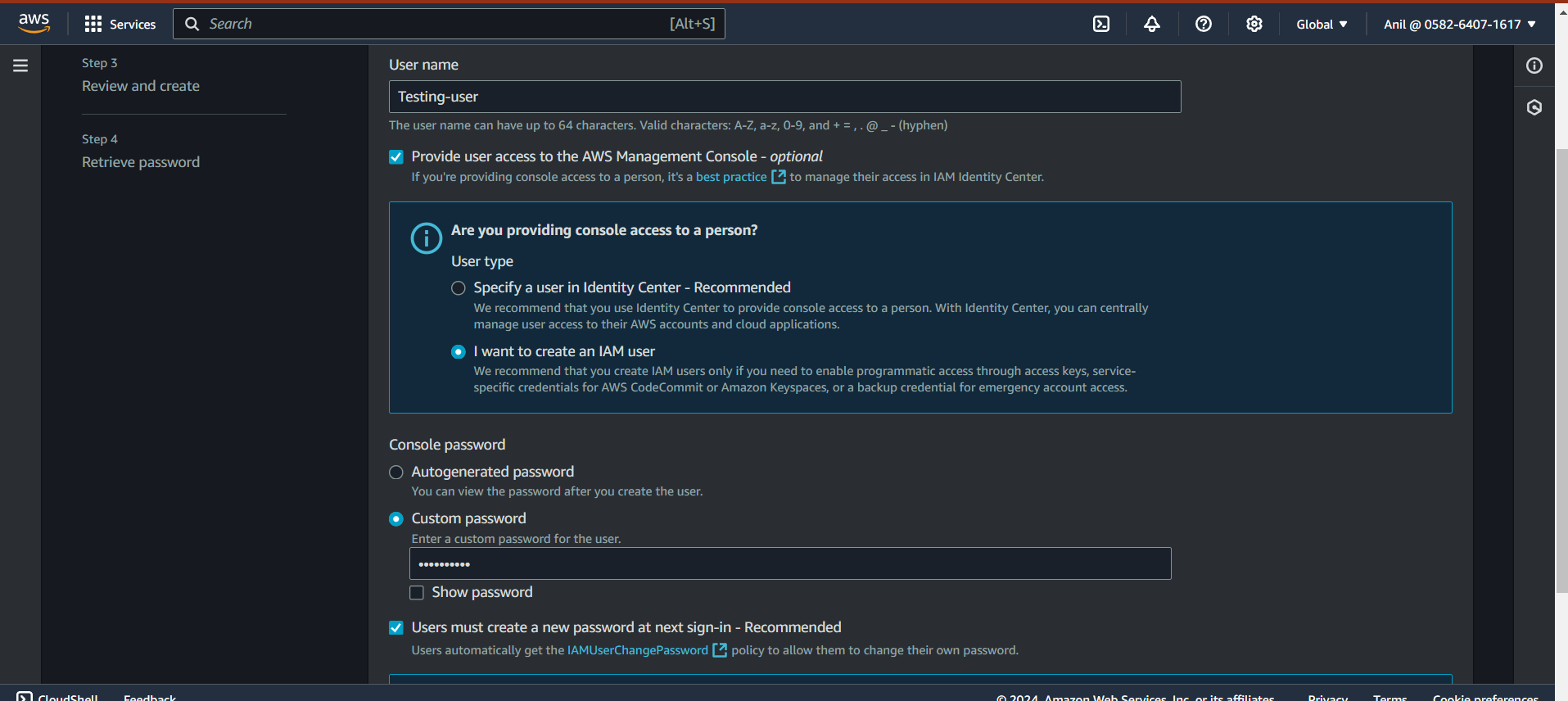
**IAM, Ec2 snapshot  
==================**

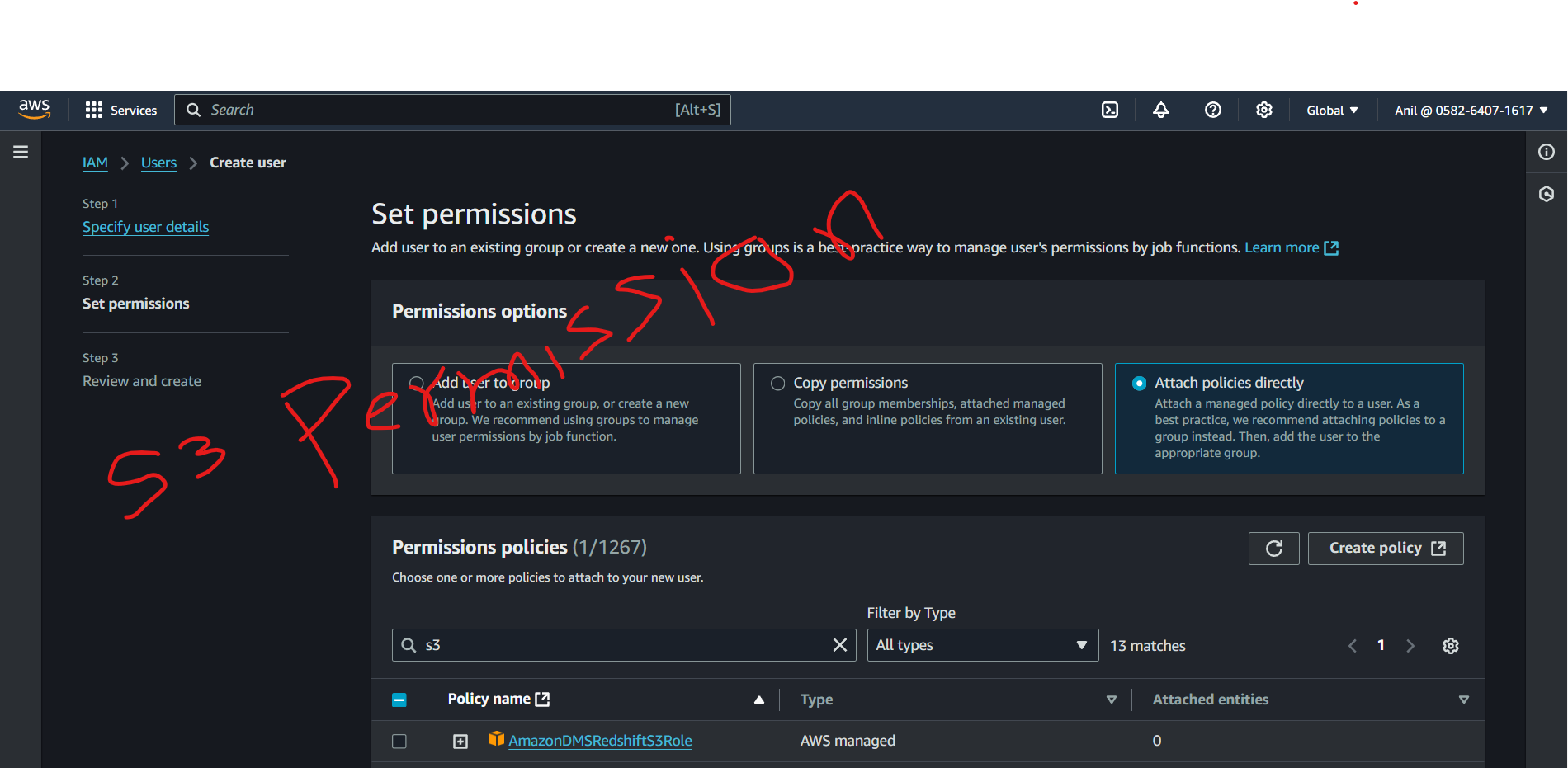
**1) Create one IAM user and assign ec2,s3 full access role.**

