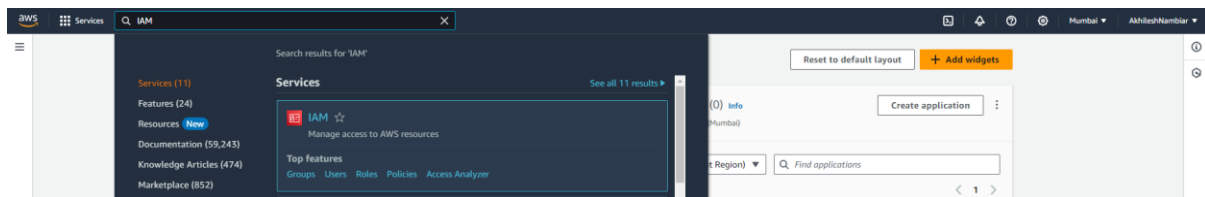


Name: Aditi Kothawade
Roll No: A074

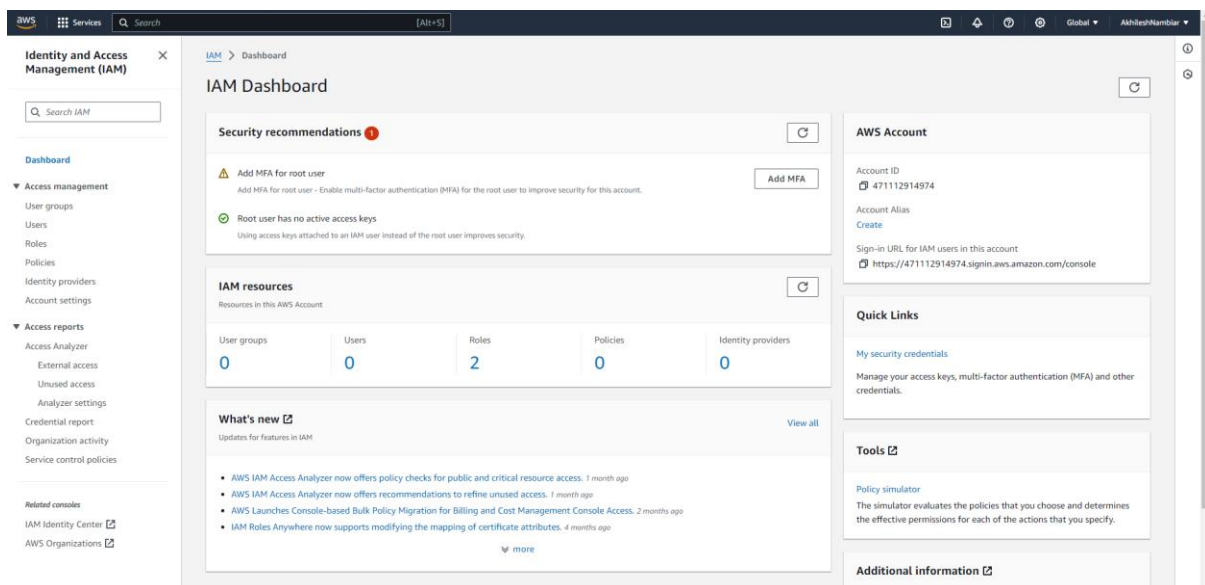
Practical 3 Identity Access Management (IAM)

Step1: Log in to your AWS account and log in.

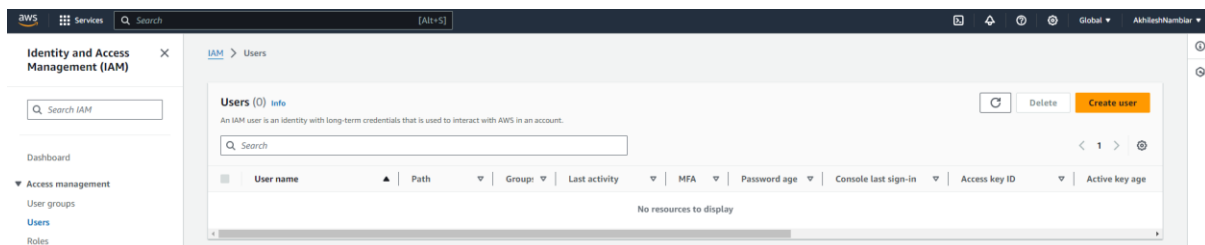
Step2: On the search bar search IAM.



