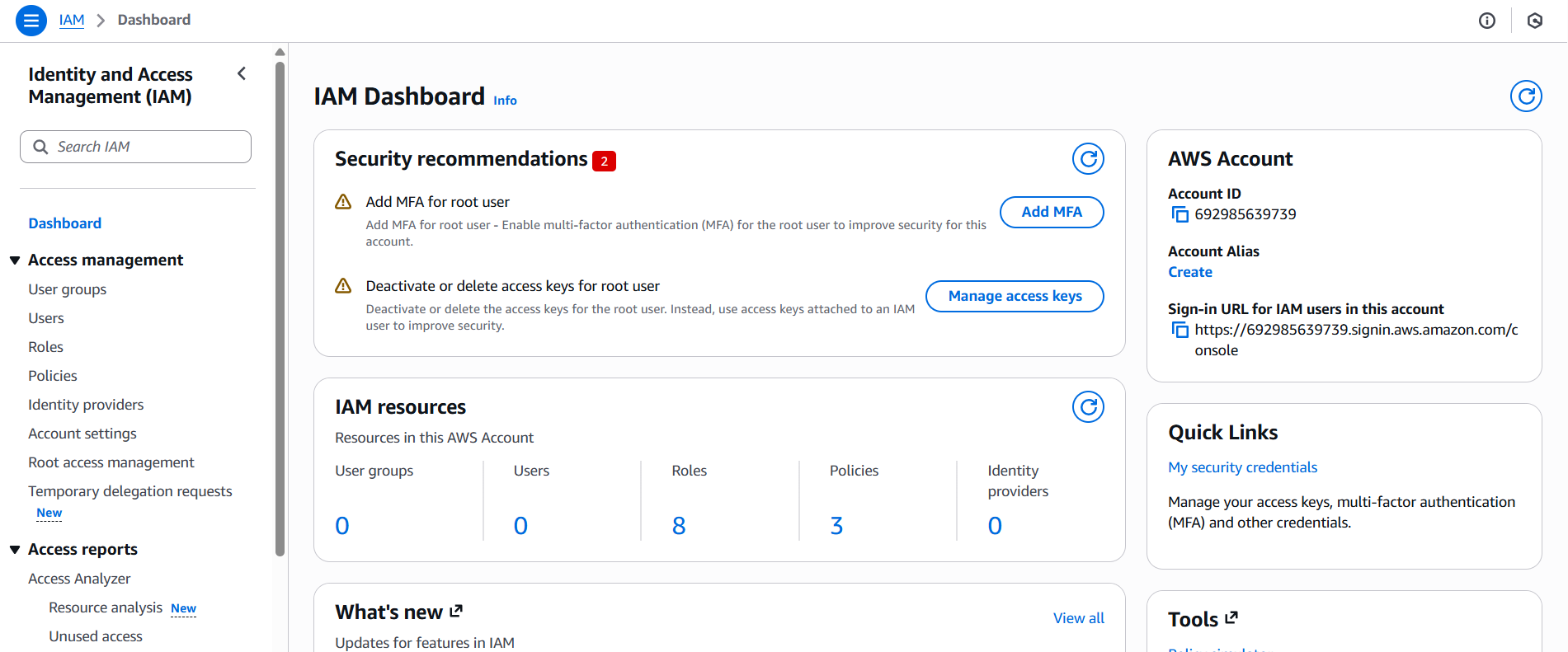
**Task on IAM**

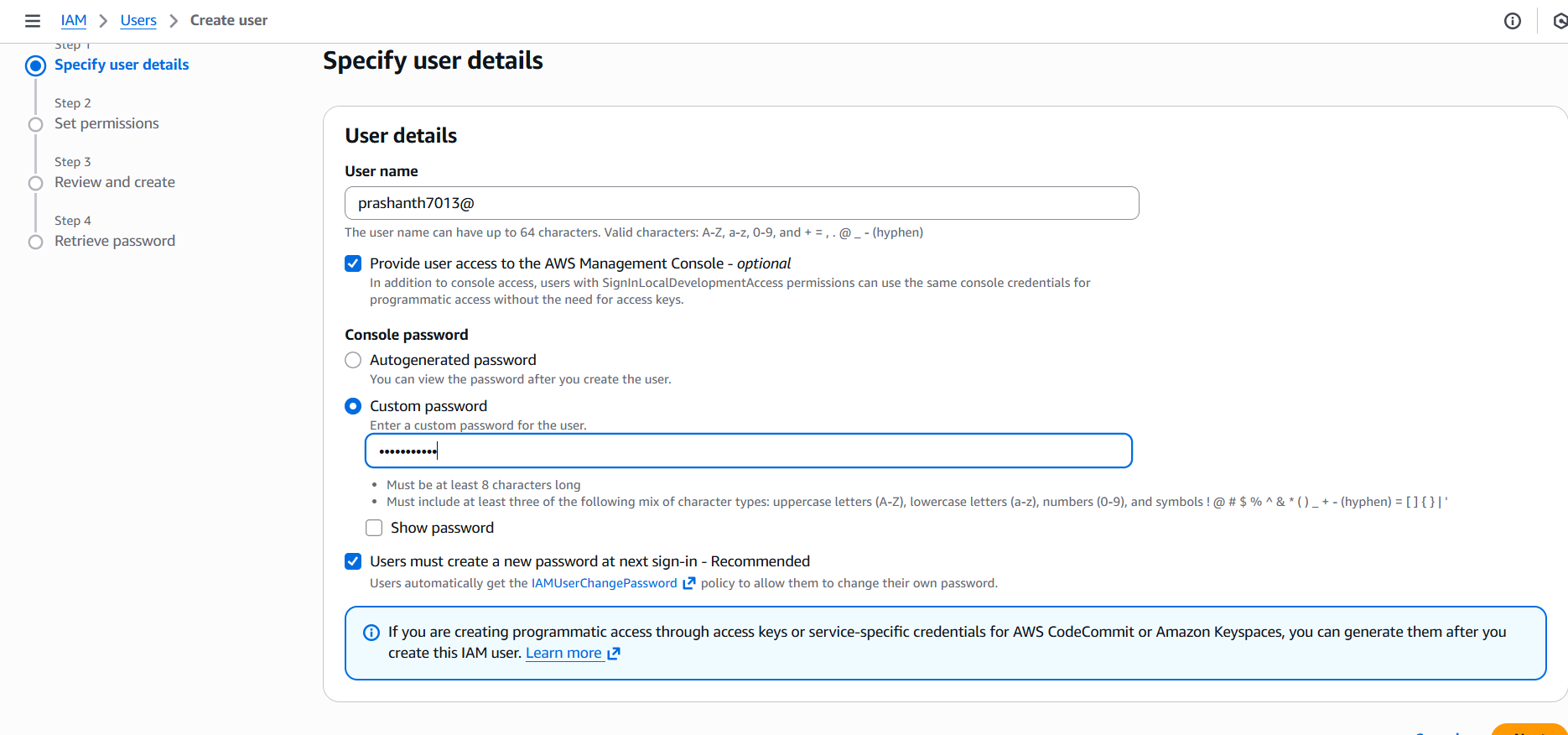
1. **Create one IAM user and assign EC2 and S3 full access roles.**

