* AWS IAM(Identity and Access Management) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
* When you create an account in AWS, then you are creating an root account which has full admin access
* AWS recommends that you do not use the root user for everyday tasks, even the administrative ones.

IAM Features:

Shared access to your Account:

* You can grant other people permission to administer and use resources in your AWS account without having to share your access credentials(password or access key)

Granular Permissions:

* You can grant different permissions to different people for different resources.
* For instance, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but noting else.

Secure access to AWS resources for applications that run in Amazon EC2:

* You can use IAM feature to securely give applications that run on EC2 instances the credentials that they need in order to access other AWS resources. Examples include S3 buckers and RDS or DynamoDB databases.

Multi-factor authentication (MFA):

* You can add two-factor authentication to your account and to individual users for extra security.
* With MFA you or your users must provide not only a password or access key to work with your account, but also a code from a specially configured device.

Identity federation

* You can allow users who already have password elsewhere – for example, in your corporate network or with an internet identity provider – to get temporary access to your AWS account.

Identity information for assurance

* If you use AWS CloudTrail, you receive log records that include information about those who made requests for resources in your account. That information is based on IAM identities

PCI DSS Compliance

* IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS)

Free to use

* AWS Identity and Access Management is a feature of your AWS account offered at no additional charge.
* You will be charged only for use of other AWS products by your IAM users

AWS Security Token Service

* Is an included feature of your AWS account offered at no additional charge.
* You are charged only for the use of other AWS services that are accessed by your AWS STS temporary security credentials

Access IAM:

* AWS Console: It requires a username and password
* Programmatic access through SDKs, HTTPS API, and CLI: It requires the Access Key and Secret Access Key

Users:

* End Users such as people, employees of an organization etc

Groups:

* A collection of users. Each user in the group will inherit the permissions of the group

Policies:

* Policies are made up of documents, called policy documents. These documents are in a format called JSON and they give permissions as to what a User/Group/Role is able to do.

Roles:

* You create roles and then assign them to AWS Resources.