CLF-C02 Cloud Practitioner Study Guide

AWS Core Concepts and Services

Abstract

The Cloud Practitioner exam tests the key concepts in the AWS system architecture, including the Well-Architected Framework and core AWS technologies. This study guide seeks to concisely and efficiently cover all relevant topics related to the exam.

info@CyberVista.com

Overview

Thank you for purchasing this CyberVista practice test.

This study guide is designed to help you prepare for the **CLF-C02 Cloud Practitioner Exam** quickly and effectively. This study guide is organized into two parts:

- **Core Topics Compendium** – This section contains focused coverage of the essential Cloud Practitioner topics. The "What to Use When" tables provide guidance on using AWS services. The versus or "vs" charts allow you to compare features of different AWS technologies.
- **AWS Services Dictionary** – This section contains brief descriptions of key AWS technologies in alphabetical order. **Tip:** Try and memorize as many of these as you can for a more efficient test experience. Many of these current AWS technologies will be covered in this exam.

This study guide alone may not be sufficient to pass the exam. Additional preparation recommendations include:

- Further study of the key topics.
- Taking practice tests.
- Studying the tutorials included in the practice test diagnostic feedback. These contain detailed information on specific exam topics.

You can send us any feedback related to this study guide or practice tests at: feedback@CyberVista.com.

Contents

Core Topics Compendium

Introduction to Cloud Computing

What is Cloud Computing?

Cloud computing is a service providing access to computing resources on demand over the Internet with pricing based on actual usage. Amazon Web Services (AWS) is a provider of cloud computing services.

Benefits of Cloud Computing with AWS

- **Security** – Using a shared responsibility model and best practices, you can help ensure greater safety of your operations using the AWS cloud. These practices include enforcing strong permission policies and performing data encryption.
- **Reliability** – Helps ensure your workloads can perform correctly, handle failures, and automatically fix any issues that may arise. This also covers data backups, fault isolation, and ensuring your systems are prepared for disaster scenarios.
- **High Availability** – Ensures that your applications are always ready to serve customers promptly with little downtime. A standard measure of availability is five 9s which corresponds to a system being available 99.999% of the time.
- **Elasticity** – The ability to scale your computing resources to match consumer demand without provisioning resources manually or guessing future capacity needs.
- **Agility** – The ability to swiftly deploy new applications by removing unnecessary operational overhead, allowing development teams to focus on product creation and innovation.
- **Pay-as-you go pricing** – A flexible payment option where a cloud consumer only pays for resources consumed.
- **Scalability** – Using serverless technologies like AWS Lambda and DynamoDB to easily adjust your applications to meet growing demands on a massive scale.
- **Global Reach** – Using edge locations and data centers around the world, AWS Cloud Global Infrastructure can improve user experience with low latency for end-users regardless of their location around the globe.
- **Economy of scale** – Providing lower pay-as-you-go (PAYG) pricing due to accumulated cloud usage from a very large pool of cloud customers.

Cloud Deployment Models

There are three main cloud deployment models:

- **Cloud-based** (aka Cloud native) – This deployment includes applications that are fully functional in a cloud and have no portions which are running on-premises.
- **On-premises** (aka private) – In this, all the infrastructure and applications that are part of the cloud or virtualization system are running on systems which are inside a company's on-premises data center.
- **Hybrid** – This shares infrastructure and applications between an on-premises environment and a cloud.

Compute in The Cloud

Computing Services

Amazon Elastic Compute Cloud (EC2) – EC2 is a service that provides computing capability using virtual servers.

AWS Lambda – This allows you to perform serverless computing. When using AWS Lambda, you upload your code to a lambda function and then configure a trigger to initiate .

Instance Types

The instance type of an Amazon Elastic Compute Cloud (EC2) instance specifies the hardware of the host computer that is utilized for the instance. The naming convention used for instance types is indicated below using the example d7gn.xlarge:

- d – instance family
- 7 – instance generation
- g – processor family
- n – additional capability
- xlarge – instance size

These are the key Amazon EC2 instance types and their uses:

- **Memory optimized** – Ideal for all workloads with large datasets within memory. These can include high-performance databases.
- **Compute optimized** – They have high-performance processors suited for workloads which require processing for large batches.
- **Storage optimized** – Suited for workloads which need large amounts of sequential read and write access to datasets which reside on local storage, such as data warehousing.
- **General Purpose** – Suited for everyday tasks like enterprise data applications which use a balanced share of resources for computing, storage, and networking.
- **Accelerated computing** – Designed for application and game streaming workloads and graphics processing applications.

What to use when	
Memory optimized	Real-time processing of unstructured data
Compute optimized	Dedicated servers for gaming
Storage optimized	Online transaction processing (OLTP) systems
General purpose	Small databases and application servers
Accelerated computing	Floating point calculations, data pattern matches, video processing

An Amazon Machine Image (AMI) can be used to launch an instance. AMIs can contain Elastic Block Storage (EBS) snapshots which serve as backups.

EC2 Instance Pricing

Purchase Models:

- Savings Plan – For committed and consistent amount of usage of compute resources for a one- or three-year term. This saves up to 72% of costs over On-Demand.
- Reserved Instances – These provide a billing discount of up to 75% when applied, compared to using On-Demand instances. You can buy these for a one- or three-year term and consistent use is not required. You can buy Standard and Convertible Reserved instances for a period of one or three years. You can also buy Scheduled Reserved instances for a one-year period.
- On-Demand Instances – These are for short term, irregular workloads with no interruptions. You pay only for actual usage. These are best suited for developing and testing applications.
- Spot Instances – These are for workloads that can be interrupted. These can save up to 90% of the costs of On-Demand instances.

What to use when	
On-Demand Instances	Irregular workloads that are non-interruptible
Spot Instances	Irregular workloads that are interruptible
Savings Plan	For committed and consistent usage
Reserved Instances	For inconsistent usage over a long term

Dedicated or Reserved Capacity Models:

- Dedicated hosts – This is the most expensive option. You are provided with a physical host and EC2 instances that are exclusively yours. You can use your existing licenses. These hosts run in a Virtual Private Cloud (VPC) on dedicated hardware.
- On-Demand Capacity Reservations – This allows you to reserve Amazon Elastic Compute Cloud (EC2) compute capacity in an Availability Zone for any length of time. This makes it ideal for business-critical workloads that need guaranteed assurance for long- and short-term compute capacity. Capacity Reservations are useful for business-critical events, regulatory requirements, and disaster recovery situations.

Auto Scaling

Amazon EC2 Auto Scaling – This allows you to add or remove EC2 instances automatically to match changing demand. This helps ensure application availability. Scaling can be either dynamic, which scales based on changing demands, or predictive, which performs scaling based on predicted demands. Both these scaling methods can be used together for faster scaling.

Scaling up – To increase the power of the existing machines.
Scaling out – To increase the number of machines.

Auto Scaling Group – You implement Auto Scaling using an Auto Scaling group with your application. When you configure an Auto Scaling group you need to specify the minimum, desired, and maximum capacity of the instances in the group.

AWS Elastic Load Balancing (ELB) – ELB is used for distributing traffic among EC2 instances. ELB ensures that no EC2 instance is left unused and similarly, no instance is used more than required, by sharing traffic evenly across several EC2 instances. ELB is a managed service which operates at a regional level ensuring high availability automatically and supporting a single Region. It is the single point of contact for an Auto Scaling group.

Designing for Failure

You need to design your system architecture to ensure that the system will still be operational even if multiple components of the system fail. This provides fault tolerance and high availability.

Monolithic systems have a tightly coupled architecture. When one component fails, the entire system fails.

Microservices architecture is loosely coupled. If one component fails, the entire system is not affected. Such systems utilize messaging options between components that use message queues. One component leaves a message in a queue for another component, and when the recipient component is free to take in a new message, it can retrieve it from the queue.

Messaging Services

Simple Notification Service (SNS) – SNS provides a publish/subscribe (pub-sub) service. It allows a publisher to publish messages on SNS topics to multiple subscribers. These subscribers can include email addresses, AWS Lambda functions, and web servers.

Simple Queueing Service (SQS) – SQS is a service that provides message queueing. With SQS you can allow messages to be sent, received, and stored between several components of applications and microservices.

