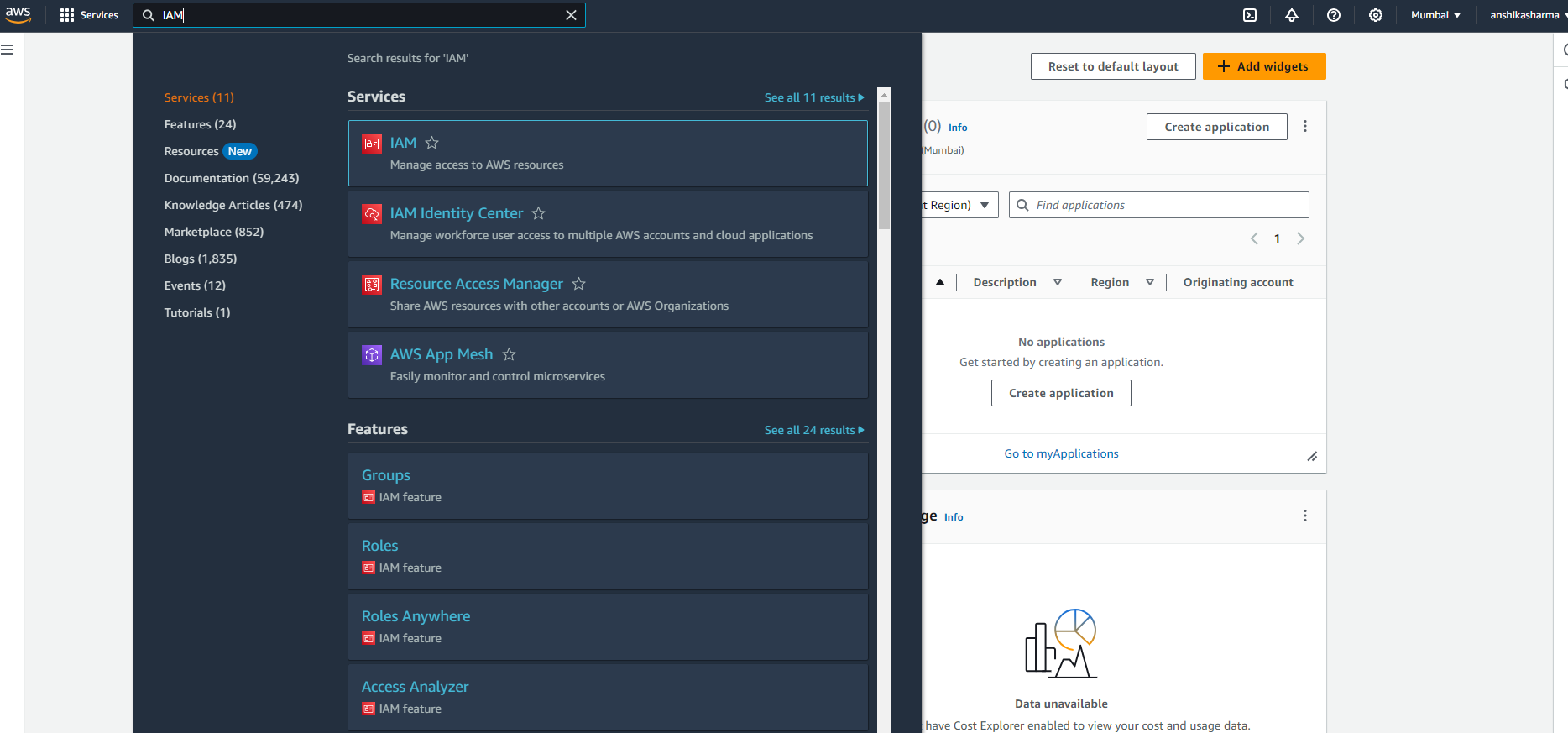
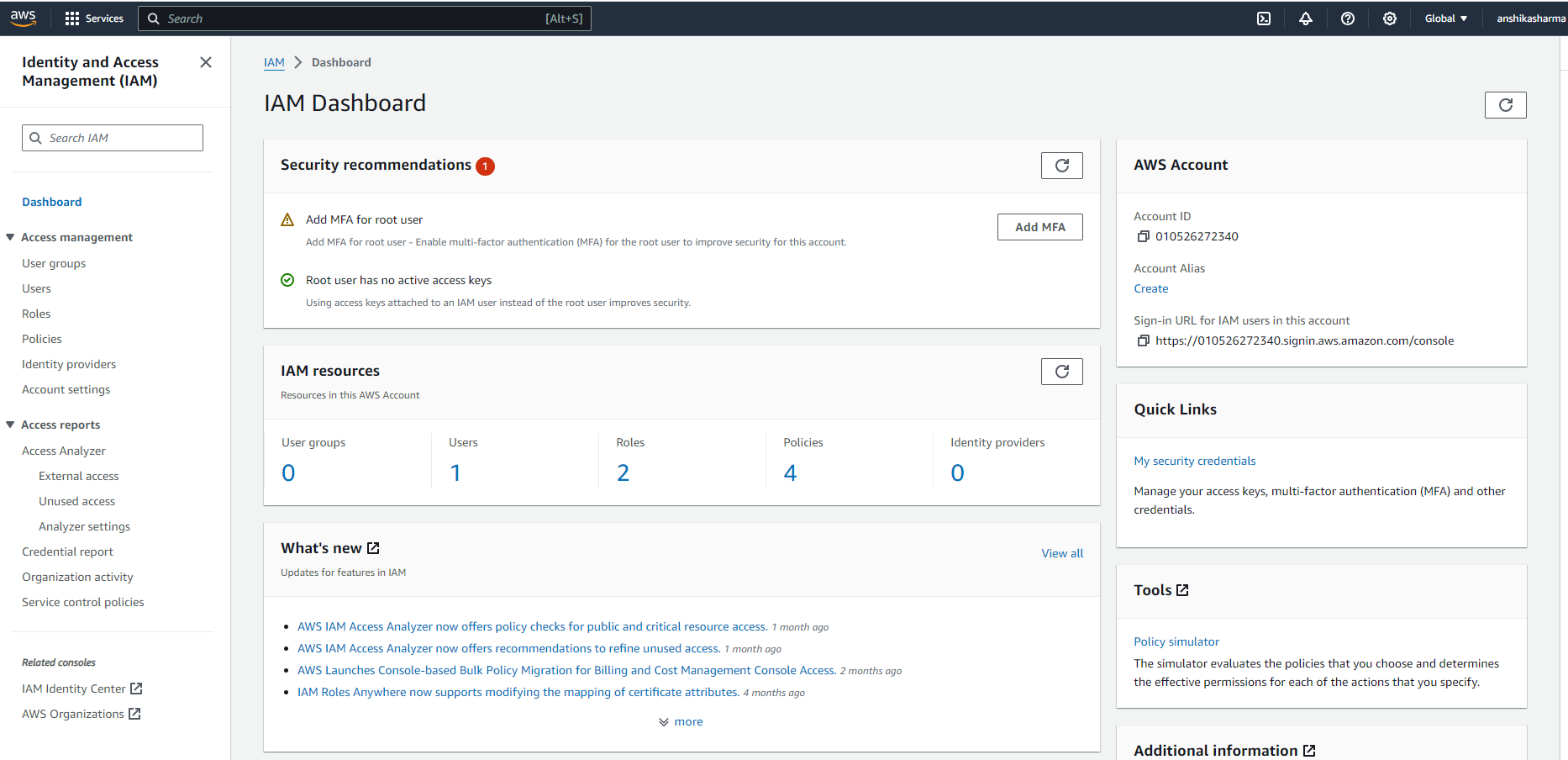
**Practical-3 Identity Access Management**

