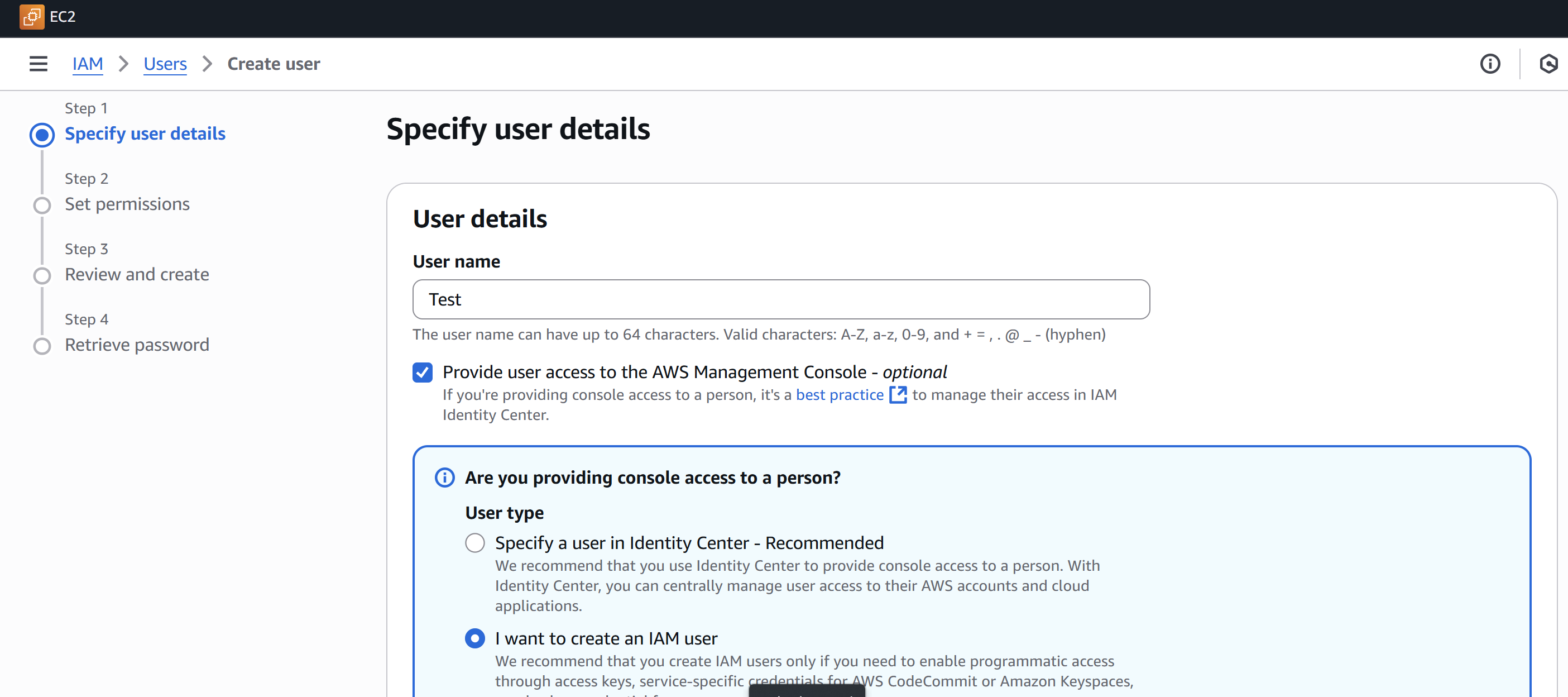
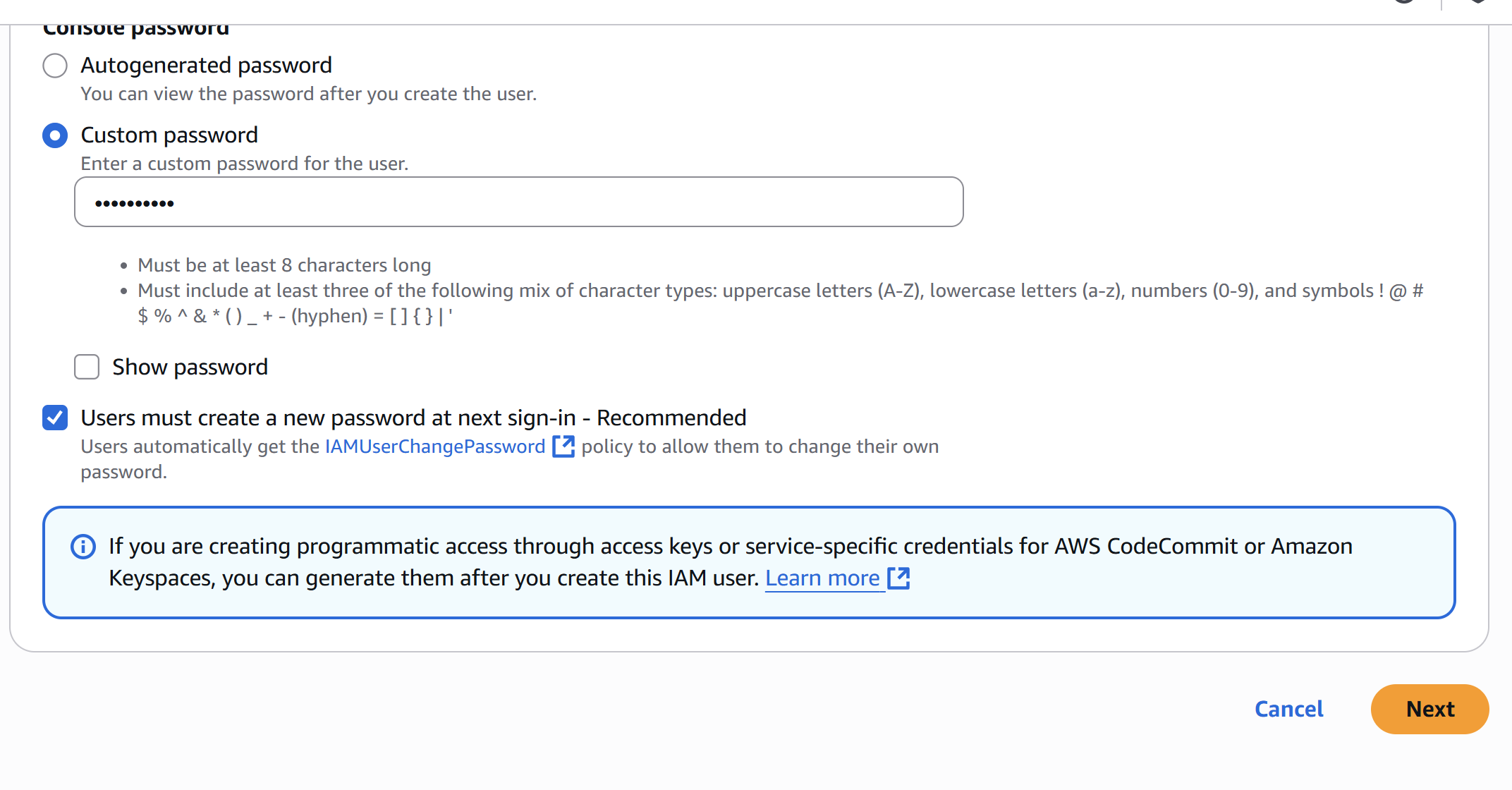
**IAM**

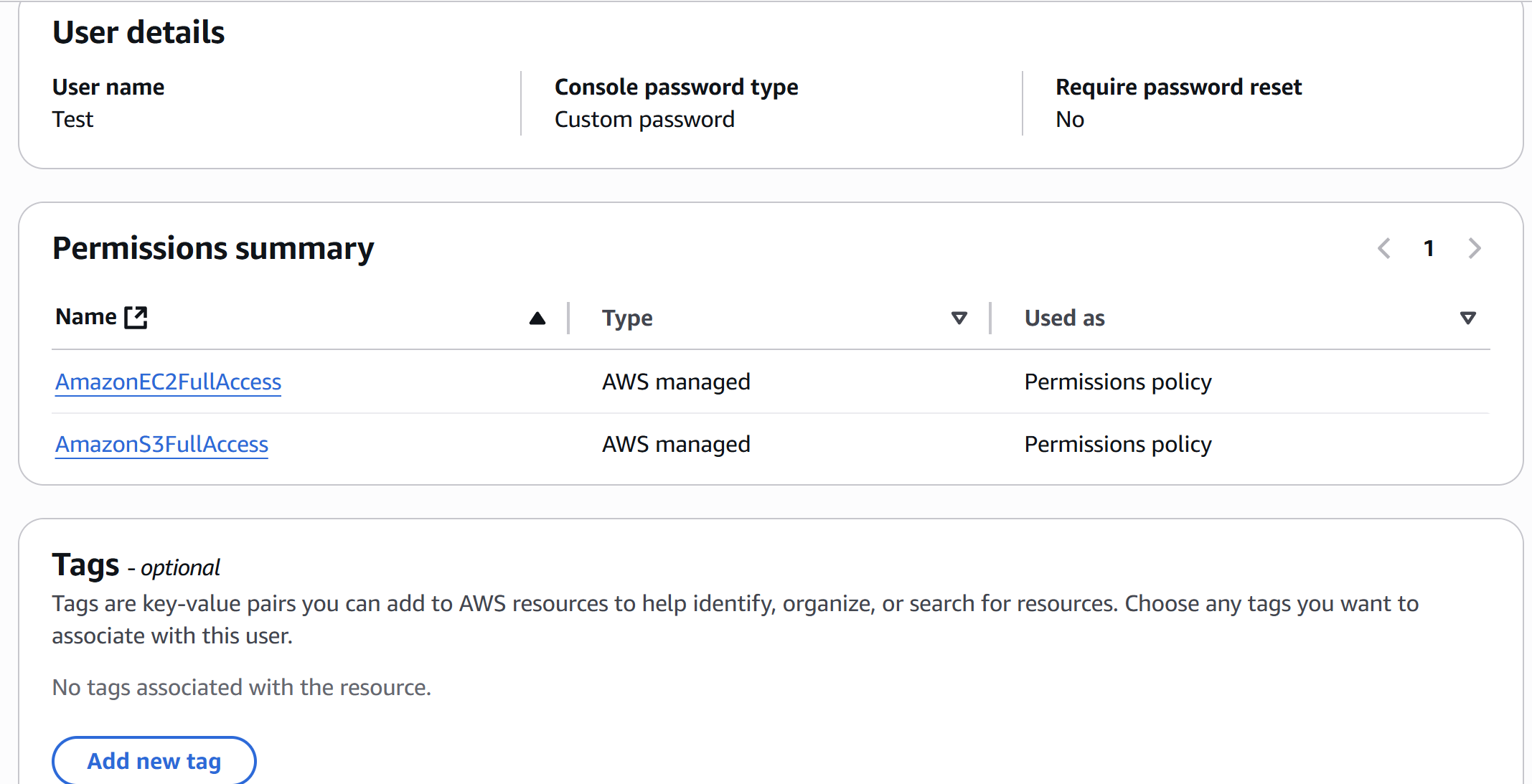
1) Create one IAM user and assign ec2,s3 full access role.