Container Orchestration

Container orchestration is the process of managing containers running on a single or cluster of EC2 instances. Docker is an example of a platform that provides a way to use software in containers using operating system-level virtualization technology.

Elastic Container Service (ECS) – This allows you to use Docker containers and utilize API calls for launching and stopping the containers.

Elastic Kubernetes Service (EKS) – This allows you to use Kubernetes on AWS. Kubernetes is an open-source technology for deploying and managing containerized software.

Elastic Container Registry (Amazon ECR) – This is a secure and scalable container image registry service that is managed by AWS.

Serverless Computing

AWS Lambda – This provides serverless computing. Your code is uploaded to Lambda and set to run a on a pre-set trigger. The code runs only when triggered and you pay only for the compute time.

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

What to use when	
Virtual servers	You need to access underlying systems like the OS
Serverless computing	Less need to manage servers so you can focus on developing new products

Global Infrastructure and Reliability

Regions and AZs

Availability Zone (AZ) – An AZ is a fully isolated portion of the AWS Global Infrastructure. It is a single or group of data centers inside a Region. Each data center has its own connectivity, power systems, and networking infrastructure. AZs are located tens of miles apart or more. For reliability, you need to launch several EC2 instances and spread these out across several Availability Zones.

Region – This is a geographical region with many locations which are isolated from each other. The choice of a Region is based on proximity, compliance, services, and costs. Some AWS services operate at the Region level and work across several AZs similar to using load balancing with ELB.

Resource Provisioning

Provisioning of resources can be done using the AWS Management Console, Command Line Interface (CLI), or Software Development Kits (SDKs).

SDKs - Allow for provisioning and interaction with AWS services using Application Programming Interfaces (APIs) created for platforms and programming languages like C++, Java, and .NET.

CLI – This allows you to use scripts to automate actions for AWS services and applications. You can start and stop EC2 instances and add them to Auto Scaling groups.

Elastic Beanstalk – This lets you quickly deploy and scale applications onto AWS without having to write code for building capacity, load balancing, scaling, and health monitoring.

AWS CloudFormation – Allows you to provision resources using templates written in YAML or JSON. This is an infrastructure as code service.

AWS Outposts – This runs infrastructure using a hybrid cloud. It extends AWS infrastructure and services to an on-premises data center.

AWS Quick Starts – These are automated reference deployments for deploying workloads into an AWS environment. They are built by AWS solutions architects and AWS partners. They allow you to use popular AWS technologies with adherence to AWS best practices so that a working environment can be set up quickly.

AWS Cloud9 – This provides an Integrated Development Environment (IDE) which is cloud-based. You use Cloud9 for writing, running, and debugging the code you create for your applications. Cloud9 has a built-in terminal and supports various programming languages and runtime debugging systems.

What to use when	
Elastic Beanstalk	Deploying applications fast
CloudFormation	Running infrastructure as code
SDKs	Accessing AWS services from your application
CLI	Creating scripts for resource provisioning

Networking

Virtual Private Cloud (VPC) – This is an isolated part of the AWS cloud which is further divided using subnets.

AWS Virtual Private Network (VPN) – This comprises two services: AWS Client VPN and AWS Site-to-Site VPN. You use AWS Client VPN for connecting users securely to on-premises networks or AWS. You use AWS Site-to-Site VPN for securely connecting a branch office or on-premises network to an AWS Virtual Private Cloud (VPC).

Subnets – A subnet is a section of a VPC where resources can be grouped based on their security or functional requirements. Public subnets are kept Internet-facing and have front-end EC2 instances. Private subnets can also have data storage using the Relational Database System (RDS).

AWS Transit Gateway – You can use AWS Transit Gateway or Software Site-To-Site VPN for integrating multiple VPCs into a larger network. The best way to achieve VPC connectivity between VPCs is to ensure that you use IP address ranges which do not overlap. For this you need to use a unique Classless Inter-Domain Routing (CIDR) range for each VPC.

Connecting VPCs – You can use the following design options when creating VPC to VPC connectivity:

- **VPC Peering** – AWS provides network connectivity between two VPCs
- **AWS Transit Gateway** – AWS provides regional router connections between VPCs
- **Software Site-to-Site VPN** – VPN connections between VPCs using software appliances
- **Software VPN-to-AWS Managed VPN** – Connectivity between VPCs through software appliances to VPN connections
- **AWS Managed VPN** – Customer-managed VPC to VPC routing using IPSec VPN connections
- **AWS PrivateLink** – AWS uses interface endpoints to provide network connectivity between two VPCs

Internet Gateway (IGW) – A VPC connects to the Internet using an IGW.

Virtual Private Gateway (VPG) – For a private connection from a VPC to a data center or corporate network you use VPG and a Virtual Private Network (VPN).

Network Address Translation (NAT) Gateway – A private subnet accesses the Internet using a NAT gateway.

Network Access Control Lists (NACLs) – An NACL is a virtual firewall for controlling traffic going in and out of a subnet. NACLs are stateless and work at subnet level. Default NACLs allow all packets in and out. Custom NACLs deny all.

Security Groups – A security group is a virtual firewall that protects an EC2 instance. These perform stateful packet filtering and work at the instance level. Default Security Groups deny all traffic in and only allow traffic out.

AWS Web Application Firewall (WAF) – This controls requests coming in from a network into your Web applications. AWS WAF permits or denies traffic based on a Web Access Control List (ACL).

Virtual Private Network (VPN) – You connect to a VPC securely over the Internet using a VPN.

AWS Direct Connect – This is used to connect directly to a VPC from an on-premises center via a high-speed dedicated fibre optic connection. Direct Connect helps reduce network costs and increases bandwidth.

AWS PrivateLink – This allows you to connect resources inside your VPC to services using private IP addresses. This works as if these services are being hosted inside your VPC.

What to use when	
VPN	Connect to a VPC over the Internet using a VPN
Direct Connect	Connect directly to a VPC from a data center using fibre optic cables

AWS Local Zones – This is an AWS technology that maintains AWS resources such as database, storage, and compute near industry and large population centers. This ensures low latency in application access for your users. Local Zones extend the concept of an AWS Region and support AWS Direct Connect and have individual Internet connectivity.

AWS Wavelength Zones – These are zones inside a carrier location where an AWS Wavelength infrastructure has been deployed. Wavelength is an infrastructure which is engineered to run workloads that need low-latency performance across mobile networks.

Global Networking

Domain Name System (DNS) – This is the phone book of the Internet which maps domain names (www.example.com) to IP addresses (192.268.4.6).

Route 53 – This provides DNS services that include transferring DNS records for any existing domain names from other registrars and registering new domain names. It also connects users to infrastructure inside or outside of AWS.

CloudFront – This is a Content Delivery Network (CDN) which caches copies of data at locations around the world that are near customers (edge locations) for high speeds and low latency. It uses geolocation headers for country-level, location-based, web content personalisation.

Origin – This is the server that CloudFront gets files from.

Edge Location – This is the site used by CloudFront to cache copies of content for faster delivery.

AWS Global Accelerator – This service improves the performance and availability of global applications by utilizing the AWS global network infrastructure.

Storage and Databases

Object and Block Storage

Storage can be object- or block-level. Block-level storage performs like hard drives. Object-level storage has data, metadata, and keys. The key difference between object and block storage is that when data in block storage is changed, only the changed blocks are updated, while the entire object is changed in object storage.

Storage Options

Instance store volumes – These provide temporary physical storage with an EC2 instance's current host. This option can be used for data that is temporary.

Elastic Block Storage (EBS) Volumes – This provides persistent block storage across changing physical hosts. Suitable for data that needs to be kept long term. You use EBS with EC2 instances. You can define, provision, and attach EBS volume to an EC2 instance. You take snapshots for backups. These are incremental backups.

Elastic File System (EFS) – This is a managed file system which scales automatically to petabyte levels with no interruptions to applications. EFS is a regional service and stores data across several AZs allowing data to be accessed concurrently from each AZ in the Region. With AWS Direct Connect you can access EFS using on-premises servers.

