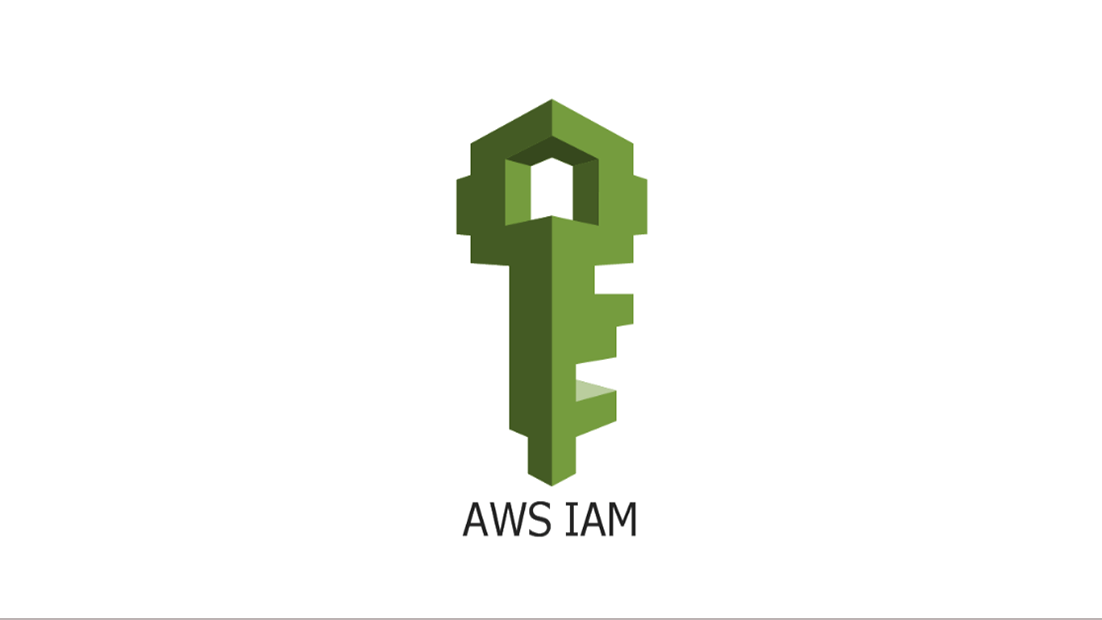
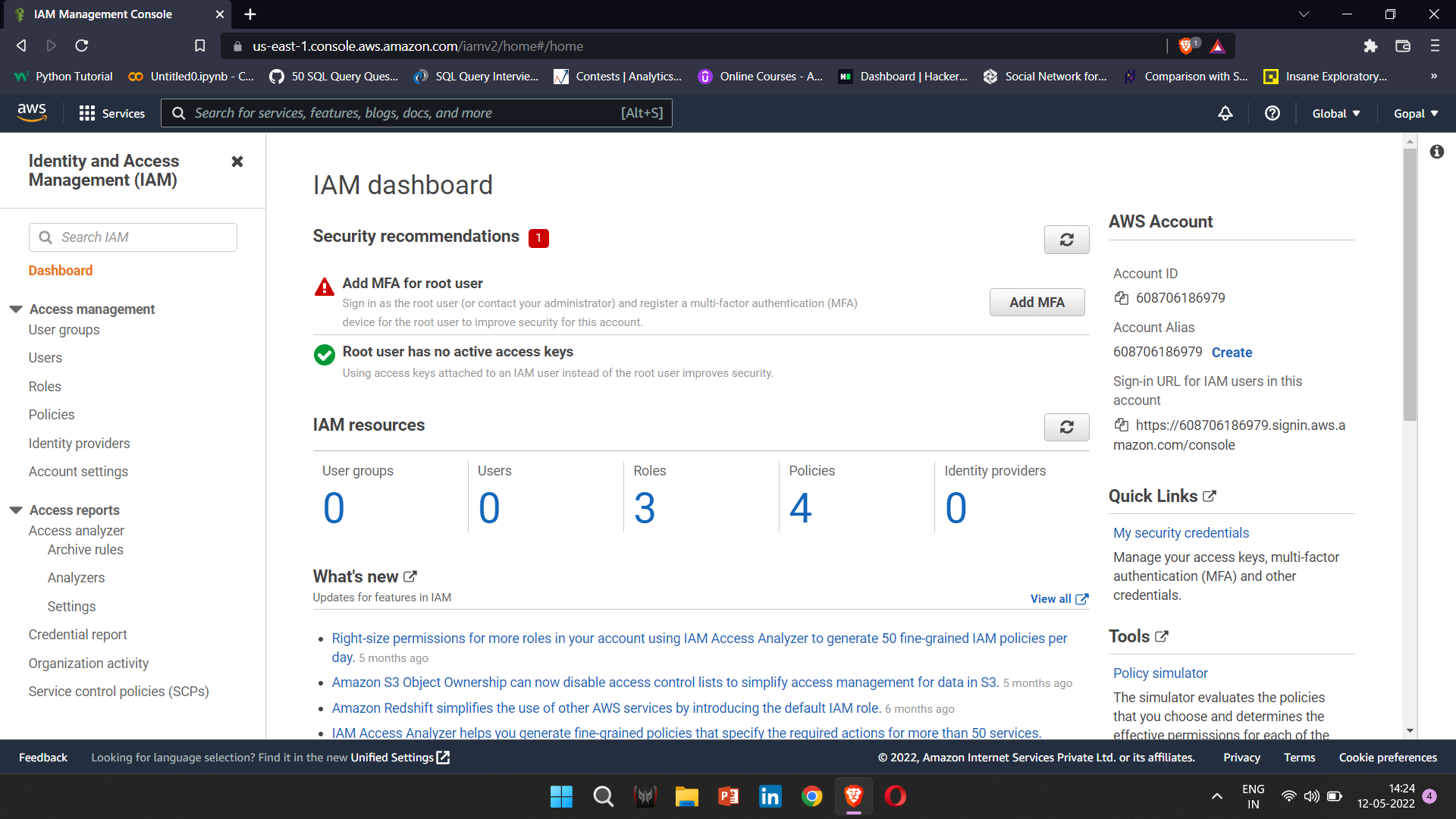
**AWS IAM**