Using AWS Management Console

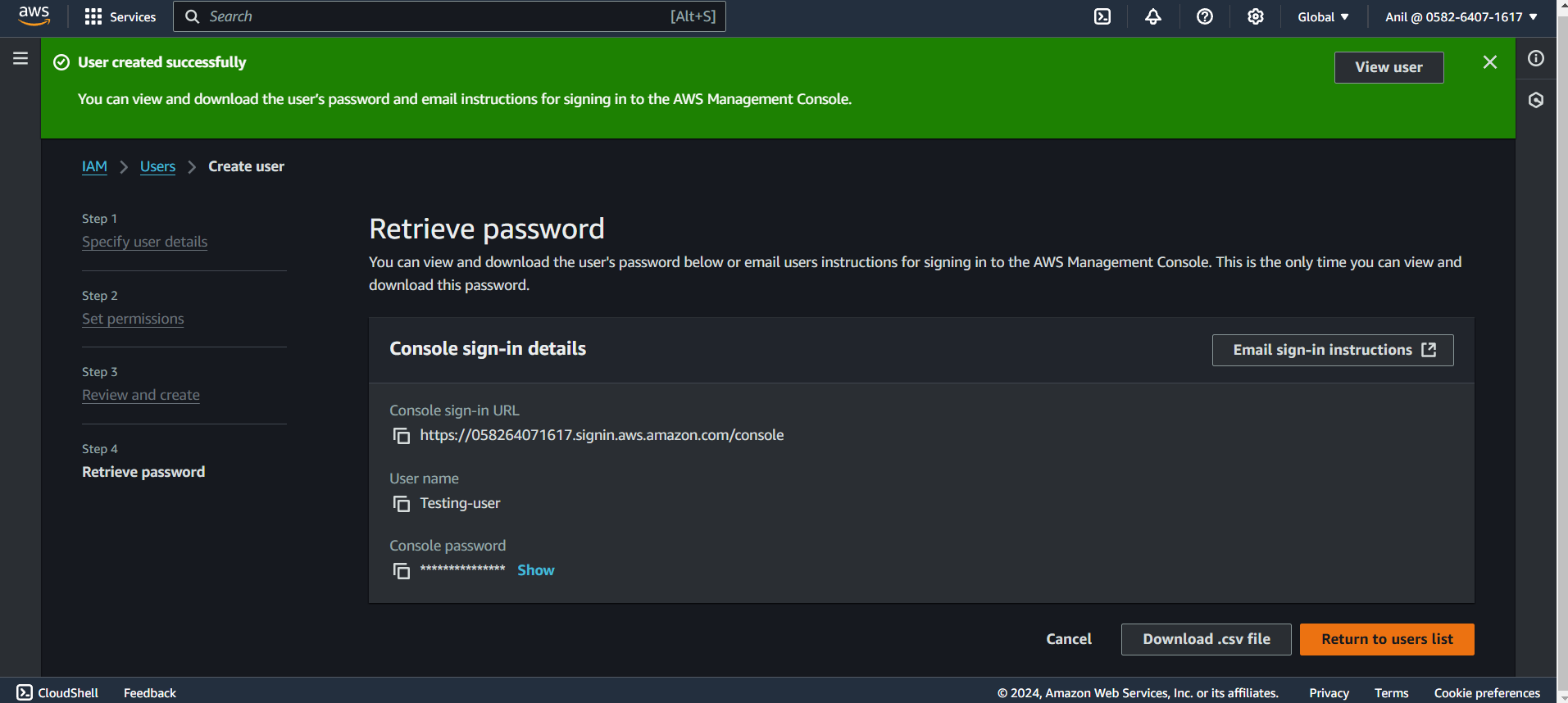
1. Sign in to the AWS Management Console
   * Go to [AWS Management Console](https://aws.amazon.com/console/).
   * Sign in with your AWS credentials.
2. Create the IAM User:
   * In the search bar, type IAM and select IAM (Identity and Access Management).
   * In the left sidebar, click on Users and then click the Add user button.
   * Enter a User name (e.g., new-ec2-s3-user).
   * Choose the Access type. For programmatic access (e.g., AWS CLI, SDKs), select Programmatic access. For access to the AWS Management Console, choose AWS Management Console access.
     + If you select AWS Management Console access, you can assign a password.

