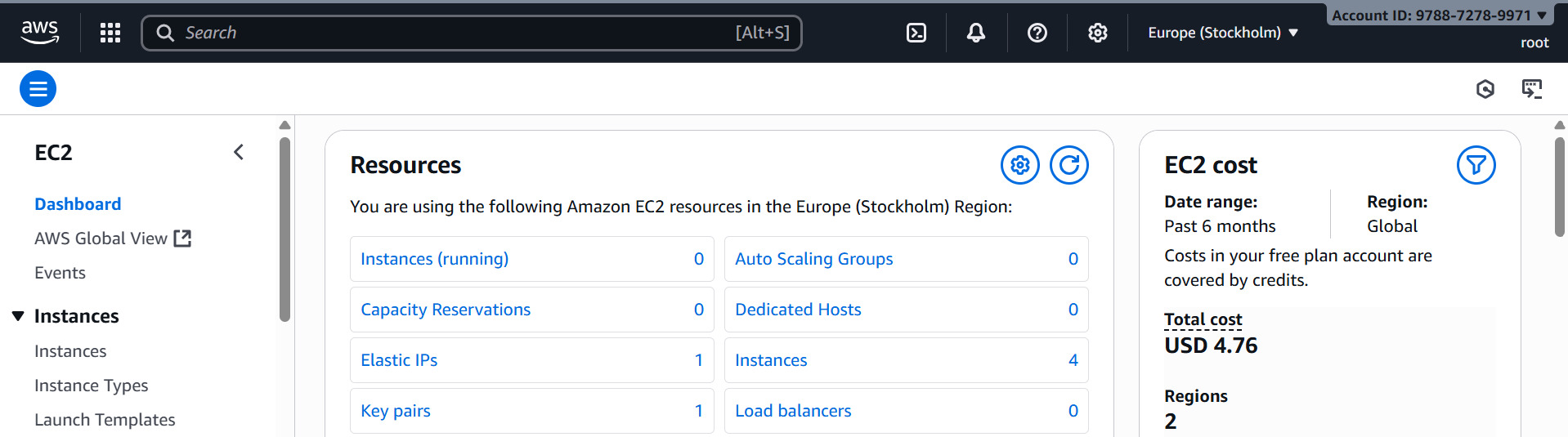
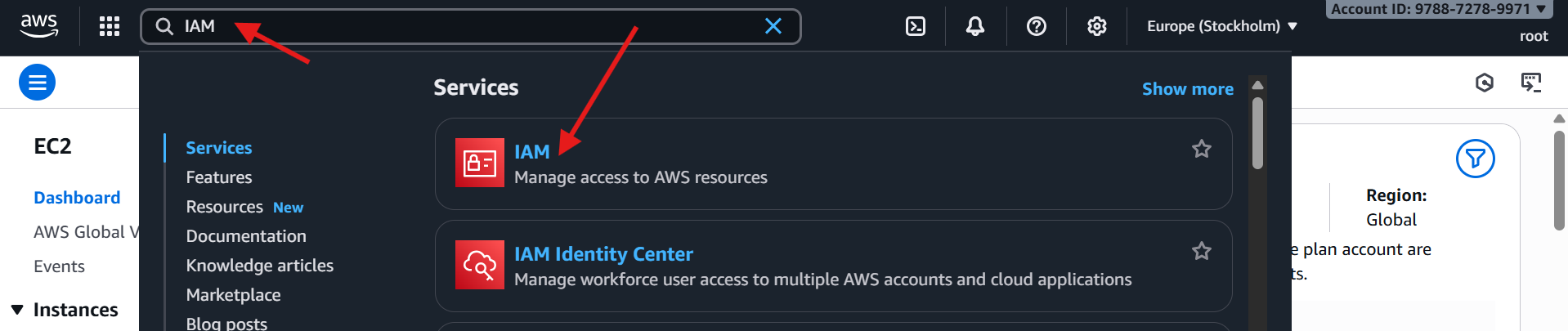
**IAM Daily Task ASSIGNMEN-1**

1. Create one IAM user and assign EC2 and S3 full access roles.

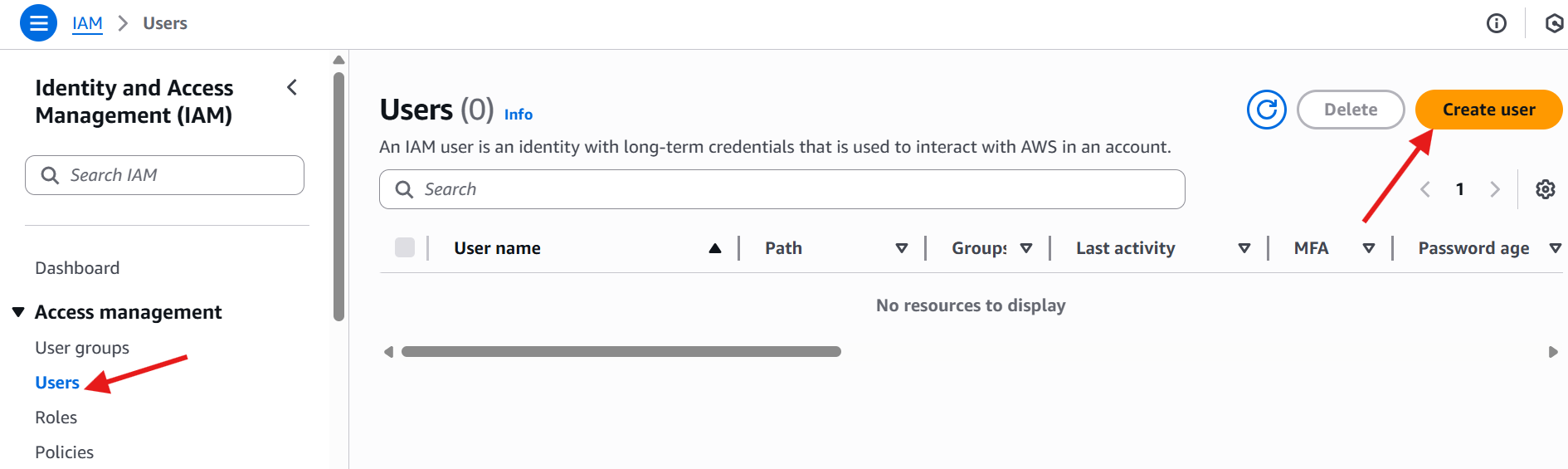
* Go to AWS Management Console.
* Sign in with your root or admin account.



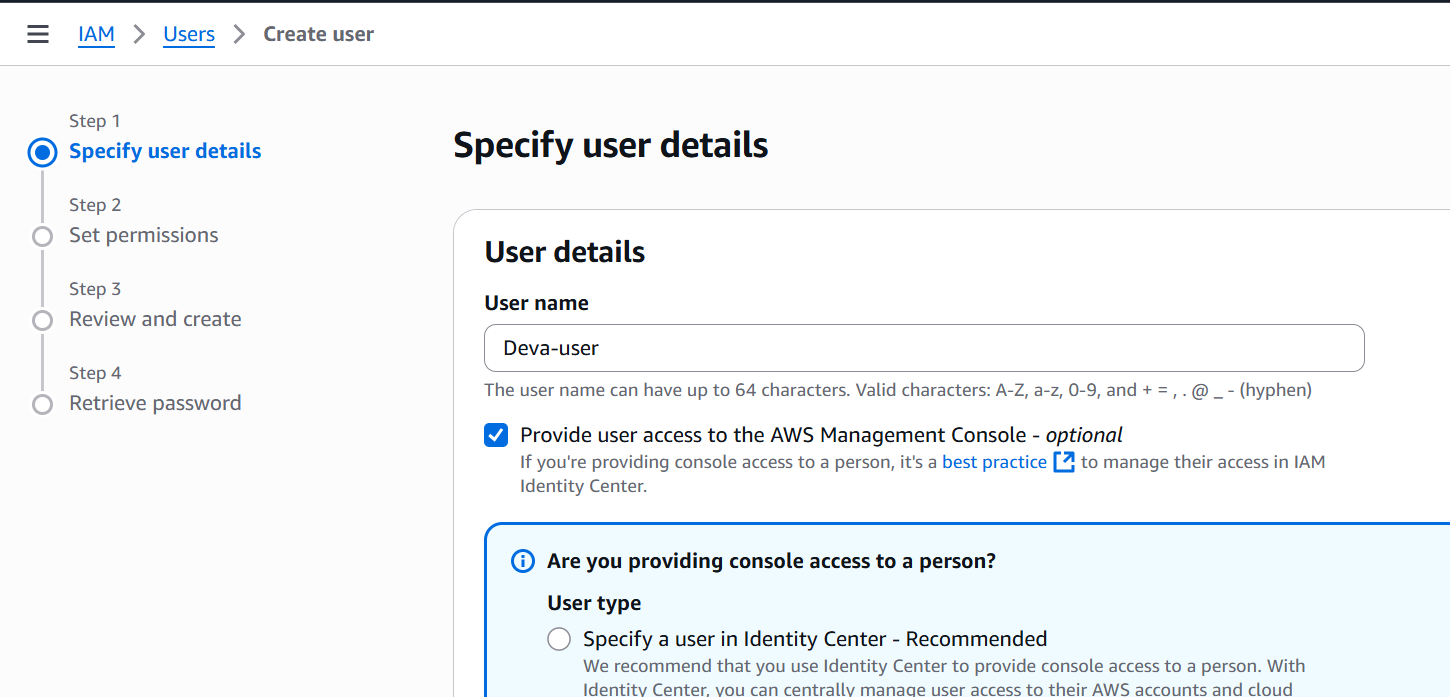
* In the search bar, type **IAM** and open it.

