective should they prioritize?"

- ✅ **Correct Answer:** People Perspective (since it focuses on training and change management).

6 strategies for migration

When migrating applications to the cloud, six of the most common [migration strategies](#)(opens in a new tab) that you can implement are:

- Rehosting
- Replatforming
- Refactoring/re-architecting
- Repurchasing
- Retaining
- Retiring

To learn more about migration strategies, expand each of the following six categories.

Rehosting

Rehosting also known as “lift-and-shift” involves moving applications without changes.

In the scenario of a large legacy migration, in which the company is looking to implement its migration and scale quickly to meet a business case, the majority of applications are rehosted.

Replatforming

Replatforming, also known as “lift, tinker, and shift,” involves making a few cloud optimizations to realize a tangible benefit. Optimization is achieved without changing the core architecture of the application.

Refactoring/re-architecting

Refactoring (also known as **re-architecting**) involves reimagining how an application is architected and developed by using cloud-native features. Refactoring is driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the application’s existing environment.

Repurchasing

Repurchasing involves moving from a traditional license to a software-as-a-service model.

For example, a business might choose to implement the repurchasing strategy by migrating from a customer relationship management (CRM) system to Salesforce.com.

Retaining

Retaining consists of keeping applications that are critical for the business in the source environment. This might include applications that require major refactoring before they can be migrated, or, work that can be postponed until a later time.

Retiring

Retiring is the process of removing applications that are no longer needed.

AWS Snow Family members

The [AWS Snow Family](#) (opens in a new tab) is a collection of physical devices that help to physically transport up to exabytes of data into and out of AWS.

AWS Snow Family is composed of **AWS Snowcone**, **AWS Snowball**, and **AWS Snowmobile**.

AWS Snowcone

[AWS Snowcone](#) is a small, rugged, and secure edge computing and data transfer device.

It features 2 CPUs, 4 GB of memory, and up to 14 TB of usable storage.

AWS Snowball - Device Types and Features

1. Snowball Edge Storage Optimized

- **Storage:**
 - 80 TB HDD for block volumes and S3-compatible object storage.
 - 1 TB SATA SSD for block volumes.
- **Compute:**
 - 40 vCPUs, 80 GiB memory.
 - Supports Amazon EC2 sbe1 instances (equivalent to C5).

2. Snowball Edge Compute Optimized

- **Storage:**
 - 80 TB usable HDD for Amazon S3 and EBS compatible block storage.
 - 28 TB usable NVMe SSD for Amazon EBS block volumes.
- **Compute:**
 - 104 vCPUs, 416 GiB memory.
 - Optional NVIDIA Tesla V100 GPU.
 - Supports EC2 sbe-c and sbe-g instances (equivalent to C5, M5a, G3, P3).

AWS Snowmobile

AWS Snowmobile is an exabyte-scale data transfer service used to move large amounts of data to AWS.

You can transfer up to 100 petabytes of data per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi trailer truck.

Amazon Q Developer

Amazon Q Developer is a machine learning-powered code generation tool designed to provide real-time code recommendations. It analyzes the code and comments written by the developer in their integrated development environment (IDE). Based on the existing code and surrounding context, Amazon Q Developer generates suggestions that align with the developer's style, naming conventions, and overall project structure, ensuring seamless integration. This tool helps streamline the coding process by automating code generation and improving productivity.

Installation

Developers can easily access Amazon Q Developer by downloading and installing the AWS Toolkit IDE extension. You can also activate Amazon Q Developer from directly within the AWS Lambda and AWS Cloud9 console code editors.

Installation instructions

Installation instructions vary depending on the environment. For more information, see “Setting up Amazon Q Developer” in the Amazon Q Developer User Guide by clicking on the button.

[Installation](#)

Compatibility

Amazon Q Developer seamlessly integrates with popular tools like Visual Studio (VS) Code, JetBrains IDEs (IntelliJ IDEA, PyCharm, etc.), Amazon SageMaker Studio, JupyterLab, AWS Cloud9, and the AWS Lambda console.

Support

It supports a wide range of programming languages and development environments, including Python, Java, JavaScript, TypeScript, C#, Go, Rust, PHP, Ruby, Kotlin, C, C++, Shell scripting, SQL, and Scala.

