**Practical-3 Identity Access Management.**

[Login as root user

Search iam (manage access to aws services)

Go to users write name create user

Giving access:- go to ARN(auto enable console ; what you want to show the user first page

Custom password you can set

Auto by computer

Then after copying the link sign in to I am user

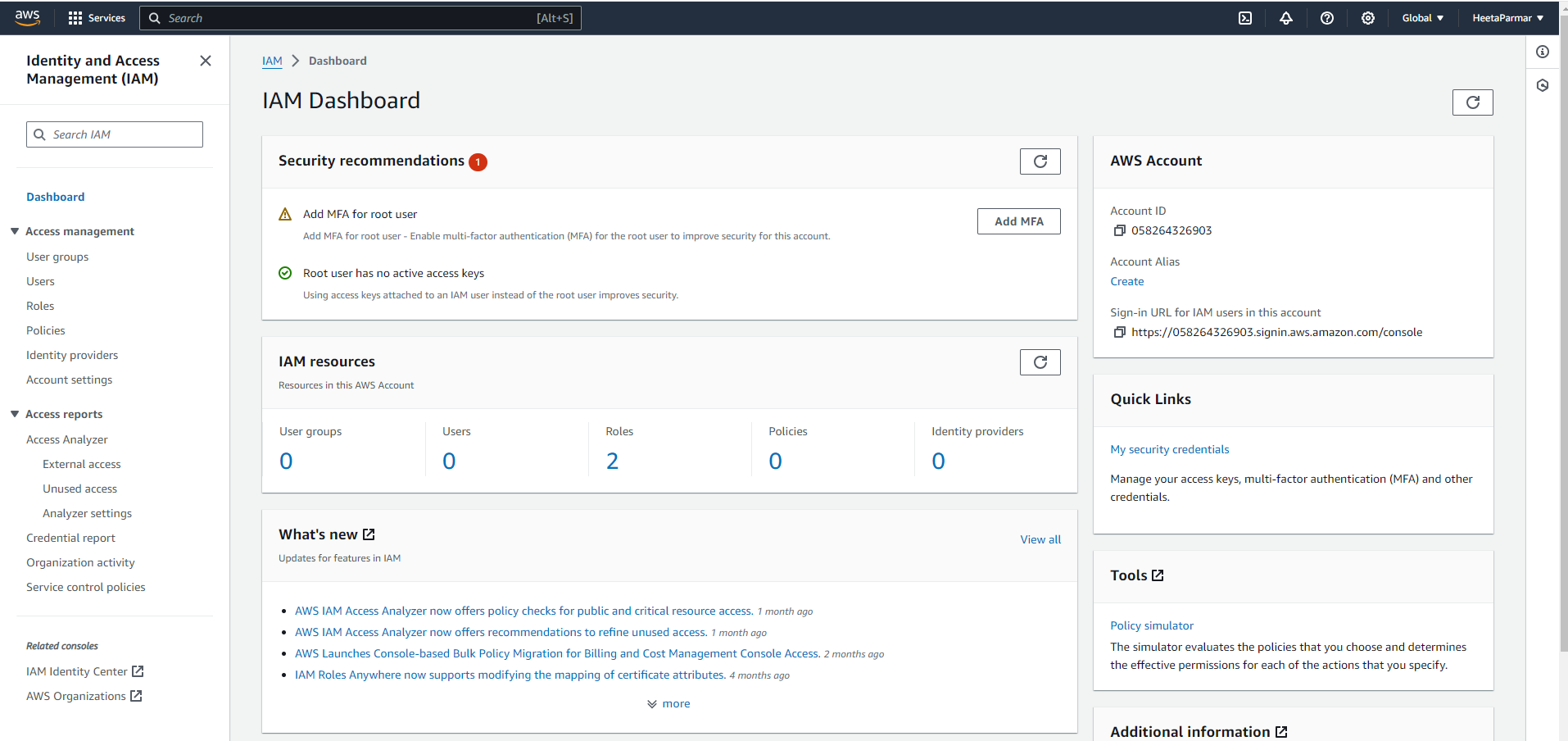
Create policies select service –S3 effect=allow sid name of root user create