Step3: Click on IAM.



Step4: Click on user on the left window pane.



Step5: Click on create user option.

Specify user details

User details

User name
ashish

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + - . _ @ - (hyphen)

☐ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice [to](#) manage their access in IAM Identity Center.

☒ 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](#)

Cancel Next

Step6: Give a name to your user and do not select the provide user access to the AWS Management Console,then click on next.

Set permissions

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](#)

Permissions options

☒ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

Set permissions boundary - optional

Cancel Previous Next

Step7: Select Add user to group option and click on next.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name ashish	Console password type None	Require password reset No
---------------------	-------------------------------	------------------------------

Permissions summary

Name	Type	Used as
No resources		

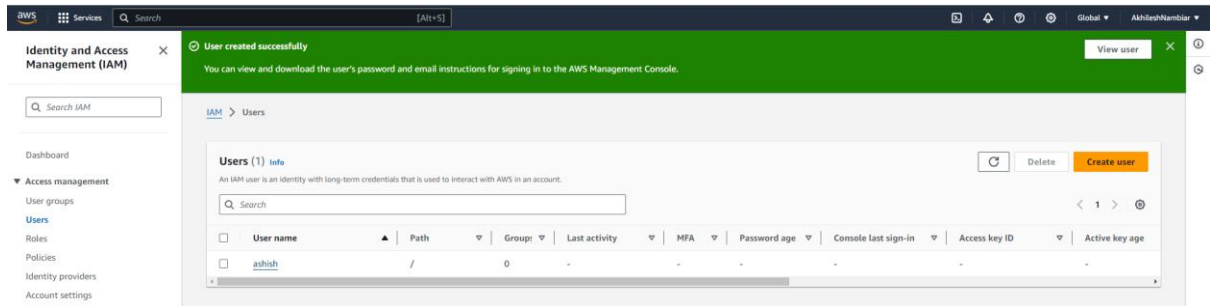
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

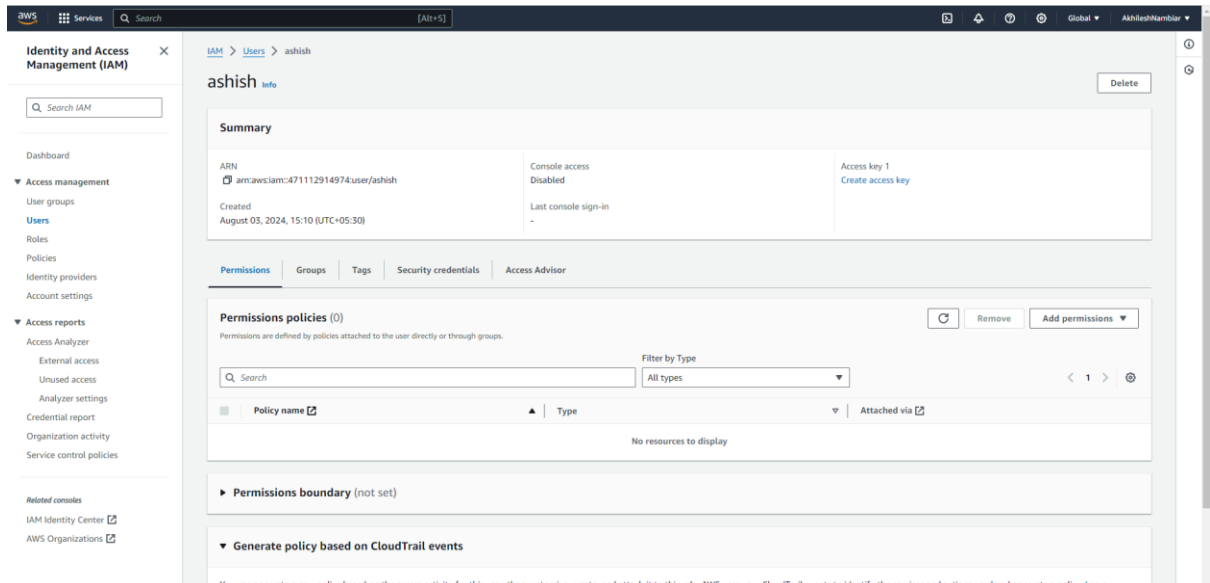
Add new tag
You can add up to 50 more tags.

