Day4-Assignment-12-July-2022

1.Explain about AWS shared responsibility model.

Security and Compliance is a shared responsibility between AWS and the customer. This shared responsibility model can help relieve the customer’s operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Physical resources are the responsibility of AWS.

The customer’ responsibility is management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS firewall and data encryption as well.

AWS responsibility – Software, Servers, Databases, Data Centres, Availability Zone, Regions, Edge locations.

Customer responsibility – Data, Applications, IAM, Operating System, Network & Firewall, Data encryption, Network traffic.

2. What is IAM service?

IAM stands for Identity and Access Management and it is a web based service in AWS that helps root user securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use the various AWS services and resources.

3. What is an IAM user, IAM role, IAM group and policy?

IAM user is a user who has o permissions by default and is given permission by the root user to access services and resources. To give permission, a policy is attached to the user and the access is given as per the rules defined in the policy.

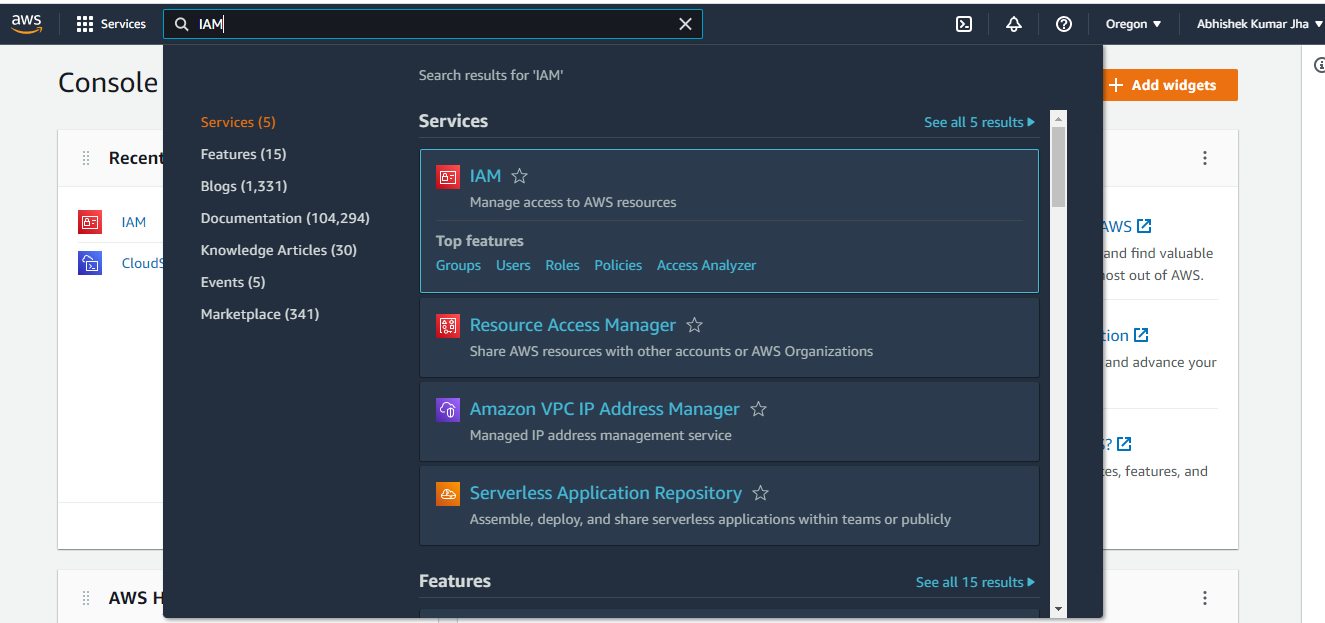
IAM group is a way of organizing users of same category in a group to give similar permissions or access. In a company developers, testers and Administrators have different permissions and so they are grouped as IAM group and a policy is attached to the group. The users in the group will have the permission of policy attached to the group.

Roles – It can be user as well as service access. When a user is given specific role, he will get permission from policy attached to that specific role.

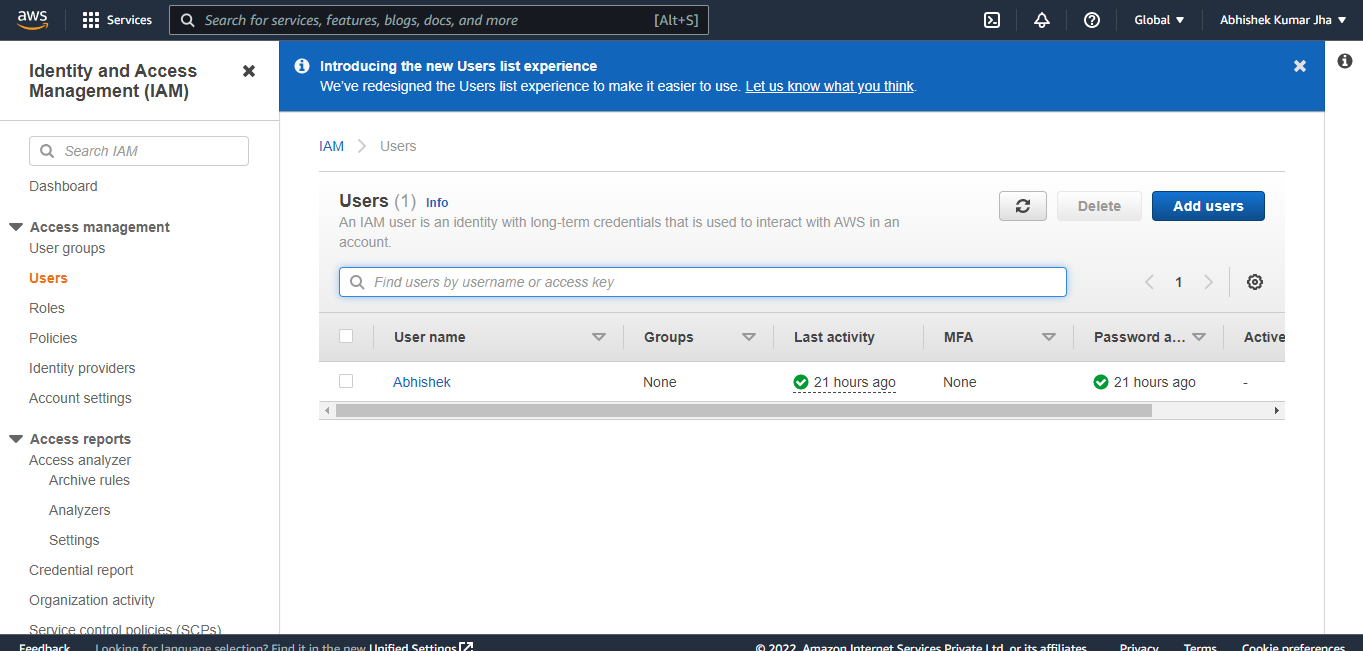
Service access can be possible by attaching role to the service and policy in turn will be attached to the roles.