EBS	vs	EFS
Has one AZ		Has several AZs
Does not scale automatically		Scales automatically
Needs the instance and EBS volume to be in the same AZ		Allows concurrent access across all AZs in a Region

Amazon Simple Storage Service (S3) – Amazon S3 allows you to store an unlimited number of objects, with each object up to 5TB in size, in S3 buckets. The files stored on Amazon S3 can be of any type including images, videos, documents, and more. Using the versioning feature on Amazon S3 can help protect objects from accidental deletion. You cannot attach an S3 bucket to an EC2 instance. Instead, you would use EBS or instance store volumes with EC2 instances.

S3 Storage Classes

Amazon S3 offers many storage classes which vary based on how available the data needs to be and how often the data needs to be retrieved. Some of these storage classes are:

- **S3 Standard** – The most expensive tier, used for frequently-accessed data and stores data cross 3 AZs. It is best suited for data analytics, websites, and content delivery. It offers 11 9s of durability.
- **S3 Standard – Infrequent Access (IA)** – This has the same availability as S3 Standard with a lower storage cost but a higher retrieval cost. This is ideal for data that is accessed infrequently.
- **S3 One Zone – Infrequent Access (One Zone IA)** – This is more affordable than S3 Standard and stores data in a single AZ. Use this when lower-cost storage is required, and you can reproduce data if the AZ fails.
- **S3 Intelligent-Tiering** – This is for data with a changing or unknown frequency of access. It requires a monthly fee for monitoring and automation for each object. S3 automatically moves objects not accessed for 30 days into the S3 Standard IA tier. If an object is accessed in the S3 Standard IA tier, S3 moves it into S3 Standard.
- **S3 Glacier** – This is a low-cost storage option meeting data archiving requirements. Retrieval of data stored in this class can take a few minutes to a few hours.
- **S3 Glacier Deep Archive** – This is the lowest-cost storage class and is suitable for archiving requirements where it is acceptable for data retrieval to take up to 12 hours. You can use S3 Static Website hosting to create instant websites.

S3 Lifecycle policy – This automatically moves data between S3 storage tiers. It archives or deletes data as specified.

S3 Transfer Acceleration – This allows fast and secure transfer of files over long distances between a client and an S3 bucket.

EBS	vs	S3

For frequent changes and edits		For uploading complete objects and requiring infrequent changes
Used with EC2 instances which are virtual servers		Serverless, does not need an EC2 instance
Good for doing micro-edits on massive files		Good when millions of files need to be indexed and accessed via the Web

What to use when	
Instance store	Temporary storage with EC2
EBS	Long-term storage with EC2
EFS	Storage with fault tolerance and high availability
S3 Standard or S3 IA	High Availability Object Storage
Glacier	Archiving
S3 Intelligent Tiering	When data access frequency is uncertain

AWS Storage Gateway – This technology provides secure and seamless access for on-premises systems and applications to unlimited storage on AWS. Access is provided using Amazon S3, Tape Library, and Amazon FSx. Storage Gateway can be accessed by endpoints like Amazon VPC and the Internet.

Database Options

Relational Database Service (RDS) – This is a fully managed service where provisioning hardware, patching, and performing backups is handled by AWS. It also offers encryption and rest and transit for several of its database engines. RDS is available for Amazon Aurora, MySQL, PostgreSQL, MariaDB, Oracle Database, and Microsoft SQL Server. RDS usage costs are based on instance hours, storage GBs, transfers (requests), and backups.

Amazon Aurora – This is a relational database operating at an enterprise-level, and it is five times faster than MySQL and three times faster than PostgreSQL. It replicates six copies of data across three Availability Zones and backs up data to Amazon S3.

DynamoDB – This is a non-relational serverless database which is purpose-built and fully managed. It has a very fast millisecond response time and is highly scalable. It can handle millions of requests per second.

Non-relational databases – These are also called NoSQL databases and store data as key (items) and values (attributes).

DynamoDB	vs	RDS
Non-relational data using key value pairs		Relational data using schemas
For contact lists and variable content		For business analytics and ecommerce
Holds vast unstructured data		Holds schema-based data accessed via SQL
Serverless		Server-based
Unlimited table size		Table size limited by underlying database engine

Amazon Redshift – This is used for a scalable data warehousing solution. It performs big data analytics and collects data from multiple sources. It is designed for business intelligence workloads and has nodes running into petabyte sizes. It allows SQL to query exabytes of data in data lakes.

AWS Database Migration Service (DMS) – This moves existing databases to the cloud with no disruptions to the original database. During migration DMS keeps the source database operational, reducing downtime for applications. DMS can be used for database consolidation, replication, or testing.

Homogenous migration – This is when source and destination databases are of the same type.

Heterogenous migration – This is when source and destination databases are of different types and require schema conversion.

What to use when	
RDS	Schema-based relational data for business analytics
DynamoDB	Unstructured non-relational data with wide scalability and millisecond response time
Redshift	Data warehousing

Note: There is no single database option for all purposes.

DocumentDB – This is used for document management, content management, and catalogs. It can be used for MongoDB workloads.

Amazon Neptune – This is a graph database used for social webs and recommendation engines. It is also useful for fraud-detection applications.

Quantum Ledger DB (QLDB) – This provides an immutable transactions database that can be used for verifying changes to the data of applications. It stores the complete history of all these changes.

Managed Blockchain –This is for creating and managing blockchain networks using open-source frameworks. Blockchain uses a ledger system that provides complete immutability for multiple parties to perform transactions. The data is shared without the need for a central managing authority.

ElastiCache – This is a database accelerator that allows you to have microsecond latency in application and database performance and meet large scaling needs using in-memory caching. ElastiCache provides compatibility with Memcached and Redis. It is used for business intelligence, real-time transactions, gaming leaderboards, and is suitable for Online Analytical Processing (OLAP).

DynamoDB Accelerator (DAX) – This improves response times for DynamoDB to microseconds using in-memory caching.

Amazon MemoryDB for Redis – This is an in-memory database suited for workloads that require a very fast primary database that is Redis-compatible. Redis is an open source in-memory data structure. It can be used as a streaming engine, message broker, cache, and database.

Amazon ElastiCache for Redis – This is a web service for managing and scaling cache environments or in-memory data stored in the cloud.

What to use when	
Amazon MemoryDB for Redis	Workloads require a durable database with extremely fast performance
Amazon ElastiCache for Redis	Caching workloads and for accelerated access to an existing primary database

Security

Shared Responsibility Model

The AWS Shared Responsibility Model – This specifies that AWS is responsible for security **of** the cloud while the customer is responsible for security **in** the cloud.

Customer's Responsibility – These include patching the OS running on EC2 instances, creating security groups, firewall configuration, managing user accounts, access rights, and permissions, AMIs, and encrypting data at the client and server side.

AWS's Responsibility – Managing the host OS of machines running virtual servers, the virtualization systems, network infrastructure including global infrastructure, the physical servers that run EC2 instances, and data centre security.

Customer's Responsibility	vs	AWS's Responsibility

Managing software on EC2 instances		Managing virtualization infrastructure
Creating security groups		Securing the data centers
Managing IAM users and permissions		Securing networking infrastructure
Security of AWS Lambda code		Patching of RDS database engines

Identity and Access Management

Identity and Access Management (IAM) – Provides secure access to AWS resources through IAM users, groups, and roles.

AWS Identity and Access Management (IAM) Identity Center – This system allows centrally managed SSO access to AWS accounts and applications. SSO authentication allows users to securely authenticate to multiple applications using one set of credentials. You can provide federated access to users using AWS IAM Identity Center.

IAM Policies – These are JSON documents that specify the permissions an IAM user has to various AWS resources and services. You must always follow the principle of least privilege when creating IAM policies.

An IAM Policy has 3 key sections: Effect, Action, and Resource. These allow you to:

Effectively Allow or Deny an API **Action** on a specific **Resource.**

AWS Managed Policy – These are created and managed by AWS and provide permissions for common use cases making the process easier for new AWS users to assign permissions to users and groups.

Customer Managed Policy – You can designate the specific permissions required for a job role following the principle of least privilege. You can create this policy by customizing an existing AWS managed policy.

The principle of least privilege – You implement this by only granting IAM users and roles the minimum permissions they need and then only add other permissions as required.