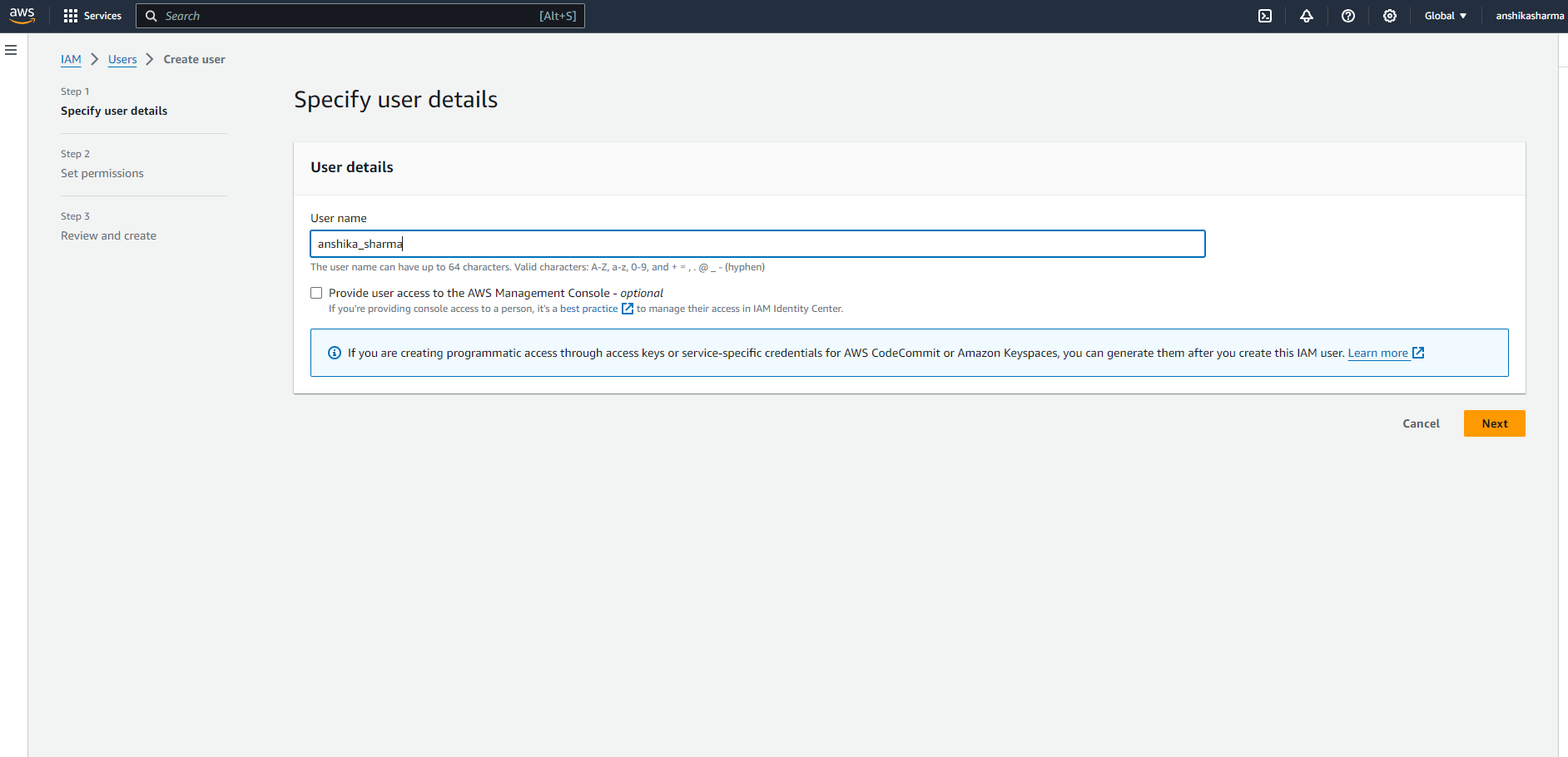
Name: Anshika Sharma

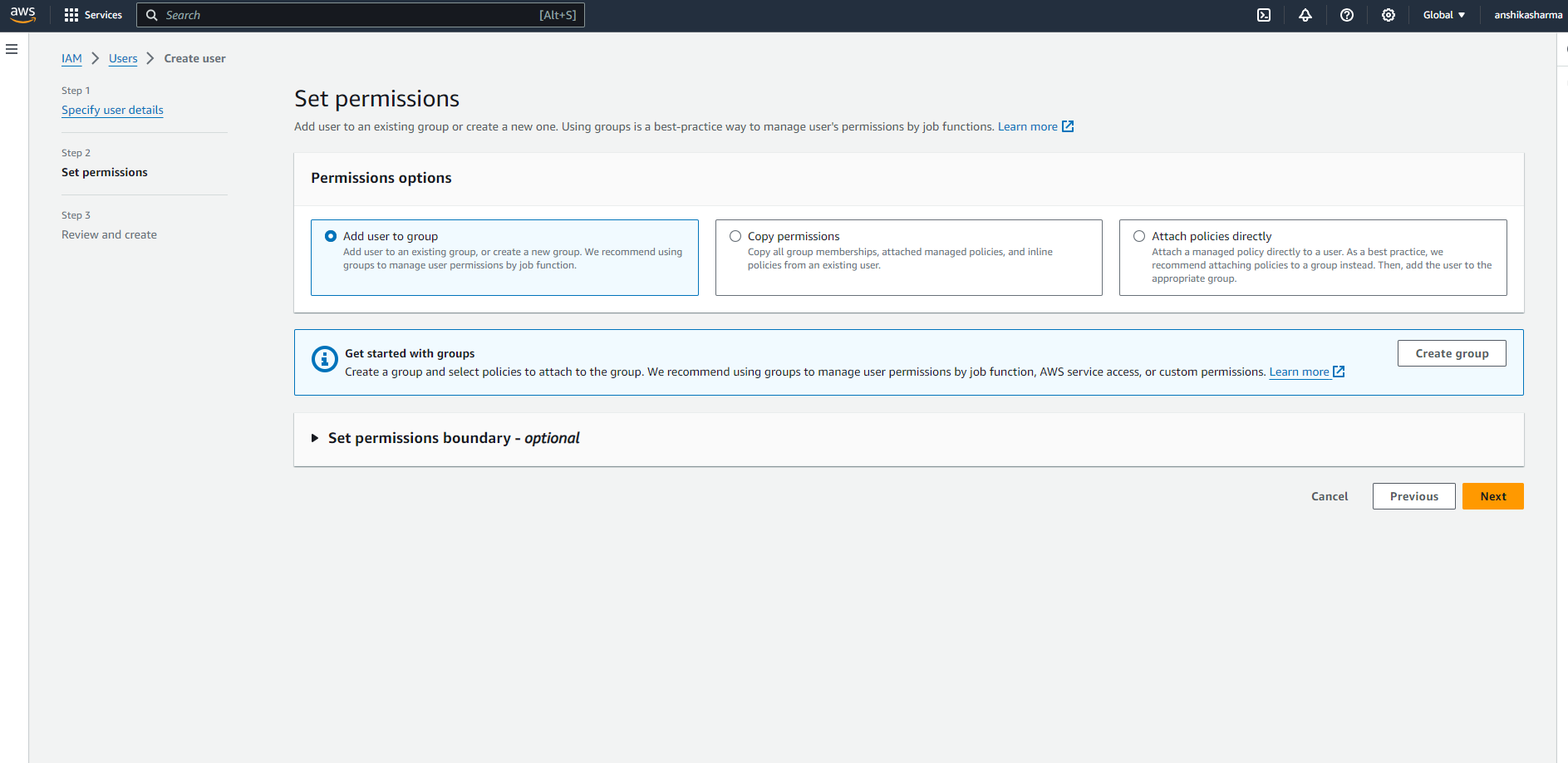
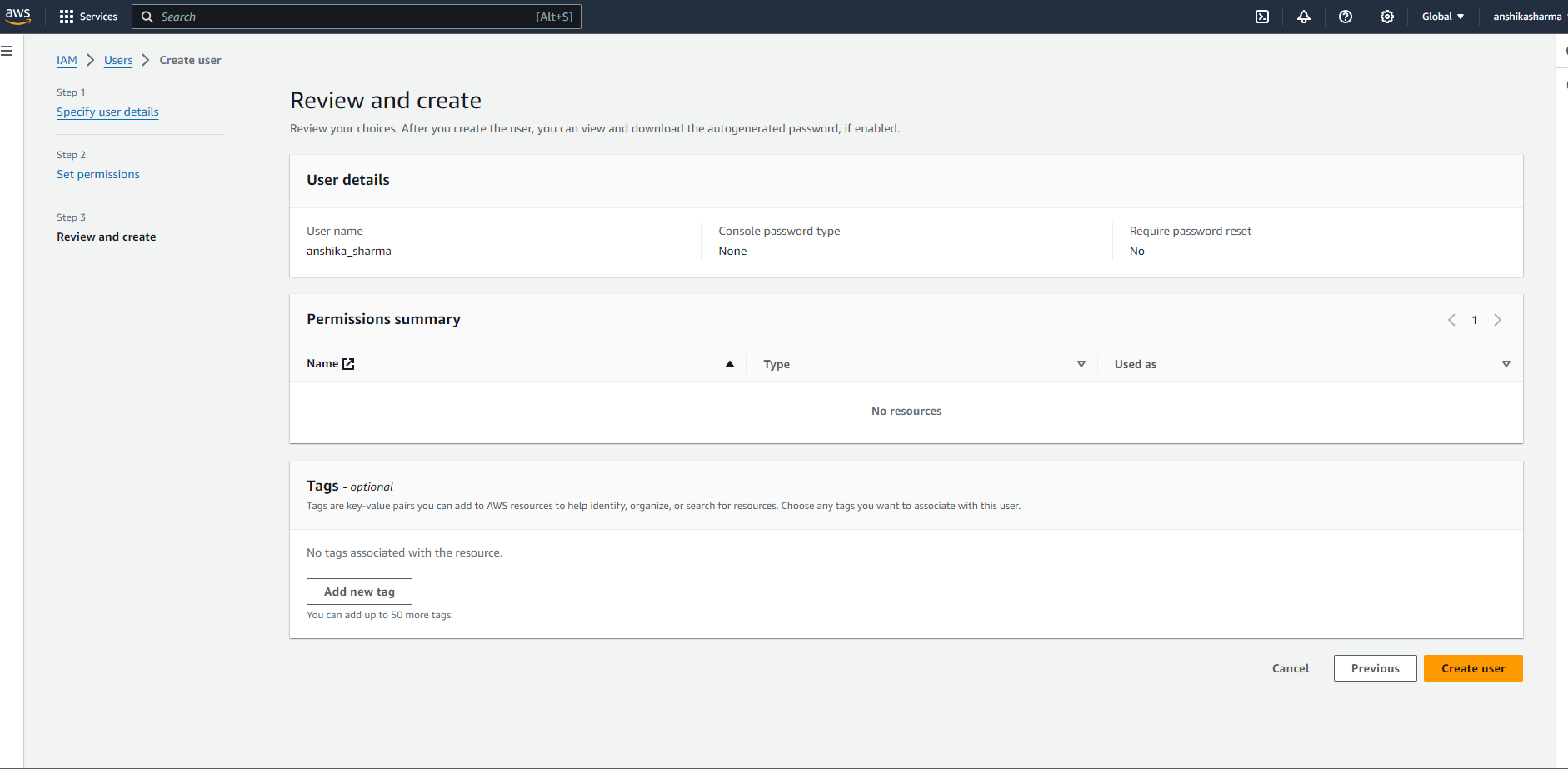
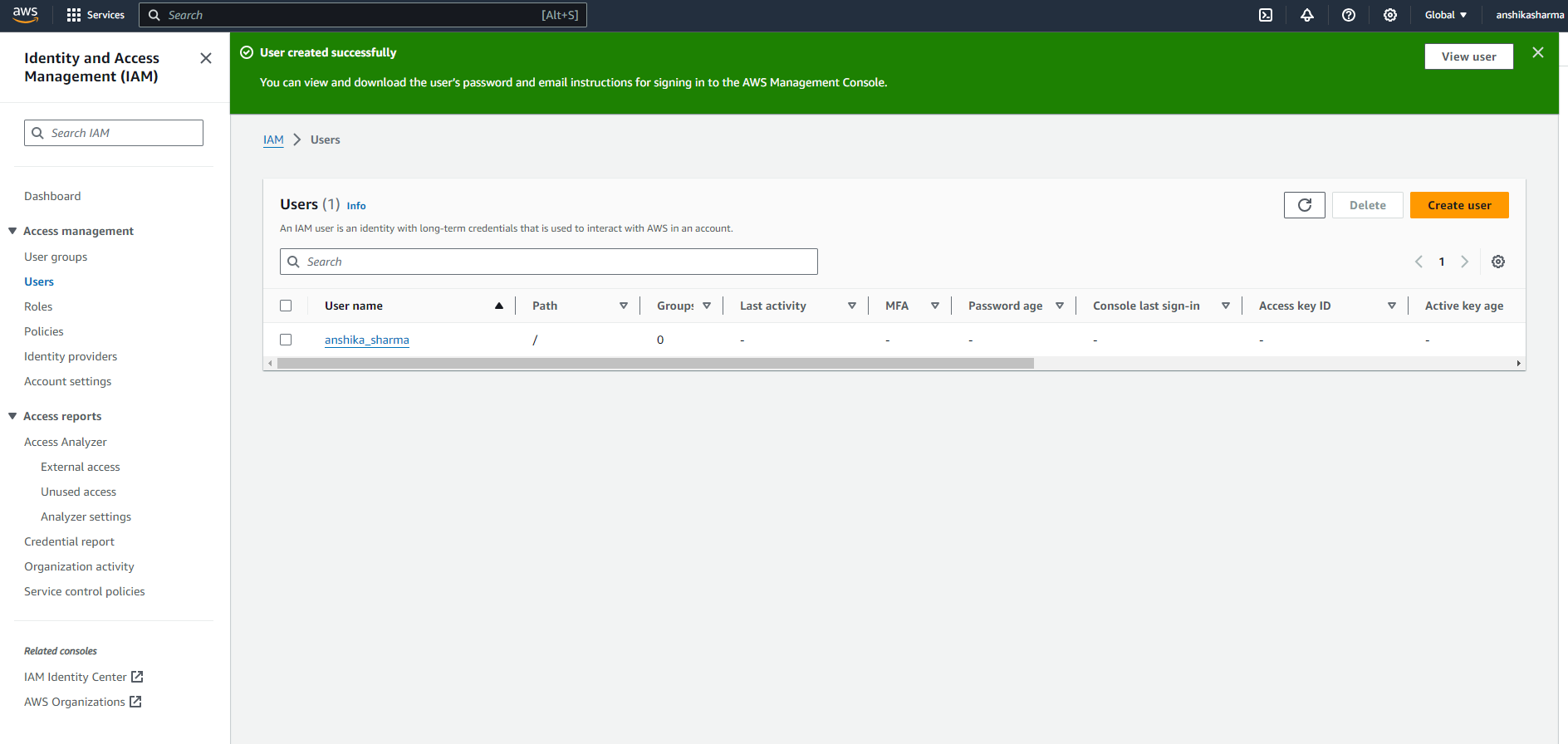
SAP ID: 86062300034