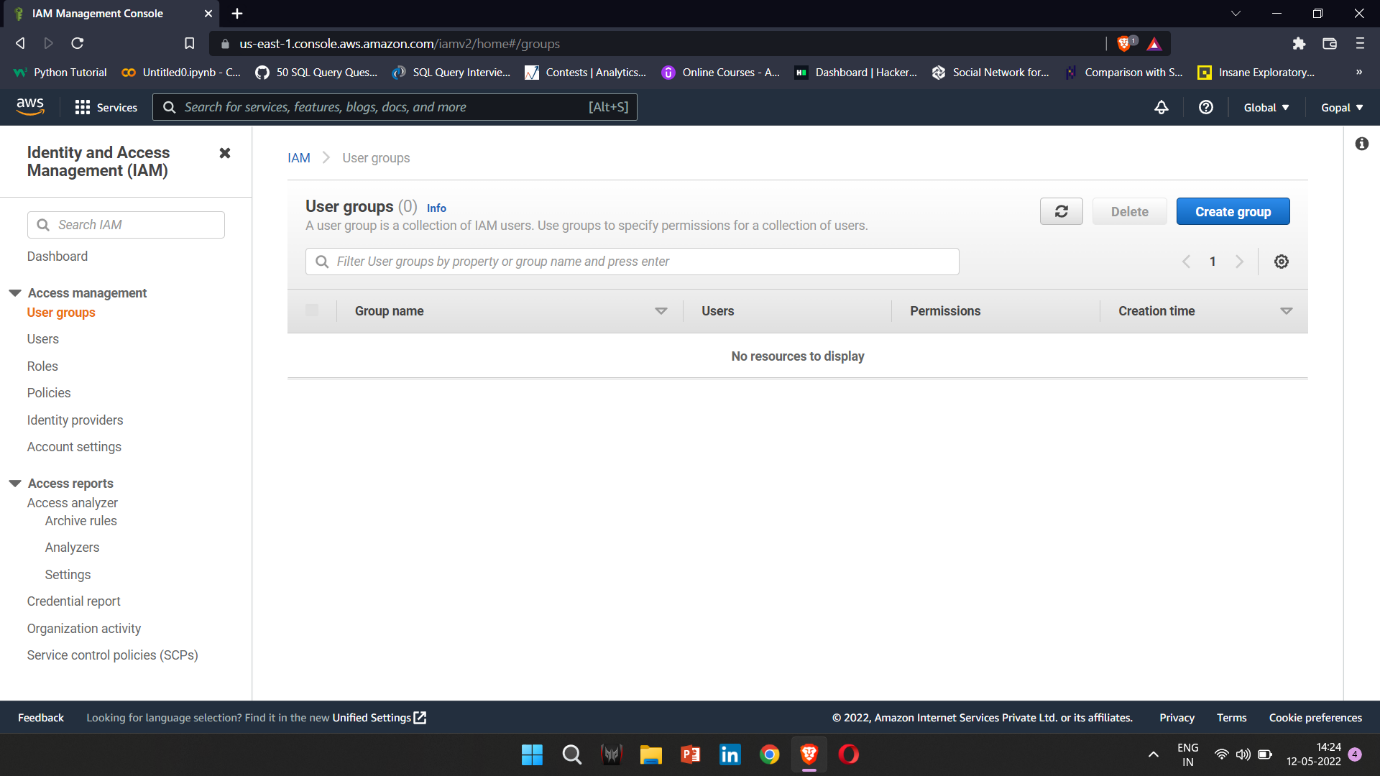
**Identity and Access Management**

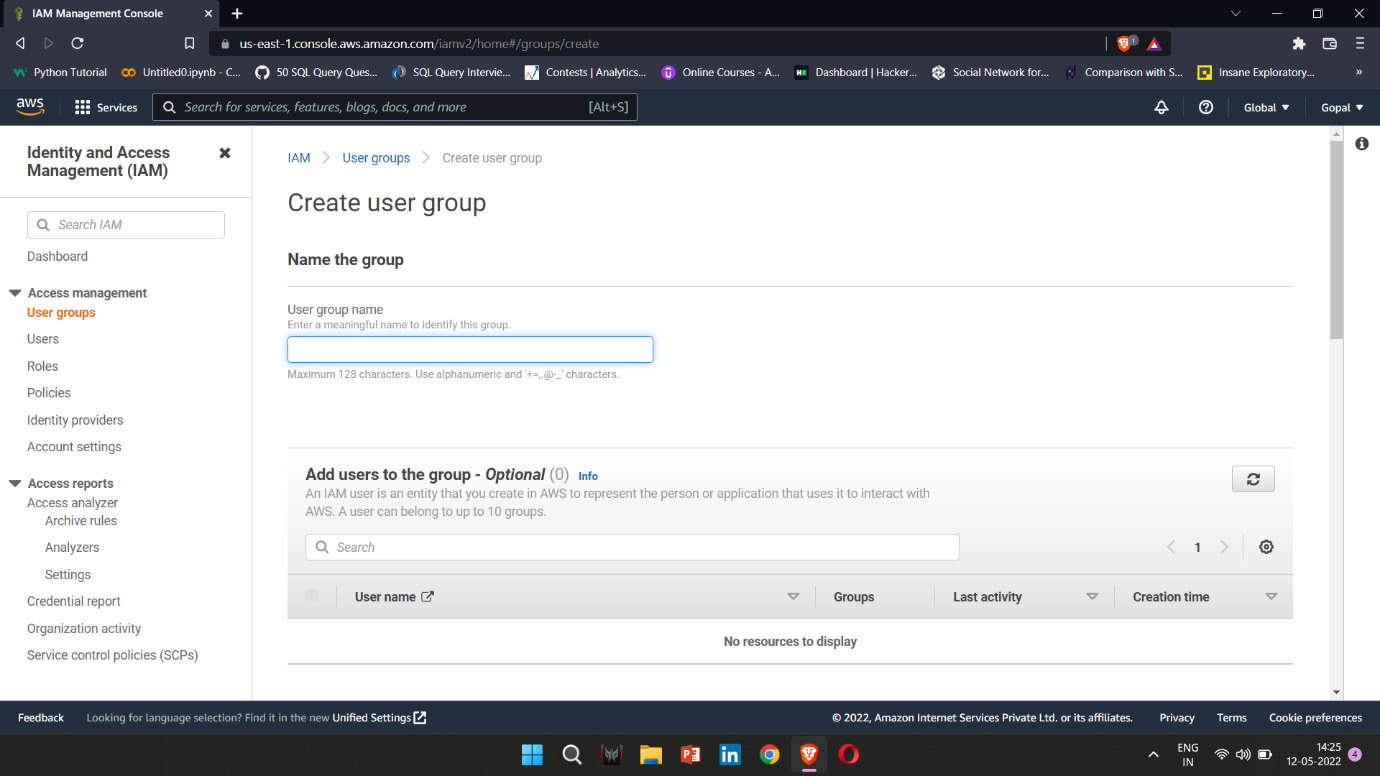
**Case Study**



**Steps to Create IAM groups:**

1. Log in to your AWS account.  
2. Click on the IAM link under the Security, Identity, & Compliance category on your AWS Services home page.

