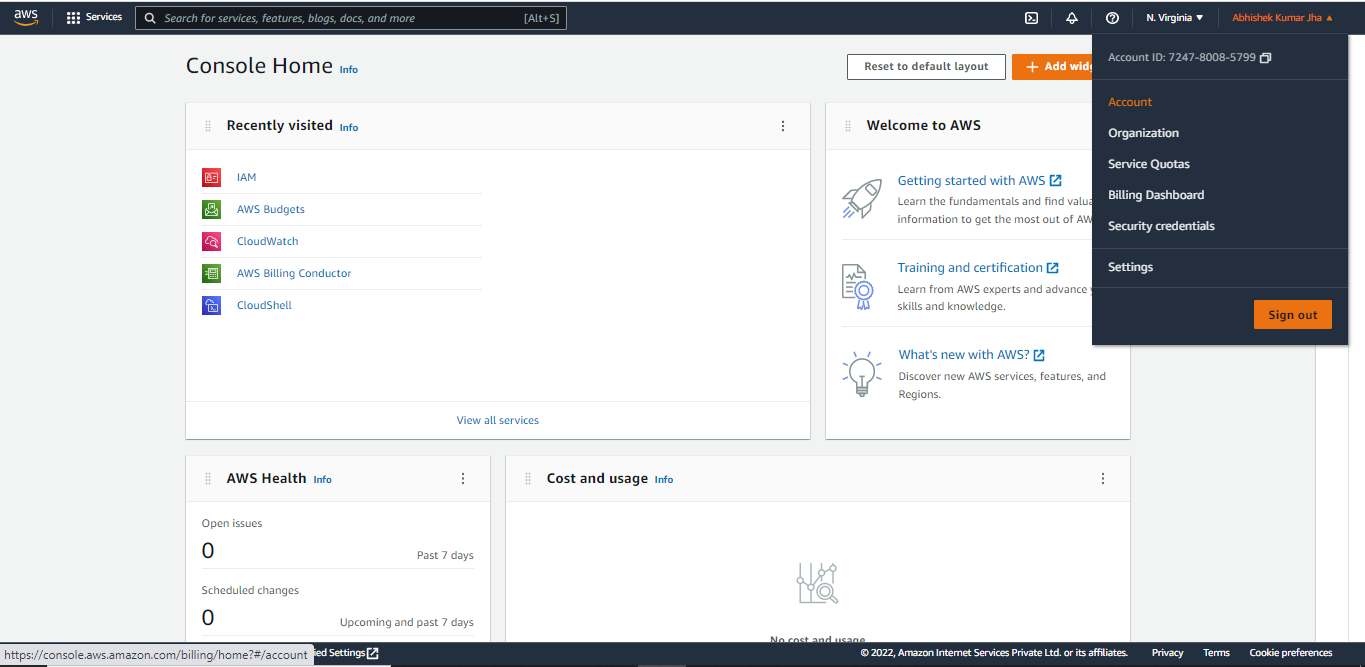
Day5-Assignment-13-July-2022

1. How to get emails on account billing invoice, free tier alerts? Hands –On

Step1 – Go to Account under Management Console by clicking on the dropdown menu under username.



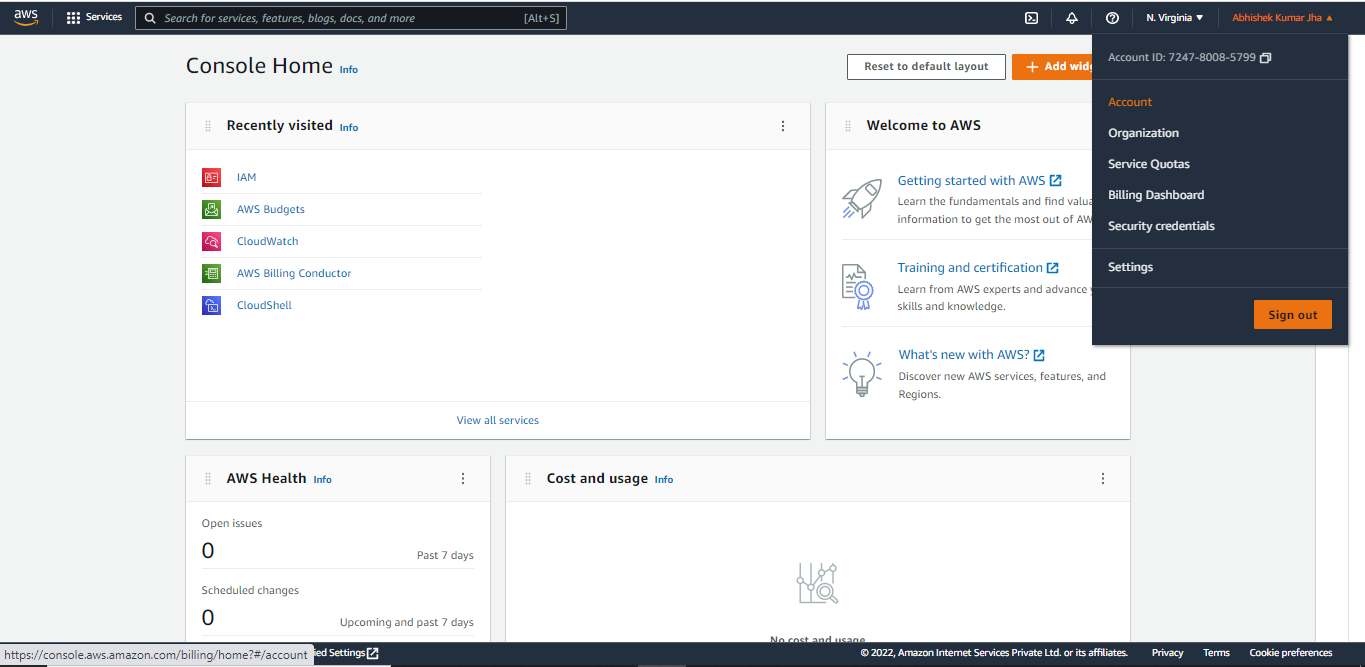
Step2 – Click on ‘Billing Preferences’ on left menu.



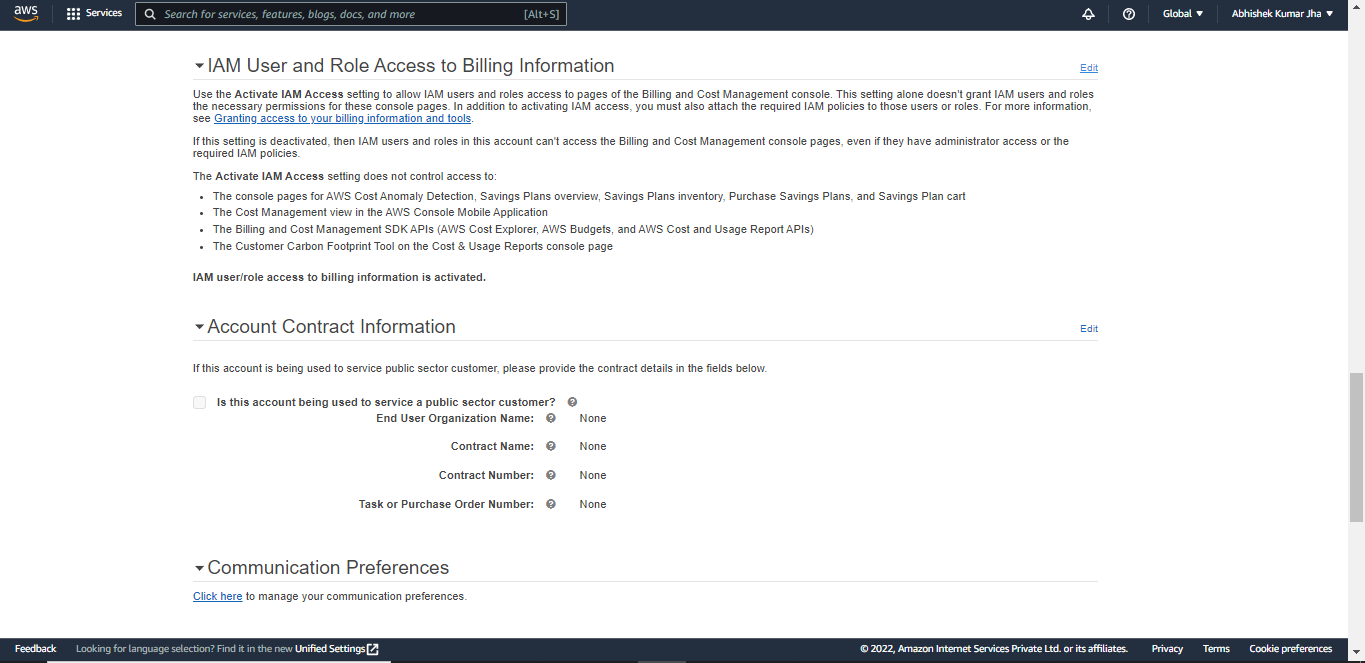
Step3 – Select ‘Receive PDF invoice by Email’ and also select ‘Receive Free Tier usage alerts and click on ‘Save Preferences’

2. How to configure the account to provide IAM user and Role Access to Billing Information? Hands-On

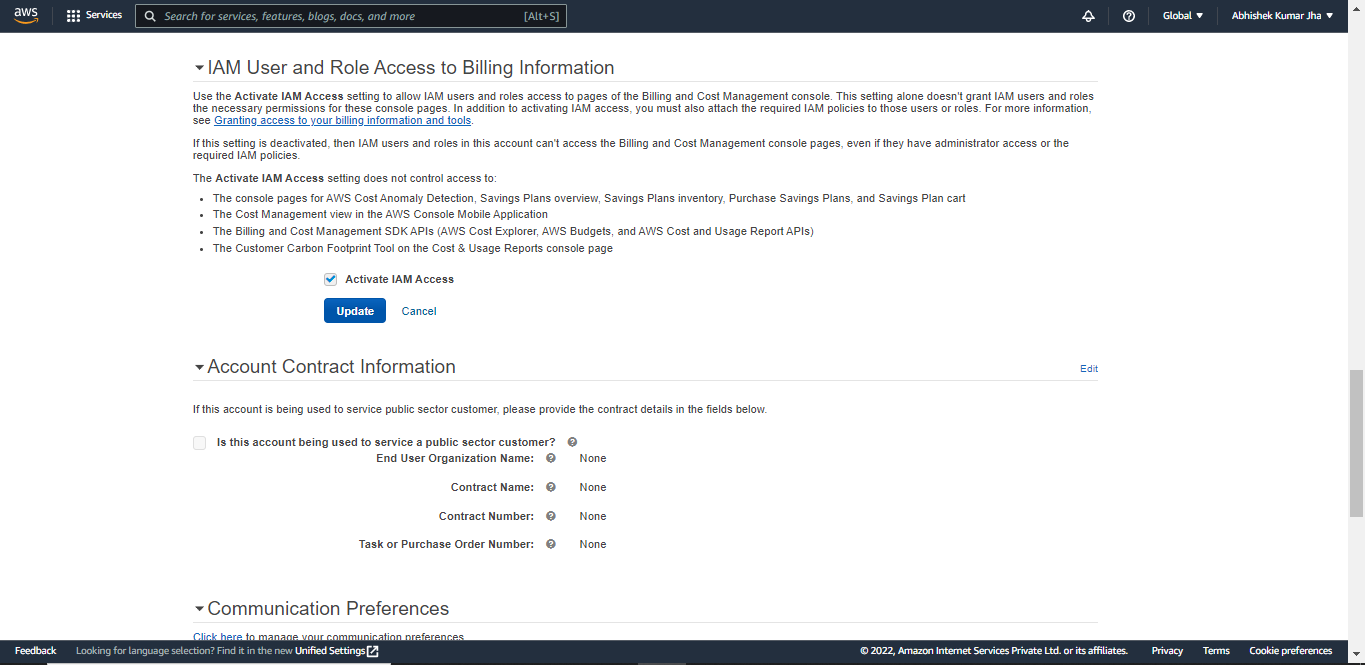
Step1 –Click on ‘Account’ under Username dropdown menu on console.



Step2 – Scroll down and click on IAM User and Role Access to Billing Information and click on ‘Edit’ on top right.

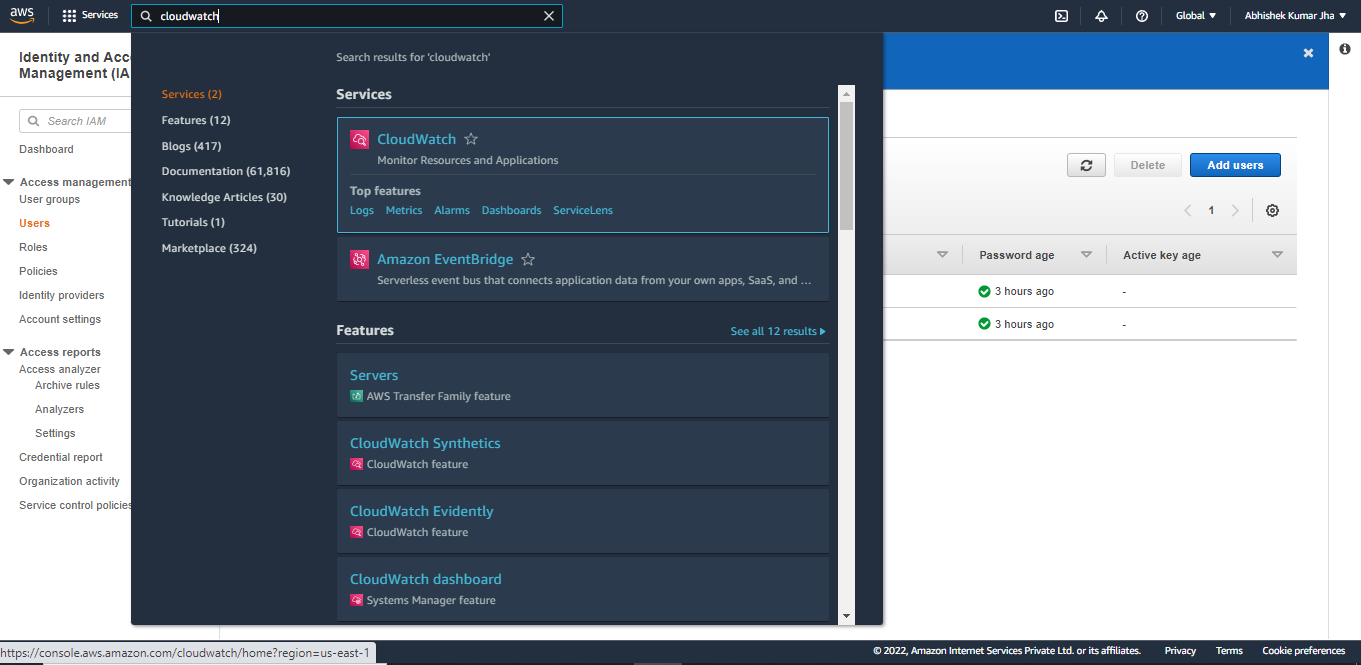


Step3 – Tick the checkbox for ‘Activate IAM Access’ and click ‘Update’.

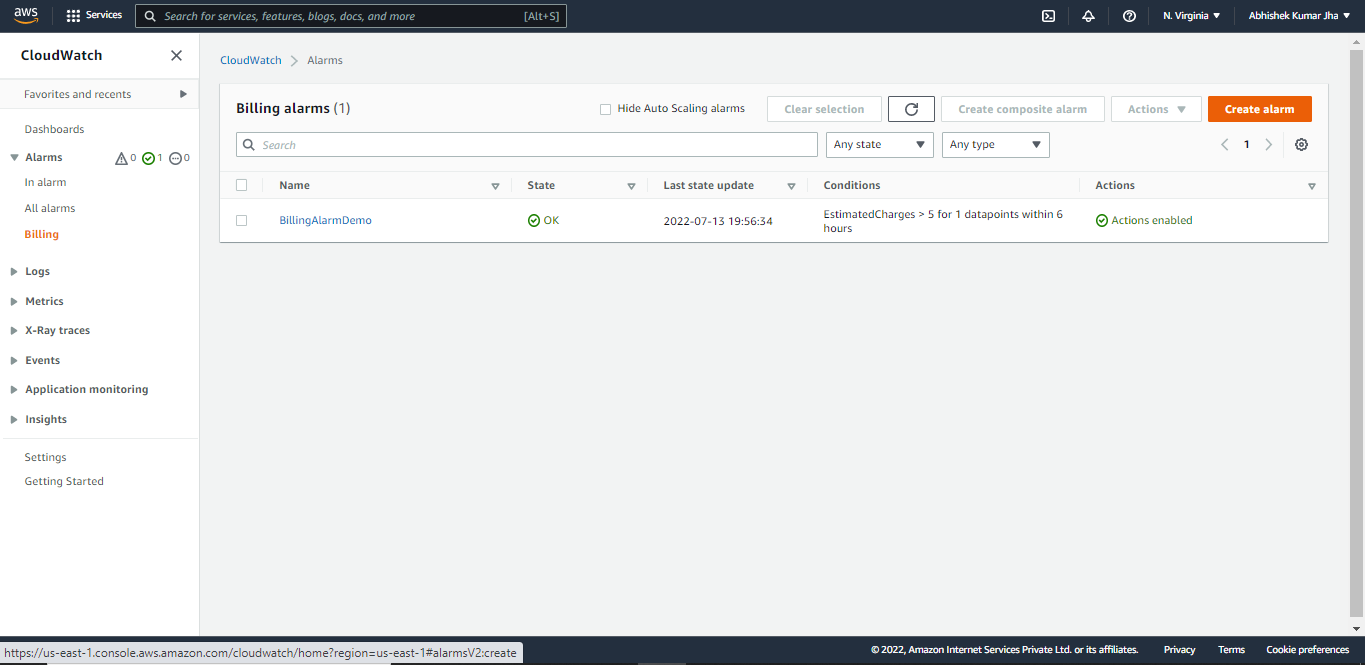


3. How to configure Billing Alarm? Hands-On

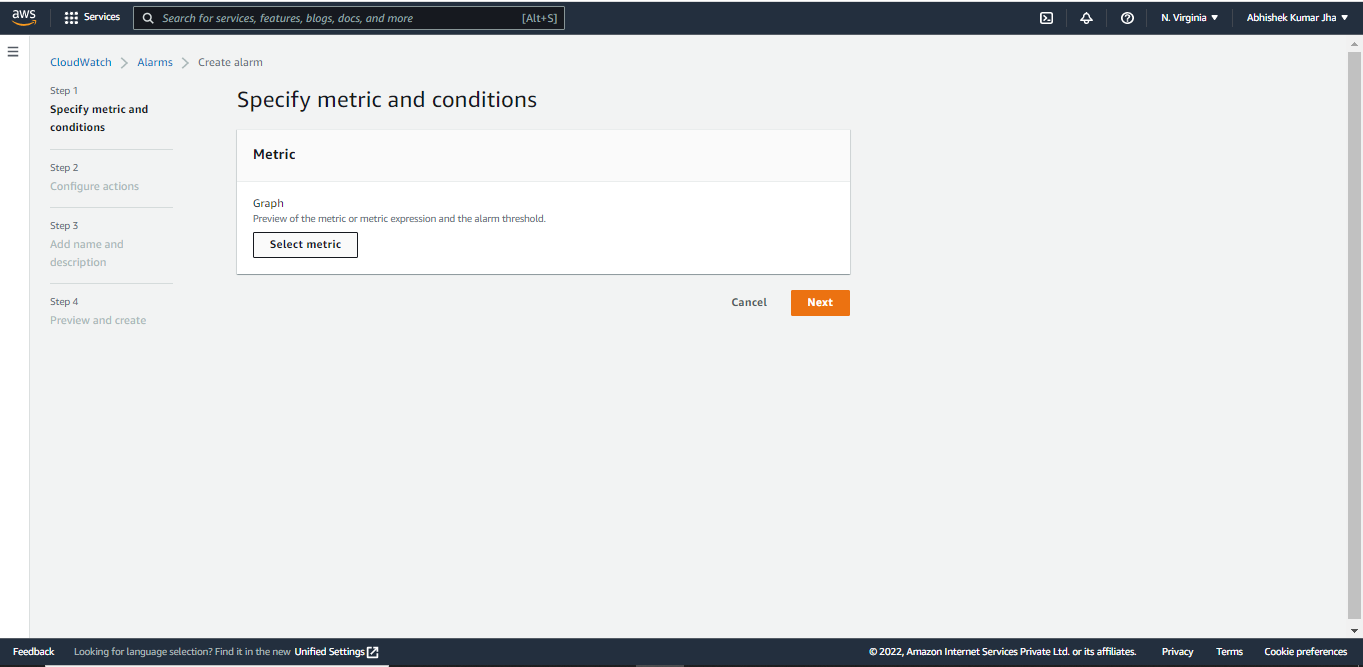
Step1 – Go to ‘CloudWatch’ by Searching on Console search Bar.