4. Hands –on – Create an IAM user

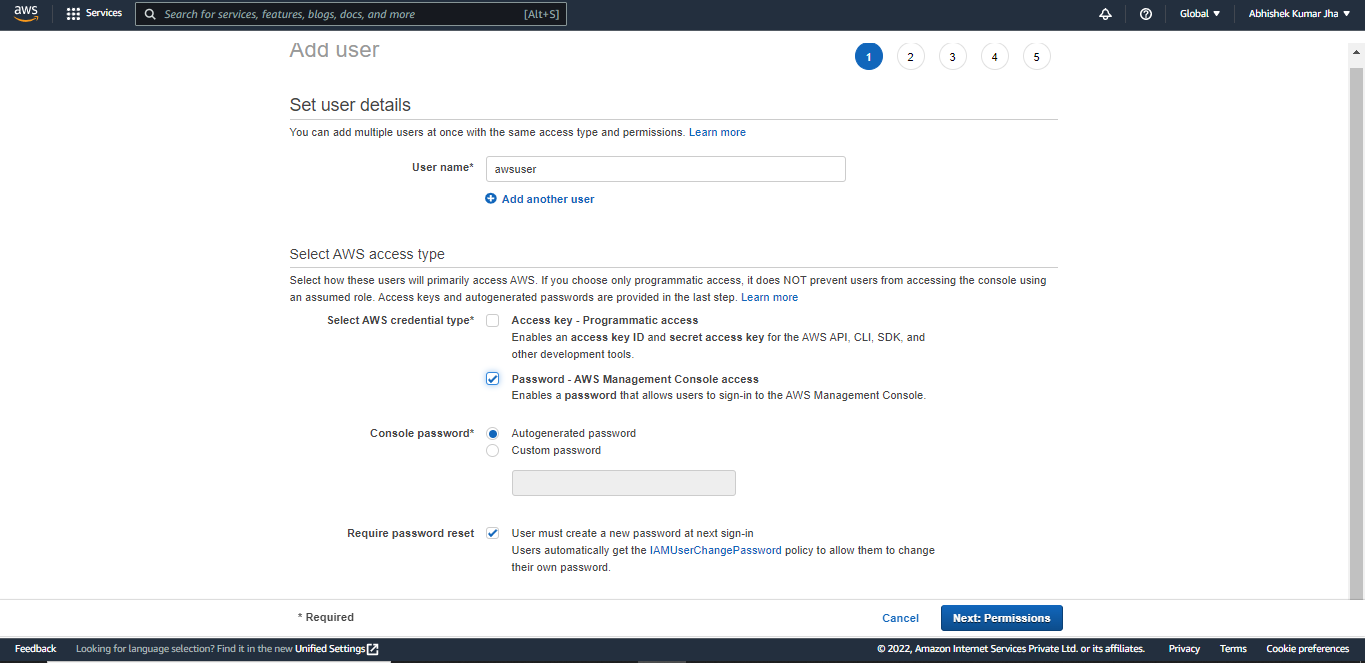
Step1 – Go to AWS management console, search for IAM, click on Users.