first go to aws console

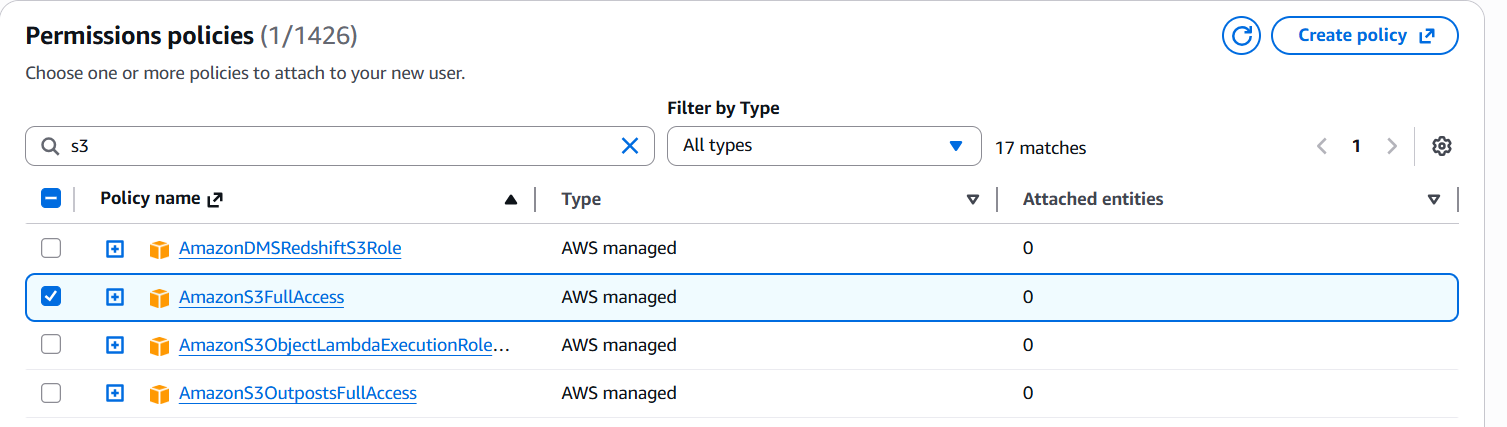
go to IAM—users—click on create user

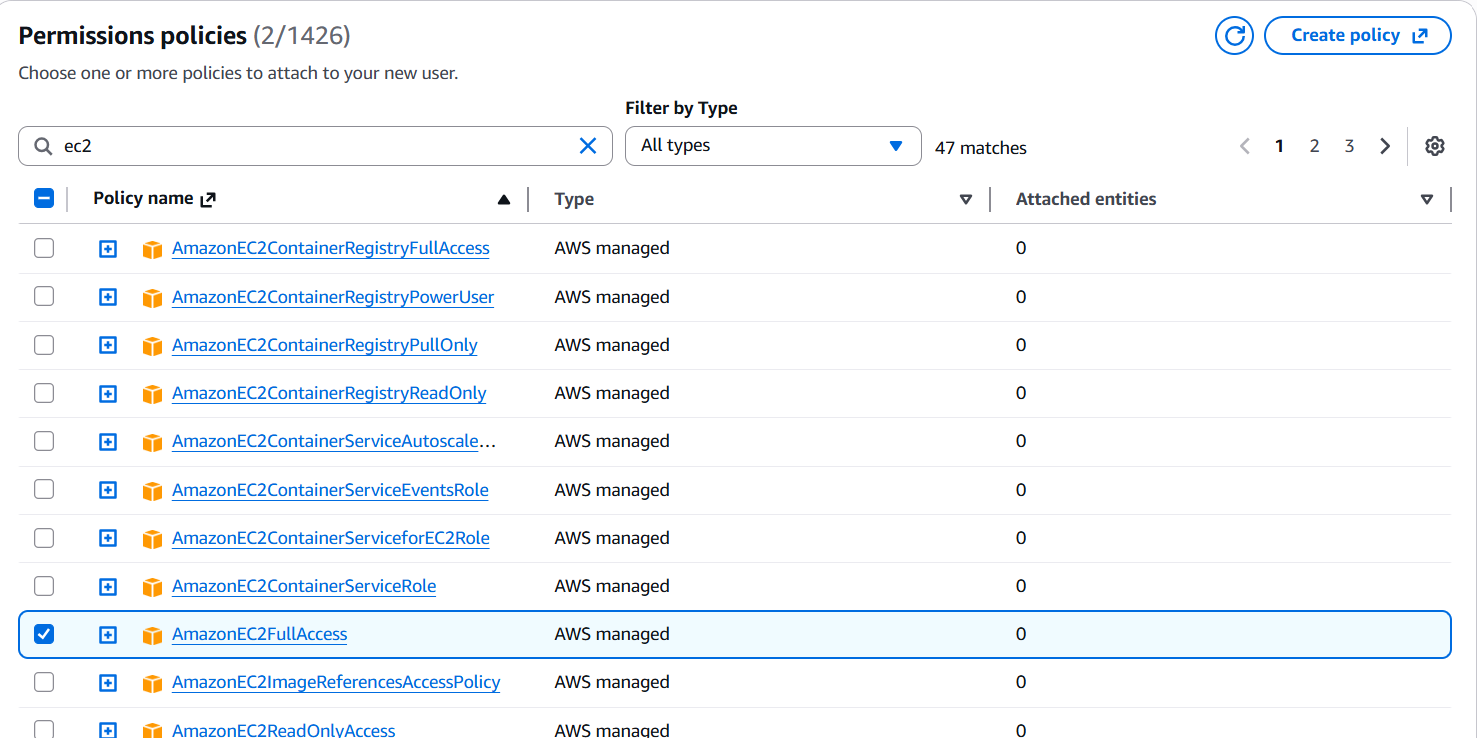
****

after clicking on create user enter the user name and u can create the password

****

**not to set permissions add s3 and ec2 in permission policy and create**

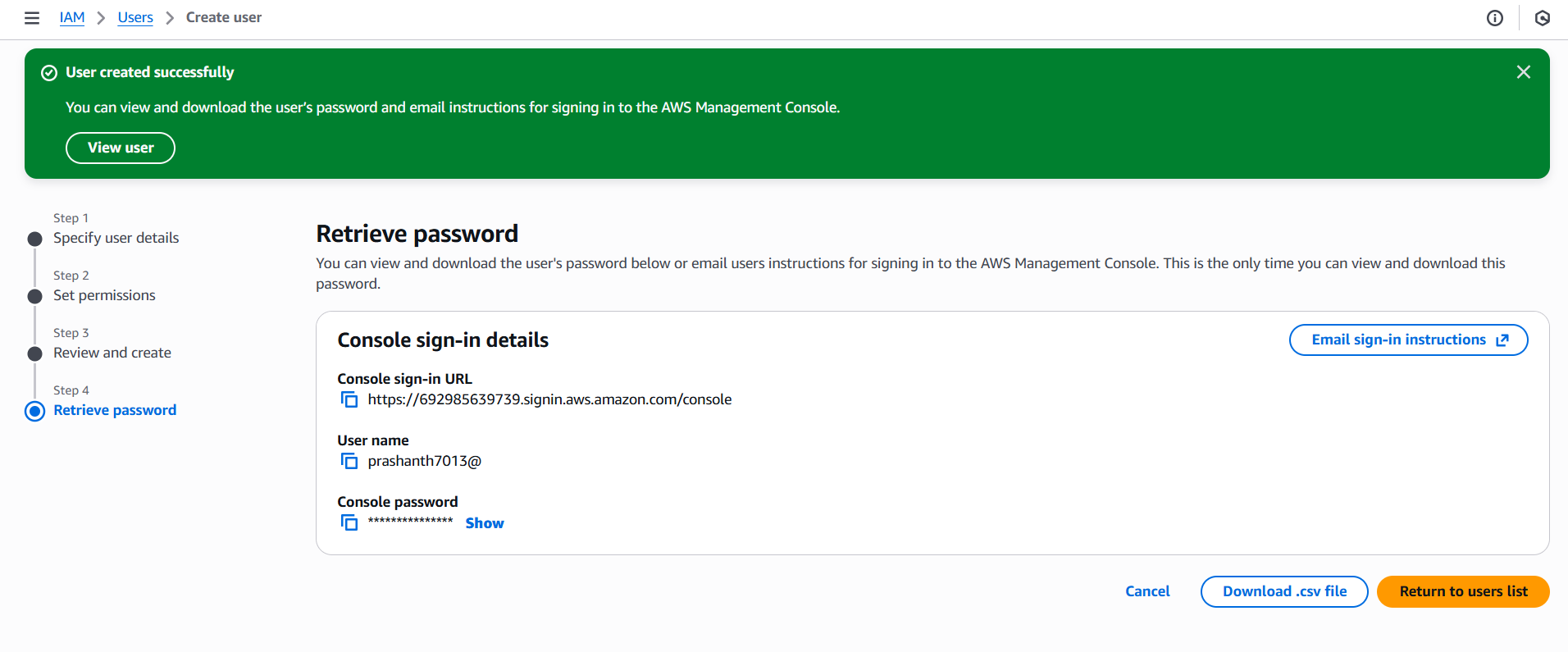
****

****

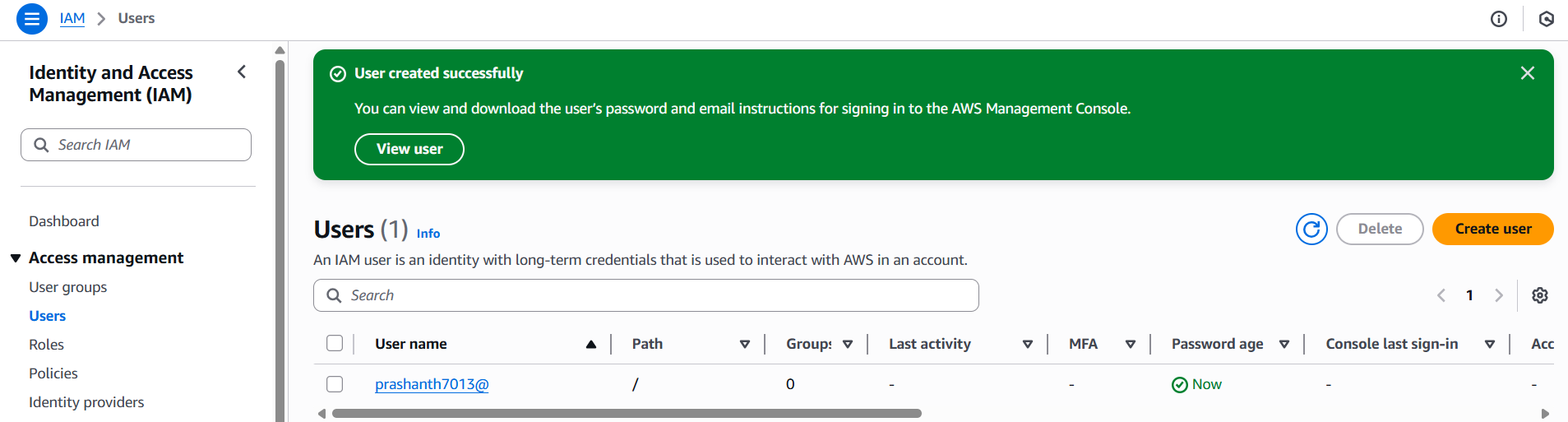
**now review the details and finally click on create user**

****

**click on return to users list**

****

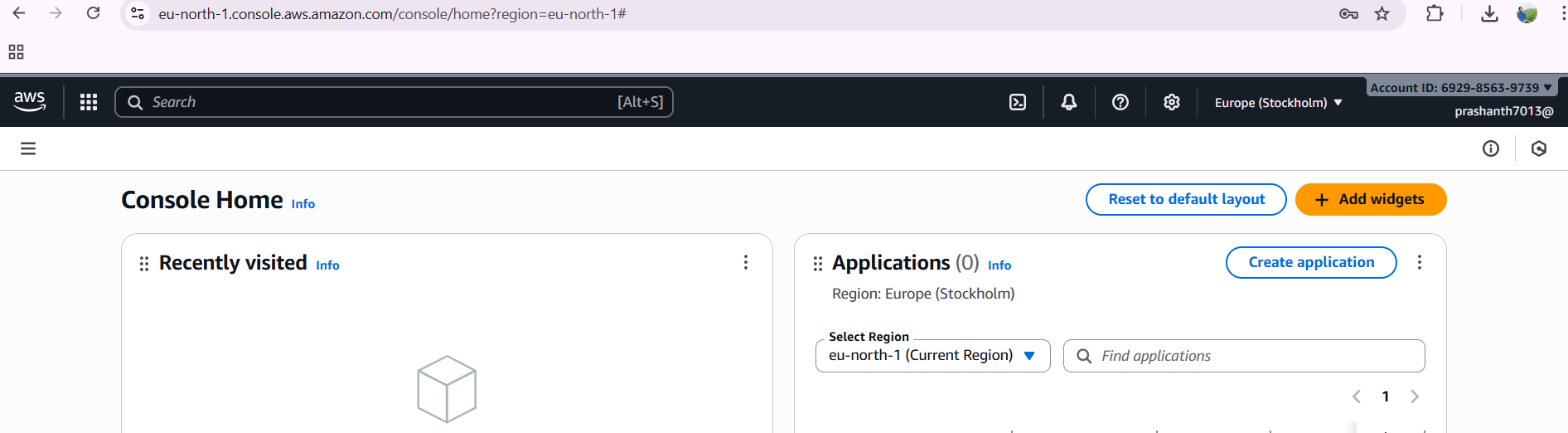
**you can see the user list**

****

**to validate**

**login in different tab**

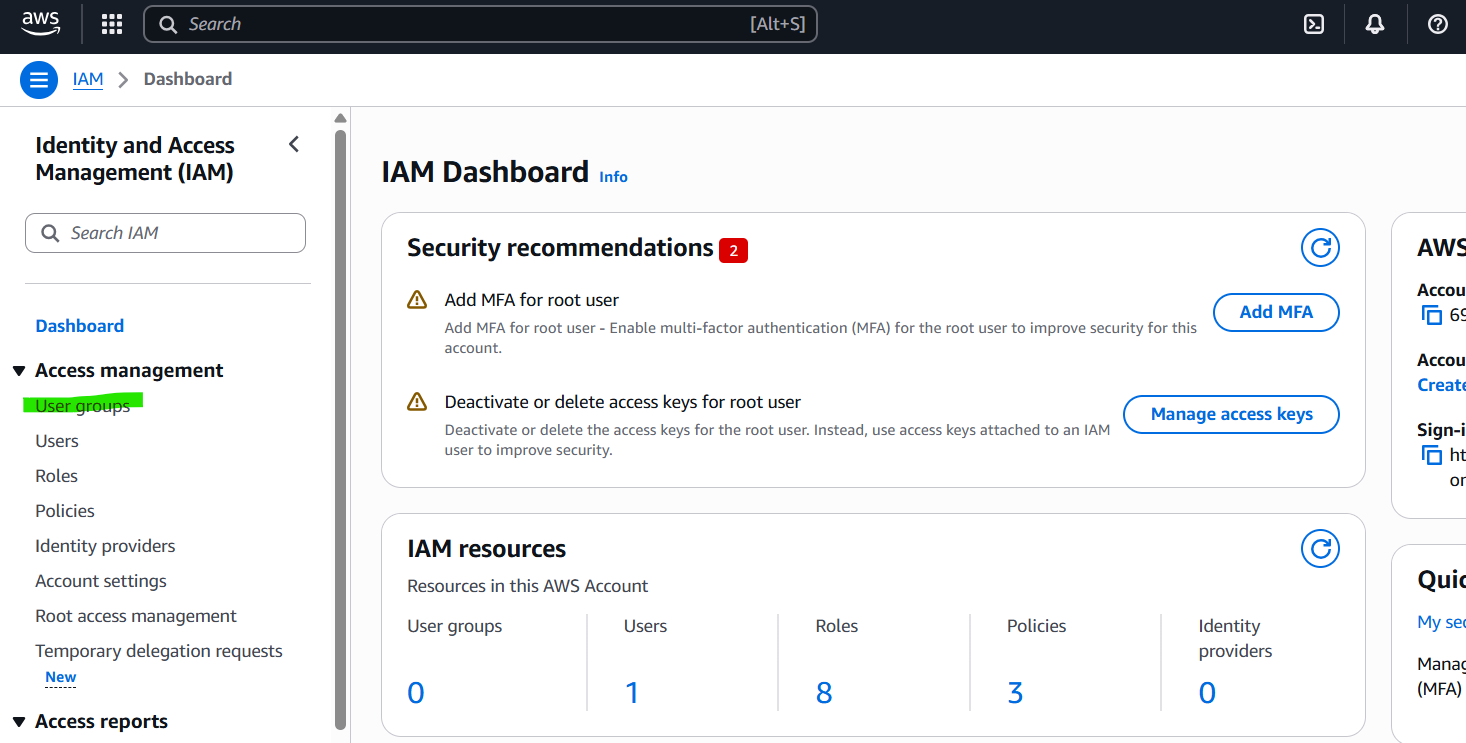
**copy the account id and enter username and password for IAM login**