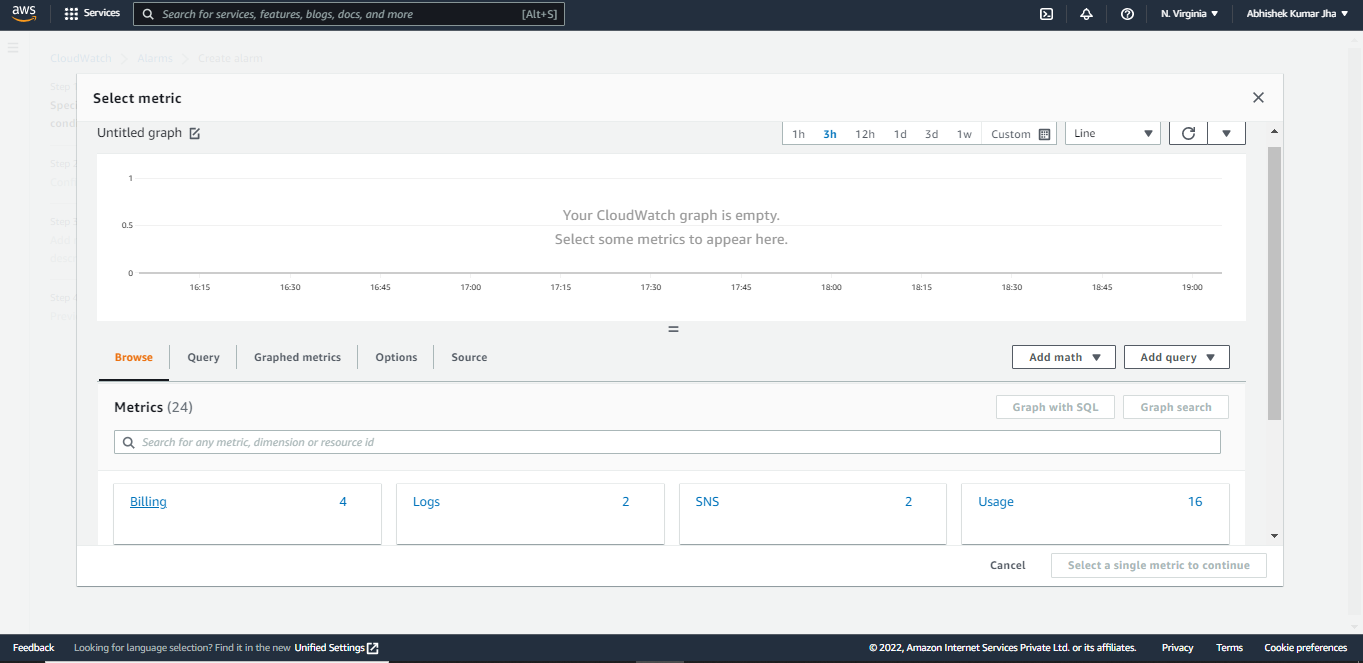
Step2 – Click on ‘Billing’ on left menu and click on ‘Create Alarm’.



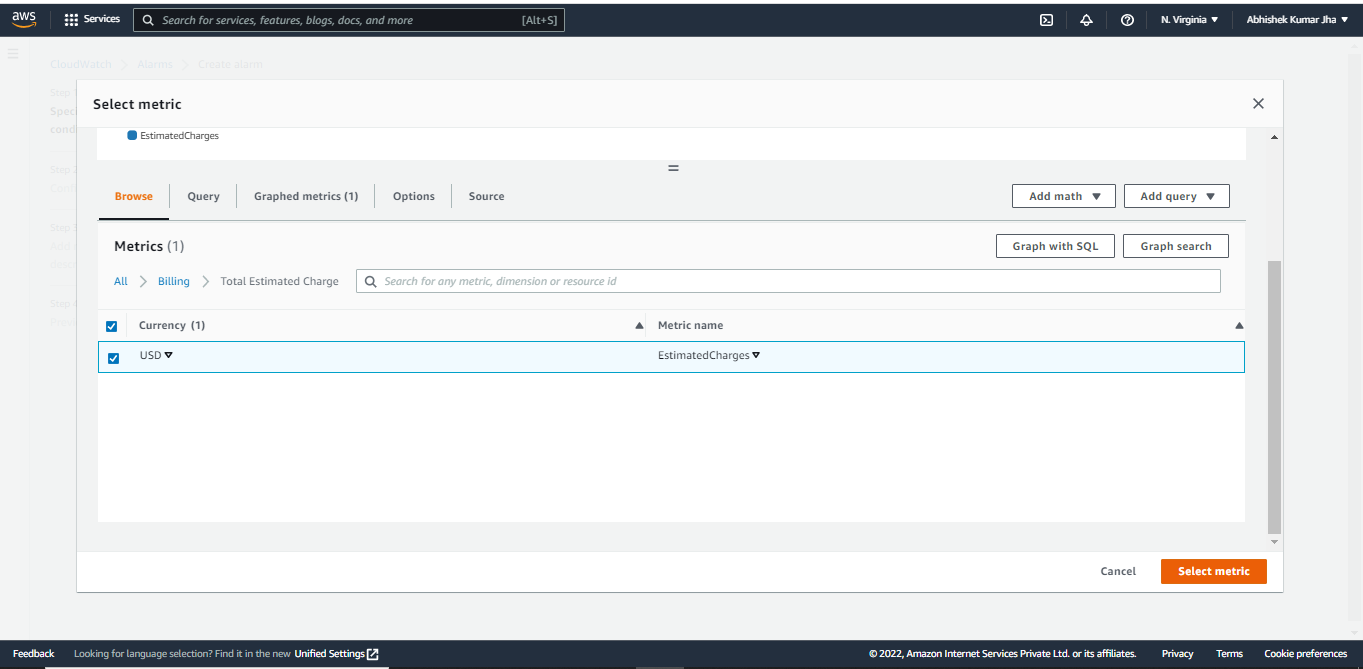
Step3 – Now under ‘Create Alarm’ specify ‘Metric and Conditions’.



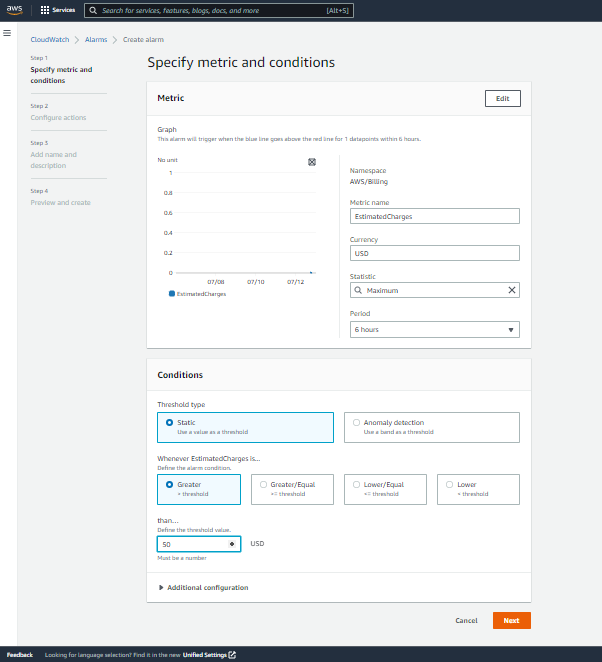
Step4- Click on ‘Billing’ under Metric.



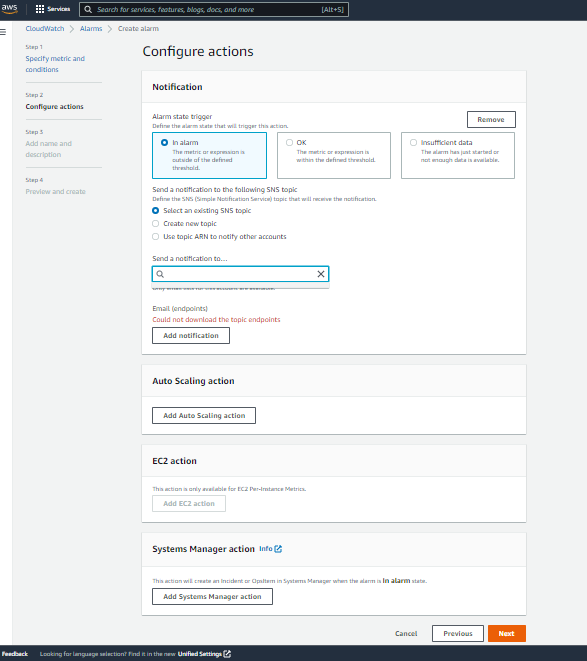
Step5 – Tick on Checkbox for USD and click on ‘Select Metric’.



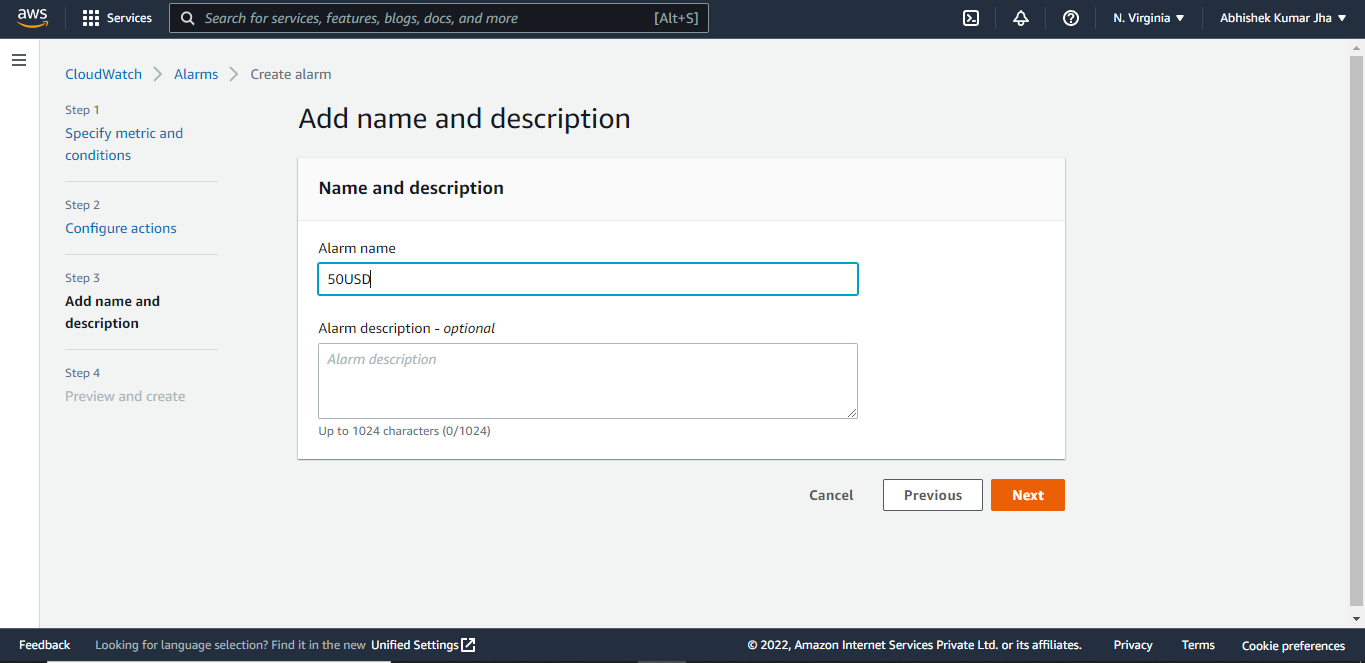
Step5 – Under ‘Metric’ Specify Threshold type and Value and click ‘Next’.



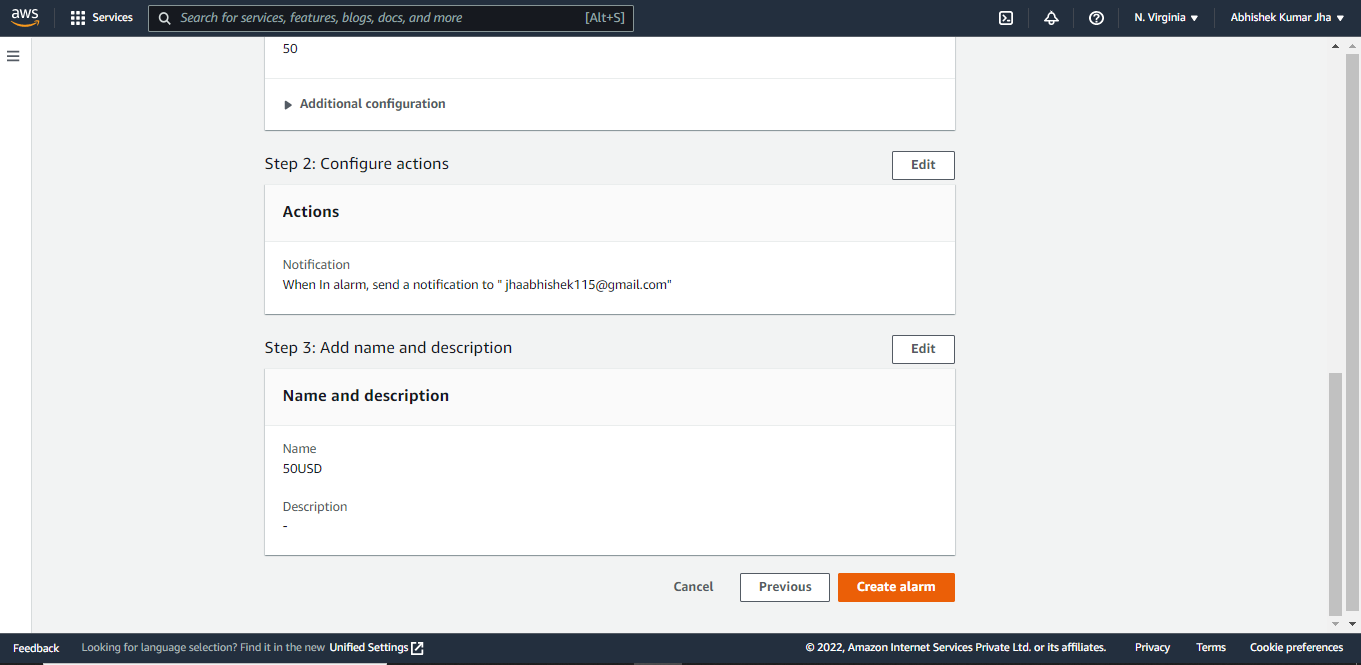
Step6 – Under ‘Configure Options’ you can add your email id to send a notification to and click ‘Next’.



Step7 – Add name and Description to Alarm and click ‘Next’.

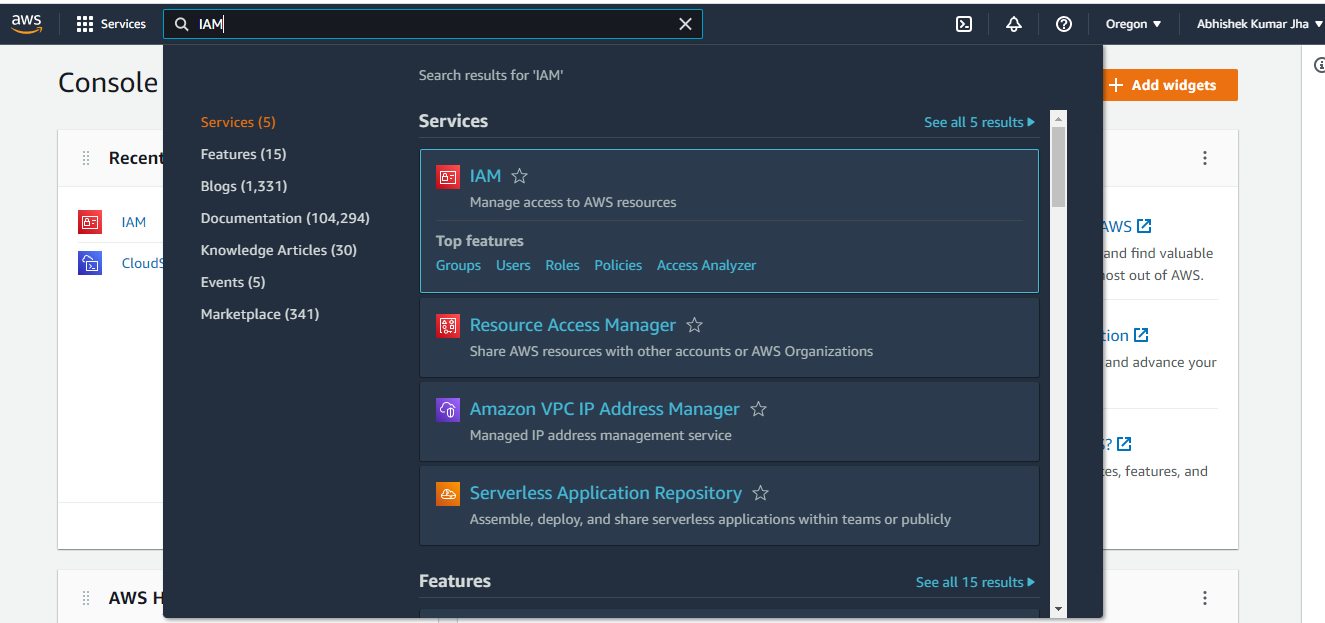


Step8 – In the next step under ‘Preview and Create’ check all options, scroll down and click ‘Create Alarm’.



4. How to attach a specific AWS managed policy to an IAM user? Hands On

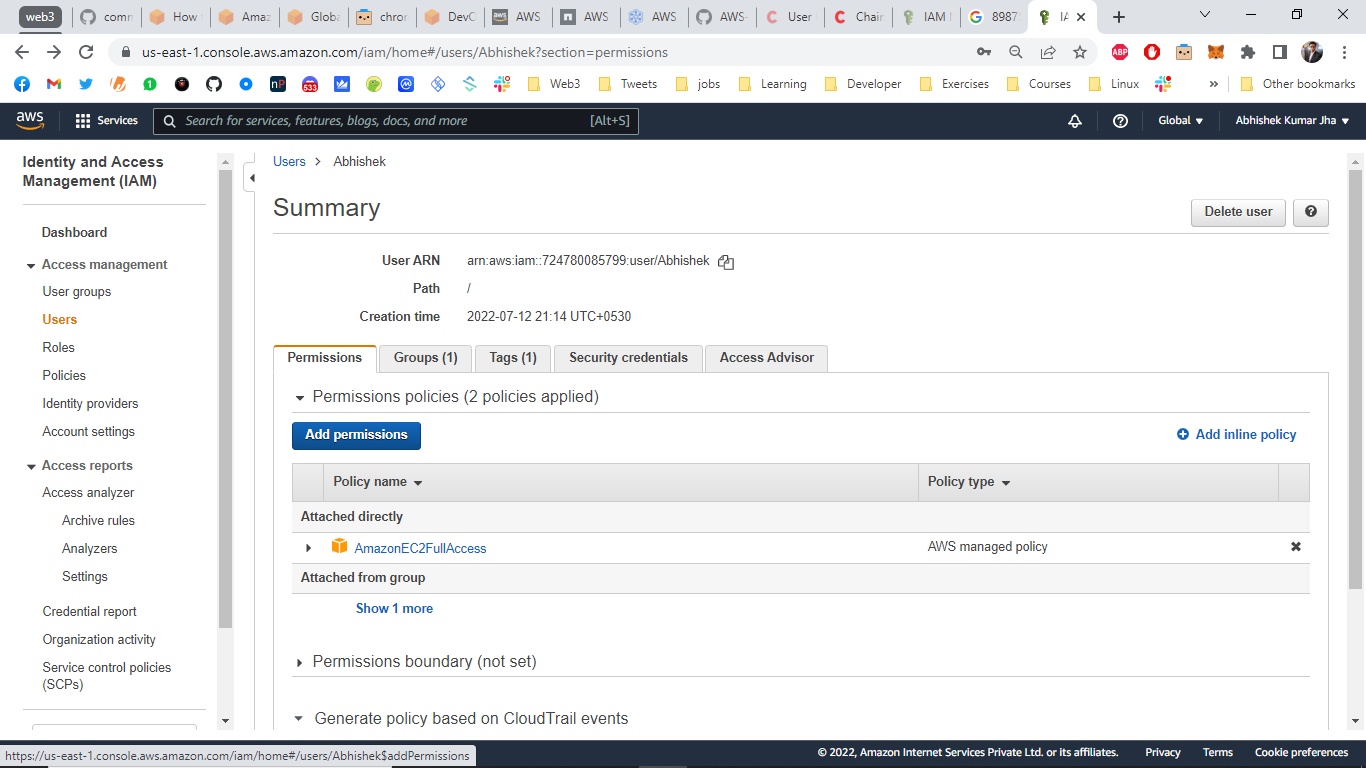
Step1 – Search for ‘IAM’ on Search bar on Management console and click on ‘Users’ .



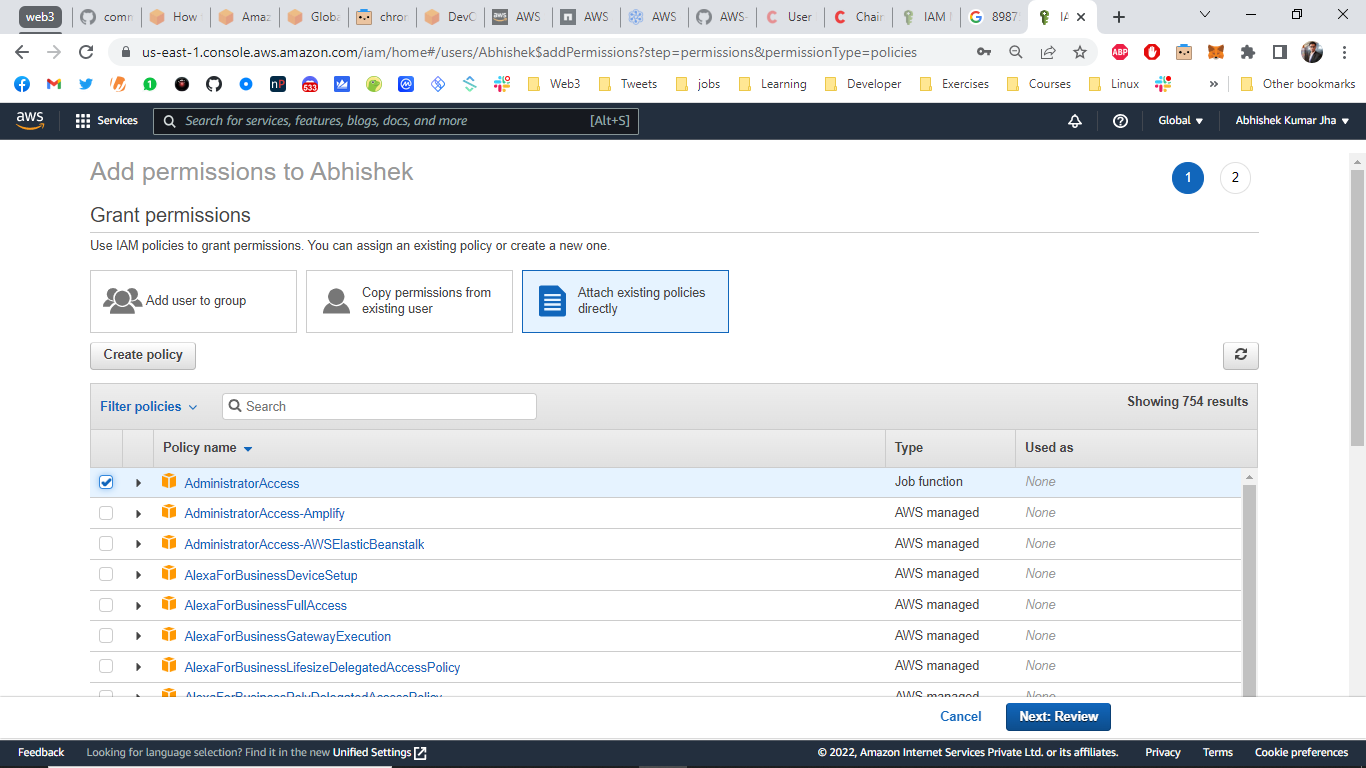
Step2 – Select the User you want to attach a policy to.