**

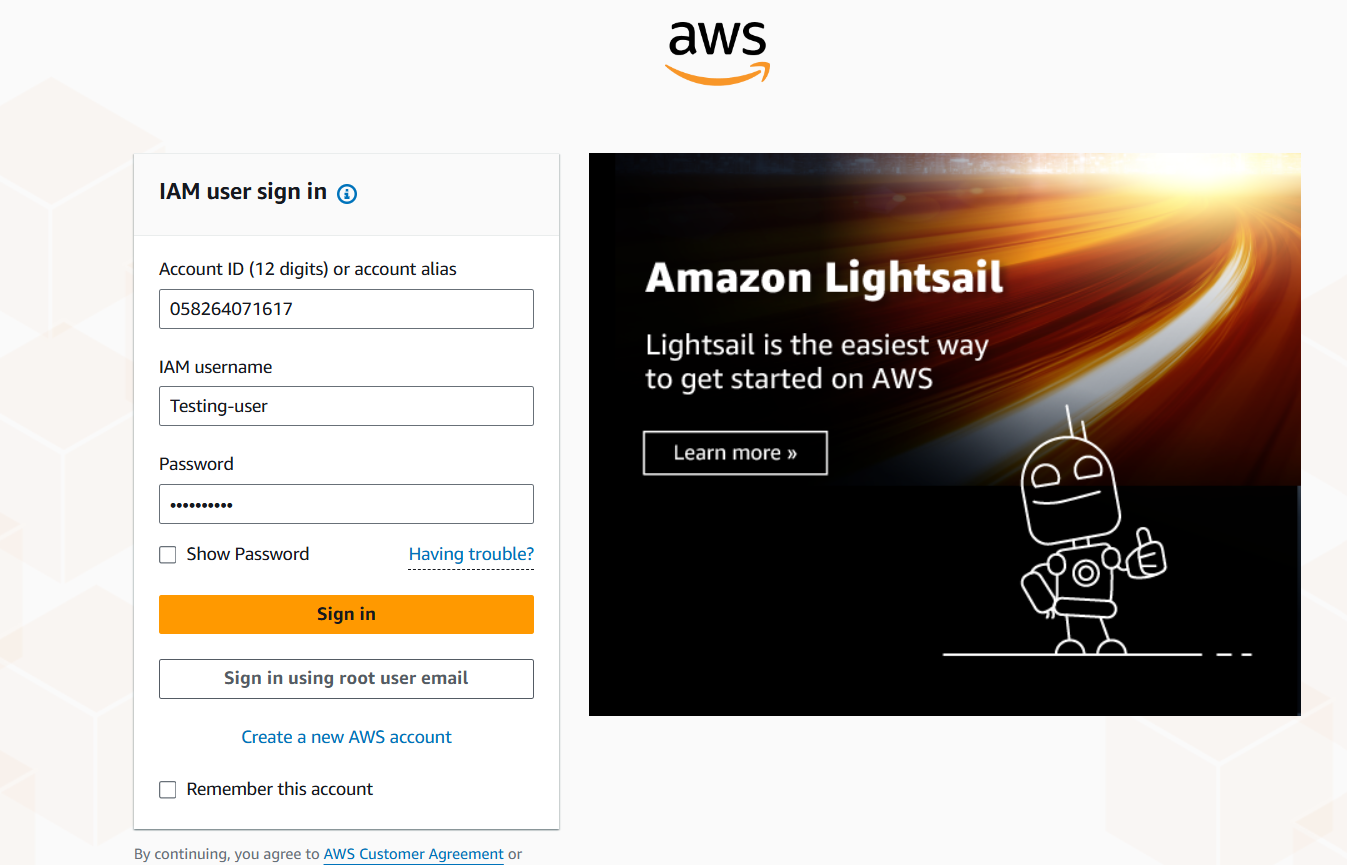
1. Set Permissions:
   * On the Set permissions screen, choose Attach policies directly.
   * In the search box, type AmazonEC2FullAccess and AmazonS3FullAccess.
   * Check the boxes for both AmazonEC2FullAccess and AmazonS3FullAccess.

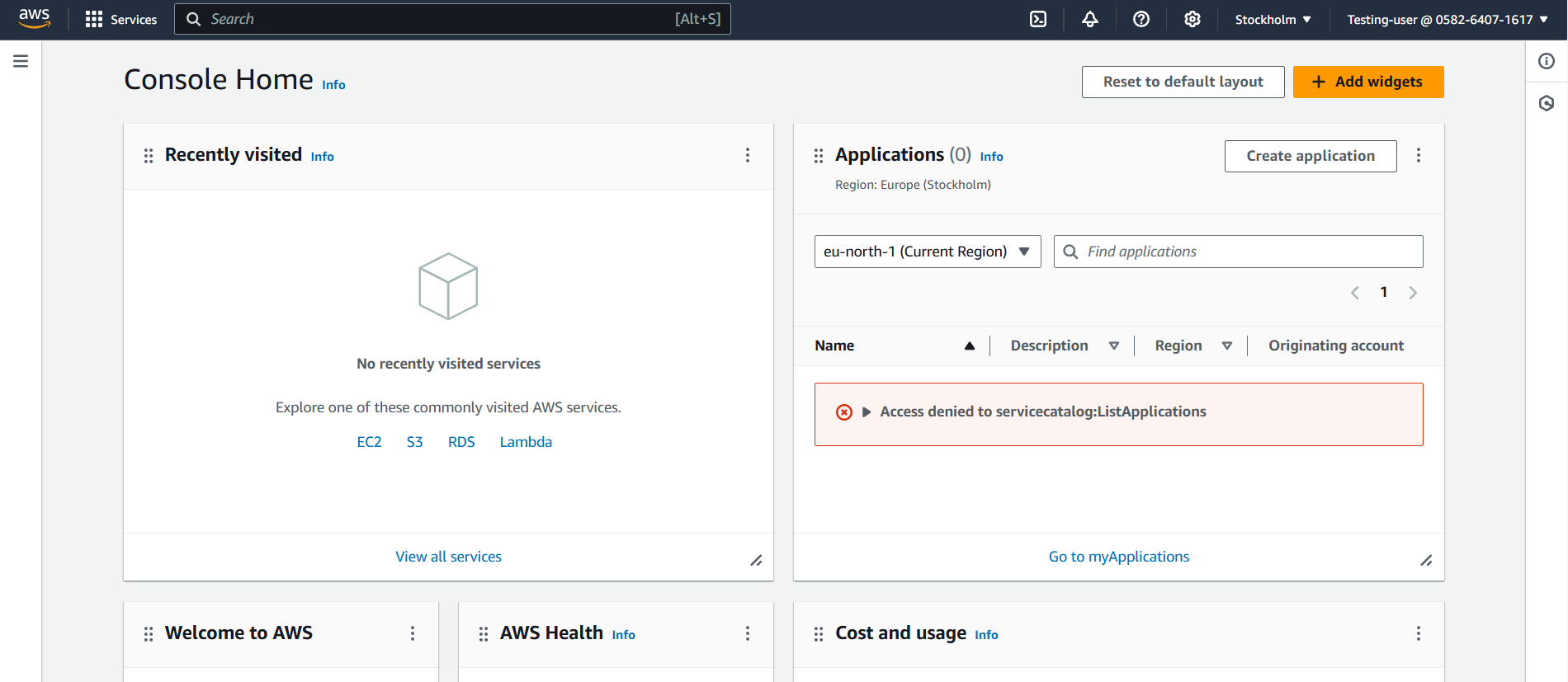
**

1. Review and Create:
   * Review the settings, and if everything looks correct, click Create user.

**

1. Download Credentials:
   * Once the user is created, you will see a success message. Make sure to download the credentials file