The AWS Well-Architected Framework

The [AWS Well-Architected Framework\(opens in a new tab\)](#) helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud. It provides a way for you to consistently measure your architecture against best practices and design principles and identify areas for improvement.

The **Well-Architected Framework** consists of six pillars:

1. **Operational Excellence:**

- Focus on running and monitoring systems to deliver business value and continually improve processes.
- Key principles: operations as code, documentation, anticipating failure, making small, reversible changes.
- There are five design principles for operational excellence in the cloud: 1) Perform operations as code 2) Make frequent, small, reversible changes 3) Refine operations procedures frequently 4) Anticipate failure 5) Learn from all operational failures

2. **Security:**

- Protect information, systems, and assets while delivering value through risk assessments and mitigation strategies.
- Key practices: automate security, apply security at all layers, protect data in transit and at rest.

3. **Reliability:**

- Ensure systems can recover from disruptions, scale to meet demand, and mitigate failures.
- Key aspects: test recovery procedures, scale horizontally, auto-recover from failure.

4. **Performance Efficiency:**

- Use resources efficiently and maintain that efficiency as demand changes.
- Key strategies: experiment, use serverless architectures, design for global scalability.

5. **Cost Optimization:**

- Deliver value at the lowest cost.
- Key tactics: adopt consumption models, analyze expenditure, use managed services to reduce ownership costs.

6. **Sustainability:**

- Improve sustainability by reducing energy consumption and increasing efficiency.
- Key actions: understand impact, set goals, maximize utilization, adopt new efficient resources, use managed services, reduce downstream impacts.

Six advantages of cloud computing:

- Trade upfront expense for variable expense.
- Benefit from massive economies of scale.
- Stop guessing capacity.
- Increase speed and agility.
- Stop spending money running and maintaining data centers.
- Go global in minutes.

AWS SageMaker

Overview:

Amazon SageMaker is a fully managed service that provides tools and frameworks for building, training, and deploying machine learning (ML) models. It is designed to simplify the end-to-end ML workflow, enabling data scientists and developers to create robust ML models quickly and efficiently.

AWS DataSync

AWS DataSync is a fully managed service that simplifies and accelerates data transfer between on-premises storage systems and AWS services like Amazon S3, EFS, and FSx. It automates data migration, synchronization, and backup tasks, ensuring high-speed, secure transfers with minimal configuration.

AWS Cloud Map

AWS Cloud Map is a service discovery tool that enables applications to discover and connect to resources dynamically. It allows you to register any resource, such as databases, microservices, and virtual machines, and provides real-time information about their availability, improving the efficiency of service communication and management in cloud environments.

AWS Application Discovery Service

AWS Application Discovery Service helps you plan migration projects by discovering and gathering detailed information about your on-premises data centers, such as servers, applications, and dependencies. It provides insights into application performance and architecture, enabling you to make informed decisions during the migration process to AWS.

AWS Cloud Map - Service that provides service discovery for containerized applications and microservices

AWS DataZone

AWS DataZone is a data governance and management service that helps organizations securely discover, share, and catalog data across various data sources within AWS and on-premises environments. It provides tools for managing data access, ensuring compliance, and simplifying the process of finding and using data across different departments and teams.

AWS Backup(it also has AWS backup vault)

AWS Backup is a fully managed backup service that enables you to automate and centralize the backup of data across AWS services and on-premises environments. It helps ensure data durability, compliance, and recovery by providing automated backup schedules, retention policies, and monitoring for resources like Amazon EC2, RDS, EFS, and DynamoDB.

AWS Transfer Family

AWS Transfer Family is a fully managed service that enables you to transfer files into and out of AWS storage services like Amazon S3 and Amazon EFS using protocols such as SFTP, FTPS, and FTP. It simplifies secure, reliable file transfers for applications without requiring custom infrastructure.

Amazon Forecast

Amazon Forecast is a fully managed machine learning service that generates accurate time-series predictions based on historical data. It uses machine learning to identify patterns and trends, allowing businesses to make data-driven decisions for inventory planning, resource allocation, and demand forecasting.