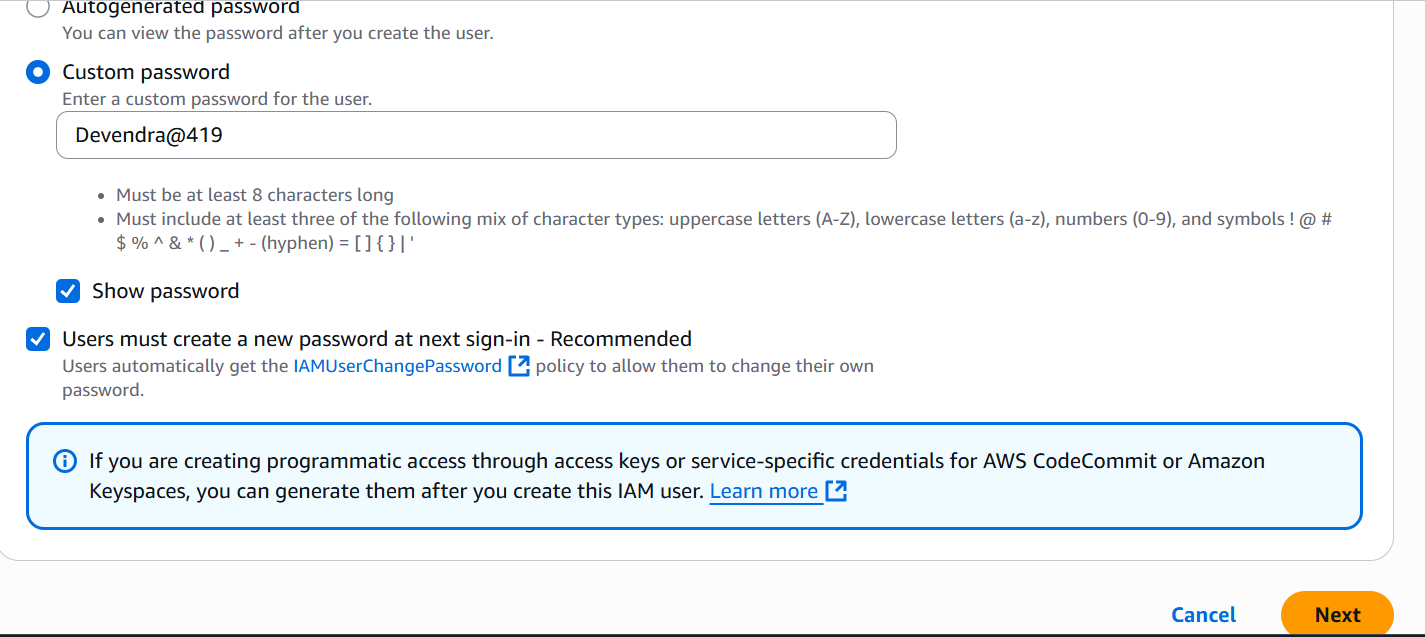


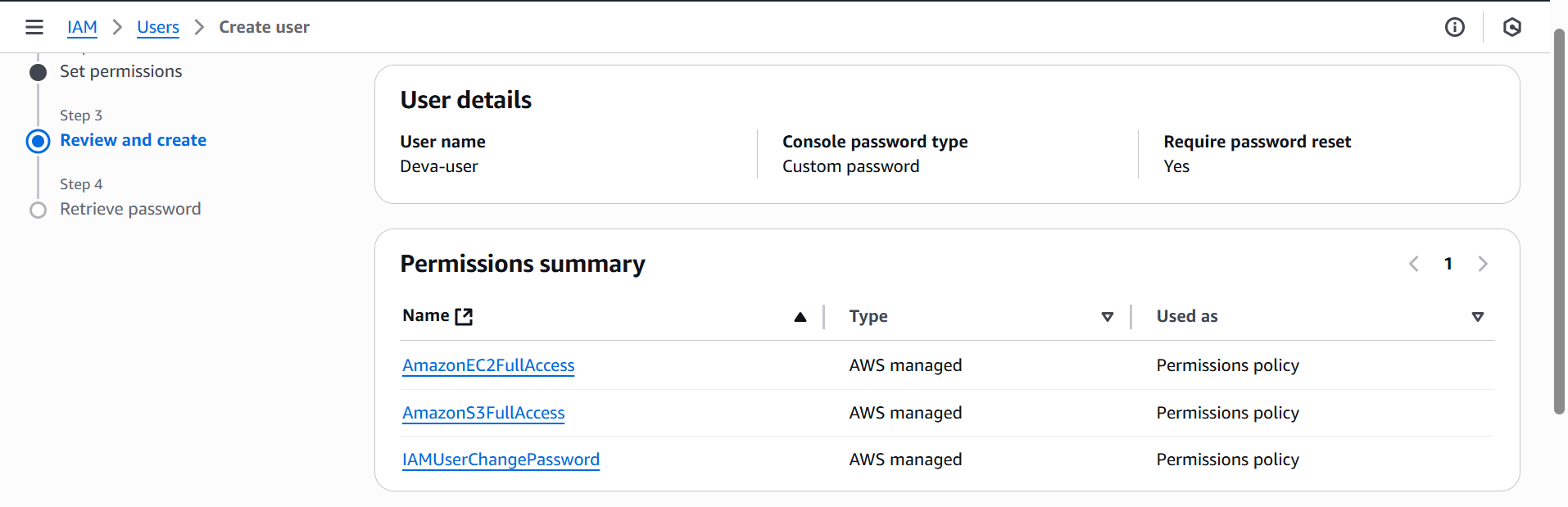
* On left menu, click **Users** → **Add users**.
* Enter **User name**

