AWS Cloud Practitioner Essentials Notes:

Table of Contents

[Module 1: Introduction 1](#_Toc112151846)

[Module 2: Compute in the Cloud 2](#_Toc112151847)

[Module 3: Global Infrastructure and Reliability 6](#_Toc112151848)

[Module 4: Networking 8](#_Toc112151849)

[Module 5: Storage and Databases 11](#_Toc112151850)

[Module 6: Security 15](#_Toc112151851)

[Module 7: Monitoring and Analytics 18](#_Toc112151852)

[Module 8: Pricing and Support 19](#_Toc112151853)

[Module 9: Migration and Innovation 22](#_Toc112151854)

[Module 10: The Cloud Journey 24](#_Toc112151855)

# Module 1: Introduction

**Cloud Computing**: On-demand delivery of IT resources and applications through the internet with pay-as-you-go pricing.

**Cloud computing deployment models:**

* Cloud Based Deployment
* On Premise Deployment
* Hybrid Deployment

**Benefits of cloud computing:**

* Trade upfront expense for variable expense
* Stop spending money to run and maintain data centers
* Stop guessing capacity
* Benefit from massive economies of scale
* Increase speed and agility
* Go global in minutes

# Module 2: Compute in the Cloud

Amazon Elastic Compute Cloud (Amazon EC2): provides secure, resizable compute capacity in the cloud as Amazon EC2 instances.

**EC2 instance types:**

**General purpose instances** provide a balance of compute, memory, and networking resources. You can use them for a variety of workloads.

* Ex. application servers, gaming servers, backend servers for enterprise applications, small and medium databases

**Compute optimized instances**are ideal for compute-bound applications that benefit from high-performance processors.

* Ex. high-performance web servers, compute-intensive applications servers, and dedicated gaming servers

**Memory optimized instances** are designed to deliver fast performance for workloads that process large datasets in memory.

* Ex. real-time processing of a large amount of unstructured data

**Accelerated computing instances** use hardware accelerators, or coprocessors, to perform some functions more efficiently than is possible in software running on CPUs.

* Ex. graphics applications, game streaming, and application streaming

**Storage optimized instances** are designed for workloads that require high, sequential read and write access to large datasets on local storage.

* Ex. distributed file systems, data warehousing applications, and high-frequency online transaction processing (OLTP) systems

**Amazon EC2 pricing:**

Pay only for the compute time that you use

Pricing Options:

**On-Demand Instances** are ideal for short-term, irregular workloads that cannot be interrupted. No upfront costs or minimum contracts apply.

**Amazon EC2 Savings Plans** enable you to reduce your compute costs by committing to a consistent amount of compute usage for a 1-year or 3-year term.

**Reserved Instances** are a billing discount applied to the use of On-Demand Instances in your account.

* Provide discount over on-demand pricing
* Can reserve capacity in an availability zone

**Spot Instances** are ideal for workloads with flexible start and end times, or that can withstand interruptions. (Pricing adjusts based on supply and demand)

**Dedicated Hosts**are physical servers with Amazon EC2 instance capacity that is fully dedicated to your use.

**Scalability**:

Involves beginning with only the resources you need and designing your architecture to automatically respond to changing demand by scaling out or in.

**Amazon EC2 Auto Scaling:**

Automatically add or remove Amazon EC2 instances in response to changing application demand.