IAM User – This is an AWS identity consisting of a name and credentials. It represents a person or application which can access AWS resources and services. A new IAM user has no permissions.

IAM Group – You can assign several IAM users to IAM groups and then attach IAM polices to those groups which will then apply to all users within that group.

IAM Role – This is an identity that can be given to a user for attaining temporary permissions. When an IAM user or service assumes an IAM role, they discard all their other permissions and assume the ones specified in the IAM role. Instead of creating individual users in IAM you can federate existing corporate credentials and map those to IAM roles.

Multi-factor Authentication (MFA) – This requires that, besides using a username and password, you also require an authentication code from an MFA device to successfully sign into your AWS account.

Root user – This is created when you create an AWS account. It has full permissions to perform any action inside the account. For security purposes, you should activate MFA for the root account.

What to use when	
Root user	For changing the AWS support plan or account email address
IAM user	For everyday tasks
IAM role	For temporary access

Programmatic Access

Programmatic Access to AWS accounts – An **access key ID** and a **secret access key** are required to use AWS programmatically. This allows AWS to verify your identity across calls made programmatically.

Account Management

AWS Organizations – This provides one place for managing several AWS accounts. Allows for consolidated billing and the hierarchical grouping of accounts.

Organizational Units (OUs) – OUs are groups of related AWS accounts. Several accounts can be grouped into Organizational Units (OUs) based on shared requirements for security or business.

Service control policies (SCPs) – These let you restrict access to API and services for roles and users inside each account. An SCP can be applied to the organization root, member accounts, and OUs. This includes all IAM users, groups, and roles in member accounts as well as the AWS account root user. An SCP, when applied to an OU, is extended to all its member accounts.

Consolidated billing – This allows you to view details on charges incurred by each account and to pay for all AWS accounts in an organization through a single bill. It also provides bulk discounts and savings across several member accounts in an organization.

AWS account root user – The AWS account root user is an identity created when you first create an AWS account. You can access this identity by using the email address and password used to create the AWS account. The root user account should only be used for required tasks such as:

- Modifying account settings, including account name, root user password, email address, and root user access keys.
- Closing an AWS account.
- Restoring IAM user permissions.
- Viewing specific tax invoices.
- Activating AWS IAM access to billing and cost management.

Compliance

AWS Artifact – This provides access to third-party compliance reports validating AWS's adherence to compliance standards such as the Health Insurance Portability and Accountability Act (HIPPA). Customers can request documentation from AWS proving that AWS data centers are being run within compliance and security standards. AWS Artifact has two sections:

- **AWS Artifact Agreements** – This allows you to sign agreements with AWS which specify how you use different kinds of information on AWS services. This is to verify compliance with regulations such as HIPAA.
- **AWS Artifact Reports** – This provides you with compliance reporting from third-party auditors. You can use these reports when you are creating an application and need information for compliance to various global regulatory standards.

AWS Compliance Center – This provides information related to compliance in one centralized location. This includes for services which enable compliance, as well as whitepapers like AWS Risk and Security, which provides details on security compliance with AWS.

AWS Audit Manager – This service provides continuous auditing of AWS usage for simplifying management compliance and risk with industry standards and regulations. Using Audit Manager, you can oversee stakeholder reviews of existing controls during audits. This also allows you to create reports that are audit-ready with minimal manual work.

AWS Control Tower – This is a service that allows you to manage a multi-account AWS system and orchestrate several AWS services, such as AWS Organizations and AWS IAM Identity Center. It provides landing zones, which are environments that contain all the organizational units (OUs), users, and resources that you need to remain within compliance.

Governance

AWS Data Exchange – This allows you to locate and use third-party information that is related to sustainability. This provides access to data sets accessible through the Open Data Sponsorship Program and Amazon Sustainability Data Initiative. AWS works with companies to make Environmental, Social & Governance (ESG), weather, satellite imagery, and air quality data accessible to clients.

Licensing

AWS License Manager – This is an AWS service that simplifies managing software licenses from multiple vendors, including IBM, Oracle, SAP, and Microsoft, through a centralized system. This covers both your AWS and on-premises systems. AWS License Manager also lets you change license types between bring-your-own-license (BYOL) and AWS-provided licenses with your licensed media. Using BYOL opportunities can help you save costs on cloud infrastructure.

Security Tools

AWS Key Management Service (KMS) – This allows you to perform data encryption using cryptographic keys. A cryptographic key is a random string of several digits which is used for encrypting or decrypting data. AWS KMS allows you to manage and control the usage of these keys.

AWS Web Application Firewall (WAF) – This provides protection to Web applications from common exploits and bots. WAF controls requests coming into your Web applications and permits or denies traffic based on a Web Access Control List (ACL). WAF works in conjunction with Amazon CloudFront as well as Application Load Balancer.

AWS Firewall Manager – This is a service for security management and enables you to configure and manage firewall rules centrally across accounts and applications inside AWS Organizations. You can also enforce a set of security rules to keep new resources and applications within compliance using Firewall manager.

Amazon Inspector – This provides vulnerability assessment services ensuring security and compliance of an AWS system. It automatically performs vulnerability scans of resources and their non-adherence to best practices, and then provides a detailed report with each security finding prioritized by severity levels.

Amazon GuardDuty – Provides intelligent threat detection via machine learning for AWS resources and infrastructure by analysing data from various sources, including VPC flow logs and DNS logs.

AWS Shield – This is a managed service for protection from distributed denial of service (DDoS) attacks and offers automatic mitigations which reduce application downtime and latency. It is available in two tiers: Shield Standard which is free and Advanced which is subscription-based.

- **Shield Standard** – This protects applications from the most common DDoS attacks.
- **Shield Advanced** – This can detect complex DDoS attacks and provides detailed diagnostics. It can be integrated with Route 53, CloudFront, and Elastic Load Balancing.

Some common DDoS attacks and defenses:

- **SlowLoris Attack** – An attacker pretends to have a slow connection to exhaust the front end of your application. The defensive action uses Elastic Load Balancing, which is scalable and operates at the Region level.
- **User Datagram Protocol (UDP) Flood attack** – An attacker redirects the response to queries to your server in order to slow down your server. The defense is using Security Groups which only allow approved request traffic.

What to use when	
Shield	DDoS protection
GuardDuty	Intelligent threat detection using machine learning
WAF	Protection from SQL Injection and Cross-Site Scripting
Inspector	Vulnerability assessment based on best practices

AWS Security Hub – Provides a detailed view of the security situation on your AWS deployment. It helps protect your AWS environment using security best practices and industry standards. Security Hub gets data from various sources including AWS services, accounts, and third-party products.

Security Best Practices

Some key IAM security best practices include:

- Never use your AWS account root access key and use strong security measures to ensure it cannot be accessed by others.
- Perform encryption of data in transit and at rest.
- Use AWS services to check for threats.
- Use IAM roles to assign permissions for performing tasks.
- Use the principle of least privilege for granting permissions.
- Review and validate all your IAM policies to ensure their security.

Monitoring and Analytics

Monitoring Services

CloudWatch – This lets you monitor your AWS infrastructure and resource metrics in real-time from one dashboard. You can also create alarms based on metrics, which can also use SNS. It helps reduce Mean Time to Recovery (MTTR) and improve Total Cost of Ownership (TCO).
CloudTrail – This service logs every API and request made on the system. It records the API caller's identity and source IP address. It can save logs indefinitely in S3 buckets. This helps maintain security audit logs. You can also filter events based on time of occurrence.

CloudTrail Insights – This helps detect unusual activity in your AWS account.

CloudWatch	vs	CloudTrail
Used for watching AWS resources		Keeps a record or trail of API calls

AWS Trusted Advisor – This tool provides guidance on how to provision your AWS resources based on AWS best practices. It continuously monitors your AWS resources and recommends actions to optimize your environment. Trusted Advisor focuses on five key pillars:

- **Cost Optimization** – Identifies underutilized resources like instances or idle databases that can be stopped or deleted to save costs.
- **Performance** – Recommends ways to improve the throughput of resources, such as analyzing how an EBS volume's performance might be tied to its associated EC2 instance type.
- **Security** – Identifies security gaps like weak password policies, lack of MFA for the root account, or public access settings for EC2 instances.
- **Fault Tolerance** – Recommends best practices for building redundancy, such as ensuring EBS volumes have snapshots and EC2 instances are launched across multiple Availability Zones (AZs).
- **Service Limits** – Monitors your usage of AWS services against designated quotas or limits. For example, it might alert you if you're approaching the maximum number of VPCs allowed in your region.