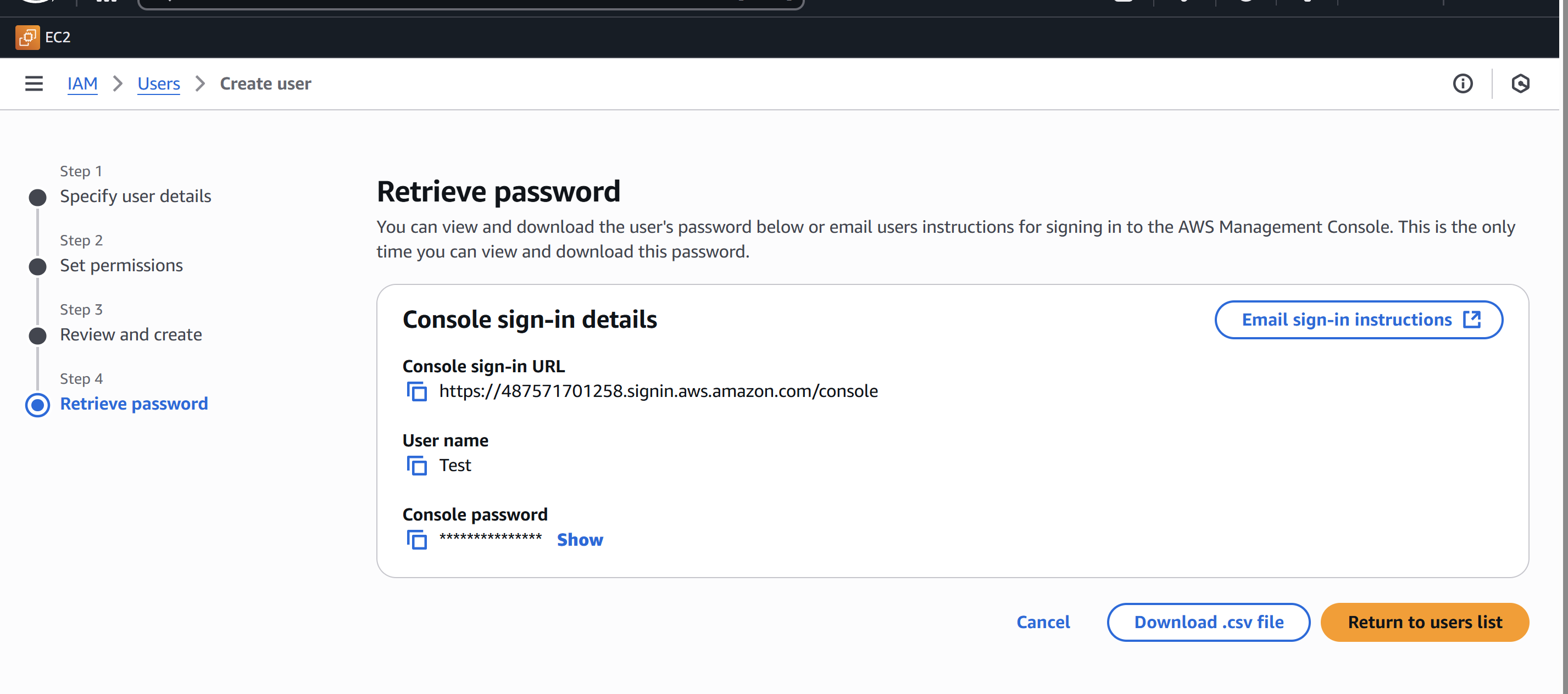
* Go to **IAM**
* Go to **Users**
* User name as **Test**

