IAM-Policies-Assignment-—-2

Problem Statement:

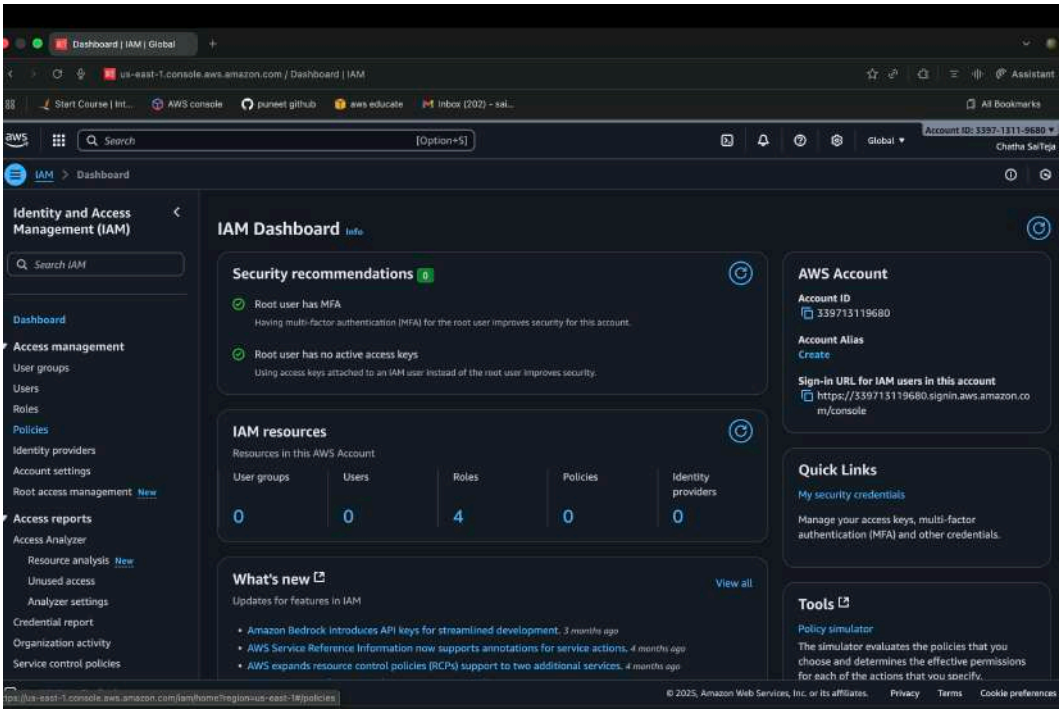
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
    a. Access S3 completely
    b. Only create EC2 instances
    c. Full access to RDS
2. Create a policy number 2 which allows the users to:
    a. Access CloudWatch and billing completely
    b. Can only list EC2 and S3 resources
3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Step-By-Step Procedure:-