Cancel Previous Create user

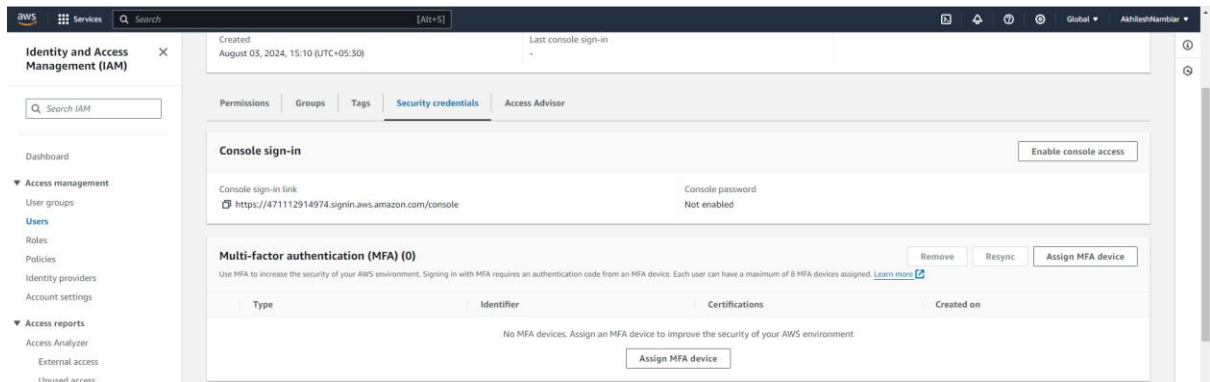
Step8: Click on create user.

