**Create a New IAM User:**

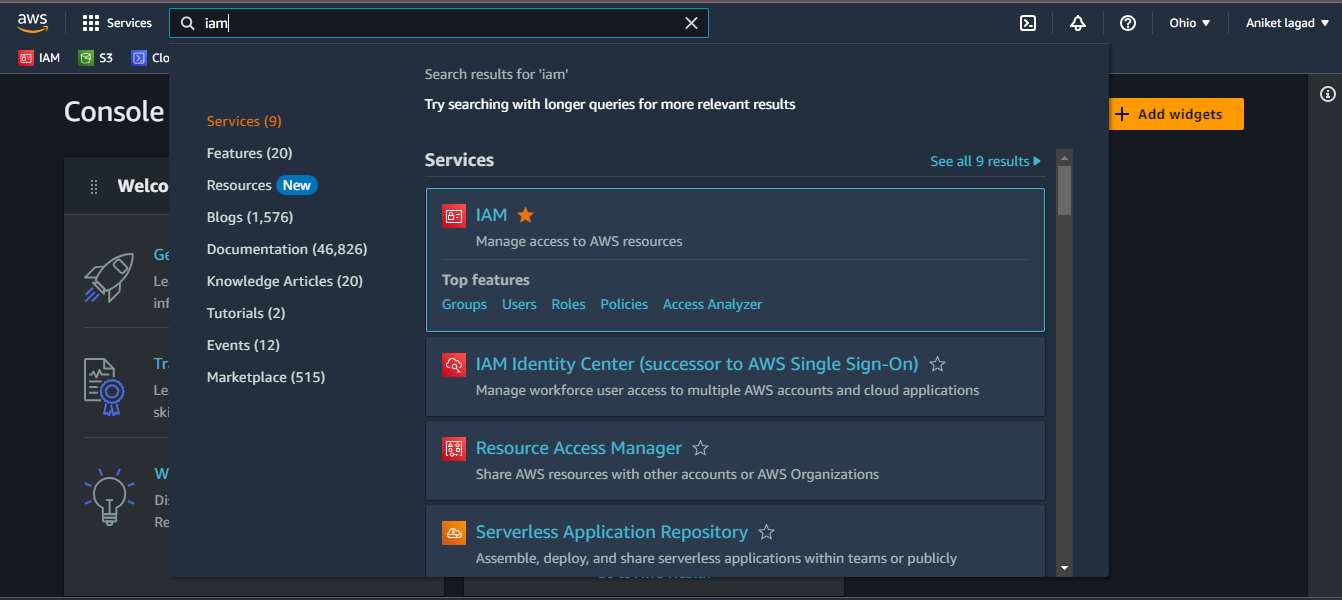
**Create a new IAM user with programmatic access.**

**Assign appropriate permissions to the user based on their role or responsibilities.**

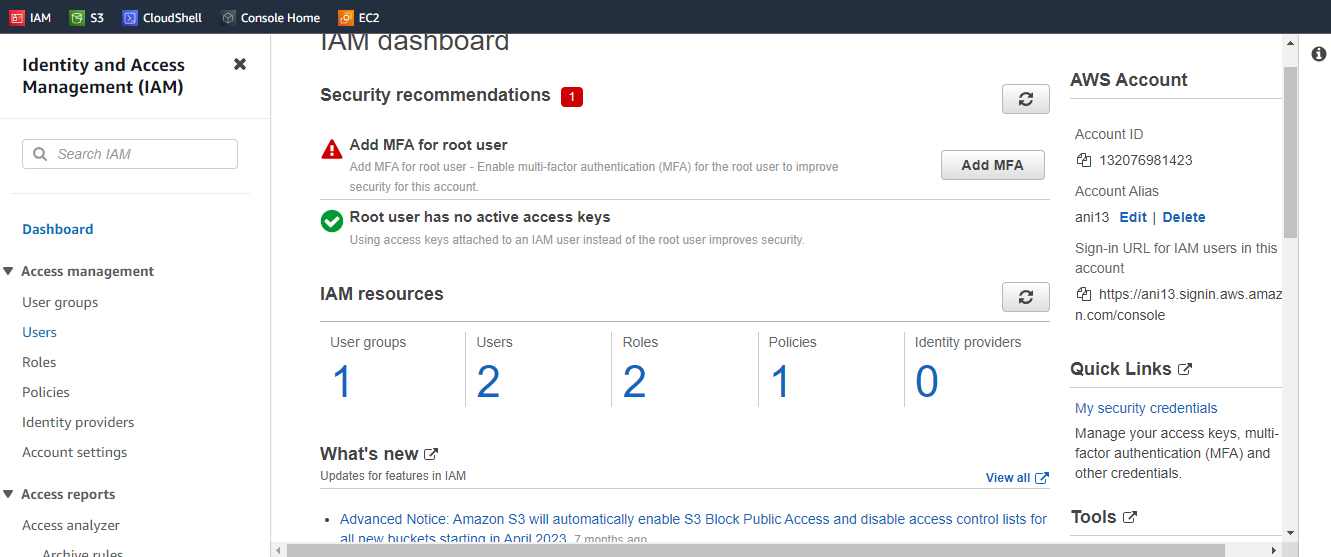
**Generate and securely provide the user's access key and secret access key.**