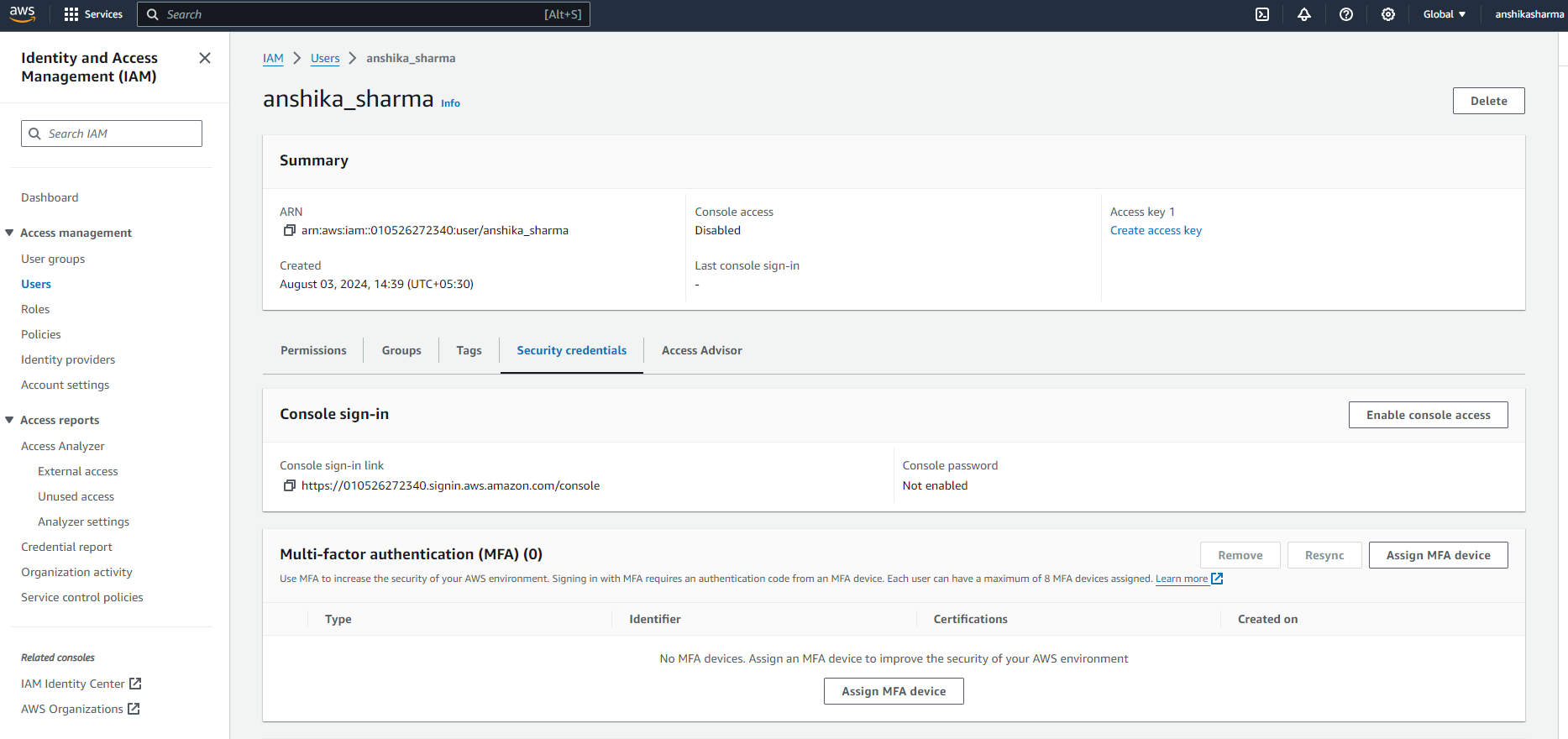
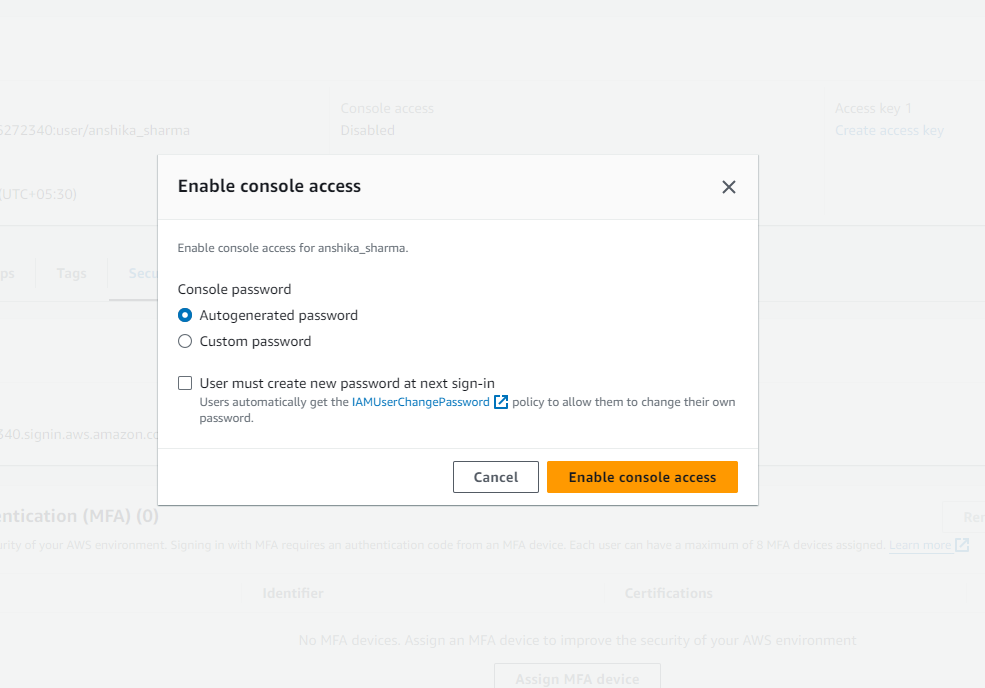
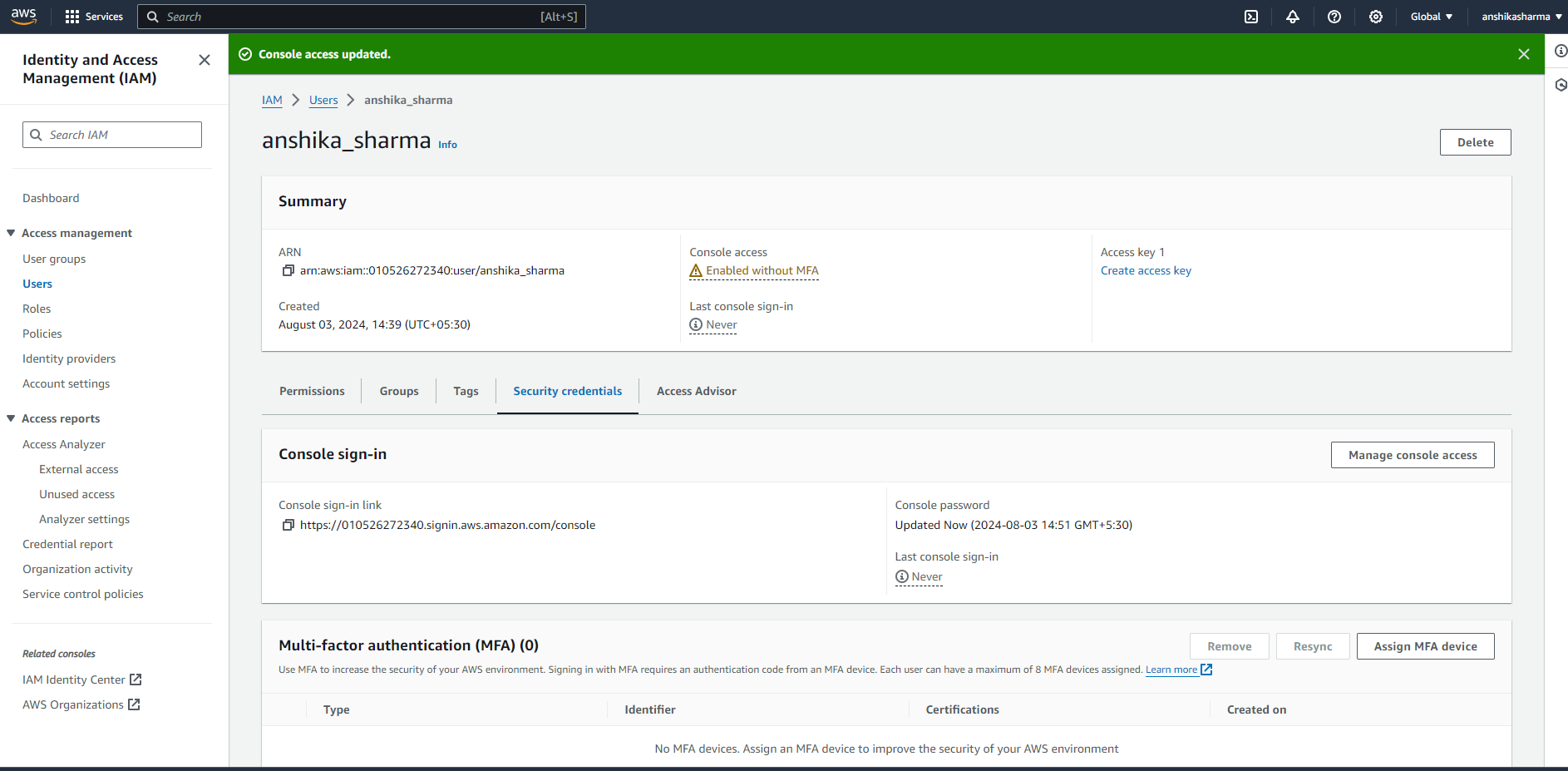
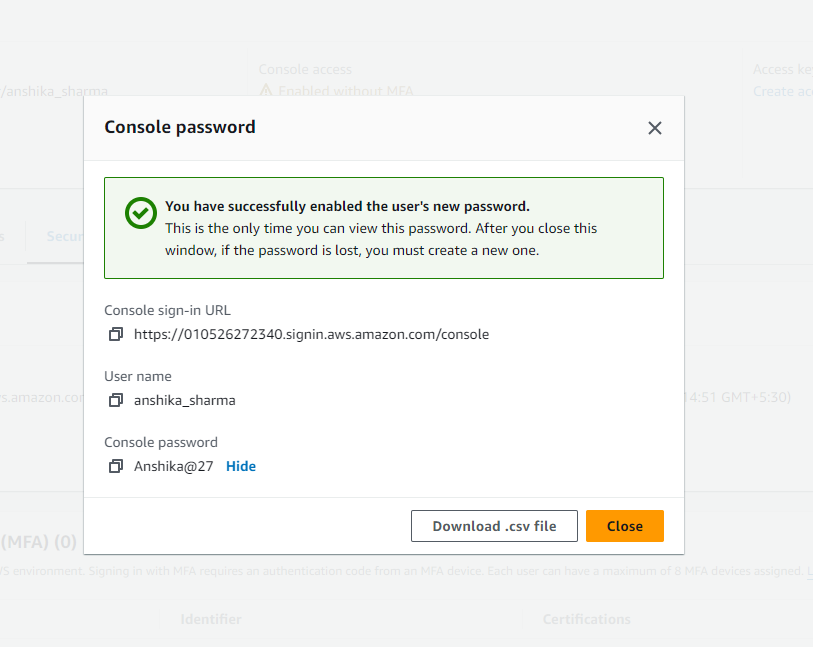
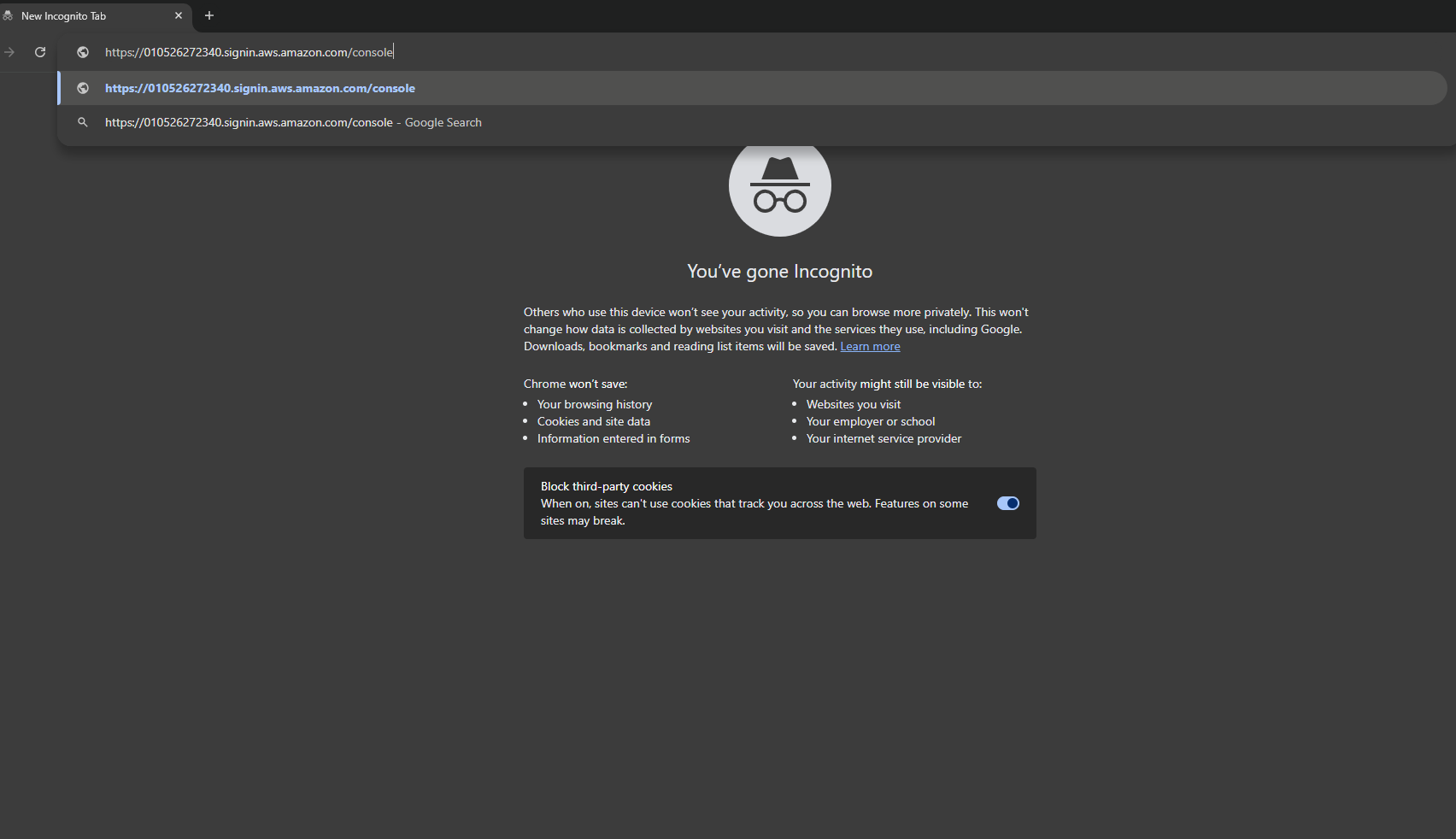
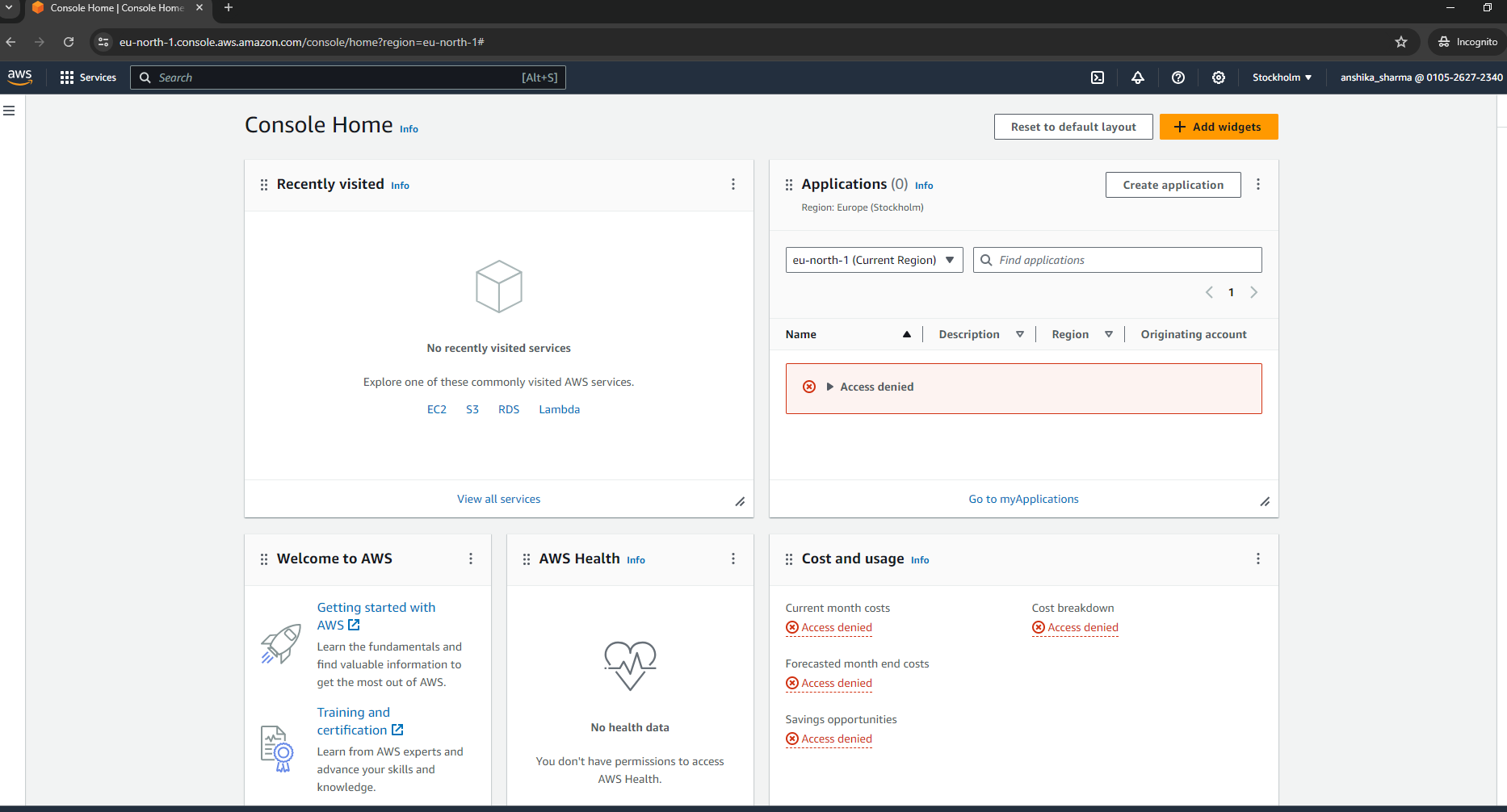
Roll No: A061

1.Navigate to the search bar and search for "IAM."