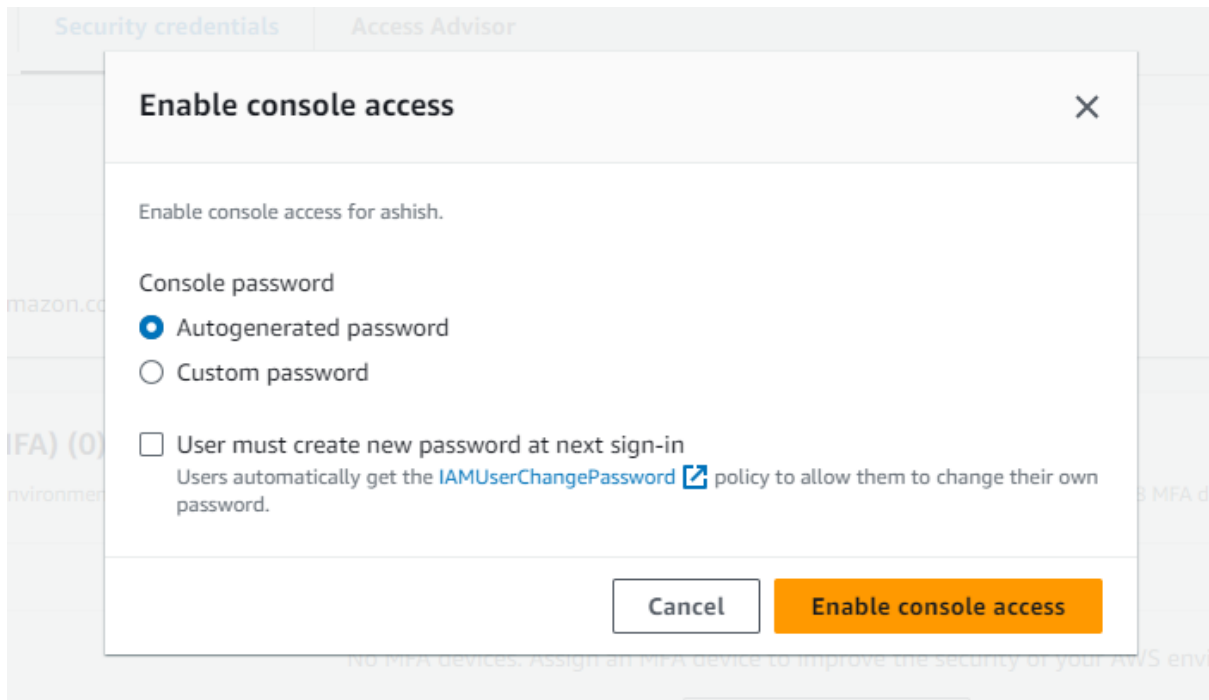


Step9: On the user name click on ashish with a underline in blue colour.

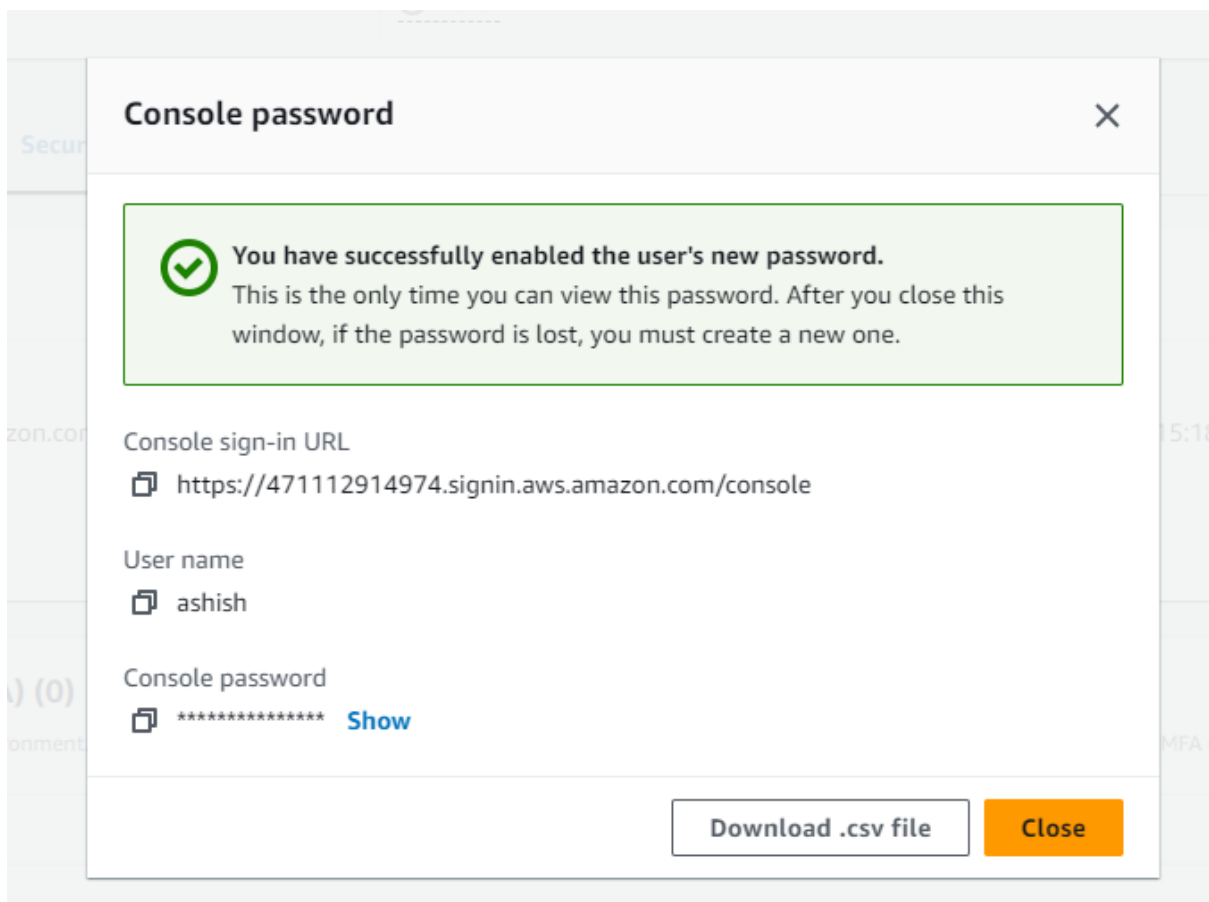


Step10: Click on Security Credentials and click on Enable Console Access.