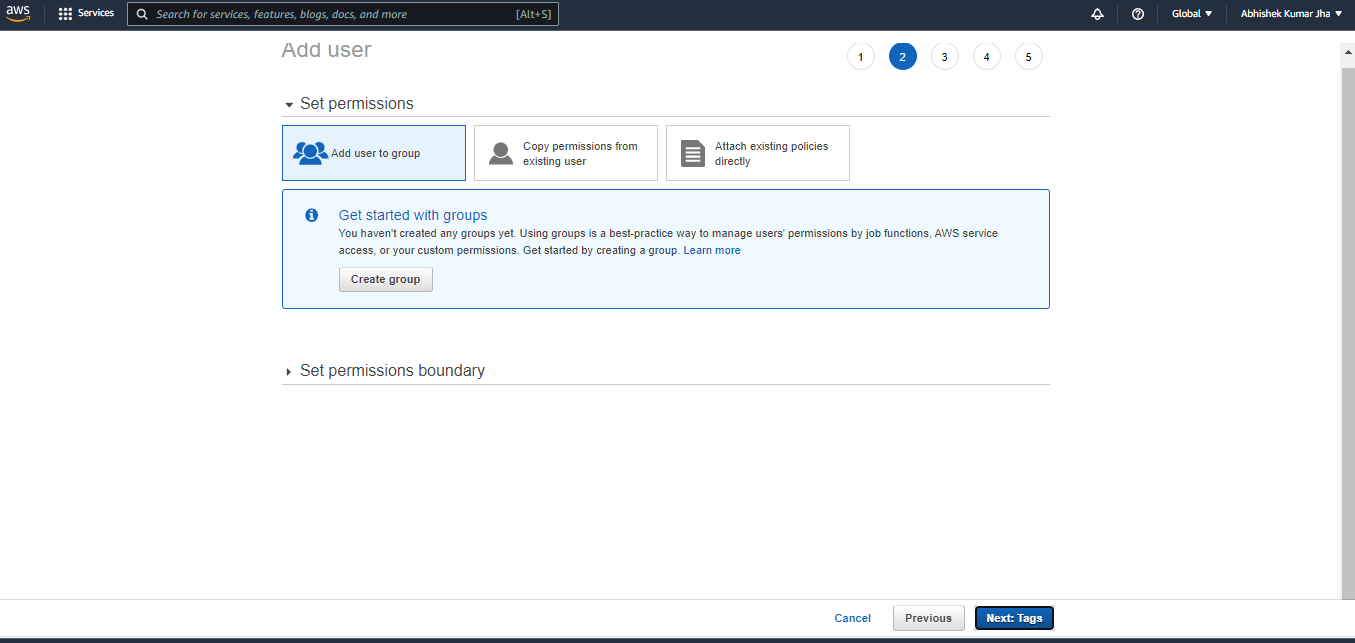
Step2- Click on Add users.



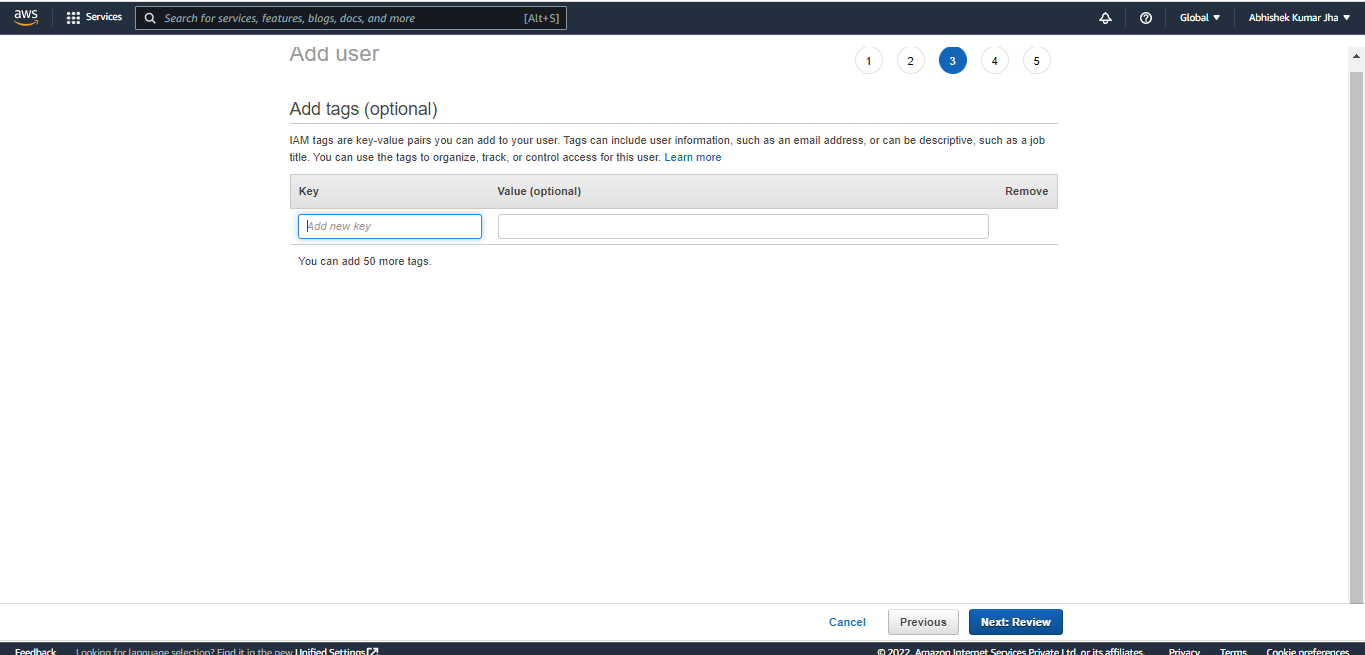
Step3 – Add user name here and choose password. Click Next.