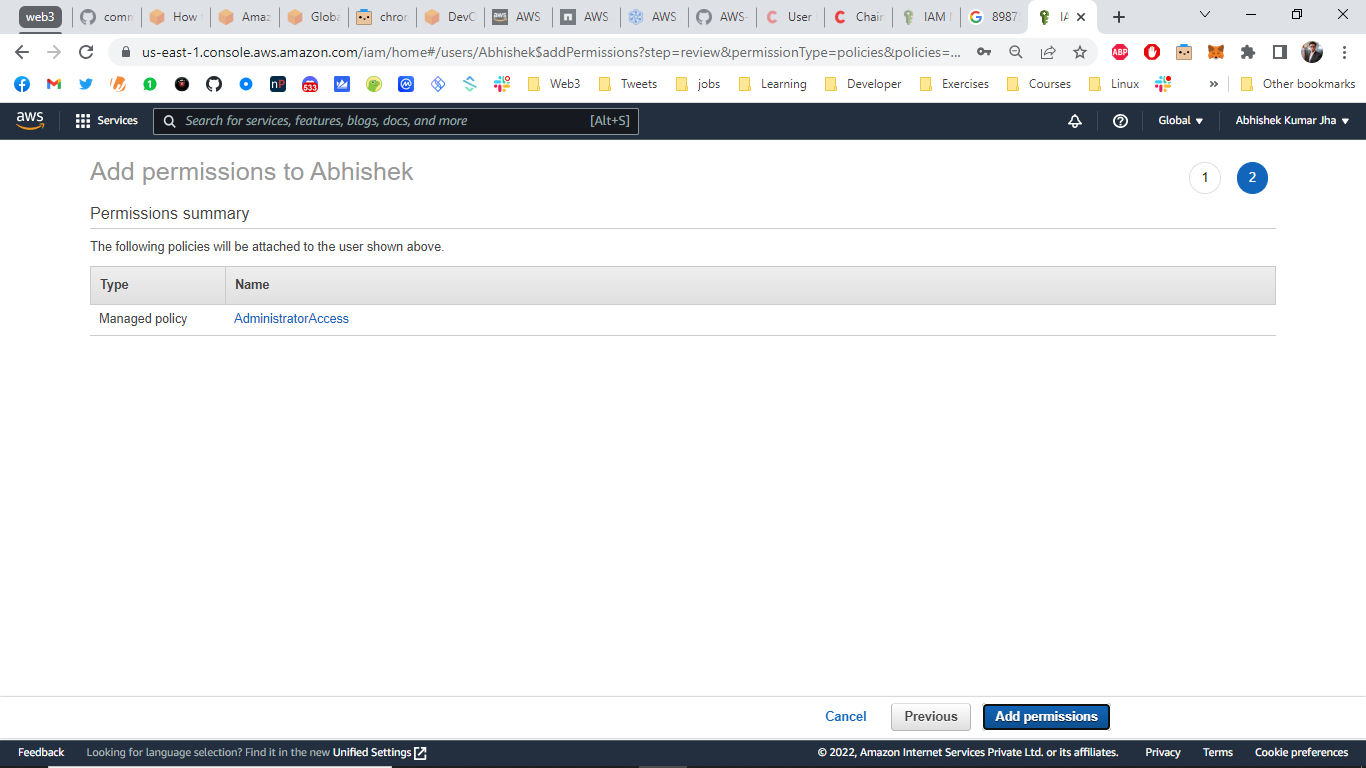
Step3 – Click on ‘Add Permissions’.



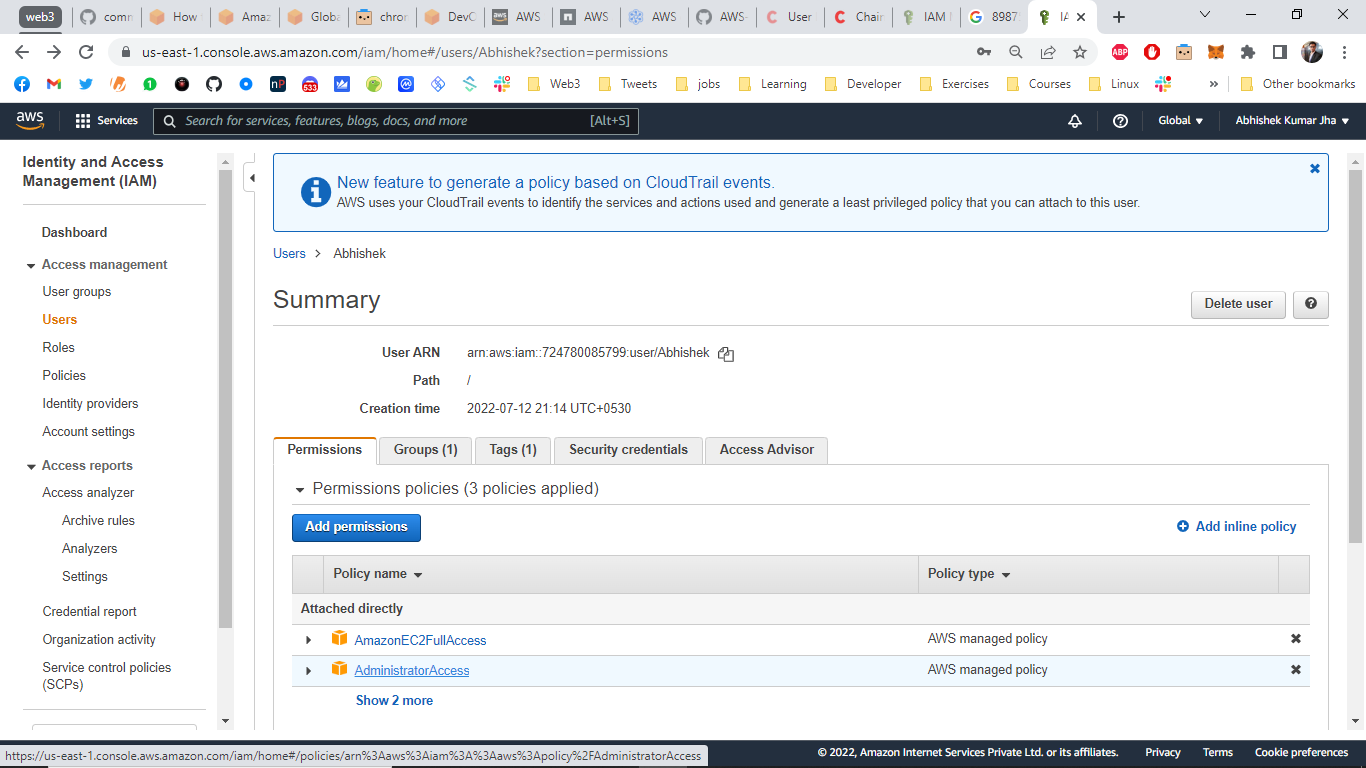
Step4 – Click on ‘Attach existing policies directly’ and search for policy. For example – I have selected ‘Administrator Access’.



Step5 - Click on ‘Add Permissions’.

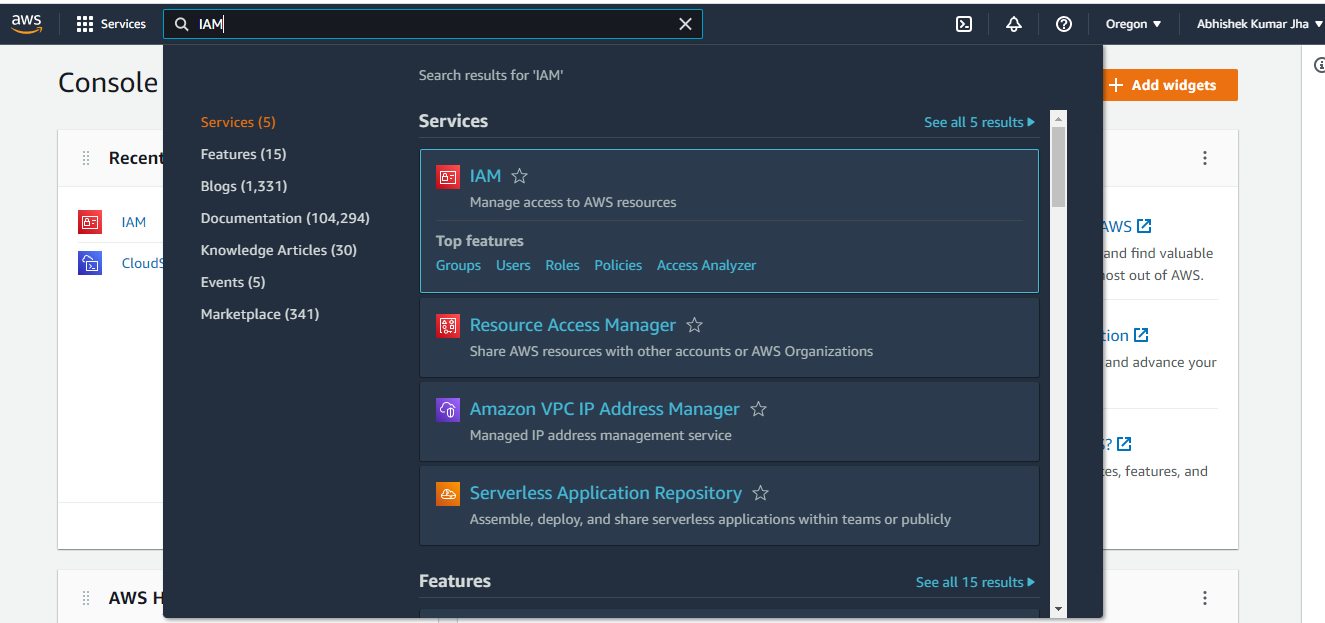


Now you can see the new permission ‘Administrator Access’ has been added to the user.



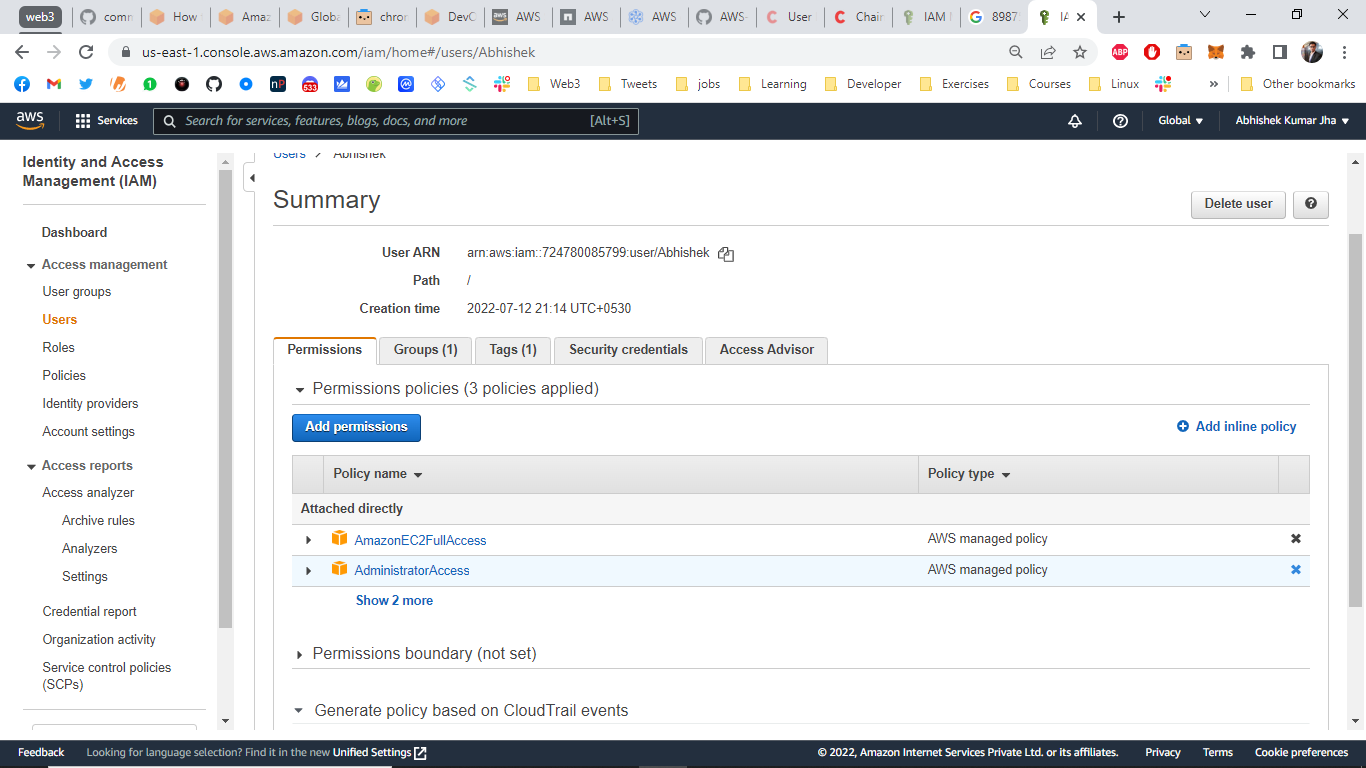
5. How to detach a policy from a user.

Step1 – Go to ‘Users’ by searching for IAM under console search bar.



Step2 – Select the user you want to detach a policy from.



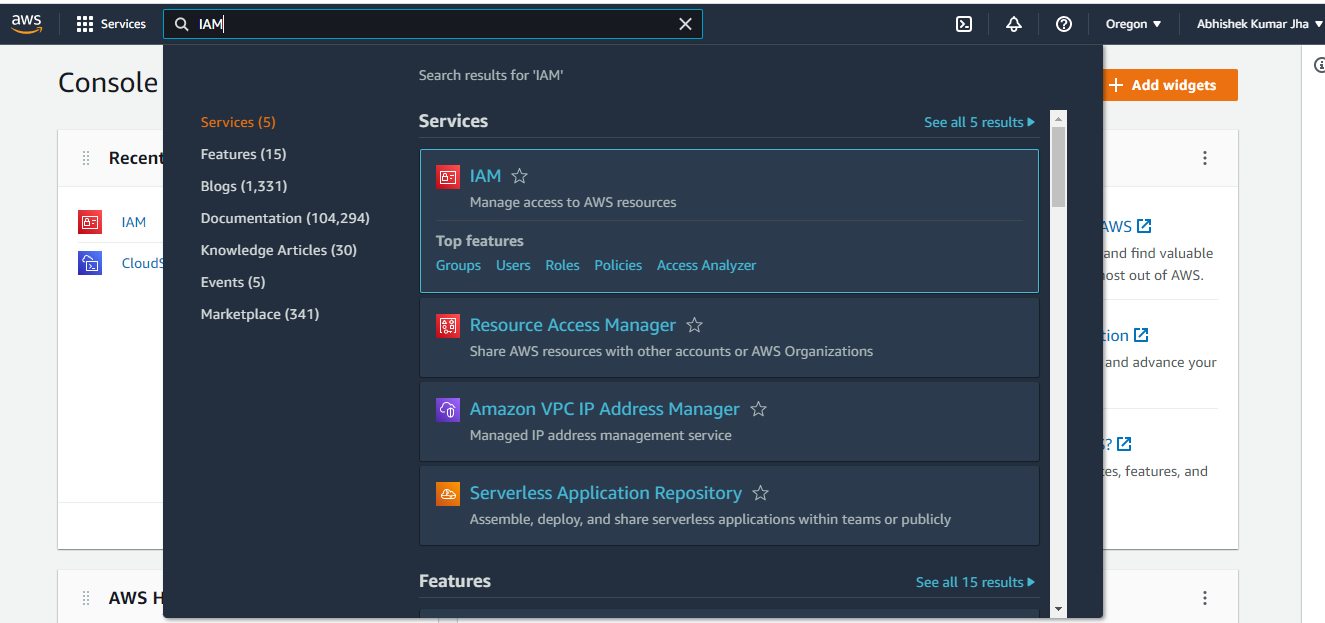
Step3 – Click on cross button beside the policy you want to detach. T

Step4 – Click on ‘Detach’ and the policy will be detached from the user.



6. How to delete a user? Hands-On

Step1 – Go to IAM > ‘Users’ by searching for IAM on Management console search bar.

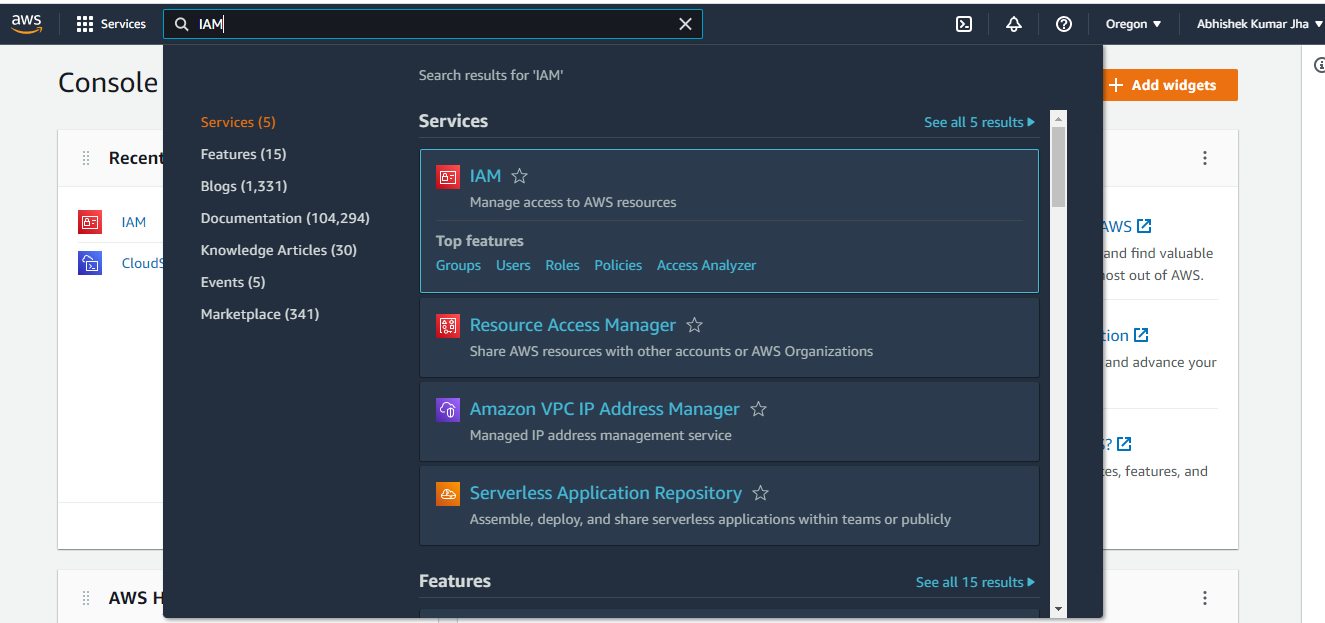


Step2 – Select the User you want to delete and click on ‘Delete’.



7. How to give a new password to an IAM user if he/she loses the credentials? Hands-On.

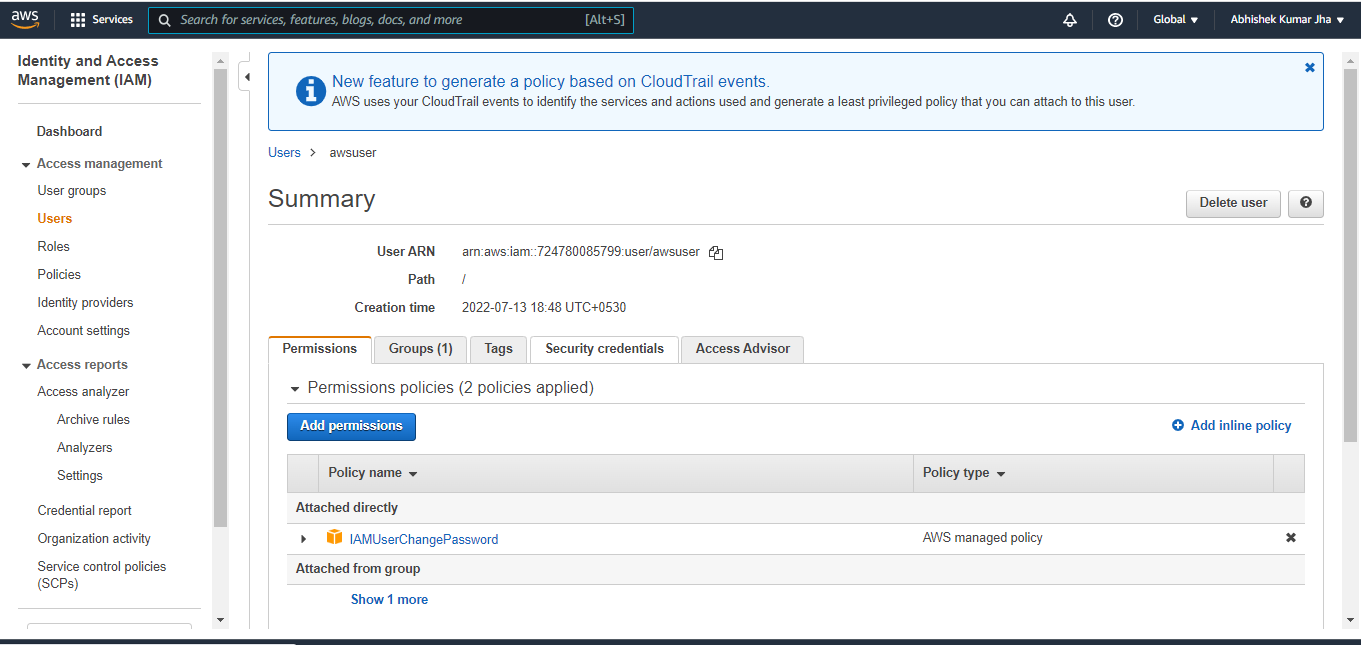
Step1 – Go to IAM > ‘Users’ by searching for IAM on Management console search bar.