Step11: Click on autogenerated pass and click on Enable console access.




Step12: Download.csv file.

Step13: Go to incognito mode and then search AWS and click on AWS services and login with the user name and password created in Step11

Try the new sign in UI

See our new improved Amazon Web Services sign in experience before we officially launch.

Enable new sign in



Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

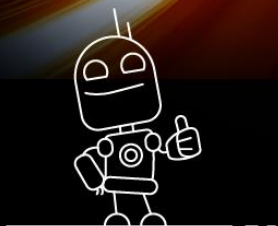
Password

☐ Remember this account

[Sign in](#)

[Sign in using root user email](#)

[Forgot password?](#)



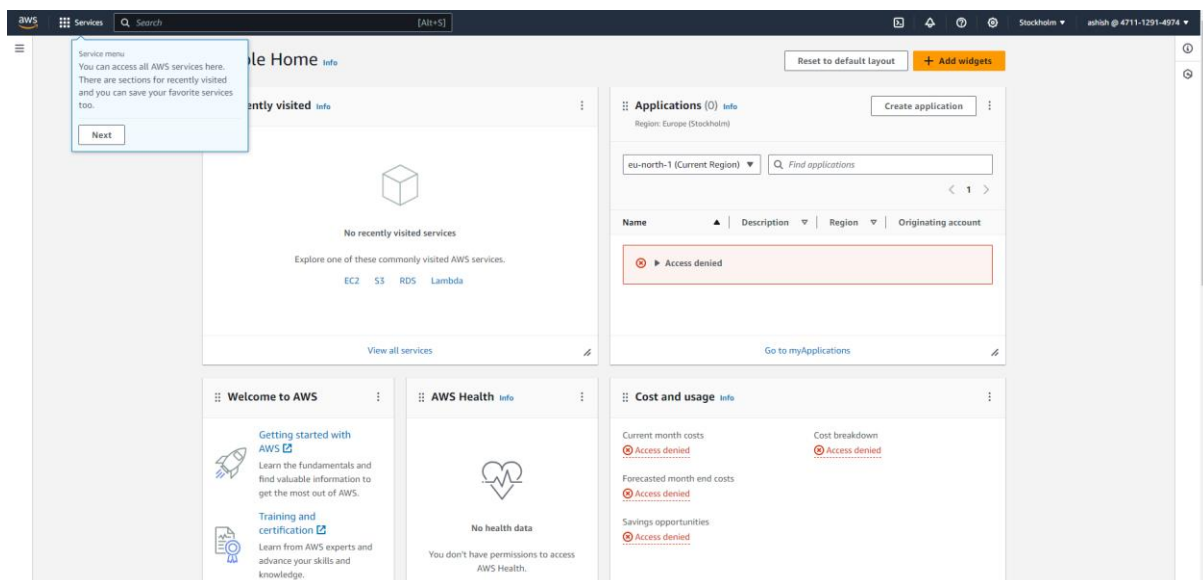
Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)