go to json

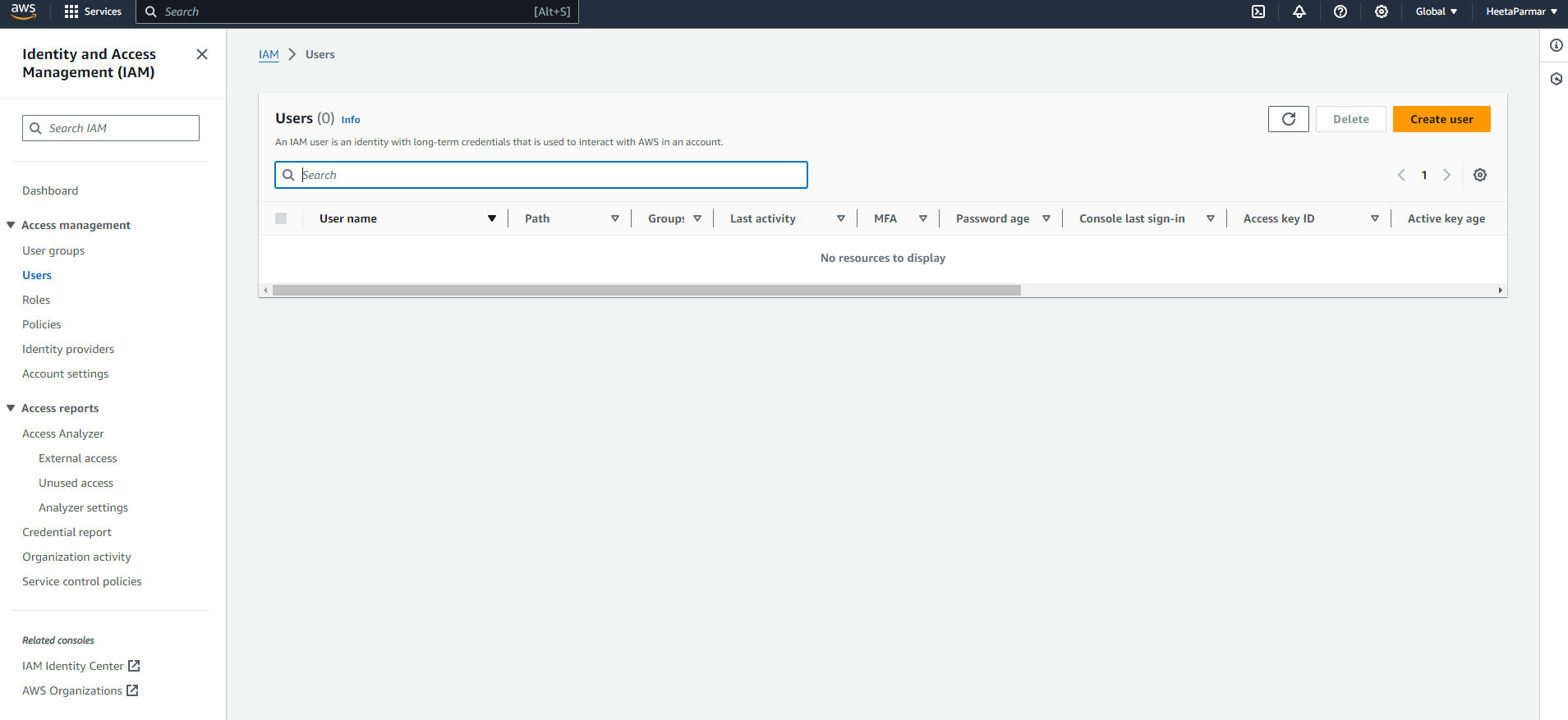
visualise : graphical access select s3 allow all options(\*)

root user add permission attach policy search and add permission ]