Amazon Timestream

Amazon Timestream is a serverless time-series database designed to store, analyze, and query time-stamped data such as application monitoring, IoT sensor data, and event tracking. It is optimized for handling large volumes of time-series data efficiently and provides fast query performance.

Amazon OpenSearch Service

Amazon OpenSearch Service is a fully managed service that enables you to deploy, operate, and scale OpenSearch and Elasticsearch clusters for search, analytics, and monitoring applications. It is used to perform log analytics, full-text searches, real-time application monitoring, and other data-intensive use cases. OpenSearch Service integrates with other AWS services and provides built-in security, scalability, and high availability.

Amazon Comprehend

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to uncover insights and relationships in text. It can analyze text to extract entities, detect sentiment, identify key phrases, and classify documents.

Amazon Personalize

Amazon Personalize is a machine learning service that enables developers to build personalized recommendation systems for applications. It analyzes user behavior and preferences to deliver tailored product, content, or service recommendations.

Amazon SageMaker

Amazon SageMaker is a fully managed machine learning service that allows developers and data scientists to build, train, and deploy machine learning models quickly and efficiently. It provides tools for every step of the machine learning workflow, from data preparation to model deployment.

AWS App Runner

AWS App Runner is a fully managed service that simplifies the deployment of containerized applications directly from source code or container images. It automates infrastructure provisioning, scaling, and load balancing to help developers quickly build and deploy web applications and APIs.

AWS Systems Manager

AWS Systems Manager is a service that provides operational insights and management for AWS resources. It helps automate operational tasks, collect and query system information, and manage configurations across your AWS environment securely and at scale.

AWS Compute Optimizer

AWS Compute Optimizer is a service that recommends optimal AWS compute resources for your workloads. It analyzes usage patterns and provides suggestions to reduce costs, improve performance, and enhance efficiency by selecting the right instance types or configurations.

Amazon Kendra

Amazon Kendra is an intelligent search service powered by machine learning that helps organizations index, search, and retrieve information from their internal documents, knowledge bases, and data repositories. It delivers highly accurate and context-aware search results.

Amazon Athena(for multiple objects)

Amazon Athena is a serverless interactive query service that allows you to analyze data stored in Amazon S3 using standard SQL. It is used for ad hoc querying and analyzing structured, semi-structured, and unstructured data without the need to manage infrastructure.

S3 Select(but only for one object)

Amazon S3 Select is a feature of Amazon S3 that allows you to retrieve and query a subset of data from an object using SQL expressions. Instead of downloading the entire object, S3 Select enables you to retrieve only the specific data you need, improving performance and reducing costs when working with large datasets.

AWS Batch

AWS Batch is a fully managed service that enables developers, scientists, and engineers to run batch computing workloads at any scale. It dynamically provisions the required compute resources and efficiently schedules jobs across instances, allowing you to process large volumes of data or tasks without managing infrastructure.

AWS Backup

AWS Backup is a fully managed backup service that enables you to automate and centralize the backup of data across AWS services and on-premises environments. It helps ensure data durability, compliance, and recovery by providing automated backup schedules, retention policies, and monitoring for resources like Amazon EC2, RDS, EFS, and DynamoDB.

Amazon Macie

Amazon Macie is a fully managed data security and privacy service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. It helps organizations identify personally identifiable information (PII) and other sensitive data, providing visibility into data security risks and ensuring compliance with privacy regulations.

AWS Consolidated Billing

AWS Consolidated Billing is a feature that allows organizations to combine multiple AWS accounts into one payment method. It enables you to manage costs more efficiently by aggregating usage across accounts, taking advantage of volume discounts, and providing a unified view of your AWS usage and spending.

Amazon ElastiCache

Amazon ElastiCache is a fully managed in-memory data store service that supports two popular caching engines: Redis and Memcached. It is used to improve application performance by caching frequently accessed data, reducing database load, and decreasing response times for applications. ElastiCache is commonly used for session management, real-time analytics, and caching web pages.

AWS Reserved Instance Marketplace

The AWS Reserved Instance Marketplace is a platform where users can buy and sell unused Reserved Instances (RIs). It allows customers to purchase RIs at discounted rates from other AWS customers who no longer need their reserved capacity, providing flexibility in managing reserved instance commitments.