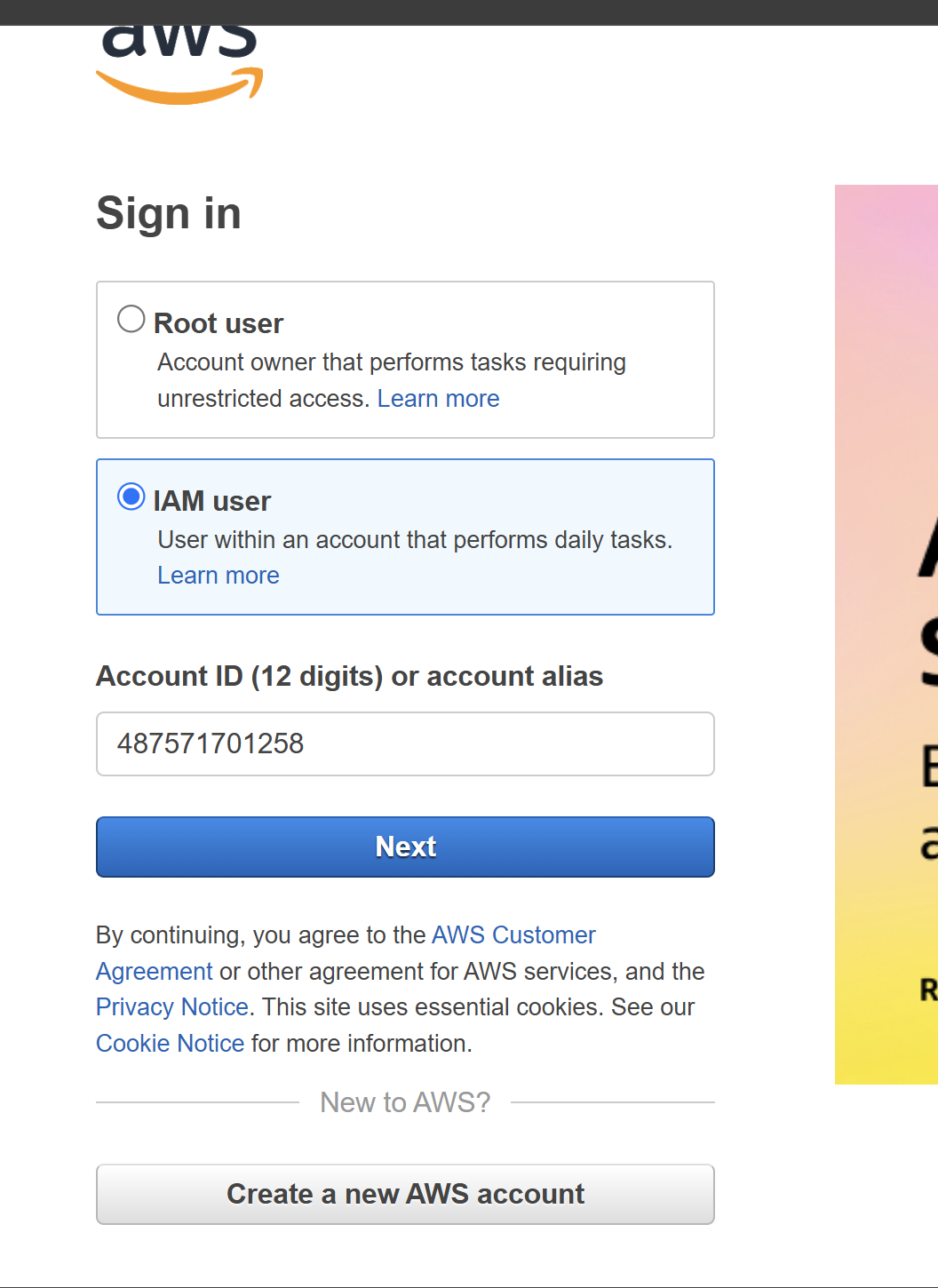


* Selected as Custom password



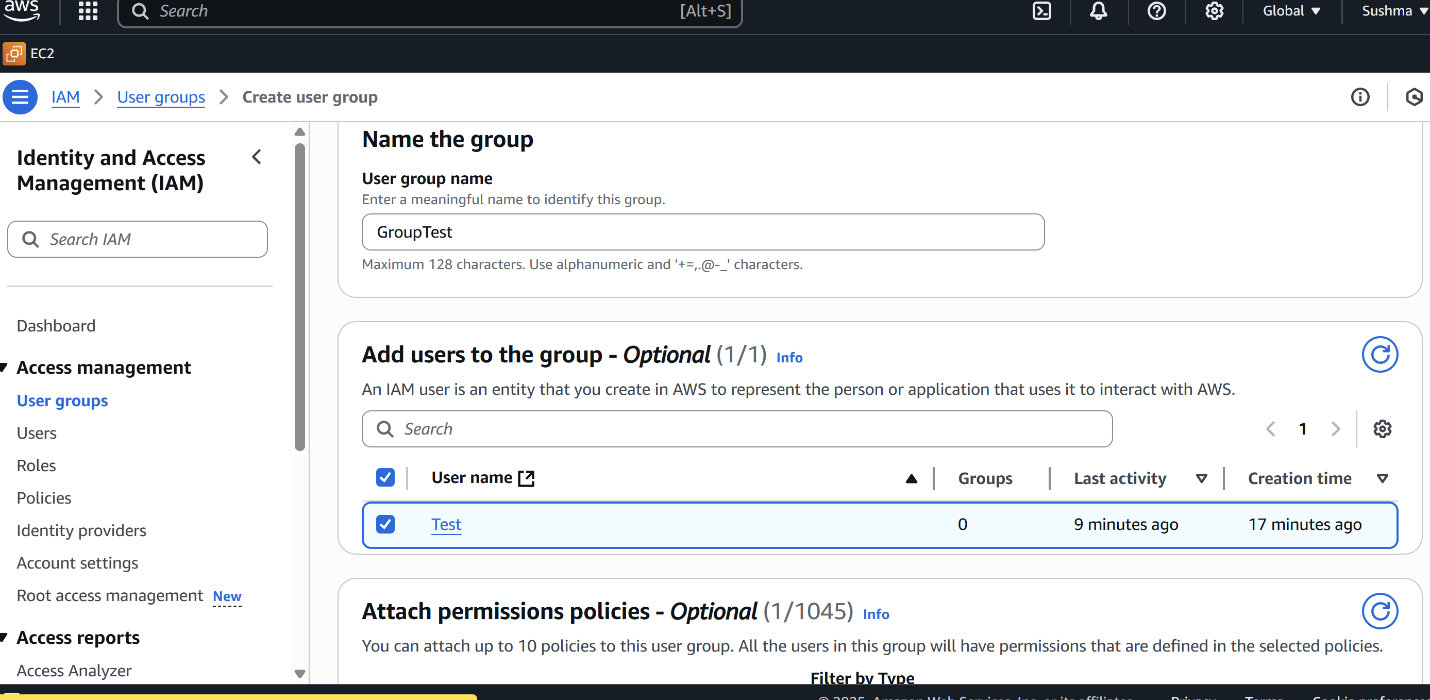




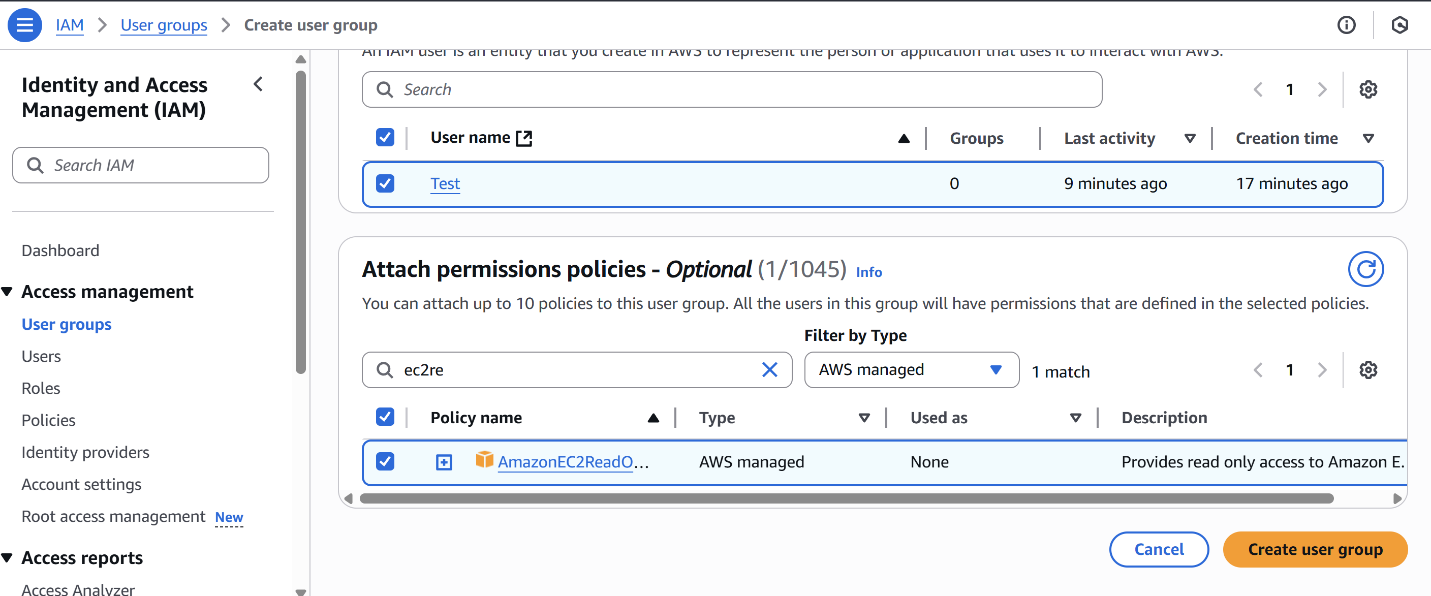


2) Create one Group in IAM and Assign Read access for ec2.

