

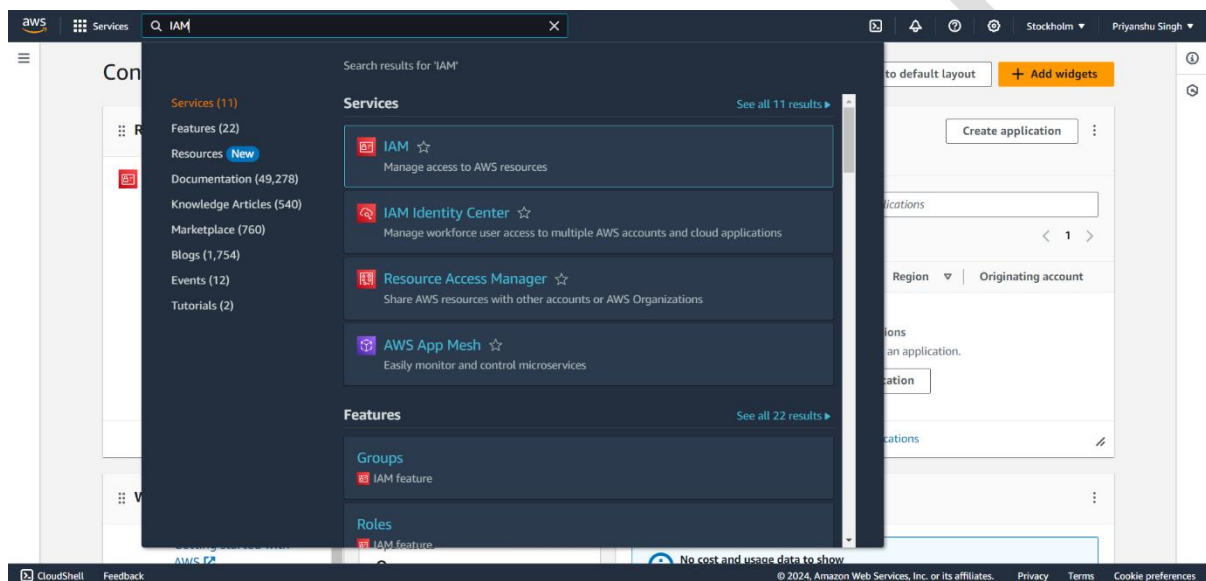
Assignment 3:

Problem Statement: Create IAM user and give full access to S3.

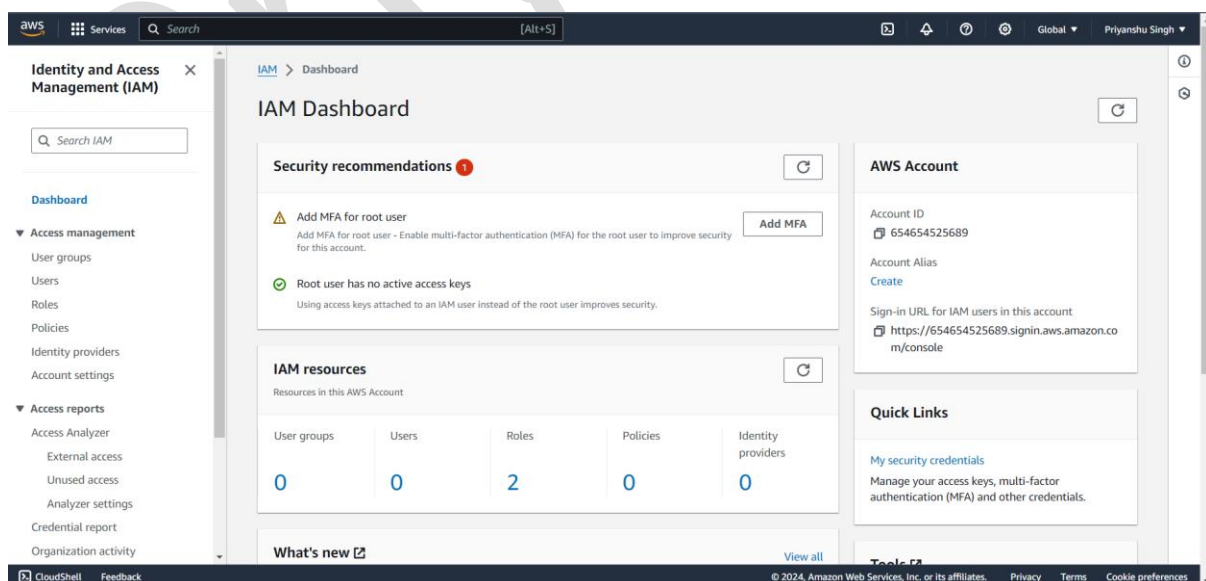
Steps:

Still now we were using Root user which has full control .It is like project manager and IAM (Identity and Access Management) users are like team members. They have to assigned with one or more than one particular tasks. If IAM is given full access with S3(Simple Storage Services) then it can not access EC2(Elastic Compute Cloud) or RDS(Relational Database Service).So the steps of this assignment are:-

