What is Cloud Computing?

Cloud computing is the delivery of online services (such as servers, databases, software) to users. With the help of cloud computing, storing data on local machines is not required. It helps you access data from a remote server. Moreover, it is also used to store and access data from anywhere across the world.

What is AWS?

AWS Meaning: The Amazon Web Services (AWS) platform provides more than 200 fully featured services from data centers located all over the world, and is the world's most comprehensive cloud platform.

AWS Services

Amazon has many services for cloud applications. Let us list down a few key services of the AWS ecosystem and a brief description of how developers use them in their business.

Amazon has a list of services:-

* Compute service
* Storage
* Database
* Networking and delivery of content
* Security tools
* Developer tools
* Management tools

Compute Service

These services help developers build, deploy, and scale an application in the cloud platform.

1. AWS EC2

* It is a web service that allows developers to rent virtual machines and automatically scales the compute capacity when required.
* It offers various instance types to developers so that they can choose required resources such as CPU, memory, storage, and networking capacity based on their application requirements.

Amazon EC2 features:-

* Global Infrastructure
* Cost and Capacity Optimization
* Storage
* Networking
* Operating Systems and Software
* Maintenance

What are volumes in EC2?

EC2 Volumes (called Elastic Block Storage by Amazon) are essentially disk images that can be mounted on any system running on EC2, and continue to exist even if the system they were attached to is deleted.

1. AWS Lambda

* [AWS Lambda](https://www.simplilearn.com/aws-lambda-function-article) is a serverless compute service. It is also responsible for executing code for applications.
* It helps you execute a program without the hassle of managing servers.

Storage

AWS provides web data storage service for archiving data. Also, its primary advantage is disaster data recovery with high durability.

1. Amazon S3

* It is an open cloud-based storage service that is utilized for online data backup.
* Amazon S3 provides storage through a web services interface and is designed for developers where web-scale computing can be easier for them

How Amazon S3 works?

Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects.

###### Topics:-

* [Buckets](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BasicsBucket)
* [Objects](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BasicsObjects)
* [Keys](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BasicsKeys)
* [S3 Versioning](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#Versions)
* [Version ID](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BasicsVersionID)
* [Bucket policy](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BucketPolicies)
* [S3 Access Points](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#BasicsAccessPoints)
* [Access control lists (ACLs)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#S3_ACLs)
* [Regions](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#Regions)

### Buckets

A bucket is a container for objects stored in Amazon S3. You can store any number of objects in a bucket and can have up to 100 buckets in your account.

### Objects

Objects are the fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The metadata is a set of name-value pairs that describe the object. These pairs include some default metadata, such as the date last modified and standard HTTP metadata, such as Content-Type. You can also specify custom metadata at the time that the object is stored.

### Keys

An object key (or key name) is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key. The combination of a bucket, object key, and optionally, version ID (if S3 Versioning is enabled for the bucket) uniquely identify each object.

### S3 Versioning

You can use S3 Versioning to keep multiple variants of an object in the same bucket. With S3 Versioning, you can preserve, retrieve, and restore every version of every object stored in your buckets. You can easily recover from both unintended user actions and application failures.

### Version ID

When you enable S3 Versioning in a bucket, Amazon S3 generates a unique version ID for each object added to the bucket. Objects that already existed in the bucket at the time that you enable versioning have a version ID of null. If you modify these (or any other) objects with other operations, such as [CopyObject](https://docs.aws.amazon.com/AmazonS3/latest/API/API_CopyObject.html) and [PutObject](https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutObject.html), the new objects get a unique version ID.

### Bucket policy

A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy that you can use to grant access permissions to your bucket and the objects in it. Only the bucket owner can associate a policy with a bucket. The permissions attached to the bucket apply to all of the objects in the bucket that are owned by the bucket owner. Bucket policies are limited to 20 KB in size.

### S3 Access Points

Amazon S3 Access Points are named network endpoints with dedicated access policies that describe how data can be accessed using that endpoint. Access Points are attached to buckets that you can use to perform S3 object operations, such as GetObject and PutObject. Access Points simplify managing data access at scale for shared datasets in Amazon S3.

### Access control lists (ACLs)

You can use ACLs to grant read and write permissions to authorized users for individual buckets and objects. Each bucket and object has an ACL attached to it as a subresource.