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

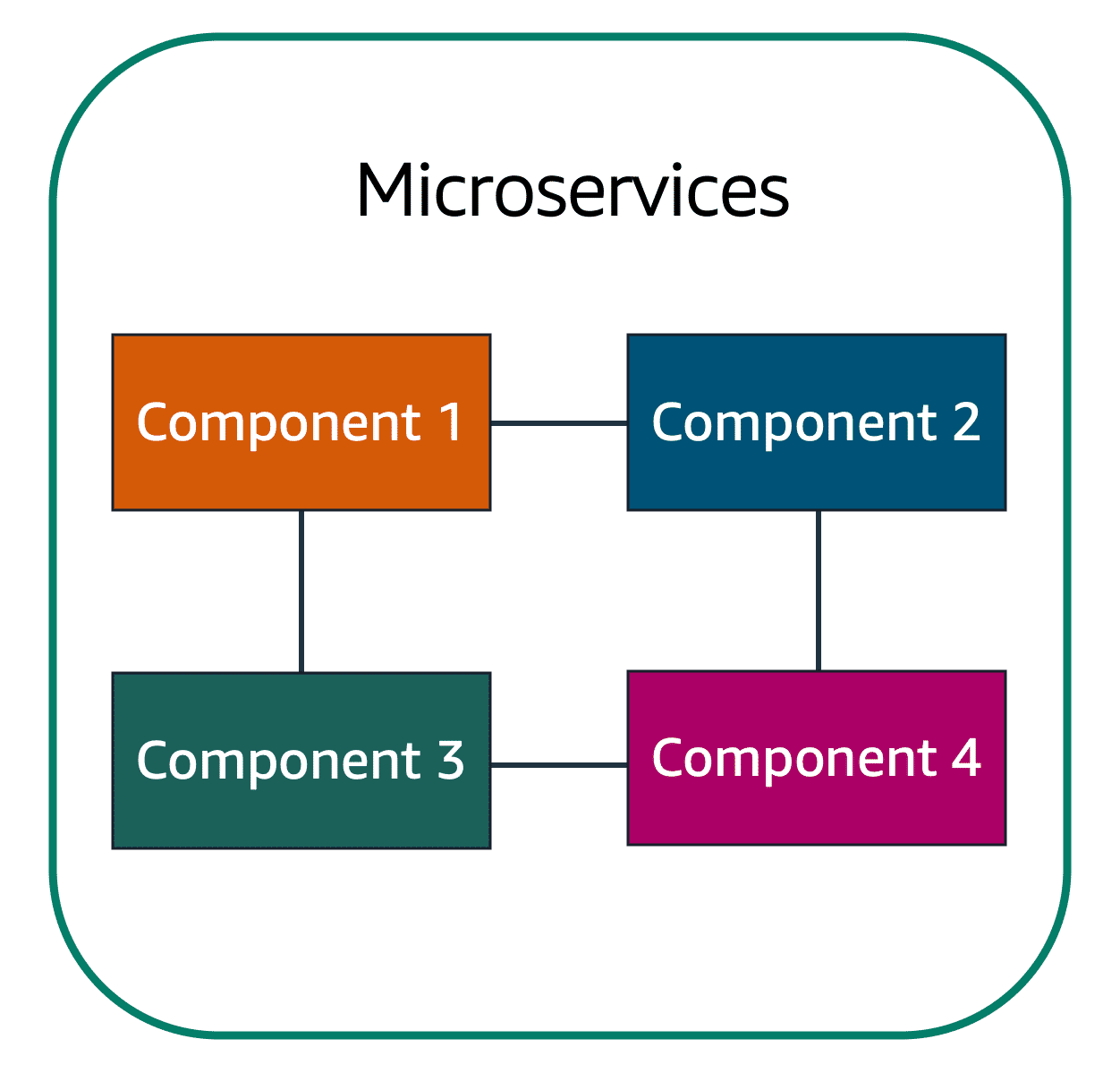
**Elastic Load Balancing**

Is the AWS service that automatically distributes incoming application traffic across multiple resources, such as Amazon EC2 instances. Ensuring that no single Amazon EC2 instance must carry the full workload on its own.

Diagram

Description automatically generated

**Messaging and Queuing**



In a microservices approach, application components are loosely coupled. In this case, if a single component fails, the other components continue to work because they are communicating with each other.

Two services facilitate application integration:

**Amazon Simple Notification Service (Amazon SNS)**

Is a publish/subscribe service.

* Subscribers can be web servers, email addresses, AWS Lambda functions, or several other options.

**Amazon Simple Queue Service (Amazon SQS)**

Is a message queuing service.

* Enables you to send, store, and retrieve messages between components

**Serverless computing:**

Your code runs on servers, but you do not need to provision or manage these servers.

**AWS Lambda** is a service that lets you run code without needing to provision or manage servers.

* Pay only for the compute time that you consume

**Containers:**

Provide you with a standard way to package your application's code and dependencies into a single object.

**Amazon Elastic Container Service** is a highly scalable, high-performance container management system that enables you to run and scale containerized applications on AWS.

**Amazon Elastic Kubernetes Service (Amazon EKS**) is a fully managed service that you can use to run Kubernetes on AWS.

* *Kubernetes* is open-source software that enables you to deploy and manage containerized applications at scale. (Orchestration)

**AWS Fargate** is a serverless compute engine for containers. It works with both Amazon ECS and Amazon EKS.

# Module 3: Global Infrastructure and Reliability

**Selecting a Region**

A Region is a geographical area that contains AWS resources and consists of two or more Availability Zones.

Four business factors:

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

**Availability Zone** is a single data center or a group of data centers within a Region.

* A fully isolated portion of the AWS global infrastructure

**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 service. It uses a network of edge locations to cache content and deliver content to customers all over the world (i.e., data, video, applications, and API’s)

Provisioning:

**AWS Management Console** is a web-based interface for accessing and managing AWS services

**AWS Command Line Interface (AWS CLI)** enables you to control multiple AWS services directly from the command line within one tool.

* Automate the actions that your services and applications perform through scripts

**Software development kits (SDKs)** makes it easier for you to use AWS services through an API designed for your programming language or platform.