****

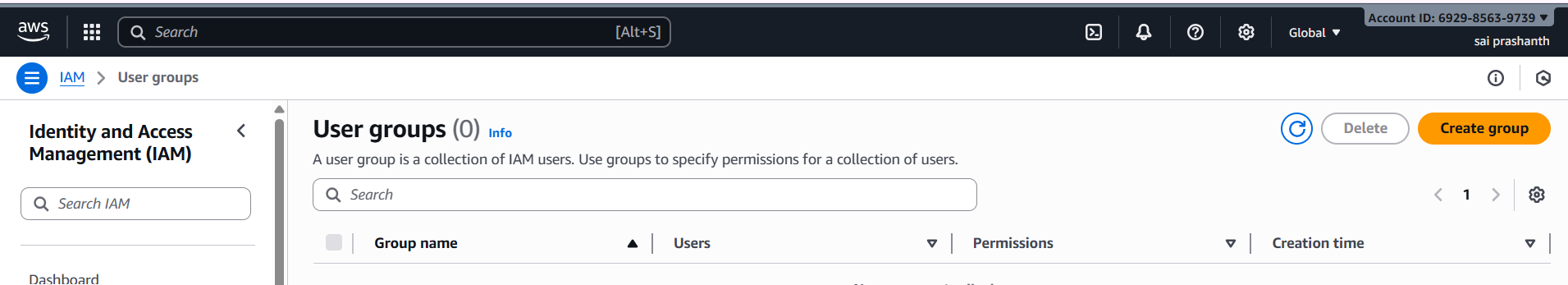
1. **Create one group in IAM and assign read access for EC2.**