English

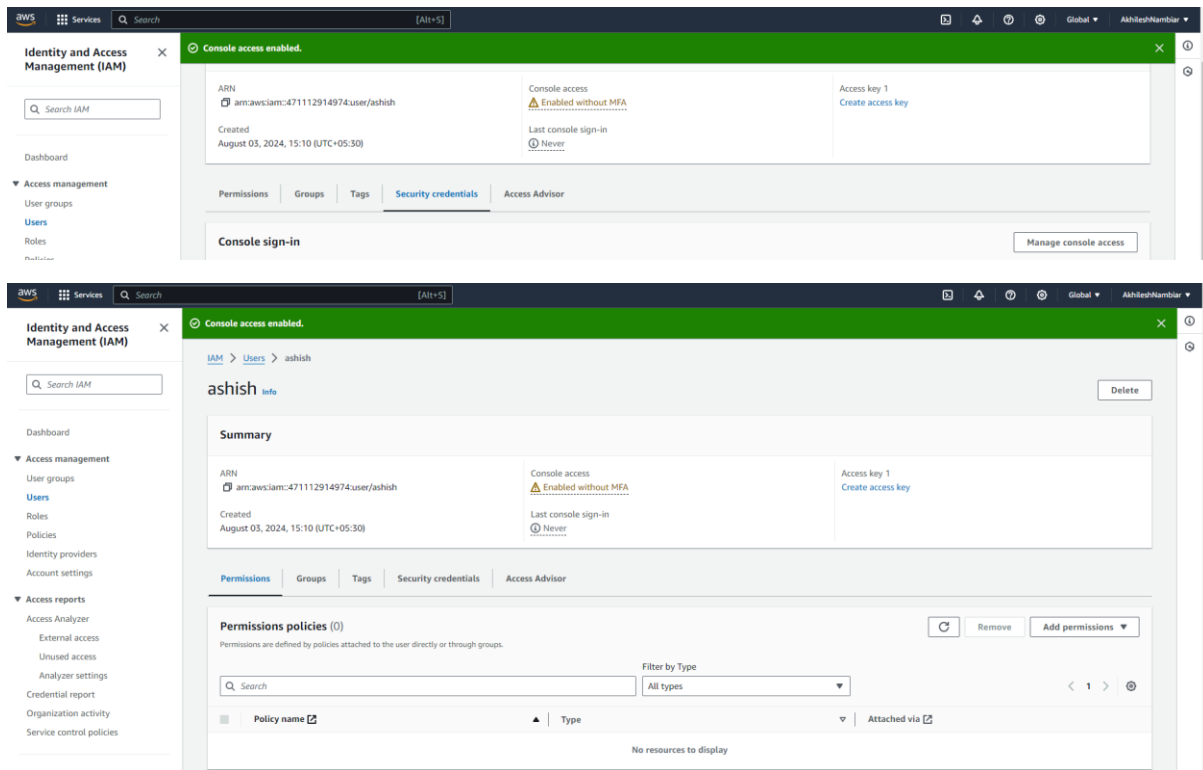
[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.



The screenshot shows the AWS Management Console home page. The top navigation bar includes the AWS logo, a search bar, and the user's name 'ashish' with their account ID '4711-1291-4974'. The main content area is divided into several sections:

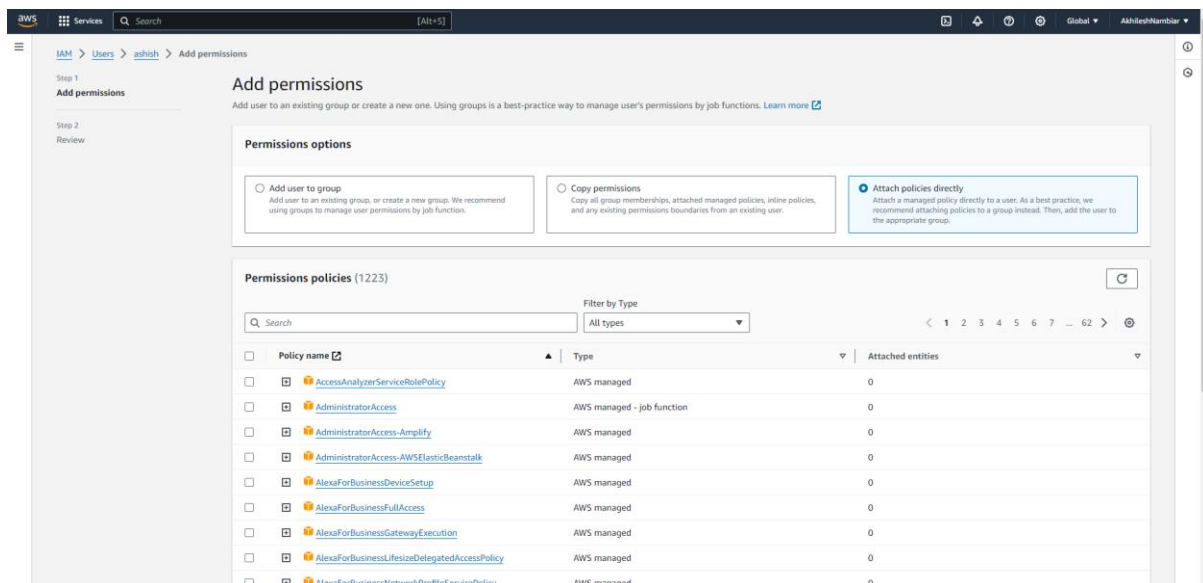
- Recently visited:** A section showing no recently visited services, with links to EC2, S3, RDS, and Lambda.
- Applications (0):** A section showing no applications, with a 'Create application' button and a 'Go to myApplications' link.
- Welcome to AWS:** A section with links to 'Getting started with AWS' and 'Training and certification'.
- AWS Health:** A section showing 'No health data' and a message 'You don't have permissions to access AWS Health'.
- Cost and usage:** A section showing 'Current month costs', 'Forecasted month end costs', and 'Savings opportunities', all with 'Access denied' messages.