* Go to **IAM**
* Go to **User Group** named as **Group Test**



* Add the user which we want to add here I have added **Test** user

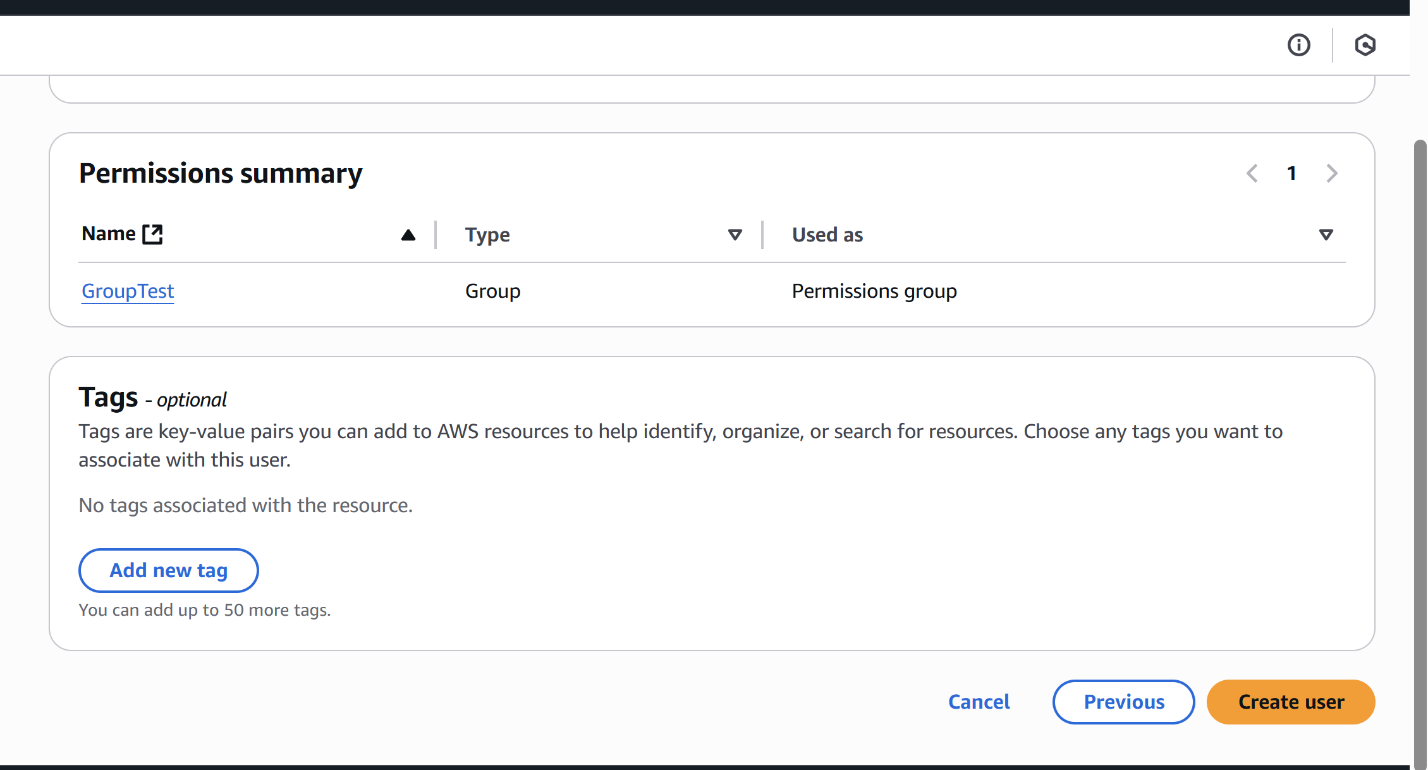


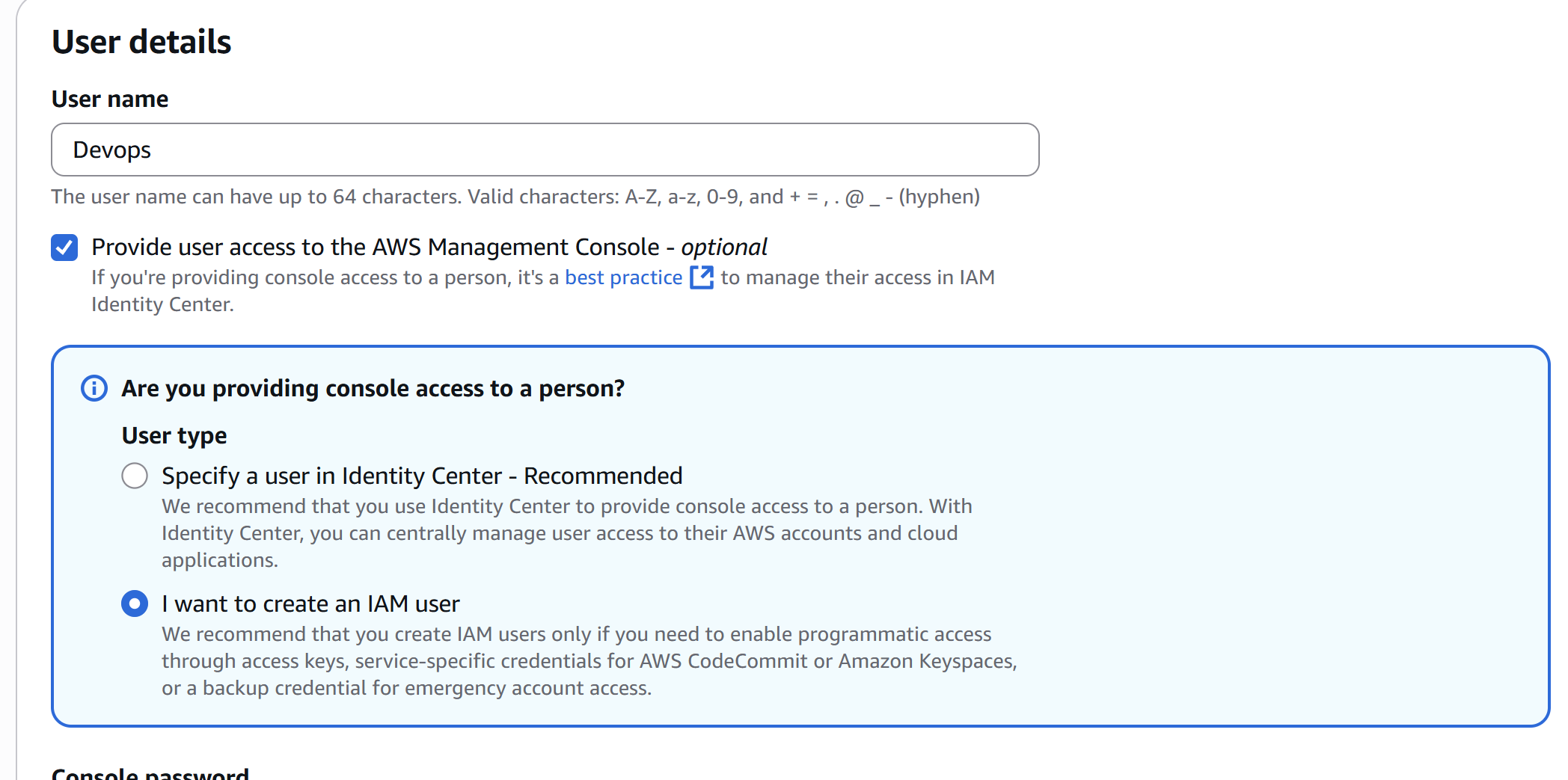
* Add the Policy of **Read acces for EC2**
* Then create the group.



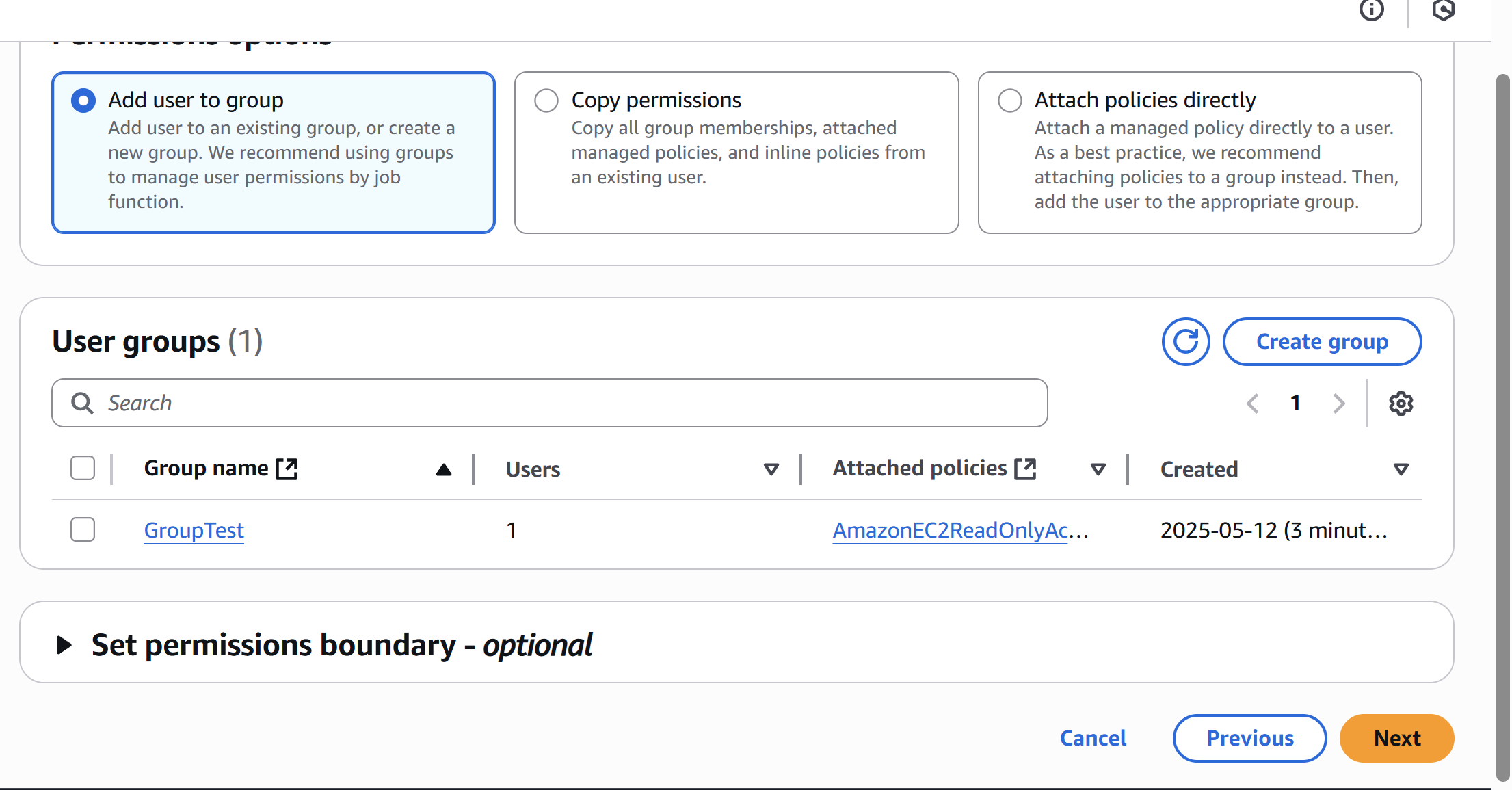
3) Create a new user with name Devops and add to the group created in task2.