AWS X-Ray – This provides detailed data on requests that your application serves. It contains tools that allow you to gain insights into all the possible issues that may exist within the application as well as methods for optimization.

Pricing and Support

Data Transfer Charges

Free – Data transferred from the Internet into AWS is not charged. Inbound data transfer across all Regions and services in AWS is free. Data transfer within an Availability Zone also does not incur any charges. An exception is VPC peering connections where data transfer charges are applied to ingress/egress traffic crossing Availability Zones. Replication between primary and standby instances in separate Availability Zones also does not incur charges.

Chargeable - Data transferred across AWS Regions is charged. All traffic crossing regional boundaries incurs costs. To reduce costs, you can use cross-Region data transfer only when business needs demand it. For an AWS resource, you incur charges for both outbound and inbound traffic in a data transfer inside an AWS Region.

Pricing

AWS Free Tier – This provides free offers for evaluating AWS services and products. There are three types of free offers:

- Always Free – AWS Lambda allows one million requests a month free and DynamoDB provides 25 GB free.
- 12 months free – Amazon RDS and EC2 allow 750 hours of usage a month free for 12 months.
- Trials – Amazon SageMaker and RedShift allow 2 months of free trial usage.

AWS Pricing – Certain usage is free up to a specified limit and you can save by reserving usage in advance and by using higher volumes.

AWS Billing and Cost Management Dashboard – This is used for analysing usage versus costs. It displays service costs by AWS Region.

AWS Budgets – This allows you to create budget plans for instance reservations and service usage and costs. You can set alerts for when expenditure exceeds or is predicted to exceed a pre-set threshold. It also allows you to view forecasts.

AWS Billing Conductor – This service provides custom billing features supporting chargeback and showback workflows for AWS Enterprise customers and solution providers. You can customize an alternative version of monthly billing information using Billing Conductor. You can also create and display rates to specific customers across a given billing period.

AWS Pricing Calculator – This provides you with all the necessary details for your cloud deployment use case and then gives you a cost estimate which you can export or share.

AWS Pricing API (or Price List API) – This provides programmatic access to AWS pricing data for predicting and managing AWS services costs. The API allows access to a pricing index allowing a customer to retrieve detailed pricing information for a listed AWS service.

AWS Cost Explorer – This shows costs associated with AWS resources like EC2, Managed Blockchain (AMB), etc. You can also view costs for resources grouped by tags. It provides historical cost data for up to 12 months. The top 5 AWS services are the default view.

Support

AWS Support Plans – AWS offers five support plans:

- **Basic support** – This plan is free for all AWS customers and provides access to support communities, whitepapers, and documentation. It provides support from AWS for billing and service limit issues. This plan also has access to selected Trusted Advisor checks.

- **Developer**, **Business** and **Enterprise support** – These plans all have benefits that you can build onto the basic support plan, as additions. All three plans offer pay-by-the-month pricing with no long-term commitments necessary. The Developer support plan is the most affordable. Each allows unlimited technical support cases. The Business and Enterprise plans have access to all Trusted Advisor checks and cost more, respectively.
- **Enterprise On-Ramp support** – This plan provides 24/7 support from engineers, technology, and tools for managing your system's health. It also provides architectural guidance based on your applications.

Technical Account Manager (TAM) – The Enterprise On-Ramp and Enterprise support plans provide access to a TAM who provides feedback and guidance and communicates with your company as you deploy and run applications with AWS.

What to use when	
AWS Support	For best practices and troubleshooting
Technical Account Manager	For guidance and architecture reviews
Trusted Advisor	For automated real-time guidance and alerts

AWS Support API – This allows you to create support cases programmatically, removing the need to create support cases using the AWS Support Center.

AWS Marketplace – This is digital library contains thousands of third-party software from varying applications and across industries. You can view detailed data on each software listing, including user reviews, pricing options, and support plans. It provides a one-click deployment of a full product that runs on AWS.

Migration and Innovation

Migration Planning

AWS Cloud Adoption Framework (CAF) – This provides guidance for AWS migration. It offers the following resources:

Non-technical planning:

- **Business** – Information for moving to a business model that integrates IT strategy and creates a case for using AWS cloud.
- **People** – Human Resources uses this to train people for cloud-based skills and organization-level change management recommendations for using the cloud.
- **Governance** – Describes governing business in the cloud, provides best practices for governance, and includes how to update people skills and processes for running business on the cloud.

Technical planning:

- **Platform** – Design for developing your AWS infrastructure to meet your business needs.
- **Security** – Guidance and standards to meet security needs and ensure audit transparency, as well as managing permissions.
- **Operations** – Instructions for operating and recovering workloads to meet the needs of stakeholders

Migration Strategies

The 6Rs of Application Migration –

1. **Rehosting** – This is also called "lift-and-shift" where few to no changes are made to the application itself while moving to the cloud, similar to using EC2 instances with on-premises databases. Cloud – Like using EC2 instances with on premises databases.

2. **Replatforming** – Changing parts of an application to make improvements in a cloud deployment without changing the main, underlying core of the application. This strategy is also referred to as “lift-tinker-and-shift.”
3. **Retiring** – Discarding any applications that are no longer required.
4. **Retaining** – Keeping all the applications that may be mission critical for the business within their original environment.
5. **Repurchasing** – Replacing an existing application with a new one that is cloud-based. This new cloud-based application (SaaS) can be acquired from AWS Marketplace.
6. **Refactoring** – Making changes to the architecture of an application by incorporating various features which are native to cloud technology.

Migration Technologies

AWS Application Discovery Service – This is a service for planning a migration to AWS, collecting configuration and usage data of on-premises databases and servers. The AWS Application Discovery is linked with AWS Migration Hub and AWS Database Migration Service Fleet Advisor.

AWS Application Migration Service (MGN) – This is a service that automates lift-and-shift migration to AWS. It also reduces the cost of migration to AWS. MGN handles any issues with compatibility, disruption of performance, and long cutover windows, and enables lifting and shifting of a large volume of cloud, virtual, or physical servers.

AWS Migration Hub – This is an AWS system used for identifying your migration plans, current servers, and for tracking the status of every application migration. The Migration Hub helps you investigate your existing portfolio of applications and streamline its planning and tracking.

AWS Schema Conversion Tool (SCT) – This converts the code and schema of the source database to match that of the destination database. You can then use AWS Database Migration Service (DMS) to perform the actual data migration process. AWS DMS moves existing databases to the AWS cloud with no disruptions to the original database.

Snow Family

AWS offers various devices as part of its Snow Family for migrating data in and out of AWS. The Snow family moves data in a secure manner and with reliable throughput. The Snow family includes:

- **Snowcone** – Ideal for edge computing and data transfer. Its specifications are: 8TB of storage, 2CPUs, and 4GB of memory.
- **Snowball Edge** – Ideal for large scale migration of data, workflows that need data transfer and high-capacity local computing. It has two variations:
    - **Storage Optimized** – 80TB of HDD for block and S3 storage, 1TB of SATA SSD for Block volumes, and has 40vCPUs with 80GiB for EC2 instances.
    - **Compute Optimized** – 42TB of EBS or S3 storage, 7.68TB of SSD storage for EBS compatible block volumes, and 52vCPUs, 208GiB of memory, and an NVIDIA Tesla V100 GPU for EC2 instances.
- **Snowmobile** – Provides 100PBs of data transfer via a semi-trailer truck with a 45-foot shipping container.

AI and Machine Learning

The following lists AWS technologies that utilize artificial intelligence (AI) and machine learning (ML).

Amazon Sagemaker – This is a fully managed service that allows you to build, train, and deploy ML models. SageMaker covers the full ML workflow which includes data preparation, algorithm selection, model training, model tuning, and optimization for development, making predictions, and taking action.