* Enable you to use AWS services with your existing applications or create entirely new applications that will run on AWS.
* Supported programming languages include C++, Java, .NET

**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

\*Used to quickly deploy and scale applications on AWS

**AWS CloudFormation**, you can treat your infrastructure as code

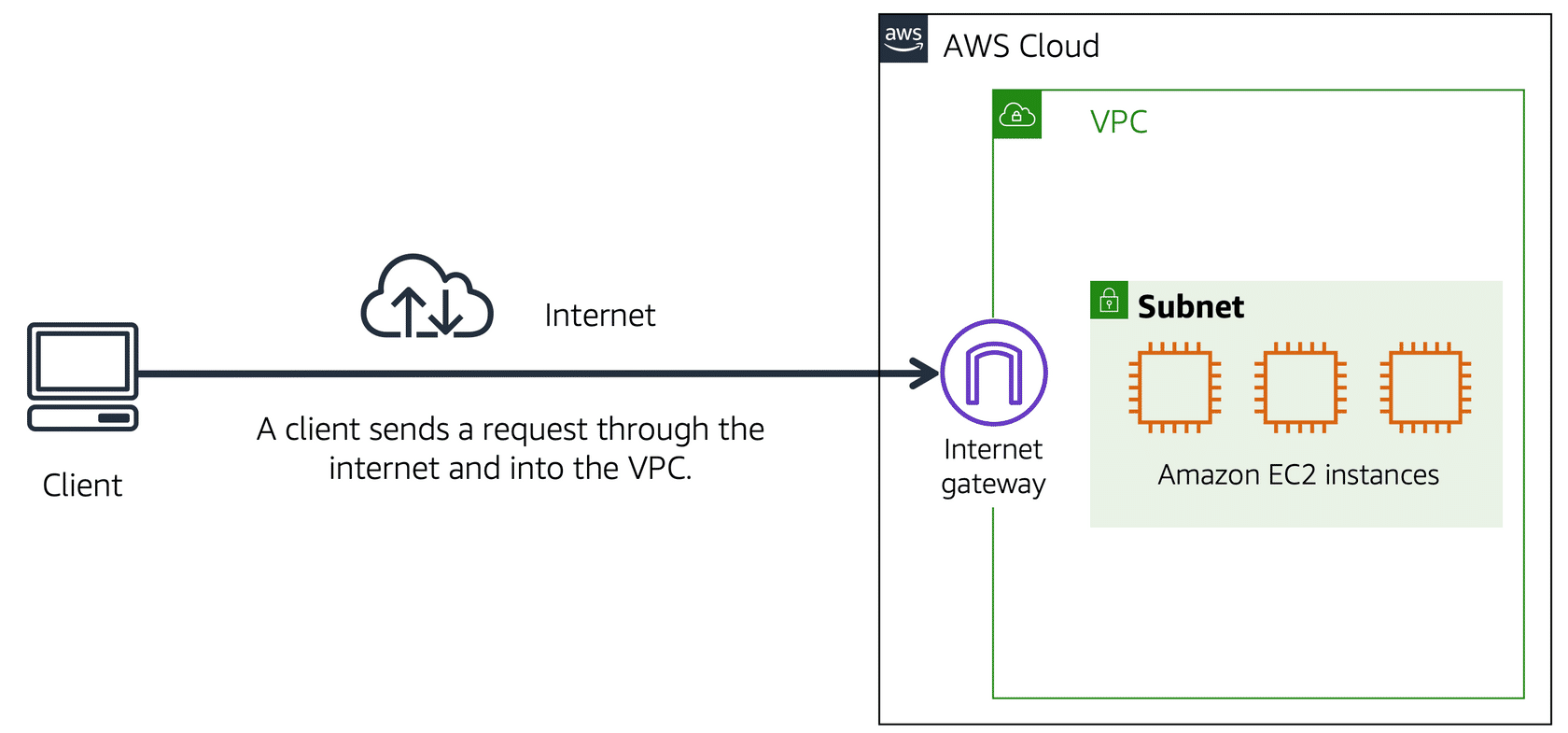
# Module 4: Networking

**Amazon Virtual Private Cloud (Amazon VPC)** is a networking service that you can use to establish boundaries around your AWS resources

* Enables you to provision an isolated section of the AWS Cloud
* Organize your resources into subnets

