**AWS IAM**

* AWS IAM stands for Identity and Access Management.
* IAM is a service using which we can give permission to different users who are using the same AWS account that we have created.
* IAM is use to control who is authenticated (signed in) and who is authorised (has permission) to use the resources.
* In an organisation, we can have only 1 AWS account on which a number of people can work. E.g: May be a developer working on our AWS account, he should have an access to EC2 or only works on EC2 instance you can decide that.
* If say a database admin comes in, he should be only able to access the db instances on our AWS account and so on. All of that is possible using IAM.
* Components of IAM:
* Users
* Groups
* Roles
* Policies

**Features:**

1. Shared access to your AWS account.
2. **Grandular Permission:** We grant different permission to different people for different resources. Eg: We might allow some for EC2 RDB, S3 and for others we allow somme for read only access, to access some S3 bucket or to access billing info or permission to monitor just some EC2 instances.
3. Secure access to AWS resources for application that runs on Amazon EC2.
4. **MFA:**  It provides an extra layer of security by generating an OTP.
5. **Identity Federation: Allows access as a guest user.**

**AWS policies are written using JavaScript Object Notation(JSON).**