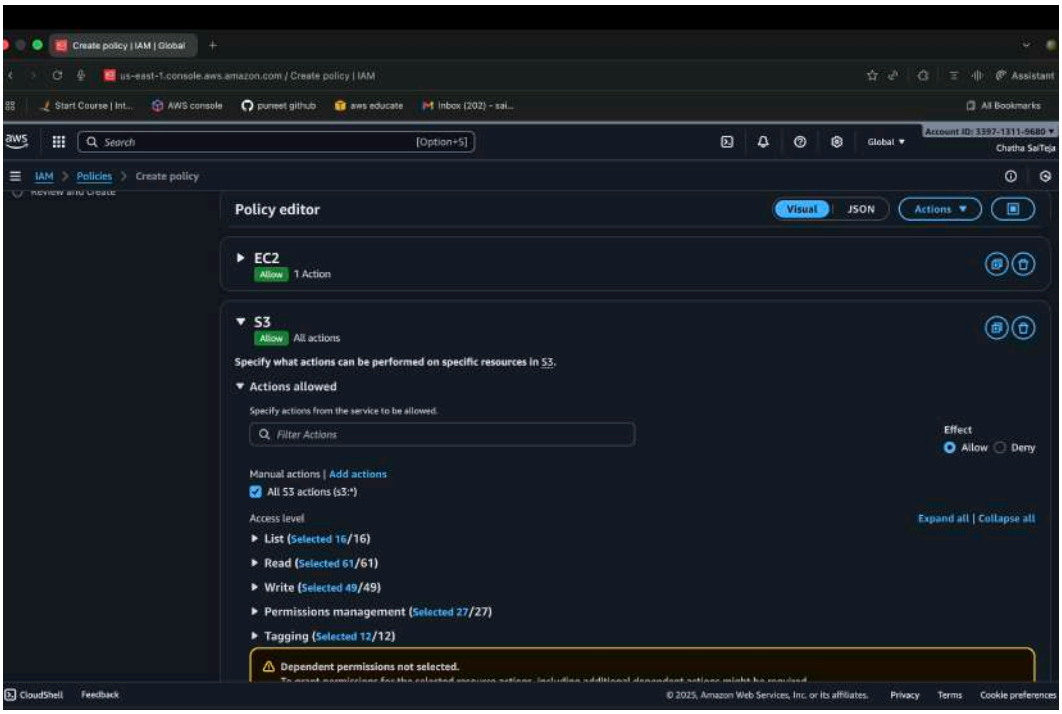
Step1:- Go to AWS and Search for IAM Service we can see a dashboard go to policies.



IAM Dashboard click on policy

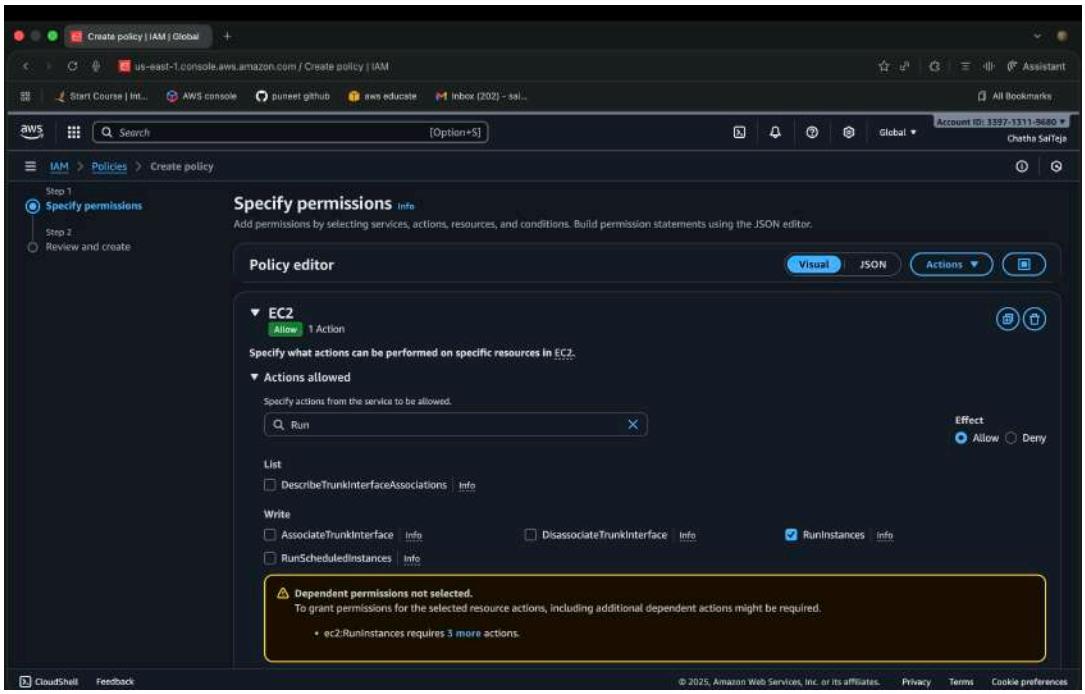
Step 2:- Click on Create Policy the first step to create policy is by specify the permissions , we can add more permissions by clicking on add more now we have to create Policy1 with Access S3 completely, Only create EC2 instances, Full access to RDS.