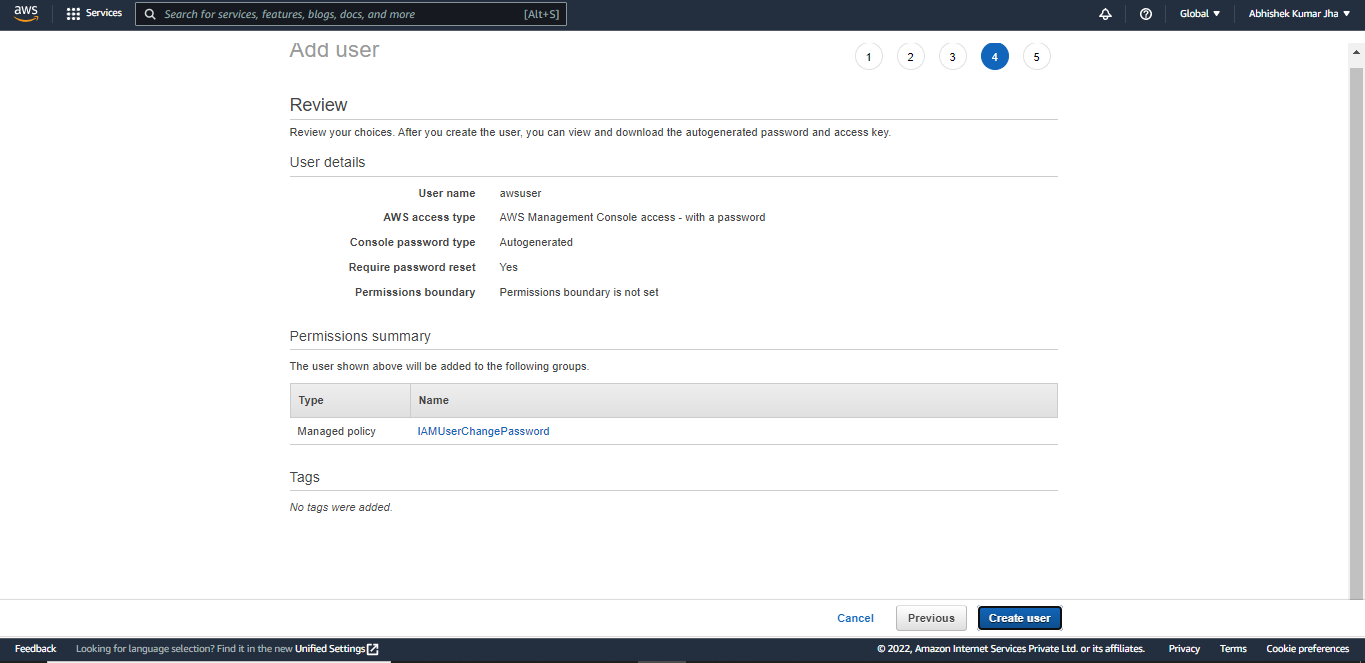
Step4 – Choose permission. Click Next.



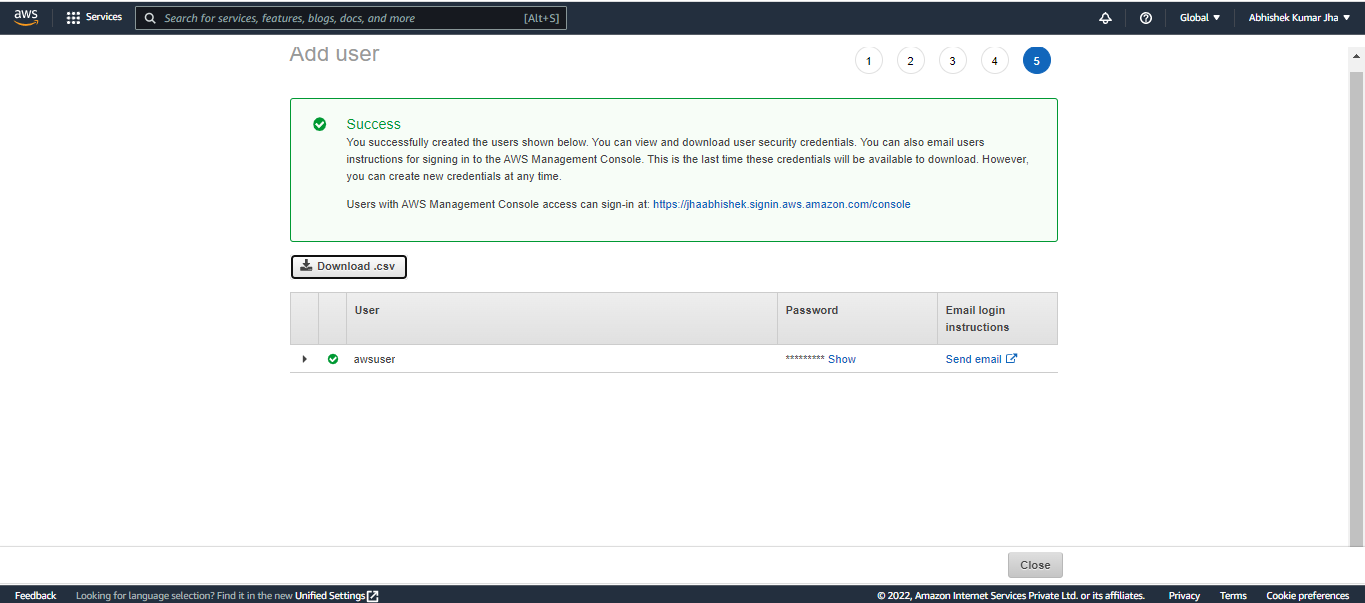
Step5 – Add tags (Optional)