3. From the left-hand menu, click Groups.

4. Next, click on the Create New Group button.

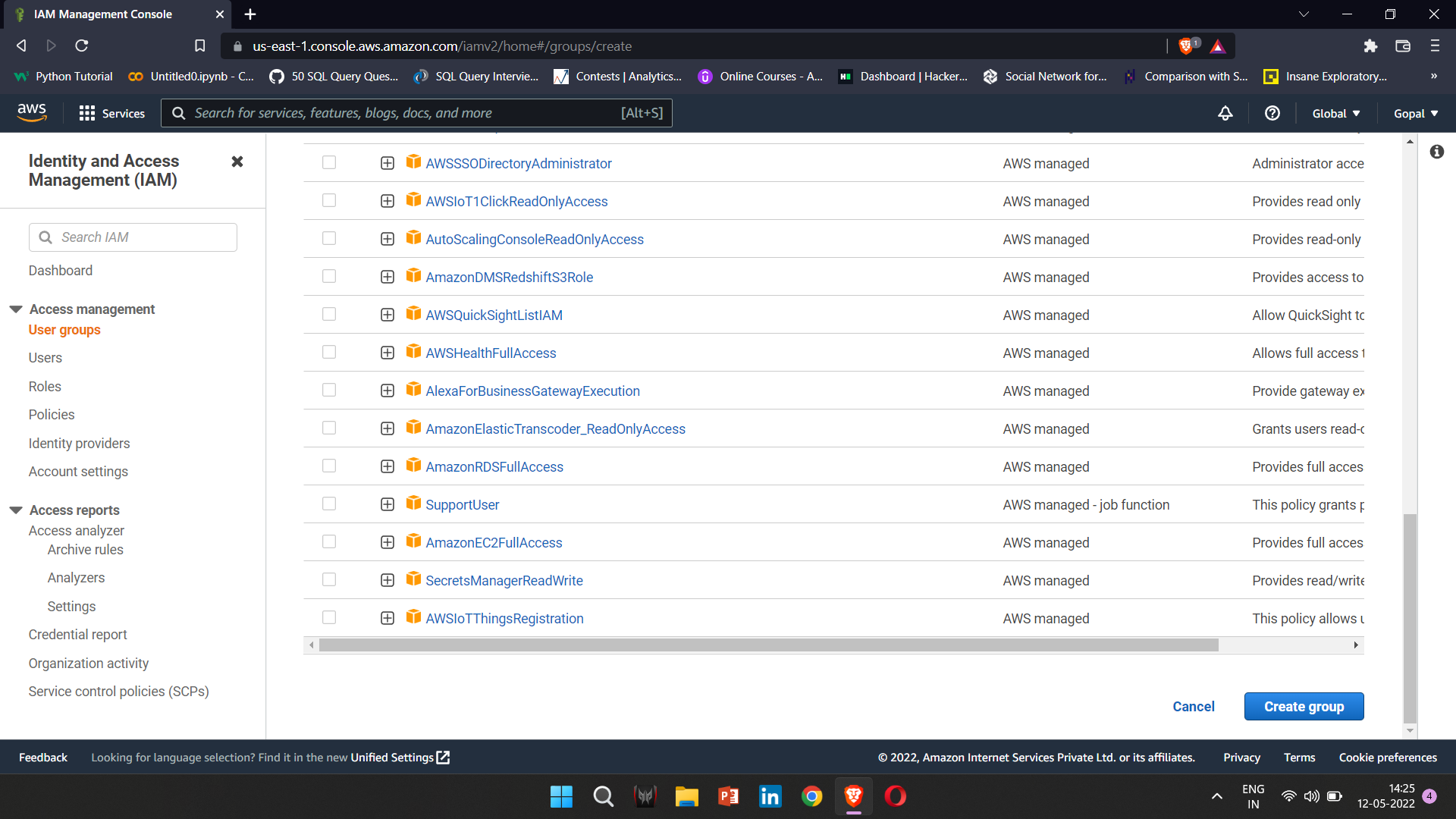
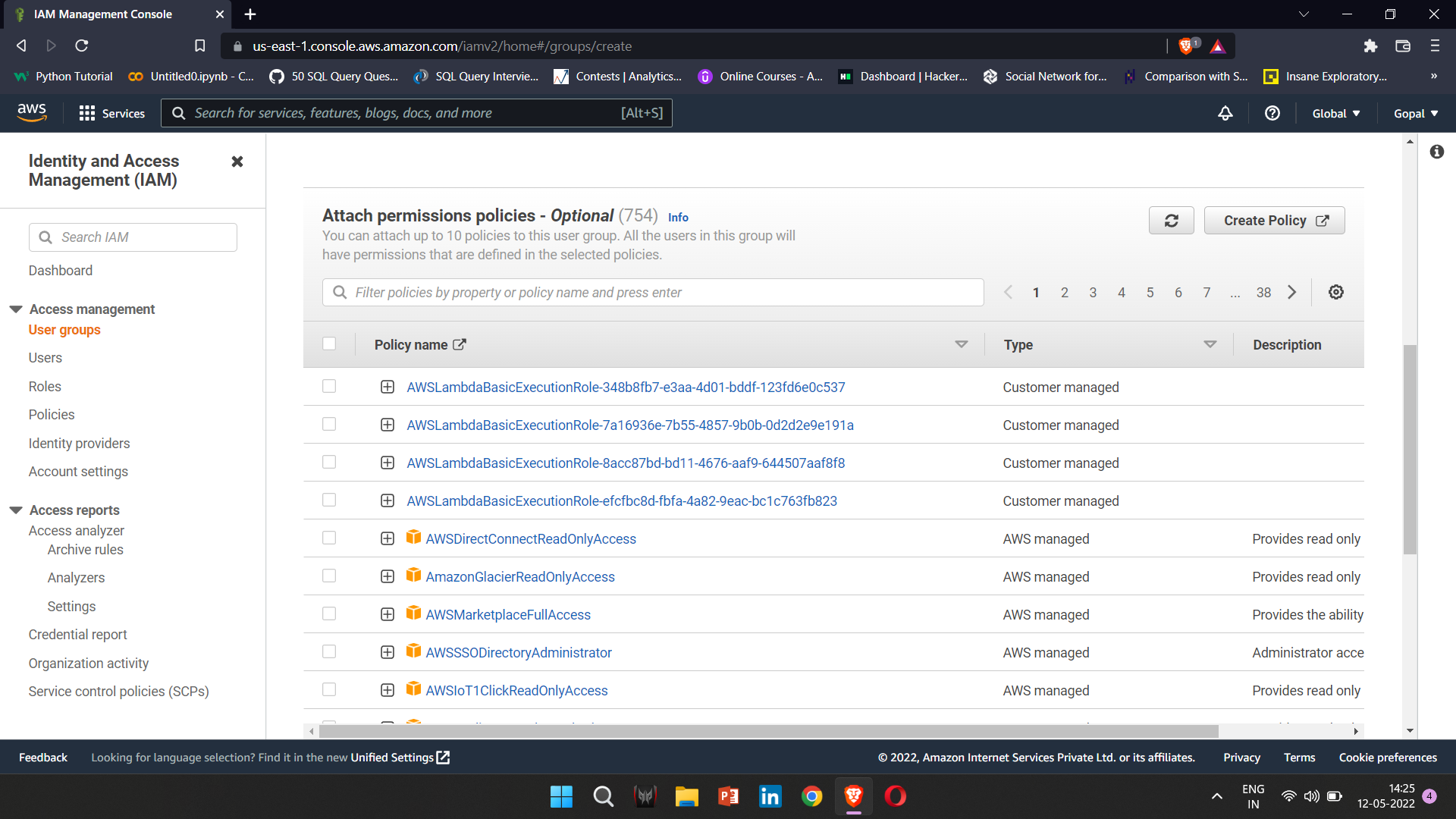
5. You will then be presented with a step-by-step wizard. Provide a group  
 name for your new group. For this exercise, type in demo\_iam.

