Identity & access Management (IAM)

IAM manages AWS users & their access to AWS accounts & servics. it control the level of access a users can have over an aws account & set users, grant permission & allows a user to use different feature of an AWS accounts.

Iam is mainly used to manage users, groups, roles, & access policies the account we created to sign in to AWS is known as the root accounts & it holds all the administrative rights & has access to all parts of the accounts

The new user created an AWS accounts by default they have no access to any services in the accounts & it is done with the help of IAM that that the root accounts holder can implements access policies & grant permission to the user to access certain servicy.

- IAM identities classified As.

1) IAM Users.

2) IAM Group

3) IAM Roles

- Root Users.

The root user will automatically be created & granted unrestricted rights. we can create an admin user with fewer powers to control the entire Amazon account

- IAM Users.

we can utilize IAM users to access the AWS Console & their administive permission differ from those of the Root user & if we can keep track of login info.

- IAM Group.

A group is a collection of users & a single person can be a member of several group.

- IAM Roles

while polices cannot be directly given to any of the service may be assumed by anybody who required them. By using roles we can provide AWS Services access rights other AWS Services.