IAM
(Identity and Access Management)

- IAM allows you to manage Users, Groups and their level of access to the AWS Services.

What does IAM give you?

- Centralised control of your AWS account
- Shared access to your AWS account
- Granular Permissions
- Multifactor Authentication
- Allows you to set up your own password rotation policy

Important Terms

- **Users** - End Users (People)
- **Groups** - A Collection of users under one set of permissions
- **Policies(Permissions)** - A document that defines one (or more) permissions
- **Roles** - You create roles and can then assign them to AWS resources

---

Roles

- Without using credentials, we can manage aws services through aws cli by using roles
- Roles give secure way to access all aws resources
- Can access one aws service with another aws service without credentials.

Important Points

- IAM is universal. It does not apply to regions at this time.
- The "root account" is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have NO permissions when first created.
- New Users are assigned Access Key ID & Secret Access Keys when first created.
- These are not the same as a password, and you cannot use the Access key ID & Secret Access Key to login in to the console. You can use this to access Command line.
- You can create and customise your own password rotation policies.