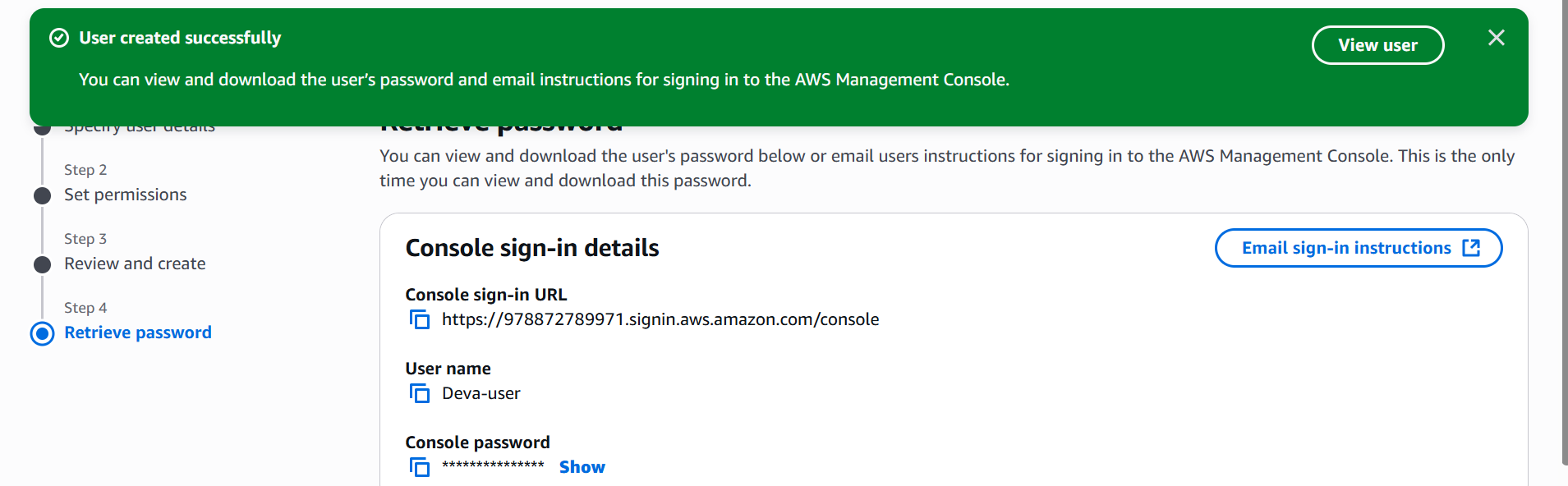


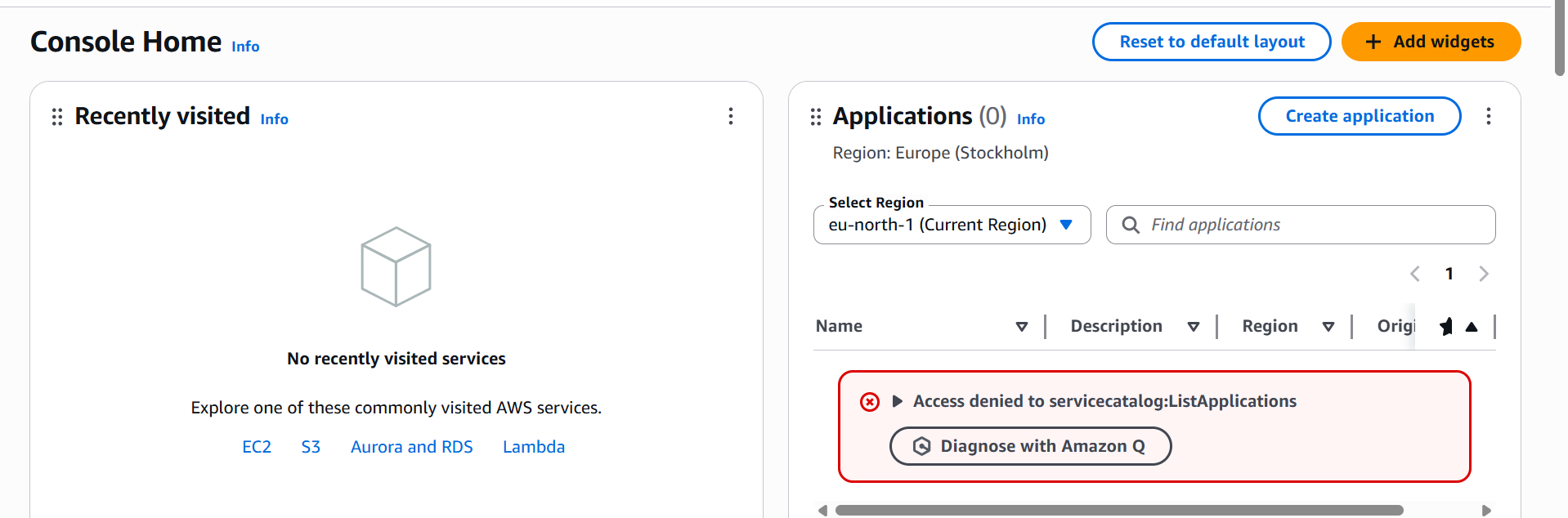
* Give user name deva-user
* And select provider user access to the AWS management console
* And select **custom password** and give password, this will help ypo for the accesskey and secreat key.
* Then gave permission step.
* Choose **Attaching existing policies**
* Open a search bar and >>
* **Ec2 full access**
* **S3 full access**