### Regions

You can choose the geographical AWS Region where Amazon S3 stores the buckets that you create. You might choose a Region to optimize latency, minimize costs, or address regulatory requirements. Objects stored in an AWS Region never leave the Region unless you explicitly transfer or replicate them to another Region.

1. Amazon EBS

* It provides a high availability storage volume for persistent data. It is mainly used by [Amazon EC2](https://www.simplilearn.com/tutorials/aws-tutorial/aws-ec2) instances.
* EBS volumes are used explicitly for primary storage such as file storage, databases storage, and block-level storage.

Database

AWS database domain service offers cost-efficient, highly secure, and scalable database instances in the cloud.

1. DynamoDB

* It is a flexible [NoSQL database](https://www.simplilearn.com/rise-of-nosql-and-why-it-should-matter-to-you-article" \o "NoSQL database" \t "_blank) service that offers fast and reliable performance with no scalability issues.
* It is a multi-region and durable database with instant built-in security, backup and restores features.

1. RDS

* It is a managed distributed relational database cloud service that helps developers to operate and scale a database in a simple manner.
* We launched it to simplify the setup, operation, and scaling process for developers while accessing a relational database.

Networking and Delivery of Content

It offers a highly secure cloud platform and connects your physical network to your private VN with a high transfer speed.

1. VPC

* It helps a developer to deploy AWS resources, such as Amazon EC2 instances into a [private virtual cloud.](https://www.simplilearn.com/tutorials/aws-tutorial/aws-vpc)
* It gives you control over the complete cloud network environment, including the section of your [IP address](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-an-ip-address) range, subnets, route table configuration, and network gateways.
* With this, developers can both IPv4 and IPv6 at a time for your resources in a highly secure environment.

1. Route 53

* It is a web service with a highly available Domain Name System (DNS) that helps users to route software by translating the text into an IP address.
* We launched it for developers to provide them a cost-effective method of routing end users to cloud applications.

Developer Tools

It helps a user build, deploy, and run an application source code automatically. It also updates the server and instance on the workload.

1. CodeStar

It is a service designed to manage application development in a single place. Here, developers can quickly develop, build and deploy applications on AWS

1. Code Build

* This removes the hassle of managing physical servers and helps developers build and test code with continuous scaling.
* In simple words, it compiles your code, executes unit tests, and gives output artifacts that are ready to deploy.

Security, Identity & Compliance

It helps in monitoring a safe environment for your AWS resources by providing limited access to specific users.

1. IAM

* Identity Access Management is a framework that helps in maintaining access to AWS services in a secure way.
* The service gives you Shared access to your AWS account and Secure access to AWS services that run on the AWS EC2 application.

Feature of IAM:-

1) Shared access to your AWS account:-You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

2) Granular permissions:-You can grant different permissions to different people for different resources.

3) Multi-factor authentication (MFA):-You can add two-factor authentication to your account and to individual users for extra security.

4) Identity federation:-to get temporary access to your AWS account.

* How many users can I create in IAM?

An AWS root or IAM admin can create an IAM user on the IAM dashboard of the AWS Console 5,000 IAM users.

* How many groups can an IAM user have?

You can assign IAM users to up to 10 groups.

IAM policies:-IAM policies define permissions for an action regardless of the method that you use to perform the operation.

Types of policies:

1. Identity-based policies

* Managed policies
* Inline policies

1. Resource-based policies
2. Permissions boundaries
3. Organizations SCPs
4. Access control lists (ACLs)
5. Session policies

Roles:-

AWS Identity and Access Management (IAM) roles are entities you create and assign specific permissions to that allow trusted identities such as workforce identities and applications to perform actions in AWS. When your trusted identities assume IAM roles, they are granted only the permissions scoped by those IAM roles. Using IAM roles is a security best practice because roles provide temporary credentials that do not need to be rotated. Roles are attach to an aws resources.

1. KMS

* It enables users to create and manage the encryption keys that are used for encrypting data.
* The service includes a key generation method where digital sign within your applications becomes easier.

Management Tools

Using this service, an individual can optimize costs, minimize risks, and automate all the resources running efficiently on the AWS infrastructure.

1. Cloud Watch

* It is a monitoring tool for AWS resources and customer applications running on the AWS platform.
* The service helps you gather and access all your operational data in the form of logs from a single interface.