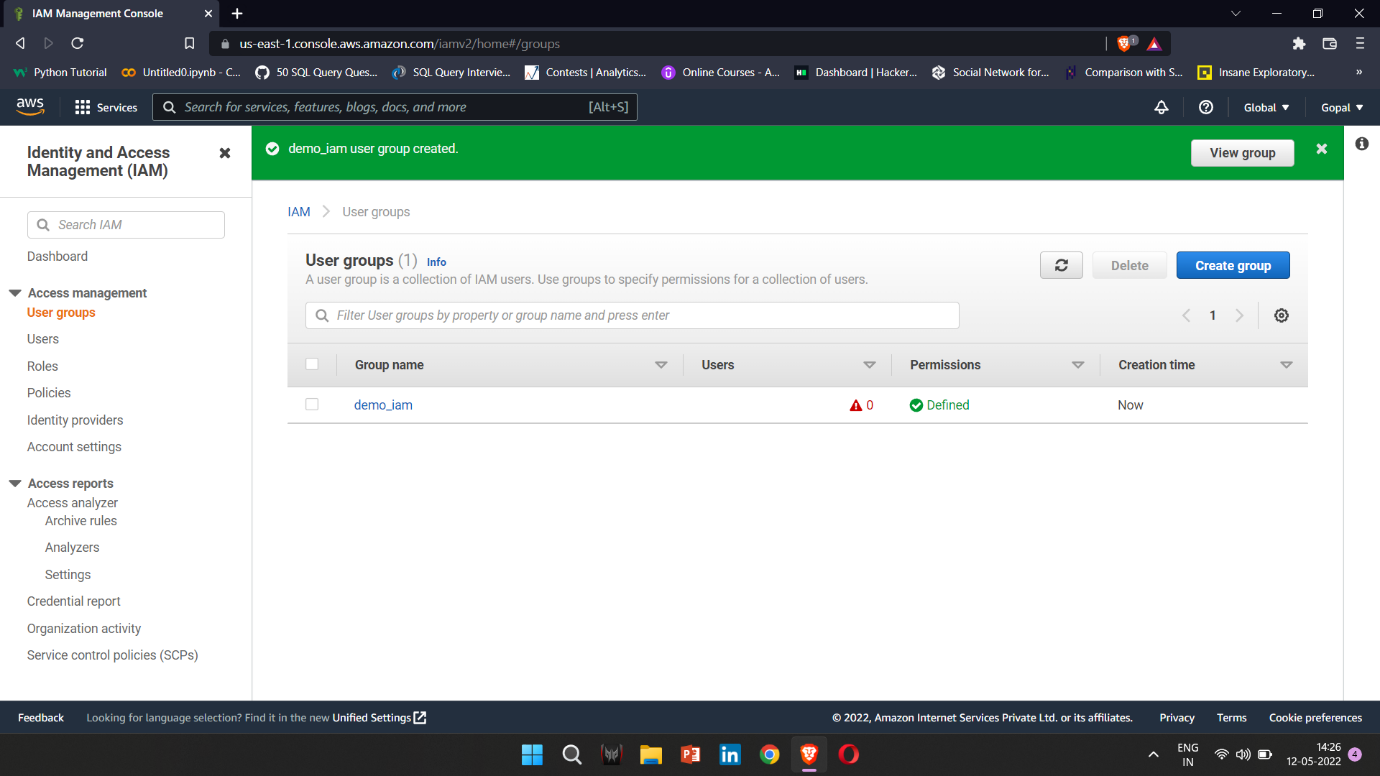
6. Click the Next Step button in the bottom right-hand corner of the  
 screen.