AWS APN (AWS Partner Network)

The AWS Partner Network (APN) is a global program that enables partners to build, market, and sell their solutions on AWS. It includes a range of technology and consulting partners who help customers design, architect, and deploy AWS solutions. APN provides resources, training, and support for partners to enhance their AWS offerings.

AWS Professional Support

AWS Professional Support offers expert guidance and assistance to customers for AWS architecture, implementation, and operational tasks. It is designed for organizations that require more hands-on help beyond standard support, providing tailored recommendations, best practices, and proactive troubleshooting to optimize AWS workloads.

AWS Trusted Advisor

AWS Trusted Advisor is an online resource that provides real-time guidance to help you provision resources following AWS best practices. It evaluates your AWS environment across multiple categories, such as cost optimization, security, fault tolerance, and performance, and offers recommendations for improvements to optimize resources and reduce costs.

Amazon Connect

Amazon Connect is a cloud-based contact center service that enables businesses to deliver customer service at scale. It provides an easy-to-use platform for setting up and managing customer service interactions, including voice and chat, with features like automated routing, real-time metrics, and integration with other AWS services.

Amazon Lex

Amazon Lex is a service for building conversational interfaces using voice and text. It is the same technology that powers Amazon Alexa and allows developers to create chatbots and virtual assistants that can interact naturally with users. Lex integrates with other AWS services to provide advanced capabilities like natural language understanding (NLU) and automatic speech recognition (ASR).

Amazon s2 express zone

For an Amazon S3 solution that offers sub-second object storage access within single-digit milliseconds, the best option is

S3 Express One Zone

Explanation:

- **High Performance:** S3 Express One Zone is specifically designed to deliver consistent, low latency access times, making it ideal for applications requiring fast data retrieval within single-digit milliseconds.
- S3 Express One Zone usually comes with a slightly higher cost compared to standard S3 due to its high-performance nature.

B. AWS Billing Conductor

AWS Billing Conductor is a customization tool for managing and organizing billing details. It helps businesses group accounts, customize billing rates, and generate invoices that reflect specific internal pricing structures.

C. Amazon CodeGuru

Amazon CodeGuru is a developer tool powered by machine learning that identifies code inefficiencies and potential vulnerabilities. It provides recommendations for code optimization and performance improvements to enhance software quality.

D. Amazon SageMaker

Amazon SageMaker is a fully managed service that simplifies the process of building, training, and deploying machine learning models at scale. It provides tools for data preparation, model training, and endpoint deployment, making ML accessible for all skill levels.

E. AWS Compute Optimizer

AWS Compute Optimizer is a service that recommends optimal AWS resources for your workloads. It analyzes the historical utilization of your Amazon EC2 instances and provides recommendations for rightsizing, which involves changing the instance type to a better fit based on the workload's requirements.

Amazon QuickSight:

Amazon QuickSight is a fully managed business intelligence (BI) service that enables users to create and visualize interactive dashboards and reports. It connects to various data sources, making it suitable for visualizing data prepared by services like AWS Glue.

AWS Glue:

AWS Glue is a serverless data integration service that makes it easier to discover, prepare, move, and integrate data from multiple sources for analytics, machine learning (ML), and application development.

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to discover, prepare, and load data for analysis. It automates the time-consuming tasks of data discovery, transformation, and job scheduling, allowing users to focus on analyzing the data

- **AWS Global Accelerator** – Improves application availability and performance using global networking infrastructure.
- **Amazon FSx** – Provides file storage solutions, including FSx for Windows File Server and FSx for Lustre.
- **AWS Secrets Manager** – Securely stores and manages sensitive information like database credentials and API keys.
- **AWS Identity Center (formerly AWS SSO)** – Centralized access management for AWS accounts and applications.
- **AWS Security Hub** – Centralized security and compliance management for AWS accounts.
- **AWS CodeDeploy** – Automates code deployment to Amazon EC2, Fargate, and Lambda.
- **AWS CodePipeline** – Automates CI/CD workflows for application development.
- **AWS CodeCommit** – A fully managed source control service that hosts private Git repositories.
- **AWS Amplify** – A development framework for building scalable mobile and web applications.
- **Amazon AppFlow** – A managed integration service to transfer data between SaaS applications and AWS services.