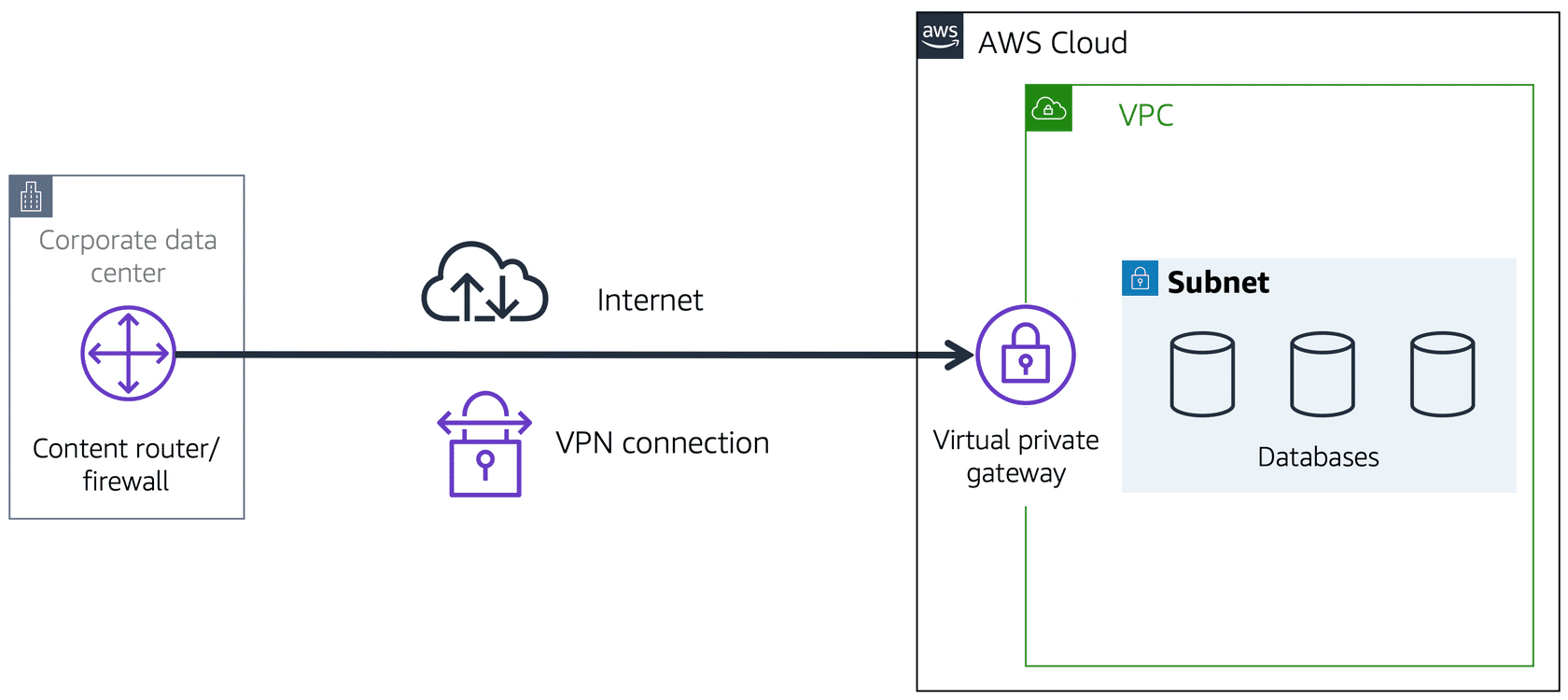
**Subnet** is a section of a VPC that can contain resources such as Amazon EC2 instances

**Internet gateway** is a connection between a VPC and the internet



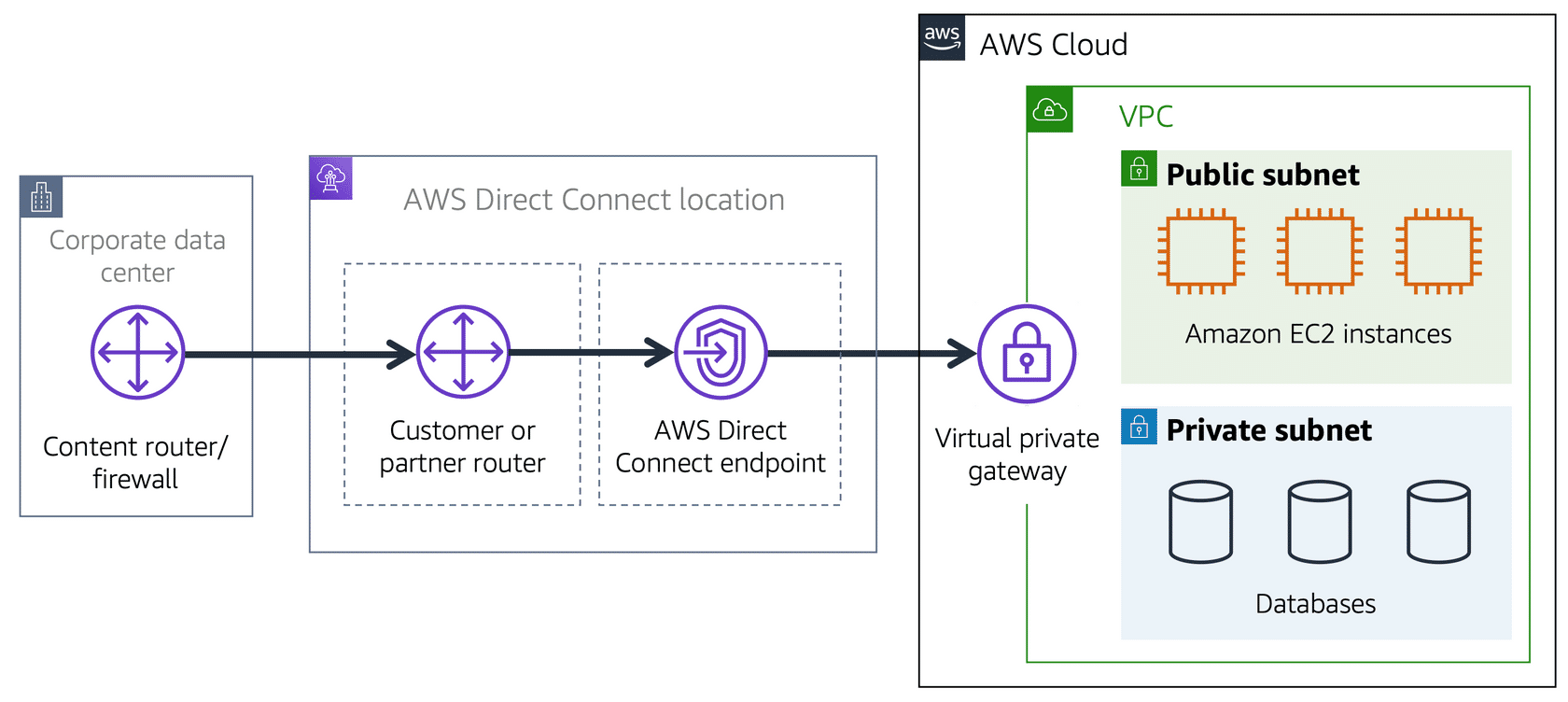
**Virtual private gateway allows** access of private resources in a VPC