7. You now need to attach a policy. You can create your own customer managed policies but for the purposes of this exercise, type S3 in the Policy Type filter search box. This will narrow down the available  
policies that relate to Amazon S3.

8. Tick the checkbox next to the AmazonS3FullAccess policy.

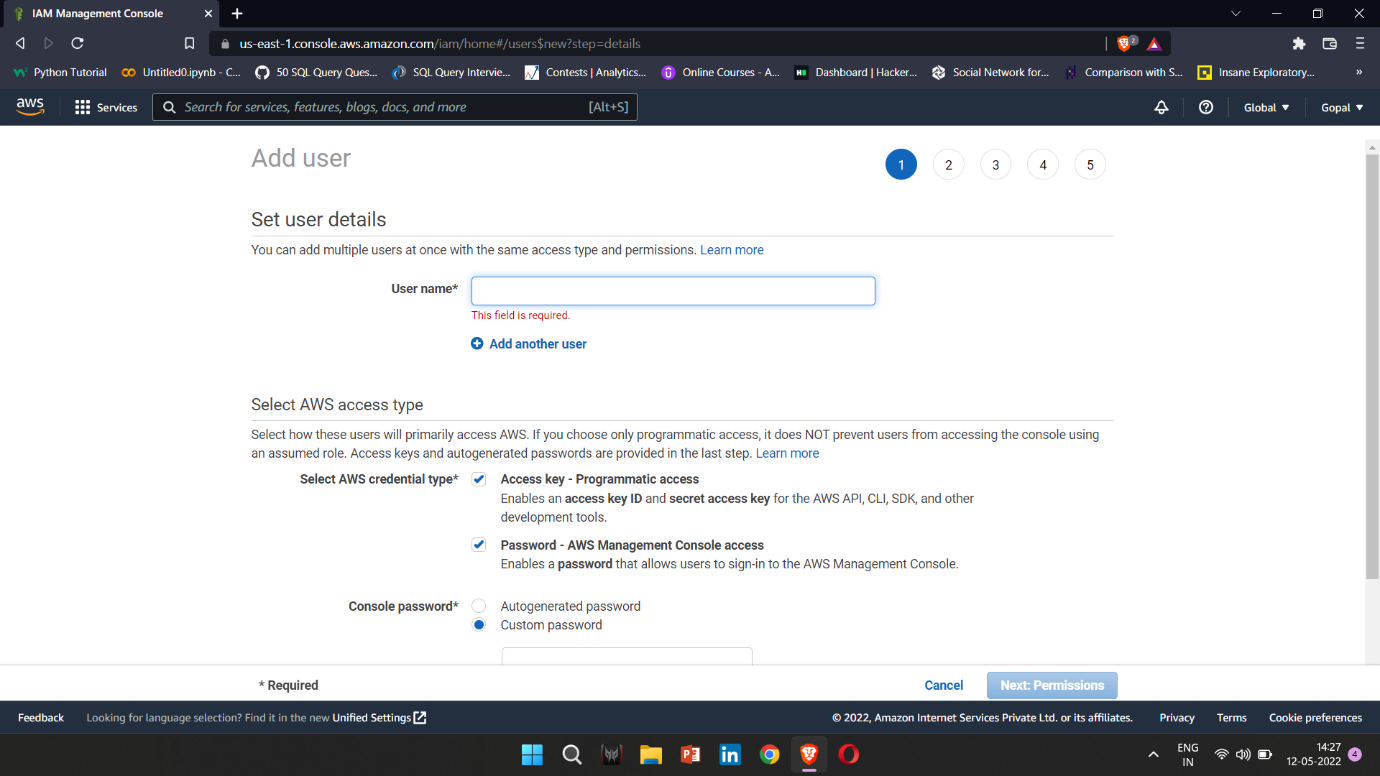
9. Click the Next Step button in the bottom right-hand corner of the  
 screen.

10. Finally, click the Create Group button in the bottom right-hand corner  
 of the screen. 

You will now see that your group has been created and listed under GroupName

**Creating an IAM user**:

1. In the IAM dashboard, click on Users from the left-hand menu.  
2. Click the Add user button.  
3. In the User name textbox, type in user name. (all lowercase).