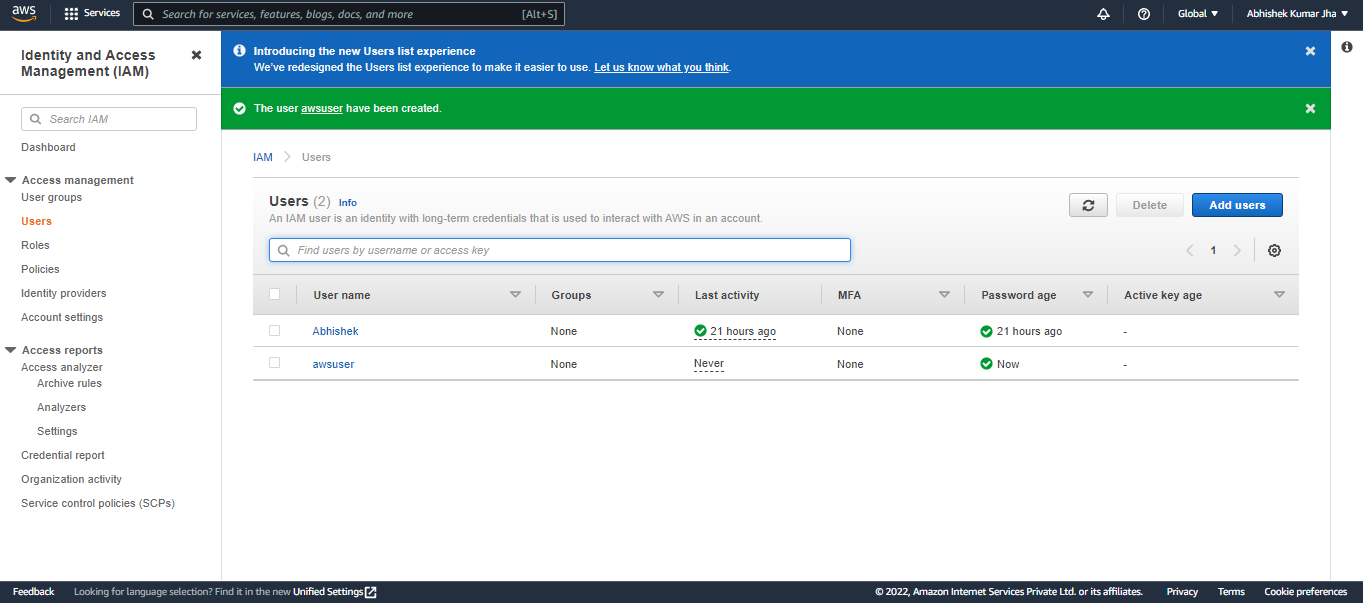
Step6 – Review the User credentials. If all seems correct, Click create user.



Step 7 – Download the csv file with user details.



Step8 - Go to IAM > Users and you’ll see the newly created user.



5. What are the 3 different ways of launching AWS services? Explain

Three different ways of launching AWS service are :

1. Management console – It is a section of the web based AWS dashboard which is used to manage and lunch several AWS services and access resources.
2. CLI – Command Line Interface is also a way to access AWS services where user has to pass various commands through the AWS CLI. For this user has to learn and remember commands and pass different commands for performing different actions.

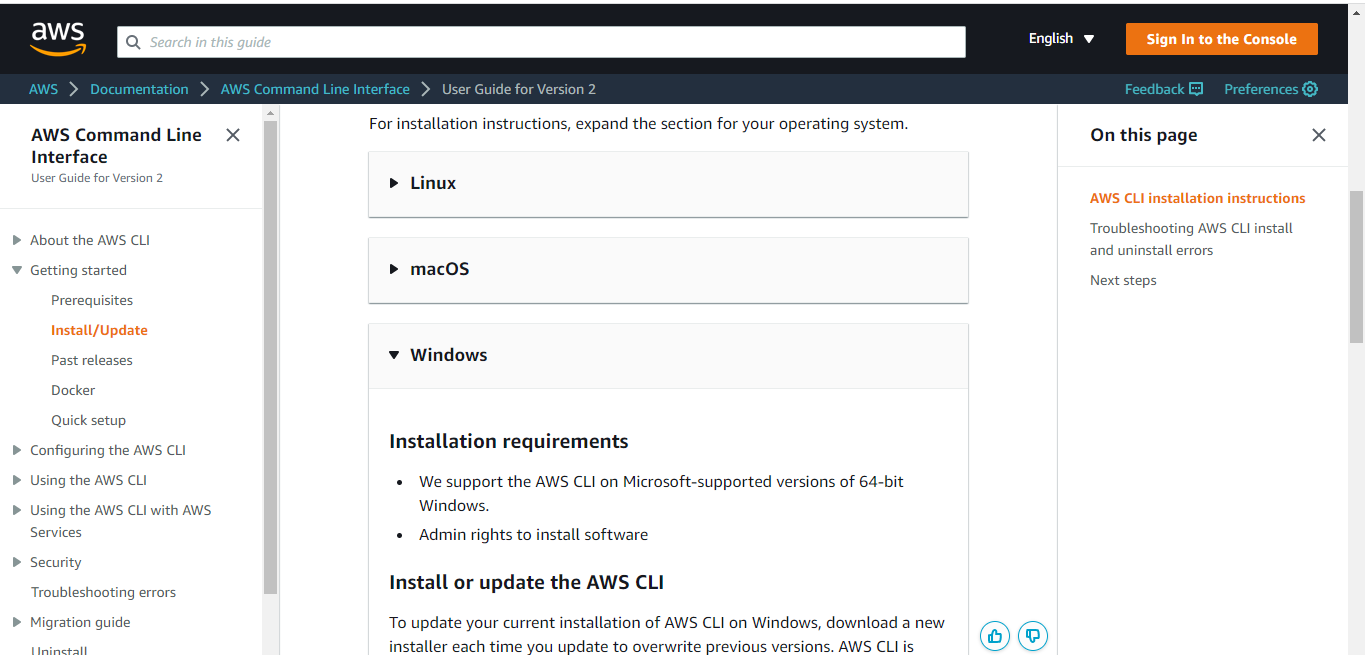
Due to firewall restrictions, some CLI commands will not work and so in this case we use AWS CloudShell.