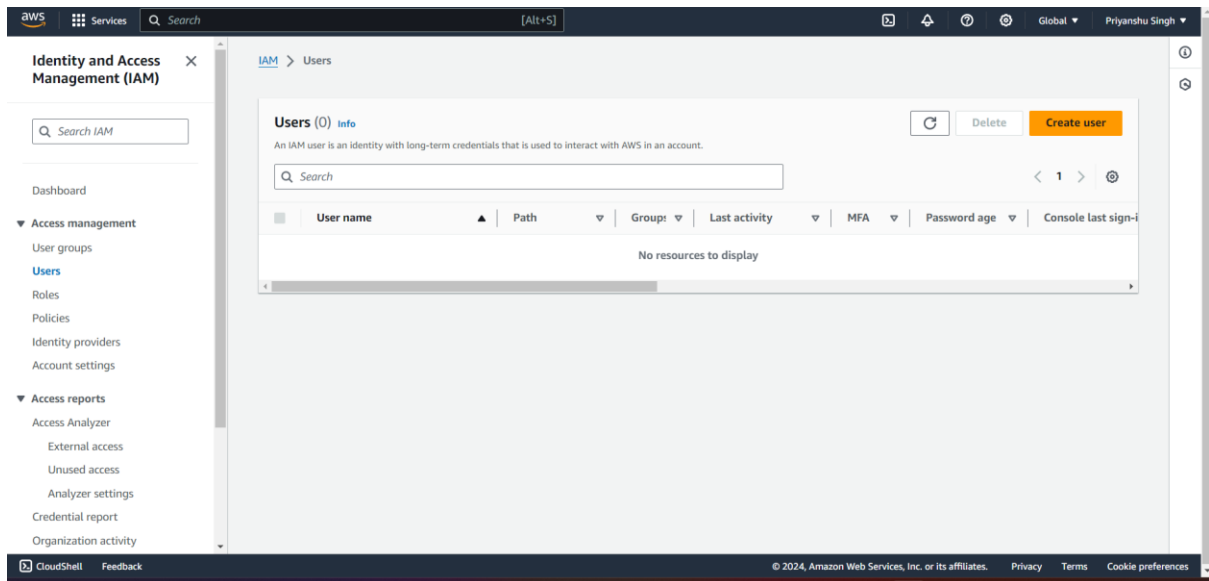
- At first search IAM and click on IAM option.



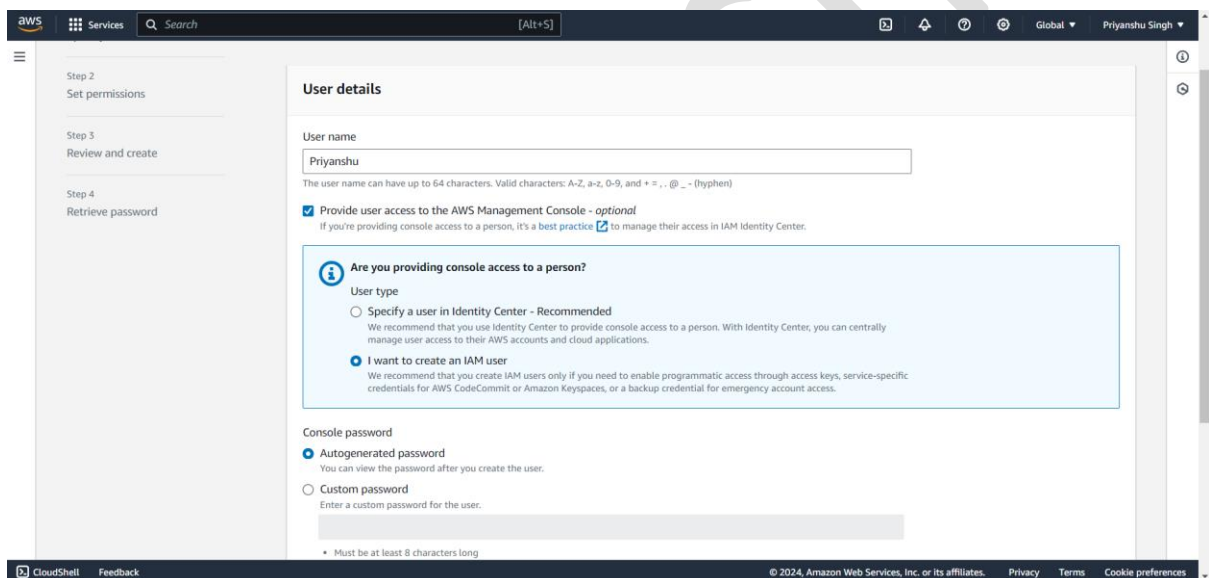
- Now go to Access management and click on Users.



- Now click on Create user.



- Now give username and click on check box stating 'Provide user access to the AWS Management Console – optional'. After that click on I want to create an IAM user.



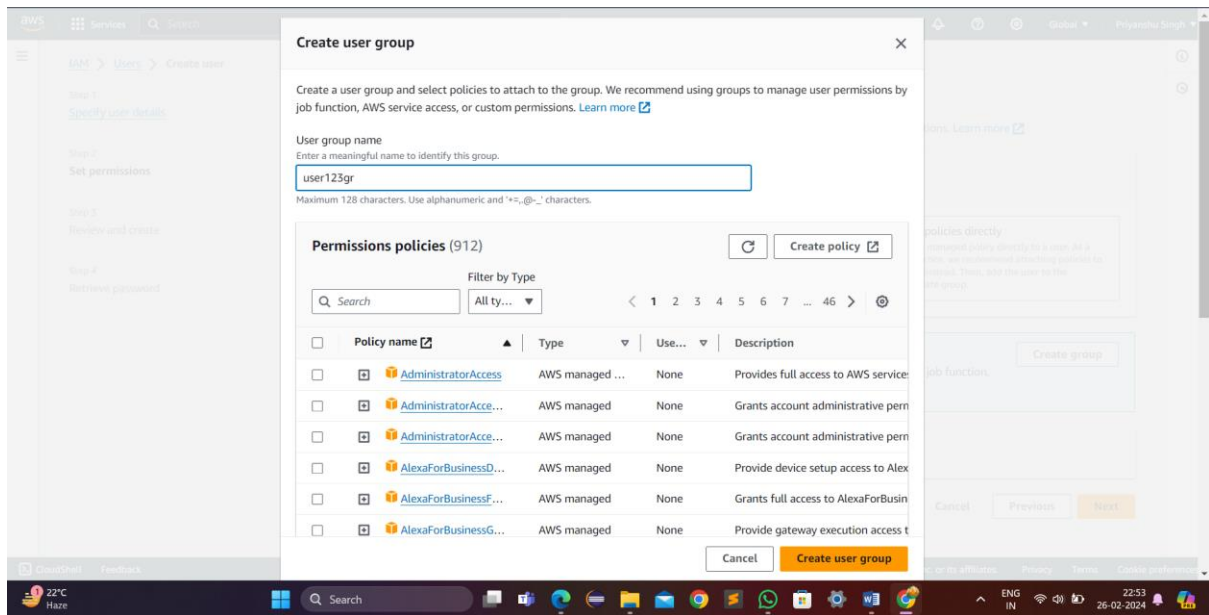
- Now click on Custom password and give password following the rules mentioned bellow and now uncheck the option stating Users must create a new password at next sign-in – Recommended. Now click on next option.