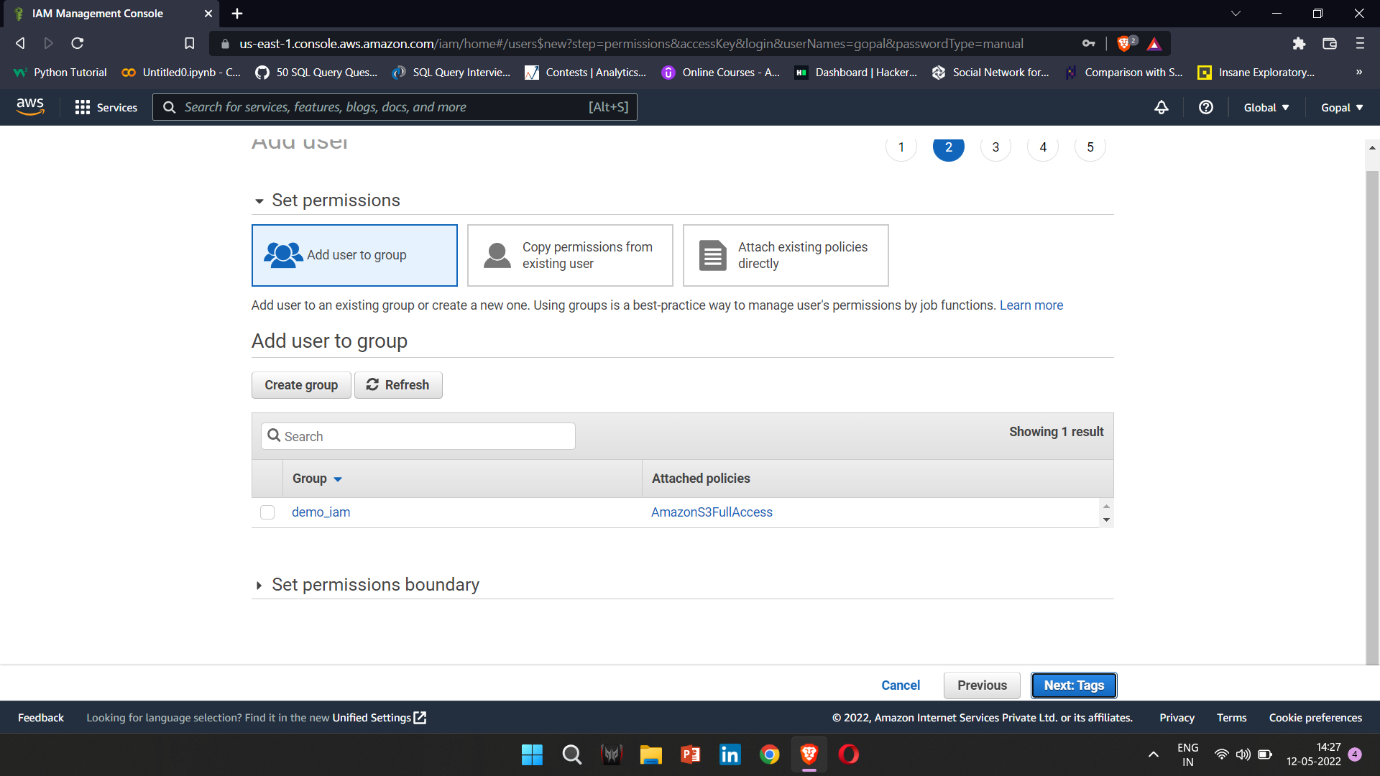


4. Next, you need to select the type of access you want to grant user. You can tick both boxes – Programmatic Access and AWS Management Console access.  
5. To access the AWS account via the console, you need to create a  
password for the user. Select Custom password and choose a complex password of your choice. Type that password in the textbox provided.

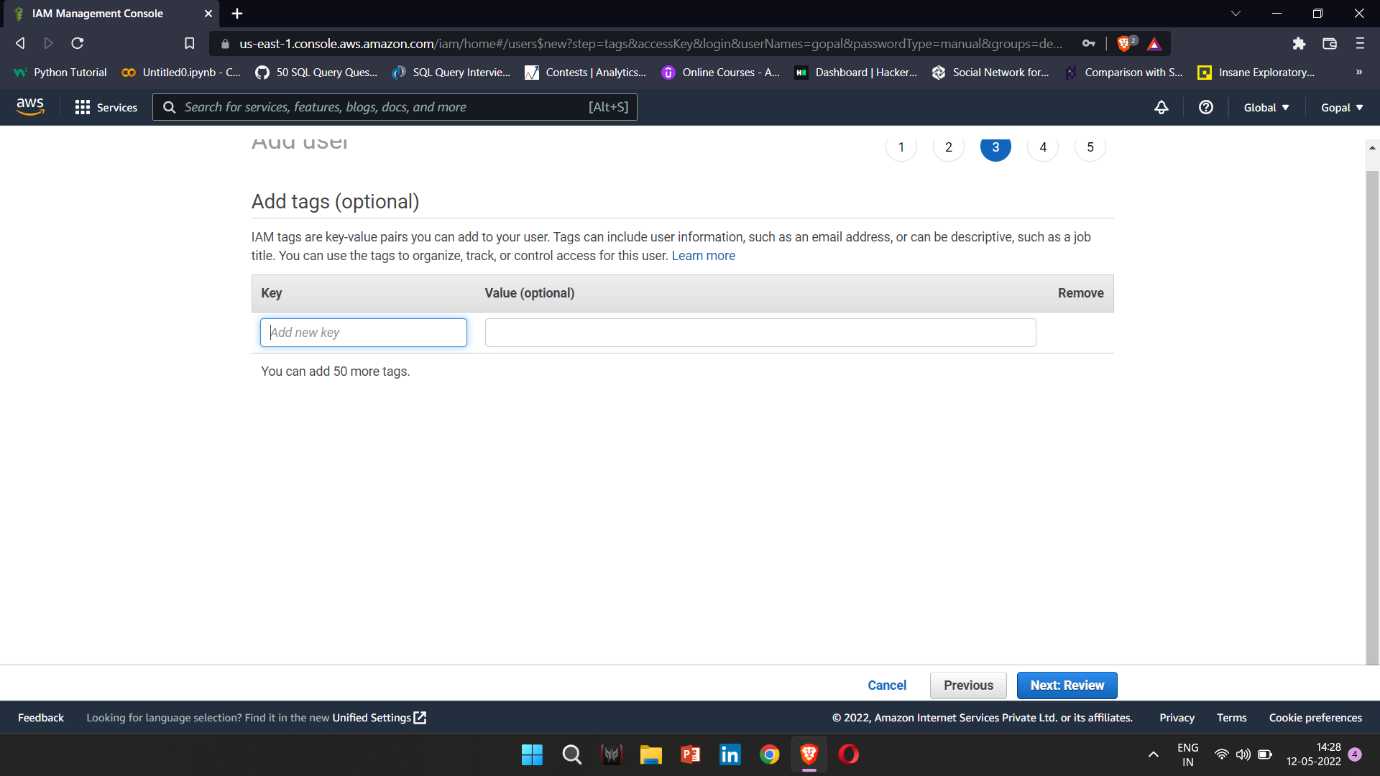
6. An additional setting, Require password reset, enables you to force  
your IAM users to change their password at the next login. That way,  
you will not know what their password is when they change it and it is  
best practice to follow