Step14: Click on Permission to give access to S3 and EC2.

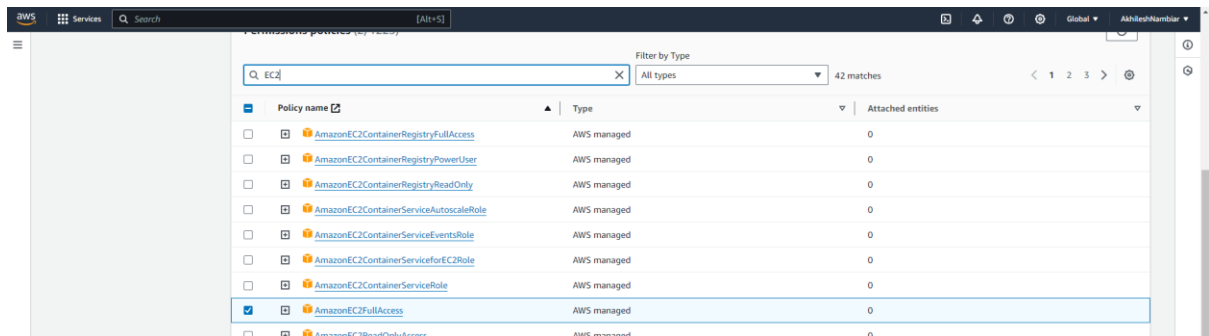
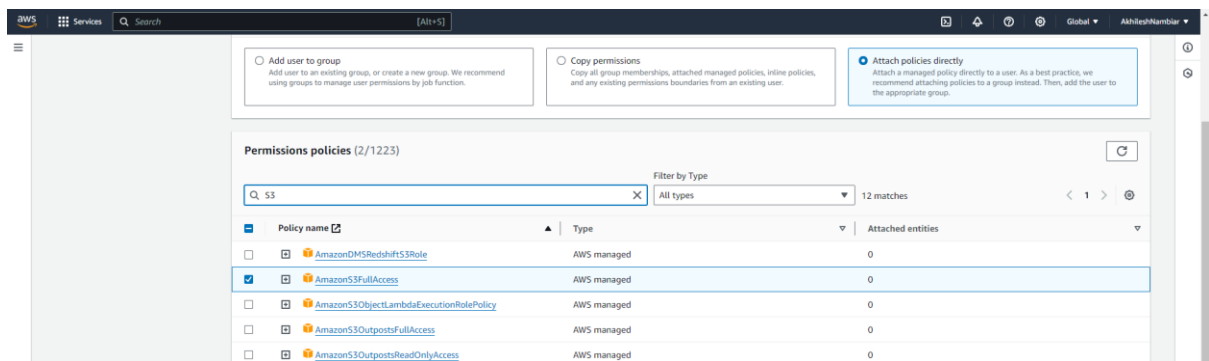


Step15: Click on Add Permissions and then select Add permissions.