The screenshot shows the AWS IAM 'Create user' console. The 'User type' section has two options: 'Specify a user in Identity Center - Recommended' (unselected) and 'I want to create an IAM user' (selected). The 'Console password' section has two options: 'Autogenerated password' (unselected) and 'Custom password' (selected). A password input field is visible with a strength indicator. Below the input field, there are requirements: 'Must be at least 8 characters long' and 'Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ~'. There is also a 'Show password' checkbox (unchecked). At the bottom, there is a checkbox for 'Users must create a new password at next sign-in - Recommended' (checked), with a note that users will automatically get the 'IAMUserChangePassword' policy. A blue information box at the bottom states: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)'. The 'Next' button is highlighted in orange.

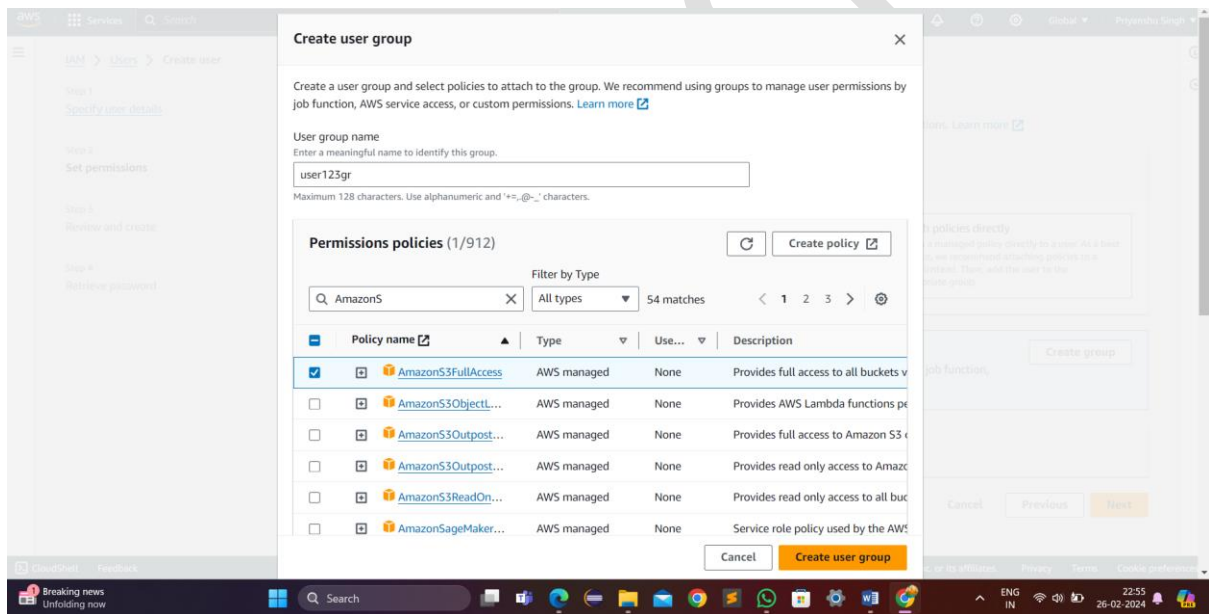
- Now click on Create group.

The screenshot shows the AWS IAM 'Set permissions' console. The left sidebar shows the navigation path: IAM > Users > Create user. The main content area is titled 'Set permissions' with a subtitle: 'Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)'. There are three 'Permissions options' cards: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below these cards is a blue information box titled 'Get started with groups' with a 'Create group' button. At the bottom, there is a section for 'Set permissions boundary - optional'. The 'Next' button is highlighted in orange.

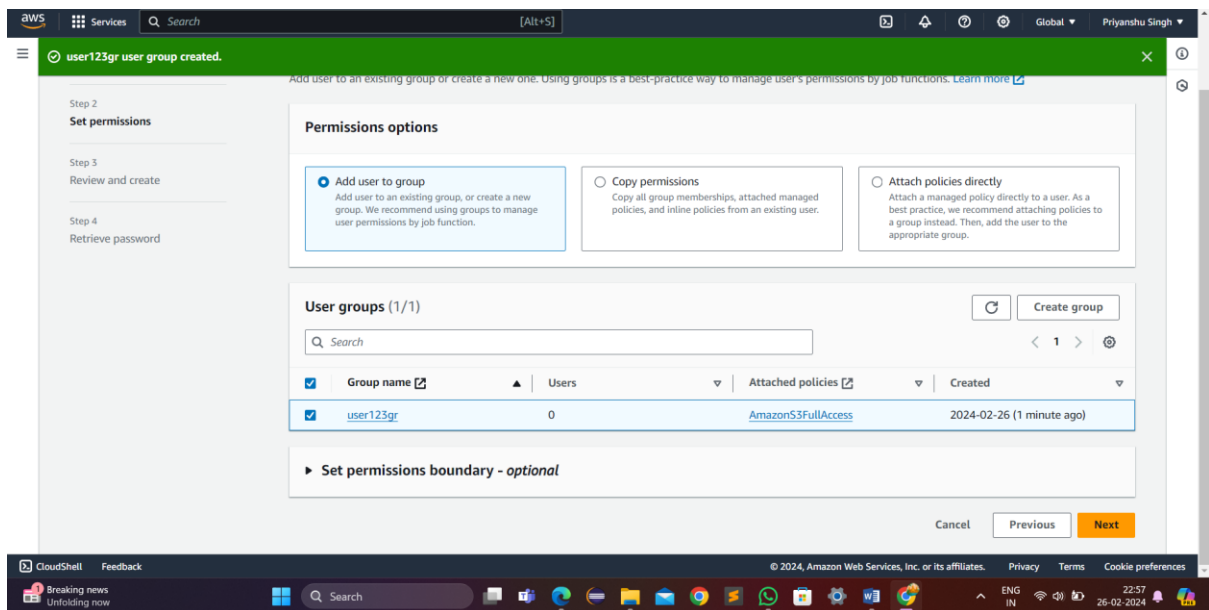
- Now give username for user group.