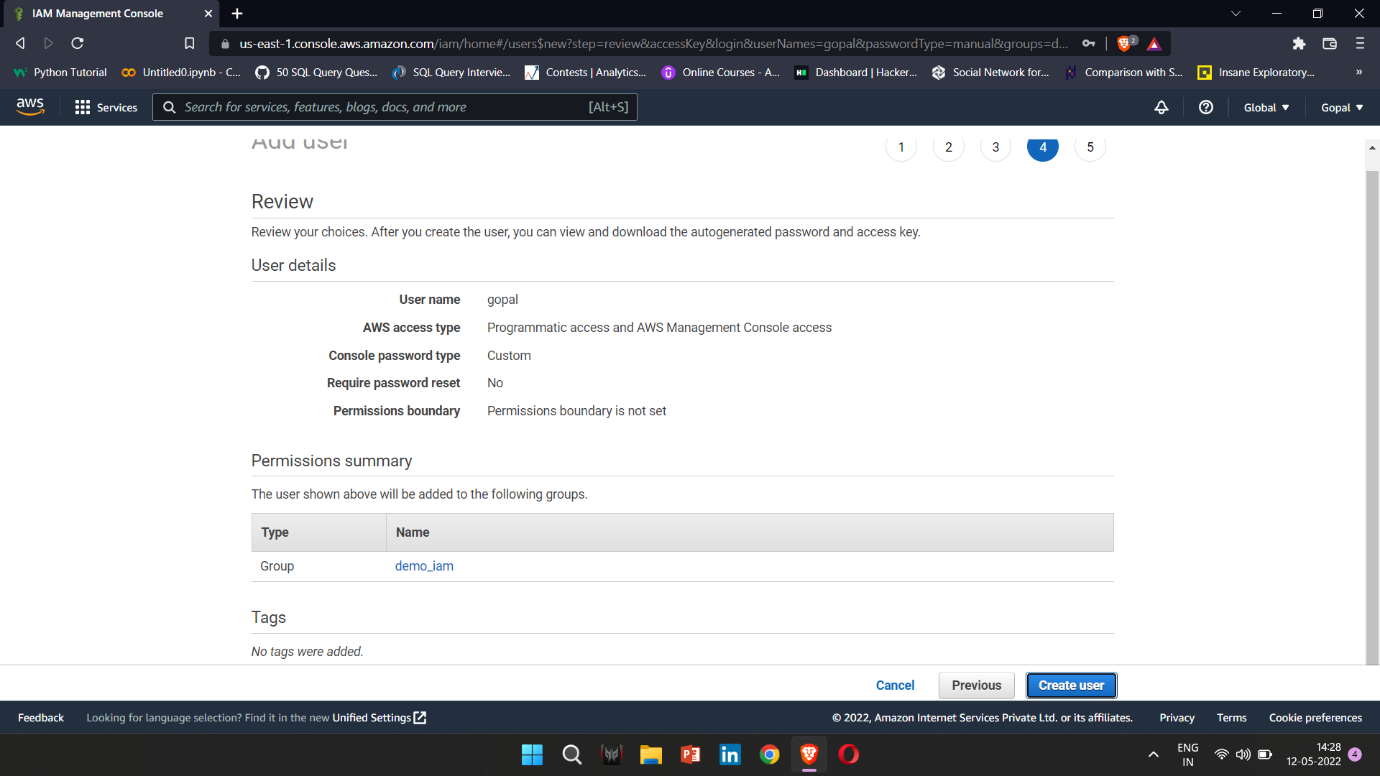
7. Click the Next:Permissions button in the bottom left-hand corner of the  
screen

8. You now have the option to set permissions for the user. As we have  
already created a group with the right set of permissions attached to it,  
we simply need to make this user a member of the group.