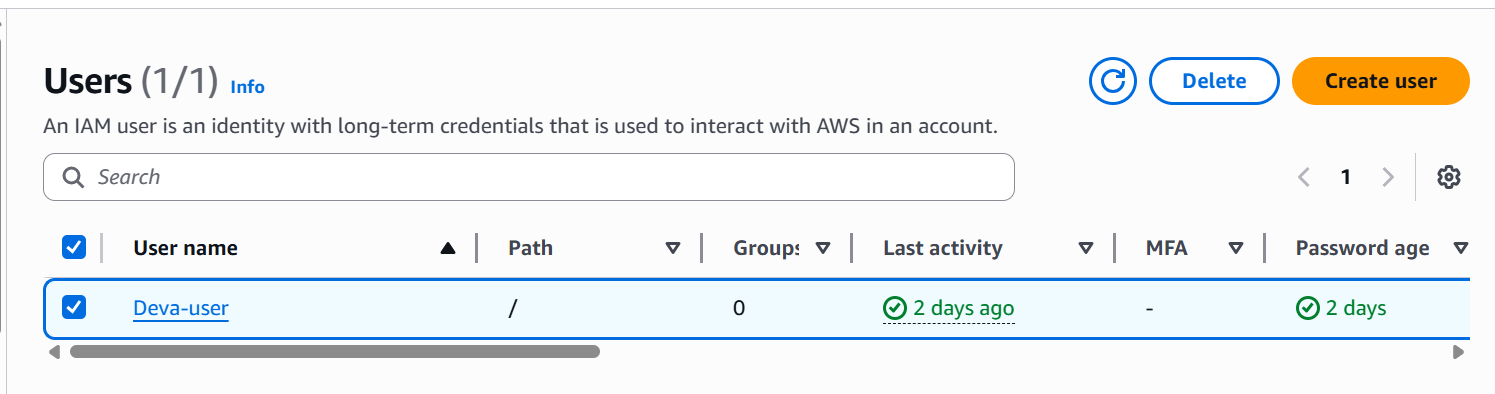






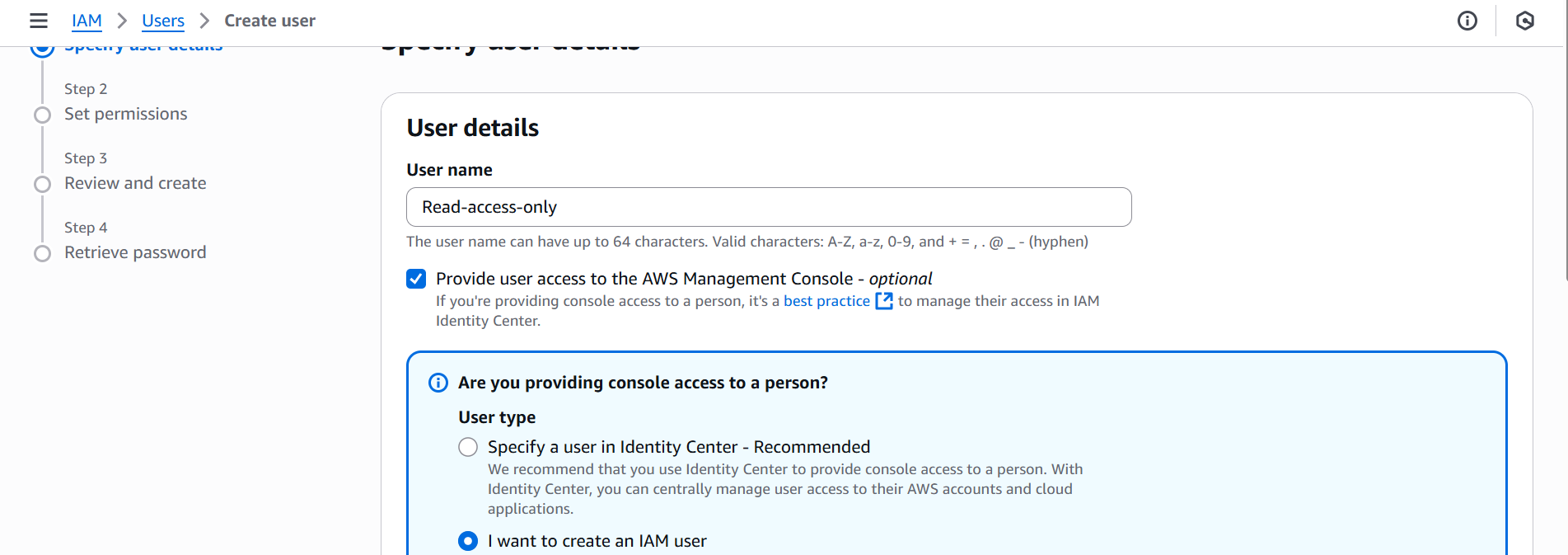


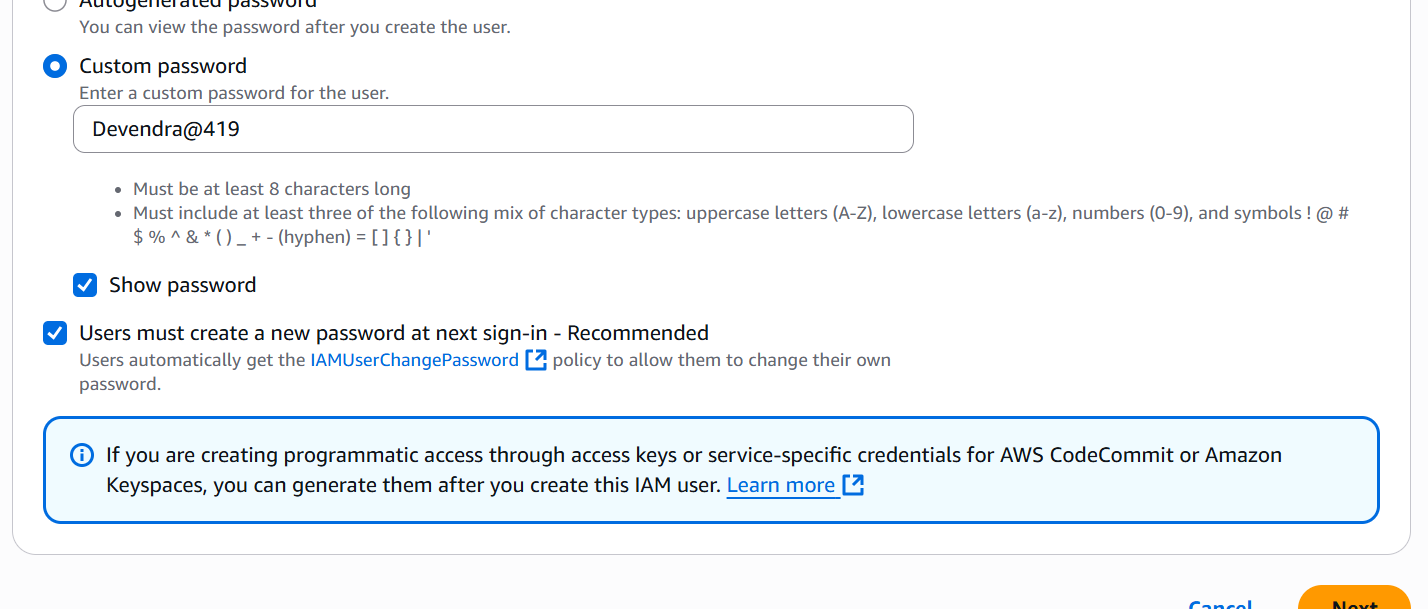




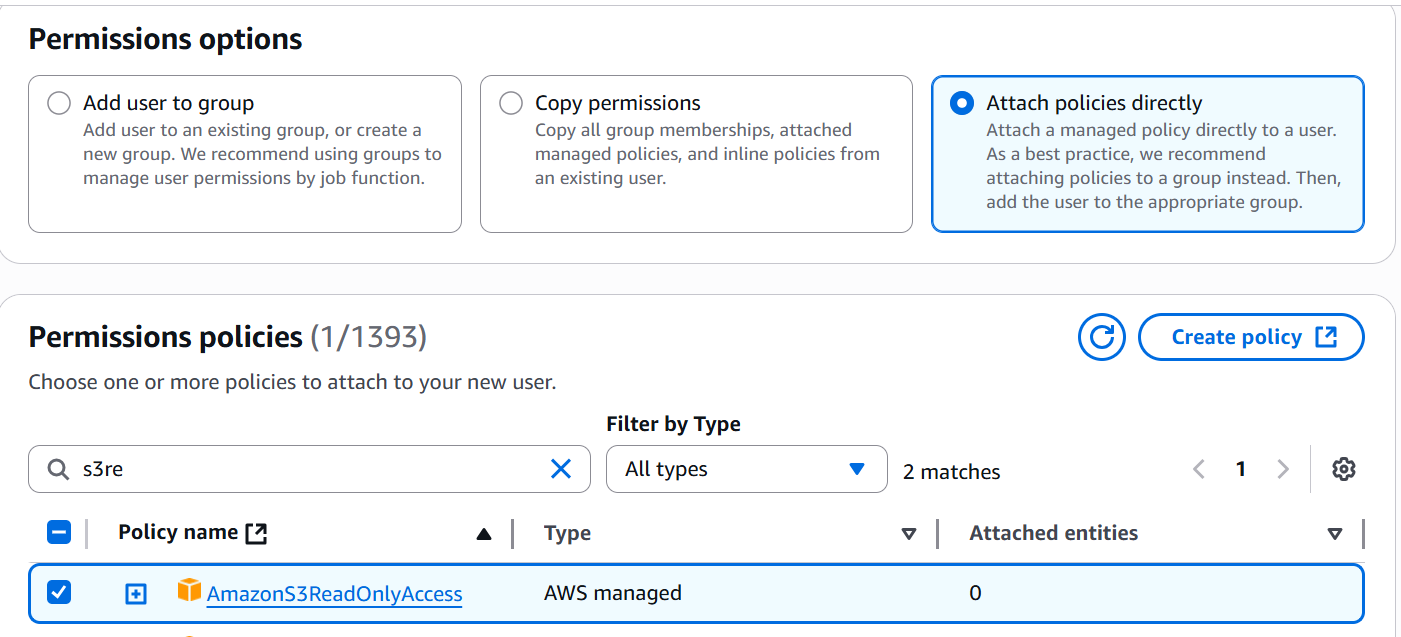
1. Create one group in IAM and assign read access for EC2.

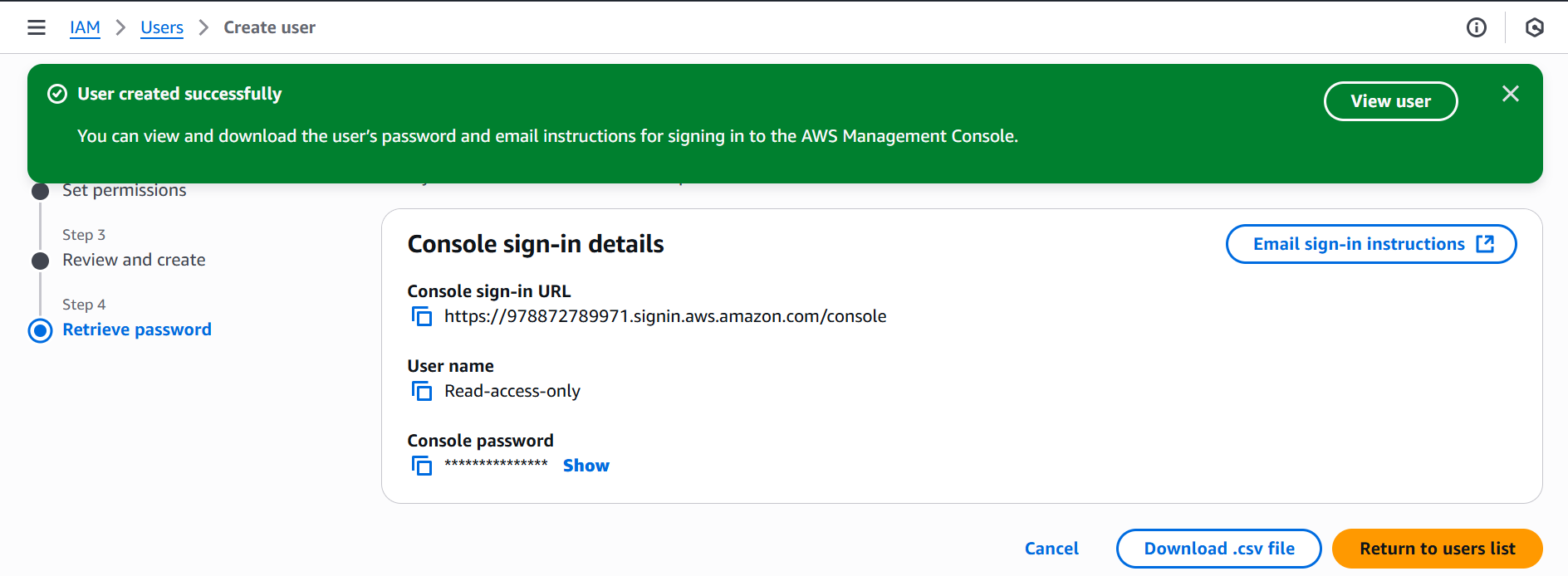
* Go to **AWS ec2** then open a search bar and enter **IAM.**
* Then create a user
* Gave a name to the user **read-access-only.**
* Then gave provide access console aws.
* Then create password.
* Click the **next page.**

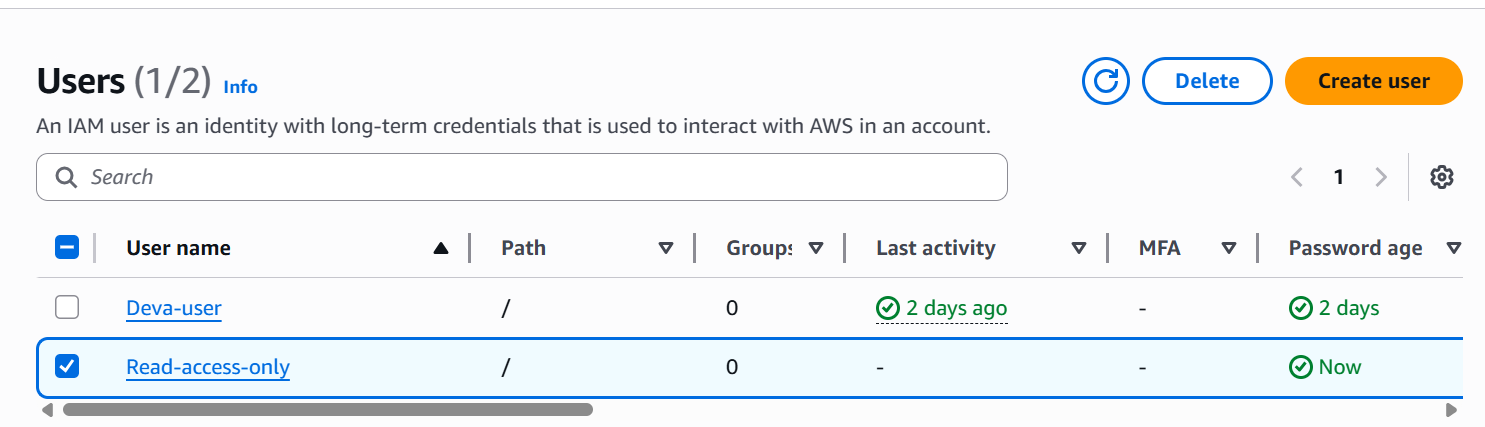




* Then existing permissions.
* Then ec2read access only.
* Review
* And create user successfully