**1: Search IAM Identify and manage access on AWS services)**

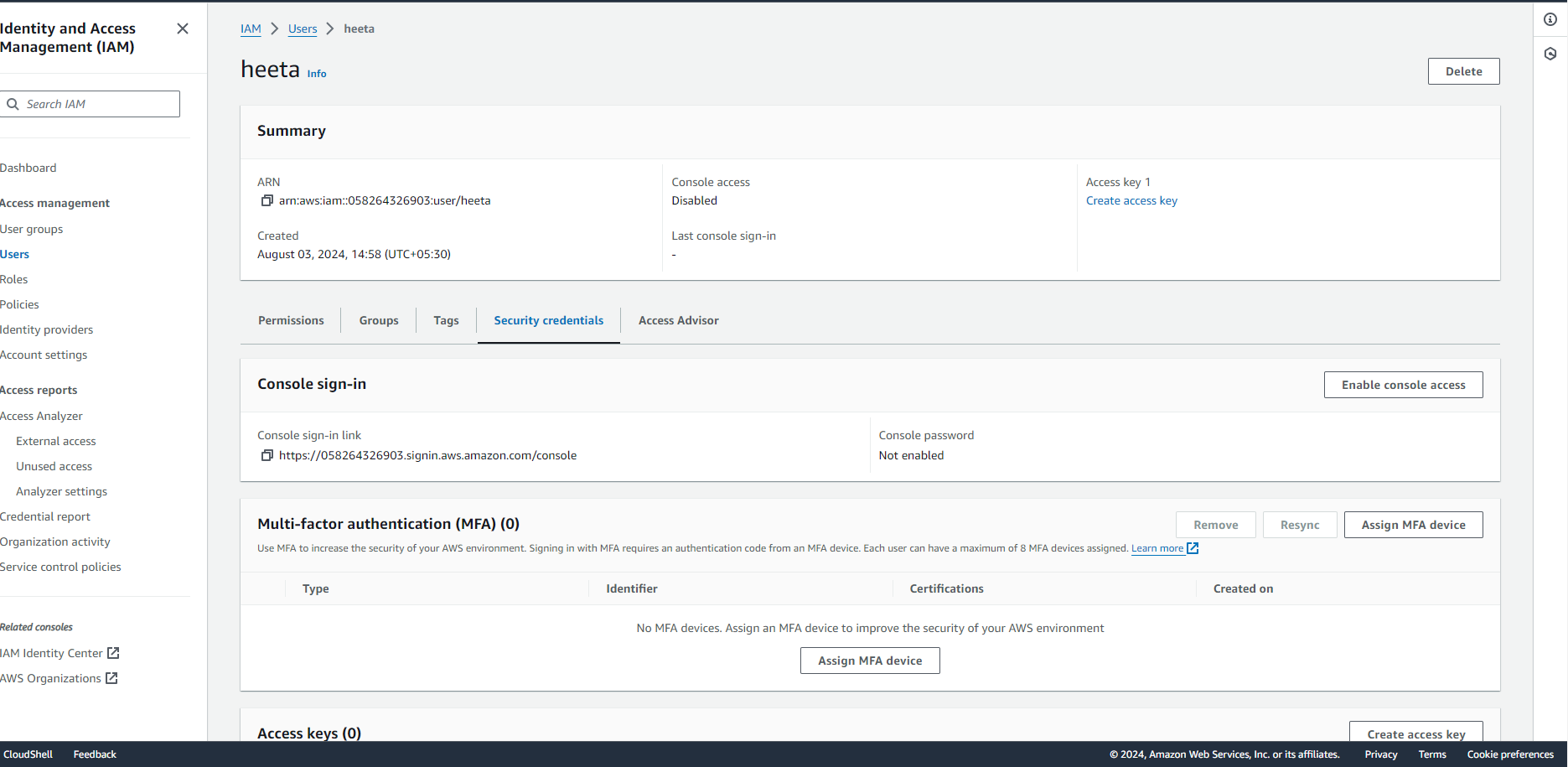


**2: Go to users ----> write name--🡪 create user**

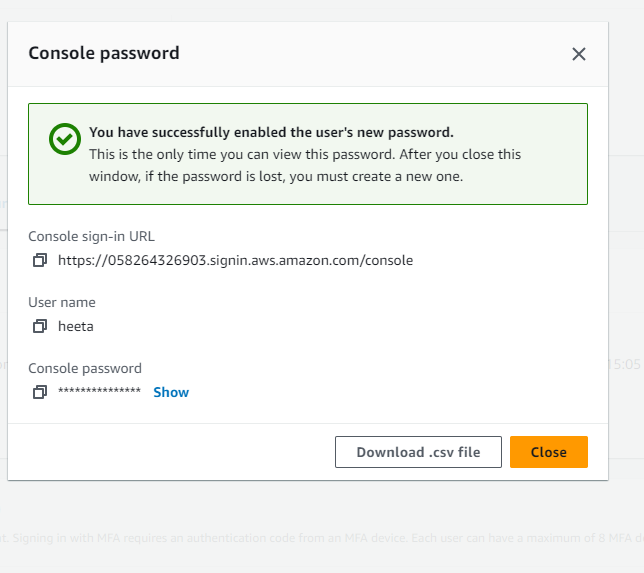


3**:Once the user is created we can create password by two method a)autogenerated b)custom**

