**Users :-**

We can give the access of a particular service to the IAM user with the help of roles

Steps:-

1. Click on add user
2. Give the user name
3. Select AWS access credential type :-
4. Access key – programmatic access ( this key is work on cli, AWS API, SDK and other development tools.
5. Password –AWS management console access (this key enable password that allows user to sign-in to the AWS management console.

In the b) option there is two options i) auto-generated password ii) custom password

In the auto-generated password this password provided by AWS. And custom password you can manage according to your requirement.

Required password reset:-

This option will check it means after the first login of IAM user it will give the massage for reset the password. And if you uncheck it then it will not ask for the reset password.

1. Click on next option
2. Set permission :- 1) add user to group 2) copy permission from existing user 3) attached existing policy directly.
3. Select policy from 3rd option click on next
4. Add tags click on next
5. Click on create user

User create successfully.

**Create roles :-**

1. Click on roles
2. Click on create roles
3. **Select types of trusted entity**
4. **AWS service** (we are using it common use cases is EC2 and lambda)
5. **Another AWS account**