* Create the user **Devops**

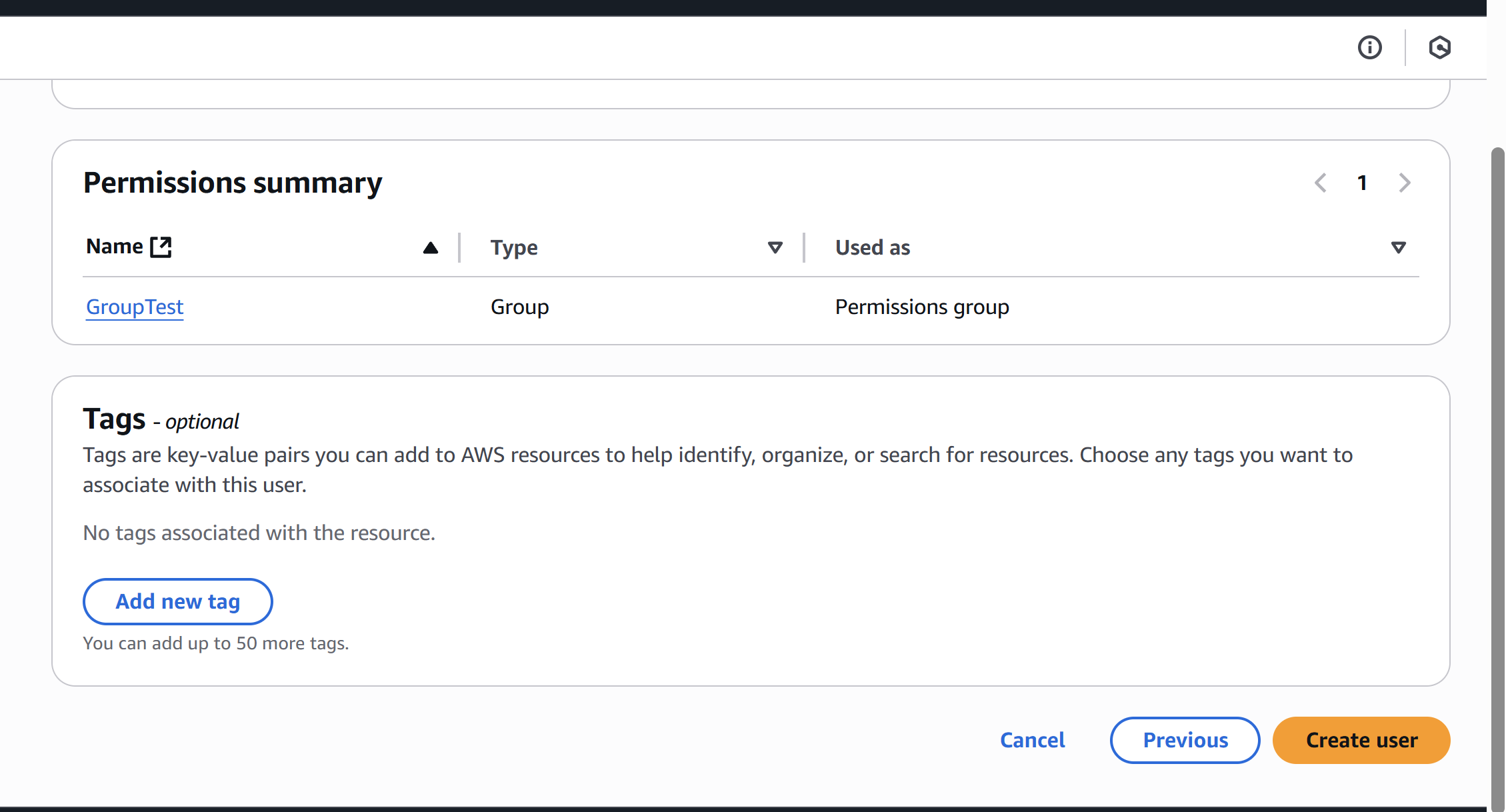


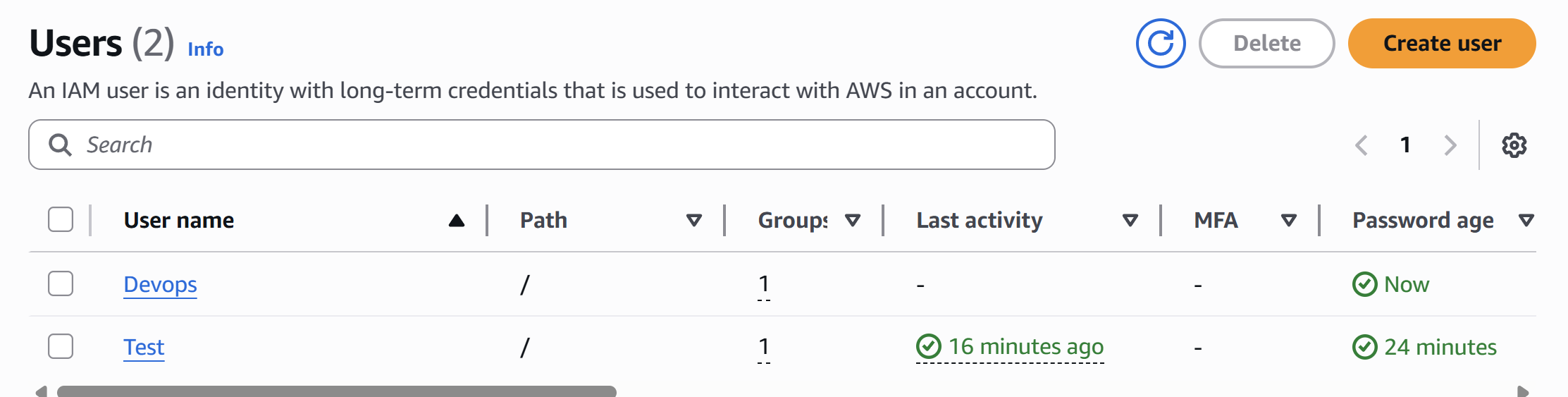


* Here I am adding the user to the group which is previously created (**GroupTest)** by selecting the option as **Add user to group.**
* Now select the group **GroupTest.**



* Now create the user then it will added to the **GroupTest** group.





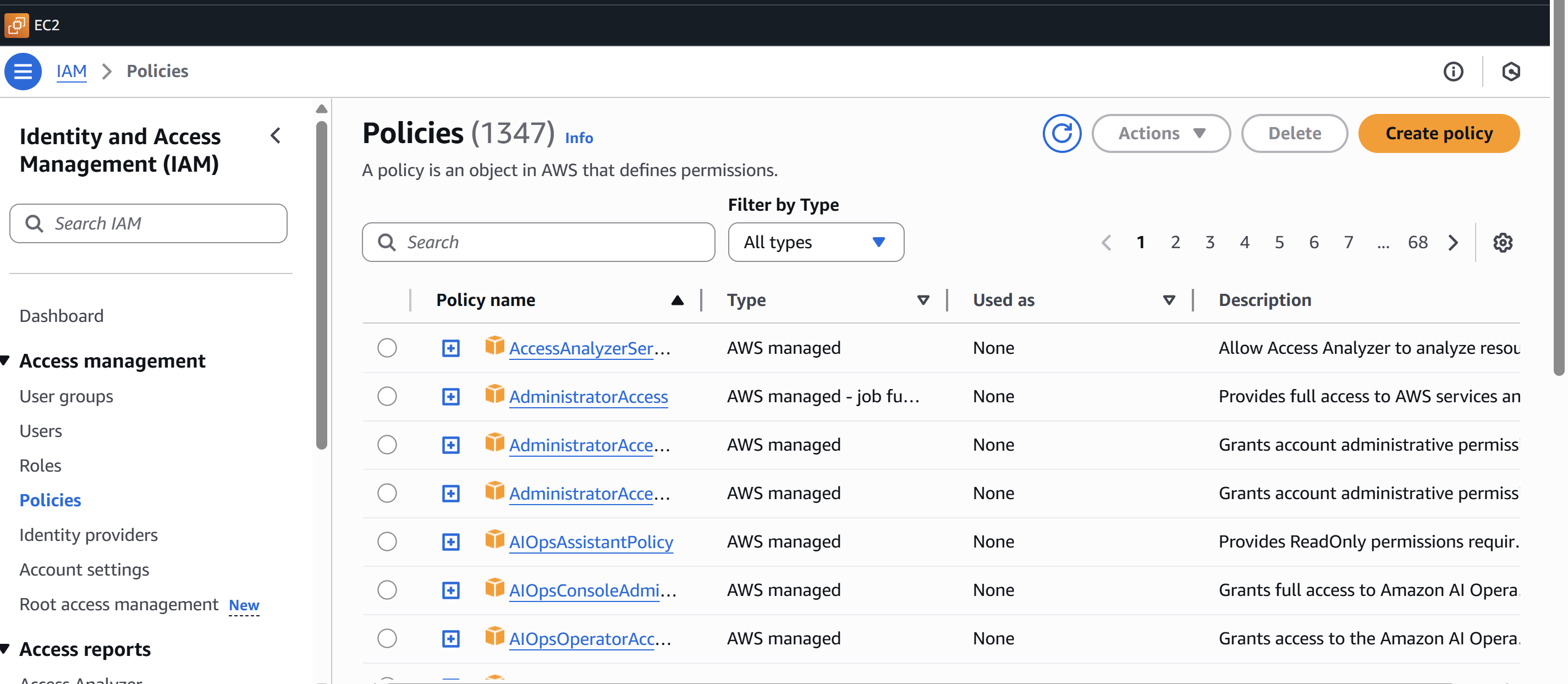
4) Write a bash script to create a IAM user with VPC full access.