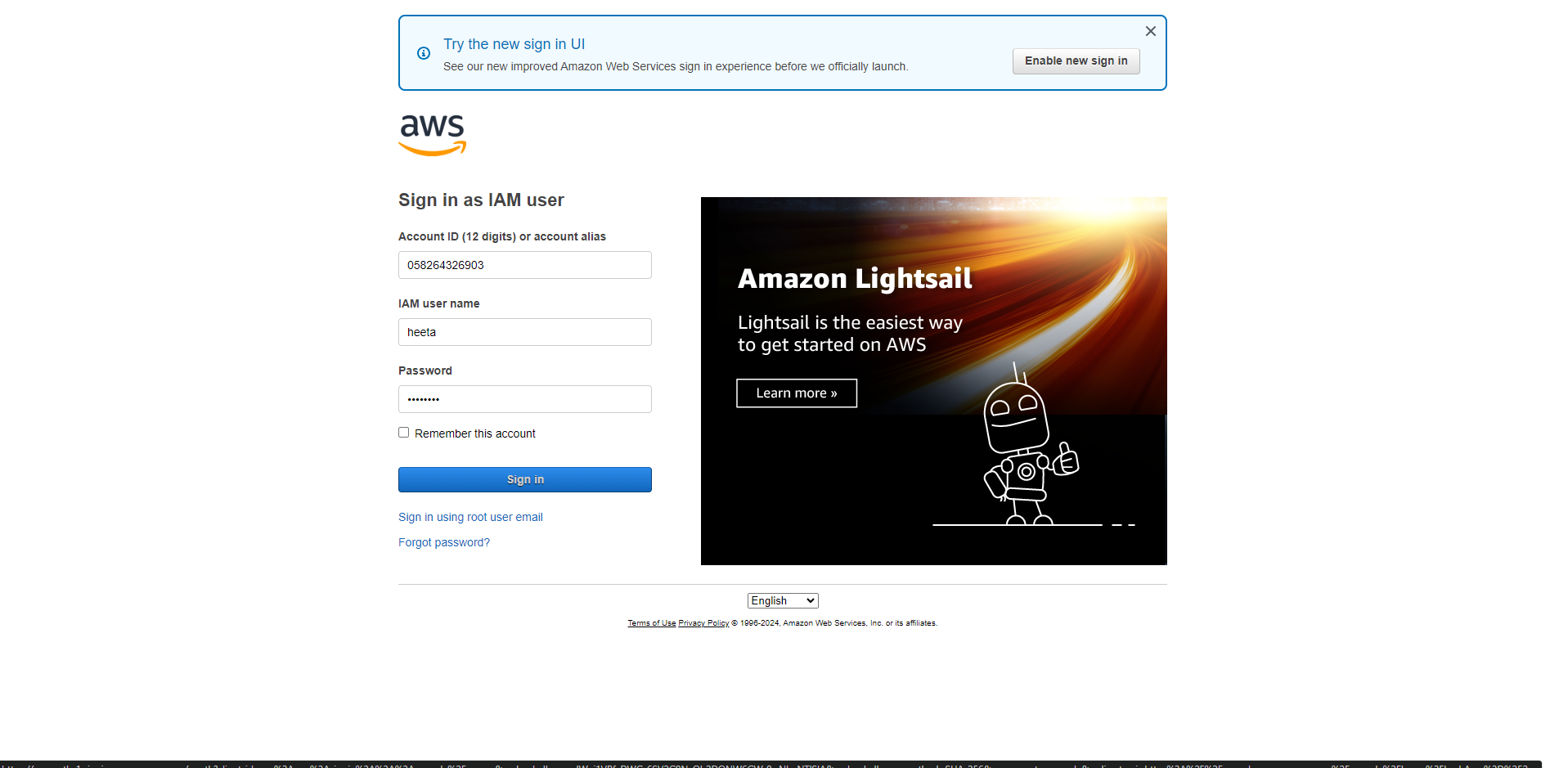
**Tap on the user name that you created. Go into the Security credentials and enable console access.**