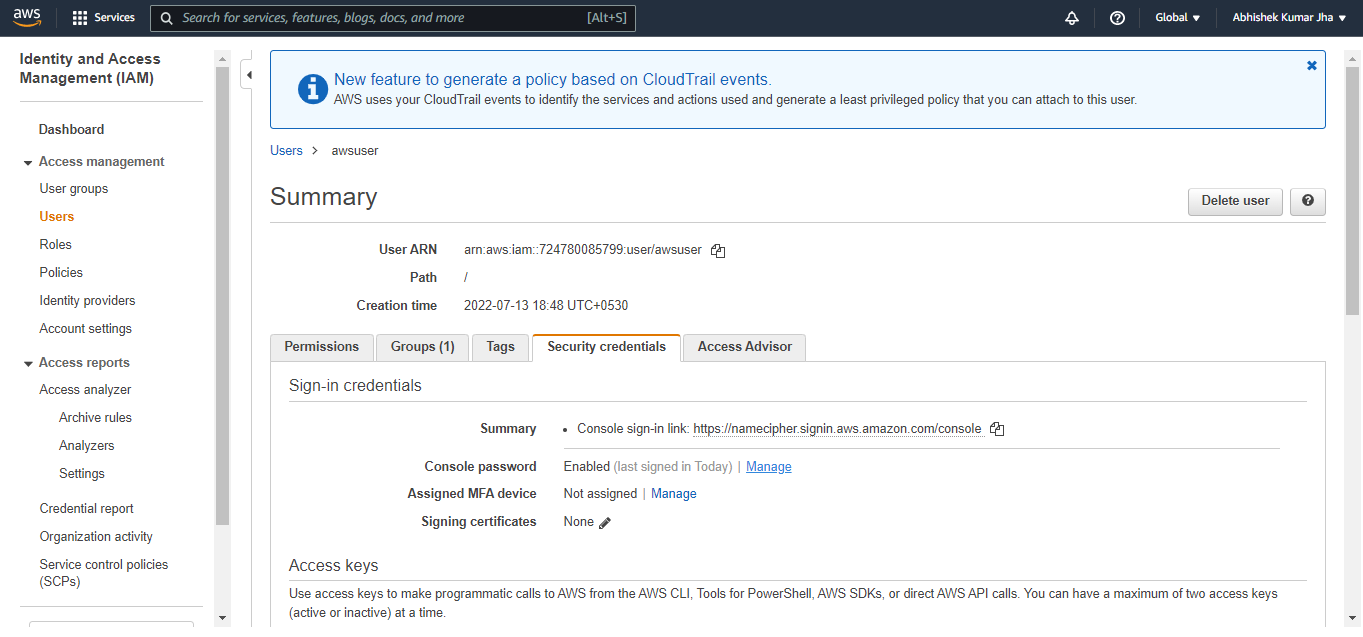
Step2 - Select the User you want to give a new password to.

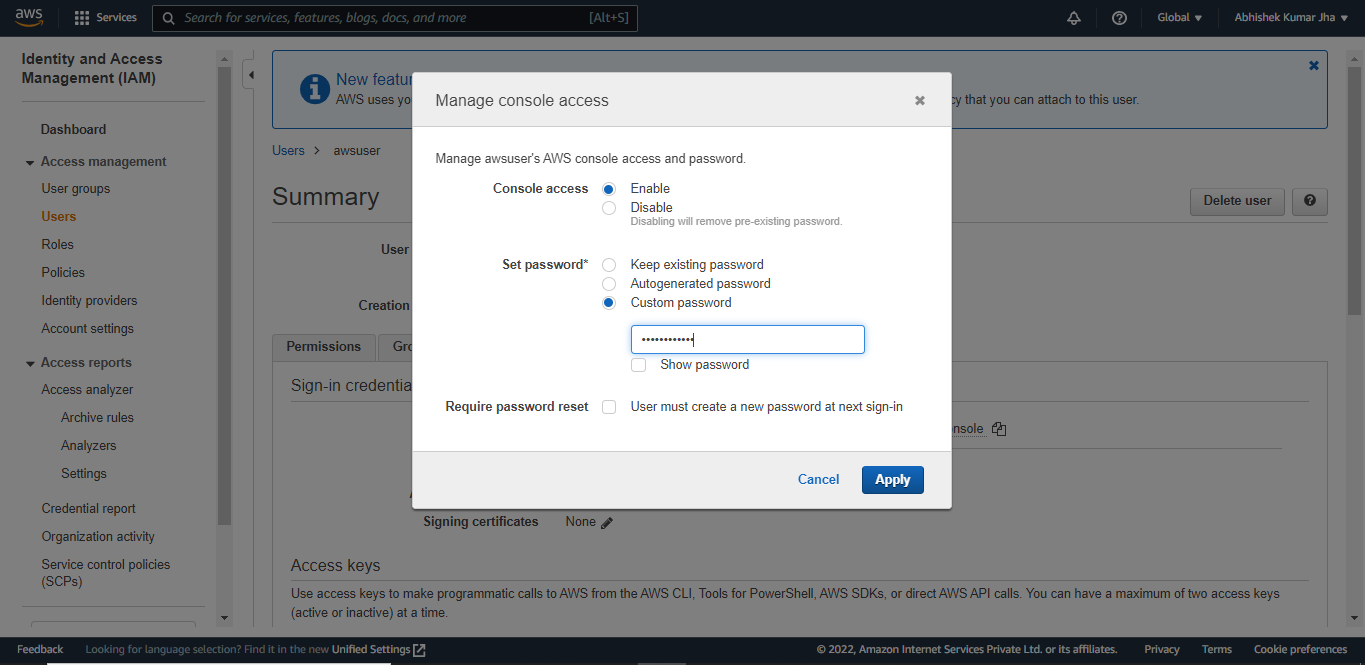


Step3 – Click on ‘Security Credentials’.



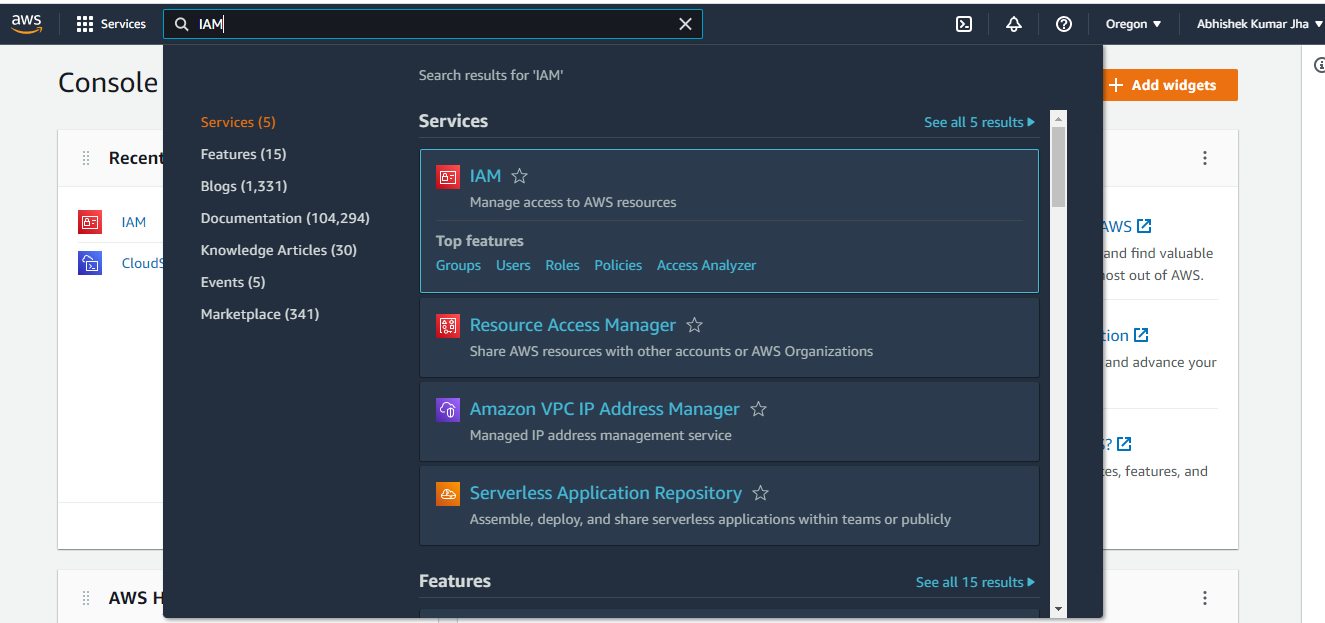
Step4 – Click on ‘Manage’ beside ‘Console Password’.



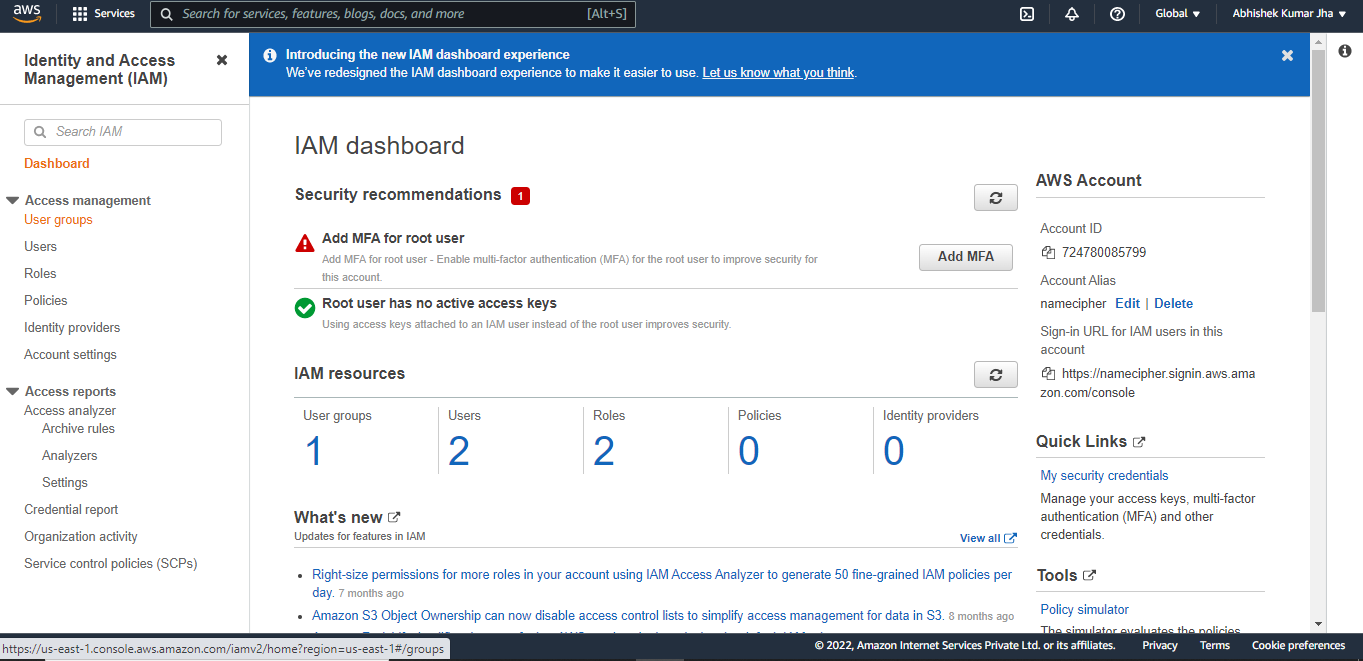
Step5 – Select ‘Custom Password’ and add a new password and click on apply.

8. How to create a user group? How to add users to the user group? How to attach policy to the user group? Hands-On

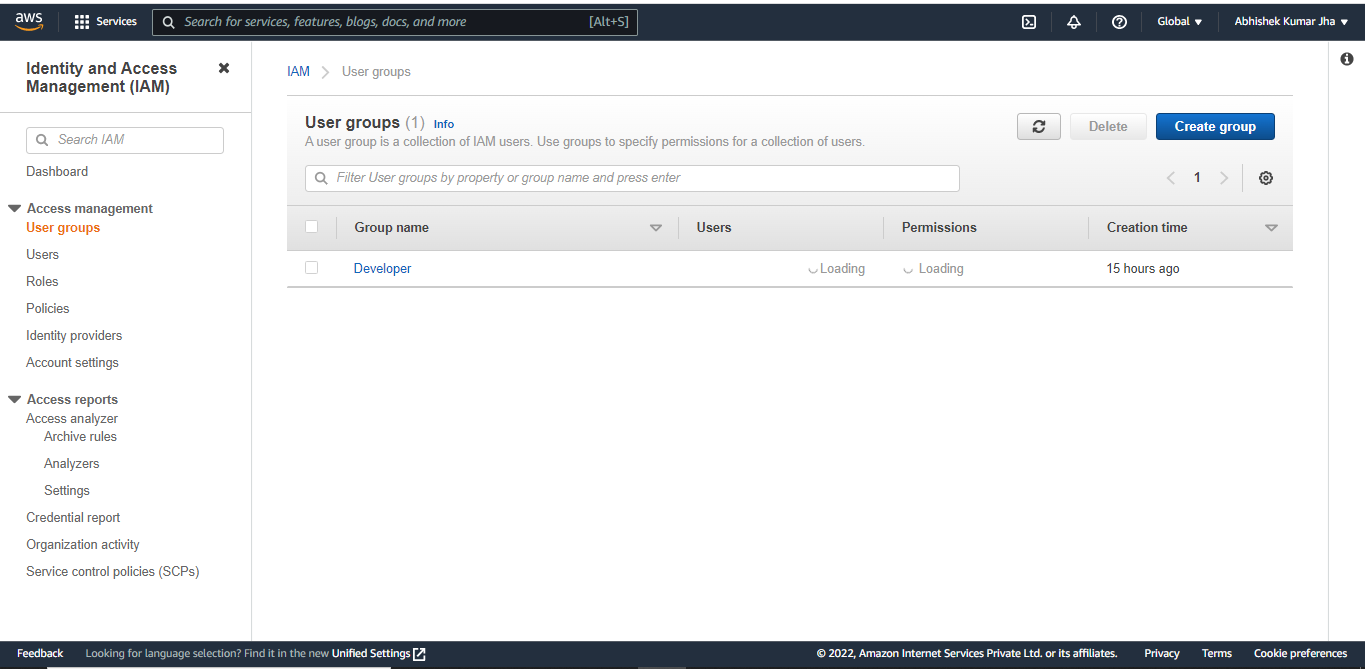
Step1 – Go to IAM Dashboard by searching for IAM on console Management search bar.



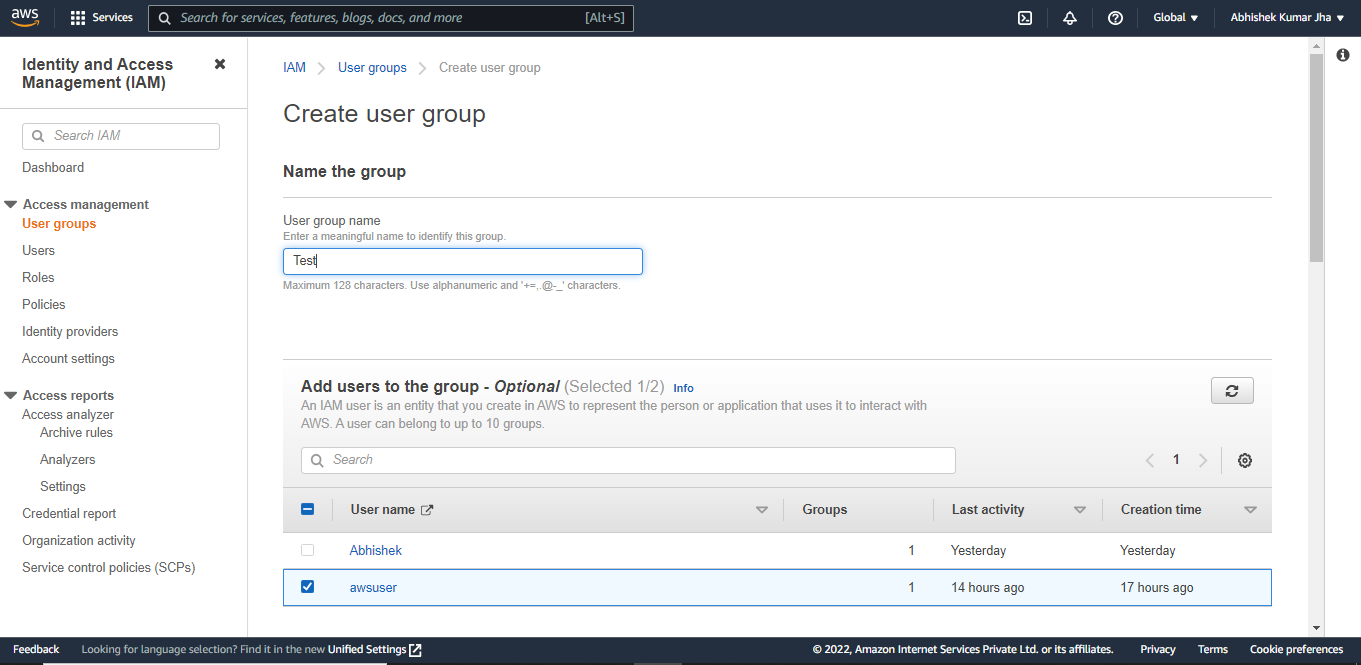
Step2 – Click on ‘User Group’ under Access Management.



Step3 – Click on ‘create Group’.



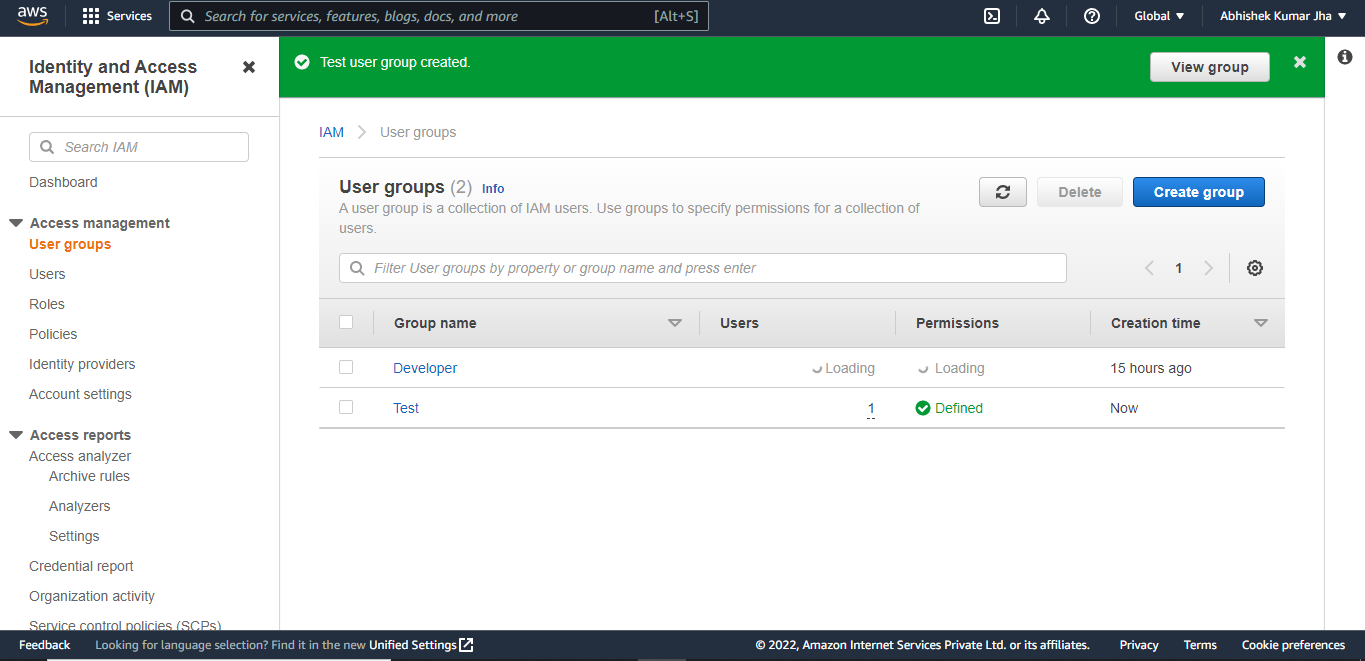
Step4 – Supply User Group Name. To add a user to the group select the user by clicking on checkbox beside User name.



Step5 – To attach a policy to the Group, select the policy, scroll down and click on create group.

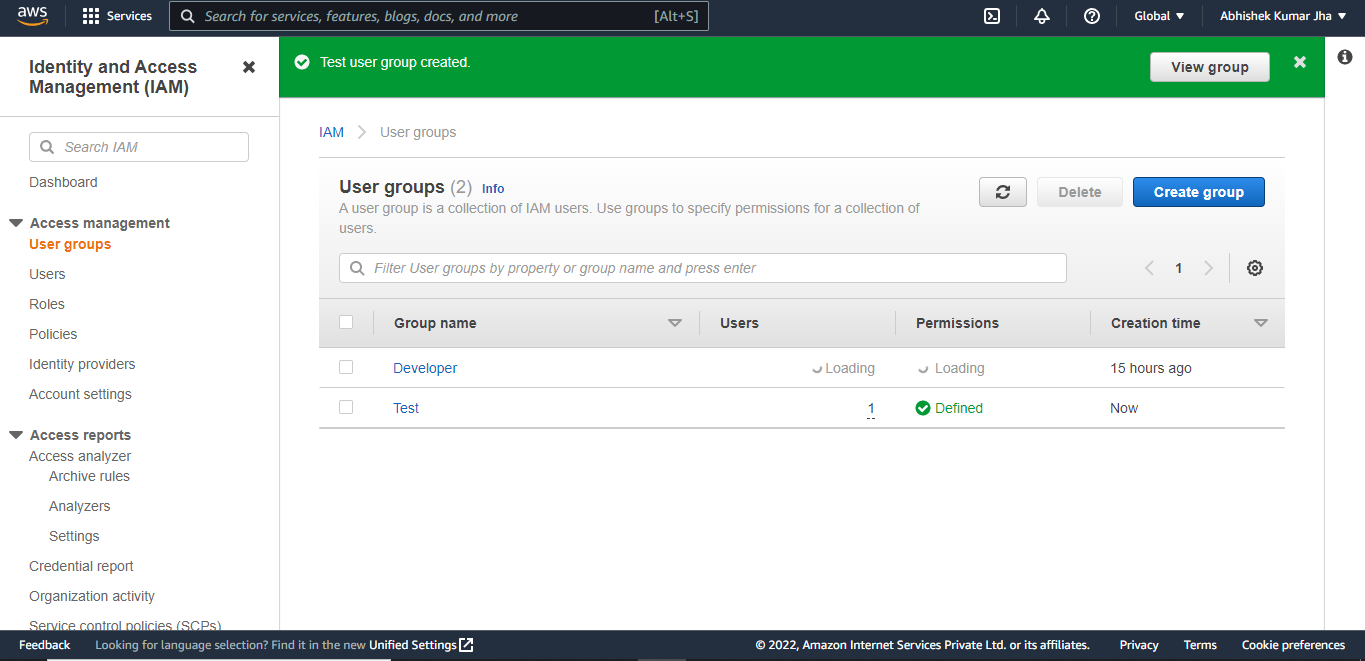


Now you can see that the “Test” user group created message on top and also see the group in the list of User Groups.