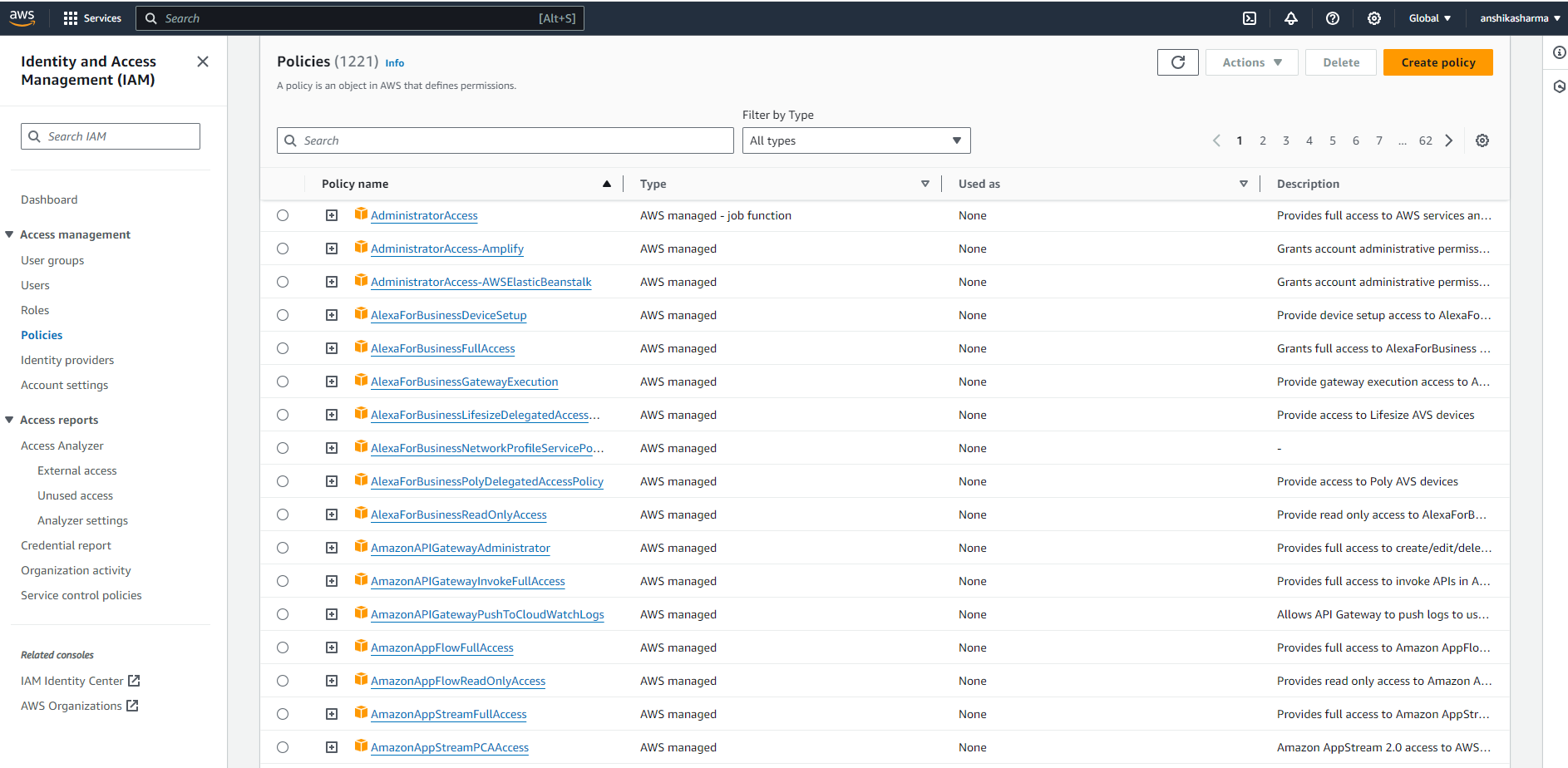
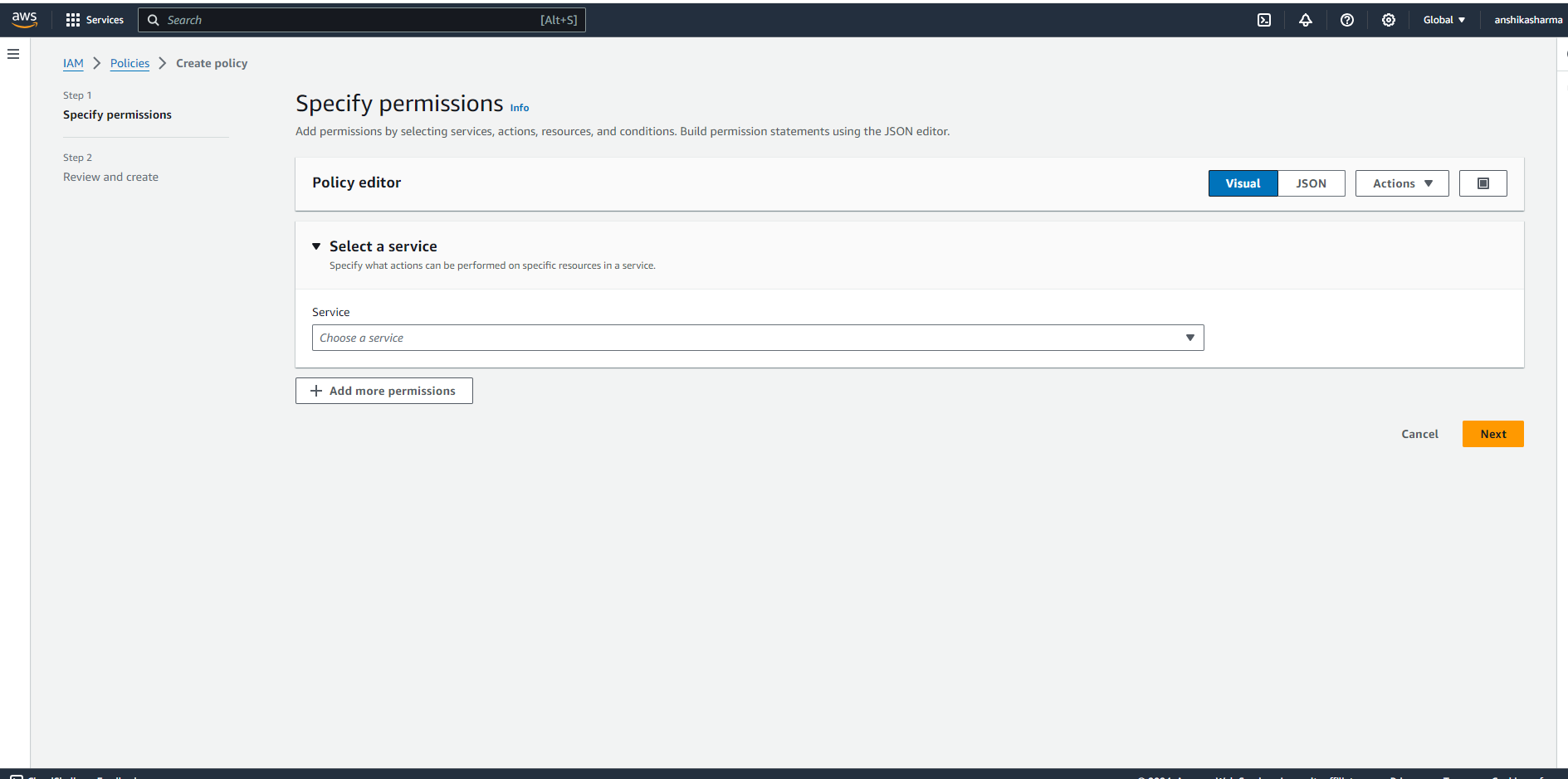
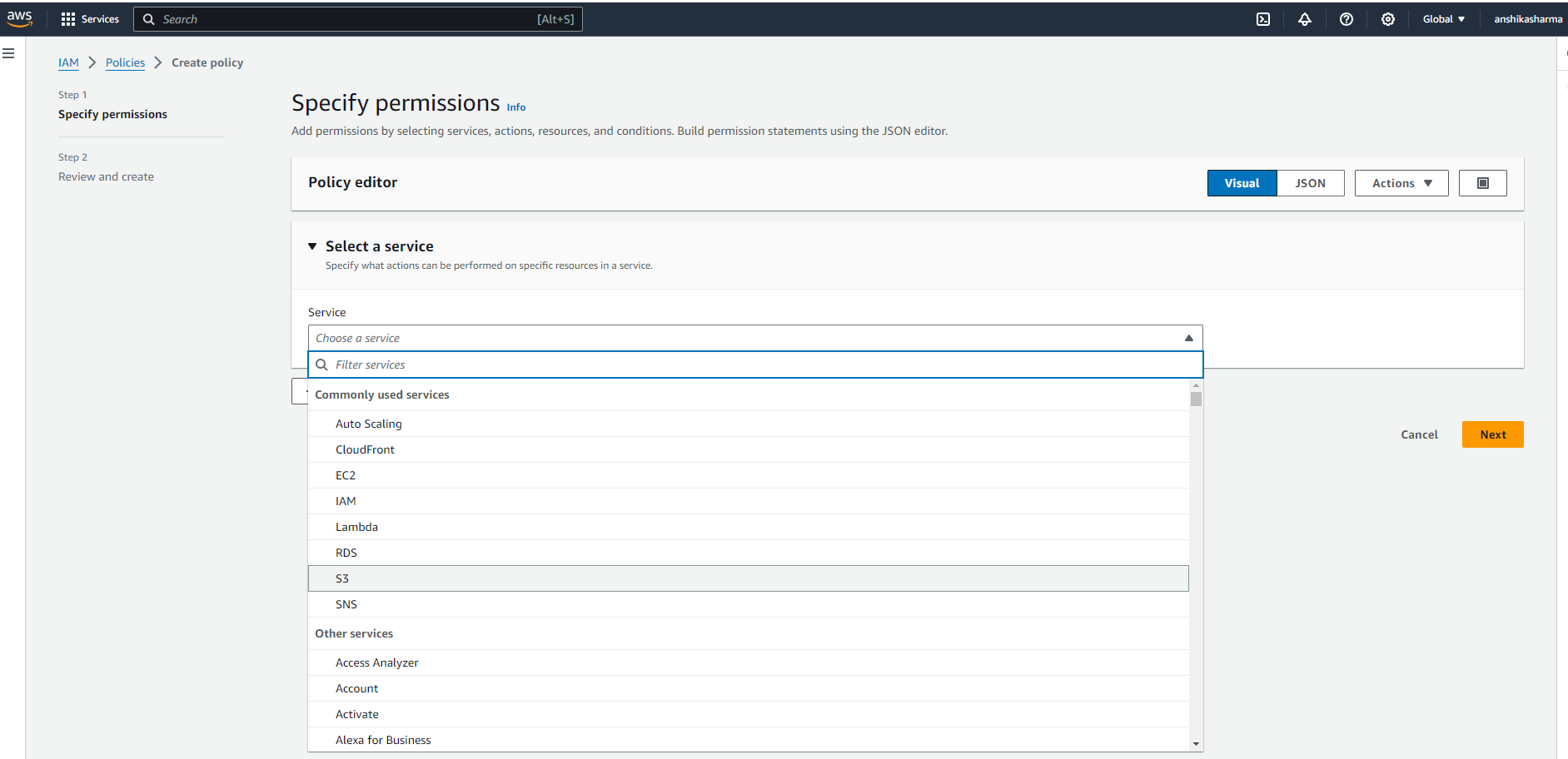
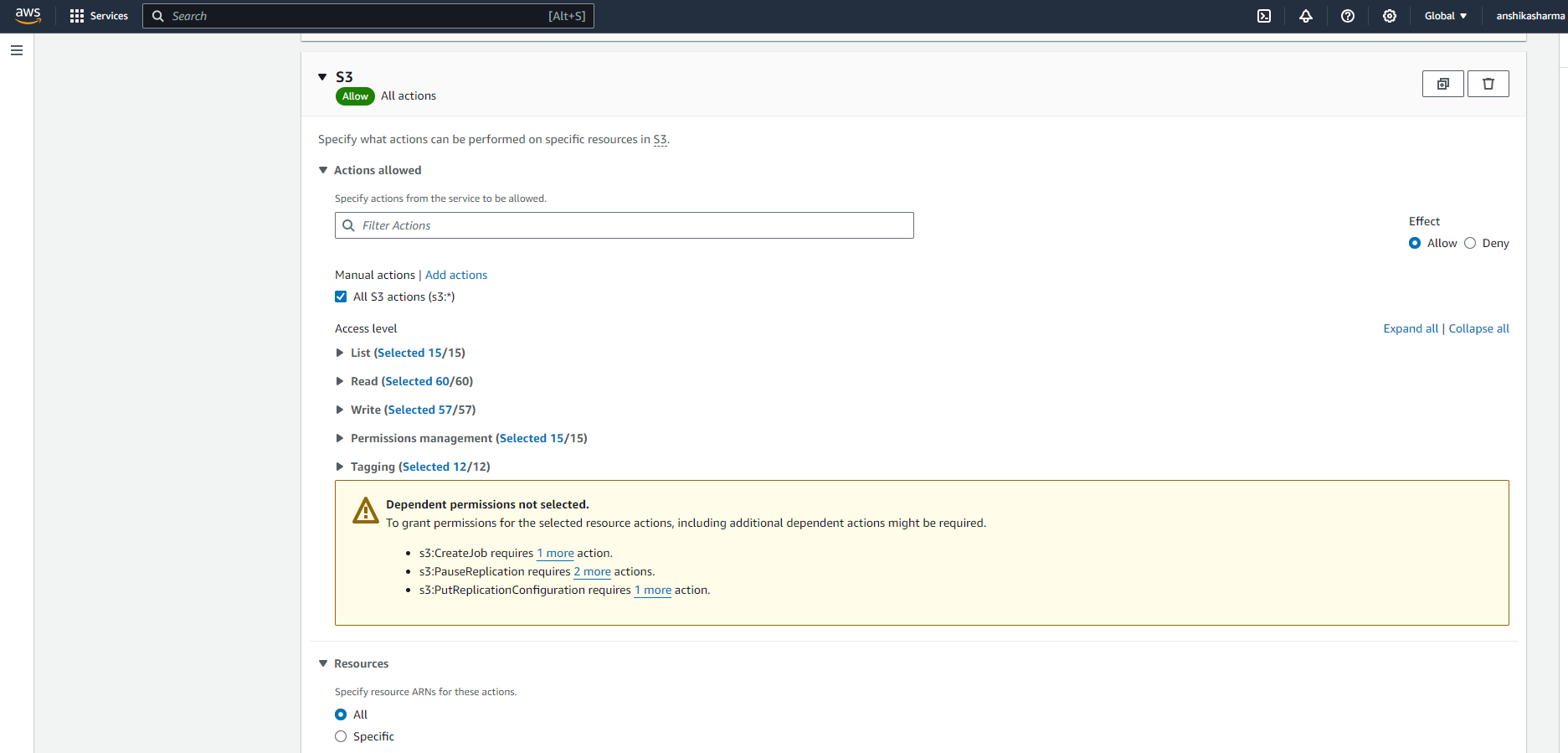
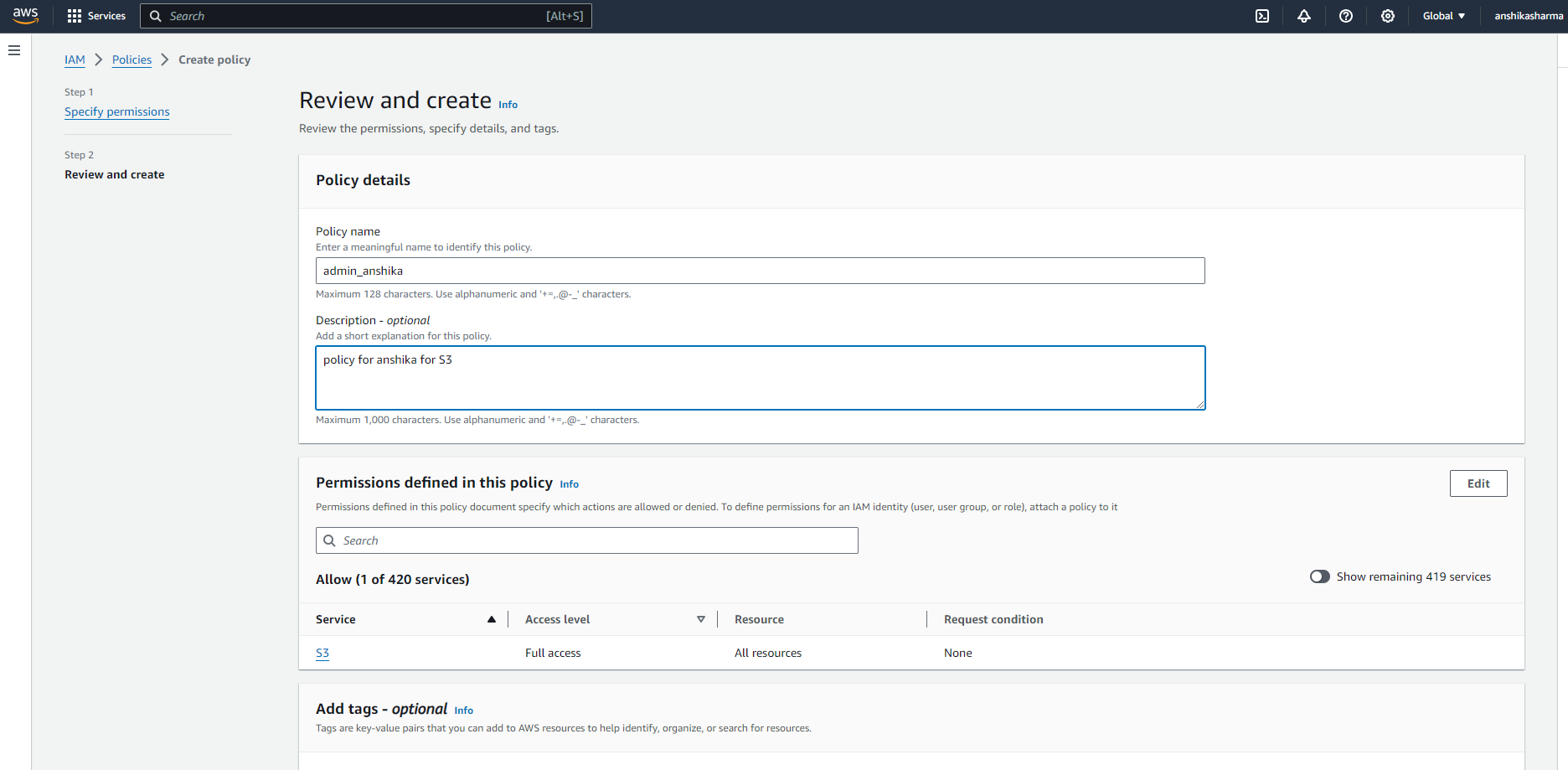
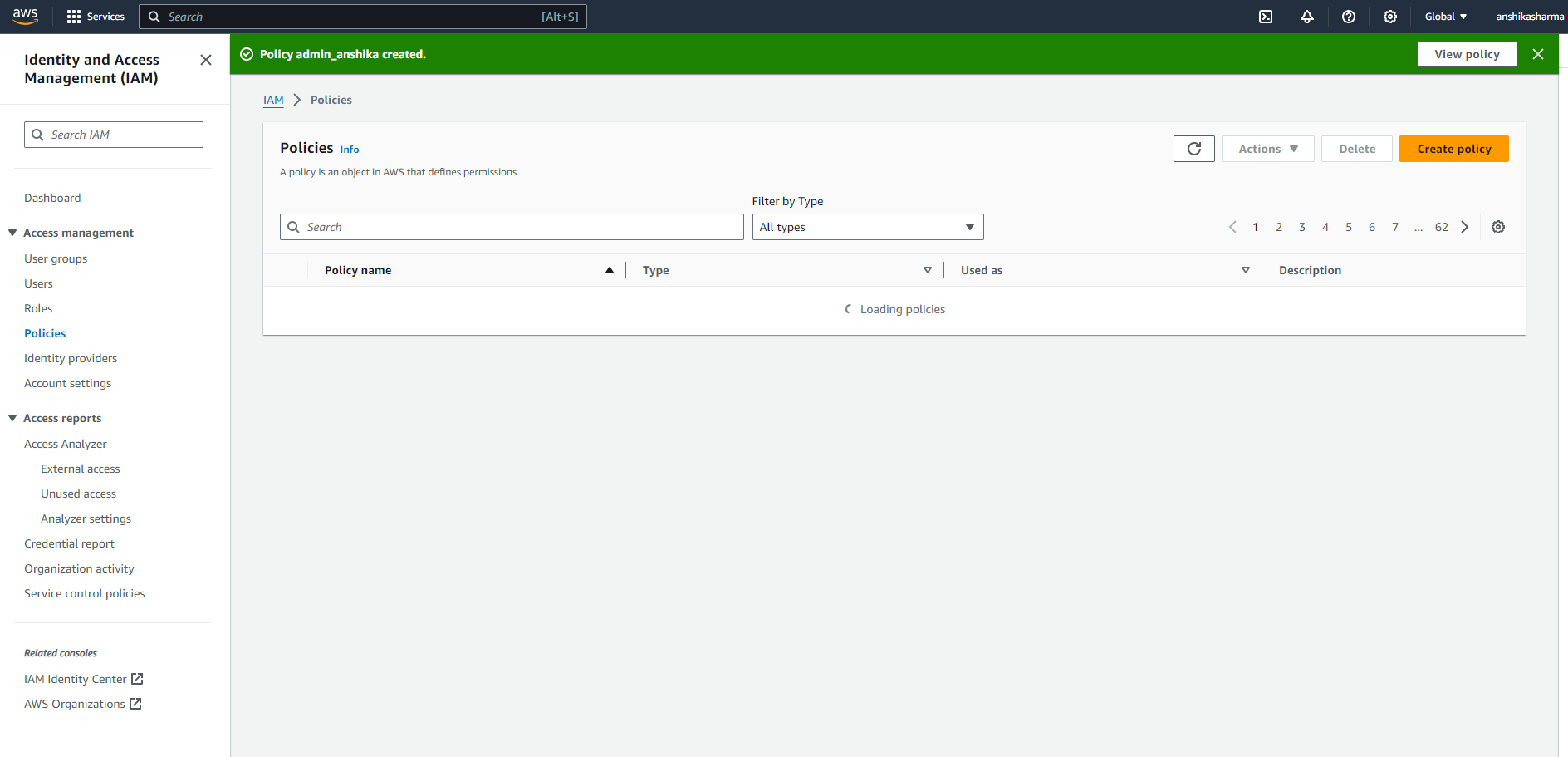
 2.The IAM dashboard will appear. 3.Select "Users" from the left pane. Enter the user details and click "Next."

