=====
IAM
=====

=> Identity and Access management

=> It is used to manage users, groups, policies and roles

=> IAM is a free service

=> In AWS cloud platform we will have 2 types of accounts

1) Root Account
2) IAM Account

Note: When we signup in aws website then by default it will consider that as root account.

=> Root account is very powerfull account with no restrictions.

=> If we login with Root user credentials, we can access everything in AWS cloud.

Note-1 : We shouldn't use root account for day to day activities.

Note-2 : We shouldn't share root account credentials with anyone.

Note-3: Company will not provide root account credentials for team members.

Note-4: It is recommended to enable MFA for root account.

MFA : Multi Factor Authentication

==========
Multi Factor Authentication (MFA)
==========

-> It is used to provide additional security for root account.

-> Enable MFA for root account using Google Authenticator app.

-> After enabling MFA, logout and login into root account and check behaviour.

============
IAM Account
============

=> For team members IAM accounts will be created with limited access

=> For daily activities in aws cloud we should use IAM account only

=> For IAM user we can provide below types of accesses

1) Console Access (web login)

- uname & pwd

2) Programmatic Access

- AccessKey and SecretAccessKey

Note: To communicate with AWS cloud using terraform then IAM user should have programmatic access.

1) Create IAM account and attach policies (RDSFullAcces, S3FullAccess)

2) Login into IAM account and check EC2 service (can't access because no permission)

==========
IAM User Group
==========

=> When we want to provide some permissions for multiple users then we can create IAM user group and we can add users to that group and we can attach policies to group.

1) Create User Group

2) Attach Policies to group

3) Add Users to group

Note: The policies attached to group, by default those policies applicable for all the users belongs to that group.

=========
IAM Role
=========

=> IAM role nothing but set of permissions

Ex-1: EC2 VM wants to create EKS cluster, Then EC2 VM should have IAM Role with EKS permissions.

1) create IAM role with all EKS policies
2) Attach IAM role to ec2 vm

============
IAM Summary
============
1) What is IAM
2) What is Root Account
3) How to enable MFA
4) What is IAM account
5) Console Access Vs Programmatic Access
6) Users Creation
7) User Groups
8) Policies / Permissions
9) Roles
10) Working with Custom Policies