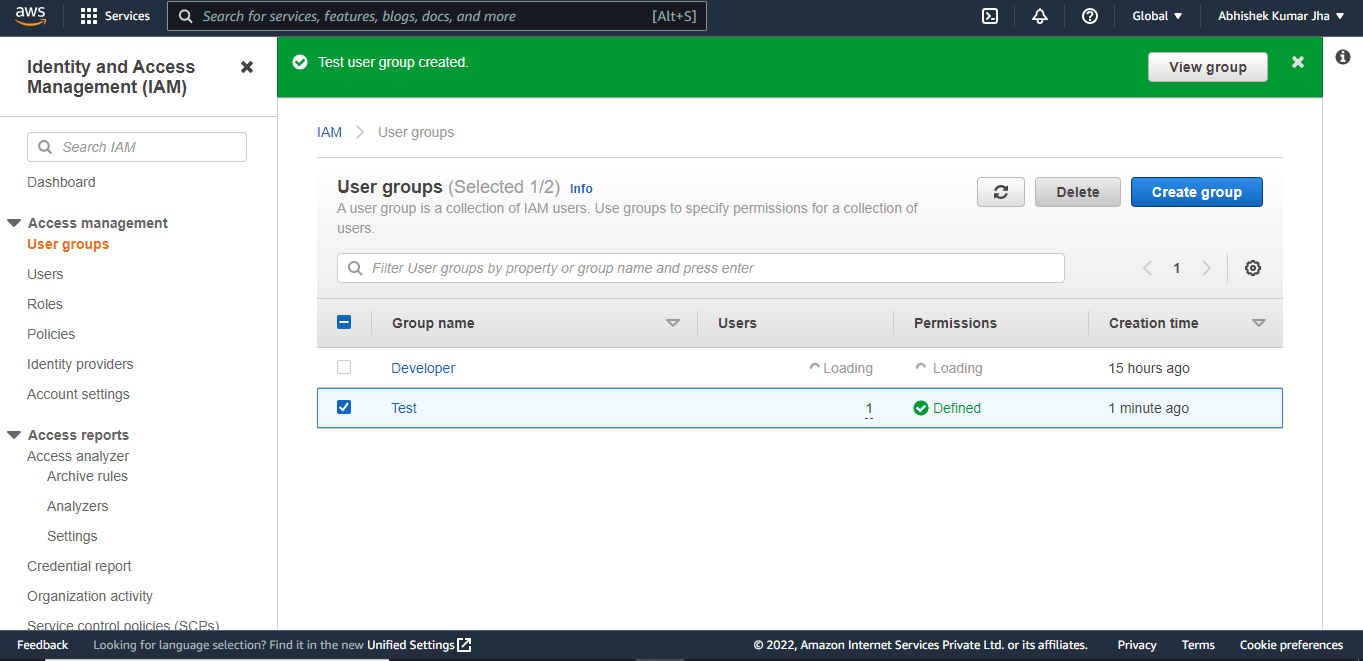


9. How to delete a user group? Hands-On

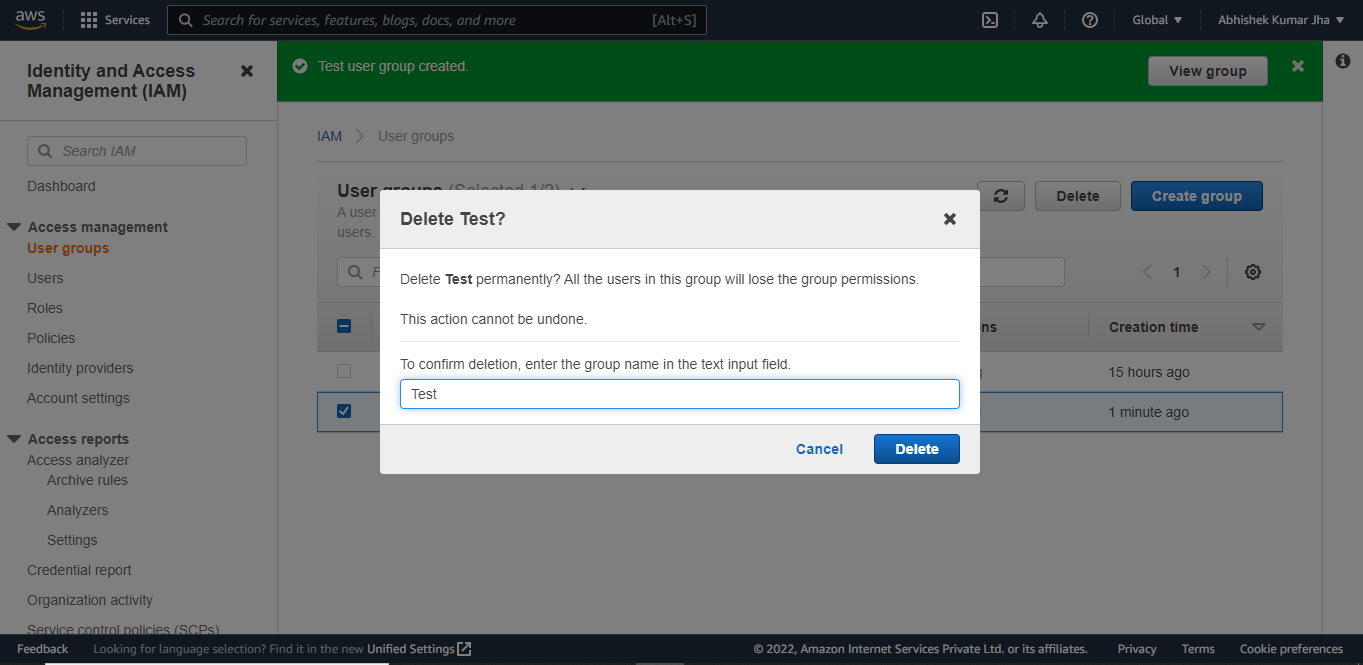
Step1 – Go to User Group under IAM Dashboard.



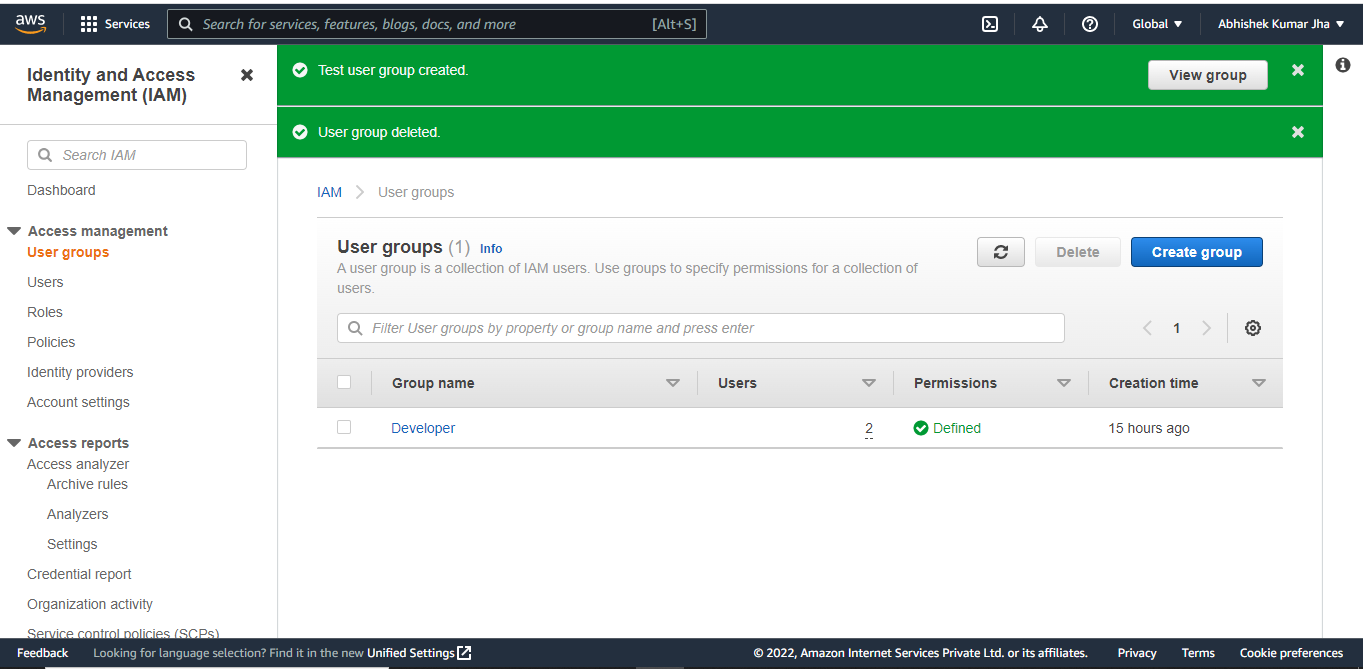
Step2 – To delete a group, select the group you want to delete and click on delete option.



Step3 – Write the Group name in input field to confirm deletion and click ‘Delete’.

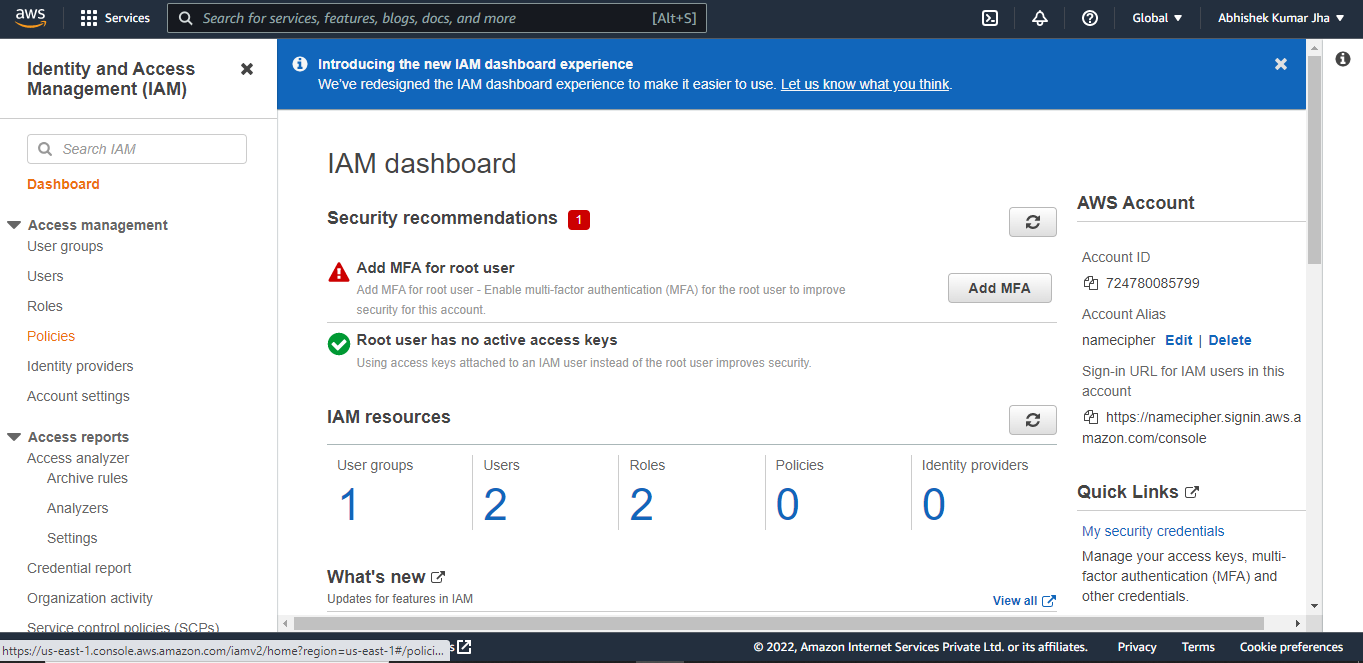


Now you can see that the user group “Test” has been deleted.

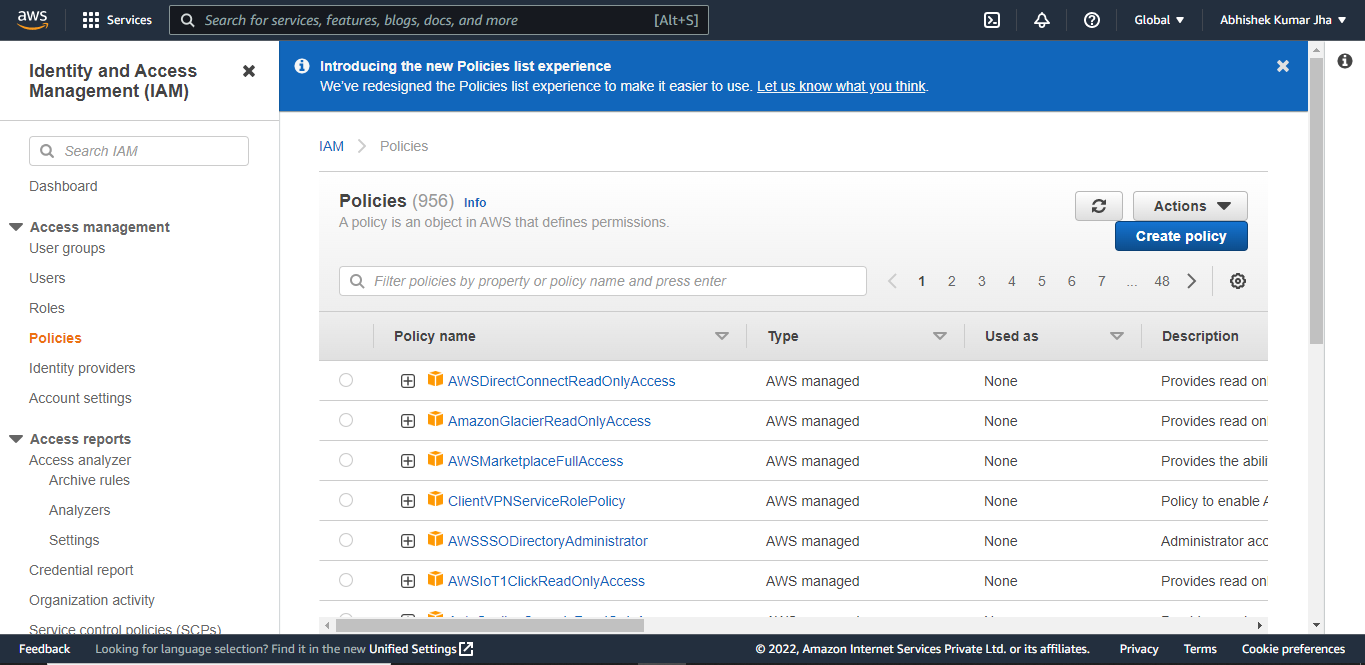


10. How to create your own policy? Hands-On

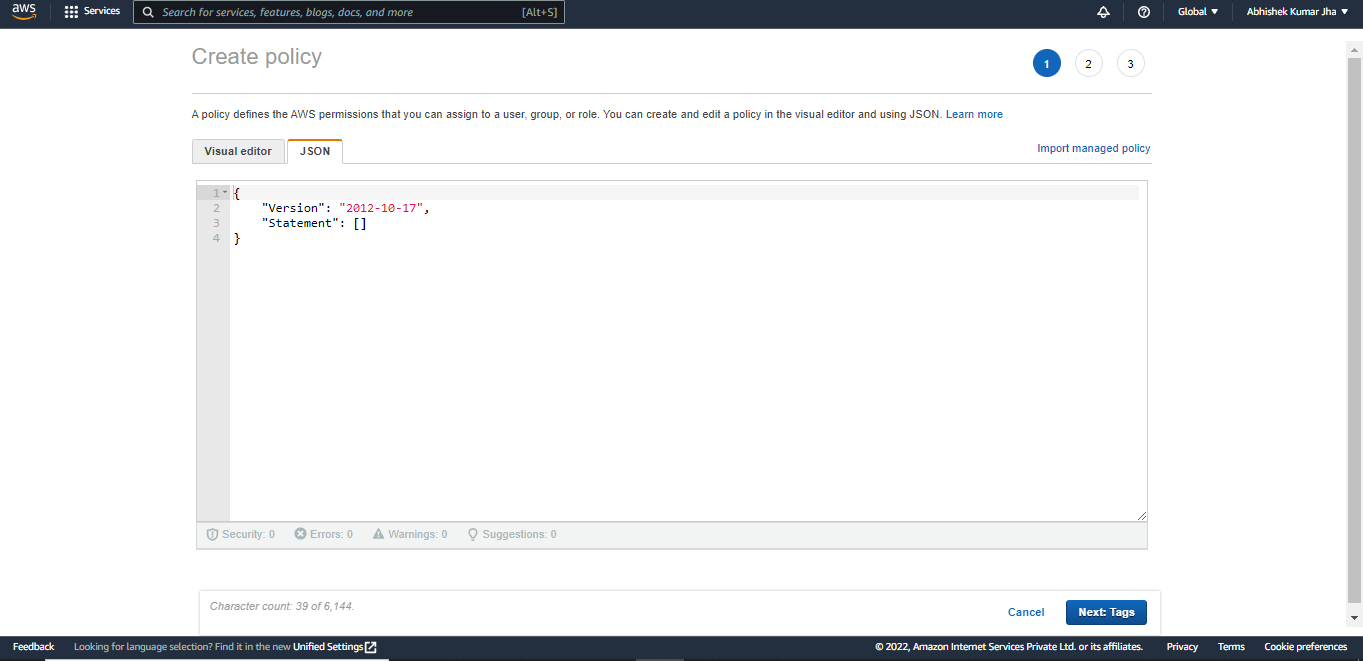
Step1 – Go to IAM Dashboard and click on ‘Policies’.



Step2 – Click on ‘Create Policy ’ .

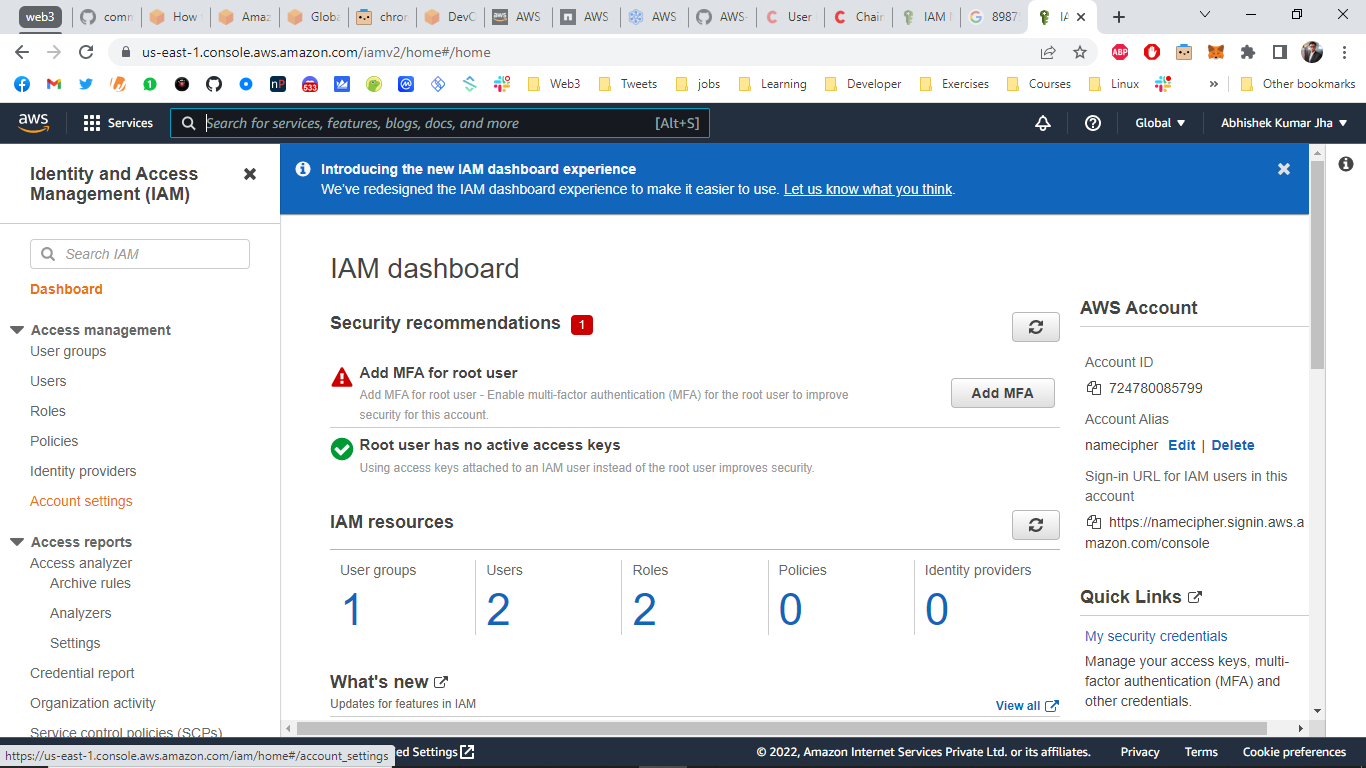


Step3 – Click on JSON tab. Add the JSON coding and click on Next.