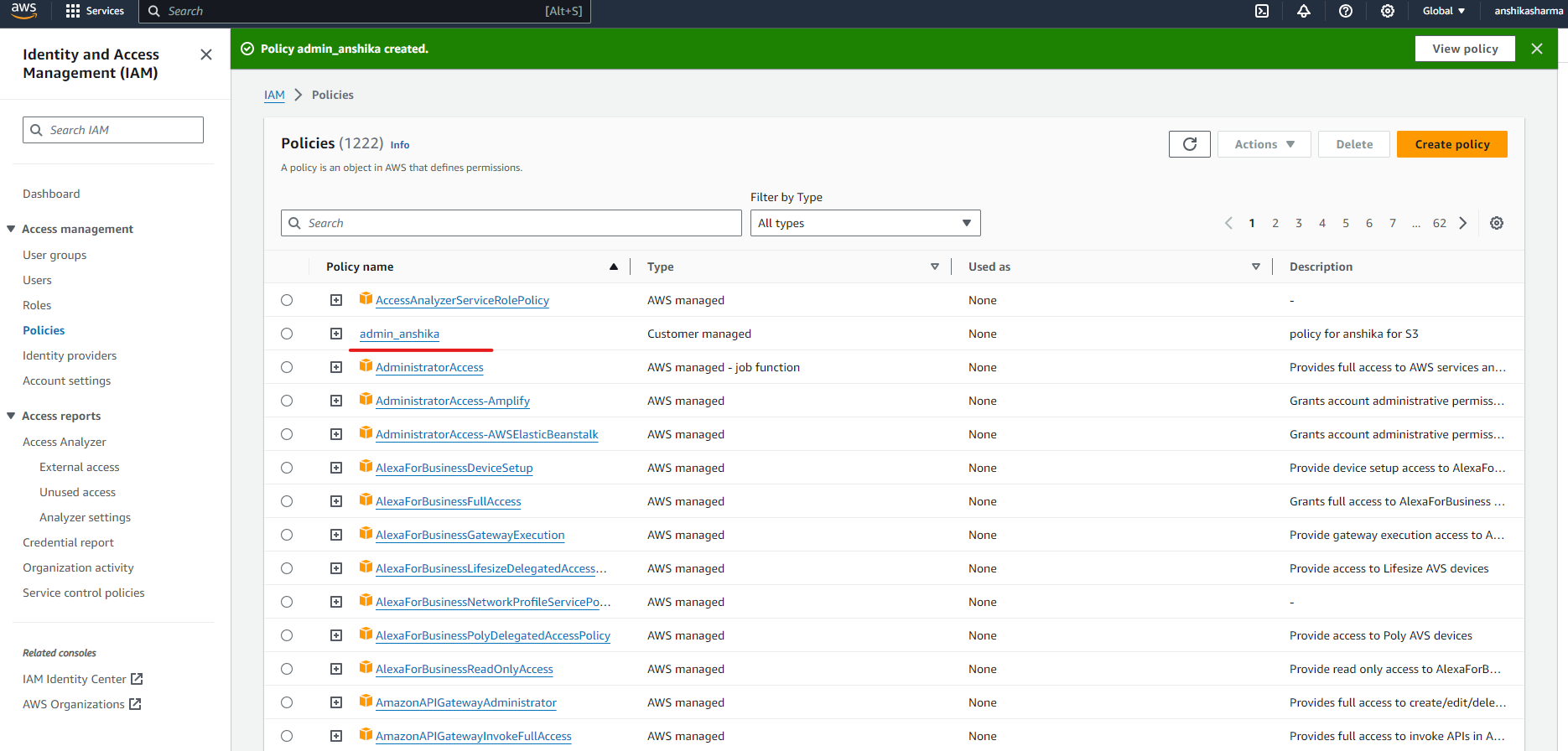
 4.Set permissions by selecting "Add user to group."