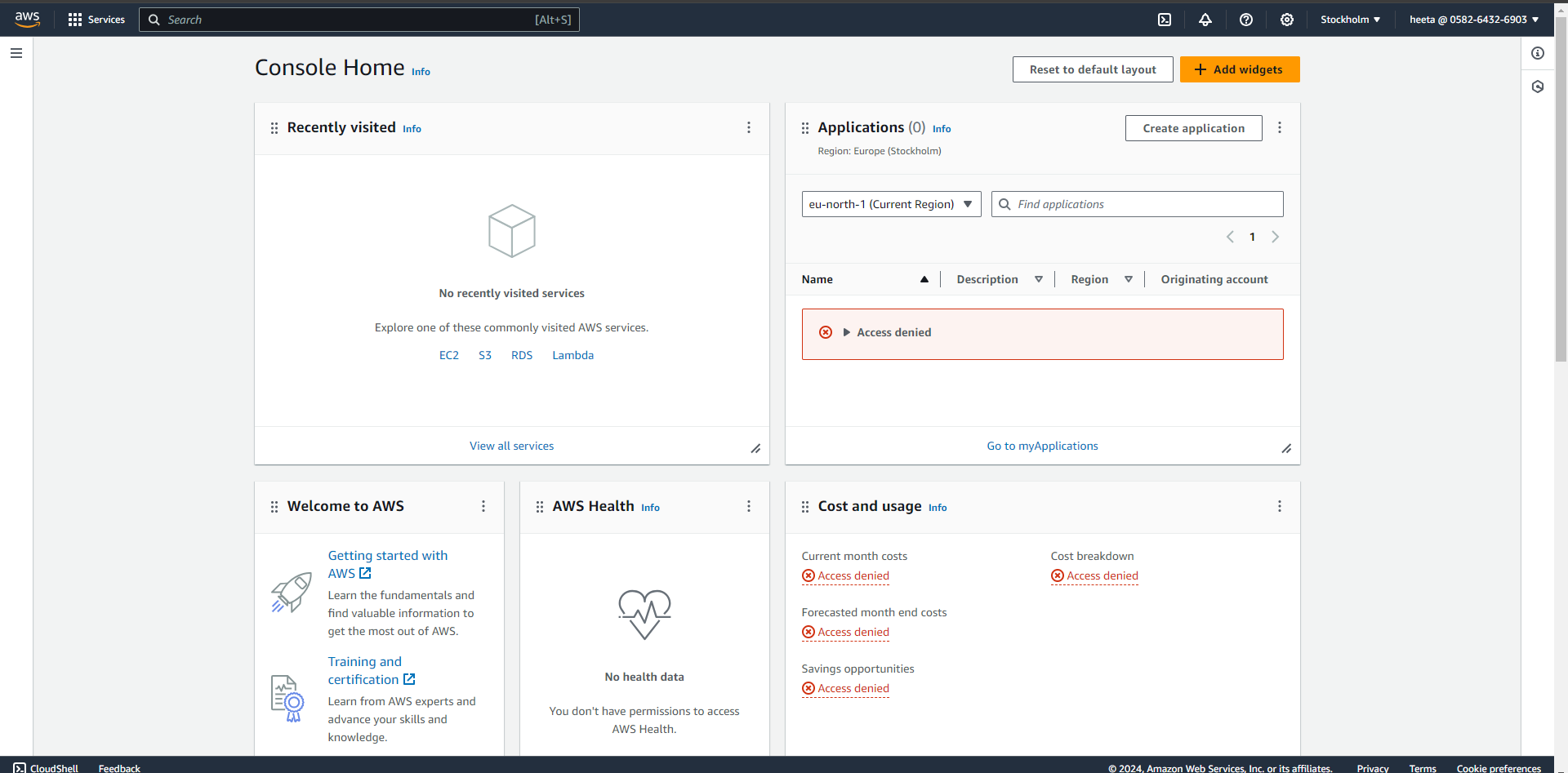
**4: this is what will appear after enabling the console access. The ARN link is the link from which other i.e I AM user can access the account .**



**5: Copying the ARN and logging with I AM user**



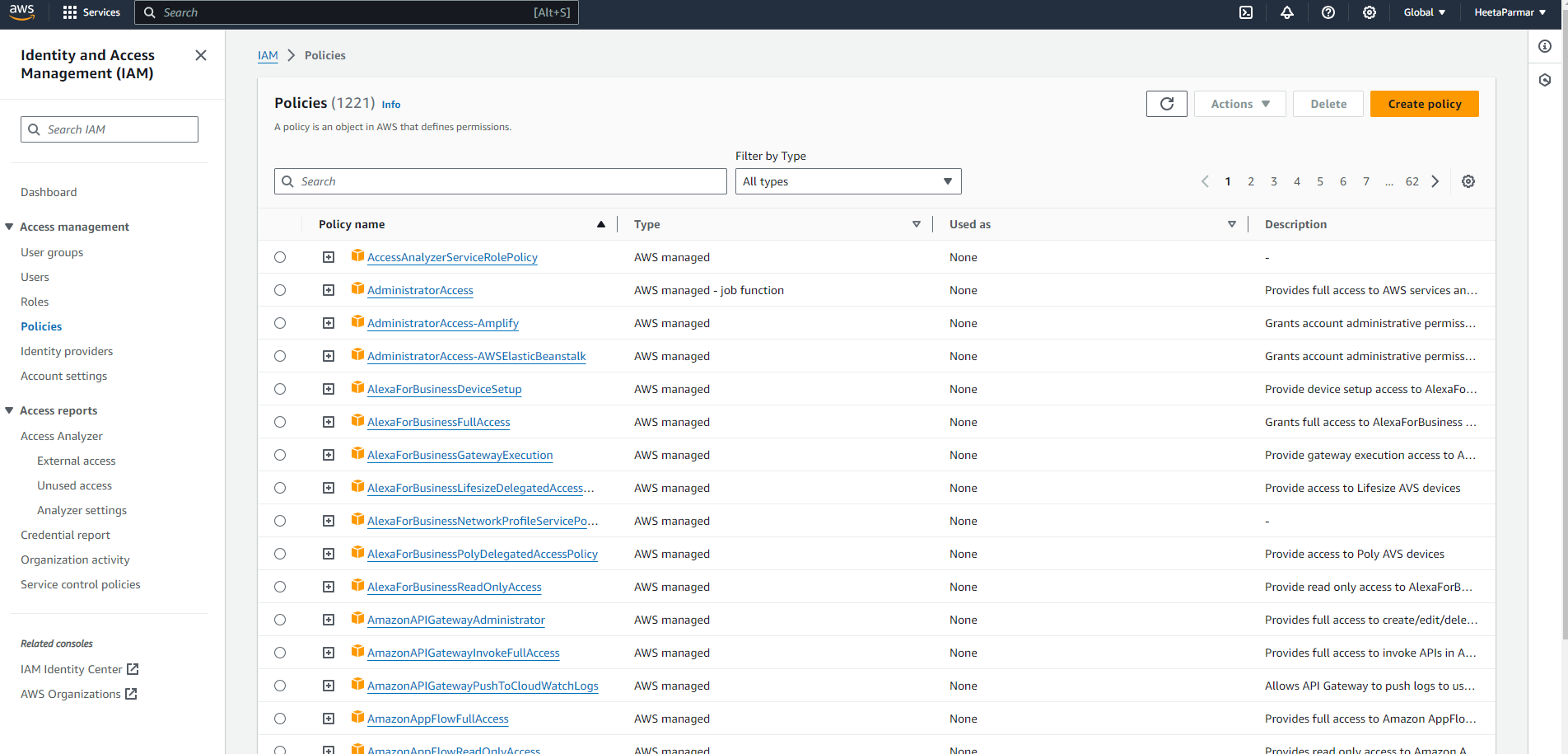
**6:Unless and until the access to delete or update or create the buckets,EC2 is granted the IAM user can’t perform those tasks the access is denied .**