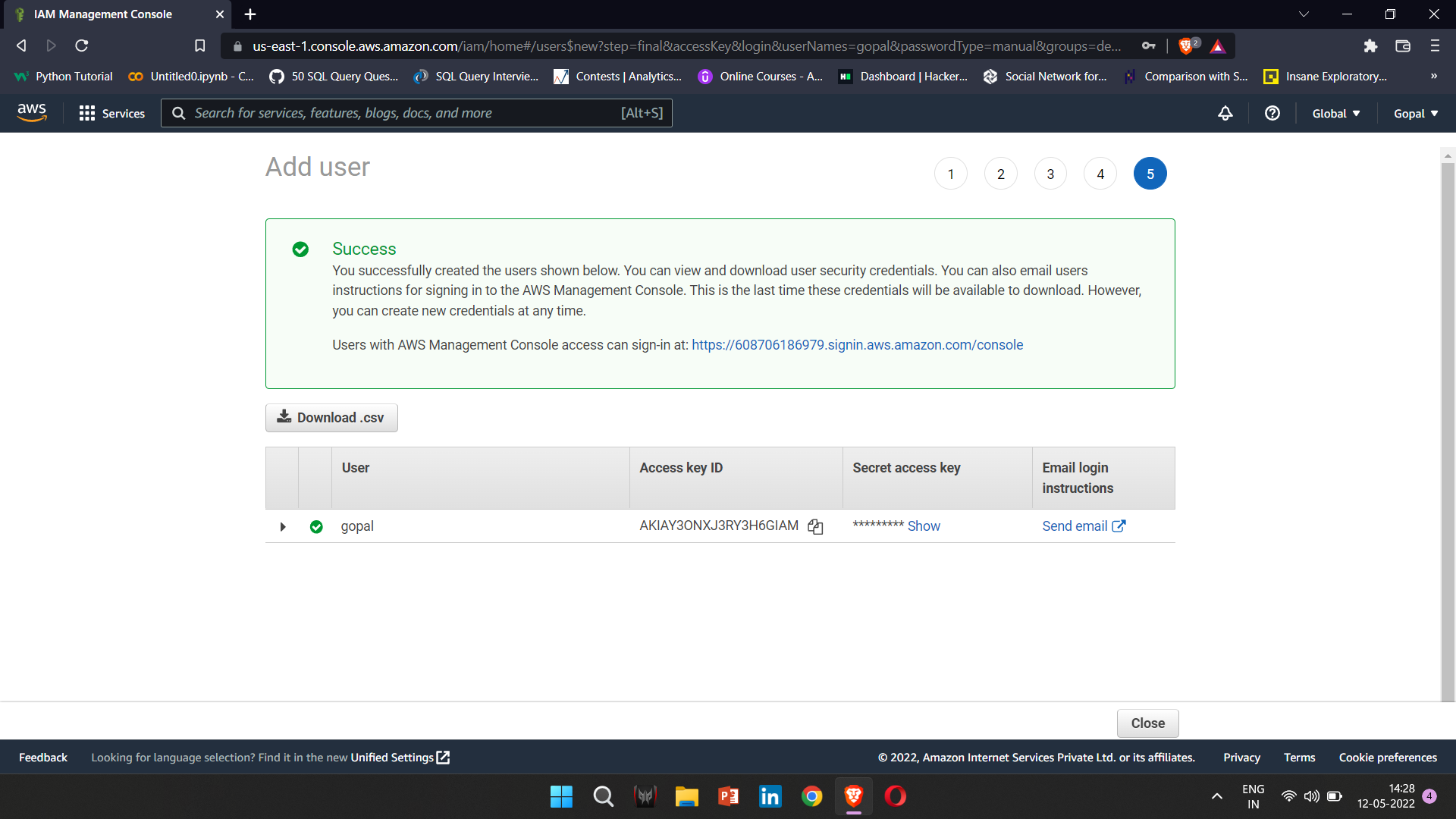


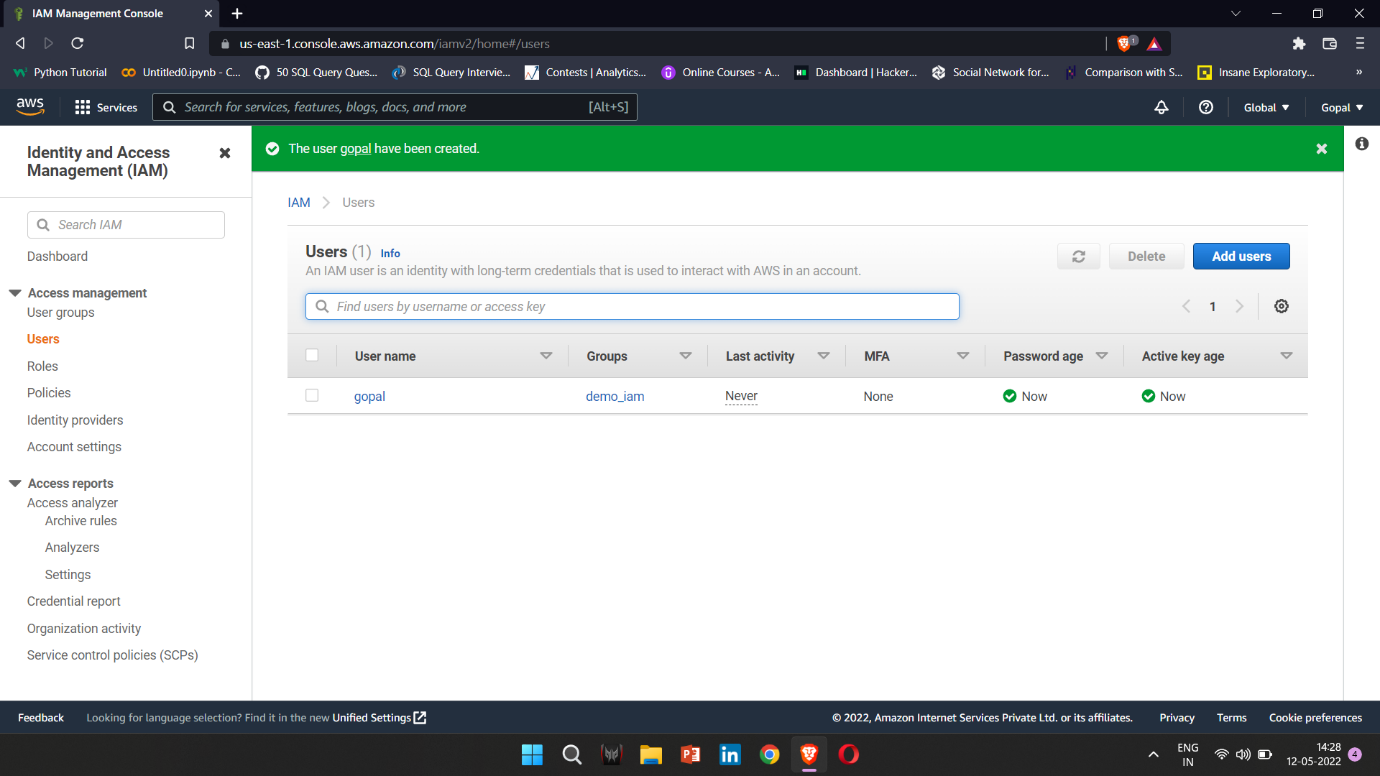
9. Tags are key-value pairs that you can attach to any resource. You can  
attach up to 50 tags to each resource and they enable you to classify  
your resources better. You can then use tags to understand cost  
allocation and to identify and manage your resources. Tags can include  
user information, such as an email address, or can be descriptive, such  
as a job title.



10. Click the Next:Review button in the bottom right-hand corner of the  
screen.

11. You can now review all your settings for the user and once satisfied, go ahead and click the Create user button in the bottom right-hand corner  
of the screen.

12. You are now presented with a Success screen, which confirms that the  
user has been created. You are also informed of the option to download  
your access keys. Access keys are like usernames and passwords and  
comprise an access key ID (similar to the username) and the secret  
access key (similar to the password). Access keys are used to grant  
programmatic access via the AWS CLI or using the AWS SDKs. It is  
important that you download these keys now and keep them safe on  
your computer. If you move away from this screen, the secret access  
key (such as the password) is no longer visible, and you would need to  
recreate the keys. So ensure that you download the keys  
by clicking on the Download .csv button. Store the .csv file.

14. Click the Close button in the bottom right-hand corner of the screen to  
exit from the user setup wizard.