**Configure IAM Roles:**

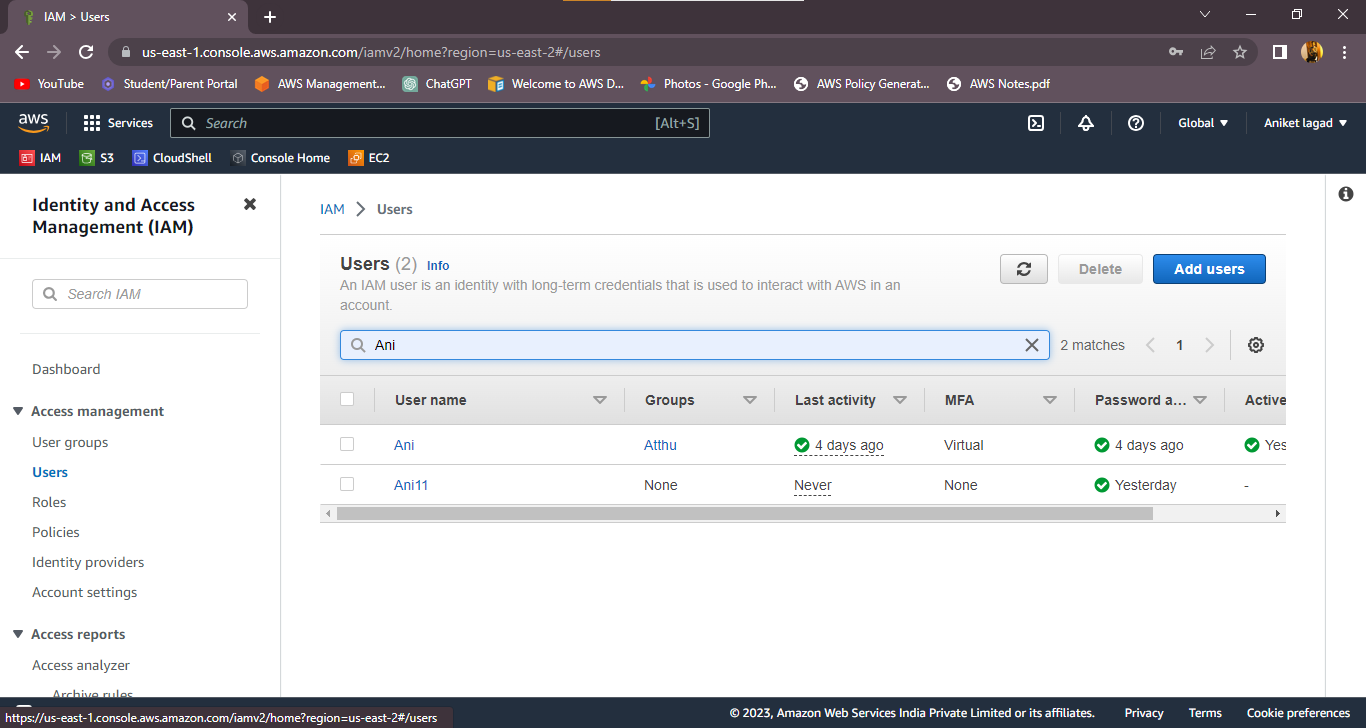
**🡪 Step 1:- First of all open aws and then open on that iam service**



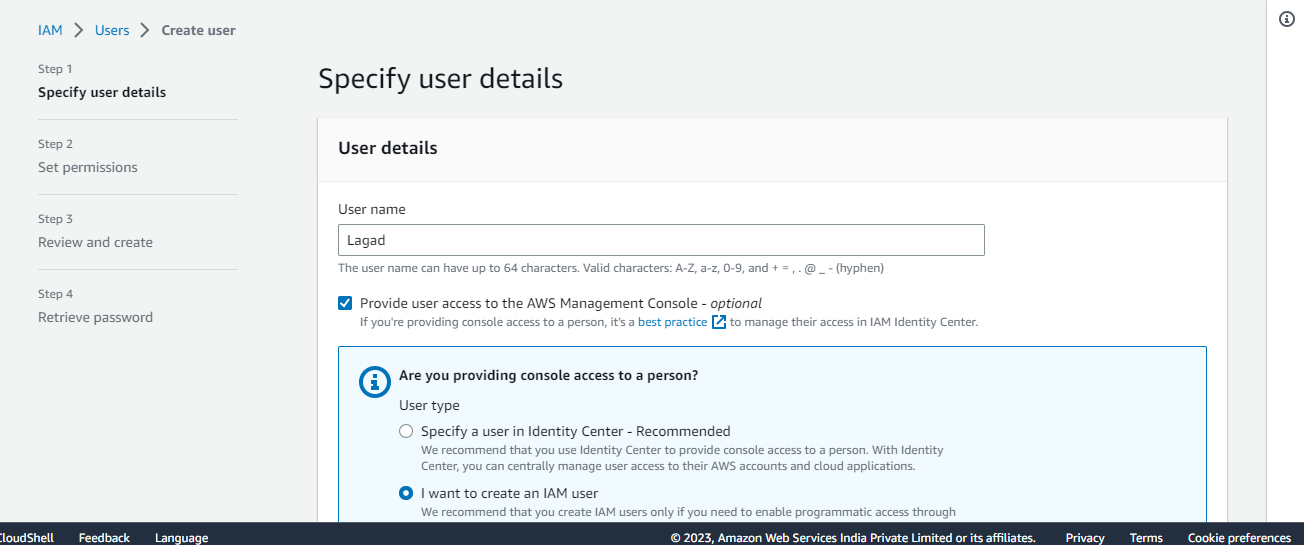
**Step 2 :- Then u will see dashboard of users then click on users**