go to aws console

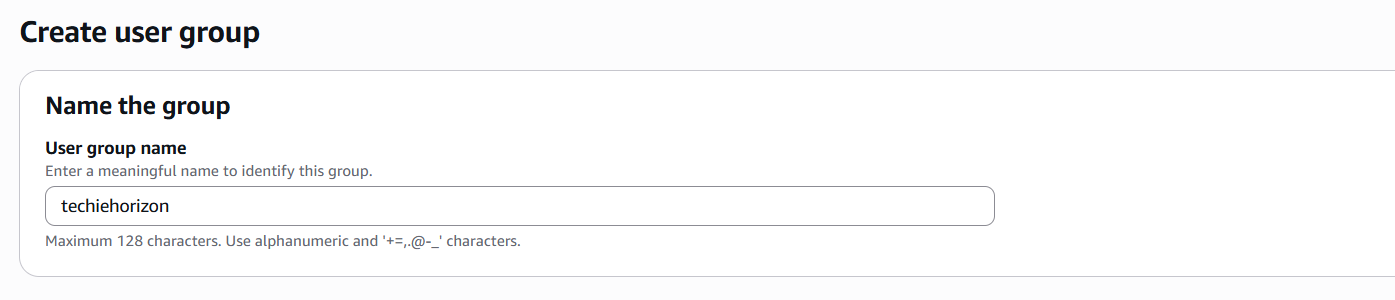
IAM—usergoup-click on usergroup

****

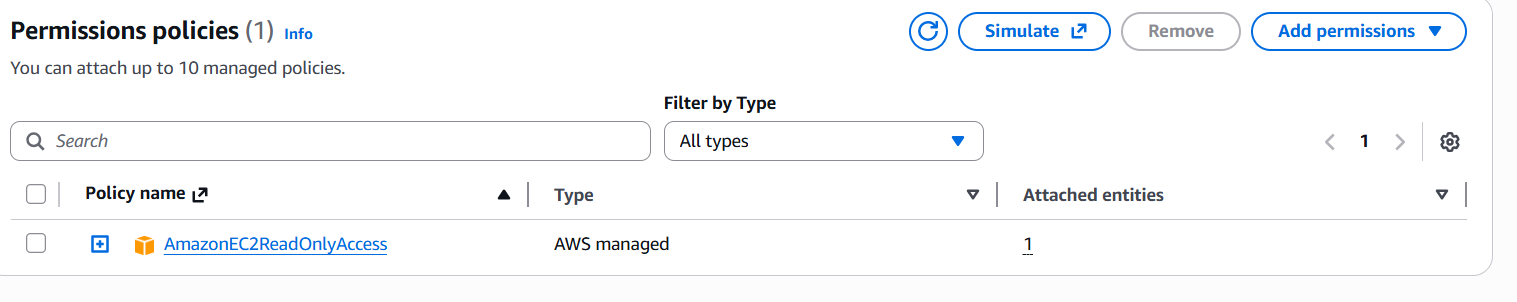
**click on create group**

****

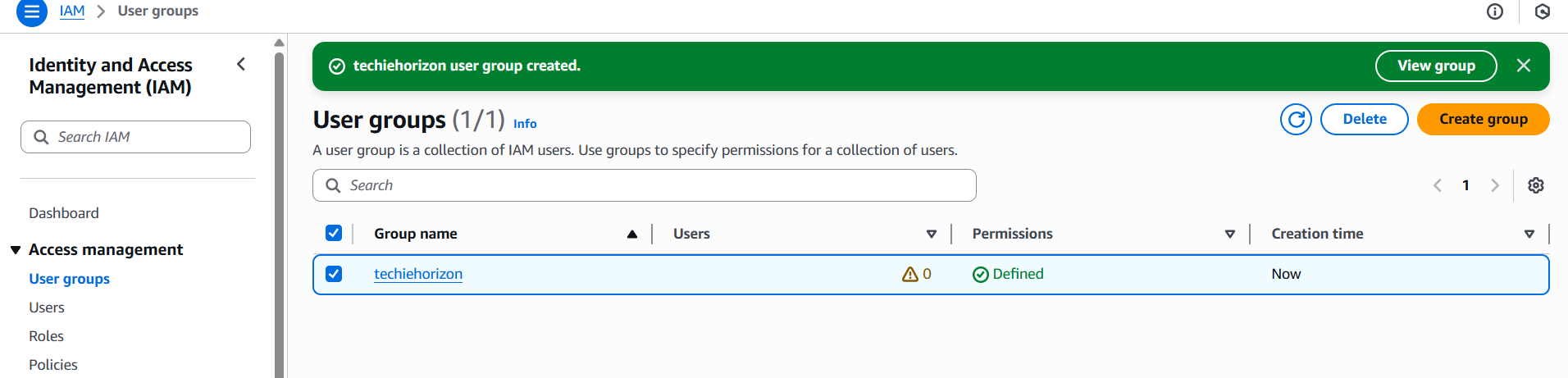
**now enter the group name**

****

**give the permission ec2 read access**

****

**and finally click on create and the group has been created successfully**

****

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

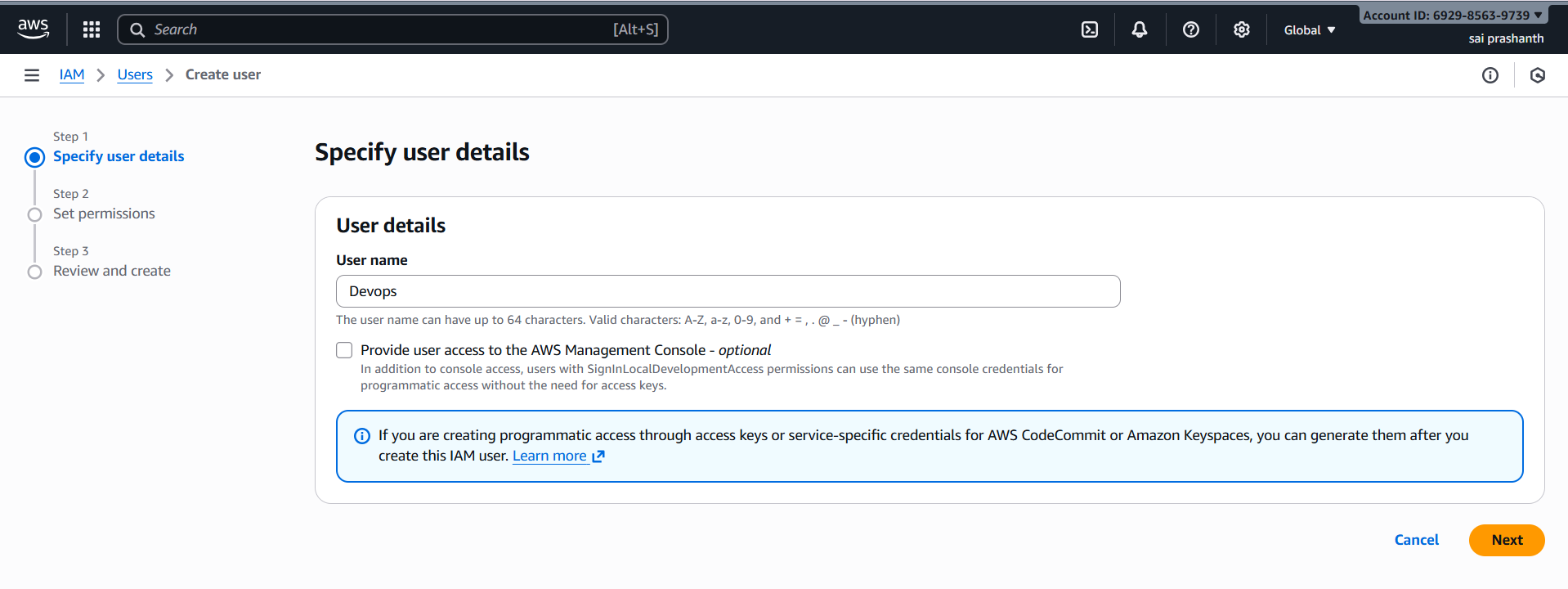
IAM

click on users

click on crate user

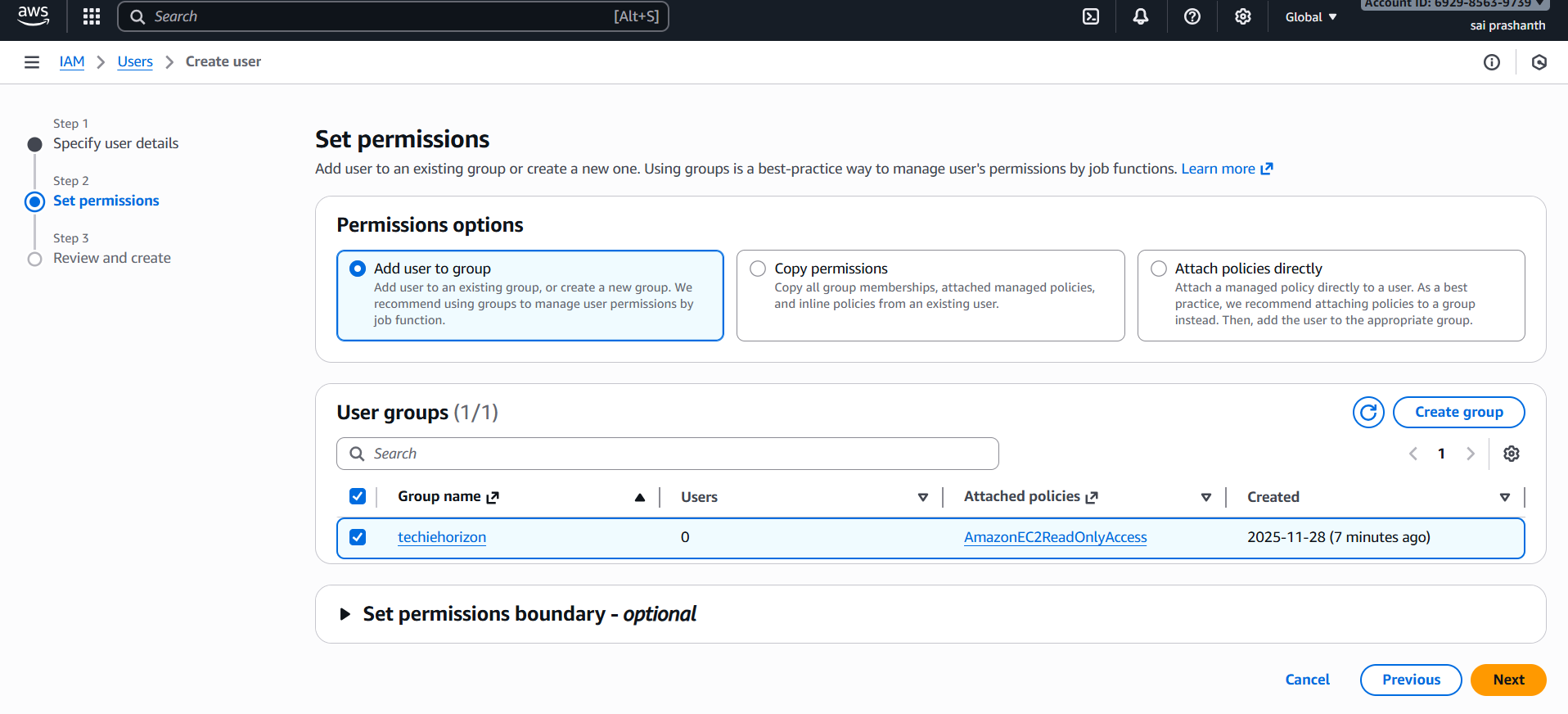
add the user name as Devops

click on create

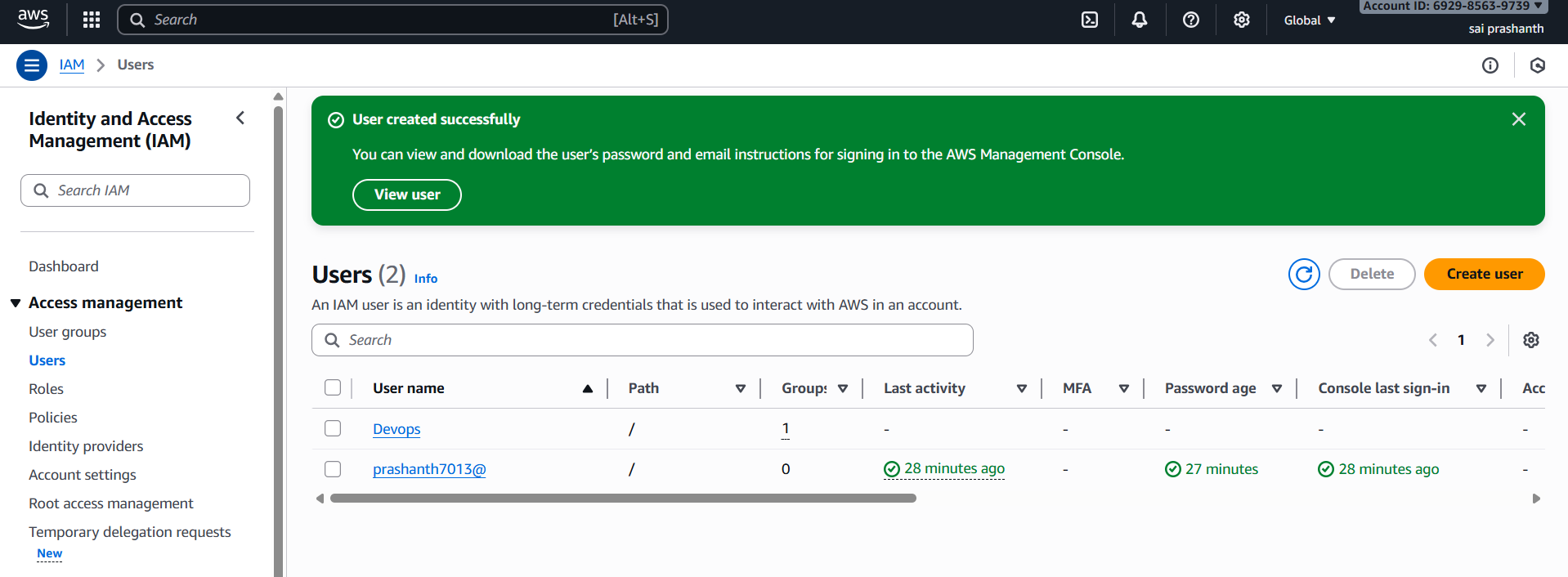
****

**now add the user group which you have created in task 2 group name as techiehorizon**

**select it and click on next**

****

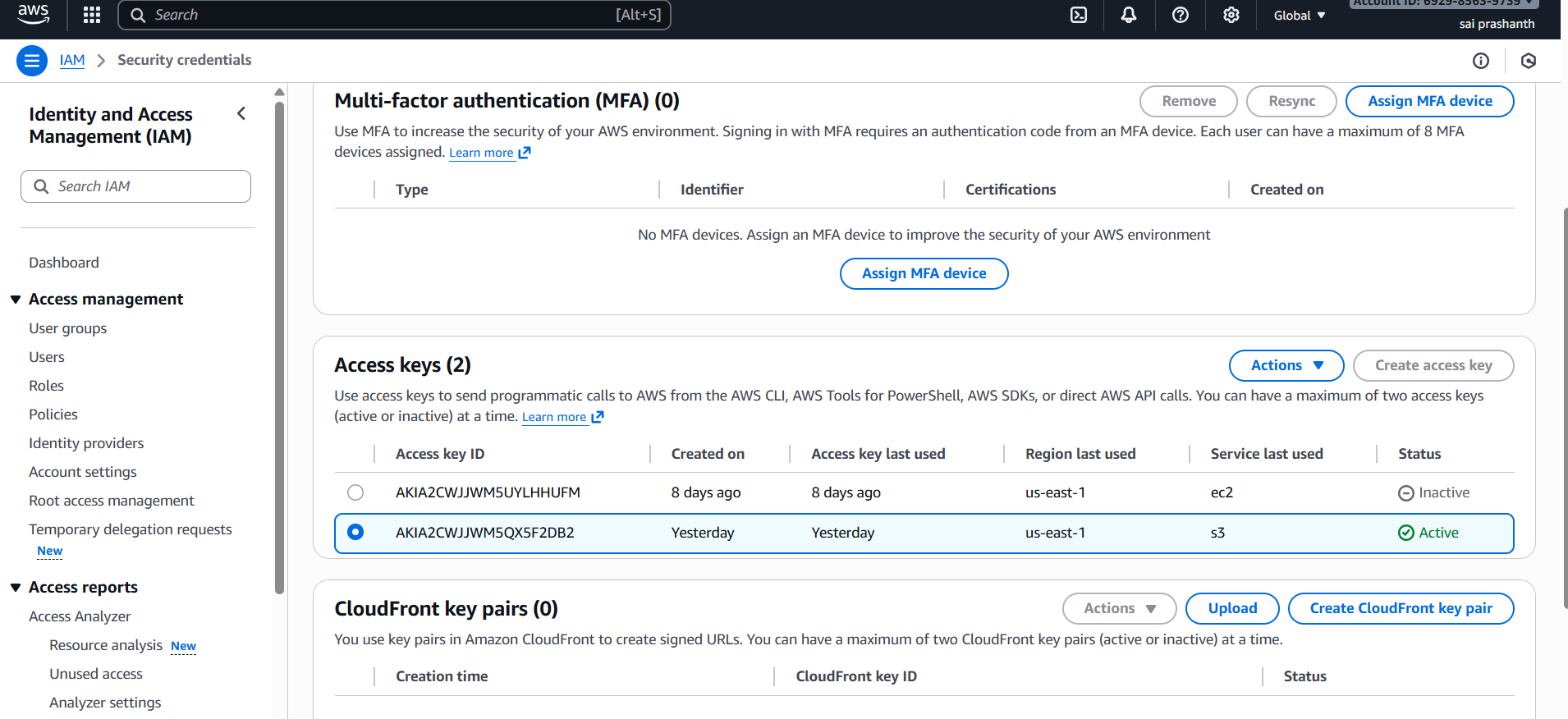
**finally the username Devops has been created with the group name techiehorizon**

****

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

**first go the security credentials for aws configure**

**download the file of access key and secret key**

****

**then create one instance with deault vpc**

****

**connect with ssh in git bash**

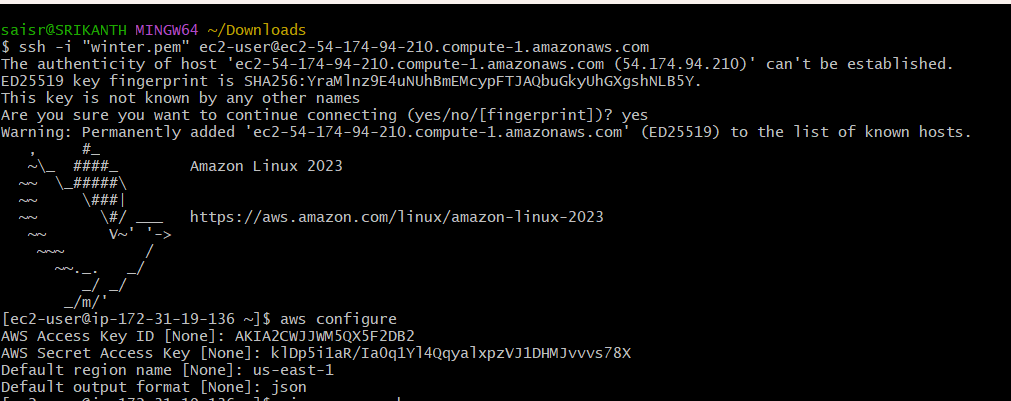
**now we want to do aws confiure**

**enter access key**

**secret key**

**region**

**output format**

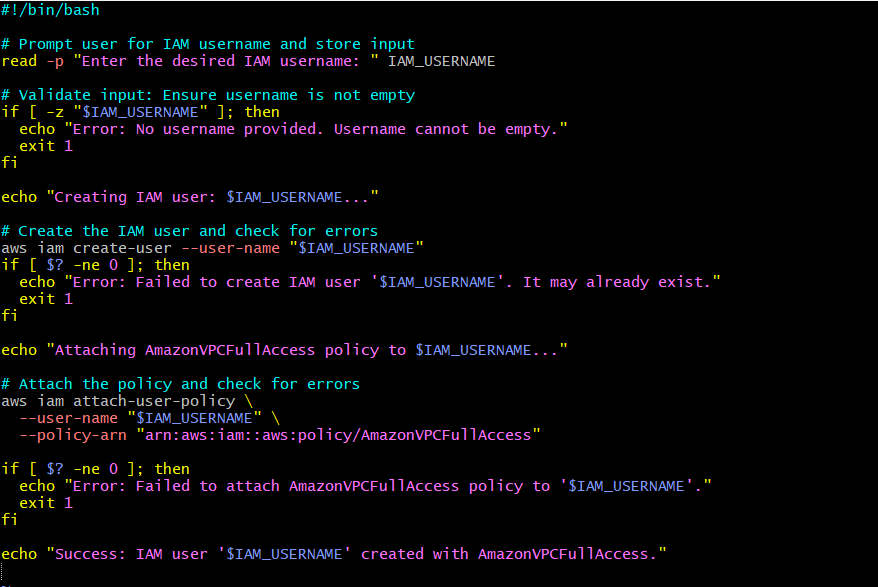
****

**now we want to add script**

**vi vpc\_user.sh**

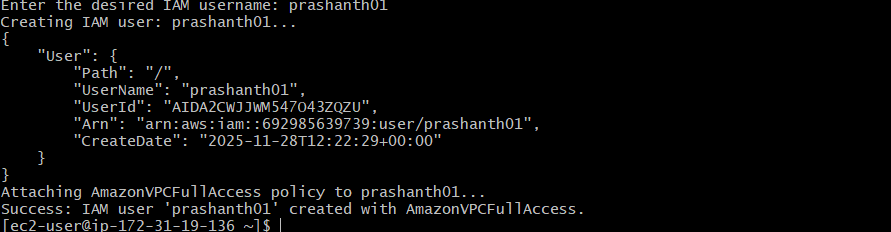
**chmod u+x vpc\_user.sh**

**./vpc\_user.sh**

****

**one it has been done**

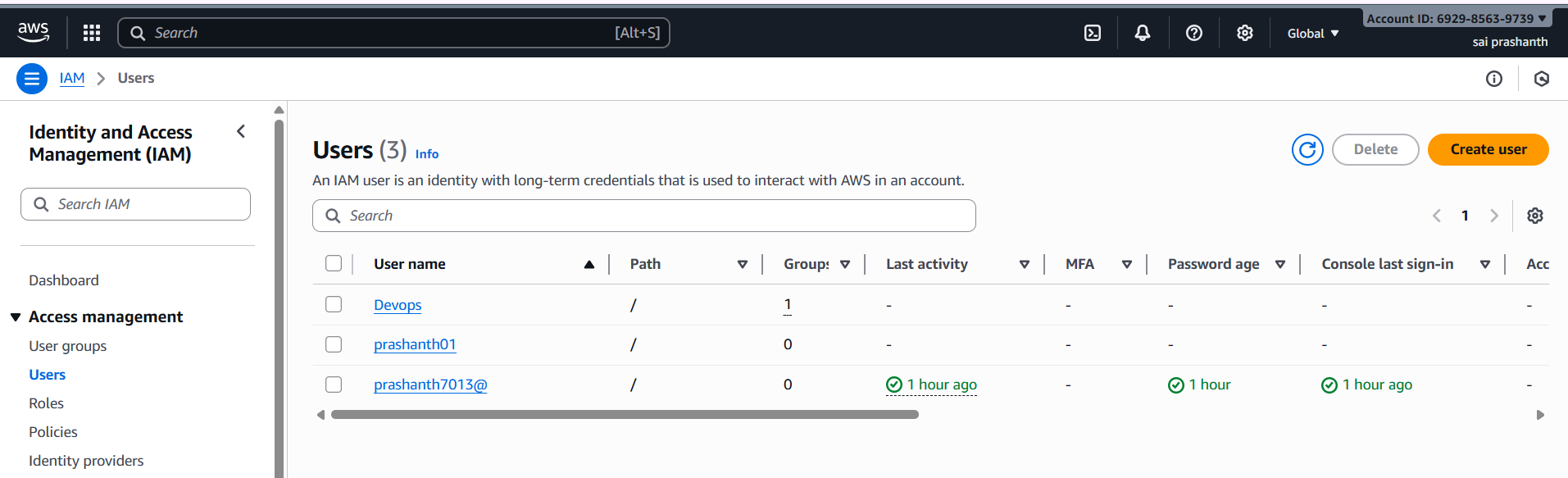
**we need to enter the user name which you want to create**