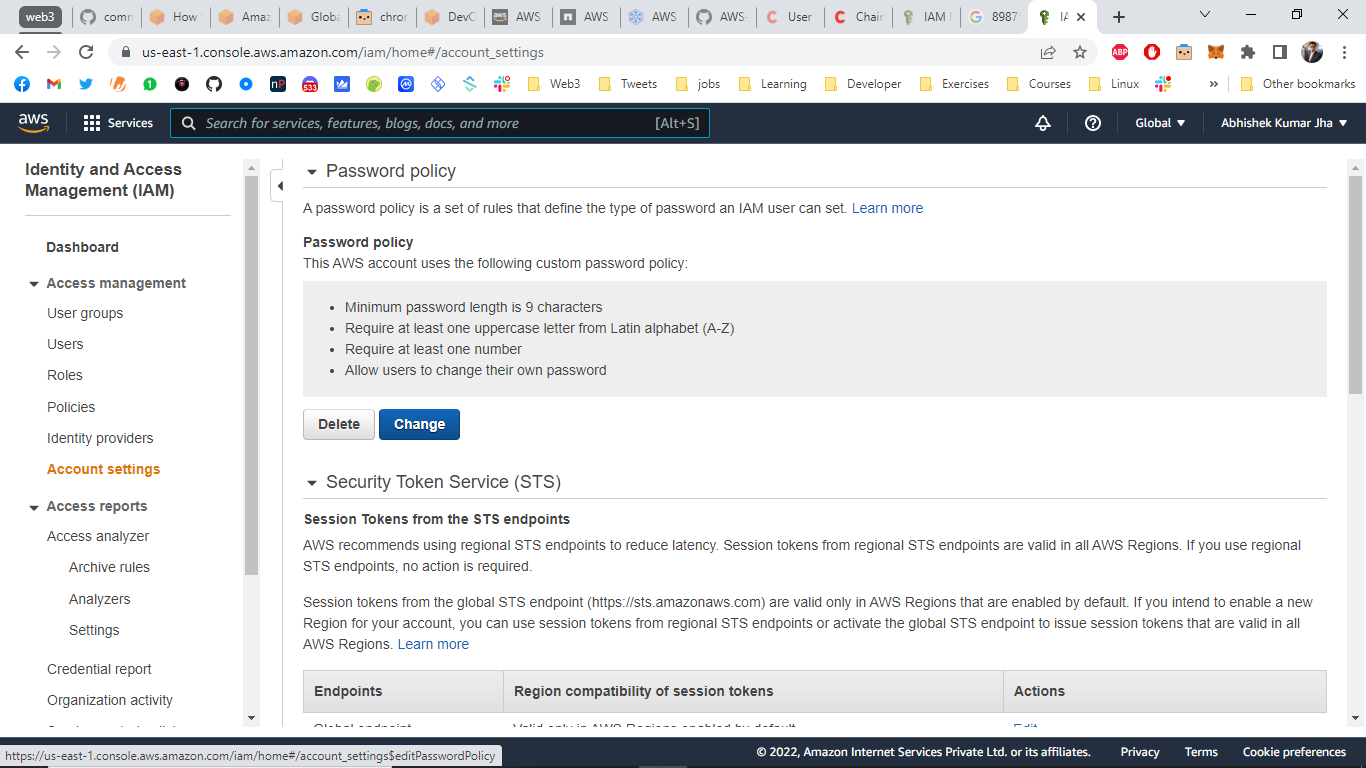


11. How to change the Password Policy? Hands-On

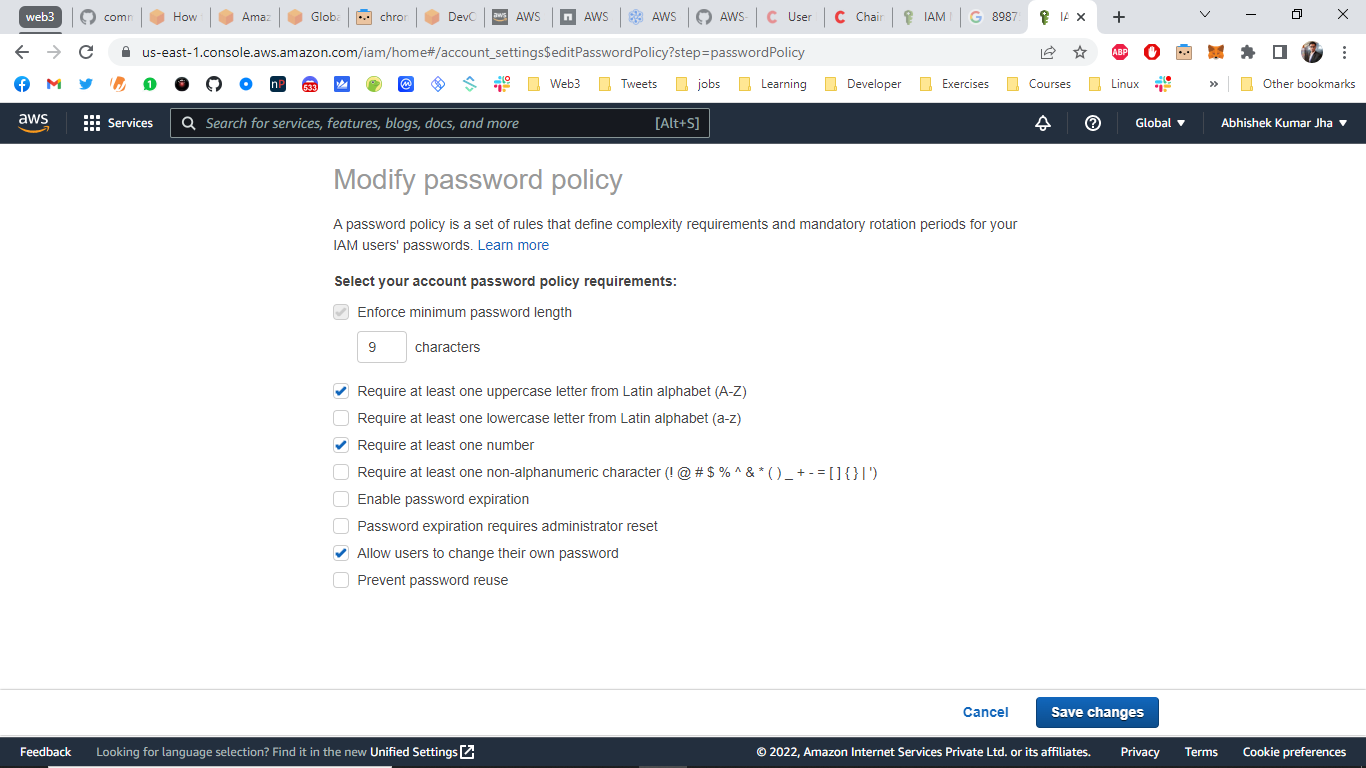
Step1 - Go to IAM Dashboard and click on Account Settings.



Step2 – Click on Change under Password Policy.



Step3 – Select the policy options and click Save Changes.



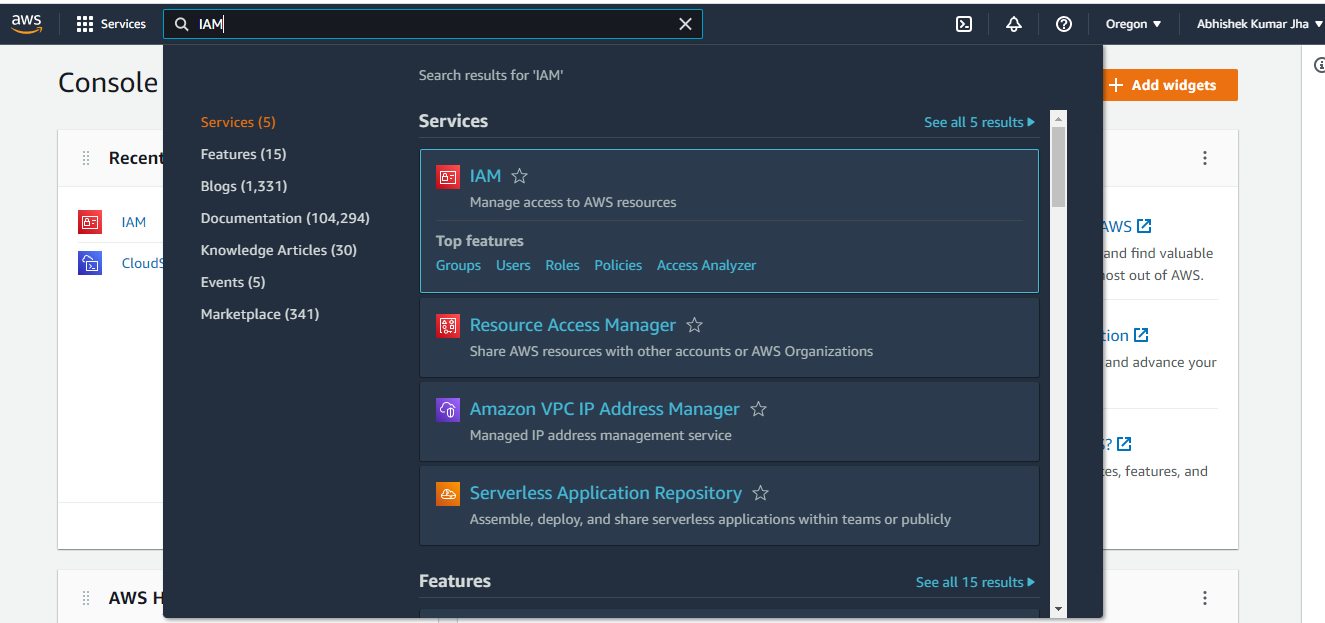
The password has been updated.

12. What is Password Policy?

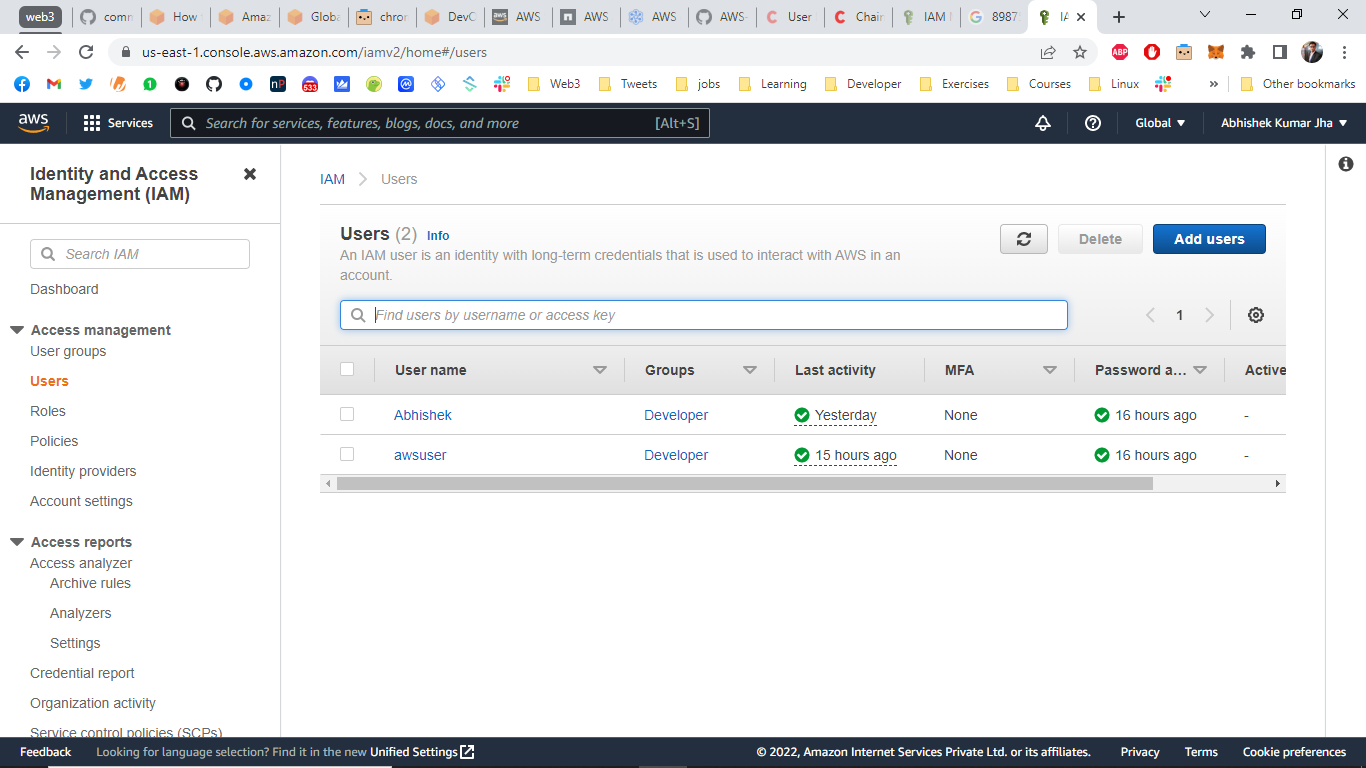
A password policy is a set of pre-defined rules according to which a user needs to set their password regarding security concerns. Password policy can be changed/updated.

13. How to copy existing policy to a new user while creating a user? Hands-On

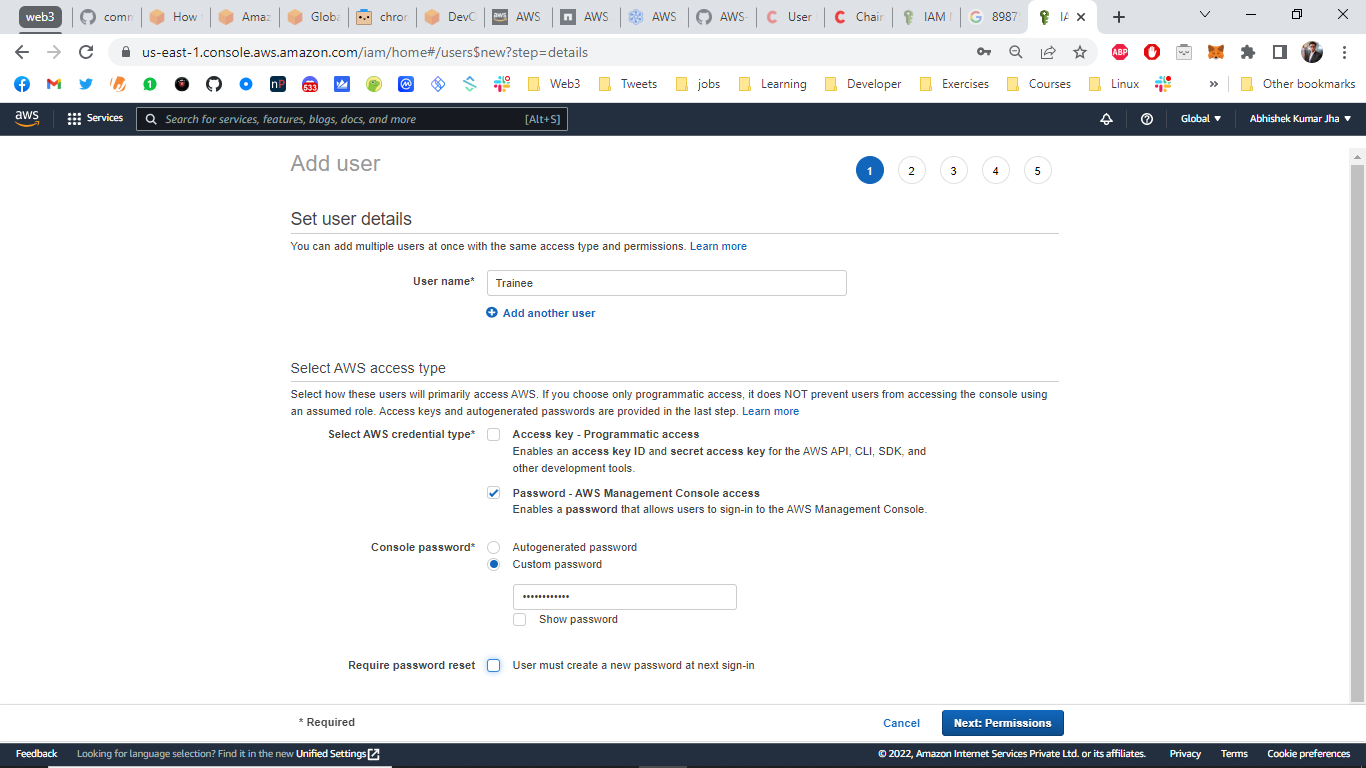
Step1 – Go to ‘Users’ on IAM Dashboard.



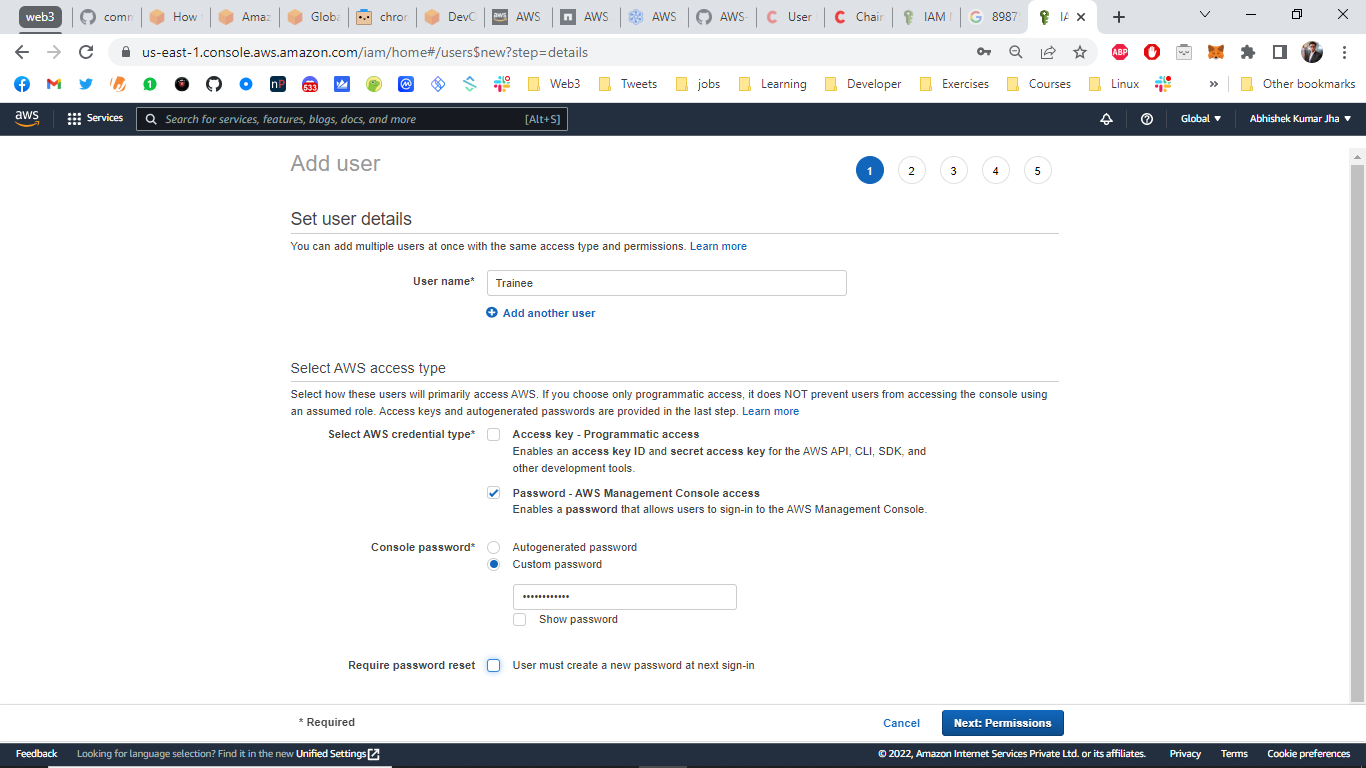
Step2 - Click on Add User.



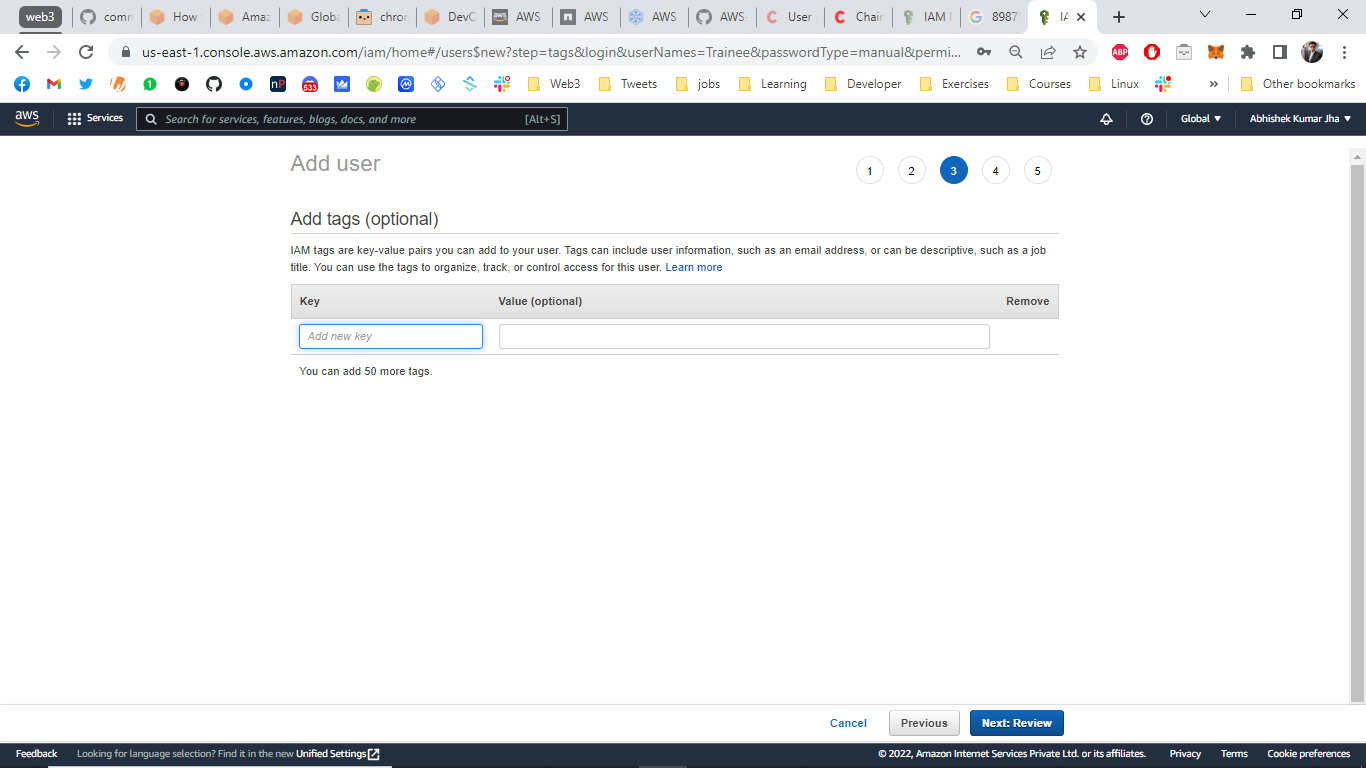
Step3 – Add User Name, Add password, click Next:Permissions.