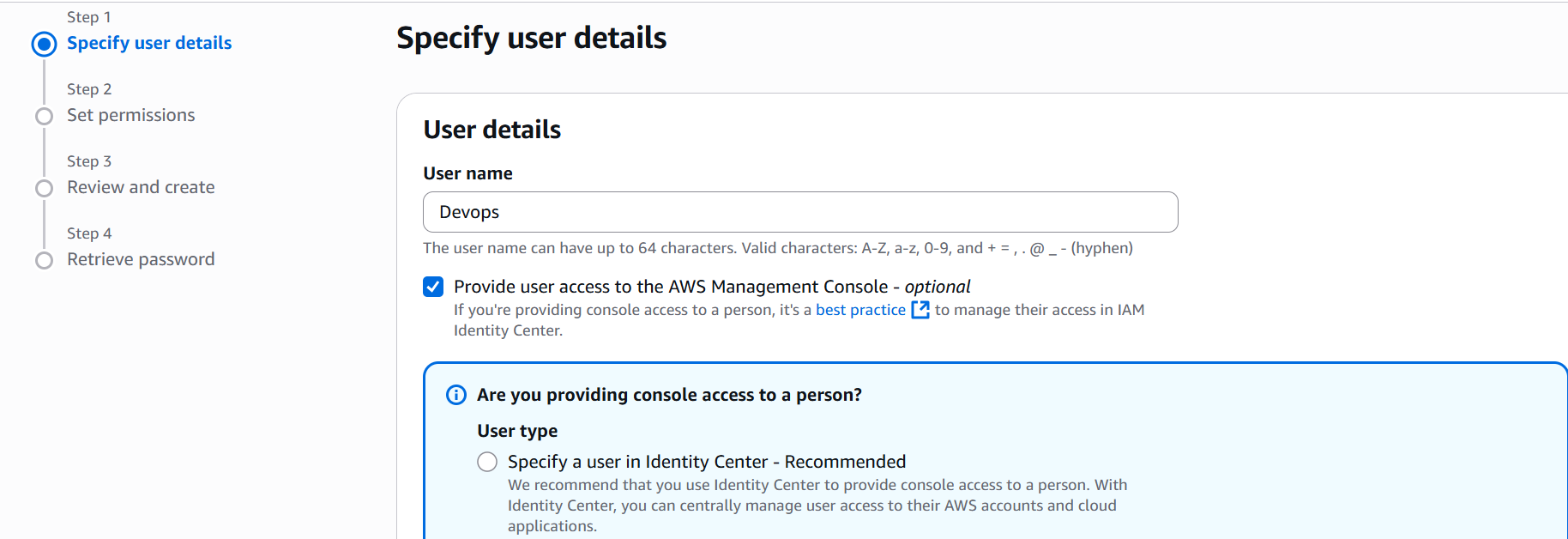


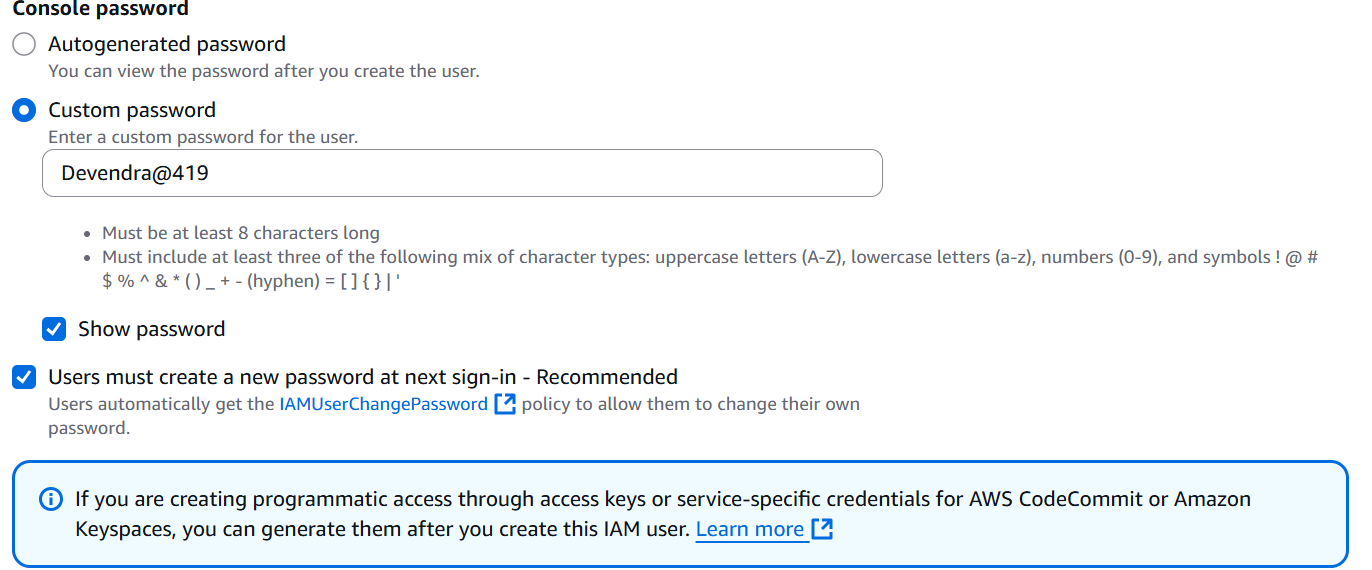




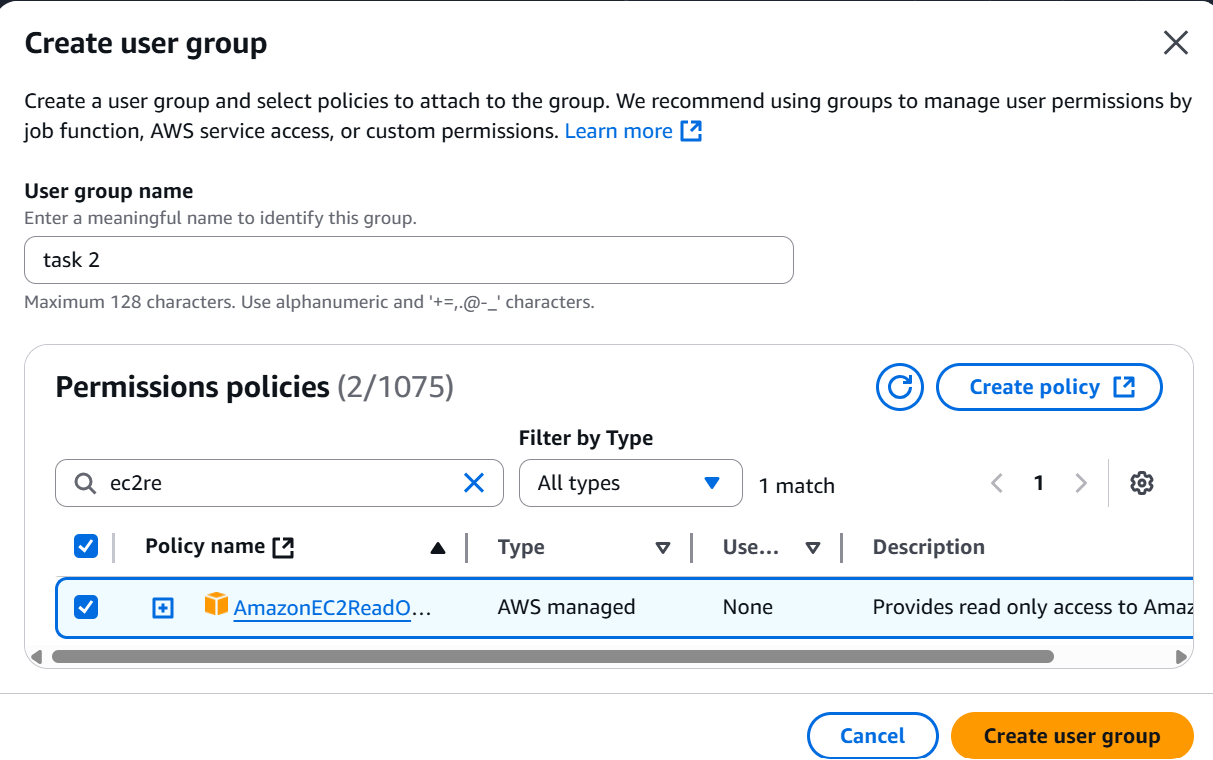
1. Create a new user named "Devops" and add to the group created in task 2