* Enables you to establish a virtual private network (VPN) connection between your VPC and a private network, such as an on-premises data center or internal corporate network



**AWS Direct Connect** is a service that enables you to establish a dedicated private connection between your data center and a VPC (“hallway”).

* Reduces network costs and increase the amount of bandwidth that can travel through your network.



**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.

**Network access control list (ACL)** is a virtual firewall that controls inbound and outbound traffic at the subnet level.

* Default network ACL allows all inbound and outbound traffic
* Perform **stateless** packet filtering. They remember nothing and check packets that cross the subnet border each way: inbound and outbound

**Security group** is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.

* Default security group denies all inbound traffic and allows all outbound traffic
* Security groups perform **stateful** packet filtering. They remember previous decisions made for incoming packets

**Domain Name System (DNS)** is the process of translating a domain name to an IP address.

**Amazon Route 53** is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS.

* Register new domain names directly in Route 53
* Transfer DNS records for existing domain names managed by other domain registrars

# Module 5: Storage and Databases

**Instance Store** provides temporary block-level storage for an Amazon EC2 instance.

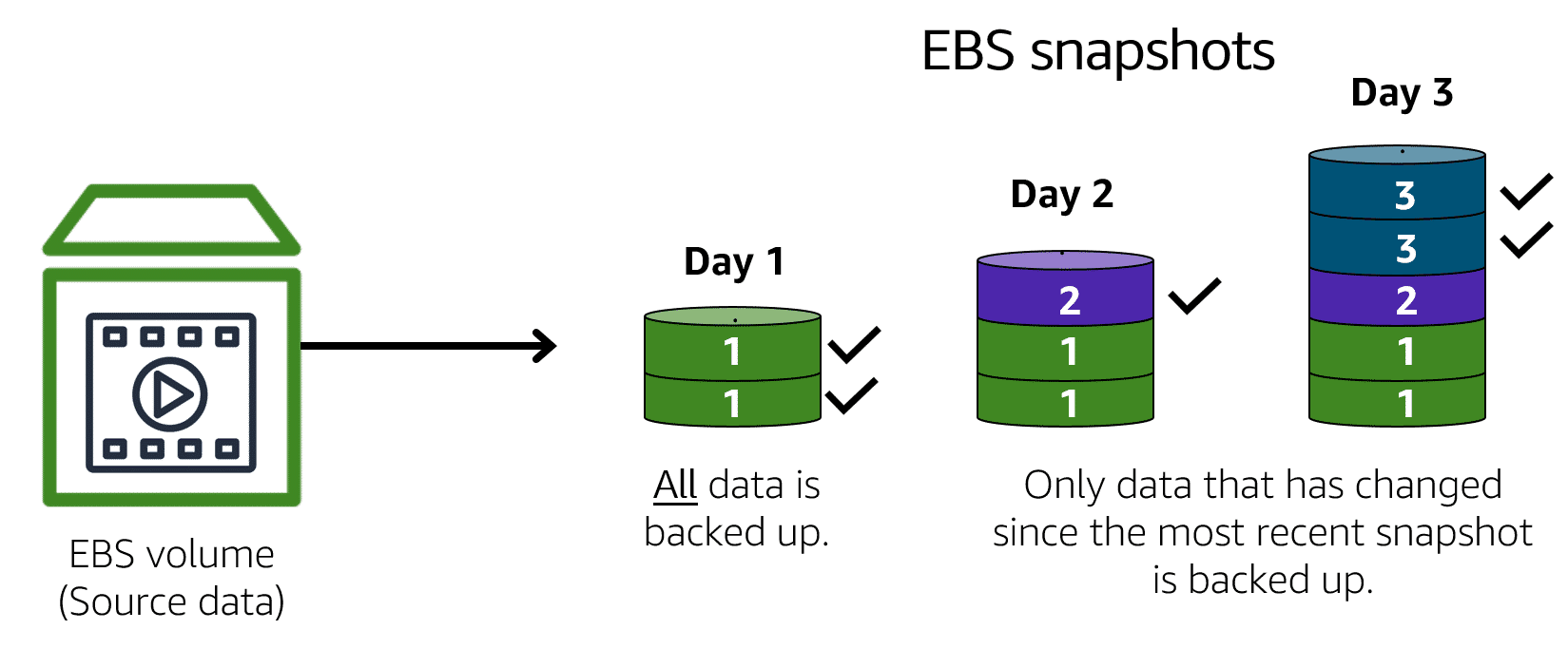
* Disk storage that is physically attached to the host computer for an EC2 instance, and therefore has the same lifespan as the instance

