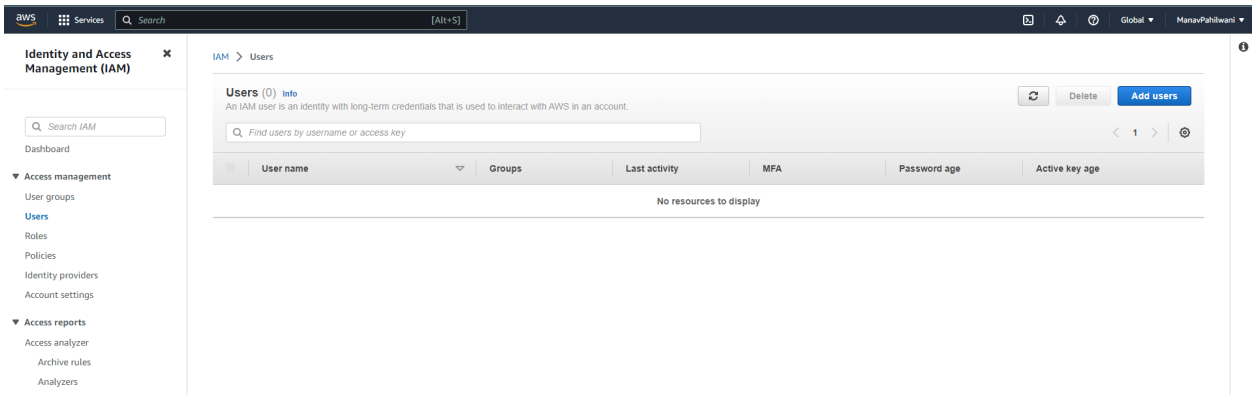
Name - Manav Pahilwani
Roll No - 37
Class - D11AD

Experiment no. 7

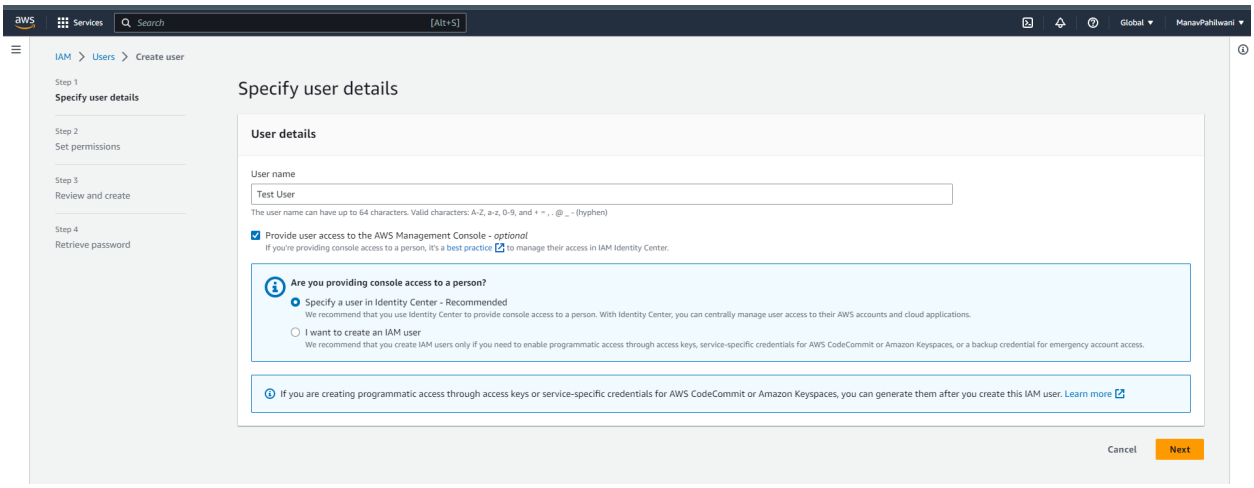
Aim: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