 5.Review the details and click "Create user." 6.The user is successfully created. 7.Click on the newly created user named "anshika\_sharma." Navigate to Security Credentials and click on "Enable Console Access."

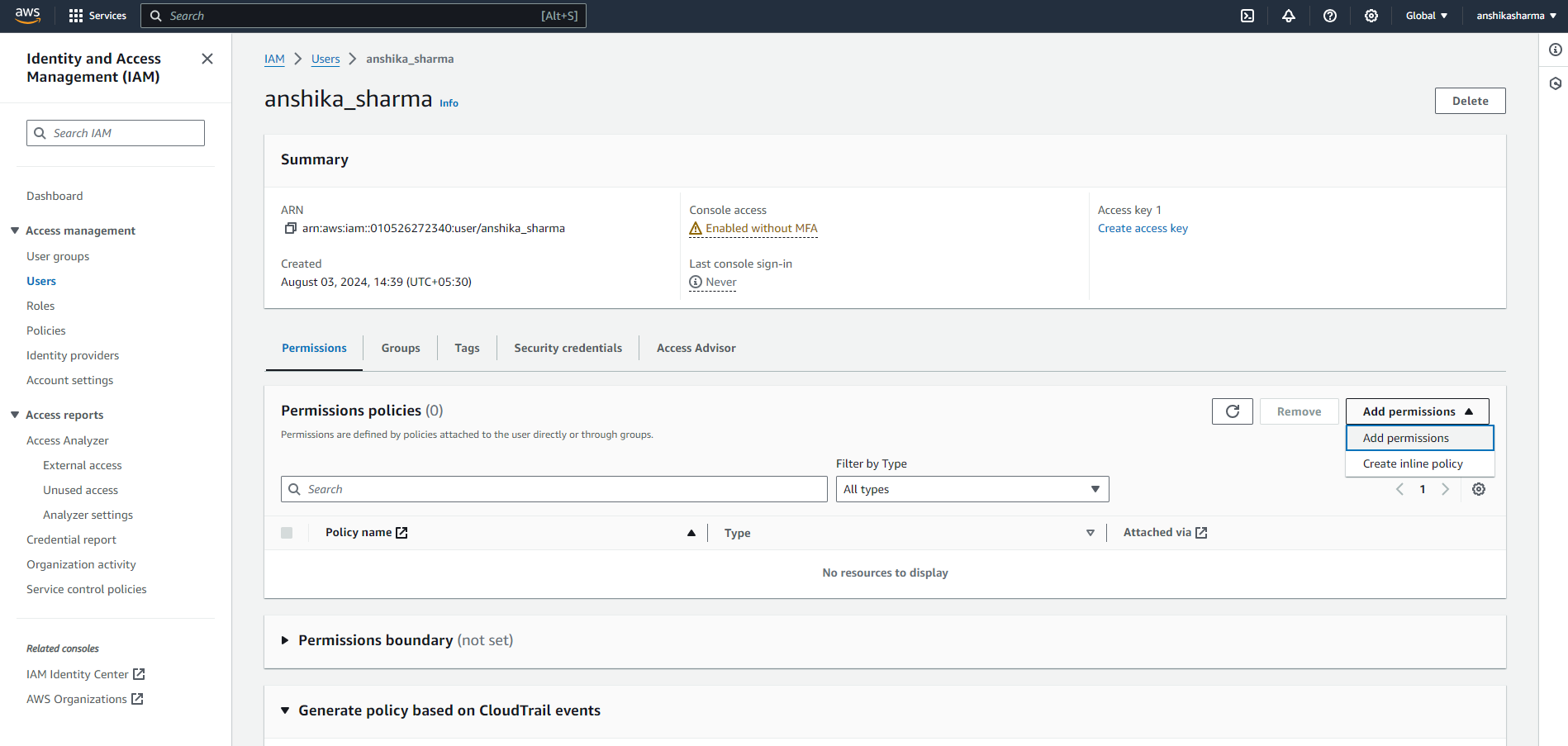
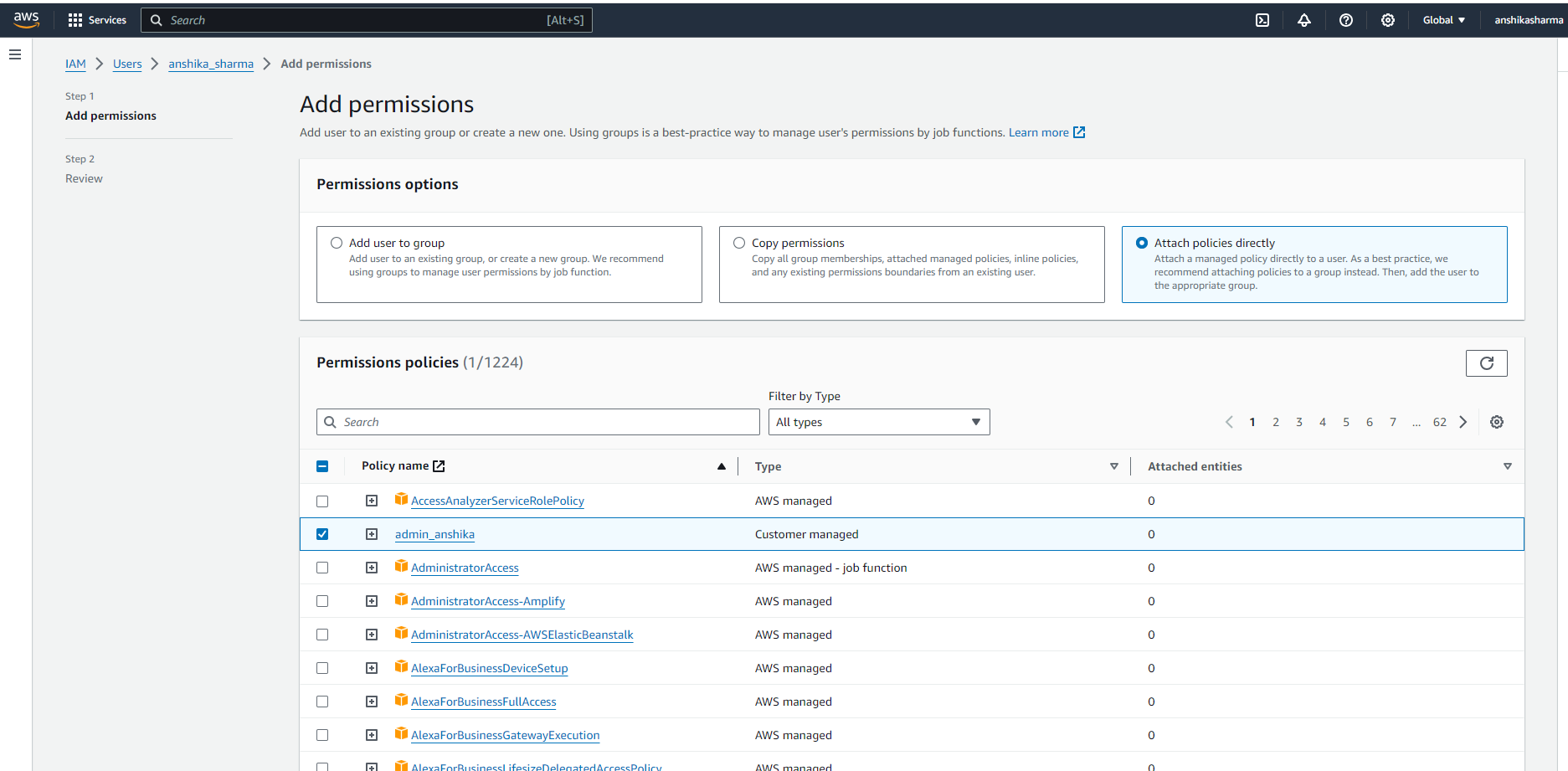
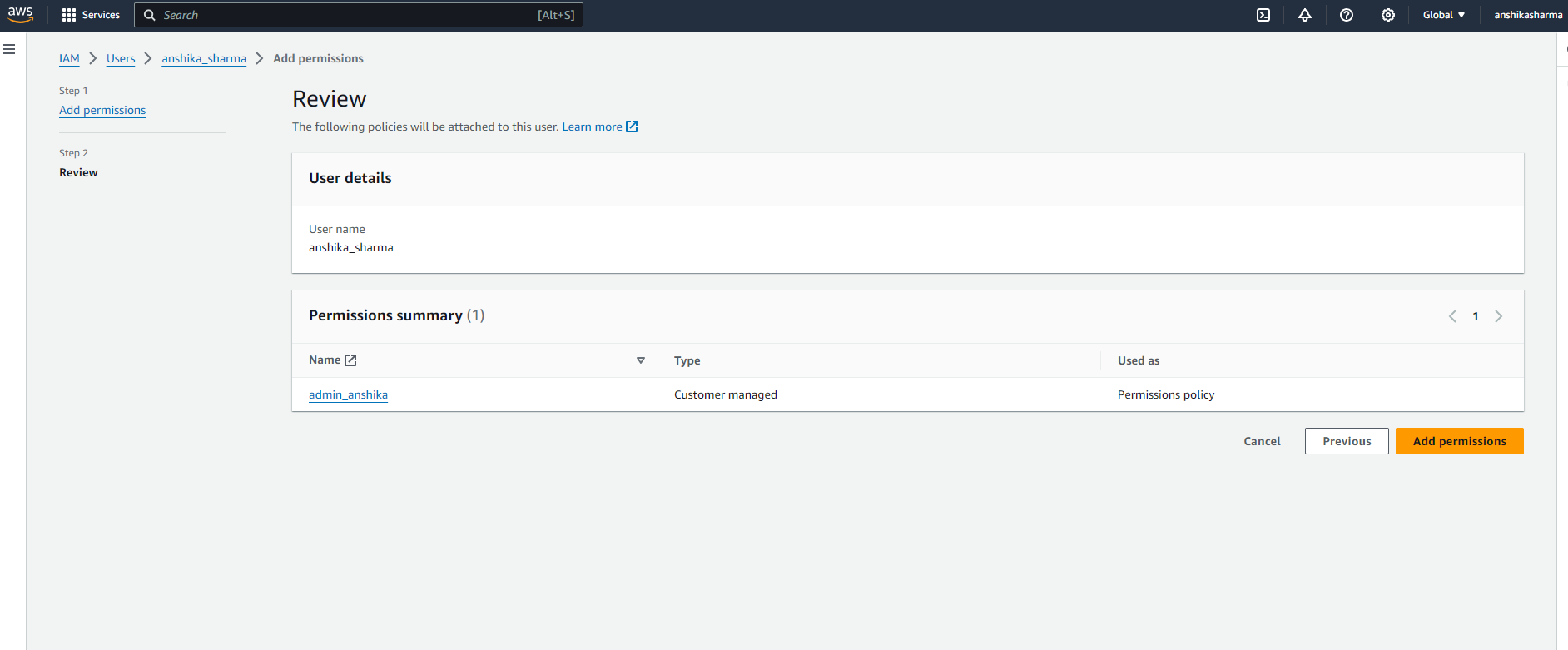
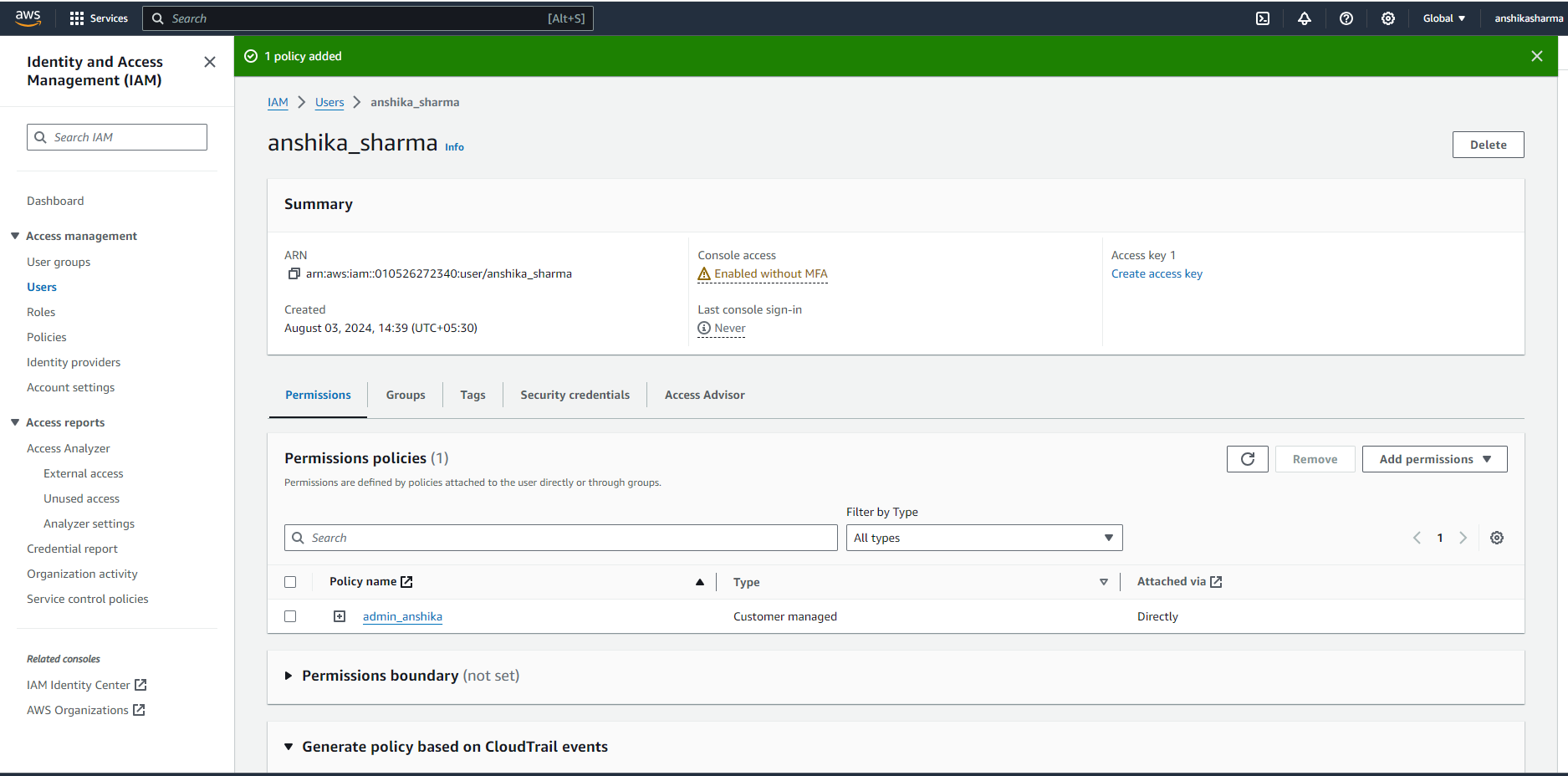
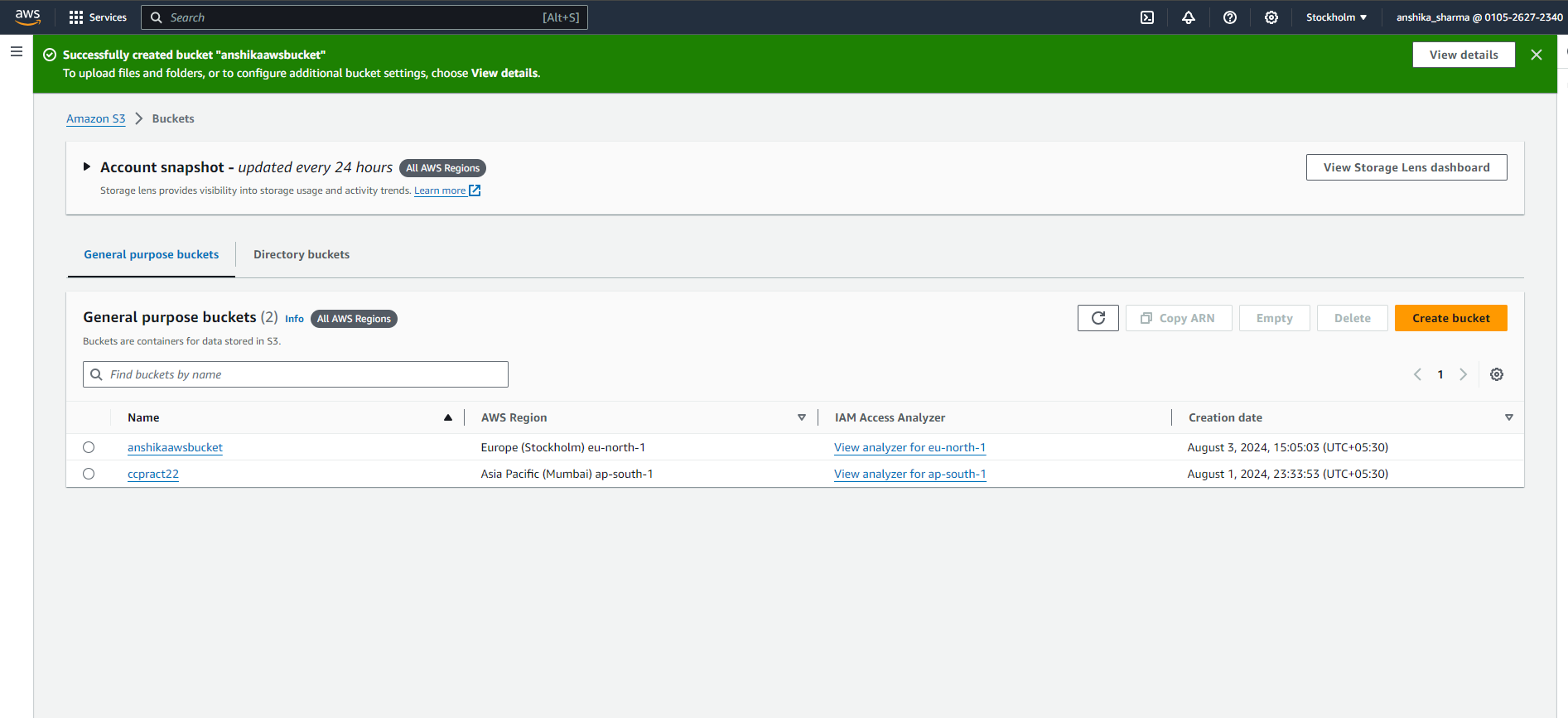
 8.Customize the password and then click on "Enable Console Access."   9.Console access has been successfully enabled with the new password.  10.Copy the Console sign-in URL and paste it into an incognito window. 11.Using the customised login id and password you login to console home. The Console Home will appear, but you'll see that access is denied for the current user. 12.To grant access to the newly created user, create policies:

* Go to your account.
* From the left pane, select "Policies."
* Click on "Create Policies."

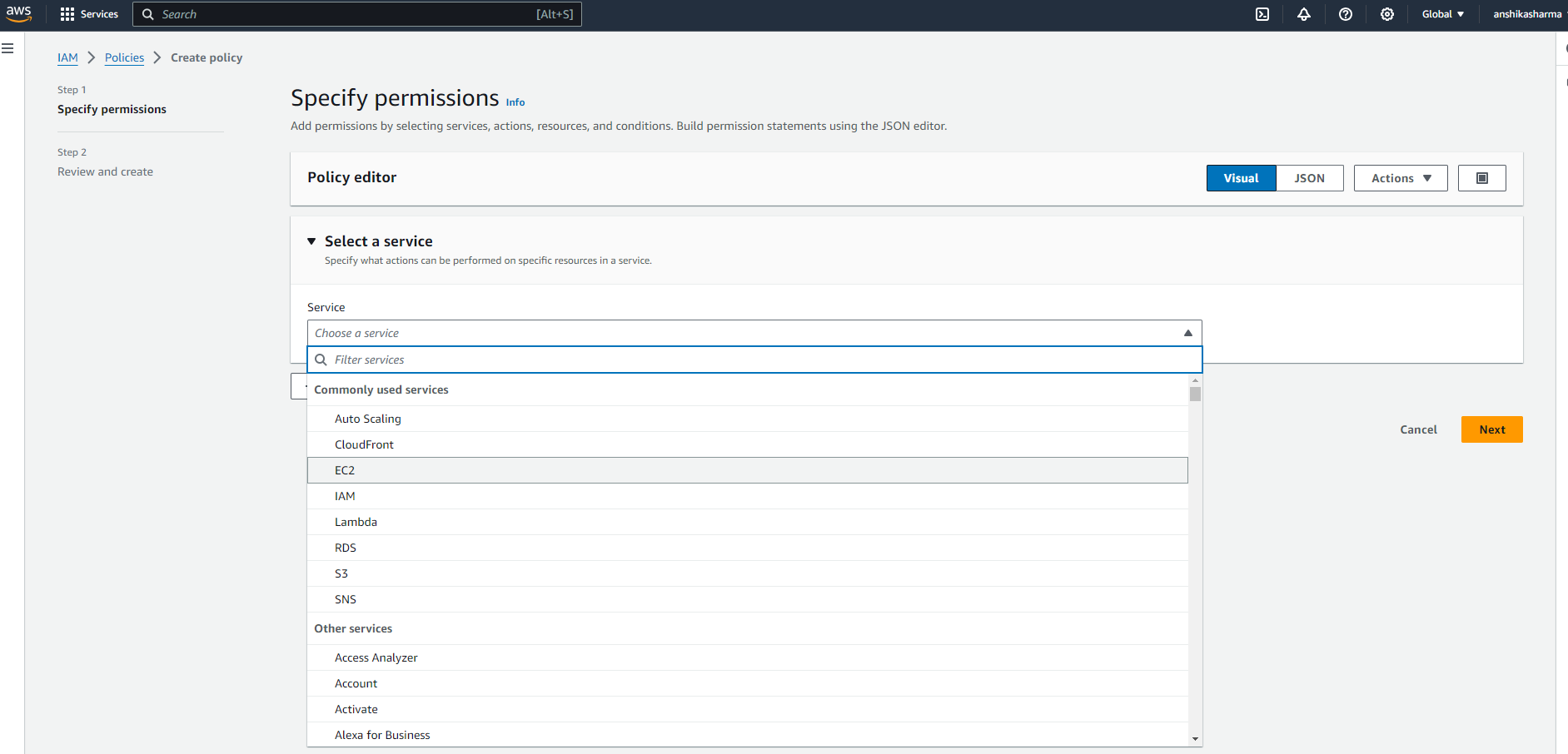
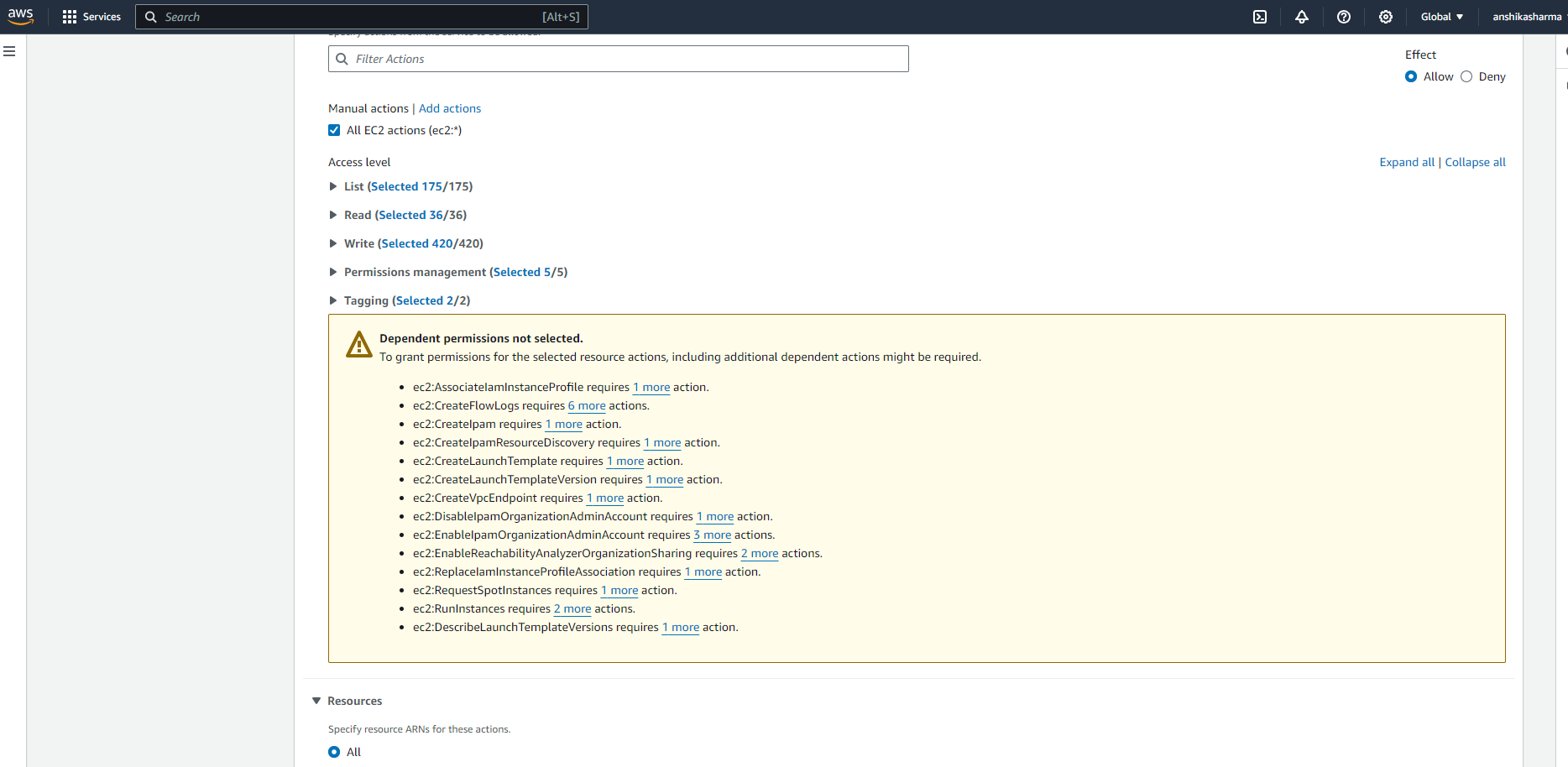
 13.Specify permissions for the user. 14.Under the Service option, select S3 to grant access for bucket creation. 15.Next, select "All S3 actions" and “All” under the Resources section. 16.Proceed to the Review and Create pane, where you'll need to specify the policy name and provide a short description for the policy. 17.Click on Create Policy, and the policy will be created successfully. 18.Your policy named admin\_anshika, underlined in red, now appears in the policy list.