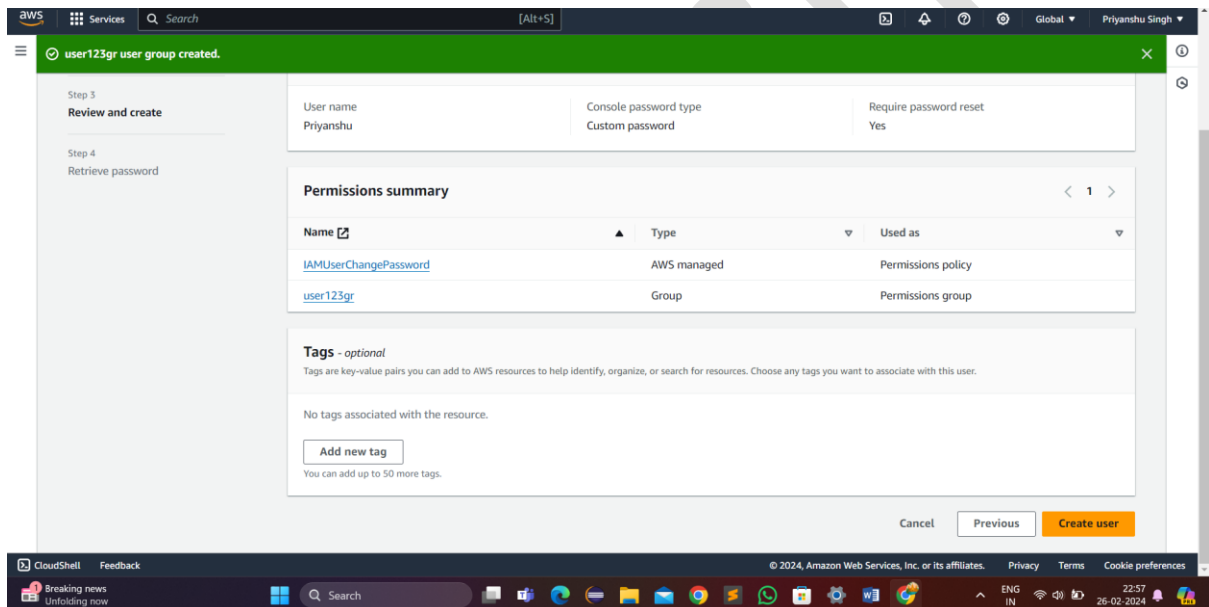
- After this in Permissions policies search s3 and search Amazons3fullaccess in Policy name not in Description. Click on searched checkbox and now click on Create user group.



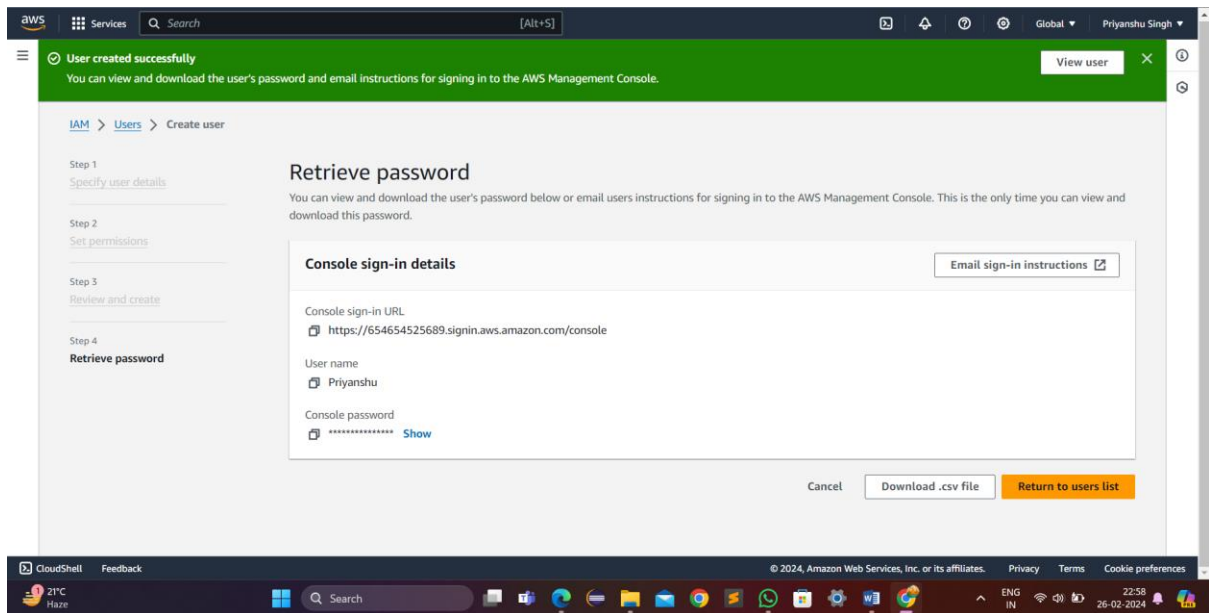
- After it our first user group will be created. Now click on Group name's checkbox and then click on Next.