****

**one it has been executed to check the user**

**go to IAM—users**

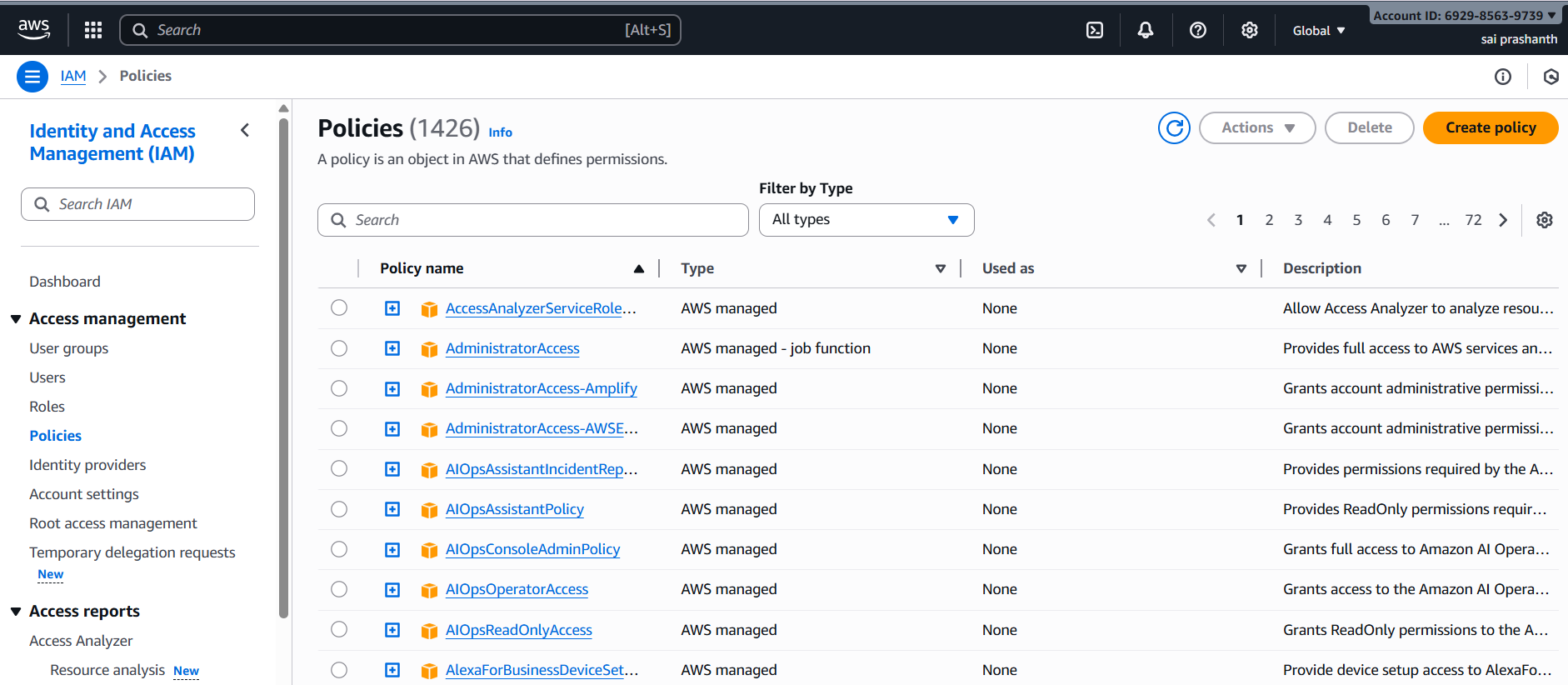
**you can see new user name has been created**

****

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

**go to aws console**

**IAM—policies—create policy**

****

**click on create policy in json format**

**policy to allow ec2 access to specific user**

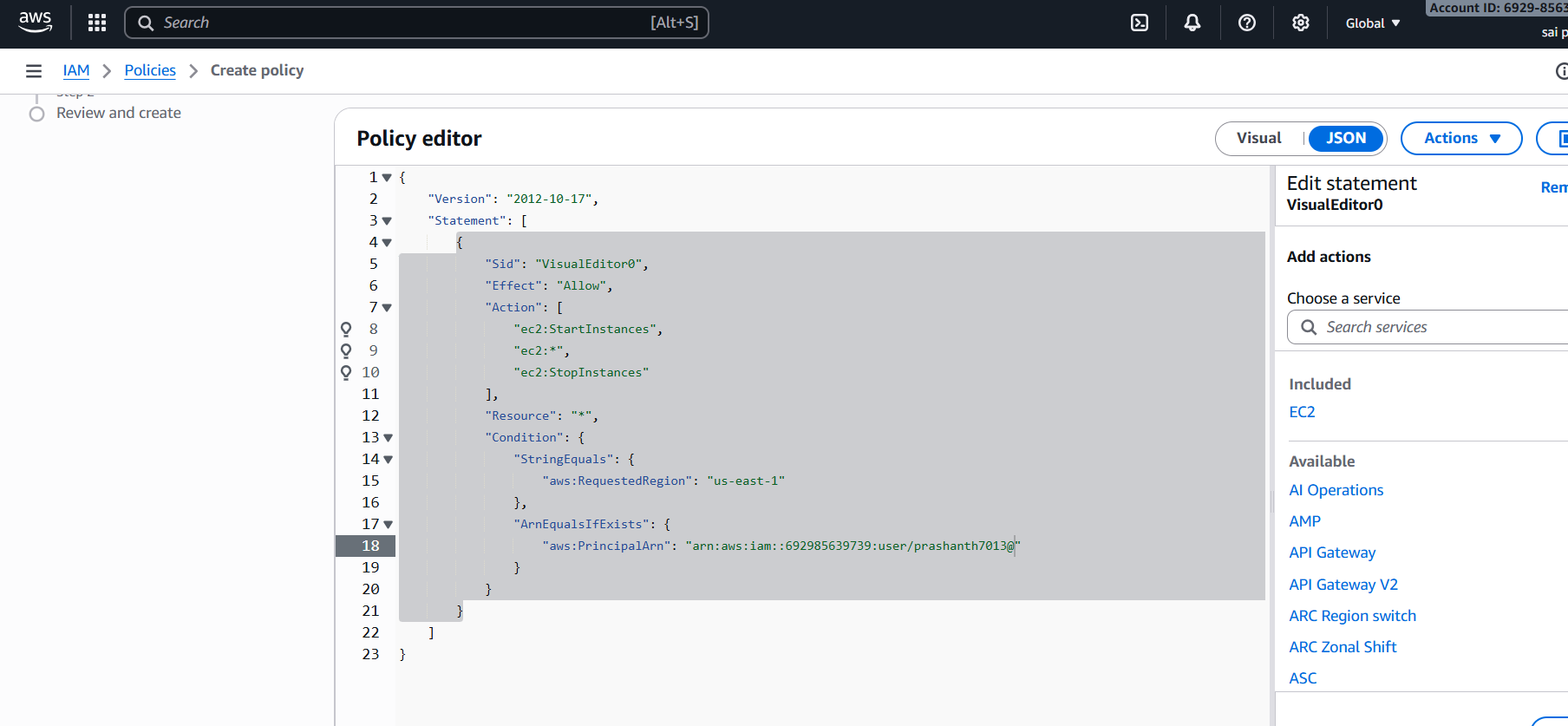
**copy the policy script and paste it in the policy editor**

**select the specific user which you have created**

**copy the arn number**

**now copy the arn number of that specific user and now remove the old arn number and paste the arn of that specific user**