Amazon Rekognition – This adds video and image analysis capabilities to your applications. Images and videos are fed to the Amazon Rekognition API which then uses the Rekognition service to identify activities, people, text, scenes, and objects in the images and videos. It can also detect content which may be inappropriate.

Amazon Comprehend – This analyzes the contents of documents and provides insights using Natural Language Processing (NLP). Comprehend works with all text files in UTF-8 format and builds insights using various elements inside documents, including observations, language, key phrases, and entities. You can use Comprehend to create new products by evaluating the contents of documents.

Amazon Textract – This uses Machine Learning (ML) technology to extract data, text and handwriting from scanned documents like tax forms and financial reports. It also can extract tables, forms, and text from documents which contain structured data with the Amazon Textract Document Analysis API.

Amazon Lex – This allows you to build conversational interfaces for an application using voice and text. This uses the same engine that is behind Amazon Alexa and supports creating chatbots which use natural language within your applications.

Amazon DeepLens – This is a video camera which has deep learning enabled. It can perform inference locally using deployed models that have been provisioned from AWS Cloud. With DeepLens you can gain insight into the latest Artificial Intelligence (AI) technology to create computer vision systems which utilize a deep learning model.

AWS DeepRacer – This is a 1/8th scale race car used for testing reinforcement learning models. It provides a cloud-based 3D racing simulation.

Amazon Fraud Detector – This is a fully managed service that uses ML technology to automatically detect online activities that could be fraudulent. These activities include creating fake accounts and initiating various unauthorized transactions.

Amazon Augmented AI (A2I) – This technology allows you to build workflows required for performing human reviews of predictions made by Machine Learning (ML).

Amazon Transcribe – This utilizes ML technology to identify spoken words from audio streams and audio files and then transcribes these into text. Transcribe allows you to add speech-to-text capability for an application and allows you to make accurate use cases with language customization options.

Amazon Translate – This allows you to translate text using ML technologies. You use Translate for creating applications which can work across several languages as well as translating unstructured text. You can translate various types of content using Translate, including media feeds, reports, articles, and meeting notes.

Amazon Forecast – This provides accurate time-series forecasts using ML and statistical algorithms. It uses the same time-series forecasting technology that is used for Amazon.com and predicts future data using historical data without the user requiring any ML experience.

Amazon Polly – This provides text-to-speech capabilities to create more engaging and accessible applications. Polly has support for multiple languages and has a wide repository of lifelike voices used to create speech-enabled applications which can then be used across many different locations with the right voice for each location.

AWS Deep Learning AMIs – These allow you to launch EC2 instances which are pre-loaded with Deep Learning interfaces and frameworks, including PyTorch, TensorFlow, Chainer, and MXNet. You can perform training for customized Artificial Intelligence (AI) models as well as work with new kinds of algorithms.

Amazon Kendra – Technology provides intelligent search capabilities. It uses powerful machine learning (ML) and natural language processing algorithms for providing focused answers to queries on your data. It enables you to build a unified search system by linking various data repositories through an index and then performing ingestion and crawling on documents.

Internet of Things Technology

The following lists AWS technologies that utilize Internet of Things **(**IoT) technology.

AWS IoT Core – Technology used for connecting IoT devices to the cloud securely and efficiently. AWS IoT Core offers messaging features that are MQTT-based, which help create scalable, efficient, and cost-optimized IoT architectures. MQTT is a messaging protocol for machine-to-machine communication.

AWS IoT Greengrass – This system enables you to add cloud capabilities to a local device. You can use IoT Greengrass to create IoT devices and logic for IoT applications. You can also manage application logic running on devices using the cloud. The main difference between IoT Core and Greengrass is that IoT Core is a cloud service running on the cloud while IoT Greengrass is an edge runtime.

The Cloud Strategy

The AWS Well-Architected Framework

The six pillars of the AWS Well architected framework are:

O – **Operational excellence** – Running workloads **effectively** to create maximum business value, using operations as code, making small reversible changes, and expecting failure.
S – **Security** – Data encryption, applying **security** at all layers, and following security best practices.
P – **Performance efficiency** – Using resources **efficiently** to meet system requirements, making the most of resources, choosing appropriate instance types, and going serverless.
R – **Reliability** – Ensures high availability and **consistency** of workloads, as well as managing failure recovery. This also includes scaling resources to meet changing demand.
C – **Cost optimization** – Analyzing **costs** and reducing them using additional managed services.
S - **Sustainability** - Building environmentally friendly architectures that are **sustainable**.
You can use the mnemonic **OSPRCS** to memorize the six pillars.

AWS Well-Architected Framework Examples	
Operational excellence	Automating the process of making changes by a deployment pipeline
Security	Encrypting data in transit and at rest and activating MFA for root users
Performance Efficiency	Choosing the right EC2 instance for the right workload
Reliability	Deploying applications across multiple AZs and taking backups
Cost optimization	Ensuring correct server sizes and suspending idle or unused resources
Sustainability	Building environmentally friendly architectures that are sustainable.

Summary of Cloud Computing

Key advantages of using cloud computing with AWS:

- Variable expenses instead of upfront expenses. (You pay only for compute time.)
- Lower costs due to massive economies of scale. (Aggregated use by many users.)
- Using auto scaling to optimize instead of guessing capacity.
- More speed and agility when deploying and testing new applications.
- No wasted capital running data centers.
- Use Regions to quickly expand globally and maintain low latency for application usage.

AWS Services Dictionary

Amazon EMR (Previously Elastic Map Reduce) – A managed cluster platform for running big data frameworks like Apache Spark and Hadoop.

AWS Cloud9 – Provides a cloud-based Integrated Development Environment (IDE).

Amazon AppStream 2.0 – This system enables users to access desktop applications instantly from any location.

Amazon API Gateway – Service for building, running, and securing HTTP, REST, and WebSocket APIs at all scales.

Amazon Athena – Runs serverless SQL queries on S3 data for analysis.

AWS Audit Manager – This service performs continuous auditing of AWS usage for simplifying management compliance and risk with industry standards and regulations.

Amazon Aurora – Amazon's fully managed relational database operating at enterprise-level and performs faster than MySQL and PostgreSQL.

Amazon CloudFront – This is a Content Delivery Network (CDN) that caches copies of data at locations around the world that are closer to customers (edge locations), enabling higher speeds and low latency.

Amazon CloudWatch – Lets you monitor your AWS infrastructure and resource metrics in real-time from one dashboard.

Amazon Cognito – Creates user access controls for Web applications and is scalable.

Amazon Comprehend – Analyzes the contents of documents and provides insights using Natural Language Processing (NLP).

Amazon Connect – Provides a cloud contact center which is omnichannel and can integrate with enterprise applications such as Salesforce.

Amazon Detective – Performs automatic security analysis of terabytes of data for IP traffic and AWS operations.

Amazon DynamoDB – A non-relational serverless database that is purpose-built and fully managed. It has a very fast millisecond response time and is highly scalable. it can handle millions of requests per second.

Amazon Elastic Compute Cloud (EC2) – This is a service that provides computing capability using virtual servers.

Amazon EC2 Instance types:

- Reserved Instances – These provide a billing discount of up to 75% when applied, compared to using On-Demand instances. You can buy these for a one- or three-year term and consistent use is not required. You can buy Standard and Convertible Reserved instances for a period of one or three years. You can also buy Scheduled Reserved instances for a one-year period.
- On-Demand Instances – These are for short term, irregular workloads with no interruptions. You pay only for actual usage. These are best suited for developing and testing applications.
- Spot Instances – These are for workloads that can be interrupted. These can save up to 90% of the costs of On-Demand instances.

- On-Demand Capacity Reservations – This allows you to reserve Amazon Elastic Compute Cloud (EC2) compute capacity in an Availability Zone for any length of time. This makes it ideal for business-critical workloads that need guaranteed assurance for long- and short-term compute capacity. Capacity Reservations are useful for business-critical events, regulatory requirements, and disaster recovery situations.

Amazon Elastic Block Store (Amazon EBS) – Provides persistent block storage across changing physical hosts. Use EBS with EC2 instances.

Amazon Elastic Container Service (Amazon ECS) – Uses Docker containers and uses API calls for launching and stopping the containers.