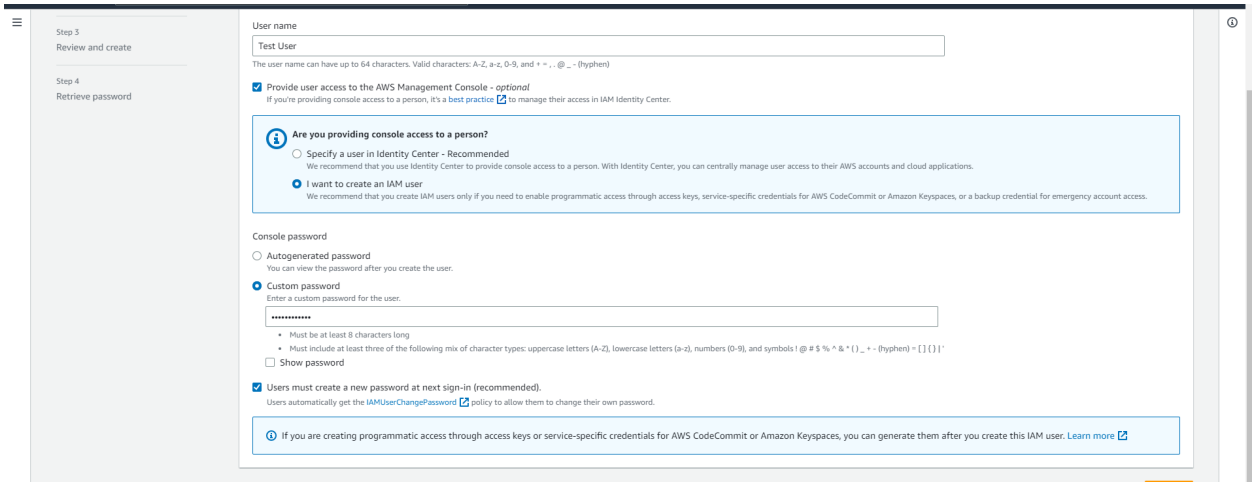
Theory:
AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
During this lab experience, you will learn how to create IAM users and groups with specific policies.

Implementation:
Create IAM user:
Step1: Click on Add user and add name of the user. Click on Next.

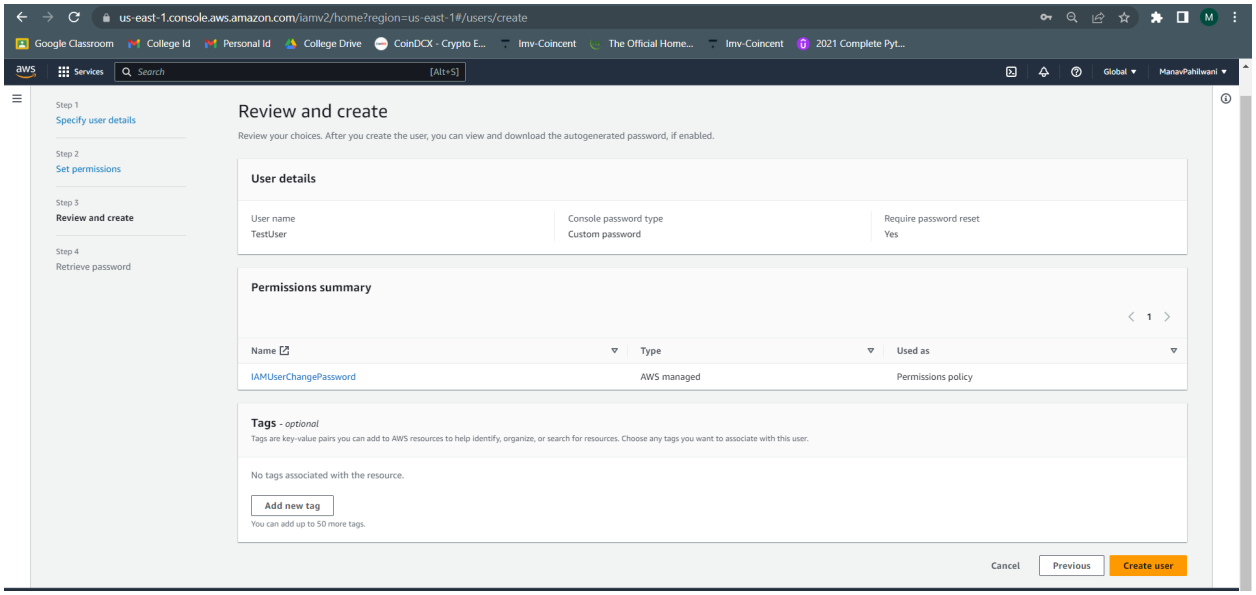


Step 2:
Select I want to create an IAM user. Enter custom password and click on next