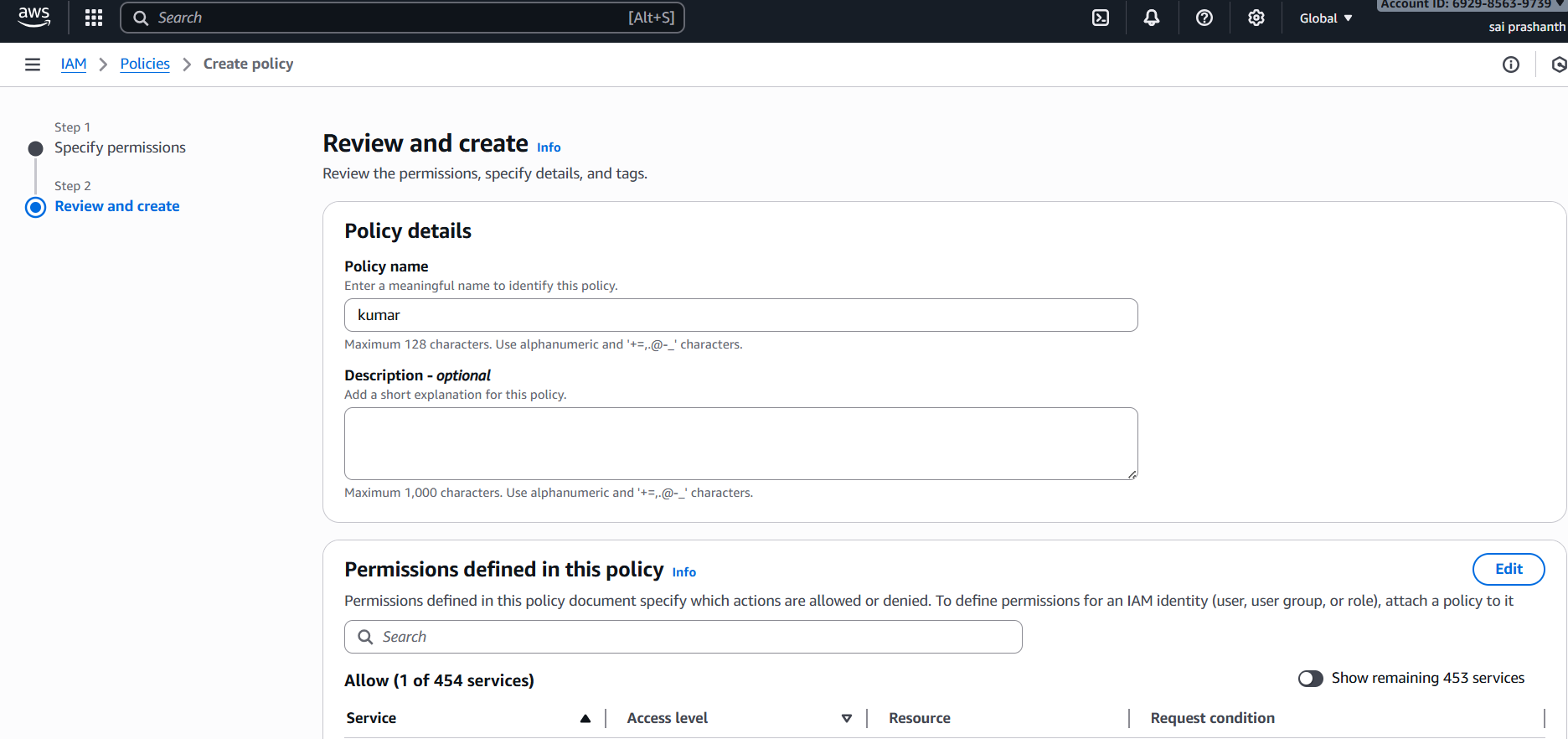
**now click on next**

****

**to review and create**

**enter the policy name what you want to give**

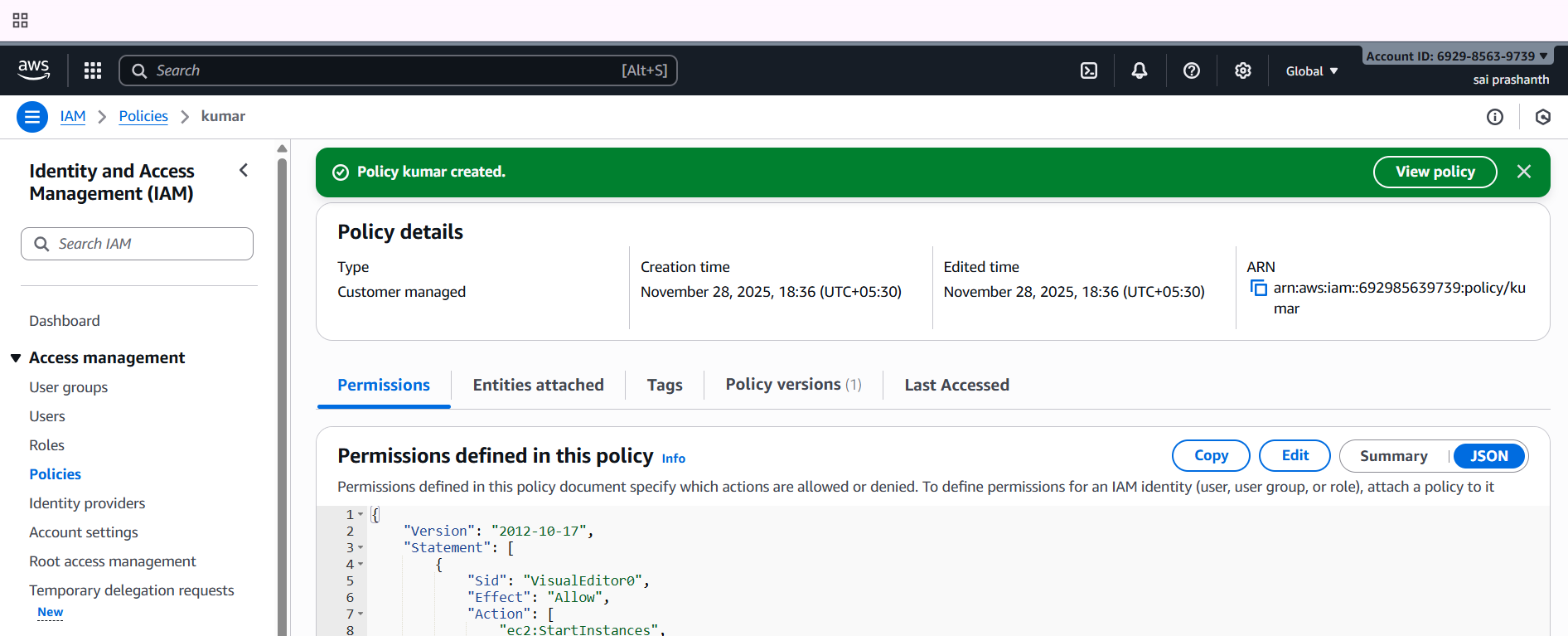
**now click on create policy**

****

**policy has been created**

**to view the policy, click on view policy**

**you can see along the policy in json format**

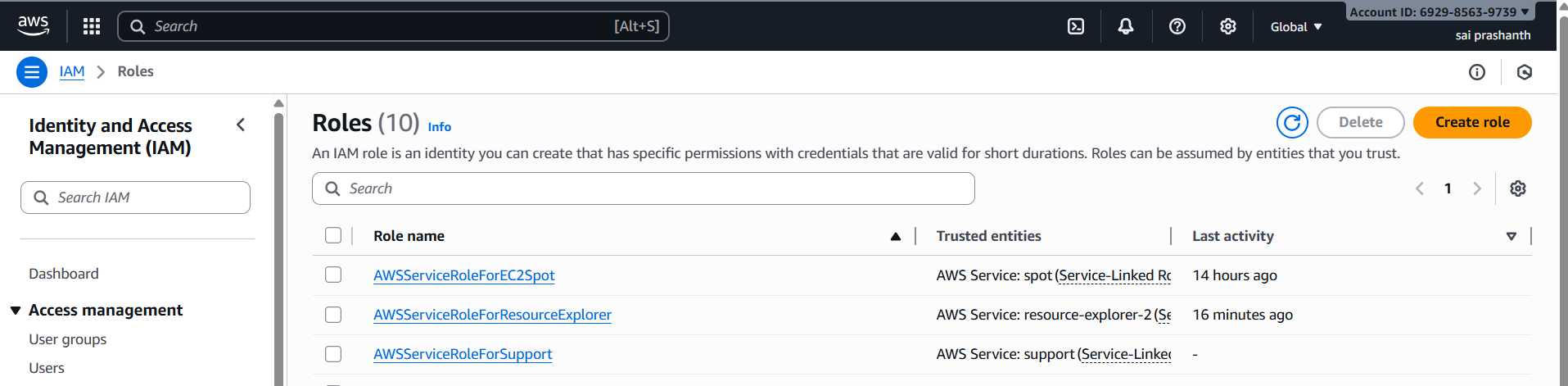
****

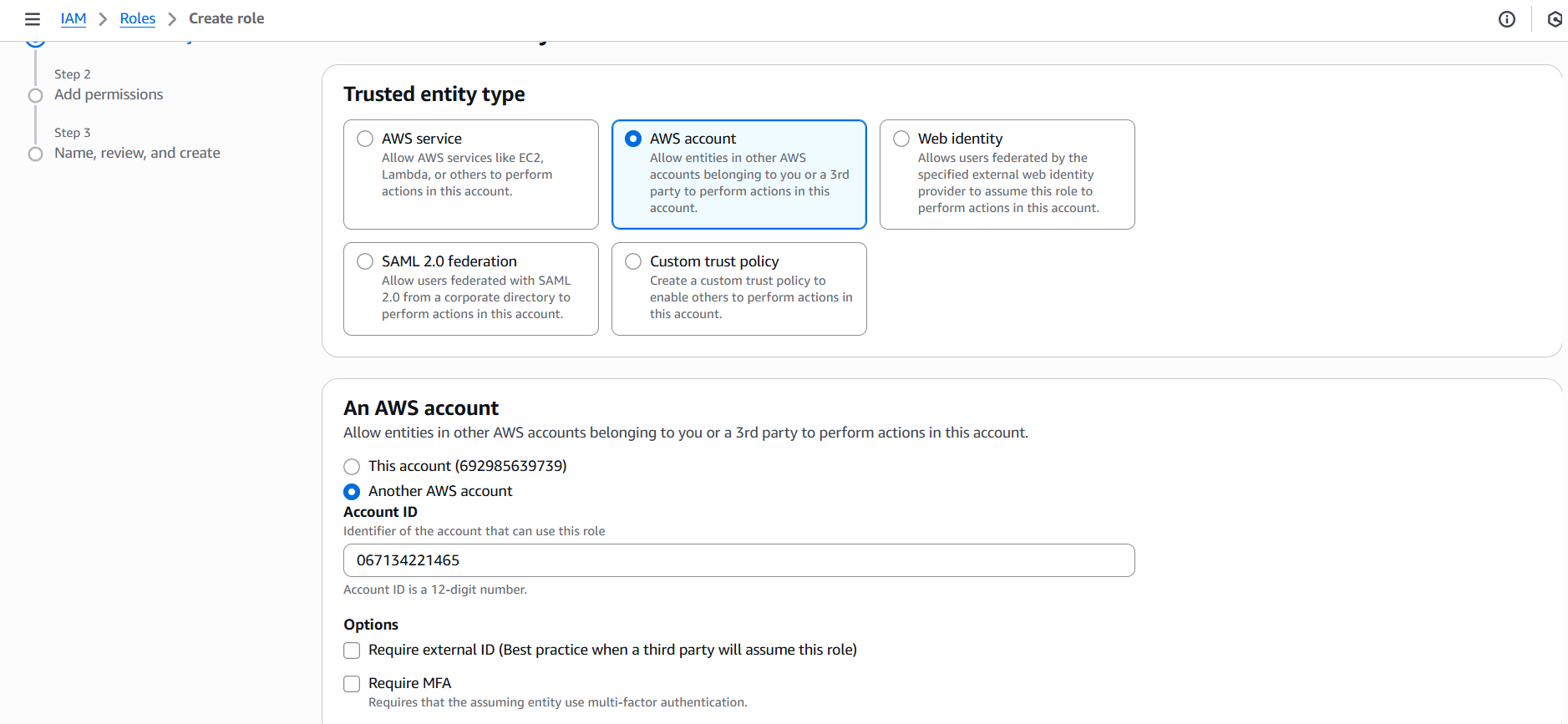
1. **We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.**