****

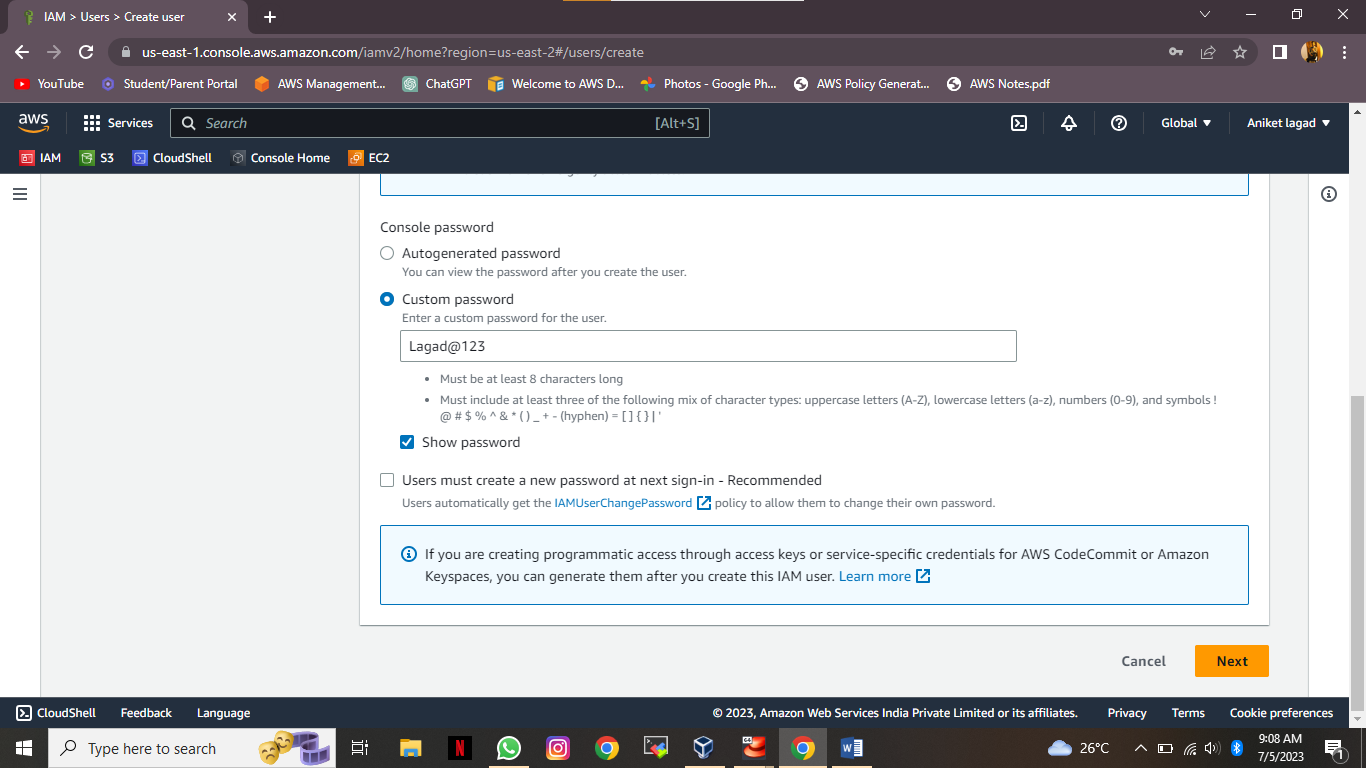
**Step 3 :- Now u wil add user by click on add users options**

****

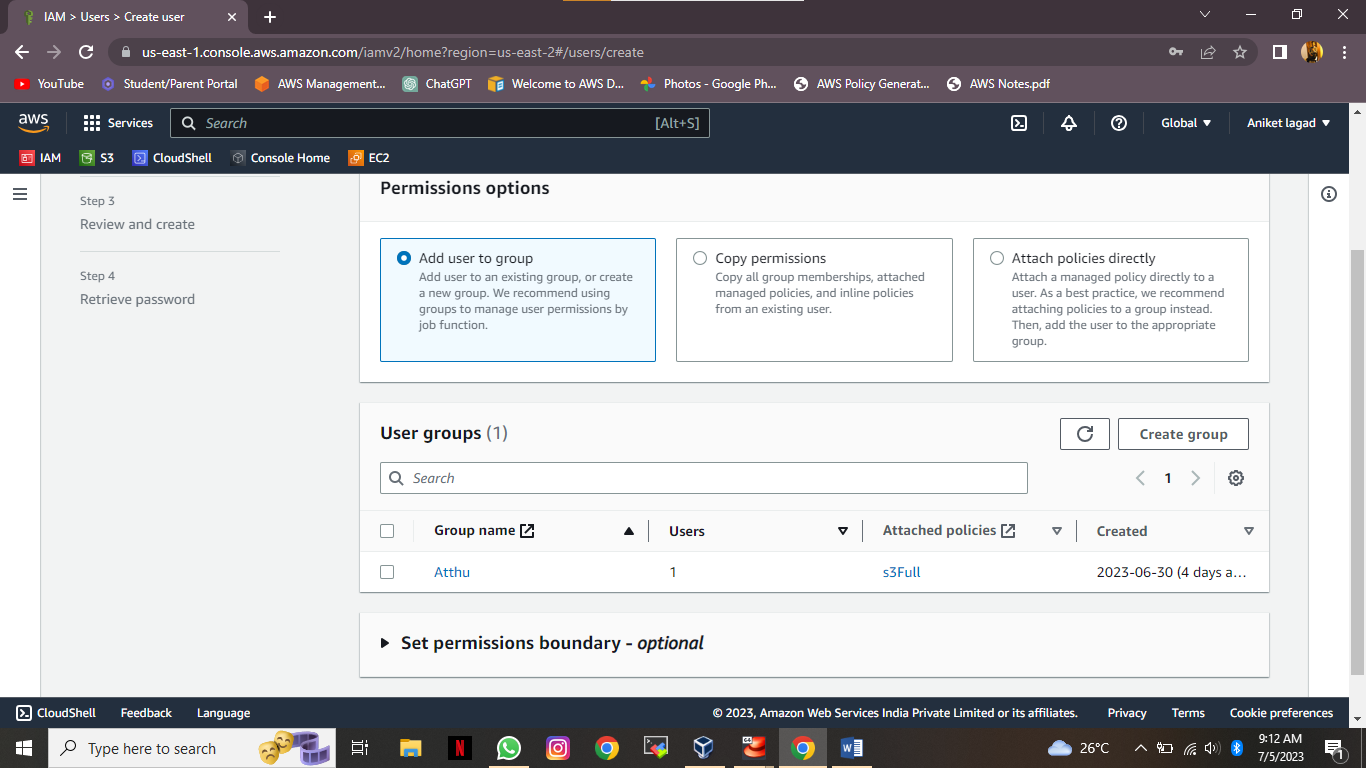
**Step 4:- Write a name which not used before and then click on provide user access of concle and then click on I want to create an I am user**