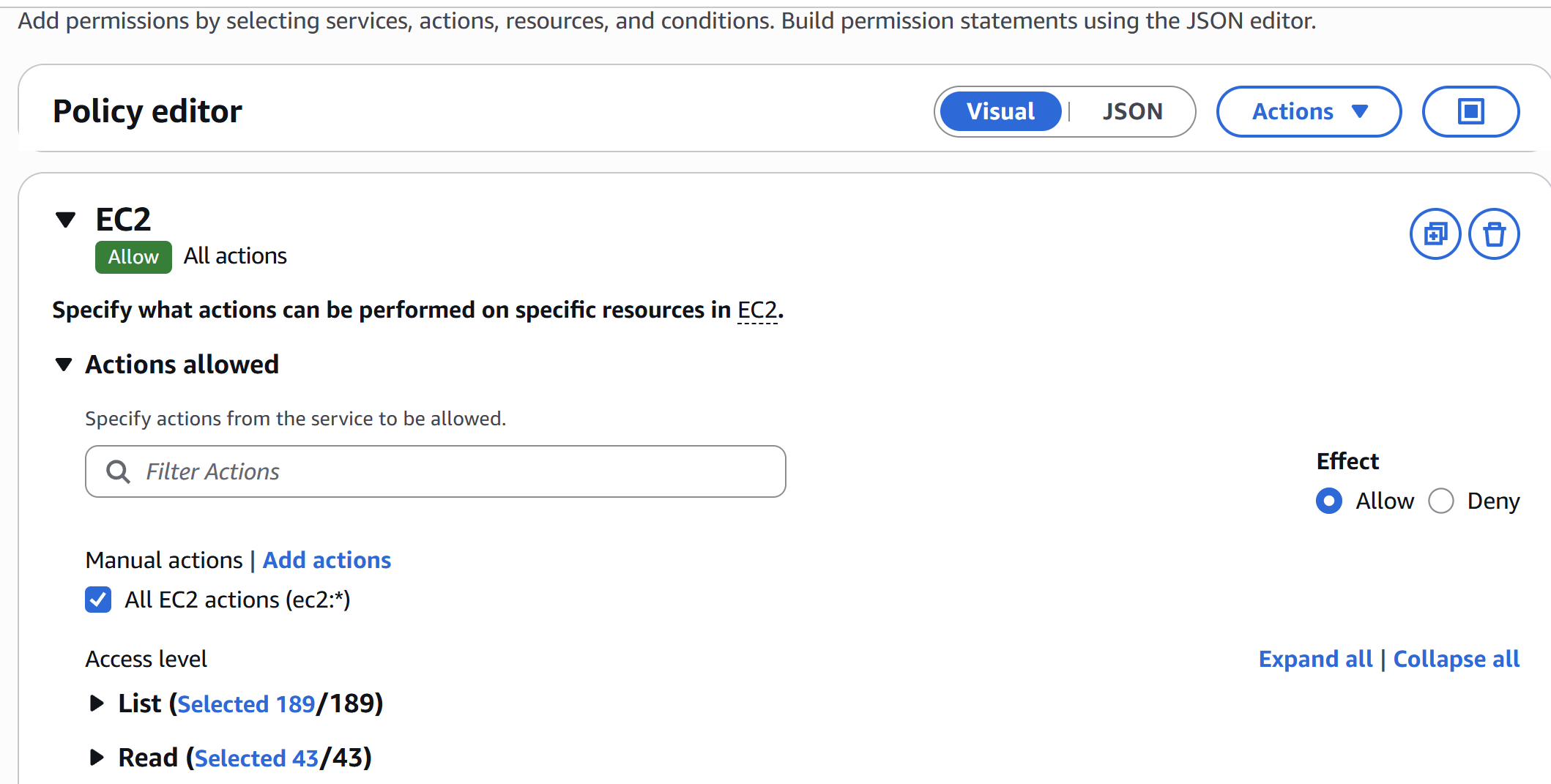
l Go to git bash  
l Enter aws configure  
l Provide access key and security key  
l $ aws sts get-caller-identity  
l Creat one file vi creatiam.sh  
l Paste this script in file#!/bin/bash  
# Set user name variable  
USER\_NAME="vpc-full-access-user"  
echo "Creating IAM user: $USER\_NAME"  
# Create IAM user  
aws iam create-user --user-name "$USER\_NAME"  
# Attach AmazonVPCFullAccess policy to user  
aws iam attach-user-policy --user-name "$USER\_NAME" --policy-arn  
arn:aws:iam::aws:policy/AmazonVPCFullAccess  
echo "User '$USER\_NAME' created and AmazonVPCFullAccess policy attached."Provide chomd +x <filename>  
./filename