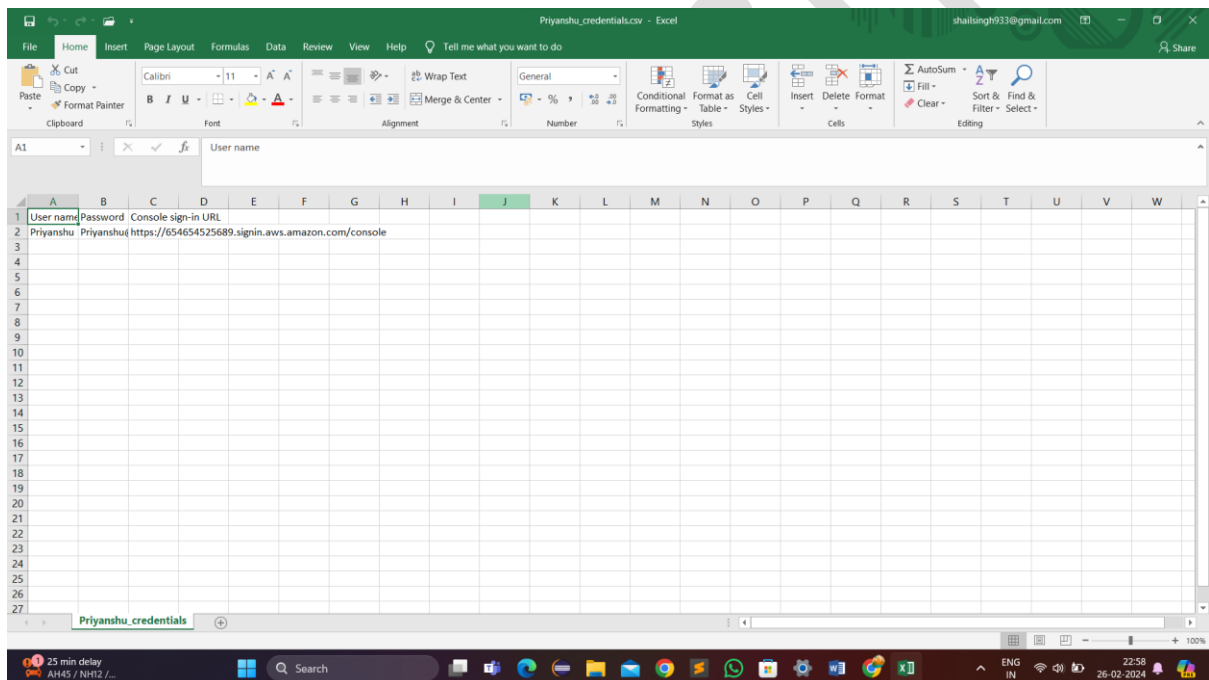
- Now again click on Create user.



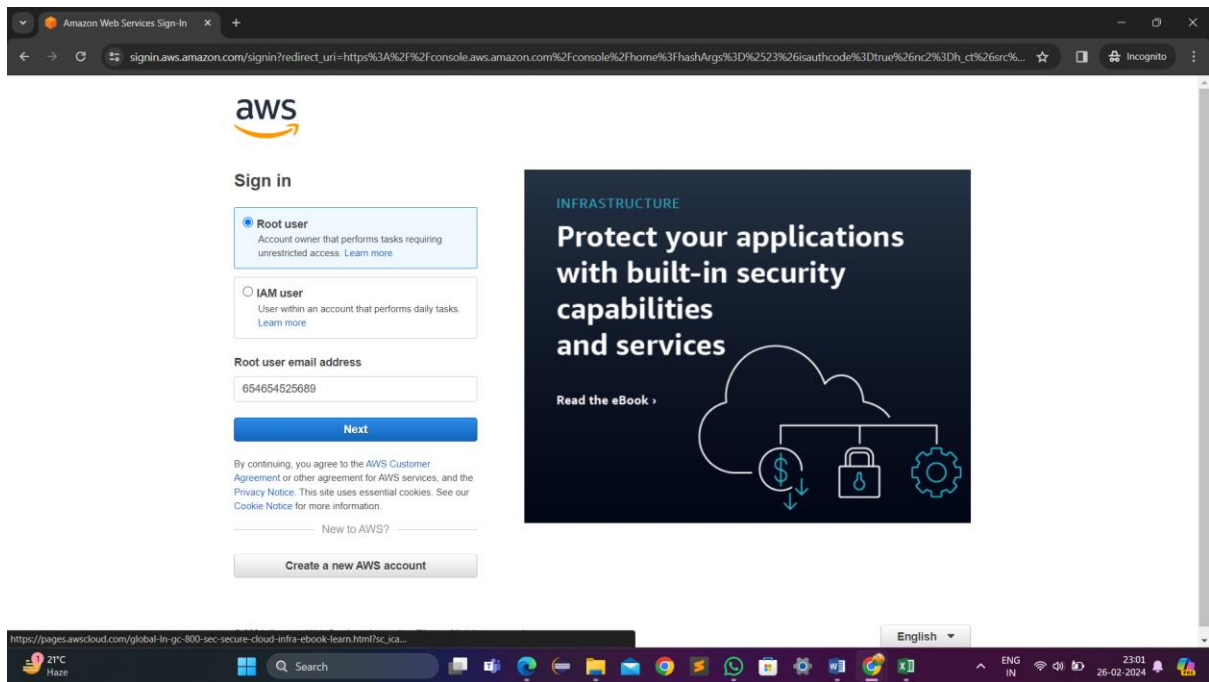
- Now user will be created successfully. Now download .csv file and click on Return on user list.