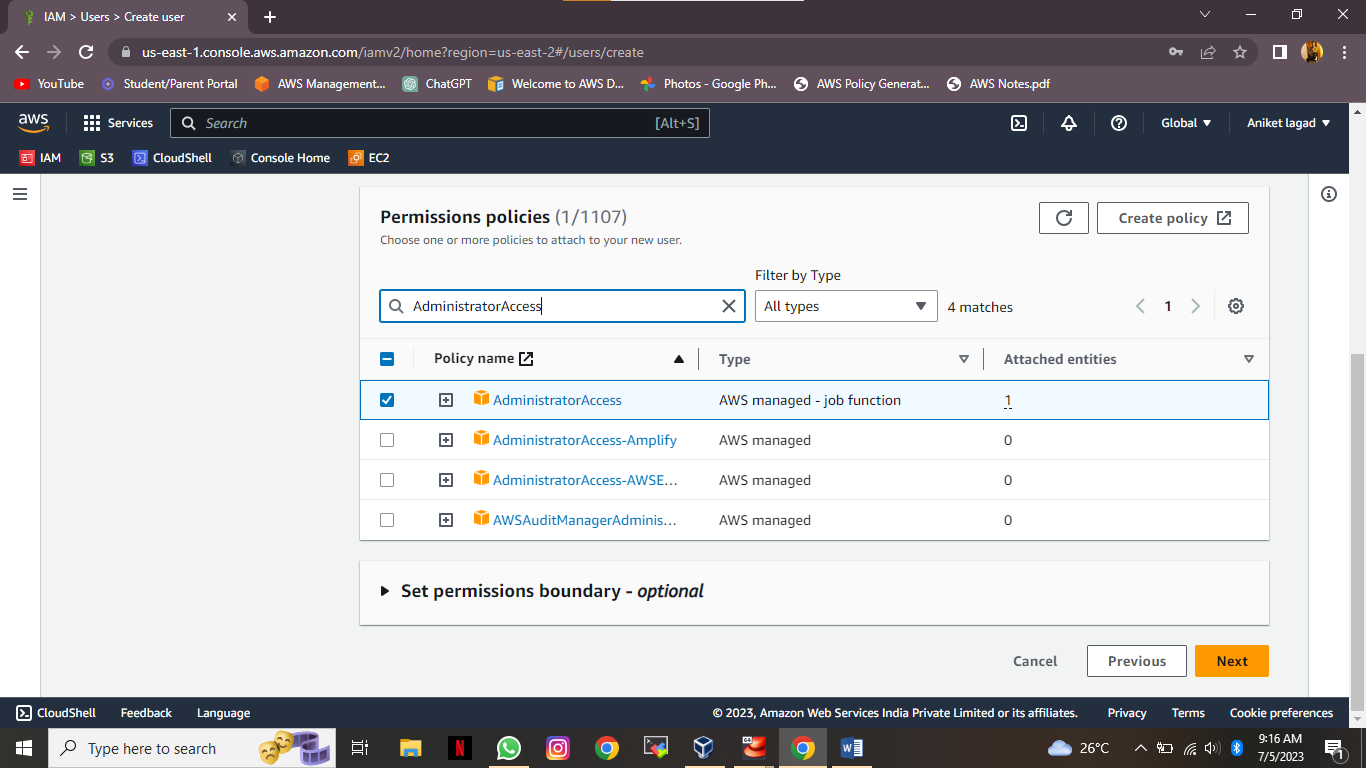
****

**Step 5:- And choose u want create password custom or autogenreated and then click if u don’t want user change password when they loggin**