A) Access S3 completely :- we have to add permission to the policy in permissions by selecting the service (S3) and allow the effect and allow all actions to give S3 Full Access.



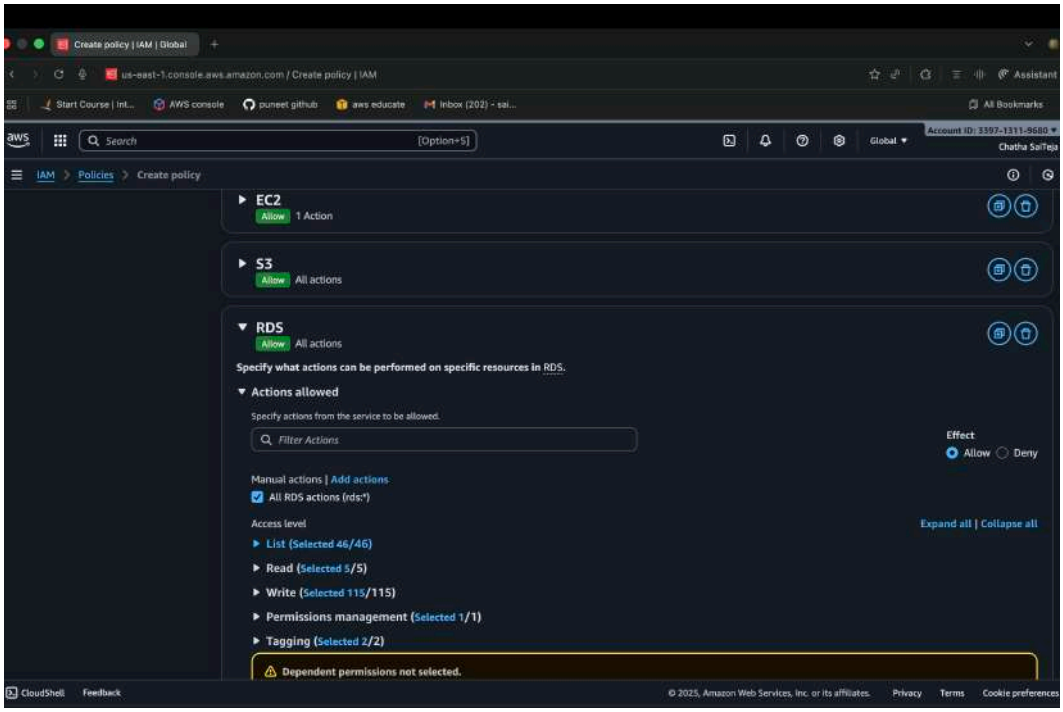
Full access to S3

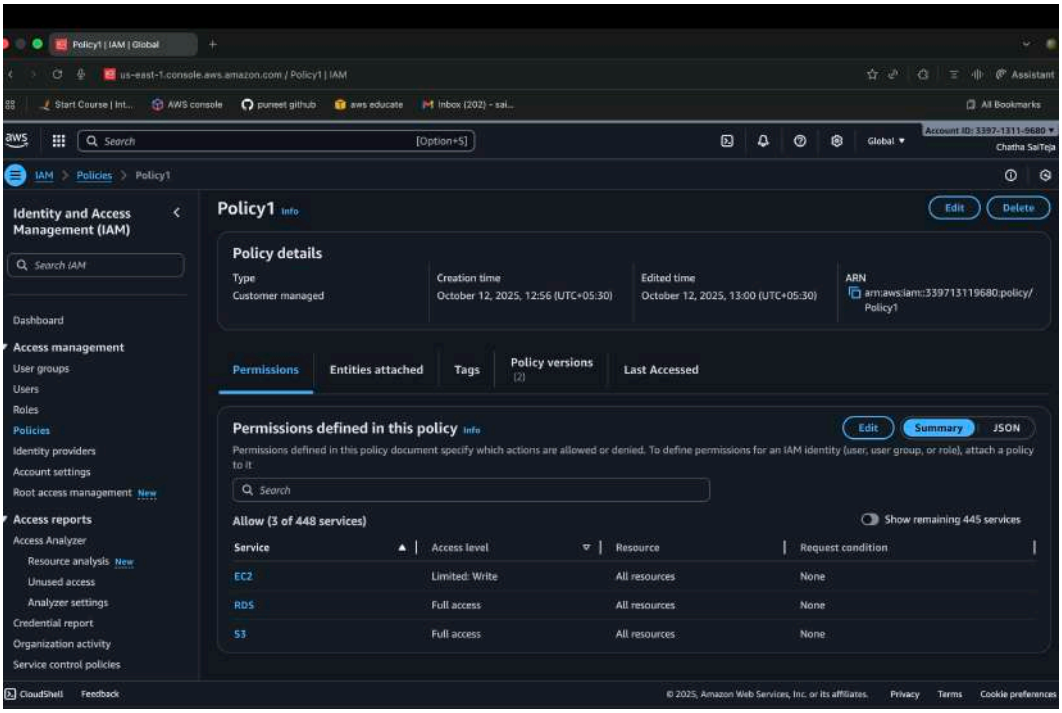
B)Only create EC2 instances:- Now we have to add the permissions to only create Ec2 Instances, so select the service in visual editor and go to actions and enable “RunInstances”(write) .



Only create EC2 instances

C) Full access to RDS :- we have to give Full access to RDS ,select the service RDS in visual editor and go to actions and enable to all Actions to give full access to the policy.