******

******

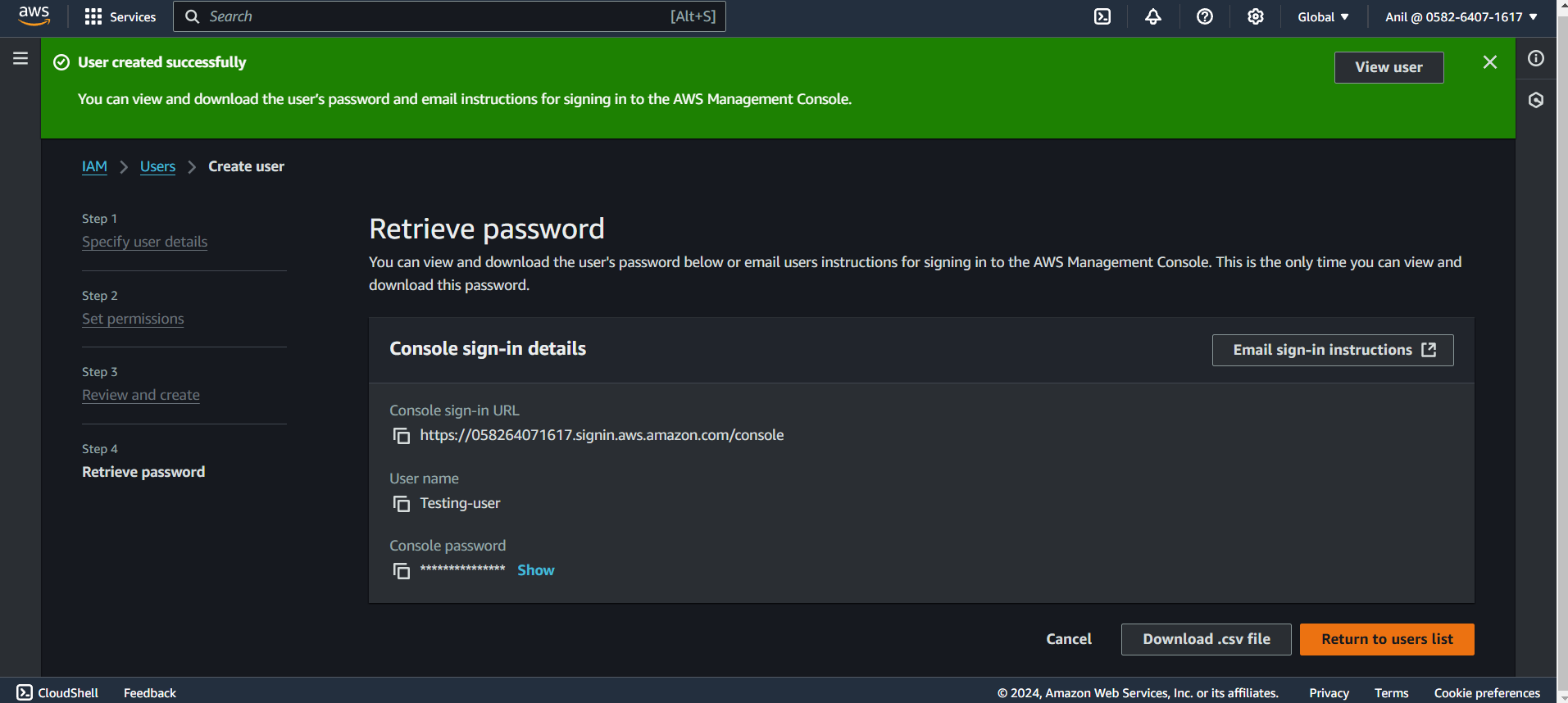
**2)** **Create one Group in IAM and Assign Read access for ec2**

Create the IAM Group

1. Log in to the AWS Management Console:
   * Navigate to the IAM service by typing "IAM" in the search bar and selecting IAM from the services list.
2. Create a New Group:
   * In the left-hand navigation pane, click Groups.
   * Click the Create New Group button.
   * Enter a name for your group (e.g., EC2ReadOnlyAccess).
   * Click Next Step.

