**Identity and Access Management(IAM):**

* **It provides the Authentication and Authorization to the user.**
* **IAM gives the login credentials and permissions to access the services in AWS console.**
* **We can create the users,groups.roles and policies in IAM dashboard.**

**Authentication:**

**It is nothing but a login id or username and password to login the console.**

**Authorization:**

**It means provide the permissions to access the services .**

**Role:**

* **Role is a task which is attached to the service in AWS.**
* **Role is same as user but main difference is user has fixed credentials like username and password whereas role has temporary credentials.**

**Policies:**

**Policies are nothing but a permissions (which services are user can access) which are attached to the users or roles or groups.**

**Types of Policies:**

* **AWS Managed Policies**
* **Inline Policies**

**AWS Managed policies:**

**There multiple aws managed policies are available in IAM .These policies are managed by AWS .**

**Inline Policies:**

**These are the customer managed policies.**

**Steps to create User in IAM:**

* **Go to IAM dashboard and click on users.**
* **Click on create user and enter the name of user.**
* **While creating user we can select the “provide user access to aws console” option or we can create this access after creation of user.**
* **Click on next and select the attach policies directly.**
* **Select the services which we want to give the access to the user in the permissions policies.**
* **Click on create user.**

**Log Into the new IAM User:**

* **Click on the username and click on security credentials.**
* **Copy the console sign in link on the browser.**
* **Enter name of the user and password (custom password).If you are not select a “provide user access to aws console” option while creating user you can recreate the new password while sign in into the console as a iam user.**
* **Now we can login to the new iam user.**

**Steps to create the IAM Role:**

* **Click on the roles which is available on iam dashboard.**
* **Click on create role and select aws service .**
* **Select the use case or service (To which service we want to add this role).In which I have selected EC2 service.**
* **Click on next and select the services which services we want to access from above service .(in which I have selected s3 service).**
* **Enter the name of role and click on create role.**

**Groups:**

* **Instead of creating and attaching policies to the users individually we can create the group and attach the policies to that group.**
* **Attach the users to the particular group.**
* **Users have all the permissions whatever permissions that group has.**

**Steps to create Group:**

* **Go IAM dashboard and click on user groups option.**
* **Click on create group and enter group name whatever we want.**
* **Add the users to this group or we can add the users to this group after creation of group.**
* **Attach the policies(to which services we want to give the access to this group) and click on create user group.**

**Login to AWS Console by using programmatic access:**

* **From AWS CLI (command line interface) We can able to sign into a AWS console by providing Access key and Secret key.**
* **We need to use “aws configure” command to provide access key and secret key on AWS CLI.**