1. API – Application programming interface is a way of accessing AWS services. Separate API is created for several AWS services by AWS and the client gives input to the API and API will connect to particular AWS service and give response back to client.

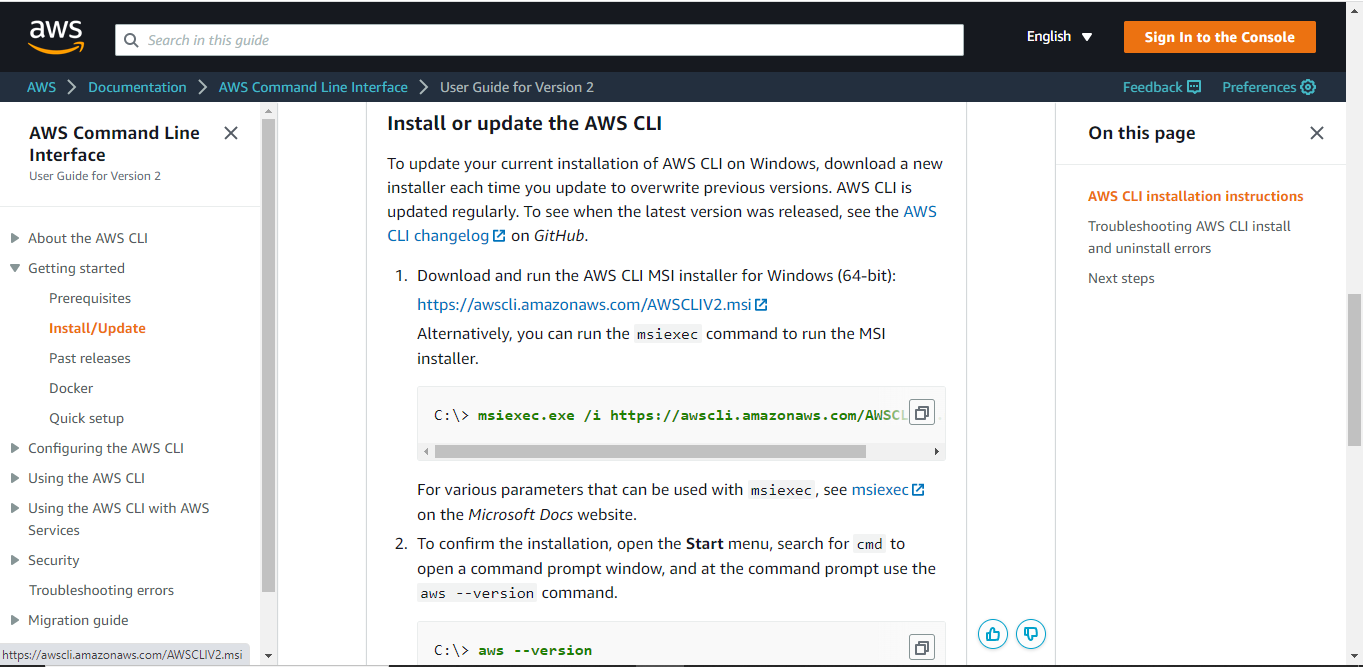
6. Hands on – Cli

Step1 - Search for AWS CLI install or go to this Link - <https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

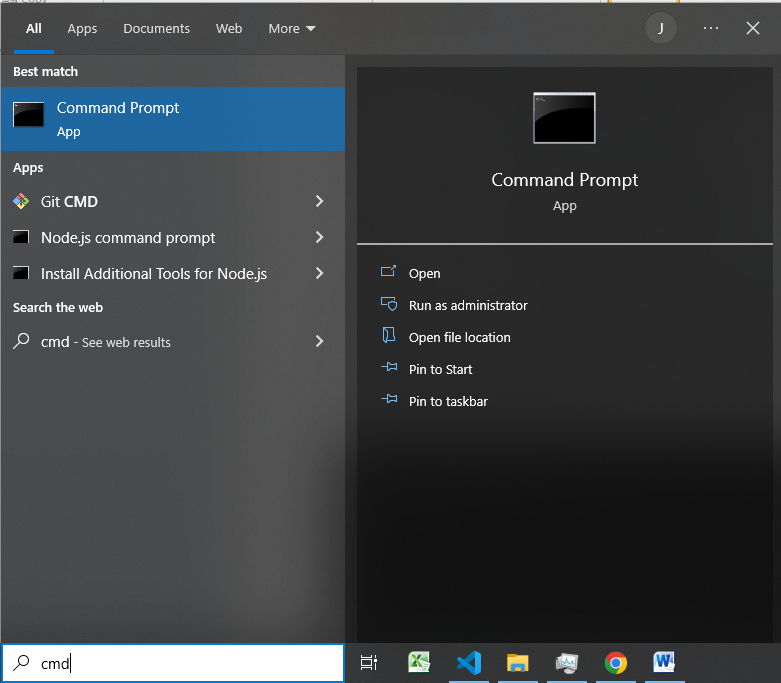
Step 2 – Click on windows tab (As per your OS)