**Amazon Elastic Block Store (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
* Stores data in single availability zone

**EBS snapshot** is an incremental backup.

* First backup taken of a volume copies all the data
* Subsequent backups, only the blocks of data that have changed since the most recent snapshot are saved



**Object storage**, each object consists of data, metadata, and a key.

**Amazon Simple Storage Service (Amazon S3)** is a service that provides object-level storage. Amazon S3 stores data as objects in buckets.

* Can upload any type of file such as images, videos, text files
* Unlimited storage space
* Maximum file size for an object is 5TB

**Amazon S3 storage classes:**

**S3 Standard**

* Designed for frequently accessed data
* Stores data in a minimum of three Availability Zones

**S3 Standard-Infrequent Access (S3 Standard-IA)**

* Ideal for infrequently accessed data
* Similar to S3 Standard but has lower storage price and higher retrieval price

**S3 One Zone-Infrequent Access (S3 One Zone-IA)**

* Stores data in a single Availability Zone
* Has a lower storage price than S3 Standard-IA

**S3 Intelligent-Tiering**

* Ideal for data with unknown or changing access patterns
* Requires a small monthly monitoring and automation fee per object

**S3 Glacier**

* Low-cost storage designed for data archiving
* Able to retrieve objects within a few minutes to hours

**S3 Glacier Deep Archive**

* Lowest-cost object storage class ideal for archiving
* Able to retrieve objects within 12 hours

**File storage**, multiple clients (such as users, applications, servers, and so on) can access data that is stored in shared file folders

**Amazon Elastic File System** is a scalable file system used with AWS Cloud services and on-premises resources.

* Is a regional service. It stores data in and across **multiple** Availability Zones

**Relational database**, data is stored in a way that relates it to other pieces of data.

* Uses **structured query language (SQL)** to store and query data

**Amazon Relational Database Service (Amazon RDS)** is a service that enables you to run relational databases in the AWS Cloud.

* Simplifies relational database administration tasks
* Read Replica creates read only copies improving scalability
* Automated backups

Supported database engines include:

* Amazon Aurora
* PostgreSQL
* MySQL
* MariaDB
* Oracle Database
* Microsoft SQL Server

**Amazon Aurora** is an enterprise-class relational database.

* Helps reduce your database costs by reducing unnecessary input/output (I/O)
* Consider if your workloads require high availability

**Amazon DynamoDB** is a key-value database service.

* Serverless
* Automatic scaling

**Amazon Redshift** is a data warehousing service that you can use for big data analytics.

**AWS Database Migration Service (AWS DMS)** enables you to migrate relational databases, nonrelational databases, and other types of data stores.

Use Cases:

* Development and test database migration
* Database consolidation
* Continuous replication

**Amazon DocumentDB** is a document database service that supports MongoDB workloads. (MongoDB is a document database program.)

**Amazon Neptune** is a graph database service.

* Highly connected datasets, such as recommendation engines, fraud detection, and knowledge graphs

**Amazon Quantum Ledger Database (Amazon QLDB)** is a ledger database service

* Review a complete history of all the changes that have been made to your application data

**Amazon Managed Blockchain** is a service that you can use to create and manage blockchain networks with open-source frameworks.

**Amazon ElastiCache** is a service that adds caching layers on top of your databases to help improve the read times of common requests.

* Supports two types of data stores: Redis and Memcached.

**Amazon DynamoDB Accelerator** is an in-memory cache for DynamoDB

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

# Module 6: Security

**Shared responsibility model** is where AWS is responsible for some parts of your environment, and you (the customer) are responsible for other parts.

**Customers: Security in the cloud** are responsible for the security of everything that they create and put in the AWS Cloud. Examples:

* Patching software on Amazon EC2 instances
* Setting permissions for Amazon S3 objects

**AWS: Security of the cloud** is responsible for security of the cloud. Examples:

* Physical security of data centers
* Hardware and software infrastructure
* Network infrastructure
* Virtualization infrastructure

**AWS Identity and Access Management (IAM)** enables you to manage access to AWS services and resources securely.

**Root user** the identity assigned when you first create your AWS account (think of as the “owner”)

**IAM user** is an identity that you create in AWS.

* Represents the person or application that interacts with AWS services and resources
* Consists of a name and credentials

**IAM policy** is a document that allows or denies permissions to AWS services and resources.

* Enables you to customize users’ levels of access to resources

**IAM group** is a collection of IAM users.

**IAM role** is an identity that you can assume to gain temporary access to permissions.

**AWS Organizations** consolidate and manage multiple AWS accounts within a central location.

* Automatically creates a **root**, which is the parent container for all the accounts in your organization

**Service control policies (SCPs)** enable you to place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access. Identities and resources can SCPs be applied to:

* An individual member account
* An organizational unit (OU)

**AWS Organizations (OU’s)** allows you to group accounts so you can easily manage accounts with similar business or security requirements.