Amazon Elastic Container Registry (Amazon ECR) – This is a secure and scalable container image registry service that is managed by AWS.

Amazon Elastic File System (Amazon EFS) – A managed file system which scales automatically to petabyte levels with no interruptions to applications.

Amazon Elastic Kubernetes Service (Amazon EKS) – Allows you to use Kubernetes on AWS. Kubernetes is an open-source technology for deploying and managing containerized software.

Amazon ElastiCache – A database accelerator for microsecond latency using in-memory caching and providing compatibility with MemCached and Redis.

Amazon EventBridge (Amazon CloudWatch Events) – Provides an event bus service which is serverless, allowing you to connect an application with data from various sources.

Amazon Forecast – Provides accurate time-series forecasts using ML and statistical algorithms.

Amazon Fraud Detector – Provides a fully managed service that uses ML technology to automatically detect online activities that could be fraudulent.

AWS Glue - This is an Extract Transform Load (ETL) service used for various ML applications for categorization, cleaning, and enrichment of data before storing as processed data in S3.

AWS IoT GreenGrass – Provides a secure way for running local messaging and computing syncing tasks for connected devices.

Amazon GuardDuty – Provides intelligent threat detection via machine learning for AWS resources and infrastructure.

Amazon Inspector – Provides vulnerability assessment services ensuring security and compliance of an AWS system.

Amazon Kendra – Technology providing intelligent search capabilities. It uses powerful machine learning (ML) and natural language processing algorithms for providing focused answers to queries on your data. It enables you to build a unified search system by linking various data repositories through an index and then performing ingestion and crawling on documents.

Amazon Kinesis – Allows for the ingestion, buffering, and processing of streaming data performed in real-time. The data is available for analysis within seconds.

Amazon Lex – This is a tool for building conversational interfaces for an application utilizing voice and text.

Amazon Lightsail – Provides an easy way to build applications or websites through virtual private server (VPS) instances, managed databases, load balancers, and storage. Costs billed monthly.

Amazon Machine Images (AMIs) – This is a maintained image provided by AWS and it acts as a template to assist you when launching an instance. It contains EBS snapshots, launched permissions, and it blocks device mappings.

Amazon Macie – Uses ML and pattern matching to provide data security and privacy services for protecting sensitive data in an AWS deployment.

Amazon MemoryDB for Redis – This is an in-memory database suited for workloads requiring a very fast primary database which is Redis-compatible. Redis is an open source in-memory data structure.

Amazon Managed Streaming for Apache Kafka (Amazon MSK) – This system allows you to create applications that use Apache Kafka for processing streaming data.

Amazon Neptune – This is a graph database used for social webs and recommendation engines. It is also useful for fraud detection applications.

Amazon OpenSearch Service – This service is used for deploying, operating, and scaling OpenSearch clusters on AWS.

Amazon Polly – Provides text-to-speech capabilities that help you create more engaging and accessible applications.

Amazon QuickSight – Provides business intelligence reporting with graphic-based dashboards, using ML for trend analysis.

Amazon RDS – A fully managed DB service that offers encryption for several of its database engines, including Amazon Aurora, MySQL, PostgreSQL, MariaDB, Oracle Database, and Microsoft SQL Server.

Amazon Redshift – Used as a scalable data warehousing solution. It produces big data analytics and collects data from multiple sources.

Amazon Rekognition – Provides video and image analysis capabilities for your applications identifying activities, people, text, scenes, and objects.

Amazon Route 53 – Provides DNS services which include transferring DNS records for any existing domain names from other registrars and connecting users to AWS infrastructure.

Amazon S3 – Amazon S3 allows you to store an unlimited number of objects, with each object up to 5TB in size, in S3 buckets. The files stored on Amazon S3 can be of any type, including images, videos, documents, and more.

Amazon S3 Glacier – This is a low-cost storage option meeting some data archiving requirements. Retrieval of data stored in this class can take a few minutes to a few hours.

Amazon SageMaker – A fully managed service that allows you to build, train, and deploy ML models.

Amazon Simple Email Service (Amazon SES) – This is a platform for emails that enables you to send and receive email through your own domains and email addresses.

Amazon Simple Notification Service (Amazon SNS) – Provides a publish/subscribe (pub-sub) service. It allows you to publish messages on SNS topics to multiple subscribers.

Amazon Simple Queue Service (Amazon SQS) – Provides message queueing. Messages can be sent, received, and stored across several components of applications and microservices.

Amazon Textract – Uses Machine Learning (ML) technology to extract data, text, and handwriting from scanned documents such as tax forms and financial reports.

Amazon Transcribe – Uses ML technology to identify spoken words from audio streams and audio files and then transcribes these into text.

Amazon Translate – Uses ML technologies to translate various types of content including media feeds, reports, articles, and meeting notes.

Amazon VPC – This is an isolated part of the AWS cloud which is further divided using subnets.

Amazon WorkSpaces – Allows provisioning of virtual desktops called Workspaces that can be Microsoft Windows- or Amazon Linux-based. You can add or remove users as needed.

Amazon WorkSpaces Web – This is a WorkSpaces capability suitable for secure, web-based workloads.

APIs – Applications Programming Interfaces (APIs) are a way that two software components communicate with each other through a set of protocols. REST and WebSocket are popular APIs.

AWS Activate – This is a startup program from AWS that provides resources and tools, such as AWS credits, to eligible startups.

AWS Amplify – This set of tools includes a visual development environment, open-source framework, and services such as static website and web app hosting.

AWS AppConfig – This service enables you to configure, validate, deploy, and monitor your application configuration.

AWS Application Discovery Service – This is a service for planning a migration to AWS, collecting configuration and usage data of on-premises databases and servers.

AWS Application Migration Service (MGN) – This service provides automation for a lift-and-shift migration to AWS.

AWS AppSync – This is a managed service for GraphQL Application Programming Interface (API). GraphQL is a language for querying APIs and uses runtimes to fulfill those queries on your existing data.

AWS Artifact – Provides access to third-party compliance reports validating AWS’s adherence to compliance standards such as HIPPA.

AWS Auto Scaling – This allows you to add or remove EC2 instances automatically to match changing demand.

AWS Backup – This is a fully managed service which provides a centralized, automated data protection process for AWS services on the cloud and on-premises. It can be integrated with Storage Gateway.

AWS Batch – These provisions compute resources and optimizes job distribution based on the resource needs and volumes of batch jobs. You can set the queues to different priority levels.

AWS Billing Conductor – This service provides custom billing features supporting chargeback and showback workflows for AWS Enterprise customers and solution providers.

AWS Budgets – Allows you to create budget plans for instance reservations and service usage and costs. You can set alerts for when expenditure exceeds or is predicted to exceed a pre-set threshold. It also allows you to view forecasts.

AWS Certificate Manager (ACM) – This handles the tasks of creating, saving, and renewing private and public SSL/TLS X.509 certificates and keys for protecting AWS applications and websites.

AWS CloudFormation – Allows you to provision resources using templates written in YAML or JSON.

AWS CloudHSM – This provides hardware security modules (HSMs) for the AWS cloud that process cryptographic functions and provide secure storage for cryptographic keys.

AWS CloudShell – This is a browser-based pre-authenticated shell that can be launched using the AWS Management Console.

AWS CloudTrail – This service logs every API and request made on the system. It records the API caller's identity and source IP address. It can also save logs indefinitely in S3 buckets.

AWS CodeArtifact – This provides a fully managed repository service. An organization can use it to securely store, publish, and share their software packages.

AWS CodeBuild – This is a fully managed service that compiles source code, performs unit testing, and provides artifacts which can be deployed.

AWS CodeCommit – This is a source and version control service which is scalable, secure, managed, and allows you to host private Git repositories as well.

AWS CodeDeploy – This provides automated application deployment services for EC2 instances, ECS services, Lambda functions, and on-premises instances.

AWS CodePipeline – This provides a continuous delivery service for modelling, visualizing, and automating the steps for the software release cycle.

AWS CodeStar – Enables creating, managing, and working with software development projects on the AWS Cloud. Use this to build and deploy applications on AWS.

AWS Command Line Interface (CLI) – This is an open-source tool that allows you to work with multiple AWS services using various commands from a command-line shell.