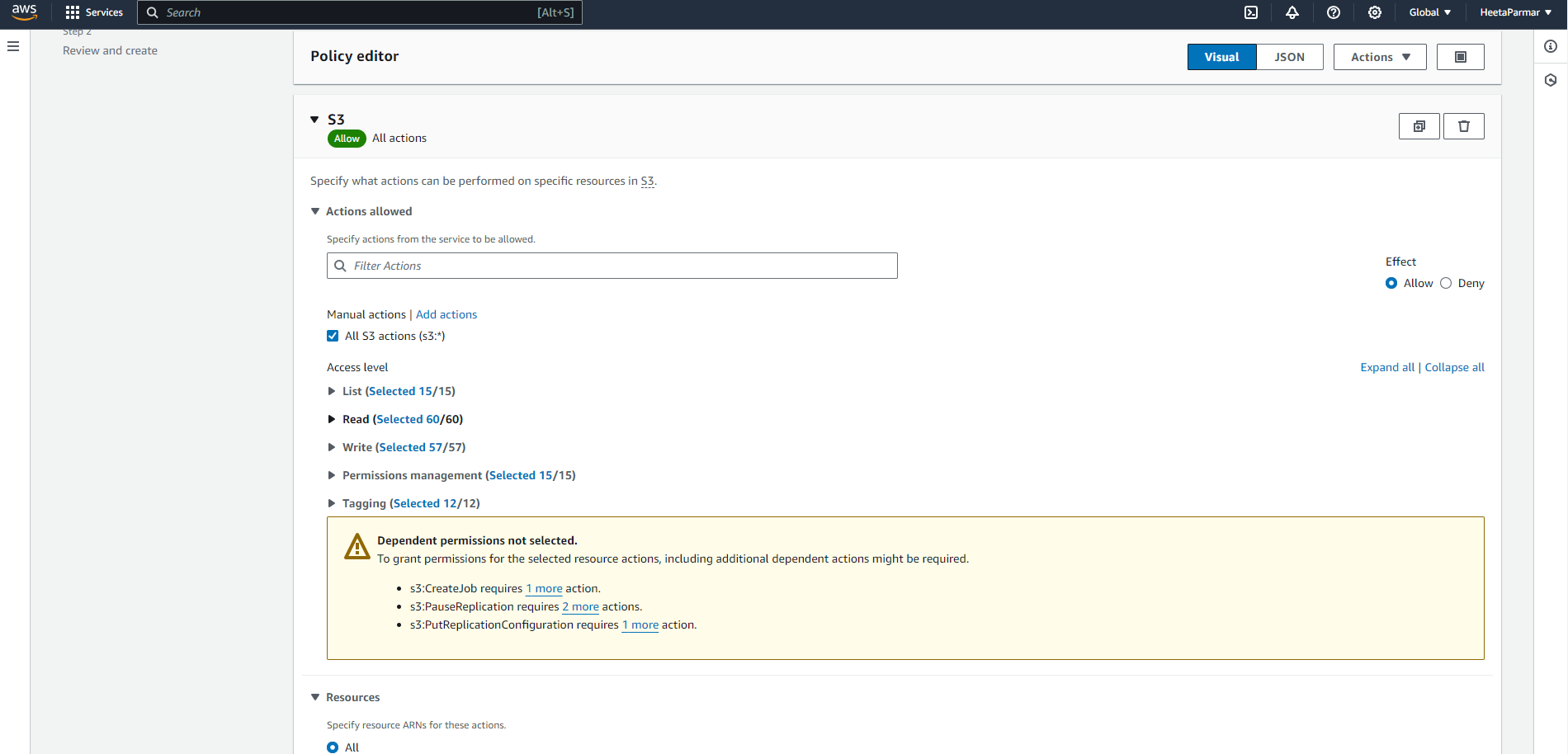
**7:To unable those access we need to create a policy for the same .**