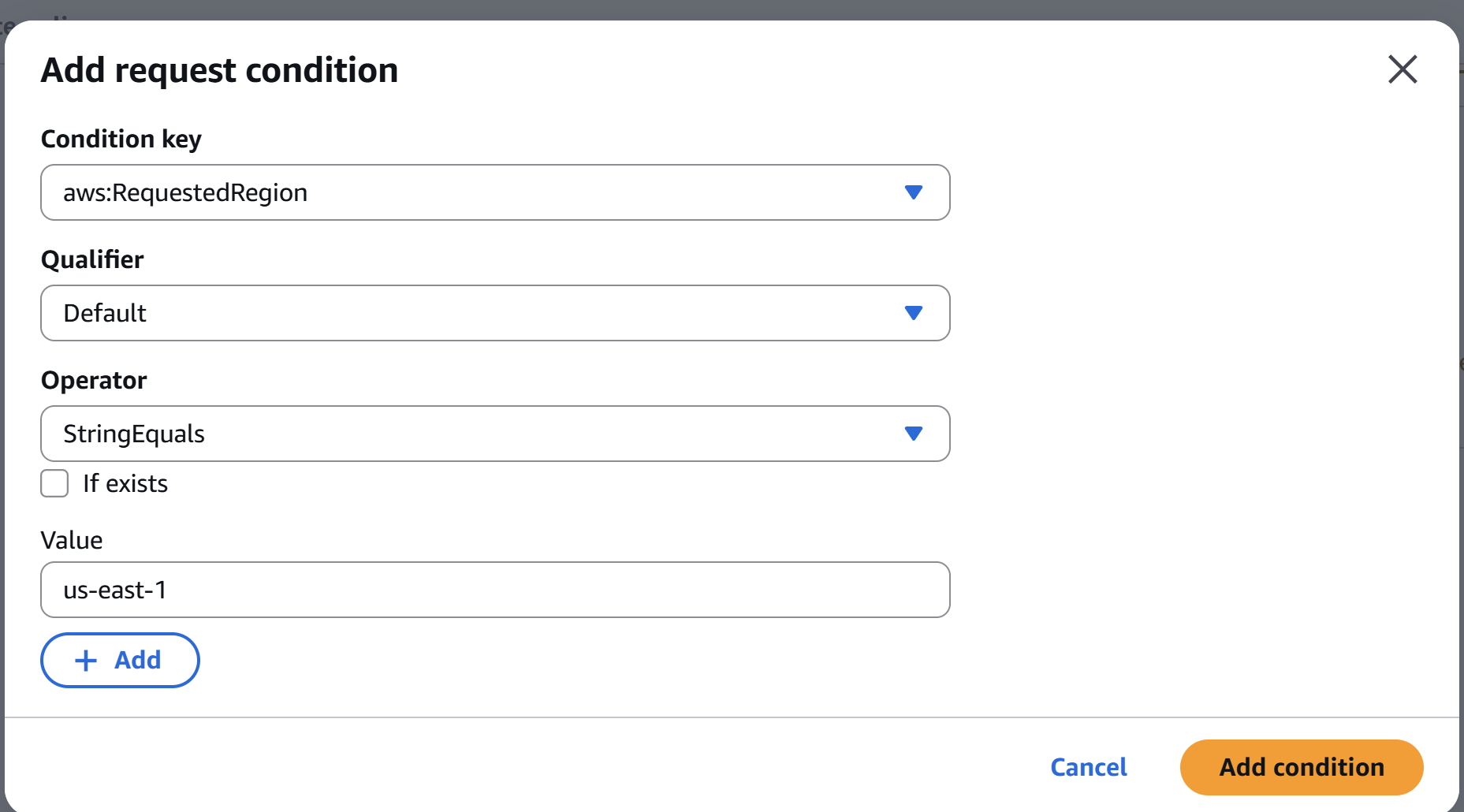


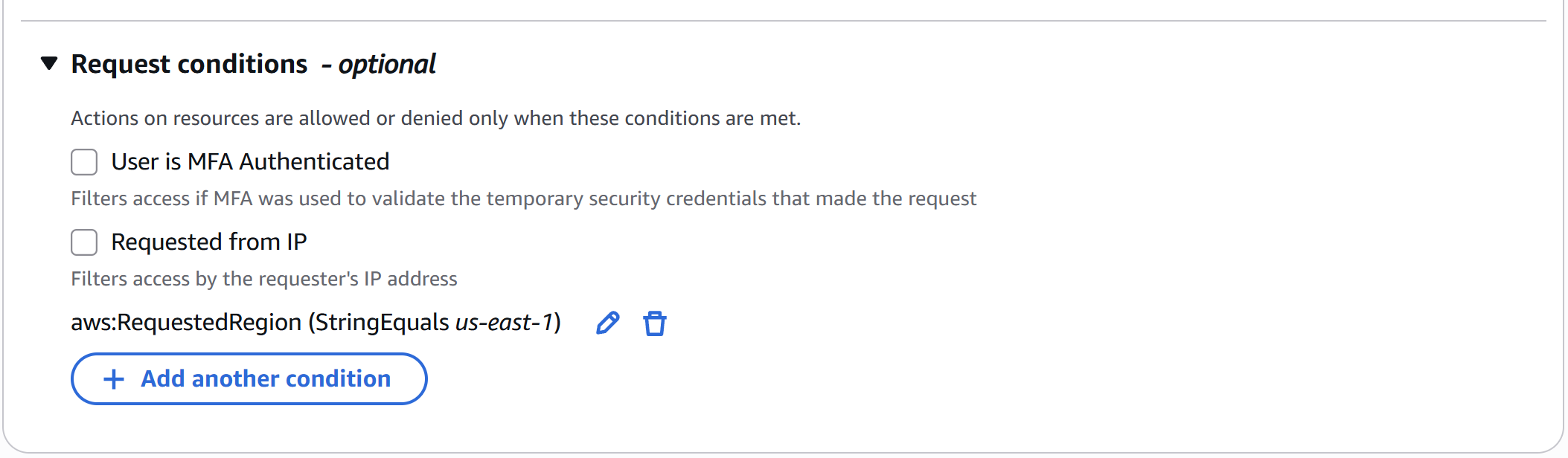


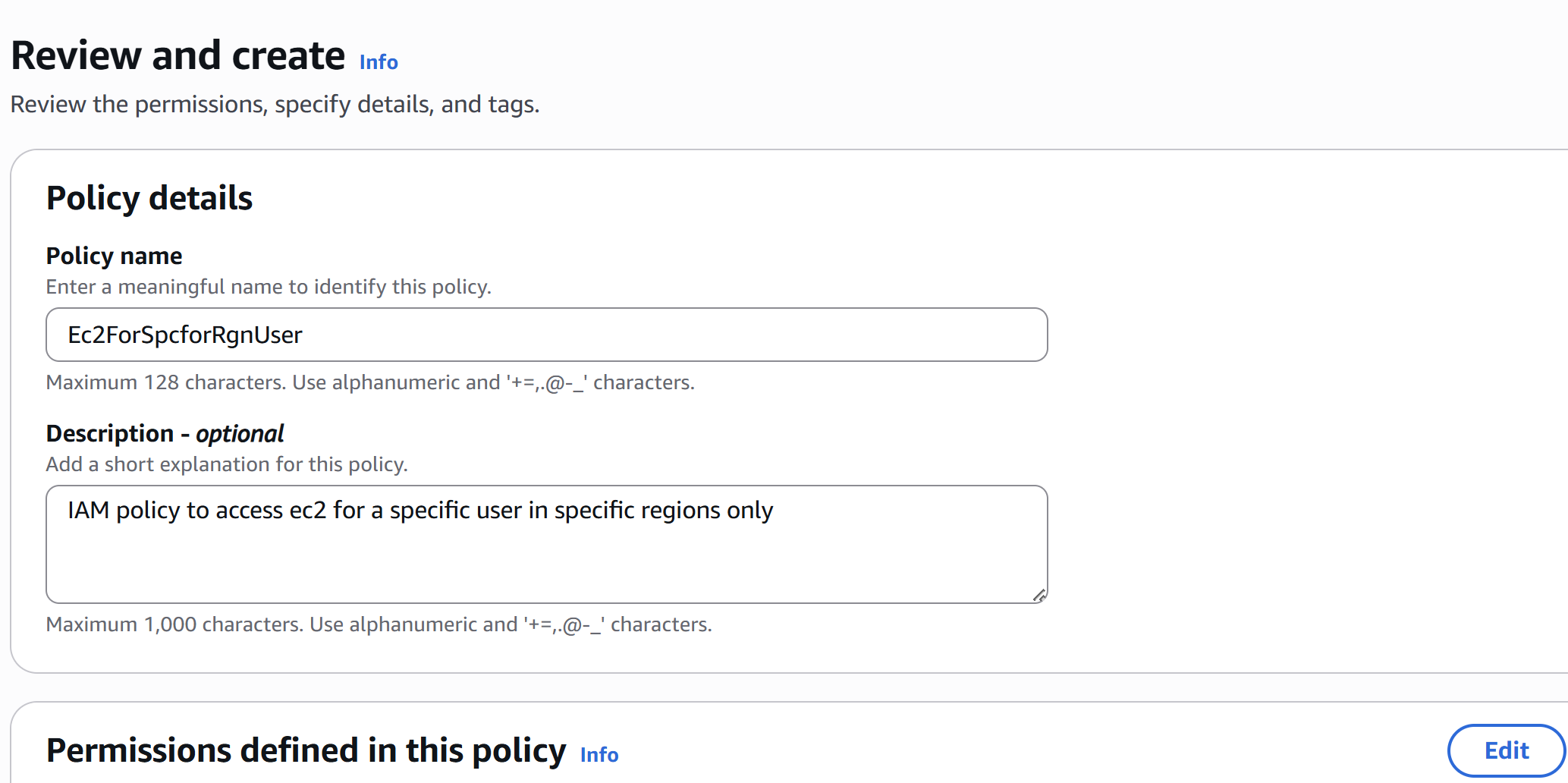
5) Create a IAM policy to access ec2 for a specific user in specific regions only.