Attach Policies to the Group

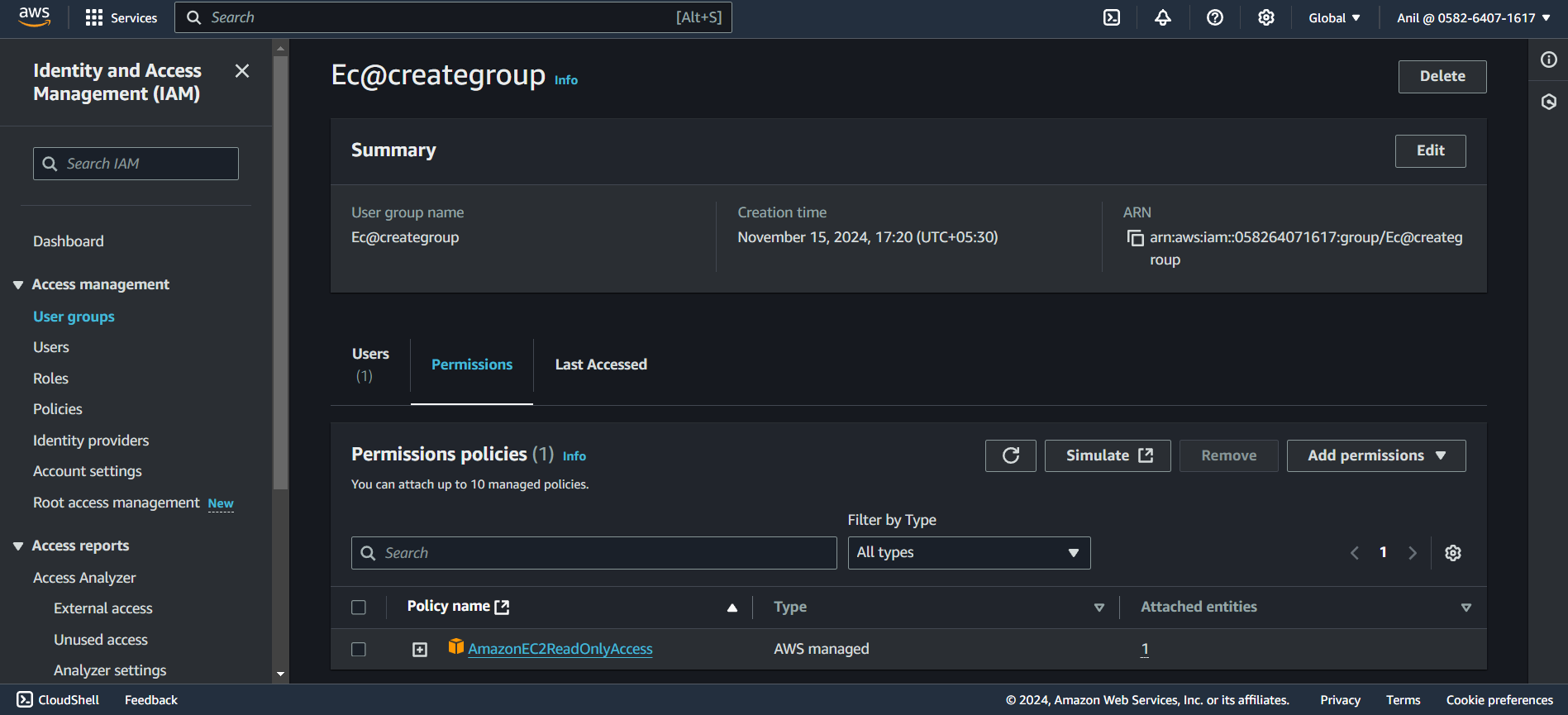
You can assign predefined policies that provide read-only access to EC2 instances.

**

1. Attach Policies:
   * On the "Attach Policy" page, search for the policy named AmazonEC2ReadOnlyAccess. This is an AWS managed policy that grants read-only access to EC2 resources.
   * Check the box next to AmazonEC2ReadOnlyAccess.
2. Review and Create:
   * Click Next Step to review your configuration.
   * Click Create Group to finalize the creation of the group.