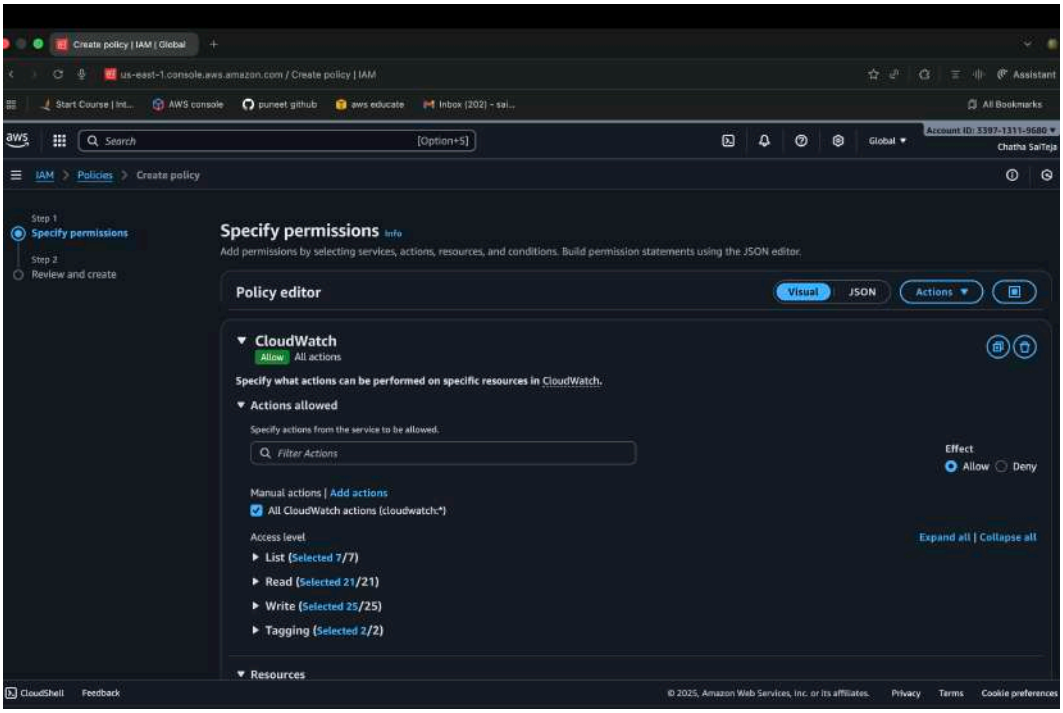




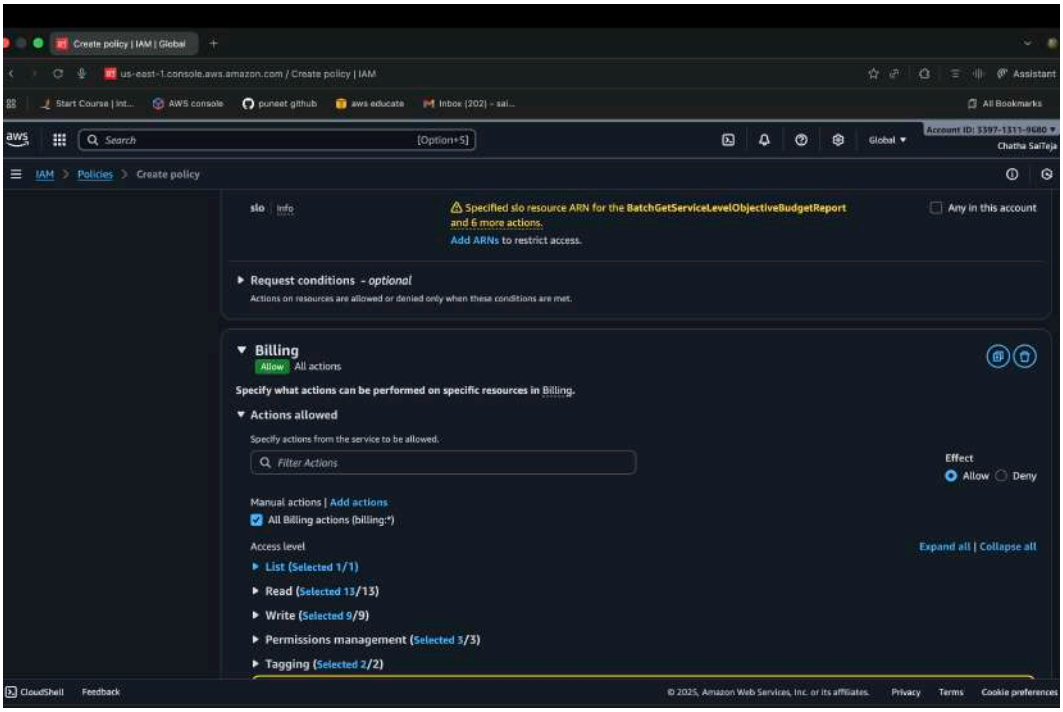
Policy1 summary

Step 3:- Now we have to create another policy - policy 2 which allows users to access cloud watch, billing completely and users can only list EC2 and S3 resources

A)Access CloudWatch and billing completely:- By clicking create policy we have to specify the permissions of cloud watch and billing completely so in visual editor select cloud watch and enable all actions , click on add permission and select Billing then enable all actions .