* When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.

**AWS Artifact** is a service that provides on-demand access to AWS security and compliance reports and select online agreements. Consists of two main sections:

**AWS Artifact Agreements** can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations.

**AWS Artifact Reports** provide compliance reports from third-party auditors

**Customer Compliance Center** contains resources to help you learn more about AWS compliance.

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

* Originates from a **single** source

**Distributed denial-of-service (DDoS)** attack, multiple sources are used to start an attack that aims to make a website or application unavailable.

* Originates from **multiple** sources

**AWS Shield** is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.

**AWS Shield Standard** automatically protects all AWS customers at no cost.

**AWS Shield Advanced** is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.

**AWS Key Management Service (AWS KMS)** enables you to perform encryption operations through the use of **cryptographic keys.**

* **Multi-tenant**

**AWS WAF** is a web application firewall that lets you monitor network requests that come into your web applications.

* Uses web access control list (ACL) to block or allow traffic

**Amazon Inspector** helps to improve the security and compliance of applications by running automated security assessments

**Amazon GuardDuty** is a service that provides intelligent threat detection for your AWS infrastructure and resources.

* Continuously monitoring the network activity and account behavior within your AWS environment

**AWS Config** is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

**U2F security key** is a device that you can plug into a USB port on your computer.

# Module 7: Monitoring and Analytics

**Amazon CloudWatch** is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.

* Ability to create *alarms* that automatically perform actions if the value of your metric has gone above or below a predefined threshold
* *Dashboard* enables you to access all the metrics for your resources from a single location

**AWS CloudTrail** records API calls for your account.

* Includes the identity of the API caller, the time of the API call, the source IP address of the API caller
* Can filter events

**CloudTrail Insights** optional feature allows CloudTrail to automatically detect unusual API activities in your AWS account.

**AWS X-Ray** to analyze and debug serverless and distributed applications such as those built using a microservices architecture.

**AWS Trusted Advisor** is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.

Five categories:

* Cost Optimization
* Performance
* Security
* Fault Tolerance
* Service Limits



# Module 8: Pricing and Support

**AWS Free Tier** enables you to begin using certain services without having to worry about incurring costs for the specified period.

* New users are given 12 months free

Three types of offers:

* Always Free
* 12 Months Free
* Trials

AWS pricing categories:

* Pay for what you use.
* Pay less when you reserve.
* Pay less with volume-based discounts when you use more.

**AWS Pricing Calculator** lets you explore AWS services and create an estimate for the cost of your use cases on AWS.

Pricing Examples:

**AWS Lambda**

* For AWS Lambda, you are charged based on the number of requests for your functions and the time that it takes for them to run.
* Allows 1 million free requests and up to 3.2 million seconds of compute time per month
* Compute Savings Plans offer lower compute costs in exchange for committing to a consistent amount of usage over a 1-year or 3-year term (**Pay less when you reserve**)
* Pay only for compute time while your code is running

**Amazon EC2**

* You pay for only the compute time that you use while your instances are running (per second billing)
* Some workloads, you can significantly reduce Amazon EC2 costs by using Spot Instances

**Amazon S3**

**Storage -**You pay for only the storage that you use.

**Requests and data retrievals -**You pay for requests made to your Amazon S3 objects and buckets.

**Data transfer -**There is no cost to transfer data between different Amazon S3 buckets or from Amazon S3 to other services within the same AWS Region.

**Management and replication -** You pay for the storage management features that you have enabled on your account’s Amazon S3 buckets.

**Consolidated billing** feature of AWS Organizations enables you to receive a single bill for all AWS accounts in your organization

**AWS Budgets** you can create budgets to plan your service usage, service costs, and instance reservations.

* Supports for *alerts* when your service usage exceeds a threshold
* Automatically terminate resources when thresholds are exceeded

**AWS Cost Explorer** is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time.

**Cost Allocation Tags** is for improved usage categorization and more granular cost reporting.

**AWS Support Plans:**

**1) Basic Support** is free for all AWS customers. It includes access to whitepapers, documentation, and support communities.

**2) Developer Support** plan have access to features such as:

* Best practice guidance
* Client-side diagnostic tools
* Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together

**3)** **Business Support** plan have access to additional features, including:

* Use-case guidance to identify AWS offerings, features, and services that can best support your specific needs
* All AWS Trusted Advisor checks
* Limited support for third-party software, such as common operating systems and application stack components

**4) Enterprise Support** plan have access to features such as:

* *Application architecture guidance*, which is a consultative relationship to support your company’s specific use cases and applications
* *Infrastructure event management*: A short-term engagement with AWS Support that helps your company gain a better understanding of your use cases. This also provides your company with architectural and scaling guidance.
* A Technical Account Manager
* Access to online training with self-paced labs

**Technical Account Manager (TAM) provided enterprise level support and is** primary point of contact at AWS.

* They provide guidance, architectural reviews, and ongoing communication with your company as you plan, deploy, and optimize your applications.