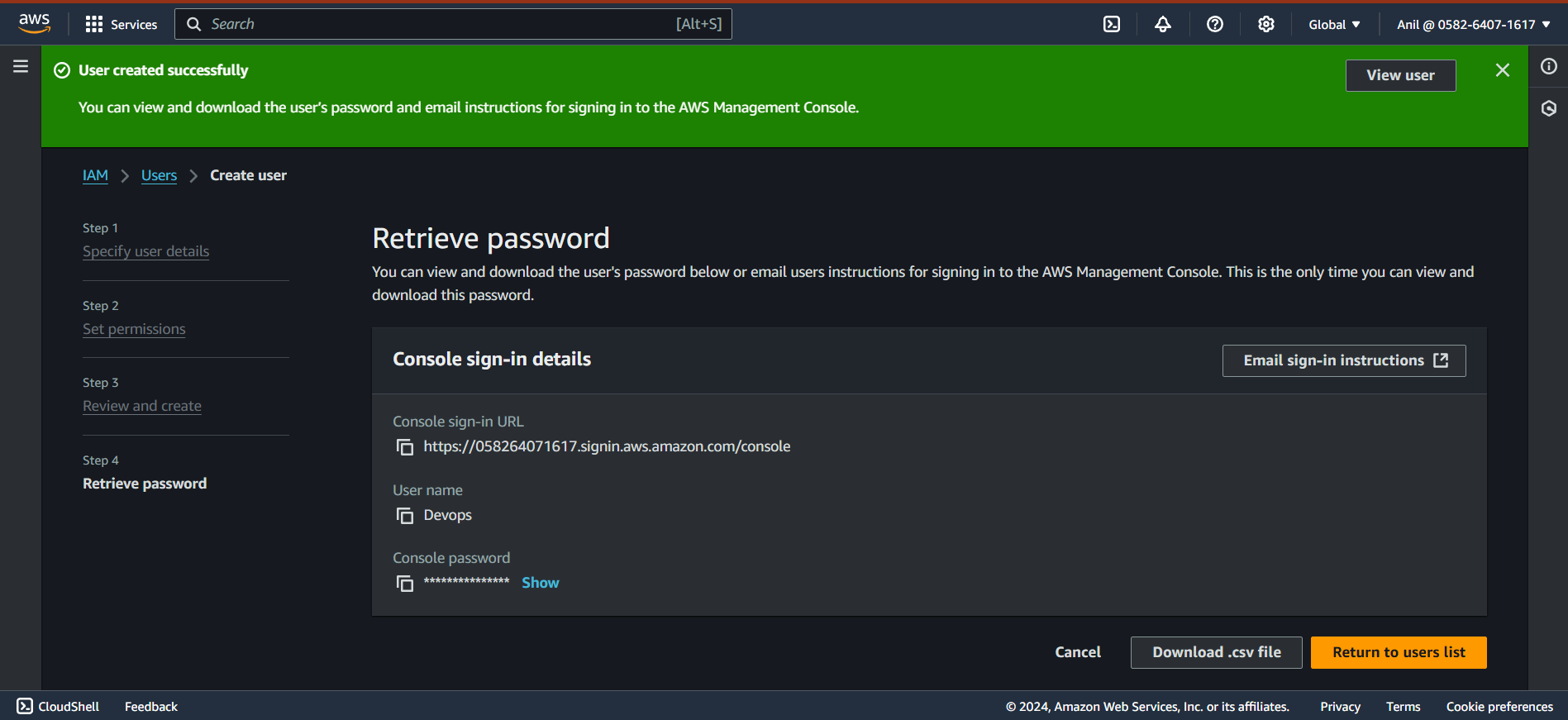
Add Users to the Group

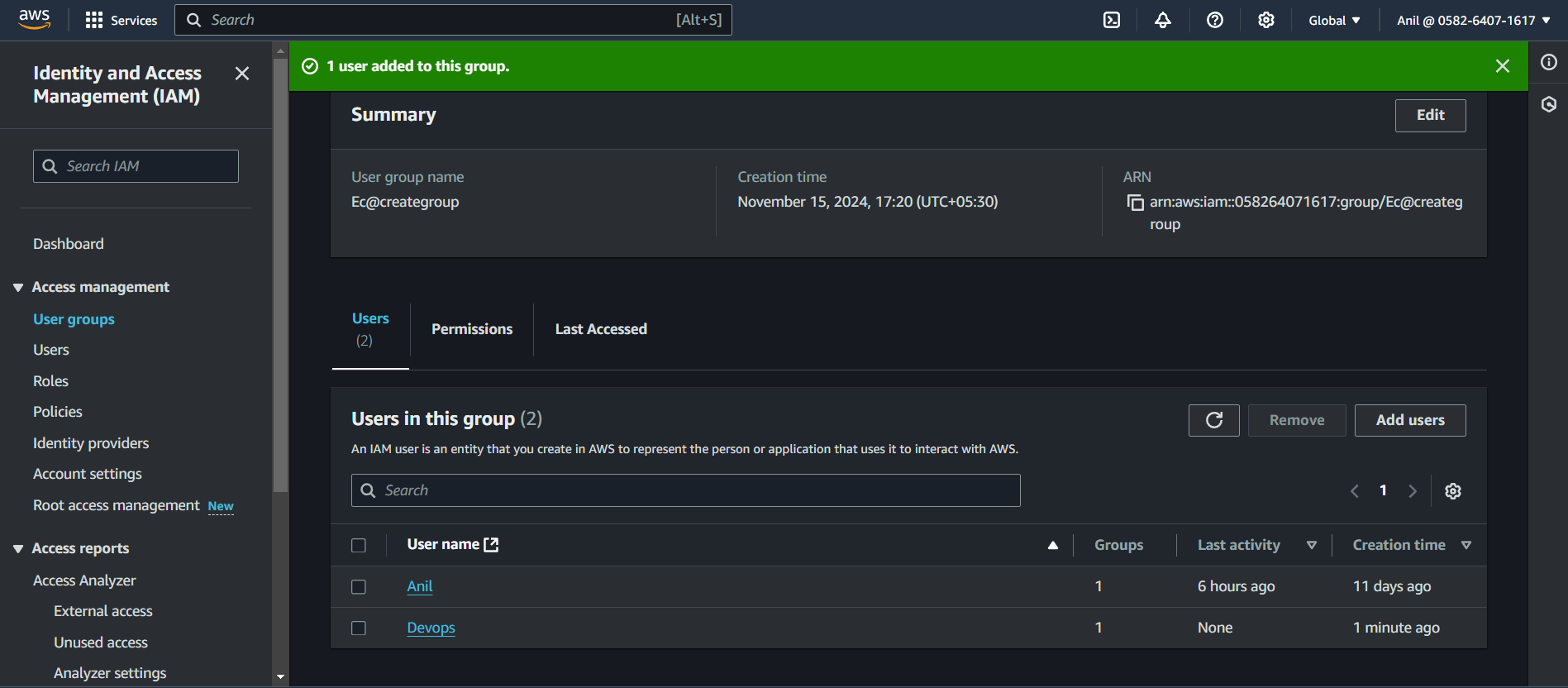
After creating the group, you need to add users who will have read-only access to EC2.

**

1. Add Users to the Group:
   * Navigate to the Users section in IAM.
   * Select the user you want to add to the EC2ReadOnlyAccess group, or create a new user if needed.
   * Click the Groups tab for the selected user and then click Add User to Group.
   * Choose the EC2ReadOnlyAccess group and click Add to Group.