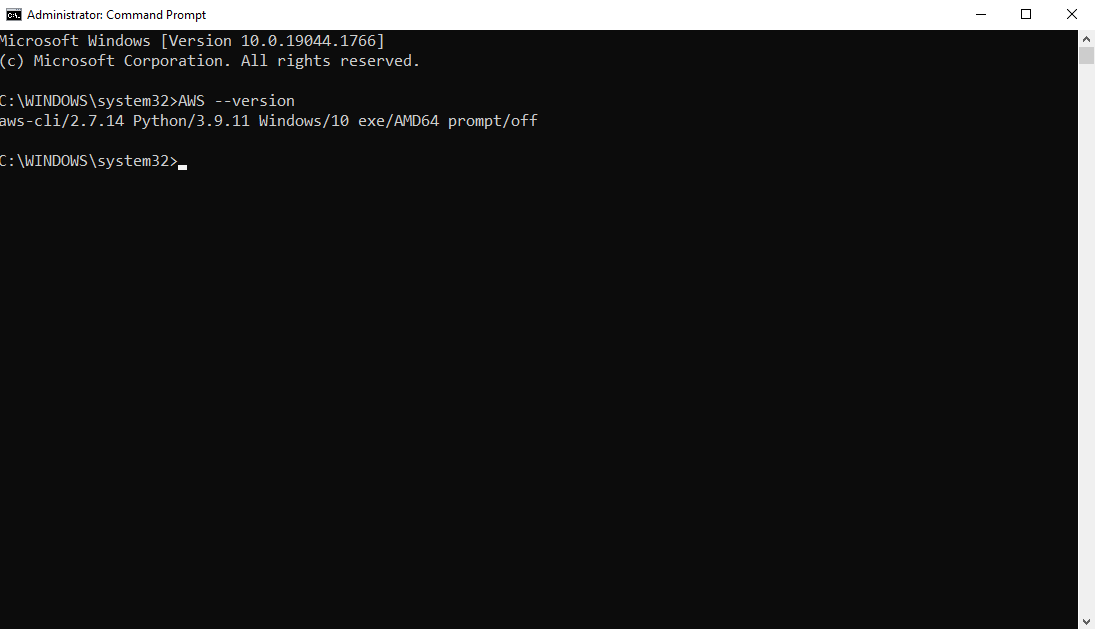
Step3 – Click on the link and download the CLI.



Step4 – Install the CLI. Search and open CMD As Administrator.



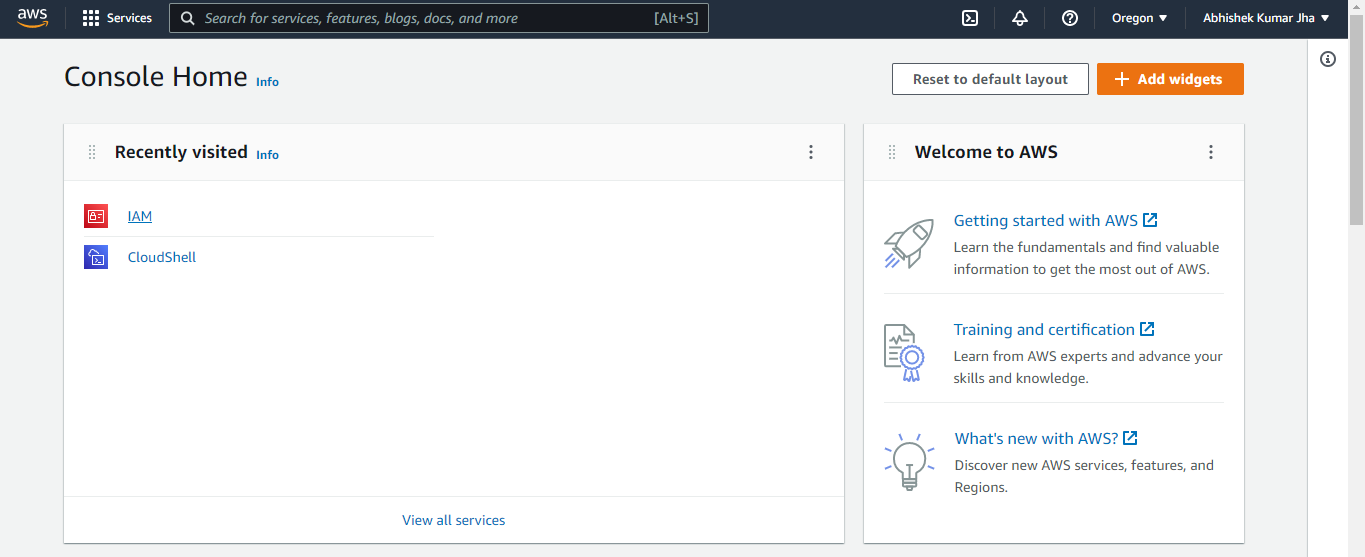
Step5 – Type the command “AWS –version” to check if AWS CLI has been installed correctly or not.