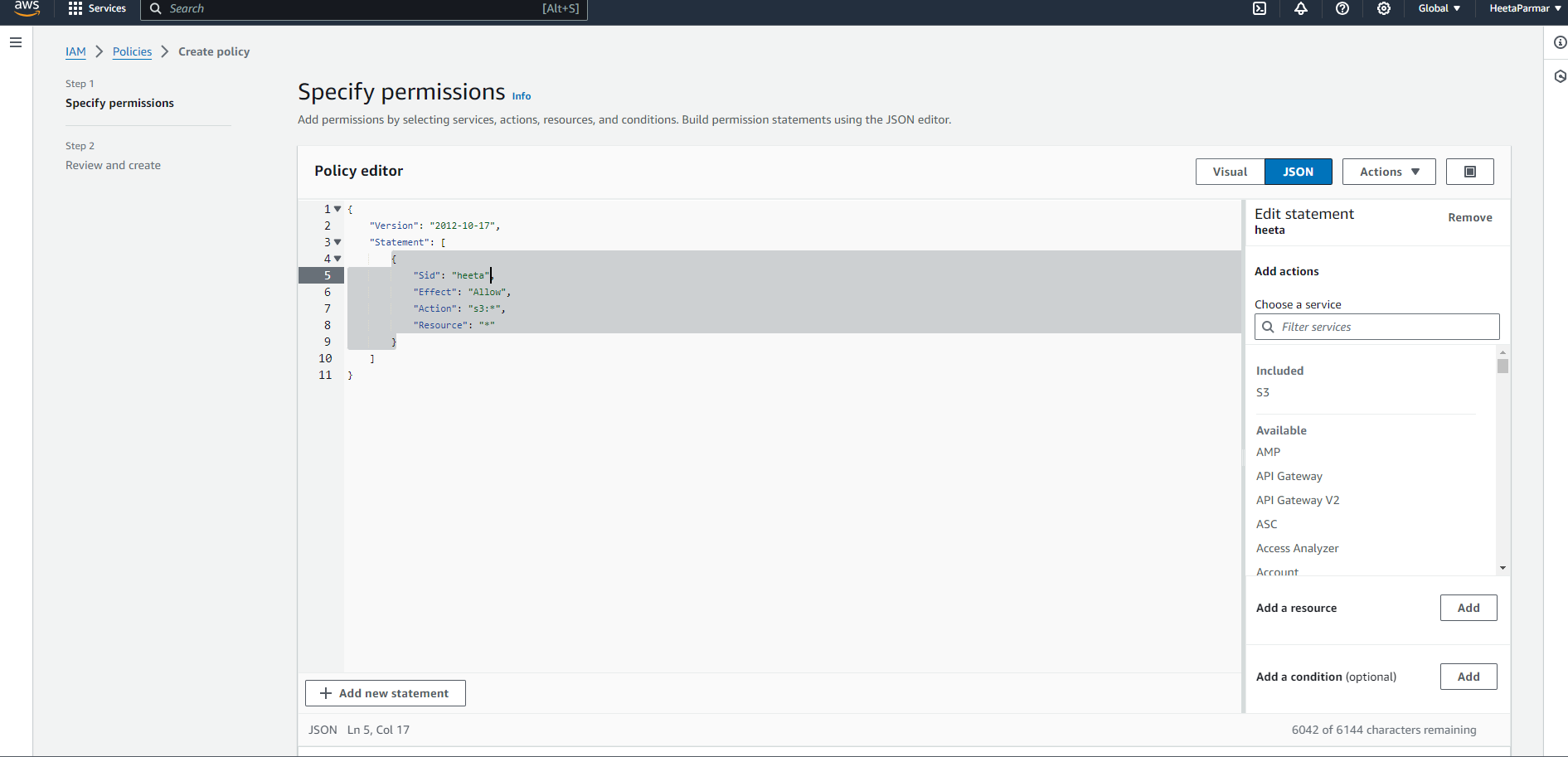
**Left side of the window comprises of the option policy then create policy .**