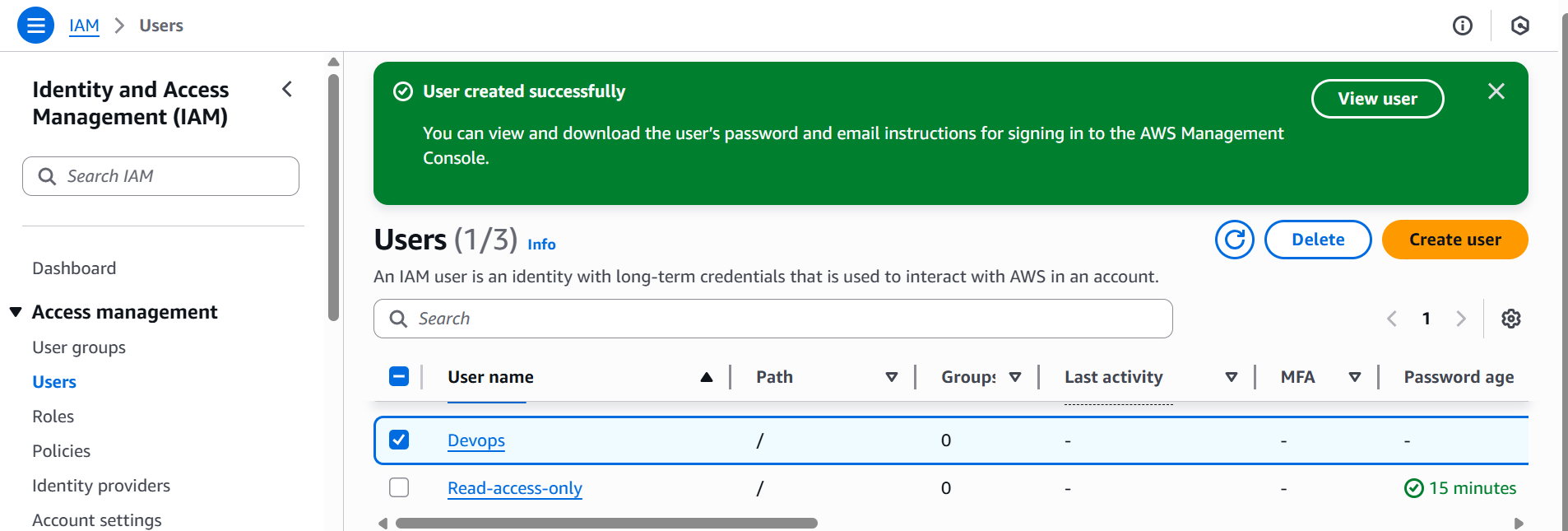
* Go to AWS ec2 then open a search bar and enter IAM.
* Then create a user.
* Give a name to the user read access.
* And provide access control aws
* Then create password
* Click on next page.
* Then set permission for add user group and create a group and gave a permission of ec2 read access only.





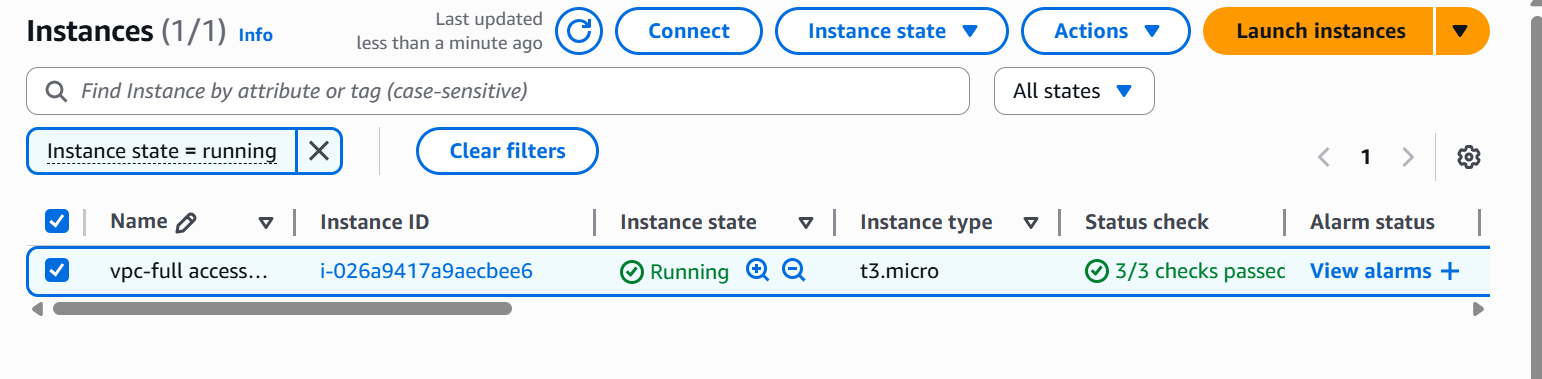
* Create a group name task2
* And review the page
* Group and user will create:
* Here the results are



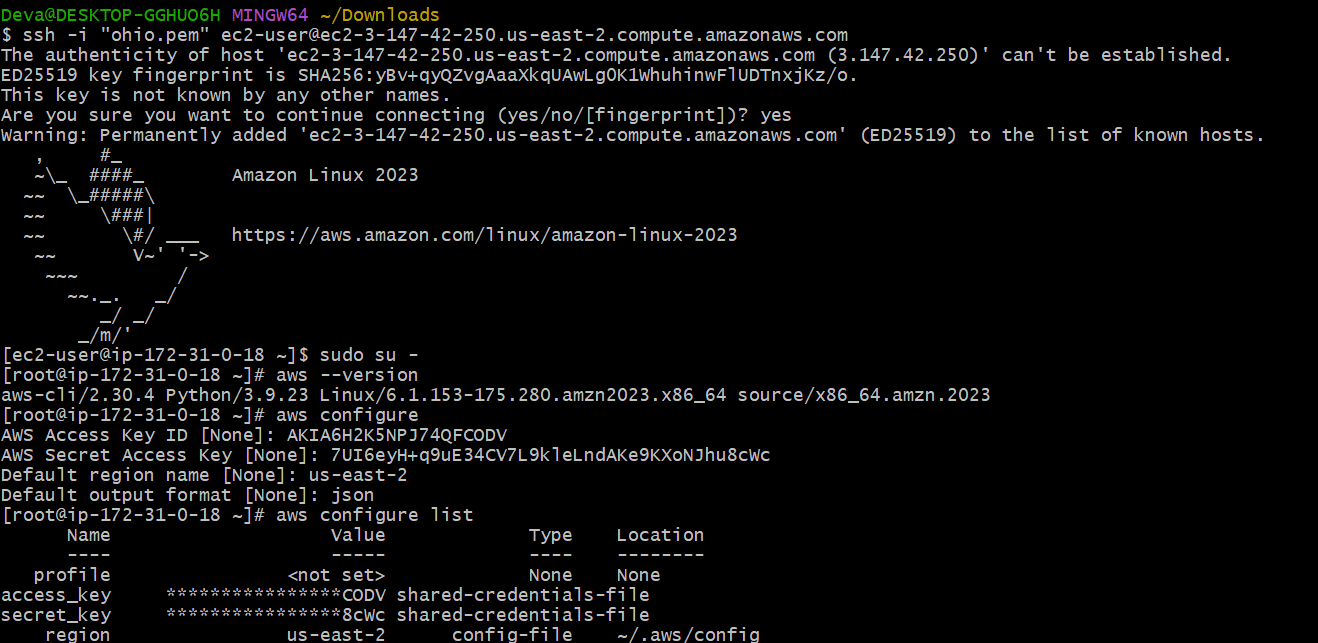


1. Write a bash script to create an IAM user with VPC full access

* Go to ec2 console launch one instance



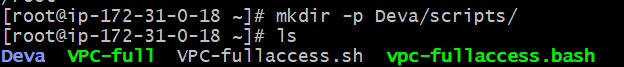
* Connect to git bash using **ssh-I ohio.pem ec2-user@<public ip>**
* Go to root user
* Check the aws version : **aws –version**
* Check the aws configure list



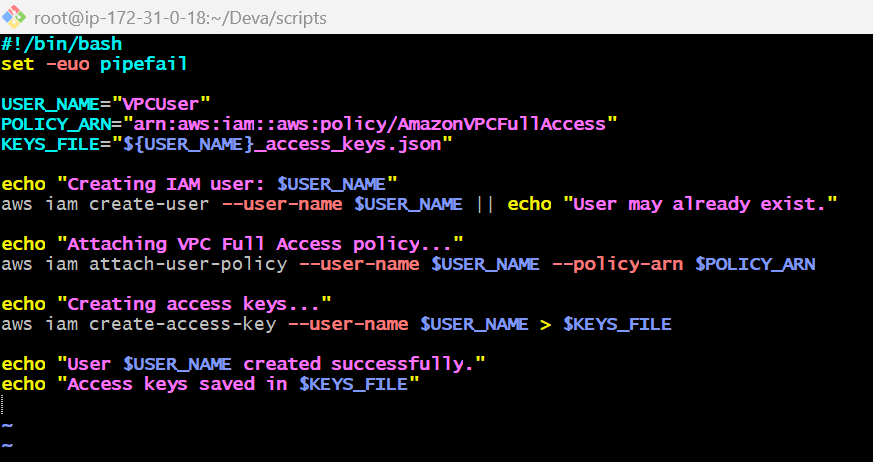
* Go to bash shell : **echo $0**



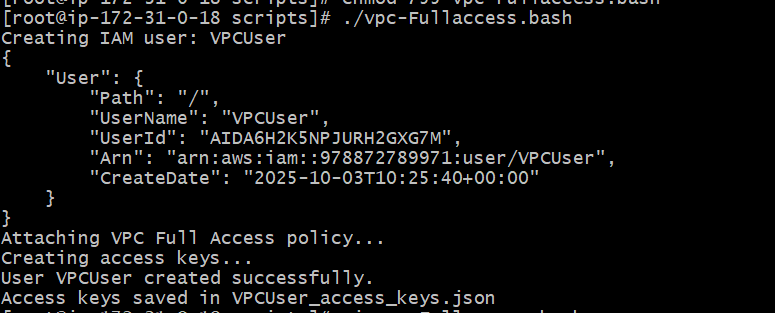
* Create one path for storing scripts : **mkdir –p Deva/scripts/**