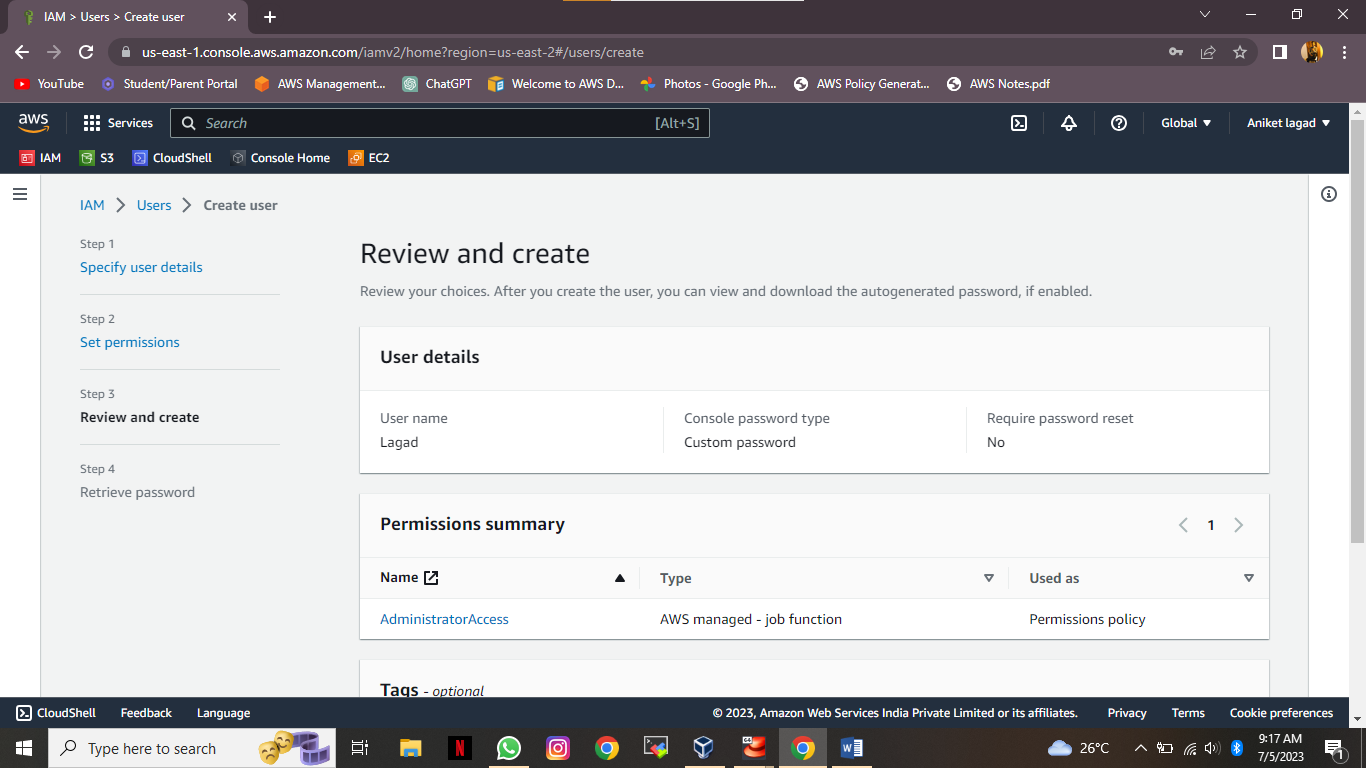
****

**Step 6:-Oky, Then u will see various options ther add group ,copy perrmissions and attach policy choose a options to attach a policy and click on next.**

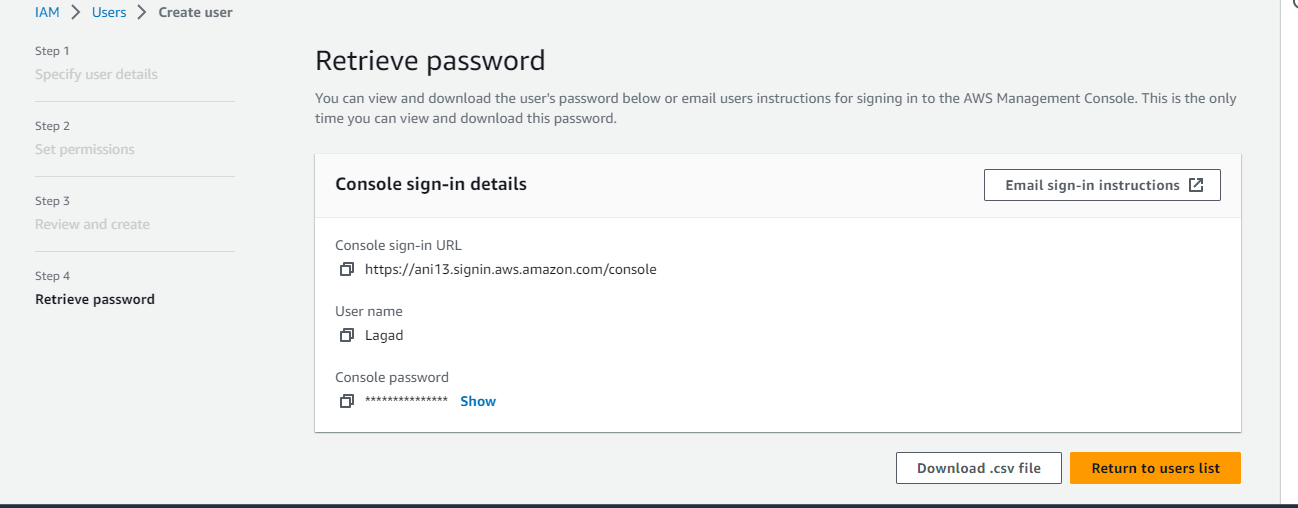
****

****

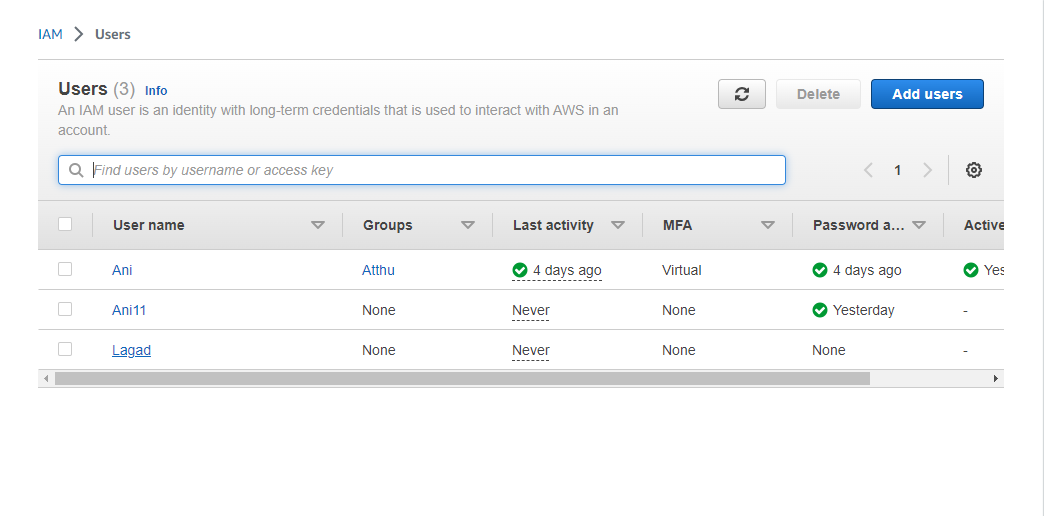
**Step 7:- Next u will see all information about user what u choose or not and then u will click on the end option create user.**