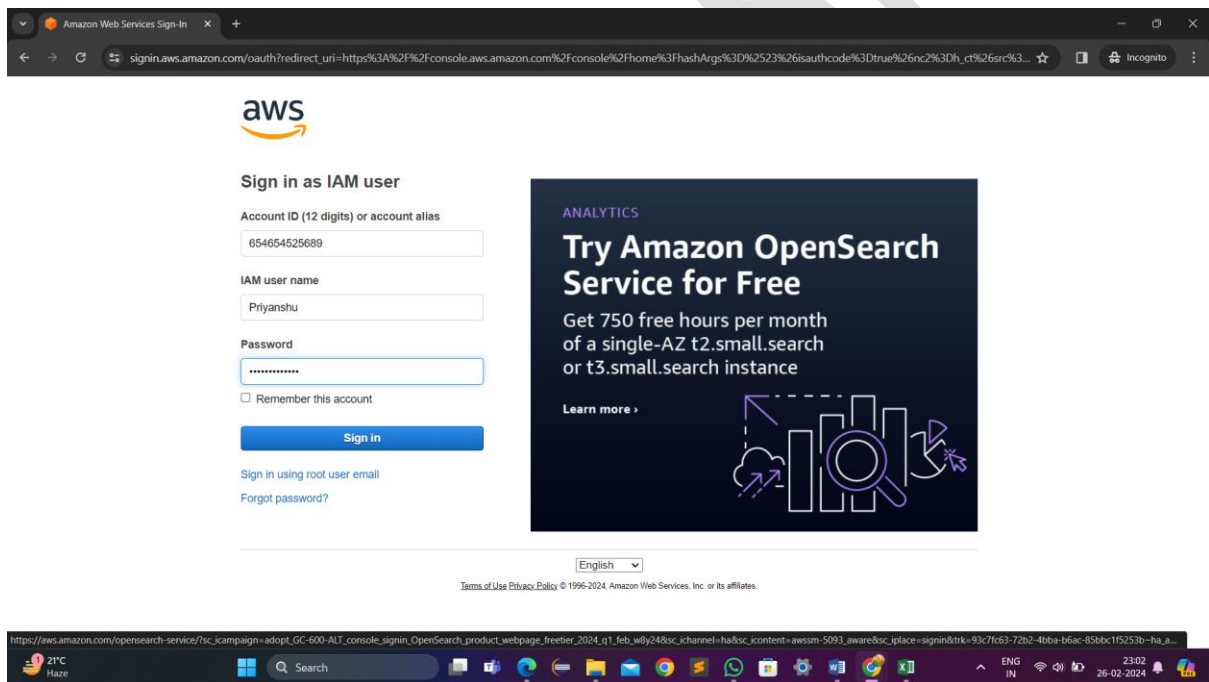
This is .csv file content:



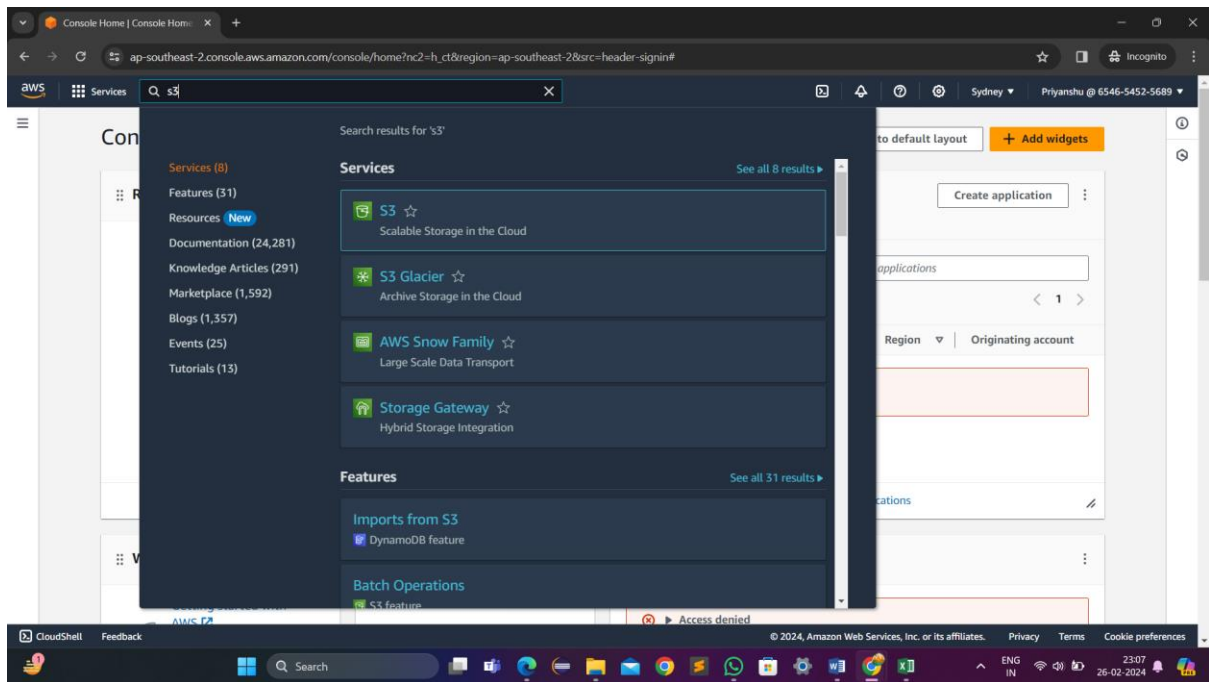
- Now go to incognito mode and search amazon console login. Click on IAM user and give 12 digit Account ID from that .csv file. Click on Next.



