IDENTITY ACCESS MANAGEMENT

# IAM [Identity Access Management]

* Essentially, IAM allows you to manage users and their level of access to the AWS Console. It is important to understand IAM and how it works, both for the exam and for administrating a company’s AWS account in real life.
* What does IAM give you?
  + Centralised control of your AWS account
  + Shared Access to your AWS account
  + Granular Permissions
  + Identity Federation (including Active Directory, Facebook, Linkedin etc) you can actually federate with different identity federators
  + Multifactor Authentication => You can actually put two factor authentication we actually going to setup in the lab
  + Provide temporary access for users/devices and services where necessary, where it can temporarily access your AWS account with web/mob device to store anything on S3 or DynamoDB for example.
  + Allows you to setup your own password rotation policy [You can set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords.]
  + Integrates with many different AWS services.
  + Supports PCI DSS Compliance [PCI DSS applies to *all* entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.]
* Critical Terms: Before we step into IAM Lab
  + Users => End Users (think as people)
  + Groups => A collection of users under one set of permissions
  + Roles => You create roles and can then assign them to AWS resources
    - Example: You might have an EC2 Instance that can write files directly It to S3, you no need to setup usernames and passwords for that EC2 Instance which we are going to do in the labs soon
  + Policies => A document that defines one (or more permissions), you usually apply policies to users, groups and roles that they connect out to each other like user, group and the role where they all can share the same document

# IAM Lab

* Sign into the Console
* Select your region that is closest to you as most of the services will not be available to particular region
* Select IAM service under Security, Identity and Compliance [You use IAM allot when you deal with real world applications ]
* If you notice IAM sits for Global as region that is because IAM is global as to serve all the users, groups and roles with same permission not depending on regions.
* You can see IAM User Sign In Link:
  + - [**https://591931265823.signin.aws.amazon.com/console**](https://591931265823.signin.aws.amazon.com/console)
    - This number is not random its actually your AWS account number => usually your account number sits in myaccount
    - you can customize it to a DNS[Domain Name Space]