****

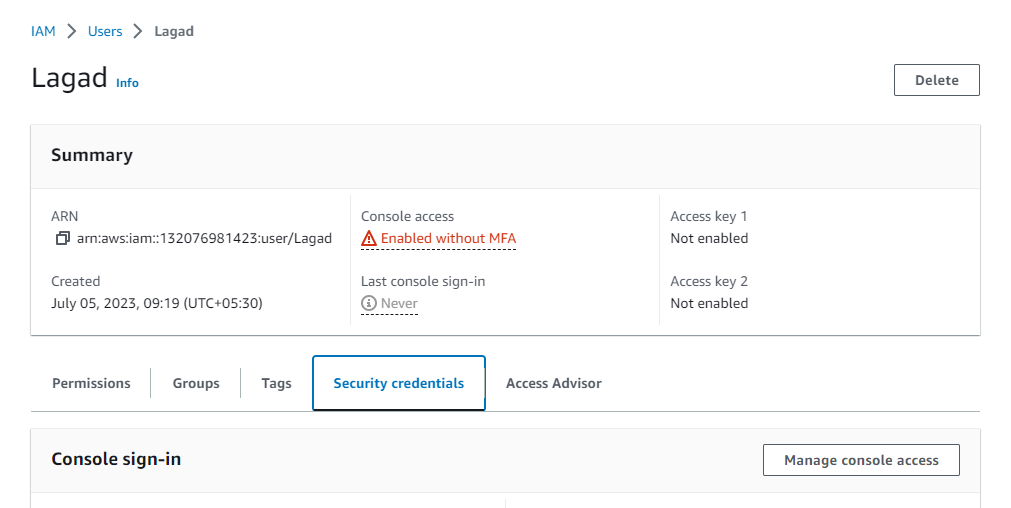
**Step 8:- Then download your users information like conolse url and password and username or stay remember of all information.**

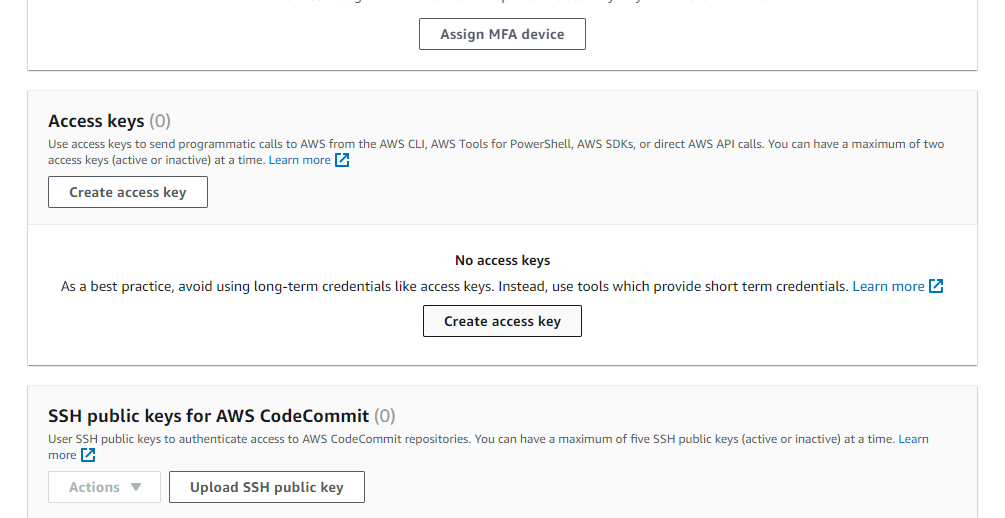
****

**Step 9:- Now user was create click on go to all user and see user was create or not and then click on user to set user key access**