 19.Next, you need to add this permission:

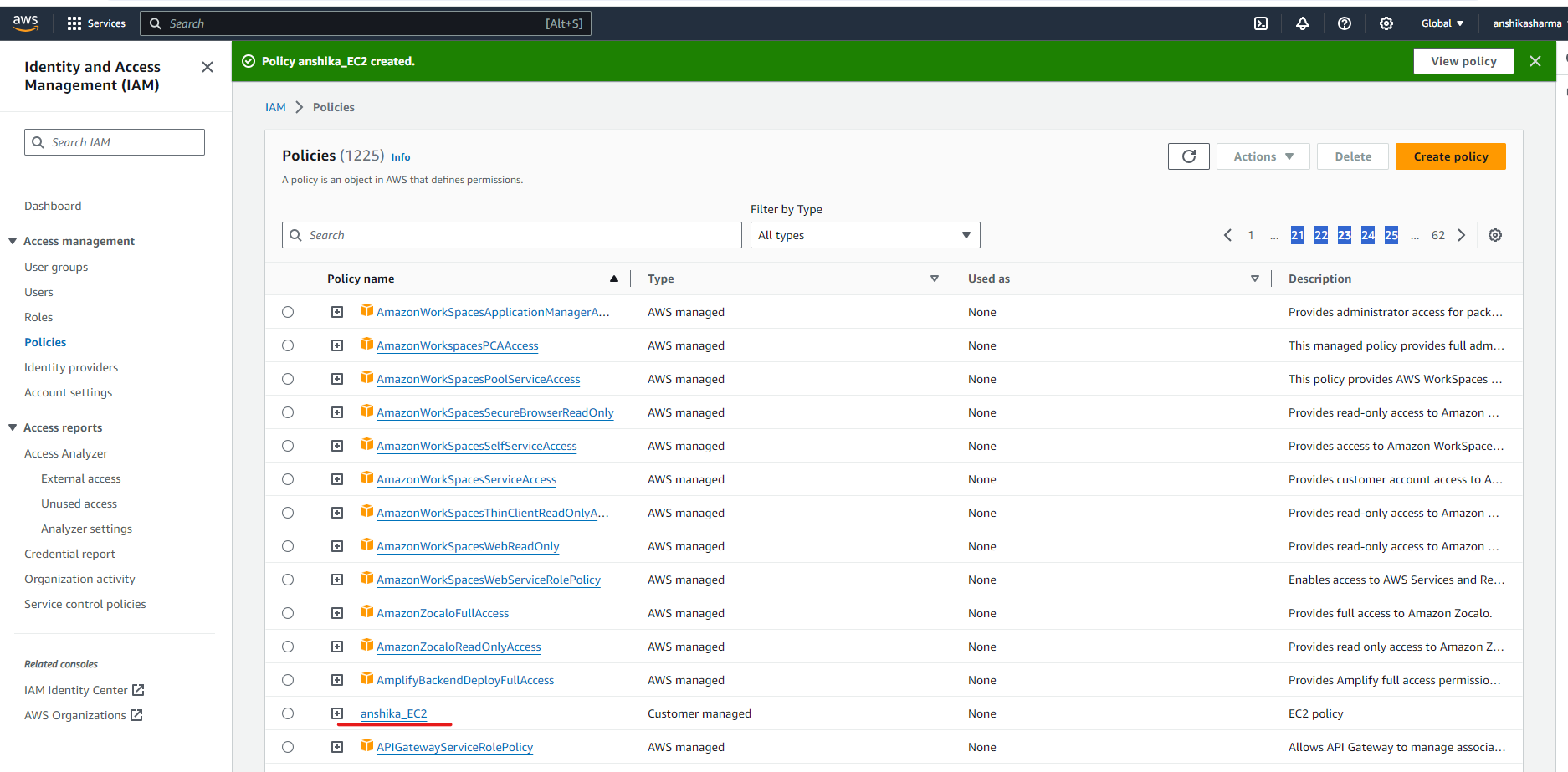
* Click on Users from the left pane.
* Select the Permissions tab.
* On the right side, click on Add Permissions.

 20.Select the policy you created under the "Add Permissions" section and click on “Attach Policy Directly”. 21.Review the details and click on Add Permissions. 22.Your policy has now been successfully added. 23.Return to the incognito window where you logged in as the new user and try to create a bucket. You'll see the bucket is created successfully, because of the granted access for S3. 24.Repeat the same process for EC2: Just as you did for S3.

Under Specify Permissions service option select EC2.

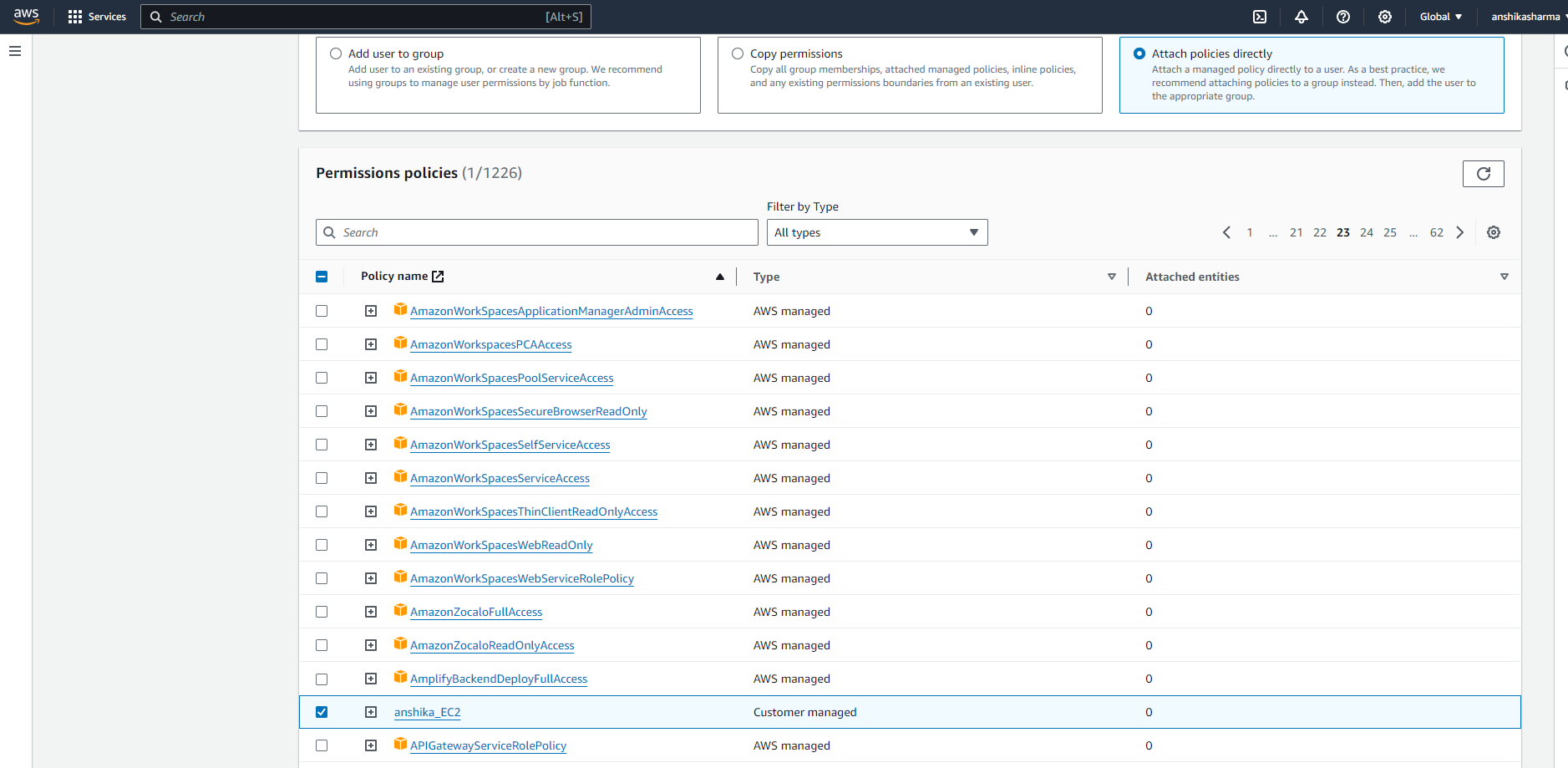
 25.Select "All EC2 actions" and “All” under the Resources section  26.Proceed to the Review and Create pane, where you'll need to specify the policy name and provide a short description for the policy. Click on Create Policy, and the policy will be created successfully.

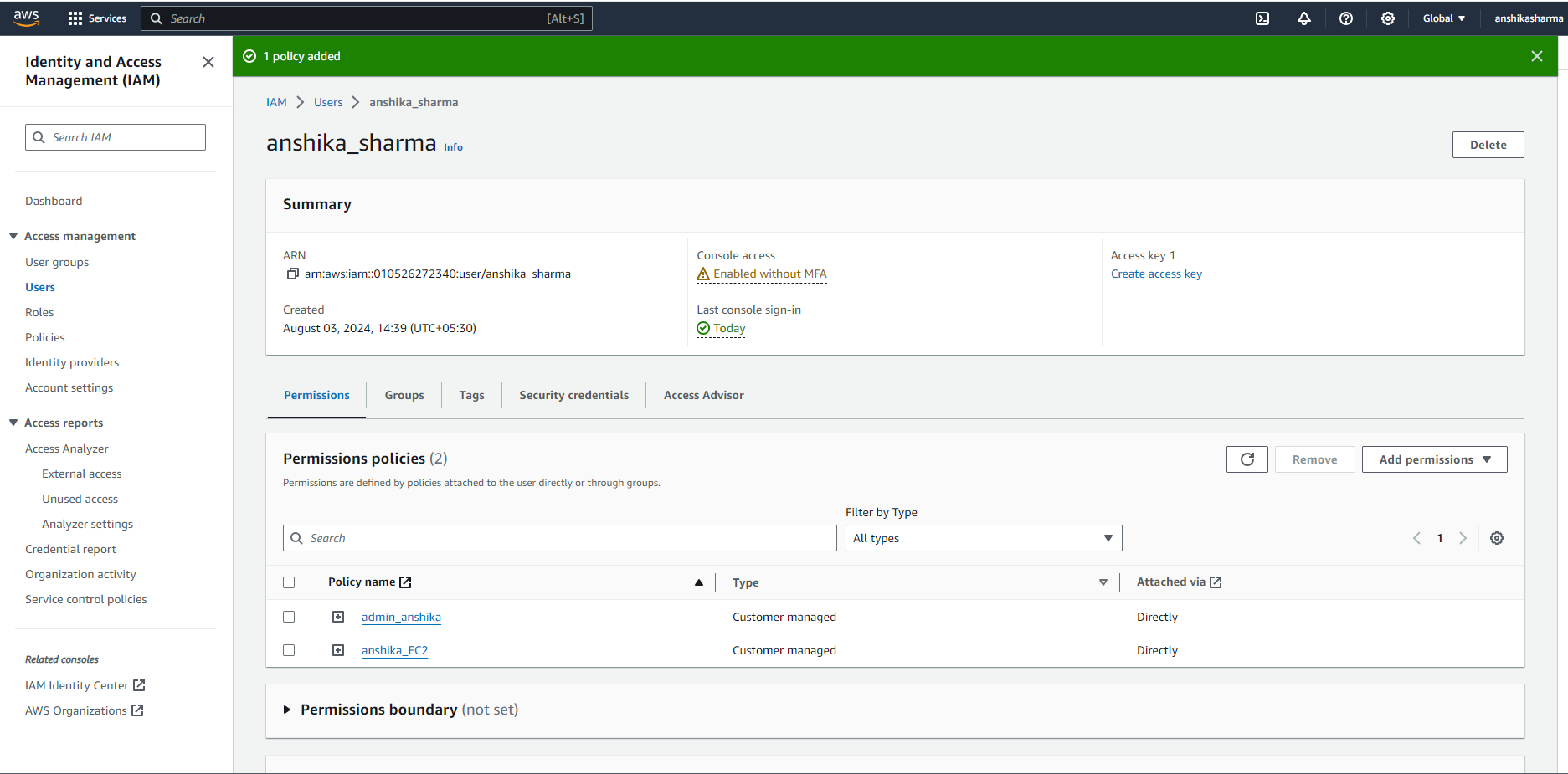
Your policy named Anshika\_EC2, underlined in red, now appears in the policy list.

  27.Next, you need to add this permission:

* Click on Users from the left pane.
* Select the Permissions tab.
* On the right side, click on Add Permissions

Select the policy you created under the "Add Permissions" section and click on “Attach Policy Directly”

 28.Review the details and click on Add Permissions.

29.Your policy has now been successfully added. 30.Return to the incognito window where you logged in as the new user and try to launch an instance. You'll see instance is launched successfully, because of the granted access for EC2.