**Once the policy is created attach it to the user name.**

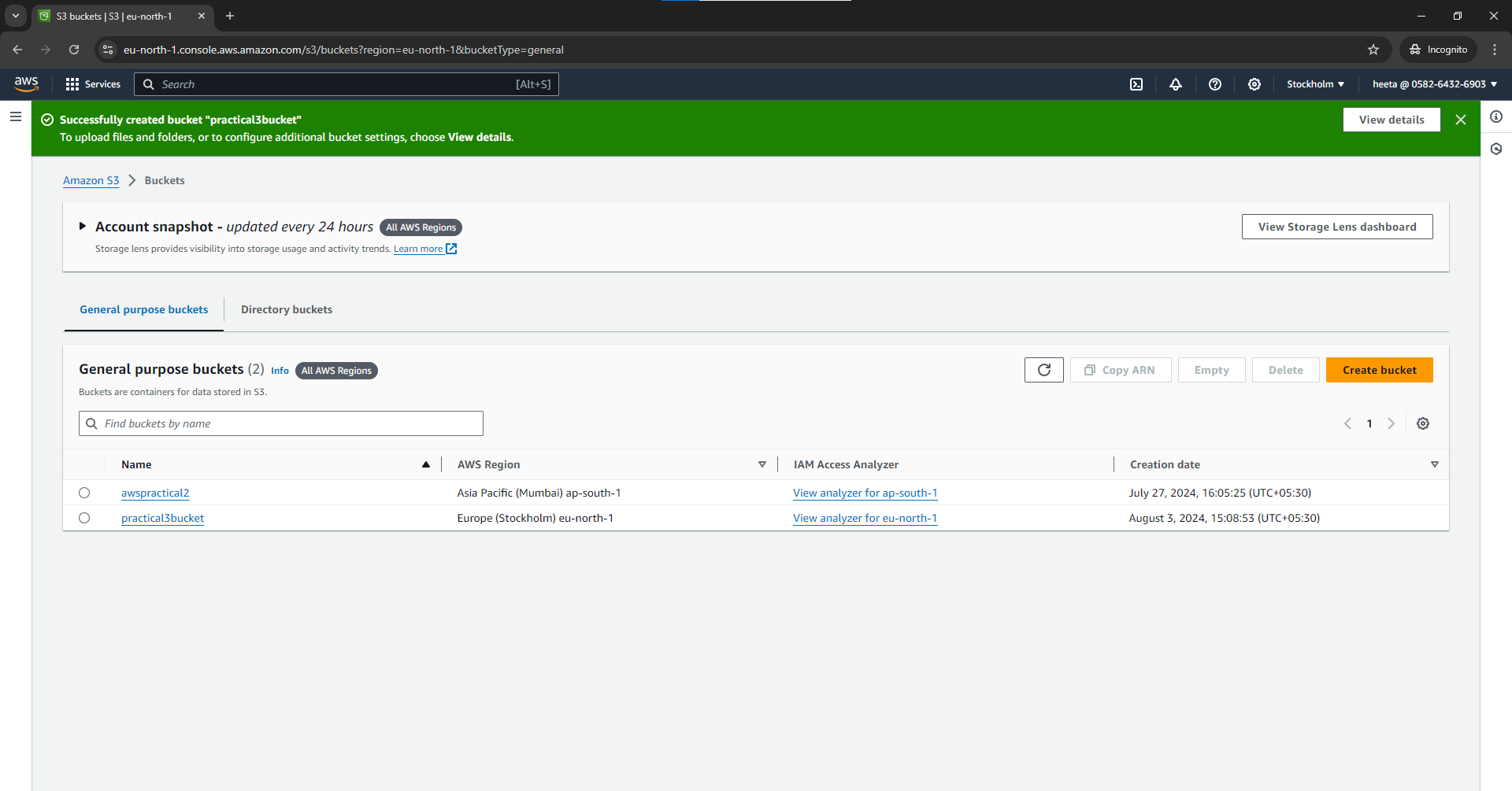


**8:Granting permission .change the sid to the user name .**





**9: Now, the IAM user can successfully create a S3 bucket .**



**#FOR EC2 . After selecting the policy select ec2 instead of s3 bucket . and do the necessary required changes. Rest all steps are same**