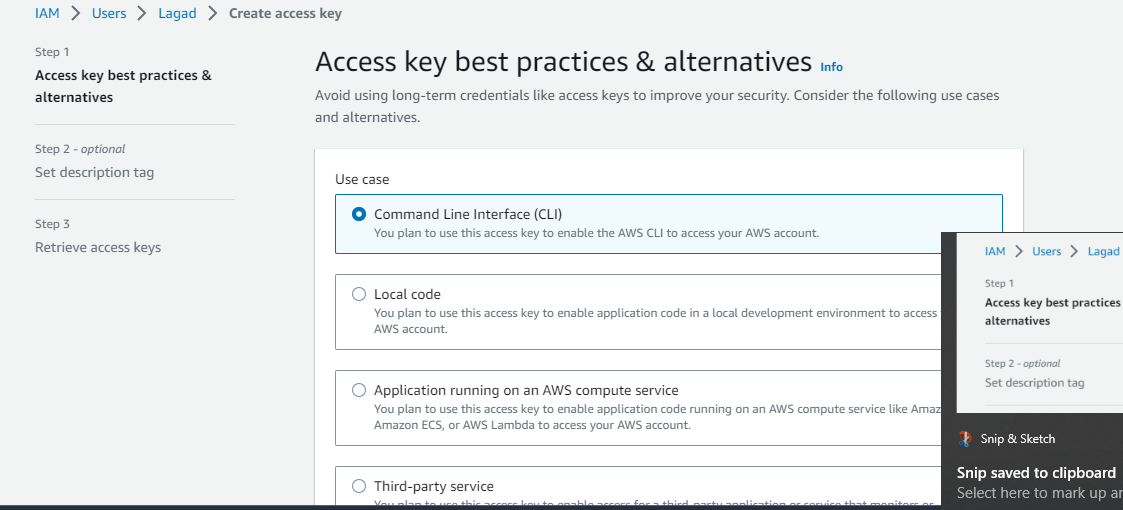
****

**Step 10:- noe click on security credentials and go down side and click on create access key**

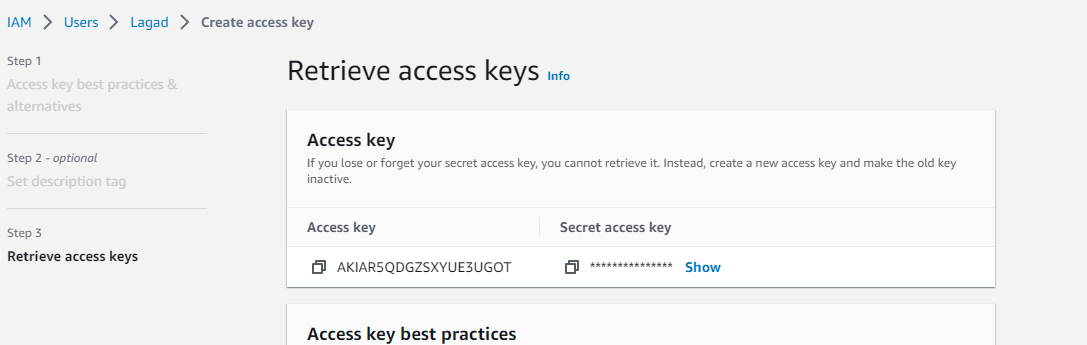
****

****

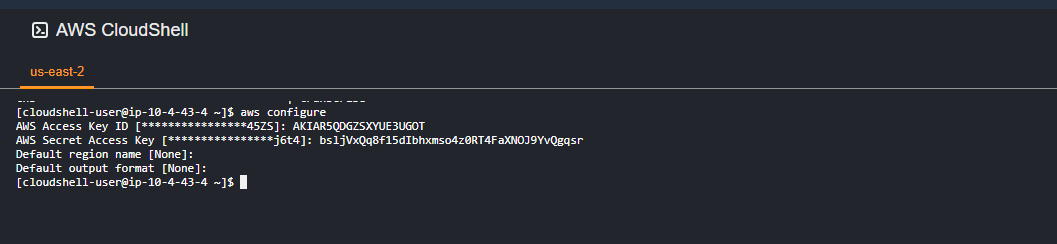
**Step 11:- next click on option command line interface and then down side click on confirmation and next.**

****

**Step 12:- Next gave a key name and then click on create and next u will see key information and download its credational.**

****

**Step 13:- Now go to cloudshell and type there a aws configure command and then paste key there and hit enter then paste the access key and hit enter and then hit enter diret 2 time and now you access has**

****

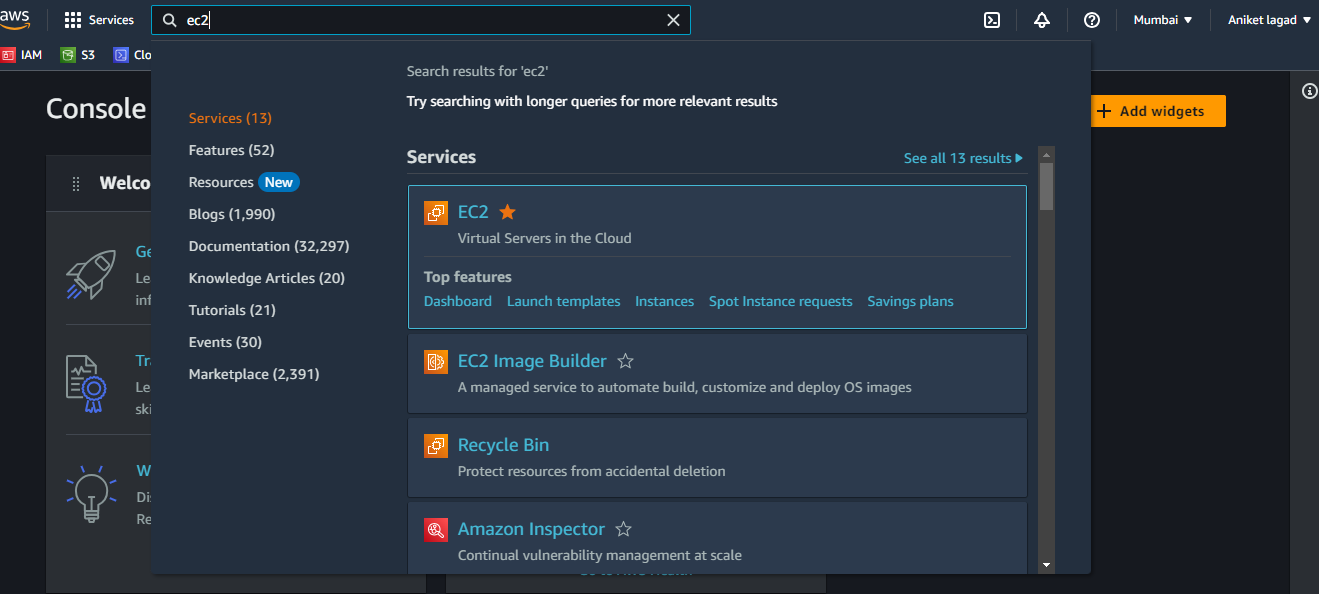
**Create an IAM role for EC2 instances or Lambda functions with specific permissions.**