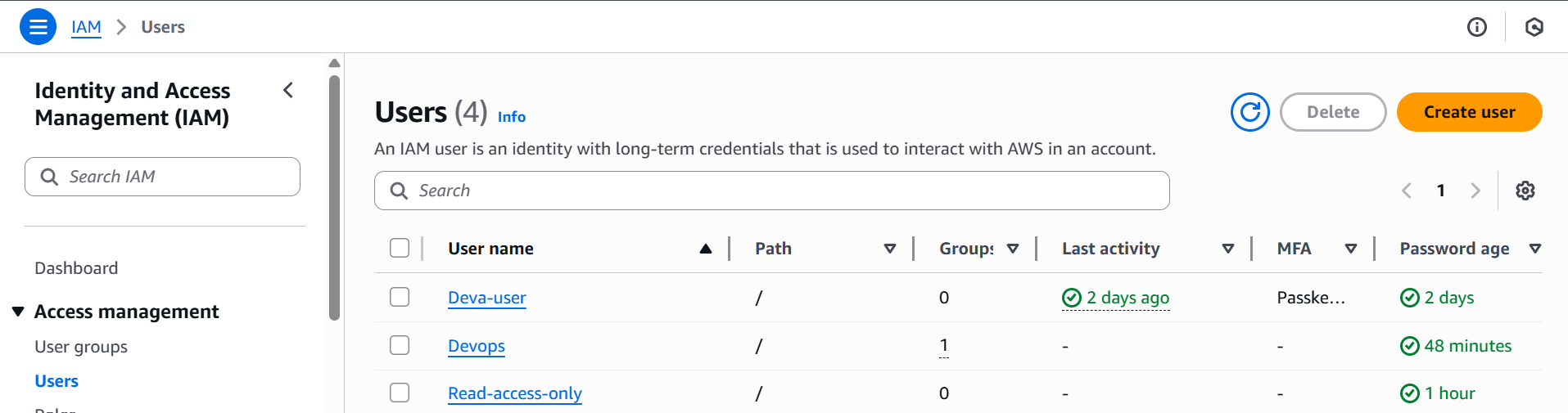
* + Create and open one file **vi <filename>**
  + Write the script to create an IAM user with VPC full access.
  + Give permissions to that file **chmod 755 <file name>**
  + Execute the script: **./<filename.bash>**

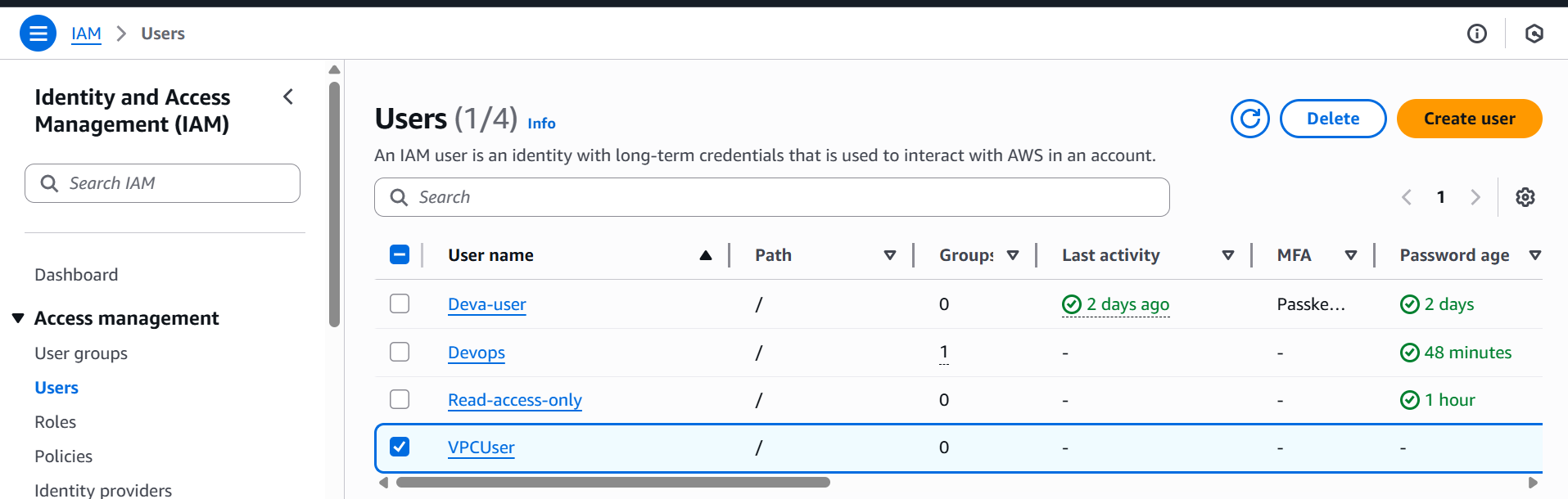






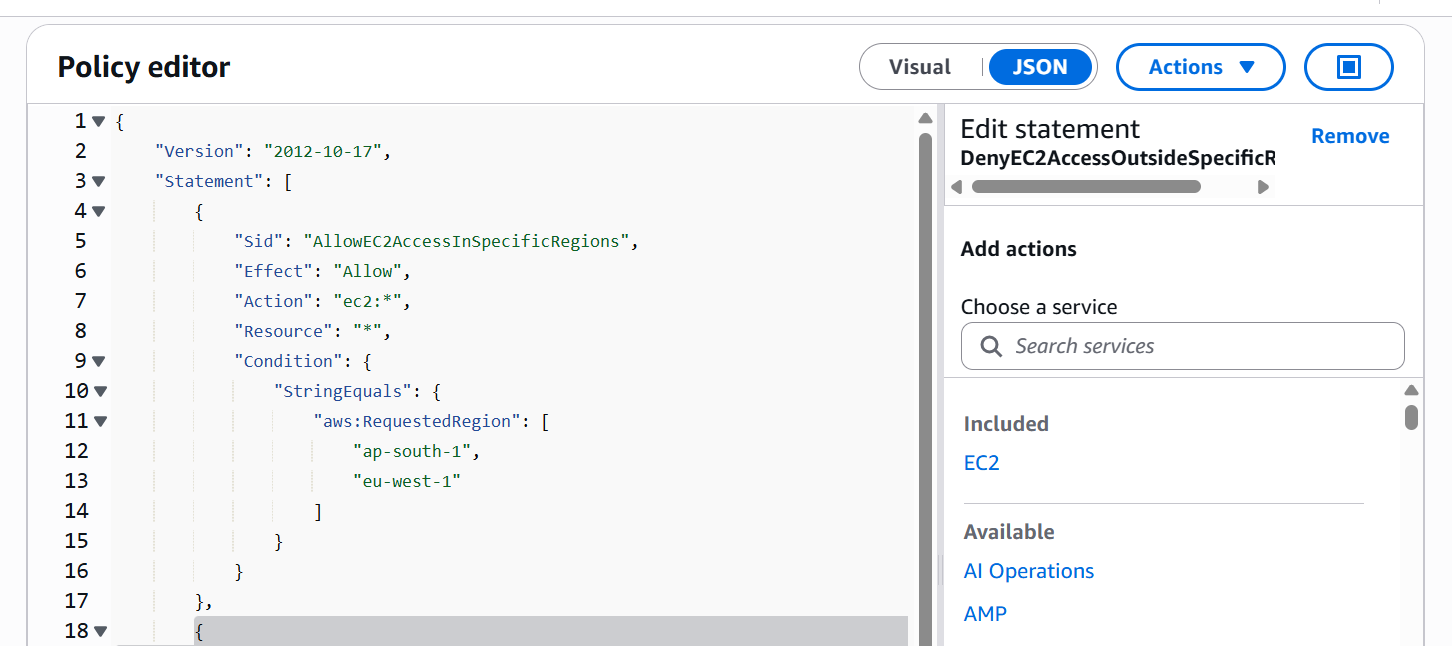
* + And go to IAM and check the user created or not
  + Refresh the page you can see the user