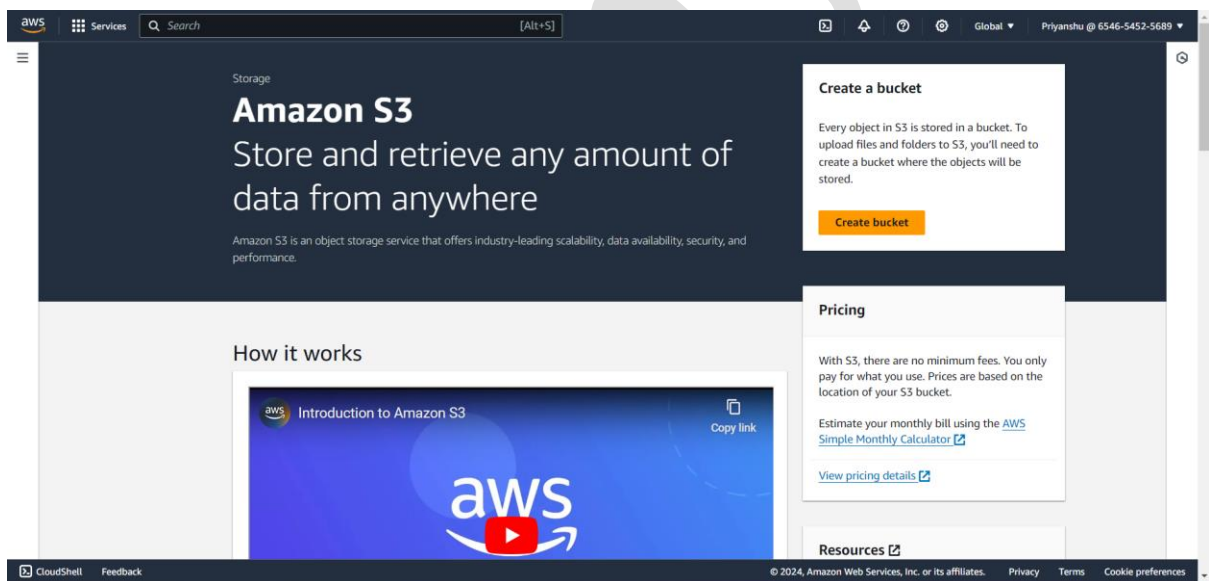
- Now give IAM user name and Password from that .csv file. Click on sign in.



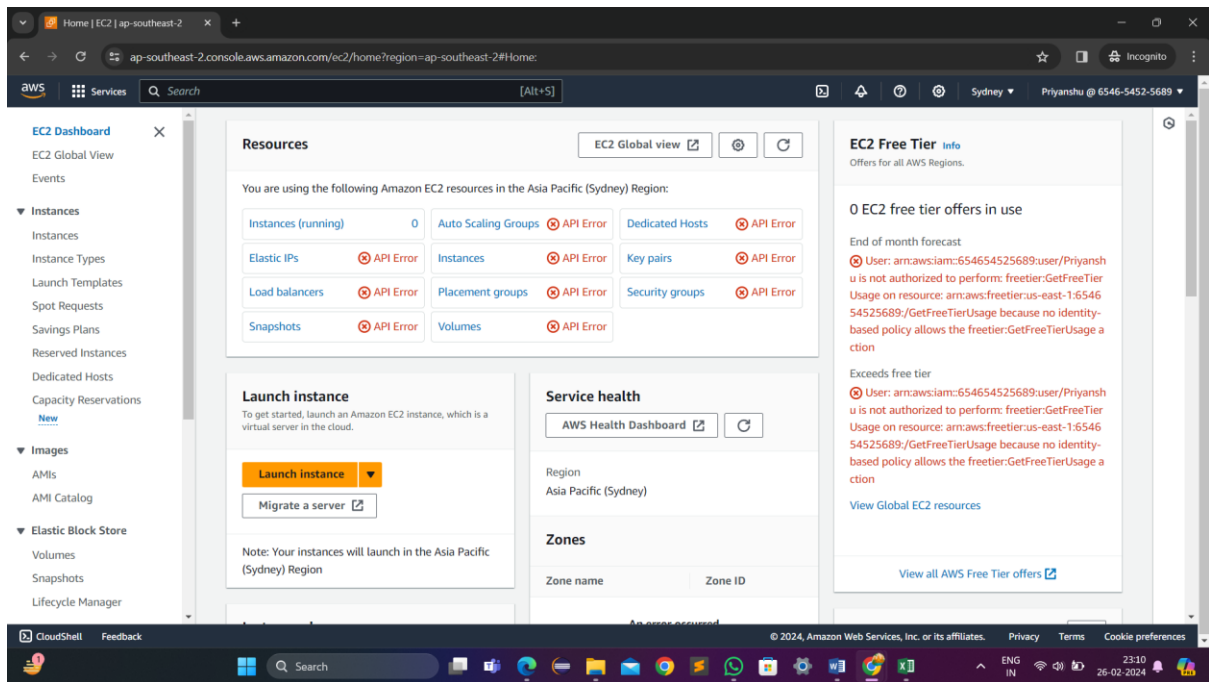
- Now search S3 in aws console and click in S3.



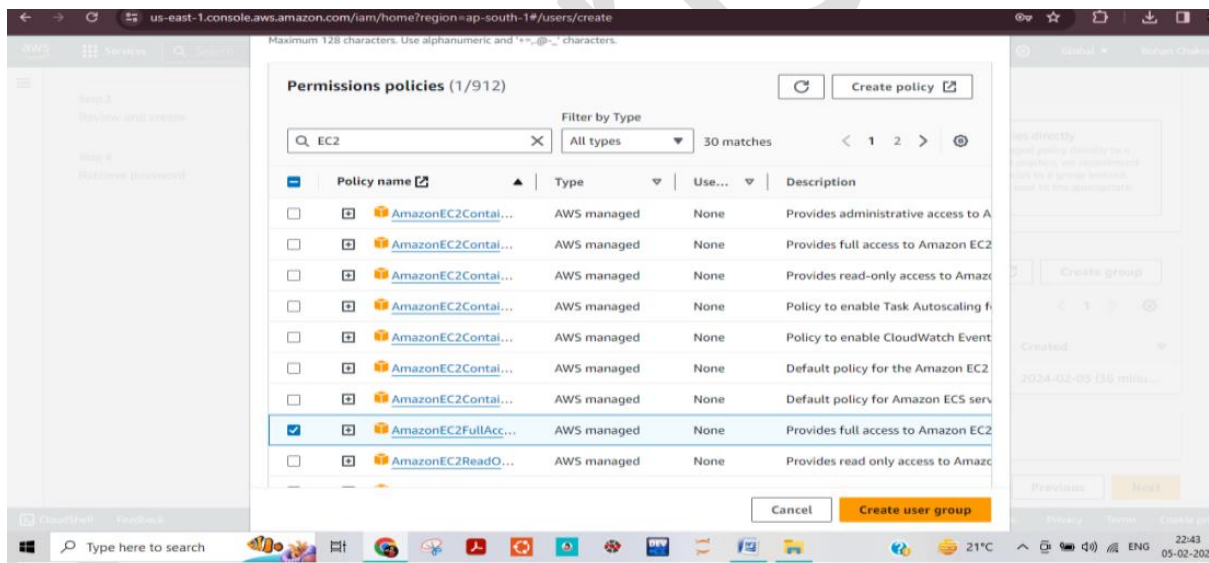
- S3 window will be opened and there is a option of Create bucket. In this bucket we can apply static website, file, folder.