AWS Config

AWS Config is a service that enables you to **assess, audit, and evaluate** the configurations of your AWS resources. It continuously monitors and records AWS resource configurations and **automatically checks for compliance** with desired configurations. AWS Config helps with **tracking configuration changes**, maintaining compliance, and troubleshooting operational issues by providing a **detailed history of resource configurations**.

AWS CodePipeline

AWS CodePipeline is a **continuous integration and continuous delivery (CI/CD) service** that automates the **build, test, and deployment** phases of application development. It integrates with AWS services like **CodeBuild, CodeDeploy, and third-party tools** to enable

rapid and reliable application updates. CodePipeline helps ensure **consistent and repeatable software releases** by defining workflows using a visual interface or AWS CLI.

AWS Service Quotas

AWS Service Quotas is a **management service** that enables users to **view and manage the limits (quotas) on AWS services**. It helps organizations **monitor and request increases** for resource limits, ensuring they can scale their workloads efficiently. The service integrates with **AWS CloudWatch** for alerts and provides **automatic quota management** for supported services.

AWS Service Catalog

AWS Service Catalog lets you centrally manage your cloud resources to achieve governance at scale of your infrastructure as code (IaC) templates, written in CloudFormation or Terraform configurations. With AWS Service Catalog, you can meet your compliance requirements while making sure your customers can quickly deploy the cloud resources they need.

Software Development Kits

Another option for accessing and managing AWS services is the **software development kits (SDKs)**. SDKs make it easier for you to use AWS services through an API designed for your programming language or platform. SDKs enable you to use AWS services with your existing applications or create entirely new applications that will run on AWS.

To help you get started with using SDKs, AWS provides documentation and sample code for each supported programming language. Supported programming languages include C++, Java, .NET, and more.

34) Which task requires using AWS account root user credentials?

- A. Viewing billing information
- B. Changing the AWS Support plan
- C. Starting and stopping Amazon EC2 instances
- D. Opening an AWS Support case

Correct Answer: B

There are only a few tasks that require you to use the root user:

- Change your account settings. This includes the account name, email address, root user password, and root user access keys. ...
- View certain tax invoices. ...
- Close your AWS account.
- Restore IAM user permissions. ...
- Change your AWS Support plan or Cancel your AWS Support plan. ...

27) Which AWS service or feature can a company use to determine which business unit is using specific AWS resources?

- A. Cost allocation tags
- B. Key pairs
- C. Amazon Inspector
- D. AWS Trusted Advisor

Correct Answer: A

You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.

AWS Cloud9

AWS Cloud9 is a **cloud-based integrated development environment (IDE)** that allows developers to write, run, and debug code directly in a web browser. It includes a **code editor, terminal, and debugger**, supporting multiple programming languages like **Python, JavaScript, and PHP**. Cloud9 provides **collaborative development features**, preconfigured environments, and deep integration with AWS services, enabling seamless cloud-native application development.

Amazon CloudWatch

Amazon CloudWatch is a **monitoring and observability service** that collects and analyzes **metrics, logs, and events** from AWS resources and applications. It helps in **real-time performance monitoring, setting alarms, visualizing operational data, and automating responses** to system changes, ensuring application health and efficiency.

AWS CloudTrail

AWS CloudTrail is a **logging and governance service** that records **API calls and user activities** across AWS accounts. It provides **detailed event history** for security analysis, compliance audits, and troubleshooting by tracking who did what, when, and from where in AWS environments.

AWS X-Ray

AWS X-Ray is a **distributed tracing service** that helps developers analyze and debug applications, especially in **microservices and serverless architectures**. It traces requests as they travel through an application, providing insights into **latency, bottlenecks, and failures** across different AWS services, helping improve performance and troubleshooting issues efficiently.

NAT Gateway

A **NAT (Network Address Translation) Gateway** is a **managed AWS service** that allows instances in a **private subnet** to **connect to the internet or other AWS services** while **preventing inbound connections** from external sources. It enables **outbound internet access** for resources that do not have public IPs, commonly used for updating software or accessing external APIs securely.

