

# IAM – Identity and Access Management

## 1. Authentication

- a. Ability to log into an aws account
  - i. Username/Password
- b. Verifies that you say you are who you are.

## 2. Authorization

- a. These is the ability to access resources once logged in the aws account

## 3. Groups

- a. To organize users in one location.
- b. Only need to grant group policy which applies to all user in same group
  - i. **Use cases**
    - 1. Administrators in Admin folder
    - 2. Developers in Dev folder
    - 3. Engineers in AWSEng folder

## 4. IAM Users

- a. Programmatic Access/Service Account
  - i. Access Key ID
  - ii. Secret Access Key
    - 1. Log into Aws account using command line interface (CLI) or powershell
    - 2. SDK – Software development kit
    - 3. APIs – Application Programming interface
  - iii. To perform application task.
  - iv. No MFA
- b. AWS Management Console Access
  - i. Log into our aws management console using the internet browser (safari, chrome, IE. etc)
  - ii. Enable MFA

## 5. IAM Roles

- a. An IAM role is an IAM entity that defines a set of [permissions](#) for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities assume roles, such as IAM users, applications, or AWS services such as EC2.**Policies**
- b. A policy is a JSON format document that contains rules **granting** or **denying** access to a service in AWS

## 6. Account Password policy

- a. Policy governing rule around setting up user passwords