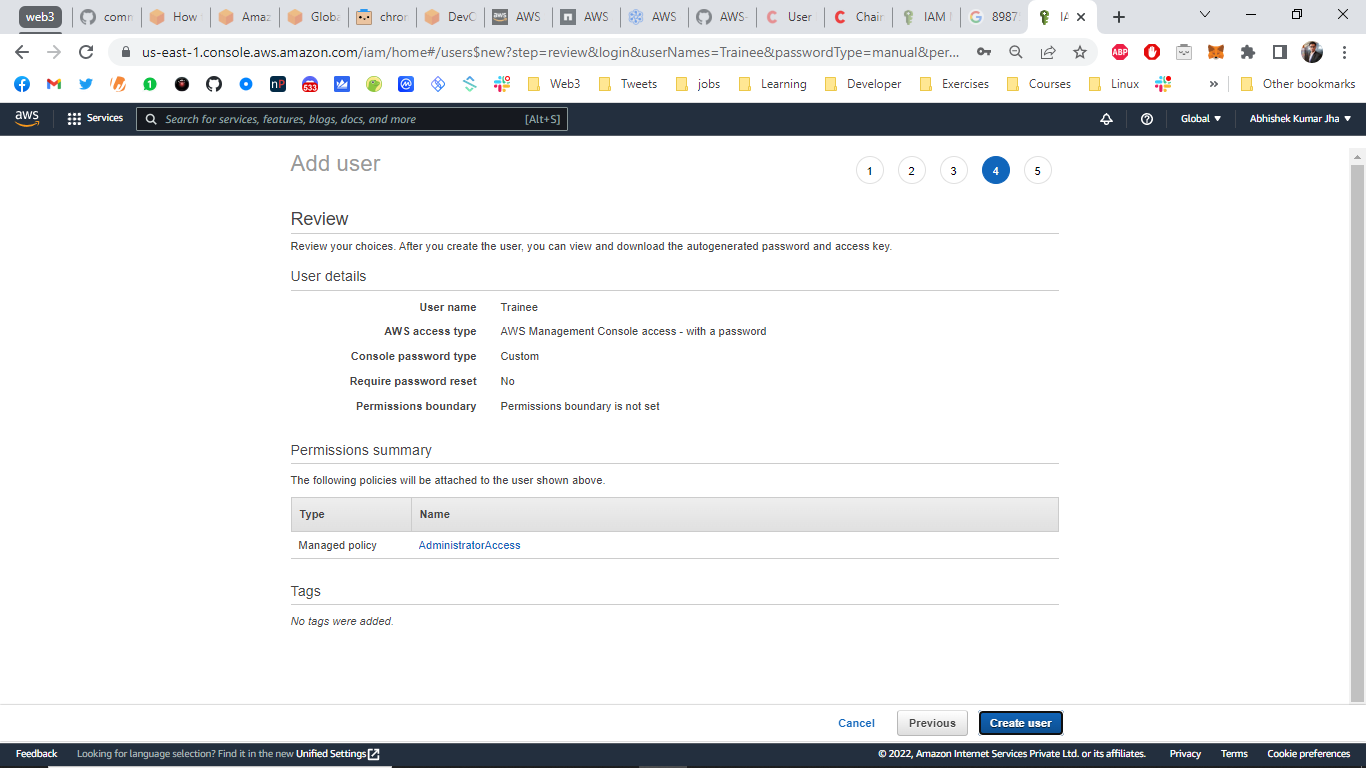
Step4 – Click on Attach Existing policy and select the policy.



Step5 – Click Next: Review.



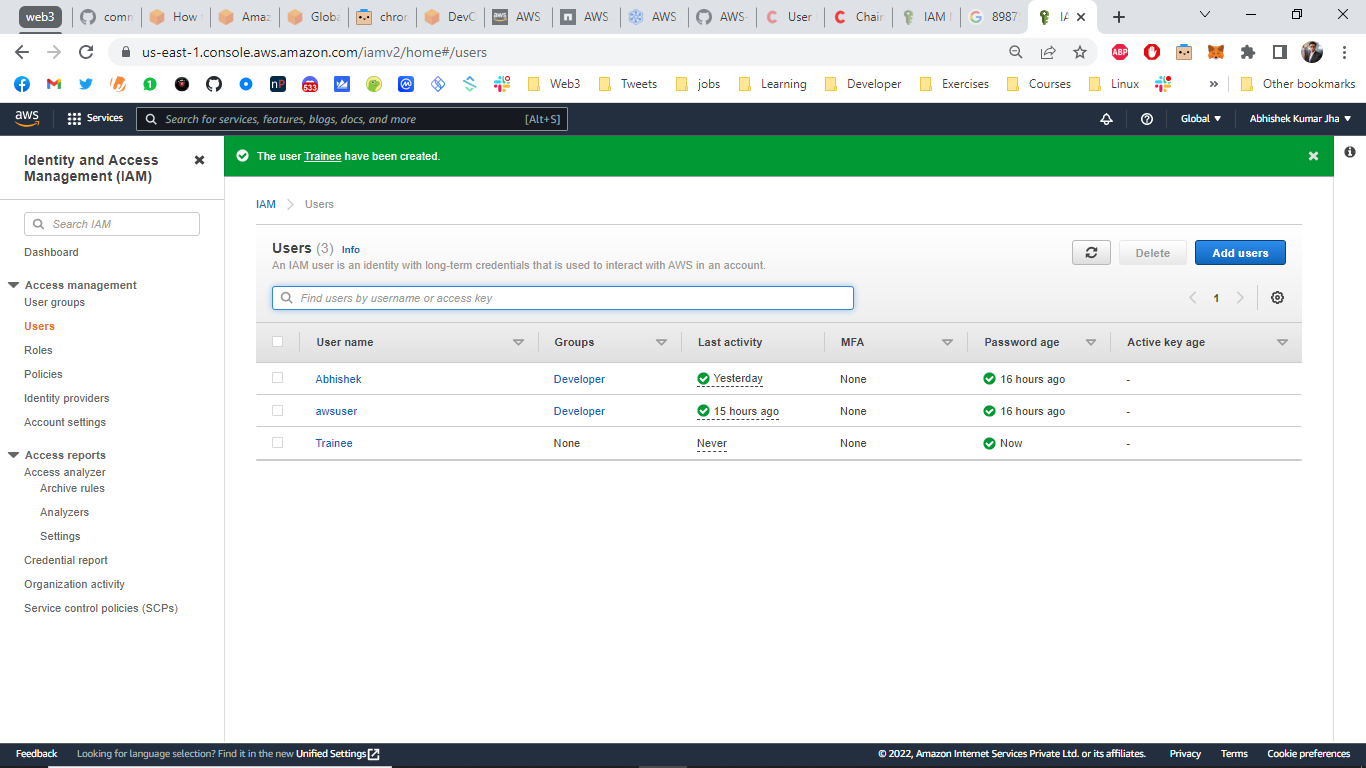
Step6 - Click Create User.



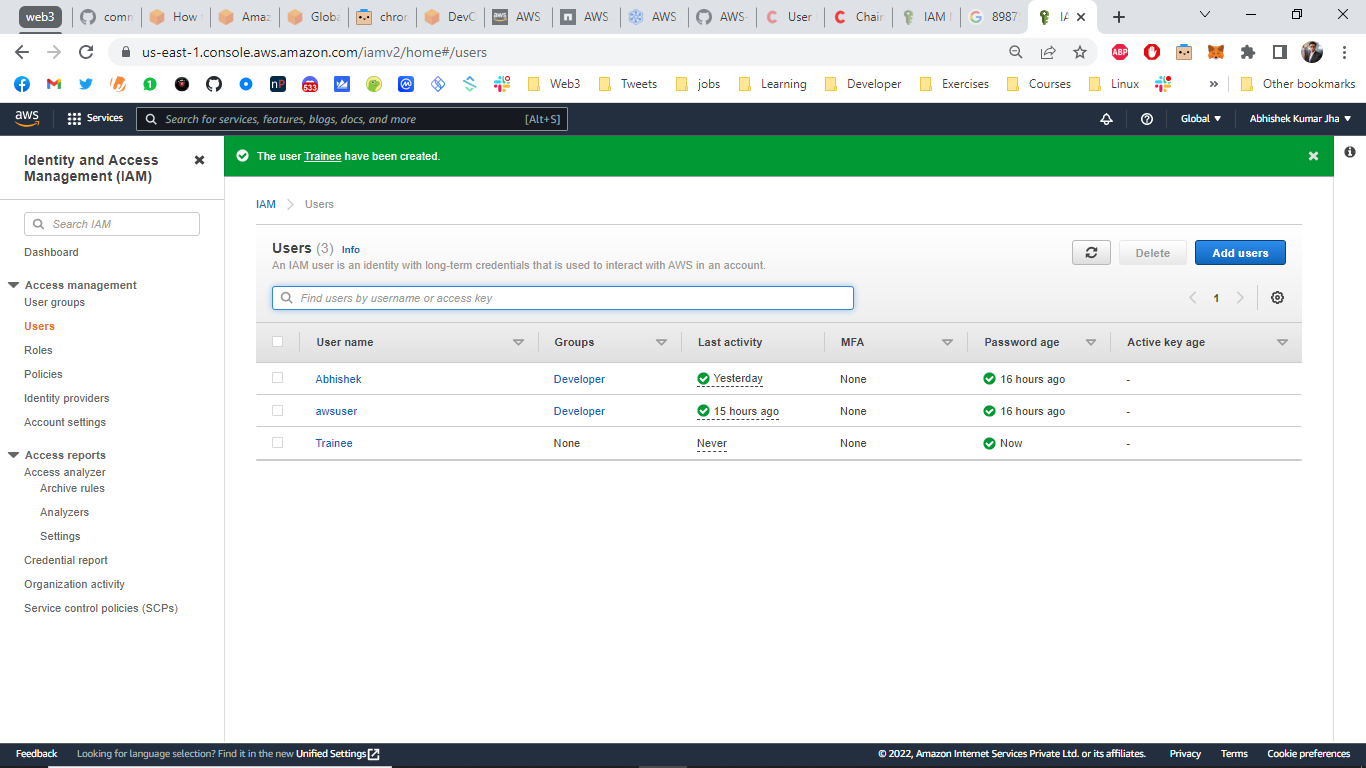
Step7 – Download the .CSV file with user credentials and click close.



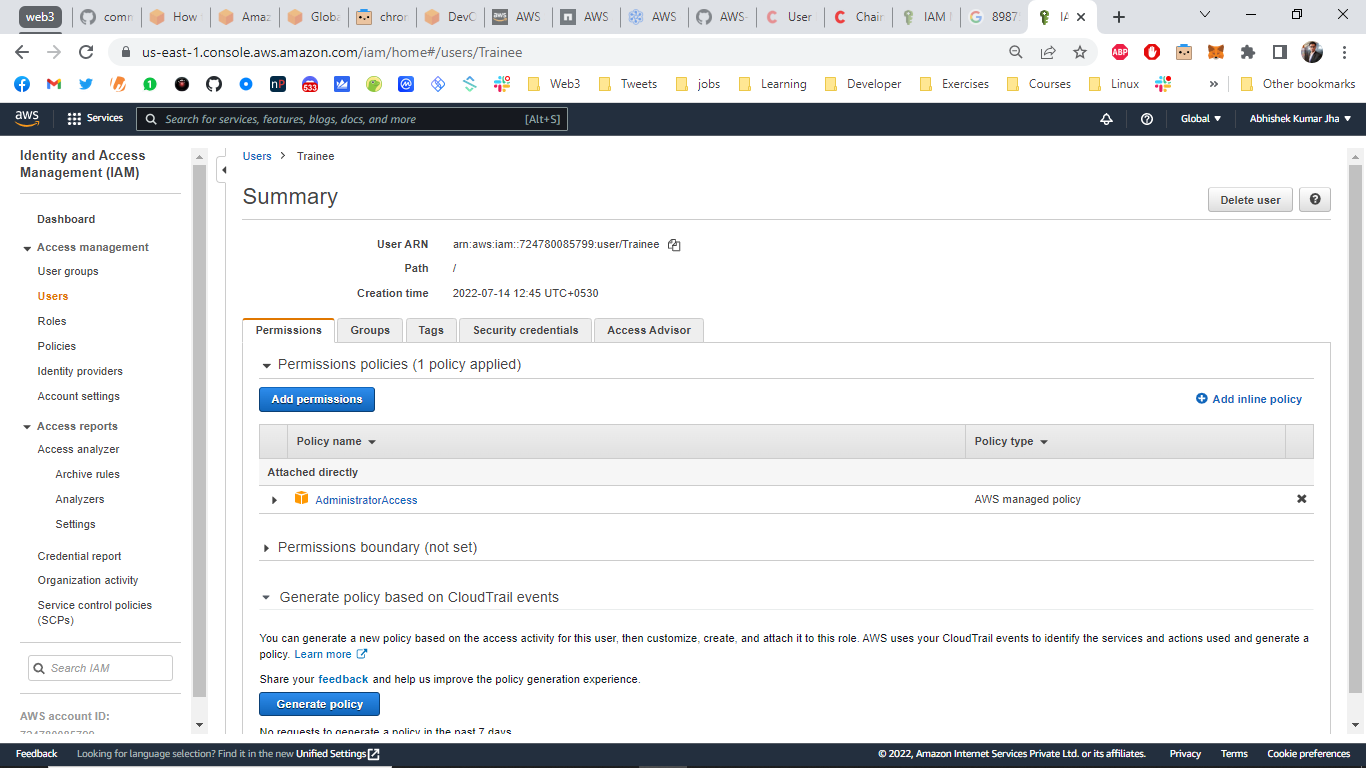
You can see that the Trainee User has been created message on the screen.



Step8 - Click on User ‘Trainee’



Now you can see that ‘Administrator Access’ Policy has be attached the user while creating the user.



14. What is SCP??(Service Control Policies)

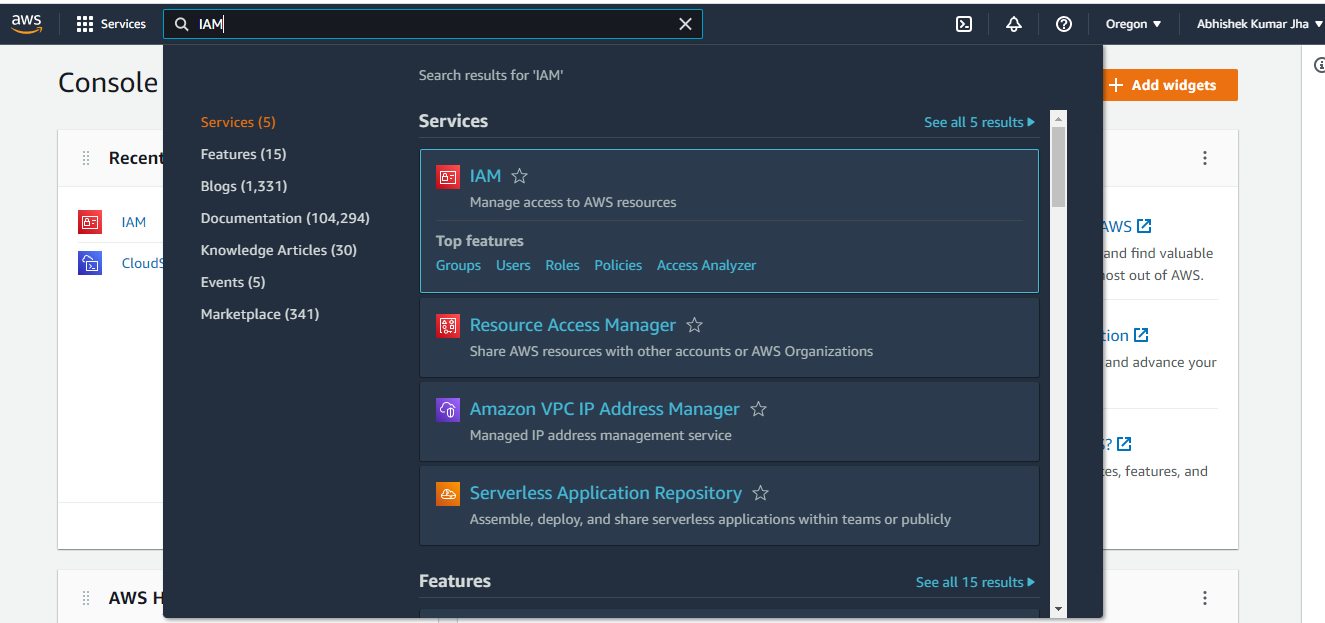
Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization.

15. What is MFA? (Multi Factor Authentication)

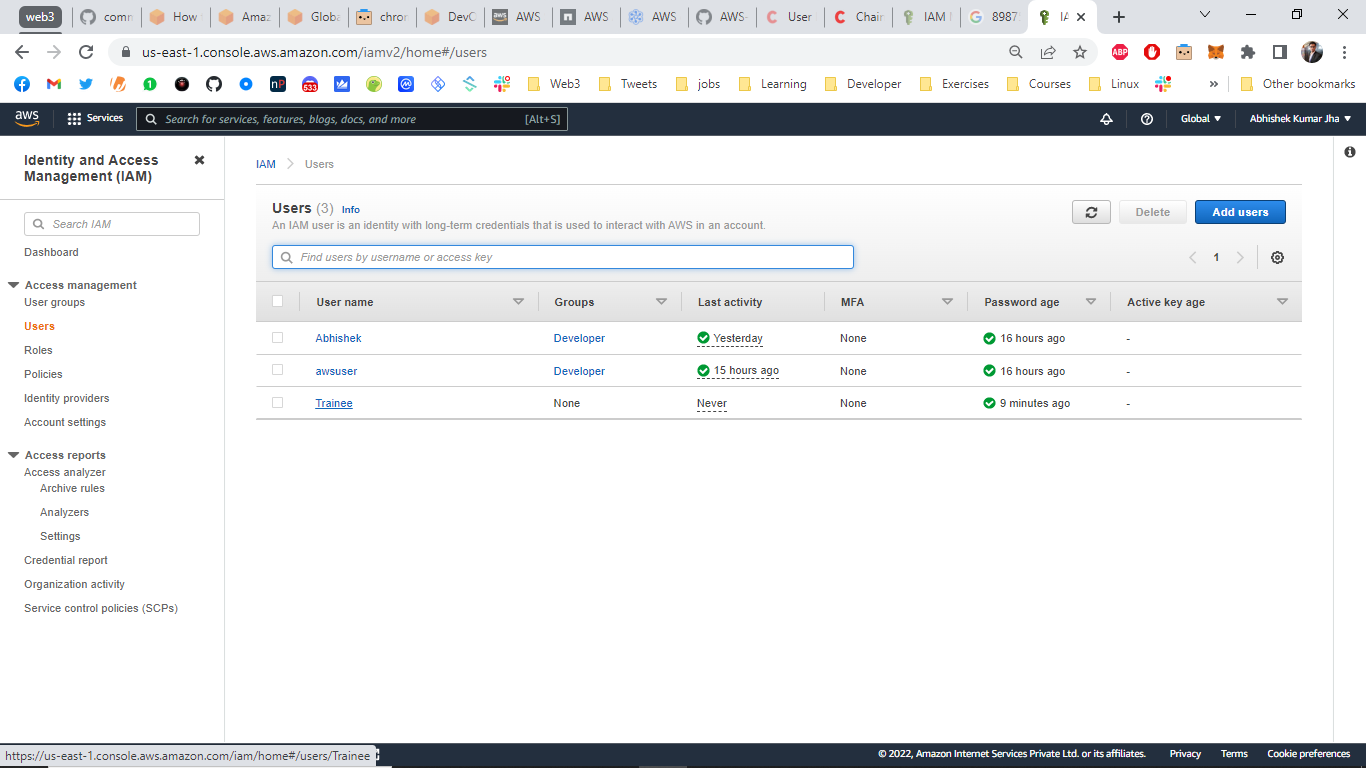
MFA or Multi Factor Authentication is a way of adding extra security to verify the user credential while logging in to AWS console as a means to verify the user and prevent fraudulent activities.