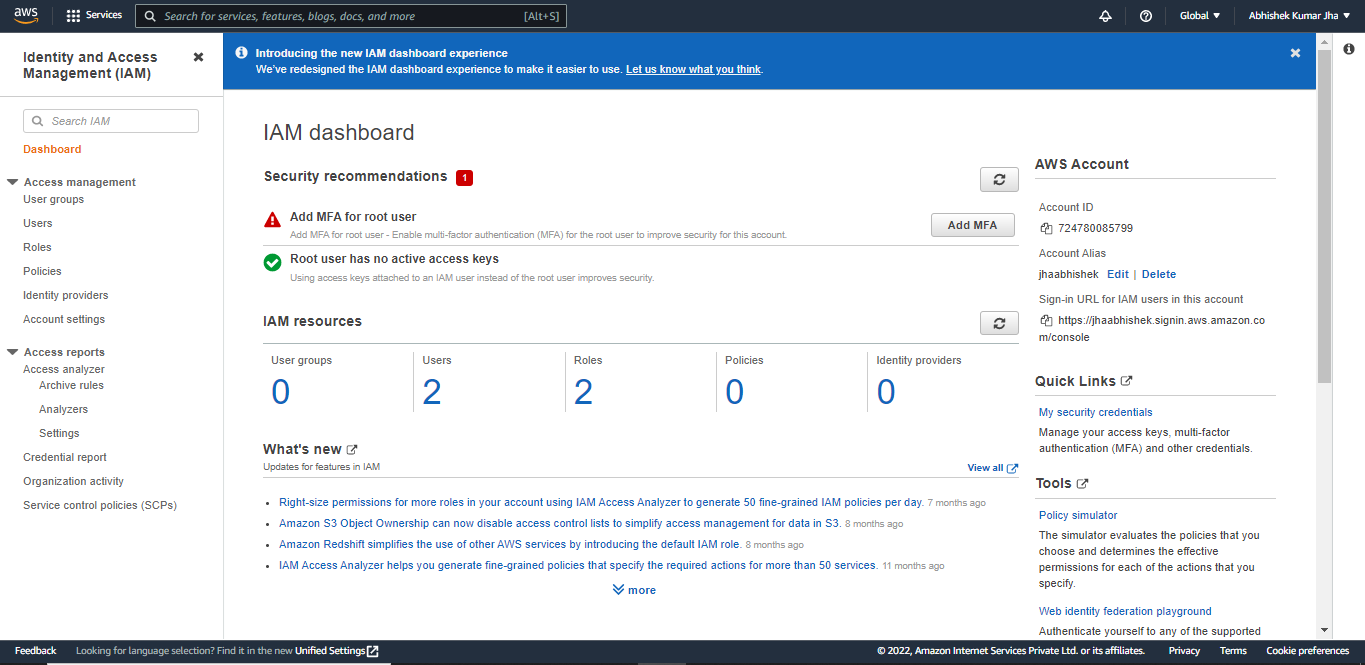
There you go.

7. How to give Account Alias – Hands –On

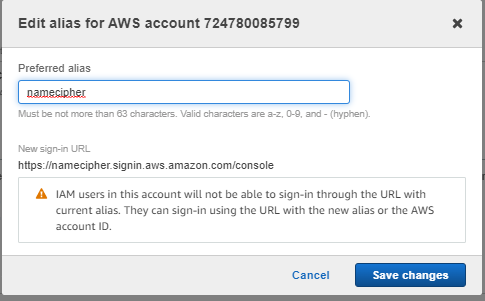
Step1 – Go to IAM Dashboard by clicking on IAM on Recebtly visited under Account Management console.



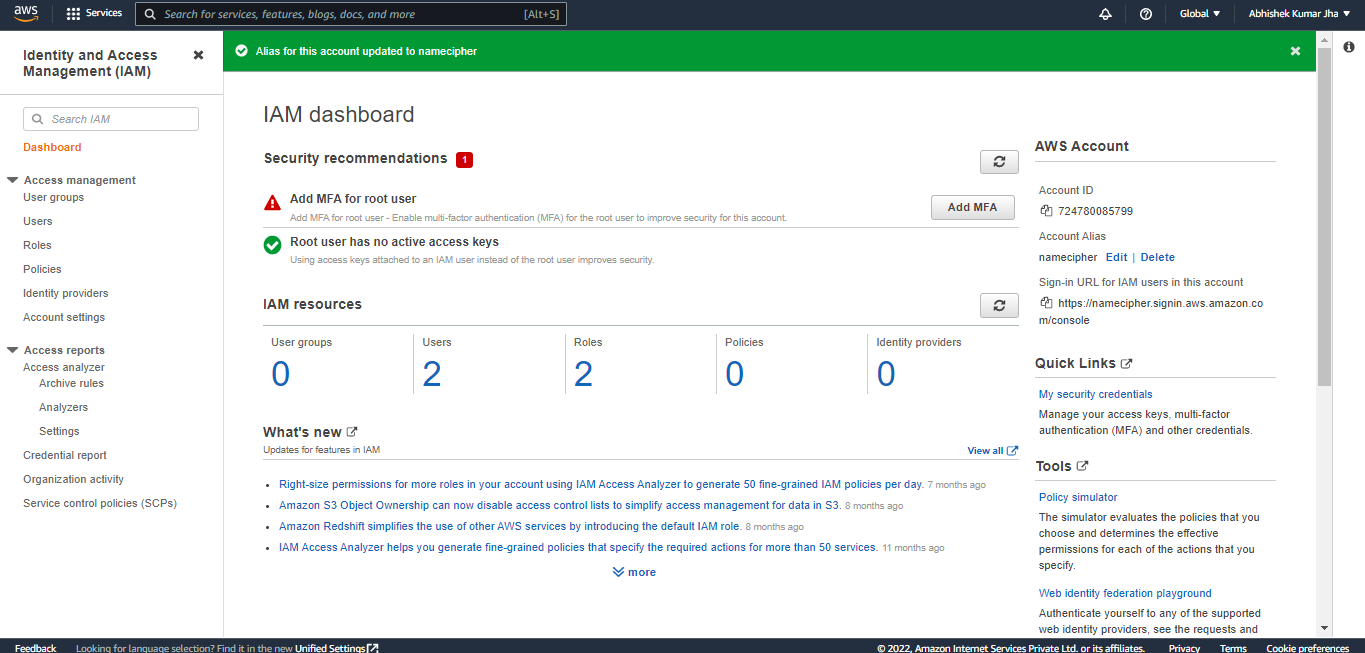
Step2 – Click on edit under AWS Account on the right hand side.



Step3 – Edit the Alias by supplying a new Alias and click on Save changes.



Step4 – Go to IAM dashboard again and you’ll see the new Alias being updated.



That’s it.

8. How to change the Account Name – Hands on