AWS Compute Optimizer – This service analyzes the configuration and metrics related to AWS resource utilization.

AWS Config – This is a service that lets you perform assessment, evaluation, and auditing of AWS resource configurations.

AWS Control Tower – This is a service that provides landing zones, which are environments that contain all the organizational units (OUs), users, and resources that you need to remain within compliance regulations.

AWS Cost and Usage Report (CUR) – This provides usage information at the account or organization level. This information is itemized based on operation, product code, and usage type.

AWS Cost Explorer – Shows costs associated with AWS resources such as EC2, Managed Blockchain, and so on. You can also view costs for resources grouped by tags.

AWS Deep Learning AMIs (DLAMI) – These are environments pre-configured to rapidly create deep learning applications. It allows you to launch EC2 instances preloaded with deep learning frameworks.

AWS DeepLens – This is a video camera that has deep learning enabled. It operates locally using deployed models provisioned from AWS Cloud.

AWS Direct Connect – Connects directly to a VPC from an on-premises center via a high-speed dedicated fibre optic connection.

AWS Directory Service – This service provides several ways to use Microsoft Active Directory (AD) with AWS services. AWS Directory Service has multiple directories and uses applications that work with Lightweight Directory Access Protocol (LDAP) and Microsoft AD.

AWS Elastic Beanstalk –Enables efficiently deploying and scaling applications onto AWS without writing code for building capacity, load balancing, scaling, and health monitoring.

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

AWS Firewall Manager – A security management service that enables you to configure and manage firewall rules centrally across accounts and applications inside AWS organizations.

AWS global infrastructure (for example, AWS Regions, Availability Zones) – An Availability Zone (AZ) is a fully-isolated portion of the AWS Global Infrastructure. It is a single or group of data centers inside a Region. A Region is a geographical region with many locations that are isolated from each other. The choice of a Region is based on proximity, compliance, services, and costs.

AWS Identity and Access Management (IAM) – Provides secure access to AWS resources through IAM users, groups, and roles.

AWS Identity and Access Management (IAM) Identity Center – This system allows centrally-managed SSO access to AWS accounts and applications. SSO authentication allows users to securely authenticate to multiple applications using one set of credentials.

AWS Internet of Things (IoT) Core – This is a technology used for connecting IoT devices to the cloud securely and reliably.

AWS IQ – You can use this system to get hands-on help from AWS Certified experts for your AWS projects.

AWS Lambda – This allows you to perform serverless computing. When using AWS Lambda, you upload your code to a lambda function and then configure a trigger to initiate it.

AWS Launch Wizard – This system sizes, configures, and deploys AWS resources for various third-party systems such as HANA-based SAP systems and Microsoft SQL Server Always On.

AWS Local Zones – This is an AWS technology that maintains AWS resources such as database, storage, and compute near industry and large population centers.

AWS Wavelength Zones – These are zones inside a carrier location where an AWS Wavelength infrastructure has been deployed.

AWS License Manager – This is a service for centrally managing software licenses from multiple vendors, including IBM, Oracle, Microsoft, and SAP, across AWS and on-premises.

AWS Managed Services (AMS) – This is an enterprise service for managing AWS infrastructure. It implements key best practices and provides maintenance for infrastructure, reducing overheads.

AWS Management Console – This is a web application that provides various consoles for managing AWS resources. The console home page is your landing page when you log in.

AWS Marketplace – This is a digital library containing thousands of third-party software applications across varying categories and industries.

AWS Migration Hub – This is an AWS system used for identifying your migration plans, current servers, and for tracking the status of every application migration.

AWS Organizations – This provides one place for managing several AWS accounts. Allows for consolidated billing and the hierarchical grouping of accounts.

The AWS Partner Network (APN) – This is an AWS system that provides expertise, programs, and resources for building and selling customer offerings through a global community of partners.

AWS Personal Health Dashboard – This allows you to view the availability and performance of your AWS services usage in real-time, including customizable alerts triggered by changes to specific services.

AWS Pricing Calculator – Use this service to create estimates for the costs of any use case you have on AWS.

AWS Professional Services – This is an expert-level team distributed globally to assist AWS customers migrating to a cloud-based IT system using AWS services.

AWS re:Post: – This is a portal that provides access to the AWS Knowledge Center for troubleshooting, query resolution through AWS support, best practices, and connection to AWS employees and partners.

AWS Resource Groups – This is a service for managing and automating tasks performed on multiple resources at the same time. Resources on AWS include entities like AWS CloudFormation stacks, Amazon Elastic Compute Cloud (EC2) instances, and Amazon Simple Storage Service (S3) buckets.

AWS Resource Access Manager (AWS RAM) – This is an AWS service for sharing resources securely across multiple AWS accounts and within organizational units (OUs) and organizations.

AWS Schema Conversion Tool (SCT) – This converts the code and schema of the source database to match that of the destination database.

AWS Secrets Manager – This uses API calls for programmatic access to replace credentials that are hardcoded in code.

AWS Service Catalog –Supports creating, distributing, and managing product catalogs for end-users. End-users can also access these products from a personalized online portal.

AWS Health Dashboard – This provides information on AWS Health events affecting AWS services or accounts.

AWS Shield – This is a managed service for protection from distributed denial of service (DDoS) attacks and offers automatic mitigations to reduce application downtime and latency.

AWS Snowball Edge – This is technology for large scale data migration, workflows requiring data transfer, and high-capacity local computing. It has two options: Storage Optimized and Compute Optimized.

AWS software development kits (SDKs) – Guidelines and instructions for provisioning and interaction with AWS services using Application Programming Interfaces (APIs) created for platforms, and using programming languages such as C++, Java, and .NET.

AWS Step Functions – This is a workflow service that allows you to orchestrate multiple AWS services and automate business processes.

AWS Storage Gateway – This technology provides secure and seamless access for on-premises systems and applications to unlimited storage on AWS using Amazon S3, Tape Library, and Amazon FSx.

AWS Support Center – AWS Support has a variety of support plans which provide round-the-clock access to tools and expert guidance, including customer support, whitepapers, and forums. You can choose the best support plan for your technical support requirements.

AWS Support Plans – AWS offers five support plans: Basic, Developer, Business, Enterprise On-Ramp, and Enterprise. The Basic support plan is free for all AWS users. The Developer support plan is the most affordable for general needs, and the Enterprise support plan is the most expensive. The Business and Enterprise plans have access to all Trusted Advisor checks.

AWS Systems Manager – Use this service to view and control your entire AWS infrastructure. For example, you can automate operating tasks and check operational data for resources.

AWS Systems Manager Parameter Store – Stores secrets management and configuration data management information, including AMI IDs and passwords, securely and hierarchically.

AWS Transfer Family – Supports the secure transfer of data into and out of storage services on AWS.

AWS Trusted Advisor – This tool informs how you should provision your AWS resources based on AWS best practices. It performs real-time monitoring of your AWS resources and recommends actions accordingly.

AWS Trust and Safety team – This is a global team that helps provide protection against AWS resource abuse and works to create trust with AWS clients and stakeholders.

AWS VPN – This is a system used for securely connecting remote workers and on-premises networks to your AWS cloud.

AWS Web Application Firewall (WAF) – This controls requests coming from a network into your web applications. AWS WAF permits or denies traffic based on a web access control list (ACL).

AWS Elastic Load Balancing (ELB) – This is used for distributing traffic among EC2 instances. ELB ensures that no EC2 instance is left unused and similarly, no instance is used more than required, by sharing traffic evenly across several EC2 instances.

Infrastructure as Code (IaC) – This is a DevOps principle where infrastructure is treated in a way similar to the way a programmer treats code, by defining configurations using declarative methods and storing them using source control systems.

Security groups – A security group is a virtual firewall that protects an EC2 instance. These perform stateful packet filtering and work at the instance level.

Service quotas – These are maximum values for any items, actions, and resources in an AWS account. You may require, and request, a quota increase to suit your business needs.

Virtual private networks (VPNs) – You connect securely to a VPC over the Internet using a VPN.

AWS X-Ray – This provides detailed data on requests that your application serves. It contains tools that allow you to gain insights into all the possible issues that may exist within the application as well as methods for optimization.