16. Hands-On – Create MFA for an IAM user.

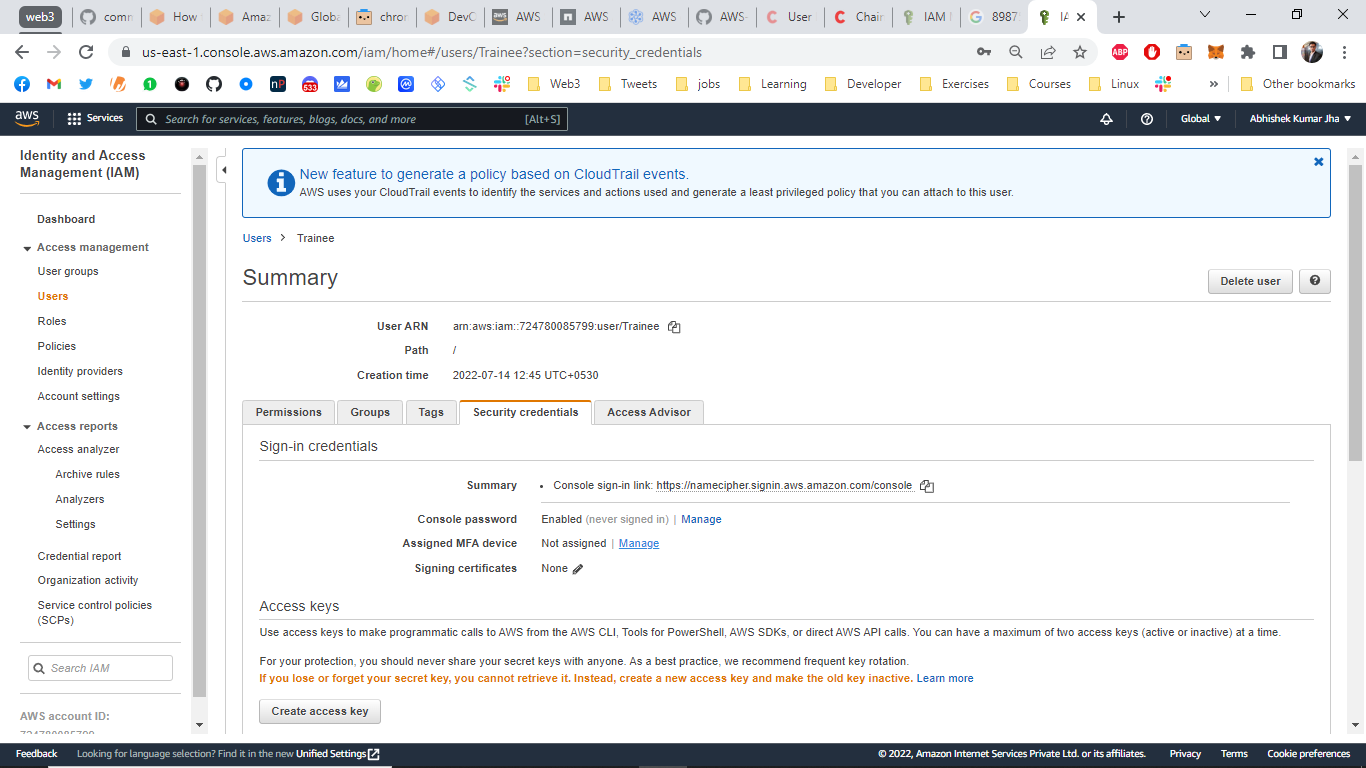
Step1 – Go to Users under IAM Dashboard.



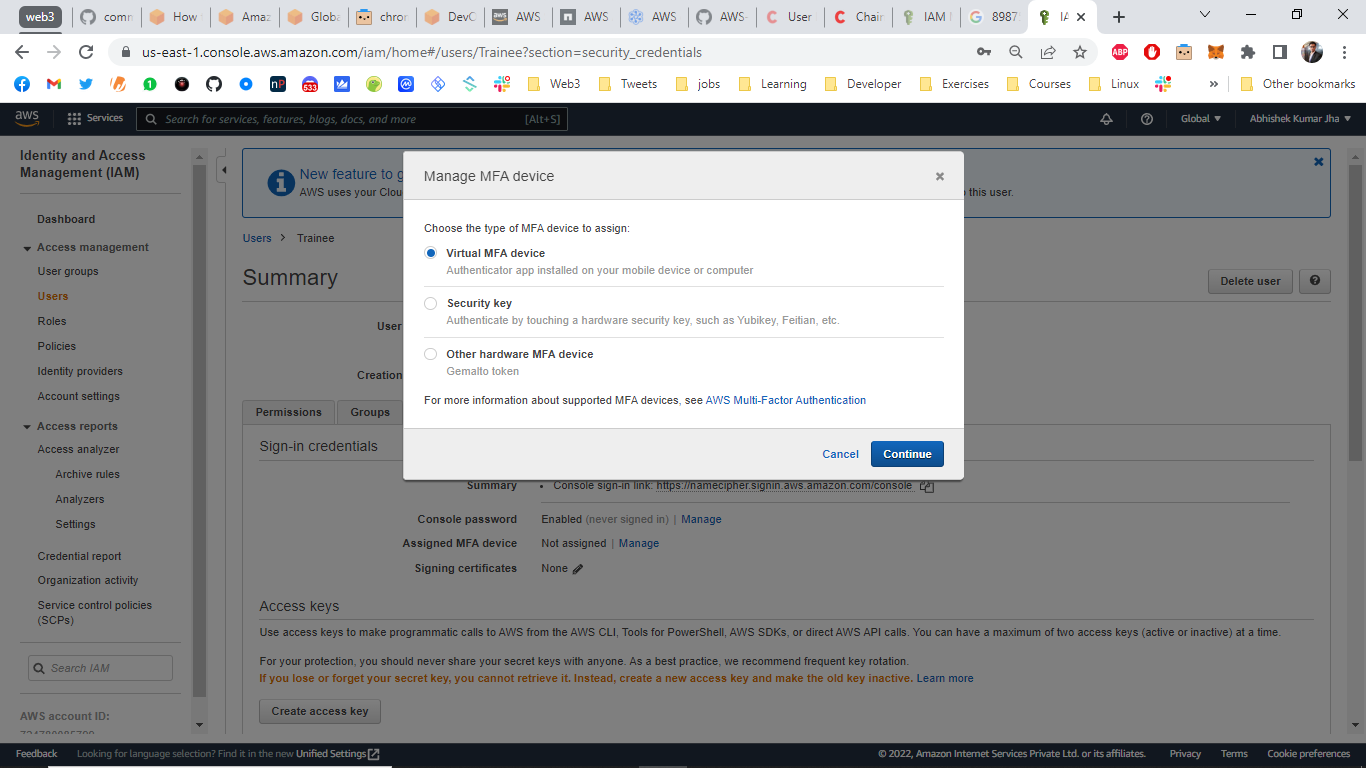
Step2 – Select the user you want to add MFA for.



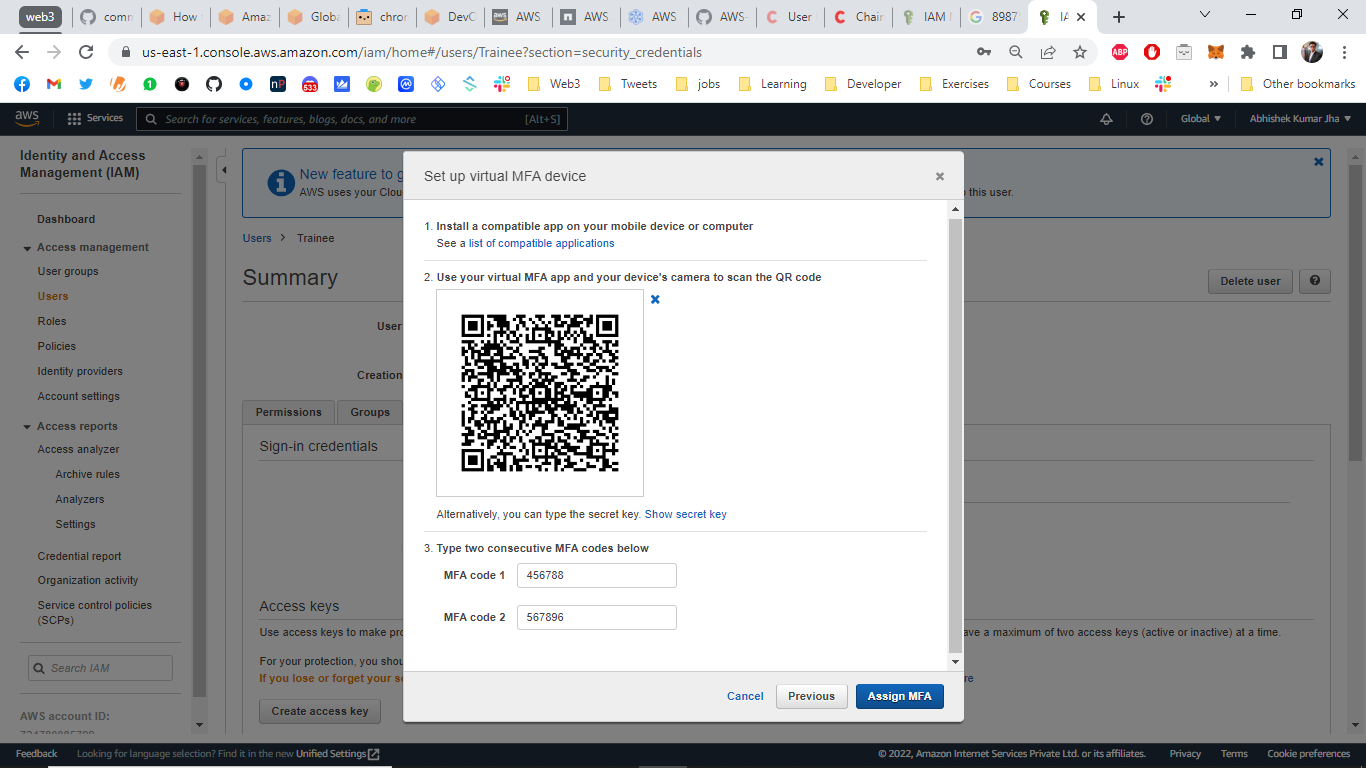
Step3 – Click on ‘Security Credentials’ tab and select Manage on Assigned MFA Device option.



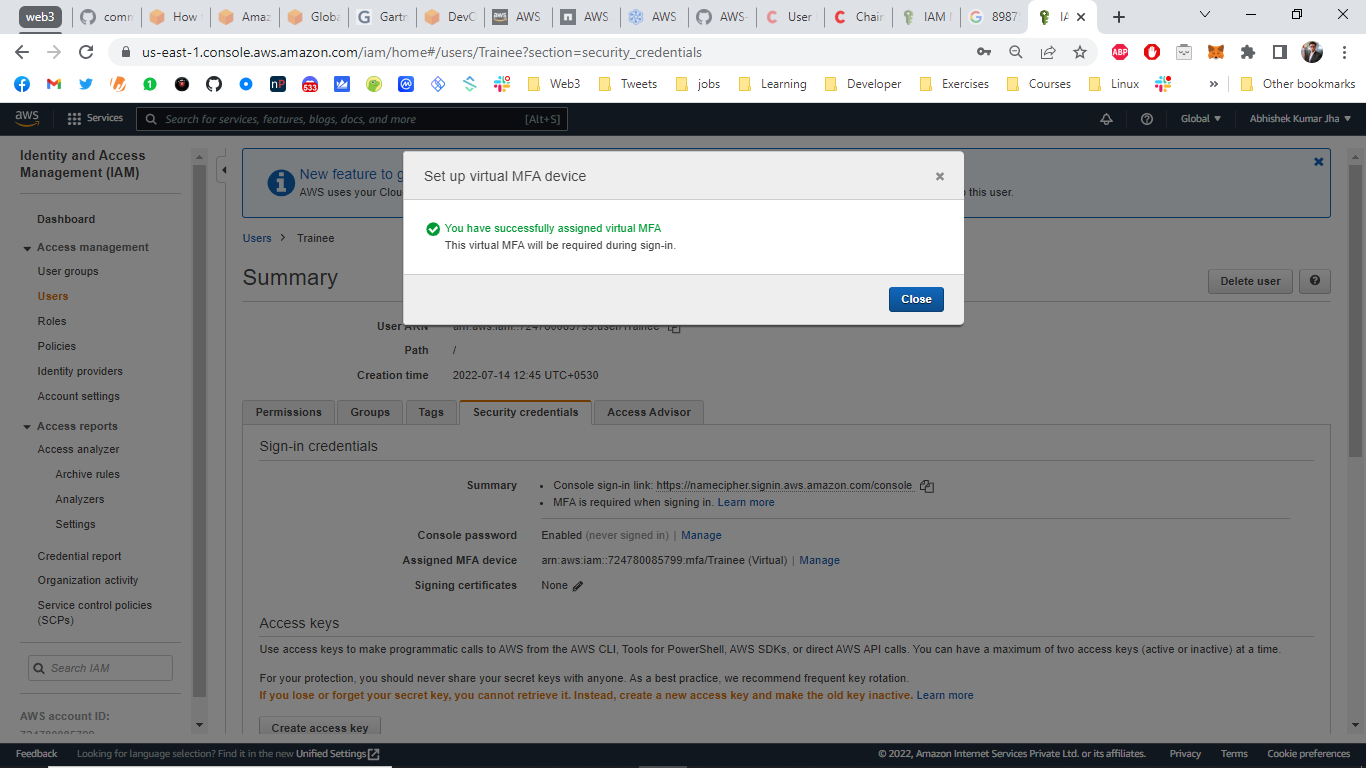
Step4- Select Virtual MFA device.



Step5 - Add the MFA codes from your Authenticator App and click ‘Assign MFA’.



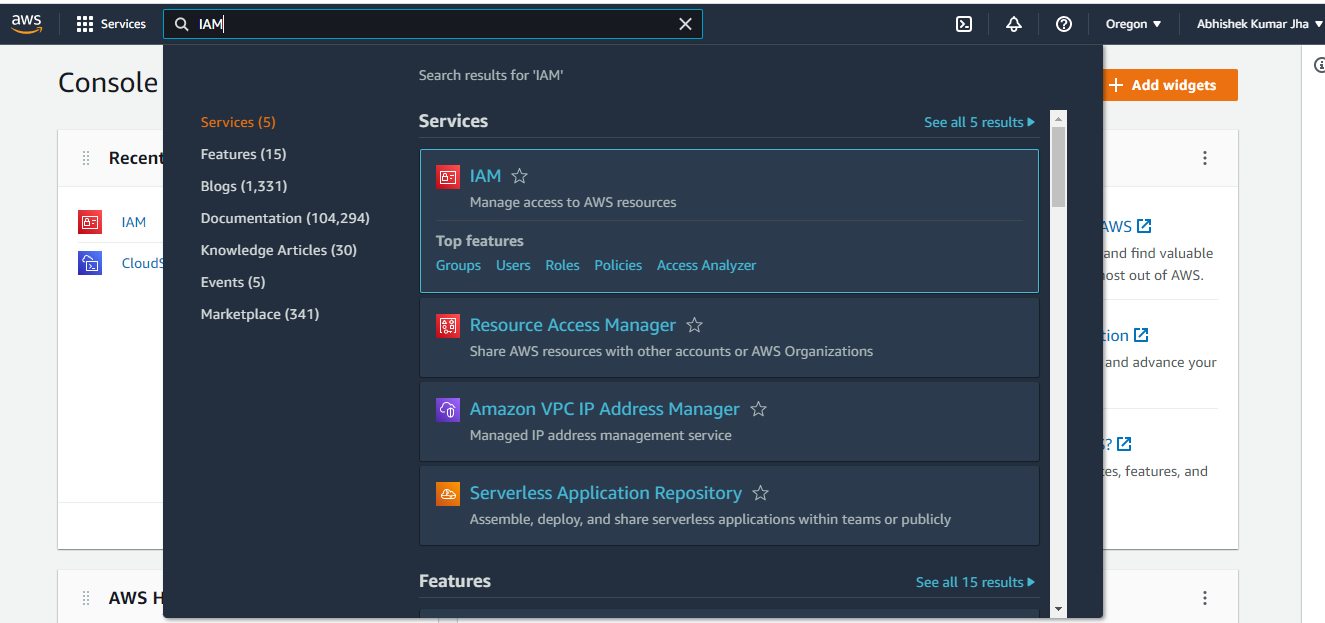
Now you get the message ‘ You have successfully assigned Virtual MFA’.



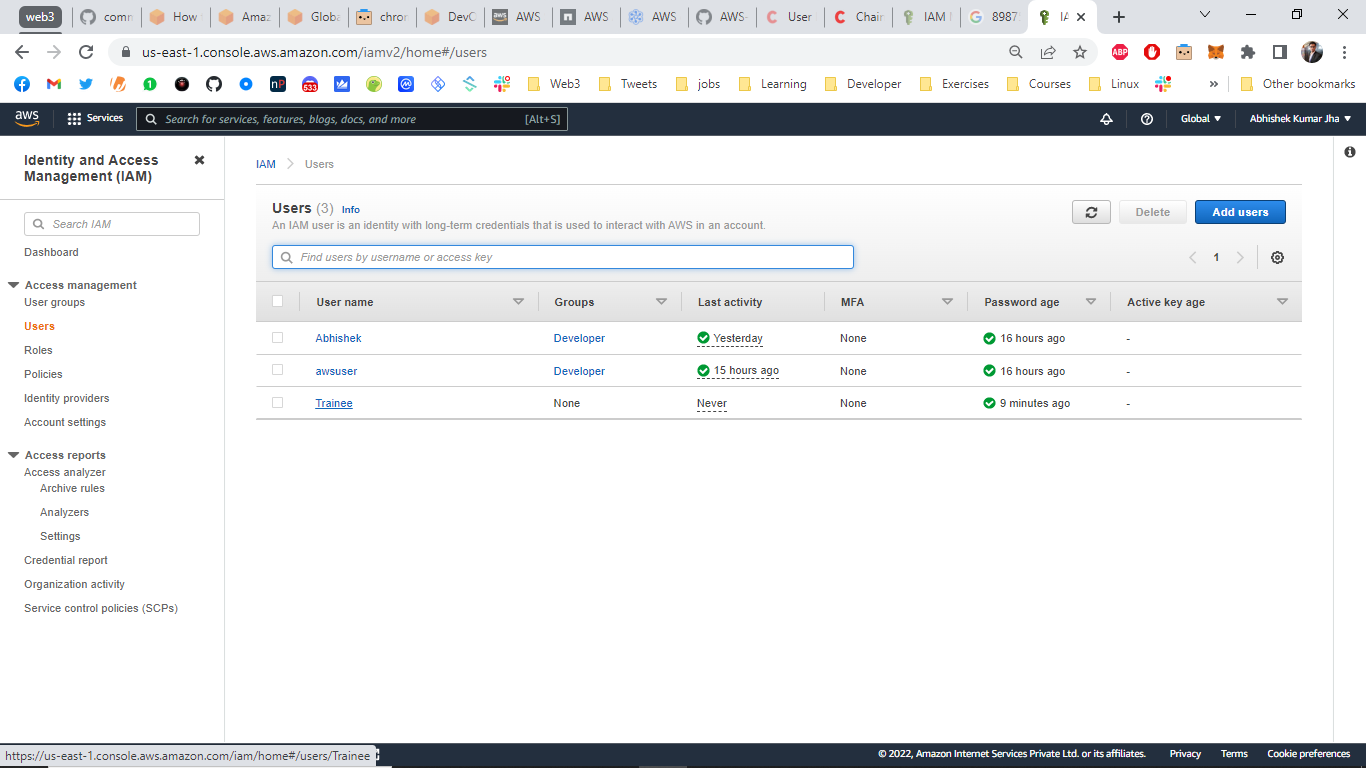
17. How to Reset the password as a user? Hands-On

18. How to remove MFA from an IAM user? Hands-On

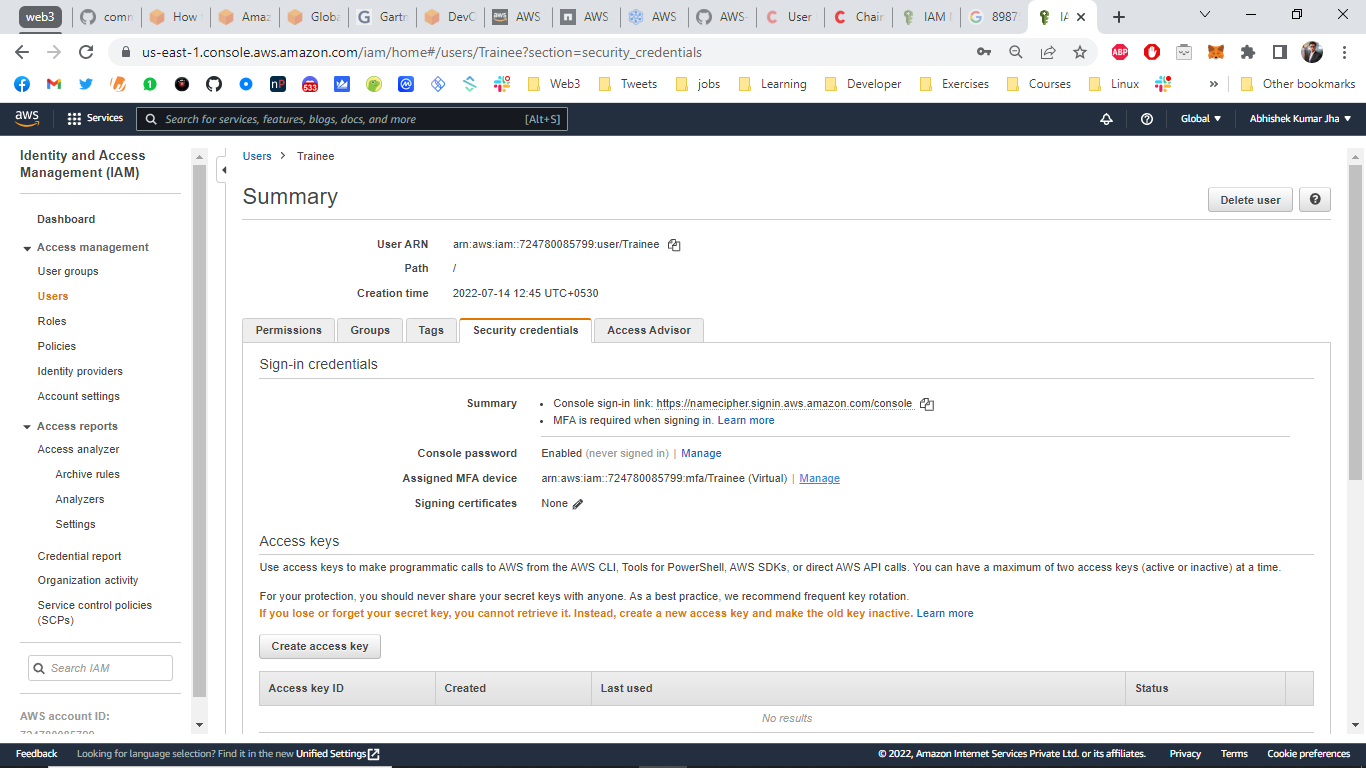
Step1 – Go to Users under IAM Dashboard.



Step2 – Select the user you want to remove MFA for.



Step3 – Click on ‘Security Credentials’ tab and select Manage on Assigned MFA Device option.



Step4 – Select ‘Remove’ and click Remove.