**3) Create a new user with name Devops and add to the group created in task2.**

****

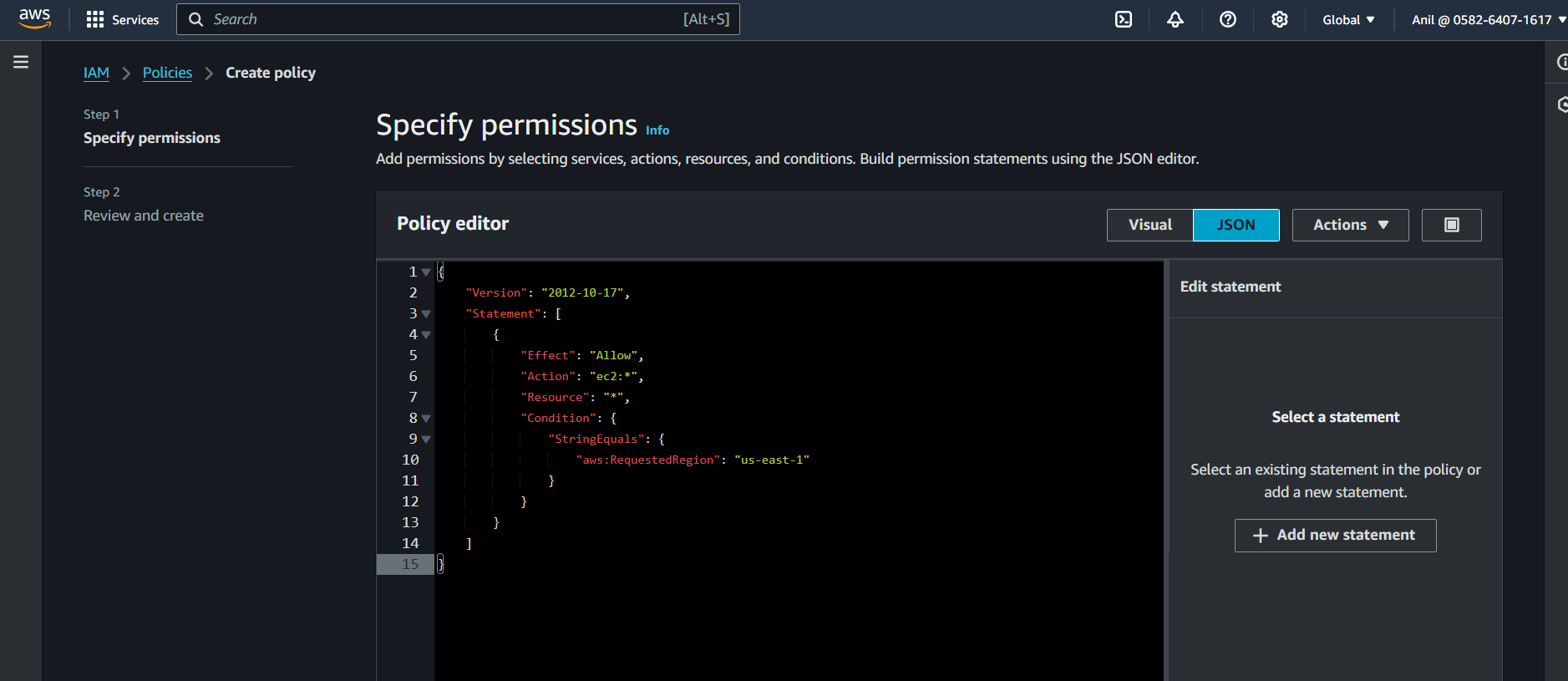
****

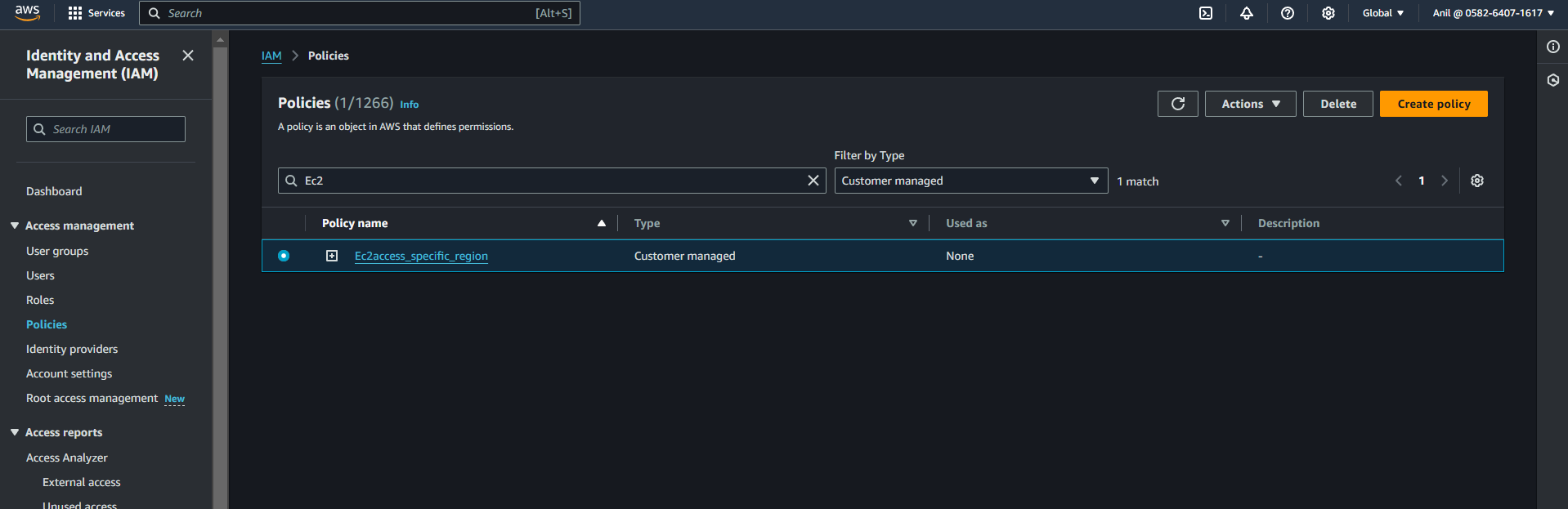
**4) Create a IAM policy to access ec2 for a specific user in specific regions only.**

#### 1. ****Create the IAM Policy****

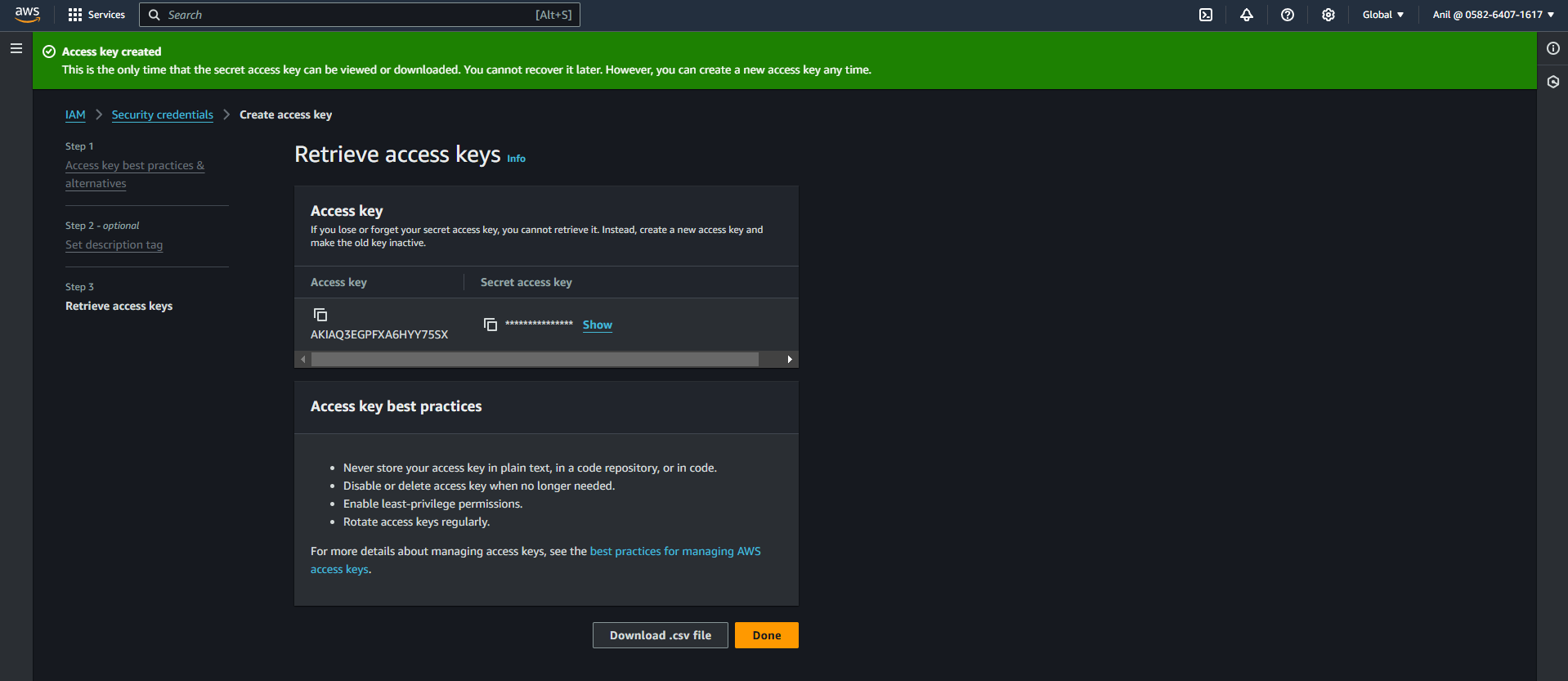
To create a custom IAM policy, follow these steps:

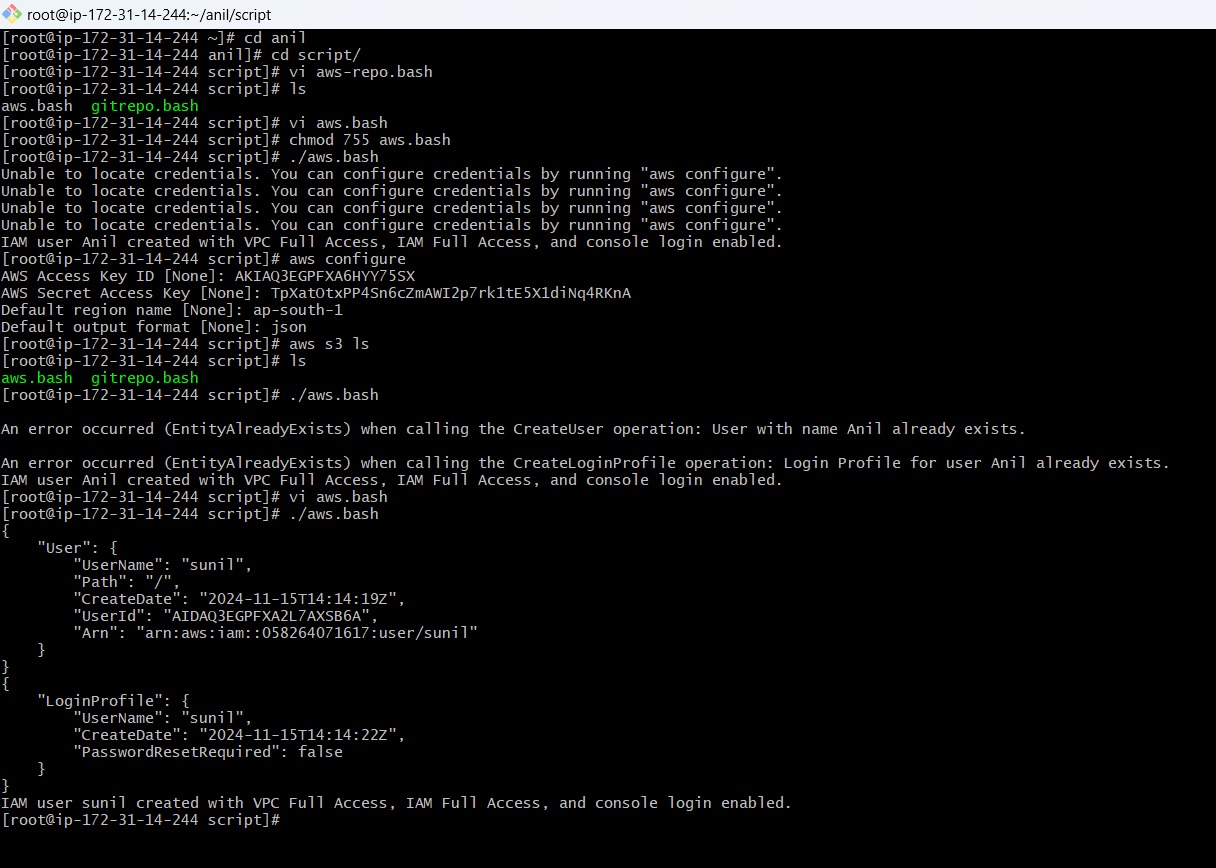
1. Log in to AWS Management Console:
   * Open the IAM service from the AWS Management Console.
2. Navigate to Policies:
   * In the left-hand navigation pane, click Policies under Access Management.
   * Click Create policy.
3. Choose JSON Editor:
   * In the "Create Policy" page, click on the JSON tab to directly input the policy in JSON format.
4. Define the Policy JSON: Below is an example of a policy that grants EC2 read-only access in specific regions (e.g., us-east-1 and us-west-2):

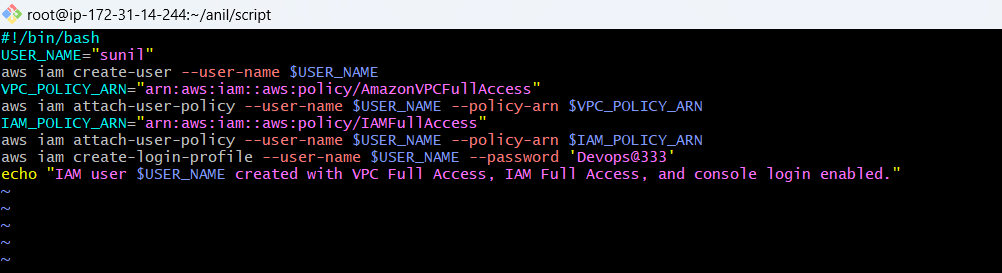
****

****

**5) Write a bash script to create a IAM user with VPC full access.**

****

****

****