**AWS Marketplace** is a digital catalog that includes thousands of software listings from independent software vendors (third party sources).

* AWS Marketplace offers products in several categories, such as Infrastructure Products, Business Applications, Data Products, and DevOps.

# Module 9: Migration and Innovation

**Cloud Adoption Framework (AWS CAF)** organizes guidance into six areas of focus, called **Perspectives**.

* **Business Perspective** ensures that IT aligns with business needs and that IT investments link to key business results.
* **People Perspective** supports development of an organization-wide change management strategy for successful cloud adoption.
* **Governance Perspective** focuses on the skills and processes to align IT strategy with business strategy.
* **Platform Perspective** includes principles and patterns for implementing new solutions on the cloud and migrating on-premises workloads to the cloud.
* **Security Perspective** ensures that the organization meets security objectives for visibility, auditability, control, and agility.
* **Operations Perspective** helps you to enable, run, use, operate, and recover IT workloads to the level agreed upon with your business stakeholders.

**6 strategies for migration:**

* **Rehosting** also known as “lift-and-shift” involves moving applications without changes.
* **Replatforming**, also known as “lift, tinker, and shift,” involves making a few cloud optimizations to realize a tangible benefit.
* **Refactoring** (also known as **re-architecting**) involves reimagining how an application is architected and developed by using cloud-native features.
* **Repurchasing** involves moving from a traditional license to a software-as-a-service model.
* **Retaining** consists of keeping applications that are critical for the business in the source environment.
* **Retiring** is the process of removing applications that are no longer needed.

**AWS Snow Family** is a collection of physical devices that help to physically transport up to exabytes of data into and out of AWS.

**AWS Snow Cone** is a small, rugged, and secure edge computing and data transfer device.

* features 2 CPUs, 4 GB of memory, and 8 TB of usable storage.

**AWS Snowball** offers two types of devices:

**Snowball Edge Storage Optimized**devices are well suited for large-scale data migrations and recurring transfer workflows, in addition to local computing with higher capacity needs.

* Storage: 80 TB
* Compute: 40 vCPUs, and 80 GiB of memory

**Snowball Edge Compute Optimized**provides powerful computing resources for use cases such as machine learning, full motion video analysis, analytics, and local computing stacks.

* Storage: 42-TB
* Compute: 52 vCPUs, 208 GiB of memory

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

* Transfer up to 100 petabytes of data

**Serverless** refers to applications that don’t require you to provision, maintain, or administer servers.

* AWS Lambda is an example

**Artificial intelligence (AI)**

* Convert speech to text with **Amazon Transcribe**.
* Discover patterns in text with **Amazon Comprehend**.
* Identify potentially fraudulent online activities with **Amazon Fraud Detector**.
* Build voice and text chatbots with **Amazon Lex**.

**Machine learning (ML)**

* **Amazon SageMaker** to remove the difficult work from the process and empower you to build, train, and deploy ML models quickly.

**Amazon Augmented AI (Amazon A2I)** provides built-in human review workflows for common machine learning use cases

* Content moderation and text extraction from documents.

**Amazon Polly** is a service that turns text into lifelike speech.

# Module 10: The Cloud Journey

**AWS Well-Architected Framework** helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud.

Five Pillars:

**Operational excellence** is the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

* Performing operations as code
* Annotating documentation
* Anticipating failure
* Frequently making small, reversible changes

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

* Automate security best practices when possible.
* Apply security at all layers.
* Protect data in transit and at rest.

**Reliability** is the ability of a system to do the following:

* Recover from infrastructure or service disruptions
* Dynamically acquire computing resources to meet demand
* Mitigate disruptions such as misconfigurations or transient network issues

Ex. Testing recovery procedures, scaling horizontally, automatically recovering from failure

**Performance efficiency** is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

**Cost optimization** is the ability to run systems to deliver business value at the lowest price point.

* Consumption model
* Analyzing and attributing expenditure
* Using managed services

**6 Advantages of cloud computing:**

**Trade upfront expense for variable expense.**

* Instead of investing heavily in data centers and servers before you know how you’re going to use them, you can pay only when you consume computing resources.

**Benefit from massive economies of scale.**

* Economies of scale translate into lower pay-as-you-go prices.

**Stop guessing capacity.**

* Instead of paying for resources that are unused or dealing with limited capacity, you can access only the capacity that you need, and scale in or out in response to demand.

**Increase speed and agility.**

* The flexibility of cloud computing makes it easier for you to develop and deploy applications.

**Stop spending money running and maintaining data centers.**

* A benefit of cloud computing is the ability to focus less on these tasks and more on your applications and customers.

**Go global in minutes.**

* The AWS Cloud global footprint enables you to quickly deploy applications to customers around the world, while providing them with low latency.