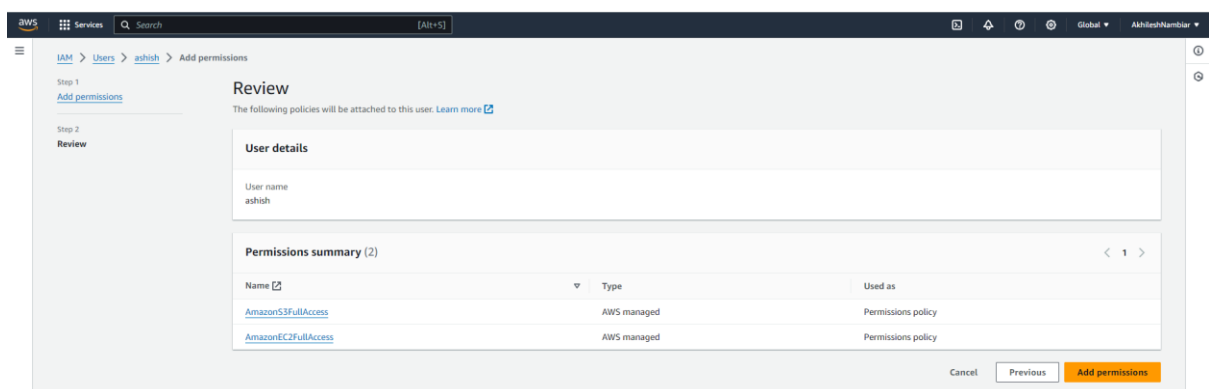
Step16: Click on Attach Policies Directly.



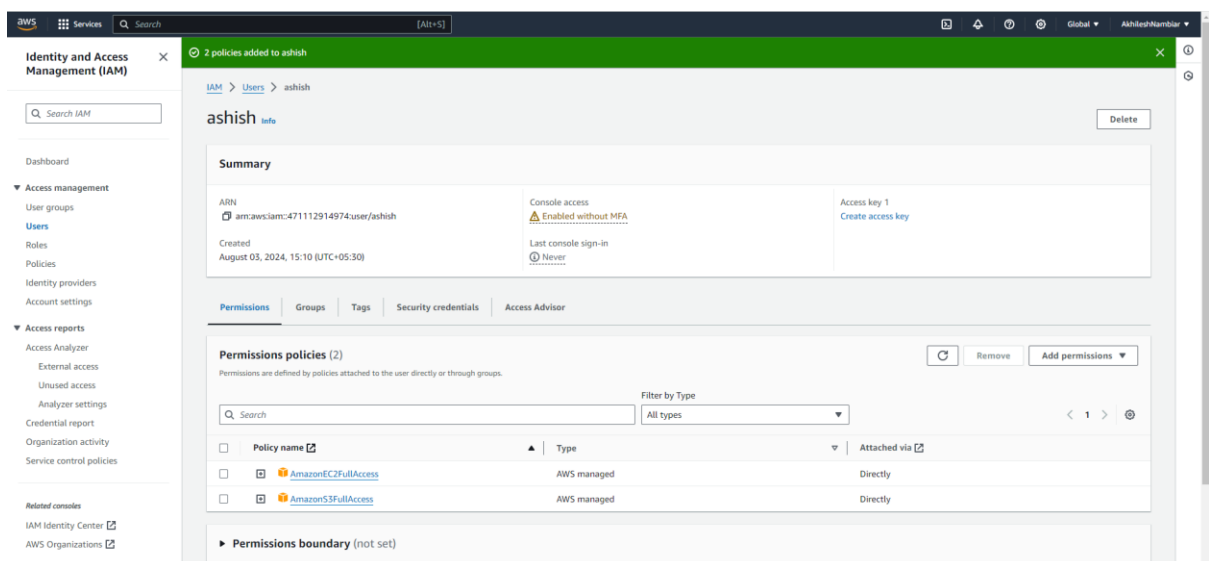
Step17: Search S3 and then select S3 give full access.



Step18: Click on next.



Step19: Click on Add Permissions.



Step20: Now go on incognitive mode and then login into aws using the ashish user name and password you have created then you can see that ashish will have full access to S3 and EC2.