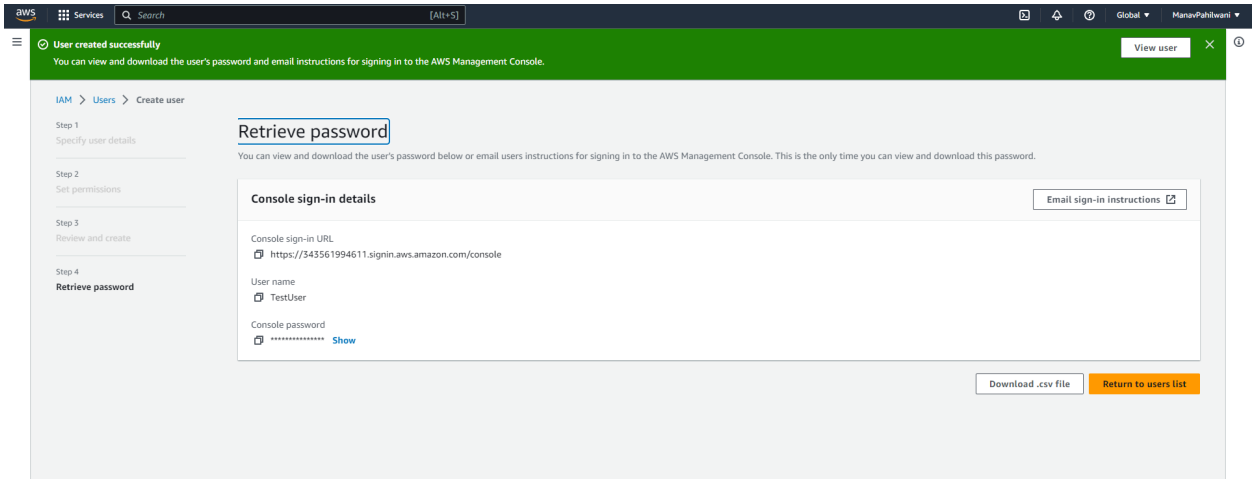




Step3: Finally click on create user.



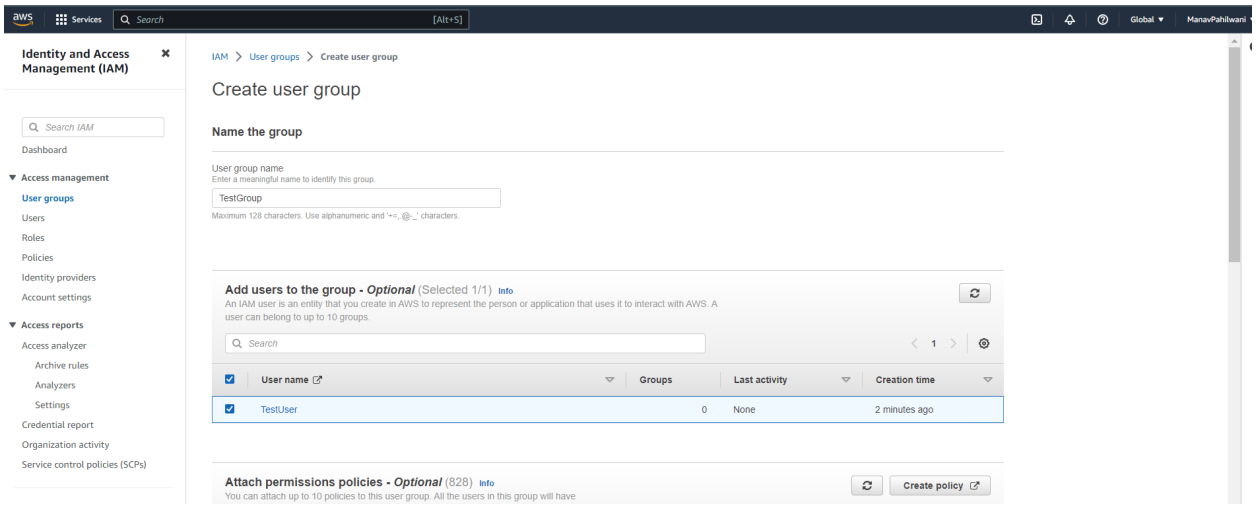
After creating a user you can download a .csv file which contains the password.