first am accessing as account B with Maninder account A

first created role with another account A id and entered A account number

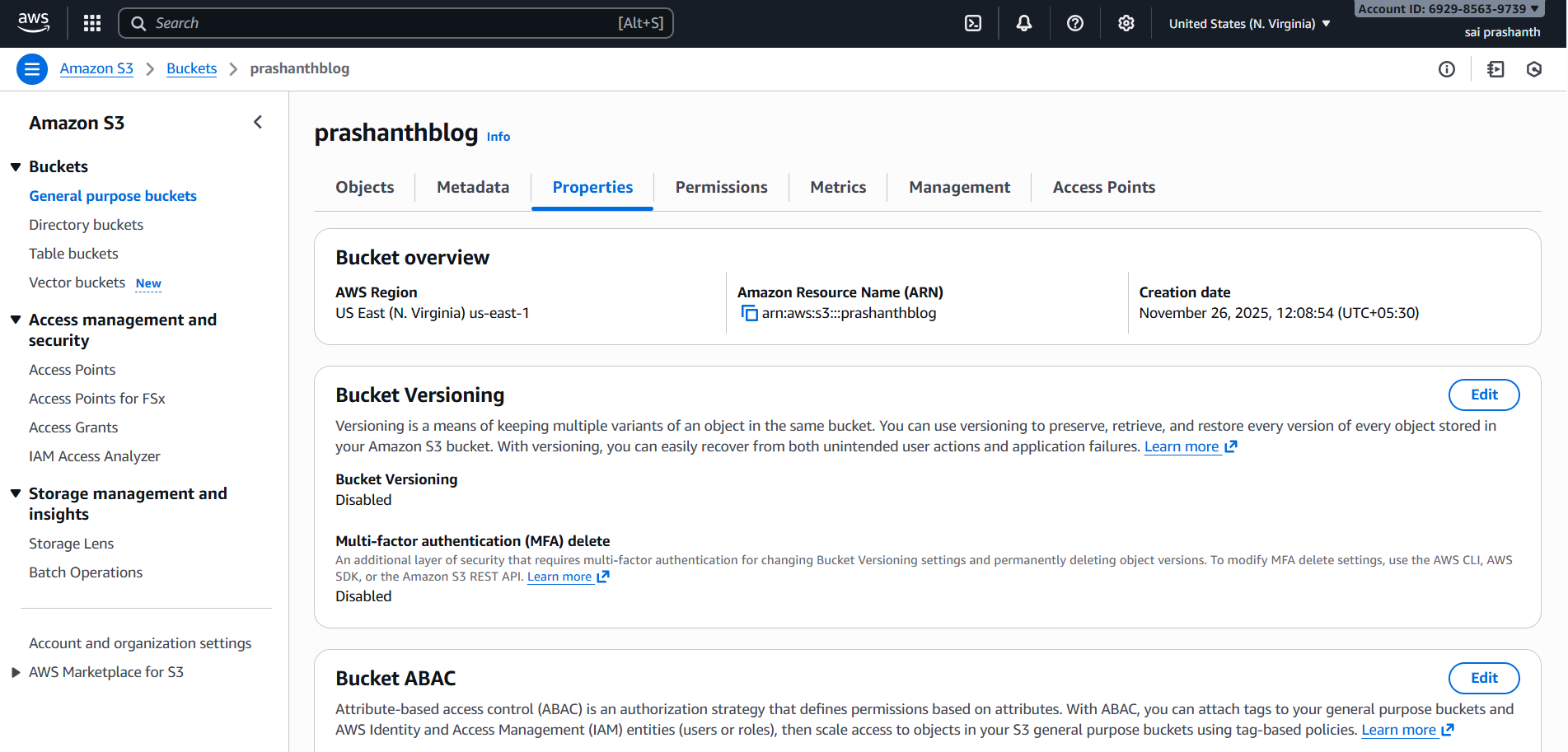
created role



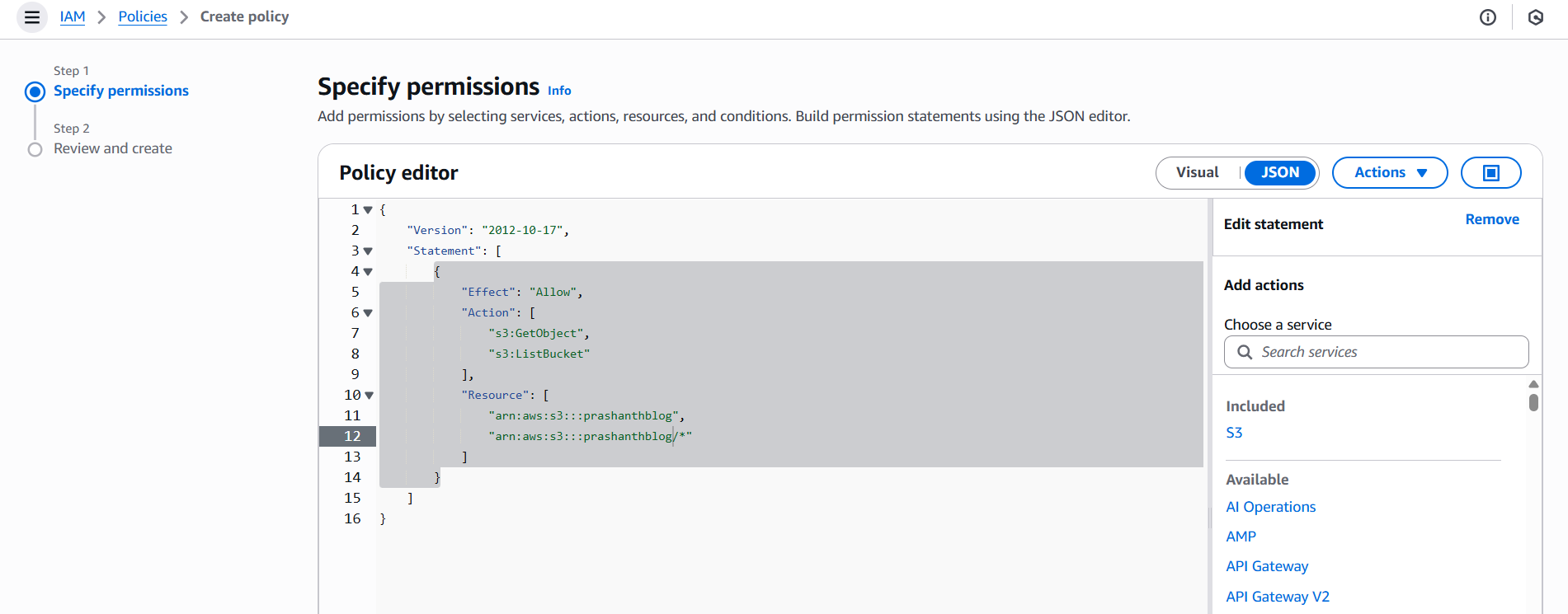


now selected the bucket which I want to give access to account A

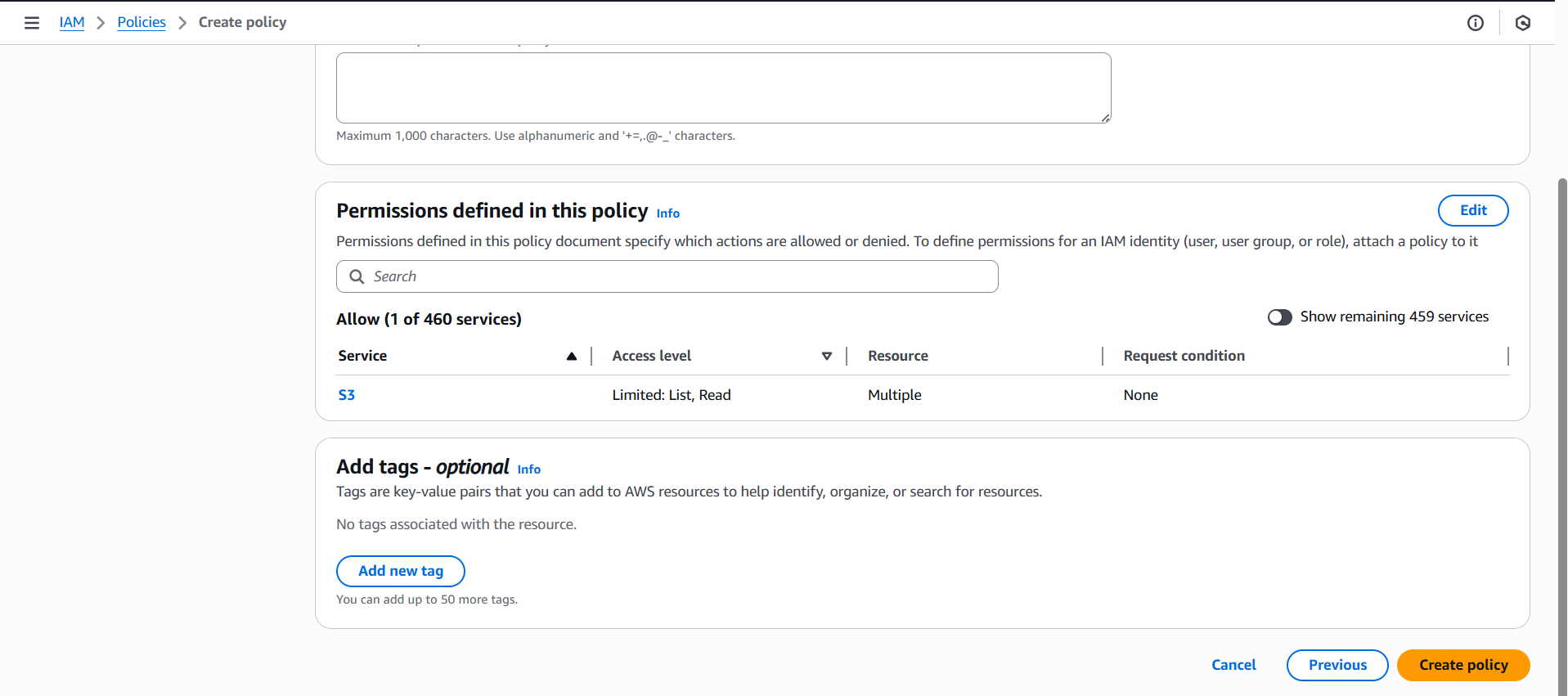
permissions—created bucket policy--



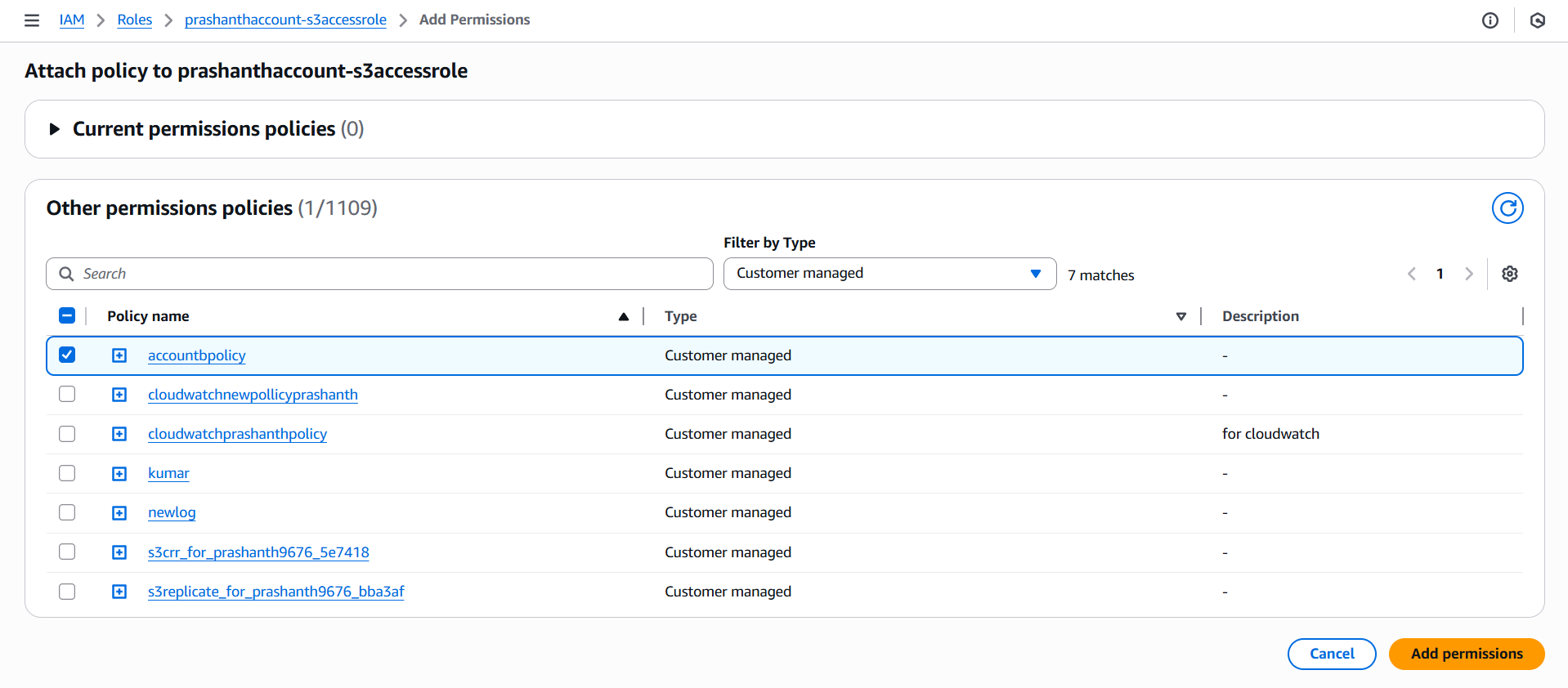
I have entered following son content in the policy editor which will give access to my bucket



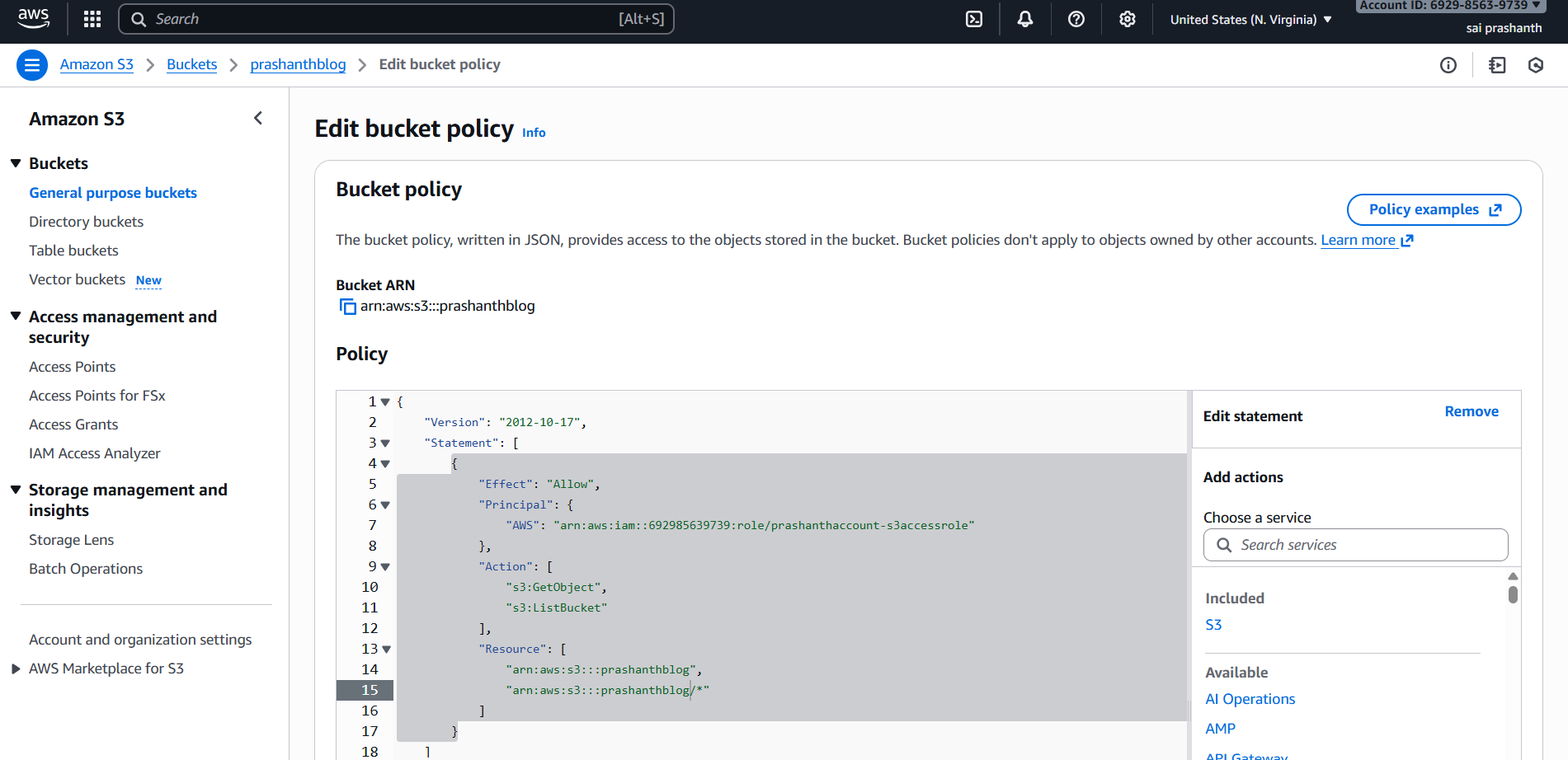
now clicked on created policy



now attached the policy to the role which have been created earlier



npw go to bucket Prashanthblog and edit bucket policy and now added the arn role number in the principle section and also given the bucket arn numbers