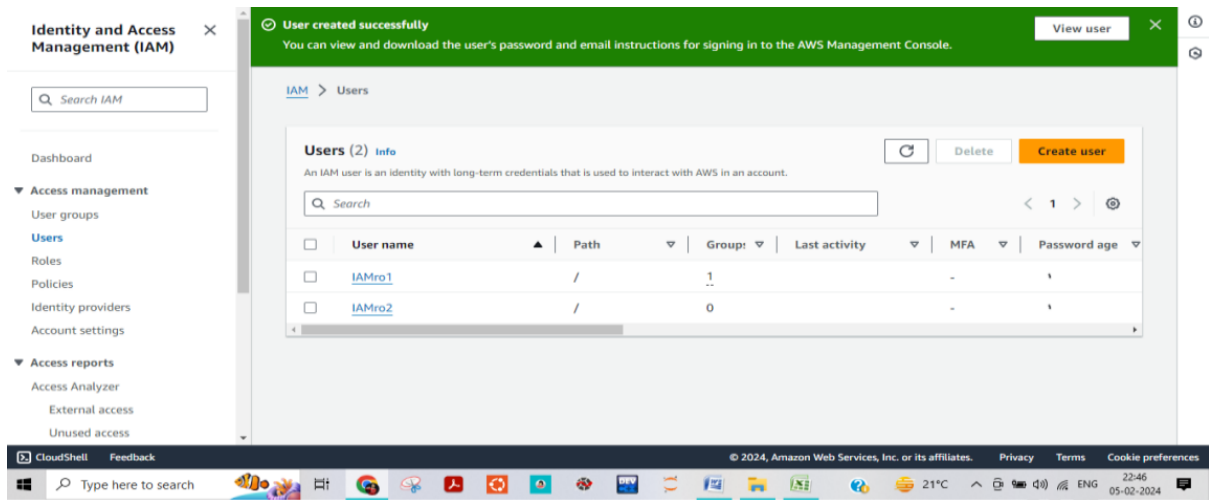
- Now back to console and search EC2 like S3 and press on EC2. You can see API errors are occurring as only s3 access was given to this user not EC2.



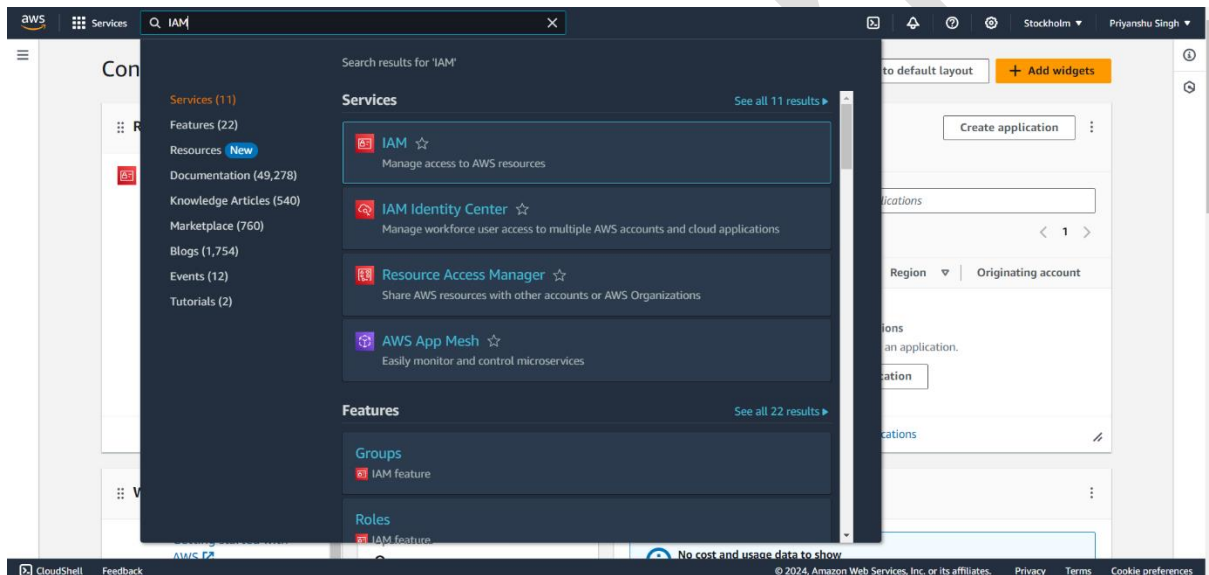
- Now do sign out and come out from incognito mode. Now make another user. Follow same steps and also make a new user group. And now in Permission policies search EC2 in search bar and click on AmazonEC2FullAccess and press on Create user group.



- In same way download .csv file and return to userslist. Now two separate IAM users will be created and both assigned with different access one is for s3 and another is for EC2.



- Now in same way return back to incognito mode and sign in to aws console and select IAM root and give 12 digit id ,username and password by copying those from .csv file like previous. Now search ec2 and click on EC2.



- Now when we go to EC2 then we can see no API Error is occurring like previous as this user has given access of EC2.