**Attach policies to the role that grant necessary permissions to access AWS resources.**

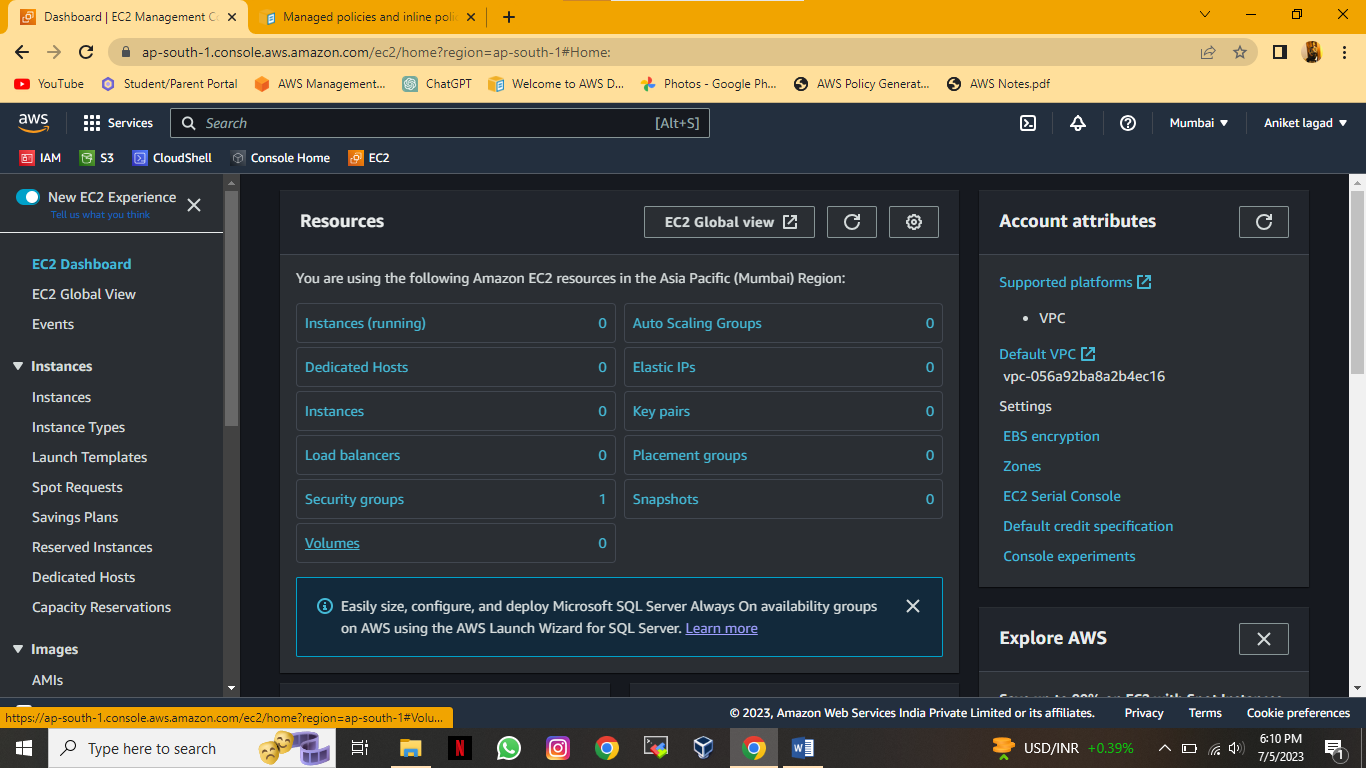
**Assign the role to EC2 instances or Lambda functions.**

**Implement Multi-Factor Authentication (MFA):**

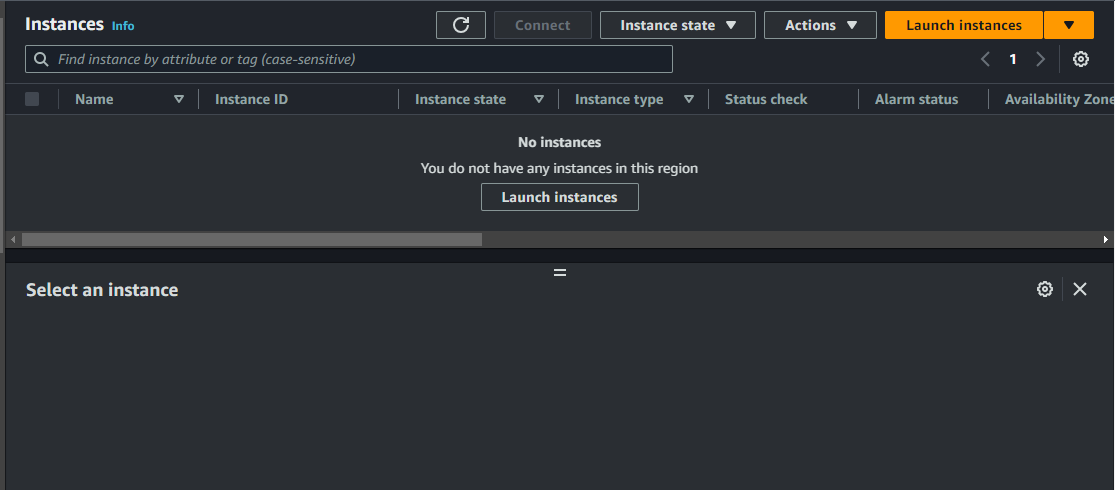
* **Step 1:-Firstly open aws and go to ec2 service**

****

* **Step 2:-then u will see all instance realated information ther is on optin instance click on that option to create instance**

****

**Step 3:- Then u will see the launch instance optin click on that option to lauch instance**

****

**Step 4:-**

**Enable MFA for IAM users to provide an additional layer of security.**

**Guide users on how to set up MFA devices (such as virtual MFA apps or hardware tokens).**

**Test the MFA configuration to ensure it functions correctly.**

**Create IAM Policies:**

**Write a custom IAM policy that allows or denies specific actions on AWS resources.**

**Associate the policy with the appropriate IAM users, groups, or roles.**

**Test the policy to verify that the desired access control is enforced.**

**Use IAM Groups:**

**Create an IAM group and assign permissions to it.**

**Add IAM users to the group to manage their access collectively.**

**Remove users from the group when their access requirements change.**

**Implement IAM Access Analyzer:**

**Enable IAM Access Analyzer to identify unintended access to your AWS resources.**

**Review and resolve findings generated by IAM Access Analyzer.**

**Continuously monitor and remediate any potential security risks.**

**Enable AWS CloudTrail for IAM:**

**Enable CloudTrail to capture API activity related to IAM.**

**Configure CloudTrail to store logs in an S3 bucket.**

**Review and analyze CloudTrail logs for any suspicious or unauthorized activities.**

**Implement IAM Password Policies:**

**Define and enforce password policies for IAM users.**

**Set requirements such as minimum password length, complexity, and expiration.**

**Regularly remind users to update their passwords according to the policy.**