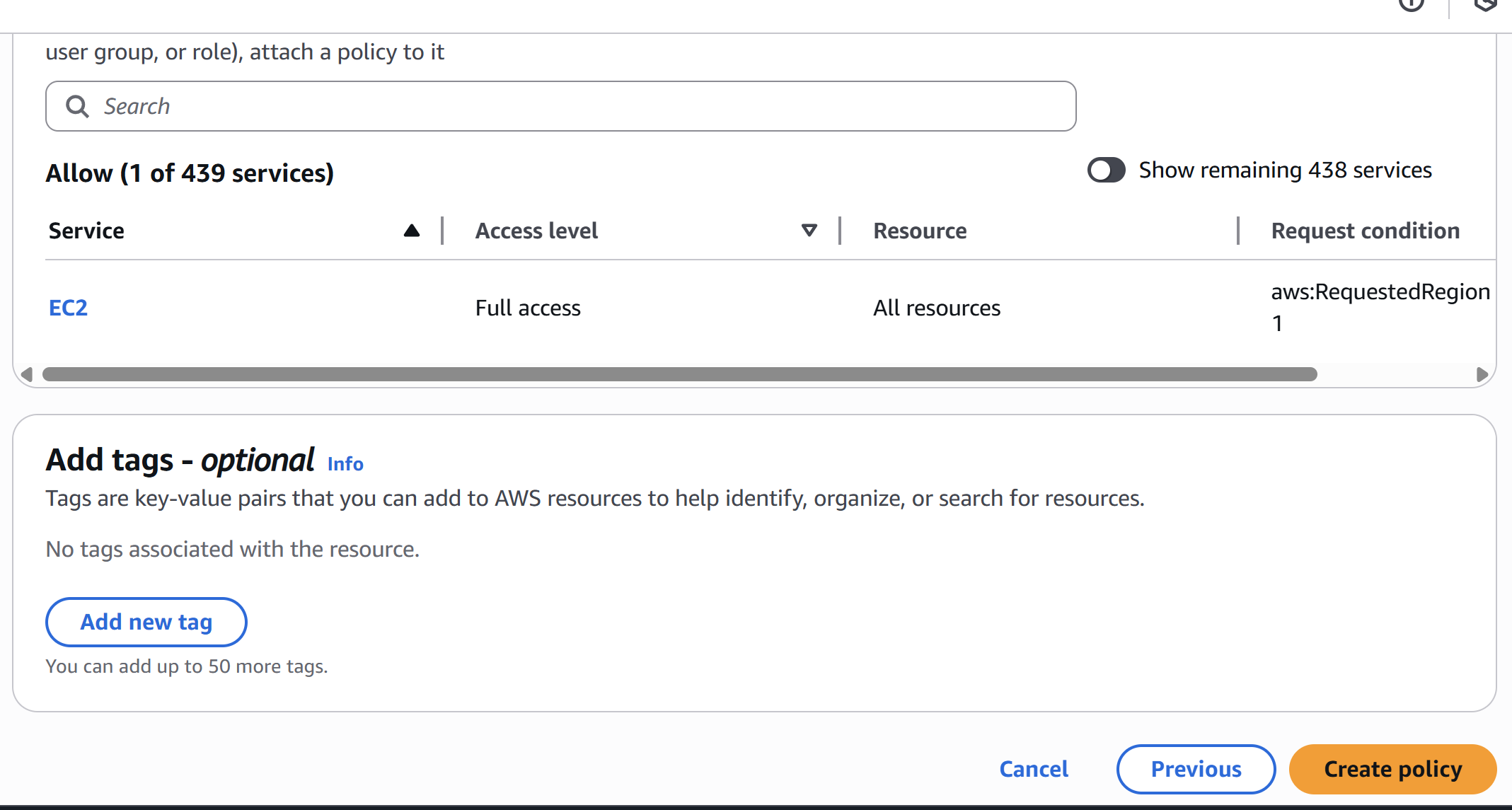


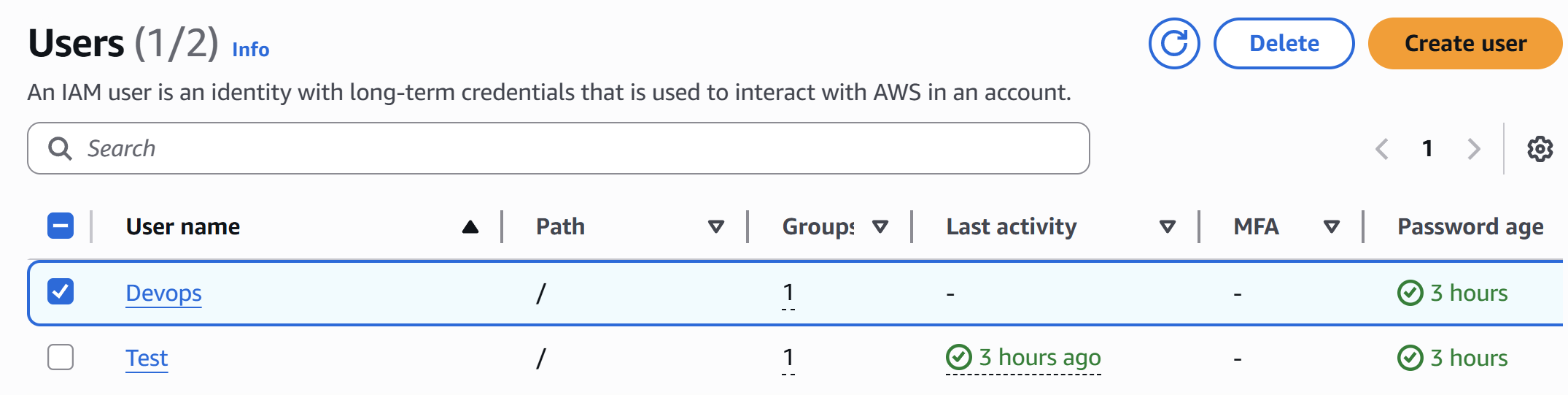


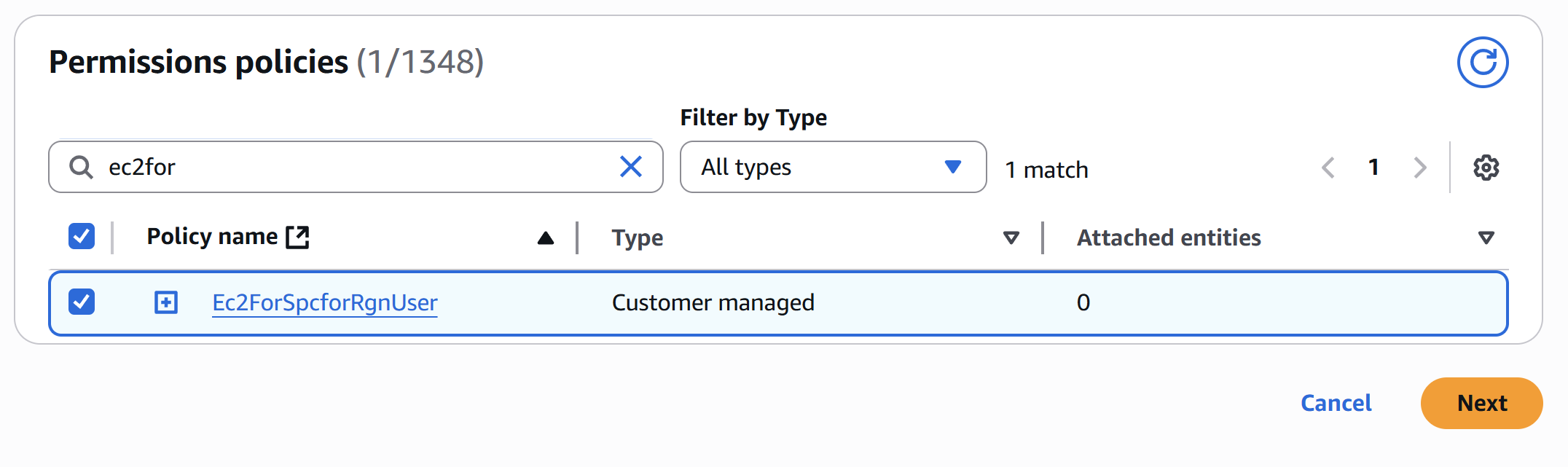


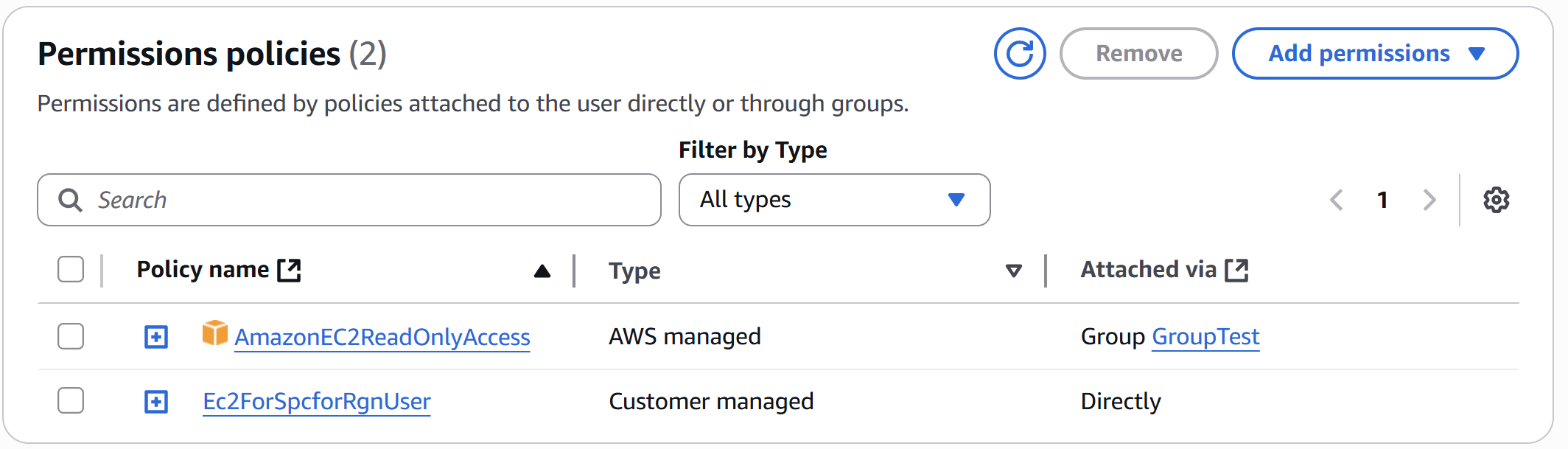


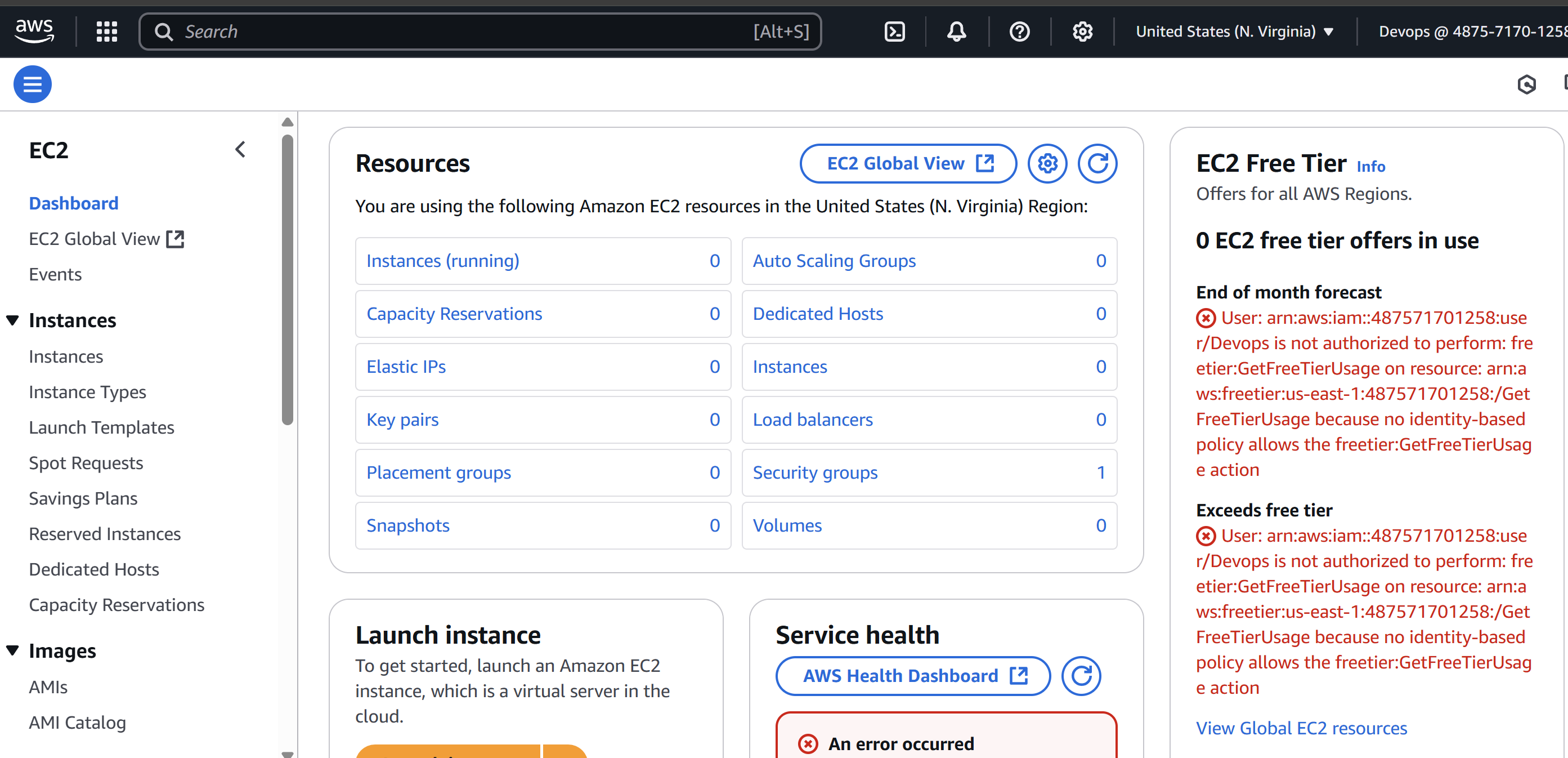












6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B.

(Collaborate with team member and execute this.Mostly asked in every interview)

Create aws IAM in account A

And s3 bucket in account B  
In aws IAM create user and and s3 bucket full access   
then provide persiion using below policy  
Account A(aws IAM inline policy )  
{  
"Version": "2012-10-17",  
"Statement": [  
{  
"Effect": "Allow",  
"Action": [  
"s3:GetObject",  
"s3:ListBucket"  
],  
"Resource": [  
"arn:aws:s3:::s3bucket4sagar",  
"arn:aws:s3::: s3bucket4sagar /\*"  
]  
}  
]  
}  
In another account that is B create s3 bucket and and this  
policy in permission in account tab  
Account B(s3 bucket policy in another account)  
{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Principal": {  
 "AWS":   
"arn:aws:iam::932181321274:user/IAM-user"  
 },  
 "Action": [  
 "s3:GetObject",  
 "s3:ListBucket"  
 ],  
 "Resource": [

"arn:aws:s3:::iamcnct123",  
 "arn:aws:s3:::iamcnct123/\*"  
 ]  
 }  
 ]  
}  
Then save all the changes  
Go to git bash  
In git bash  
aws configure --profile crossregion-IAM  
Provide access key and security key  
After this  
aws s3 ls s3://s3bucket4sagar --profile iamcnctno

Summary: To access s3 bucket from another we need s3  
bucket user name  
To connect IAM in s3 bucket the account user need ARN   
to connect