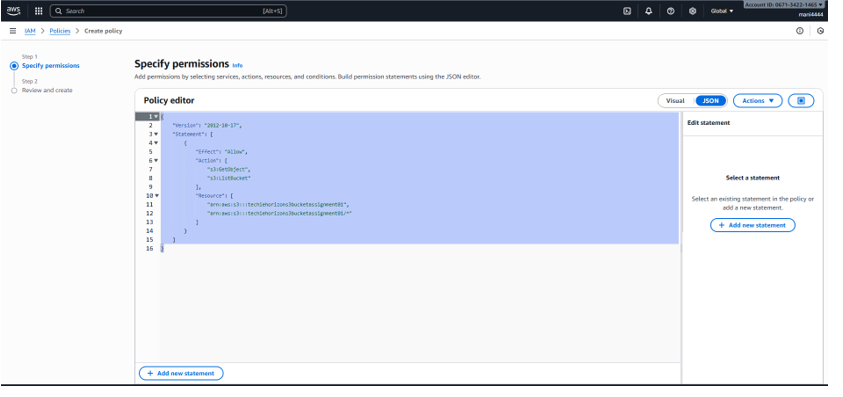
now to view the bucket list objects in account A

after doing the aws configuration account A can see the bucket objects list

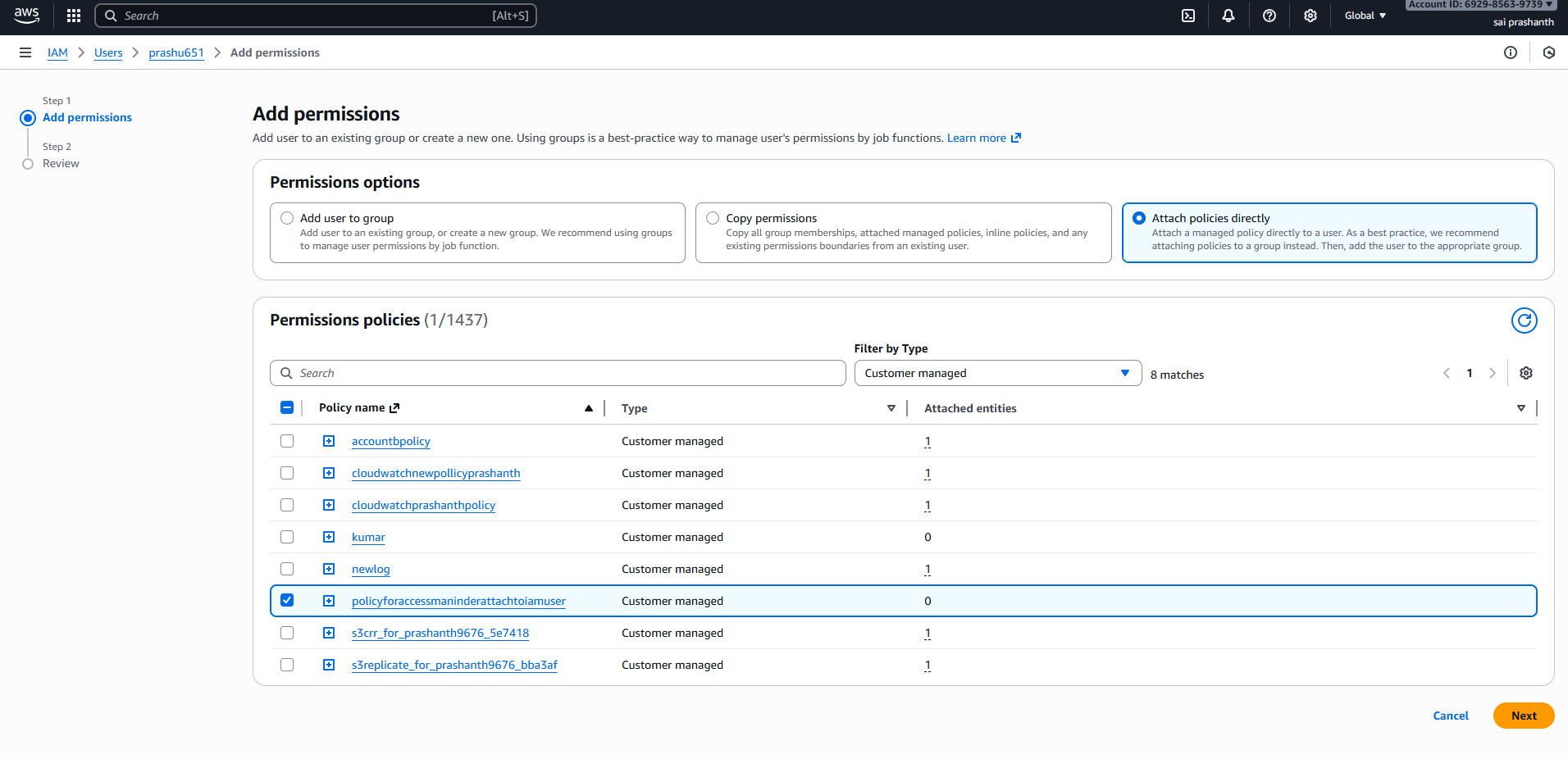
part b

now iam configuring as account A and Maninder as account B

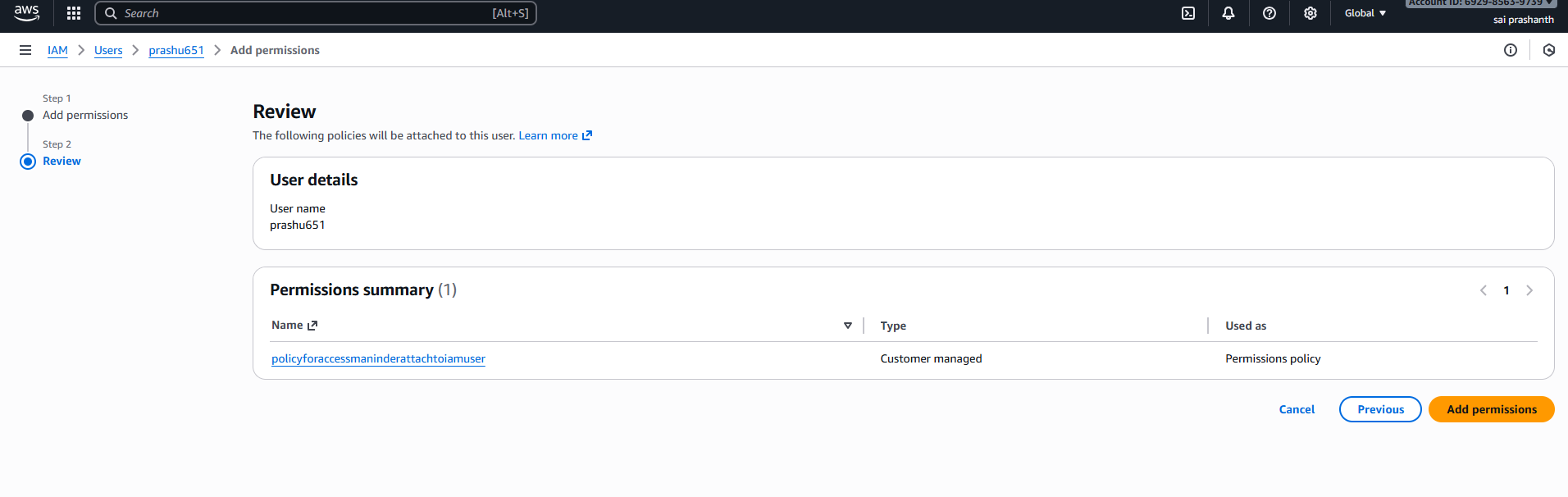
he created policy



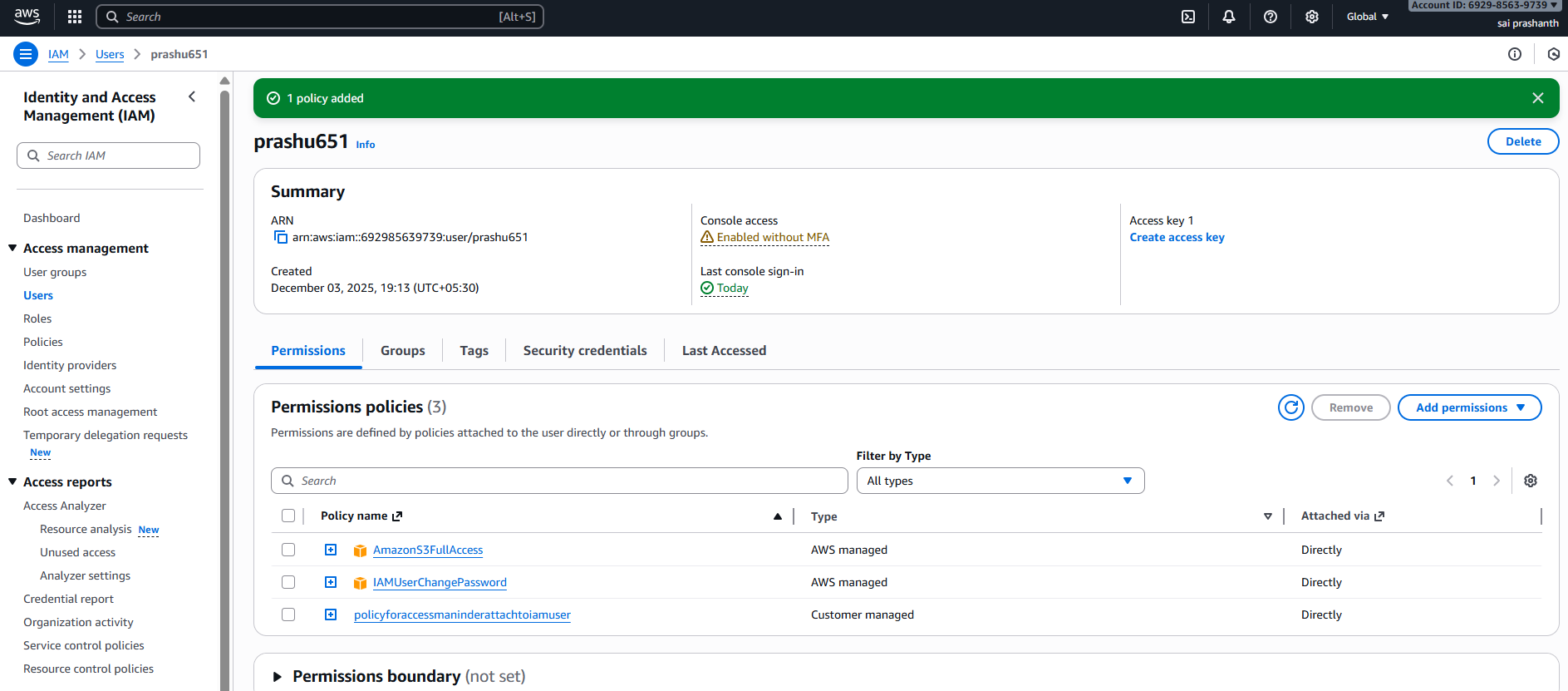
and gave name as policyforaccessrolemaninder and click on next



added permissions for particular user



and now the permissions have been added



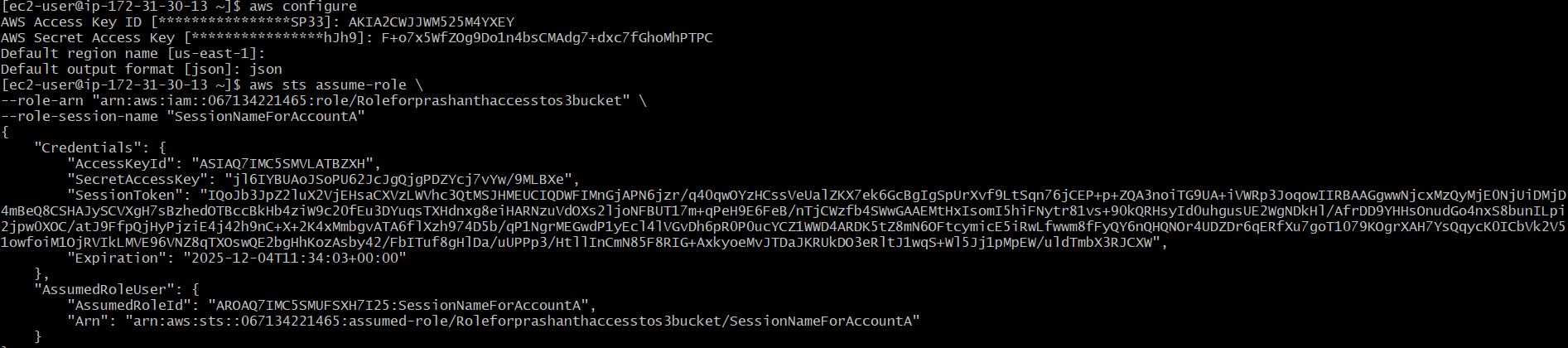
now login with iam user

copy the access and secret key to do aws configure

go to gitbash and connect through ssh

aws configure—access key—secret key—aws sts assume role/

so that temporary credentials will be received



now again we need to configure

and enter the temporary credential details

now enter his bucket name

aws s3 ls s3://techieassignment01/

we can see the list of objects in the bucket