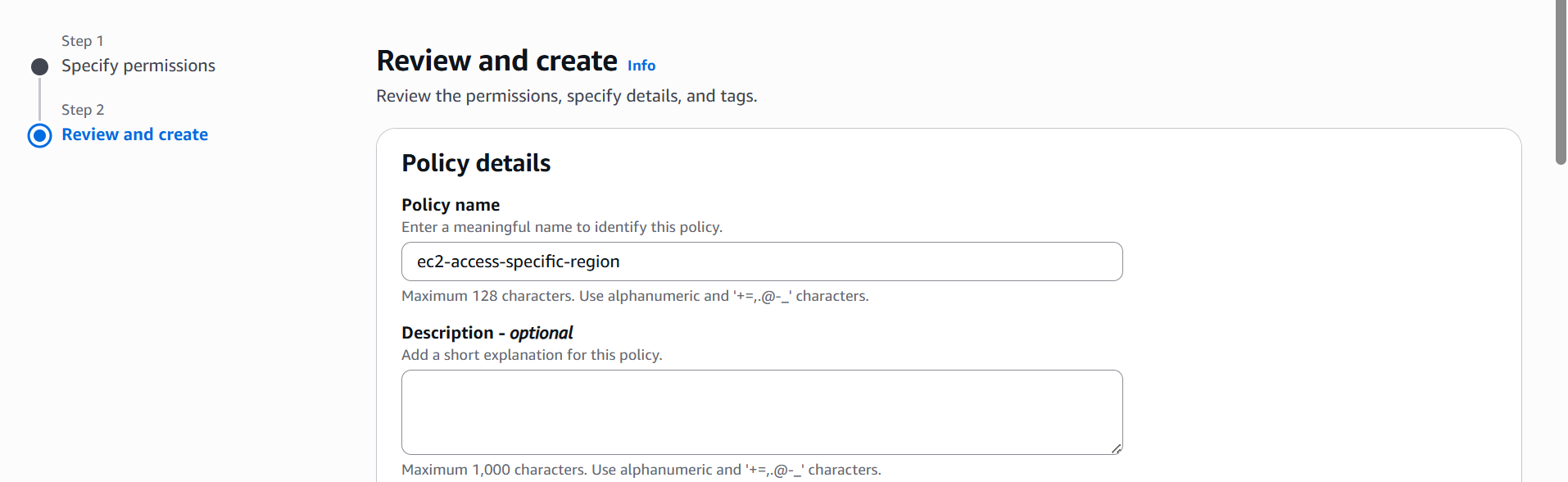


1. Create an IAM policy to allow EC2 access for a specific user in specific regions only

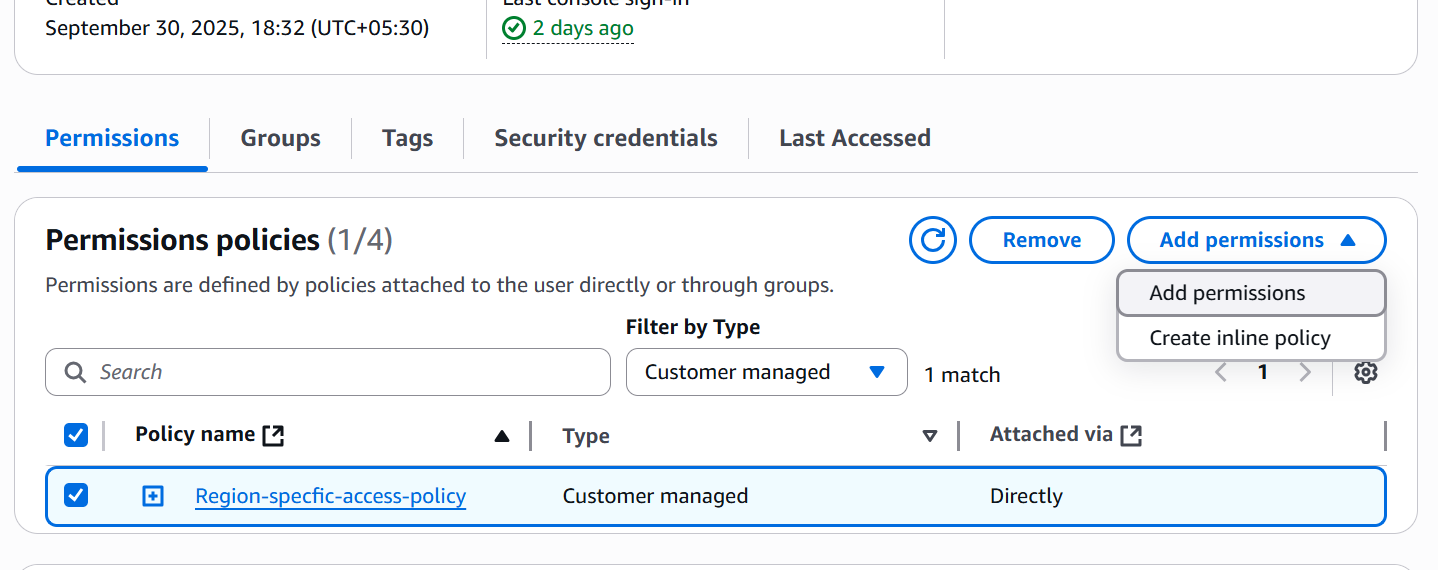
* Go to IAM
* Click on policies
* Click on create policies
* Select json
* Write the policy script
* Click next



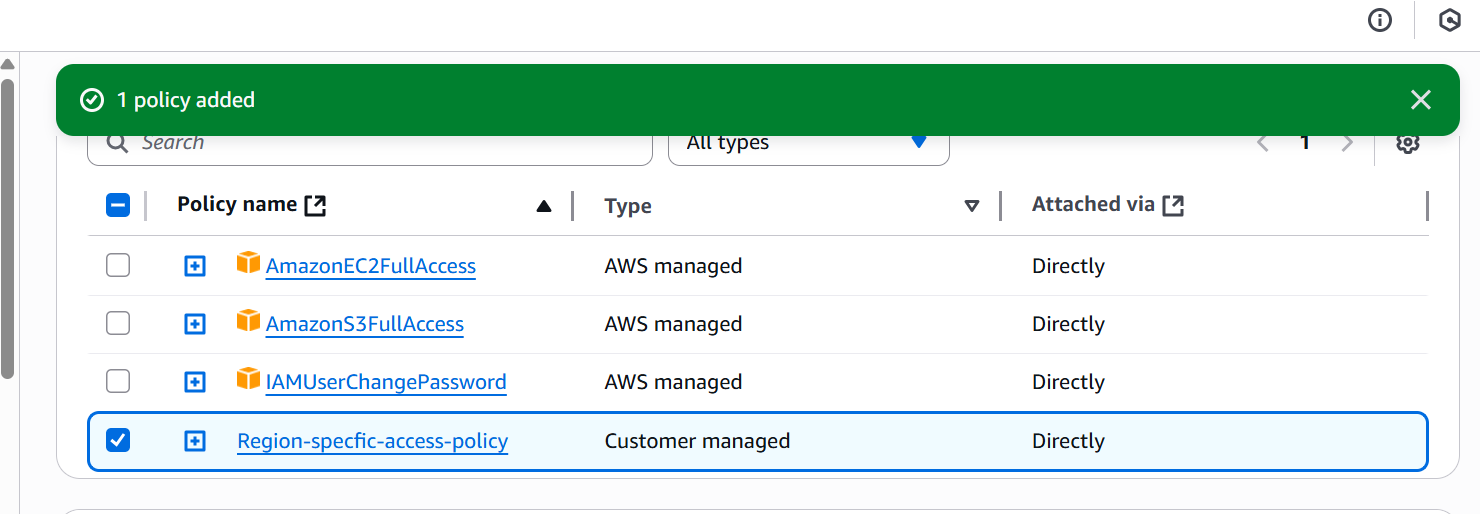
* Review and select create policy

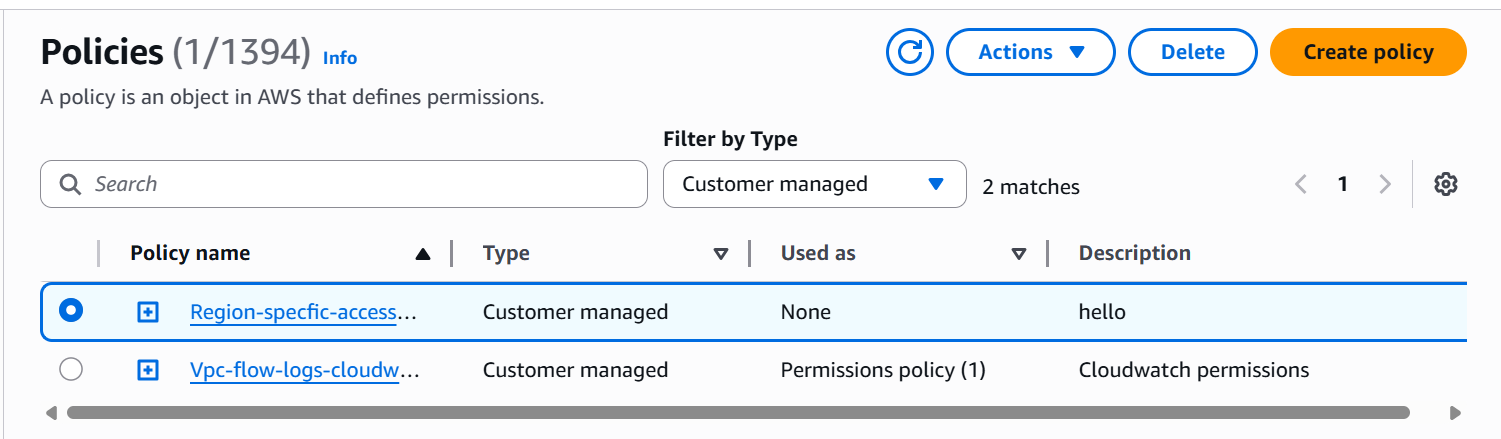


* Go to users
* Select user 🡪 select add permission under add permission



* Select attach policies directly and select policy name 🡪click Next





1. We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.