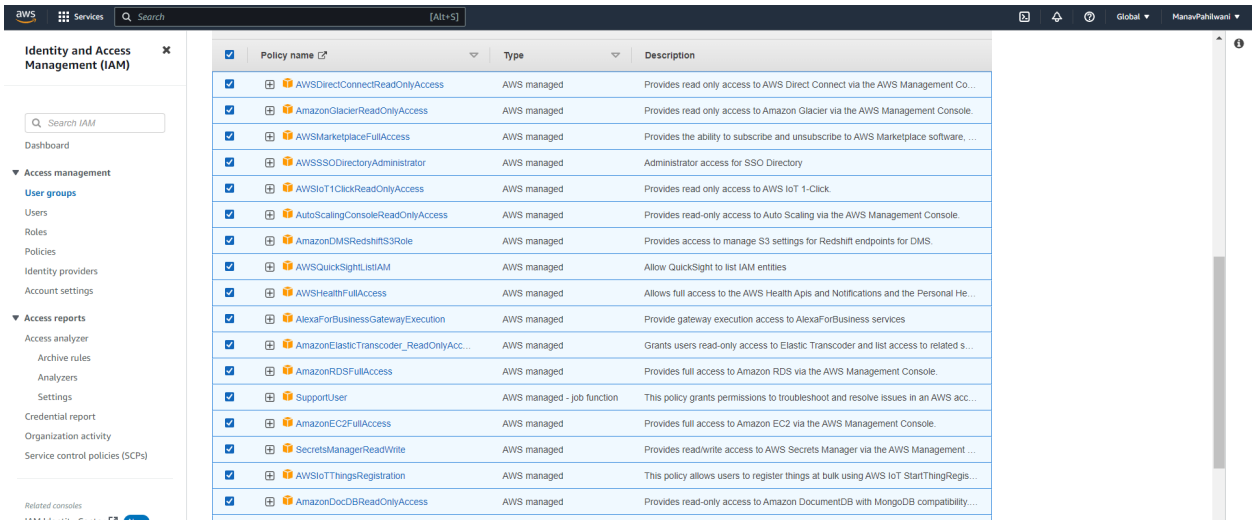
Create IAM groups:

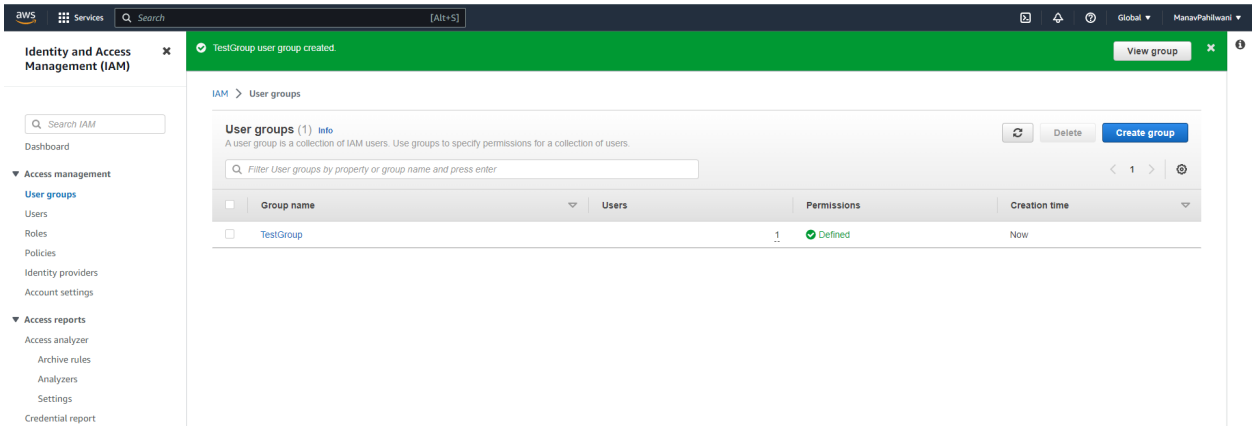
Step1:

In user group, click on Create group.



You can attach permission policies if needed. And click on the create group button.





IAM User Group is created successfully with the user you just created.

Conclusion - Identity and Access Management (IAM) is a critical component of any cloud infrastructure. IAM provides a framework for controlling access to resources in the cloud, ensuring that only authorized users have access to sensitive data and applications.