AWS Storage Gateway (Including Internet Storage Gateway Concept)

AWS **Storage Gateway** is a **hybrid cloud storage service** that enables on-premises applications to use AWS cloud storage securely and efficiently. It provides **low-latency access** to frequently used data while storing backups and archives in AWS.

It offers three main gateway types:

- **File Gateway** – Provides SMB/NFS access to Amazon S3.
- **Volume Gateway** – Offers iSCSI-based block storage with snapshots in Amazon S3.
- **Tape Gateway** – Virtual tape library (VTL) for backup and archival to AWS.

If you are referring to an **Internet Storage Gateway**, it typically relates to how **AWS Storage Gateway** enables **seamless access to cloud storage over the internet**, allowing businesses to extend on-premises storage to AWS while maintaining local performance.

Customer Gateway (CGW)

A **Customer Gateway (CGW)** is a **device or software application** on a **customer's on-premises network** that connects to an **AWS Virtual Private Cloud (VPC)** via a **Site-to-Site VPN**. It serves as the anchor on the customer's side of a **VPN connection** to AWS.

- Required for setting up a **Site-to-Site VPN** with an AWS **Virtual Private Gateway** or **Transit Gateway**.
- Supports **IPsec VPN tunnels** for secure communication between on-premises and AWS.
- Works with **hardware or software-based VPN devices** compatible with AWS.

This service is useful for **hybrid cloud architectures**, where an organization connects its **on-premises infrastructure to AWS** securely over the internet.

VPC Endpoints

VPC Endpoints allow you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without using an internet gateway, NAT device, VPN connection, or AWS Direct Connect.

Key Points:

- **Interface Endpoints** enable private connectivity to services like AWS KMS, S3, and EC2.
 - **Gateway Endpoints** are used for private connections to S3 and DynamoDB.
 - Enhance security by keeping traffic within the AWS network.
-

Customer Gateway

A **Customer Gateway** is a physical or software appliance on the customer side that provides the interface for the AWS VPN connection. It represents the on-premises VPN device that is used to establish a VPN connection with an AWS VPN Gateway.

Key Points:

- The customer gateway is used to configure and manage the VPN tunnel to AWS.
- It works with AWS Site-to-Site VPN to create secure connections between your on-premises network and AWS.

VPC Peering

VPC Peering enables you to connect two VPCs, allowing them to route traffic between each other as if they were within the same network. It can be set up within a single AWS region (intra-region peering) or across regions (inter-region peering).

Key Points:

- VPC Peering allows private communication between instances in different VPCs.
- The connection is established using private IP addresses, ensuring secure communication.
- Peering is non-transitive, meaning you need to establish separate peering connections for each VPC pair.
- It supports both IPv4 and IPv6 addressing.

AWS Step Functions - Orchestration for Serverless Workflows

◆ **Definition:** AWS Step Functions is a **serverless orchestration service** that enables the coordination of multiple AWS services into a **workflow** using a **visual workflow designer**. It allows you to build resilient, event-driven applications by managing task execution, retries, and error handling.

Amazon Kinesis – Real-Time Data Streaming Service

◆ **Definition:** Amazon Kinesis is a managed service for processing and analyzing real-time streaming data at scale. It enables applications to collect, process, and analyze continuous data streams efficiently.

Amazon Cognito

Amazon Cognito is a service that provides authentication, authorization, and user management for web and mobile applications.

AWS Bills

AWS Bills is a section within the **AWS Billing and Cost Management** service that provides detailed billing information for AWS usage.

Key Points for Exam:

- Displays **monthly charges** and **detailed usage breakdown** across AWS services.
- Allows **invoice downloads** and **payment history tracking**.

- Supports **cost allocation tags** to track spending by projects or departments.
- Works with **AWS Cost Explorer** and **AWS Budgets** for cost management and forecasting.
- Helps in setting up **consolidated billing** for AWS Organizations.

96) Which AWS services are managed database services? (Choose two.)

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon S3
- C. Amazon RDS
- D. Amazon Elastic File System (Amazon EFS)
- E. Amazon DynamoDB

Correct Answer: CE

fully managed AWS databases:

- Amazon RDS
- Amazon DocumentDB
- Amazon Keyspaces
- Amazon ElastiCache