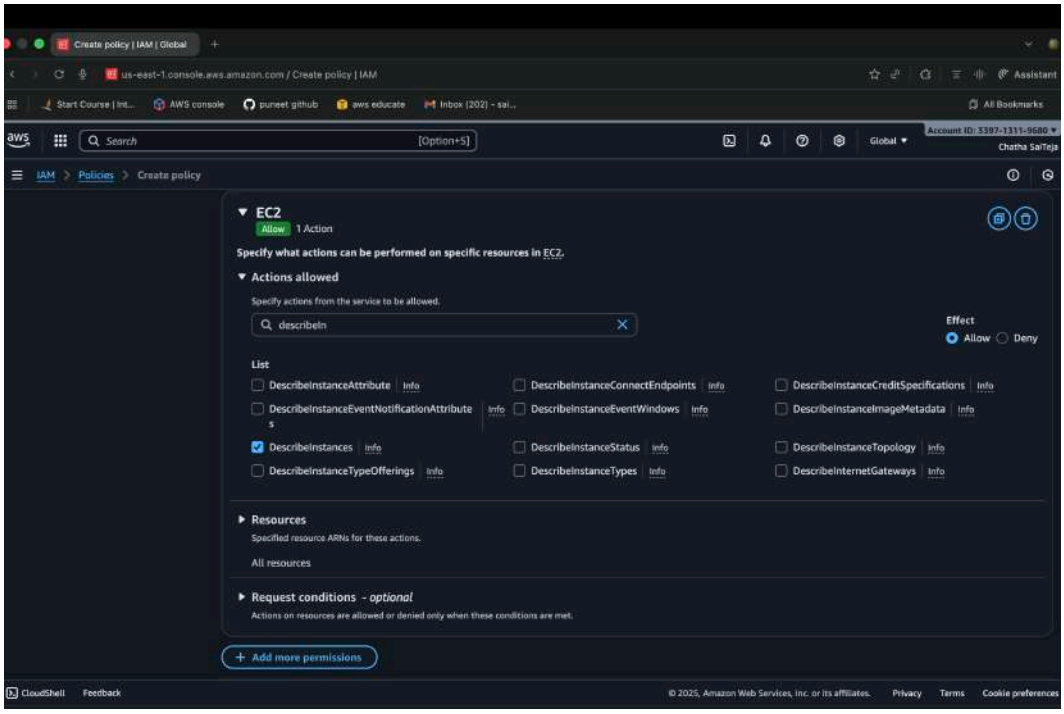


Giving Full access to CloudWatch

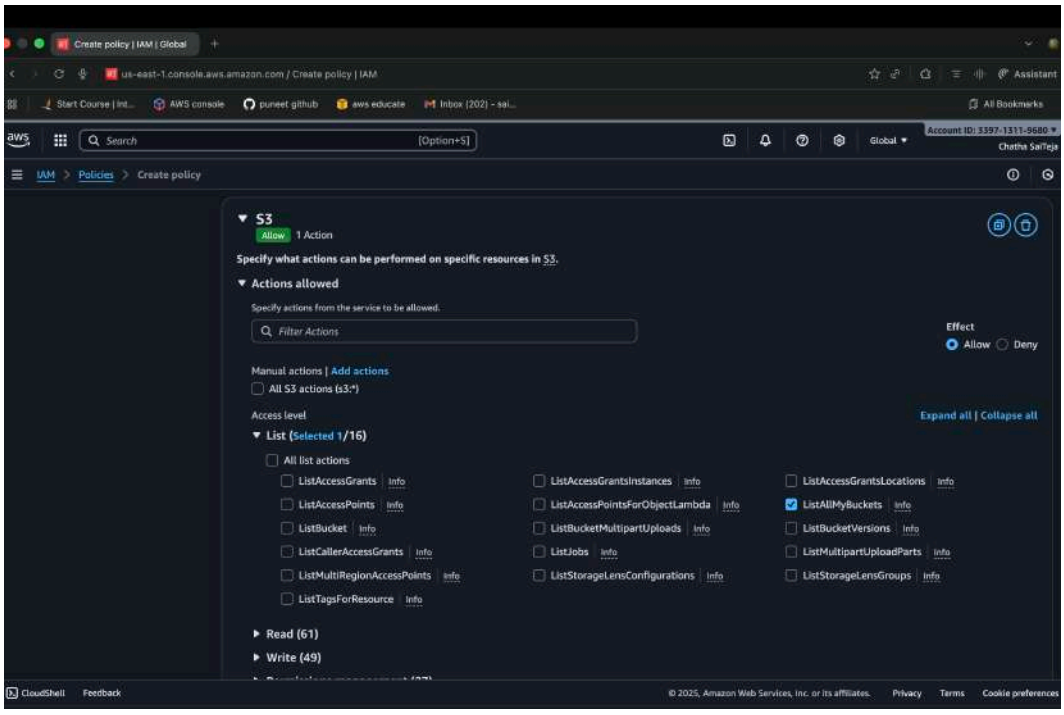


Giving Full access to Billing

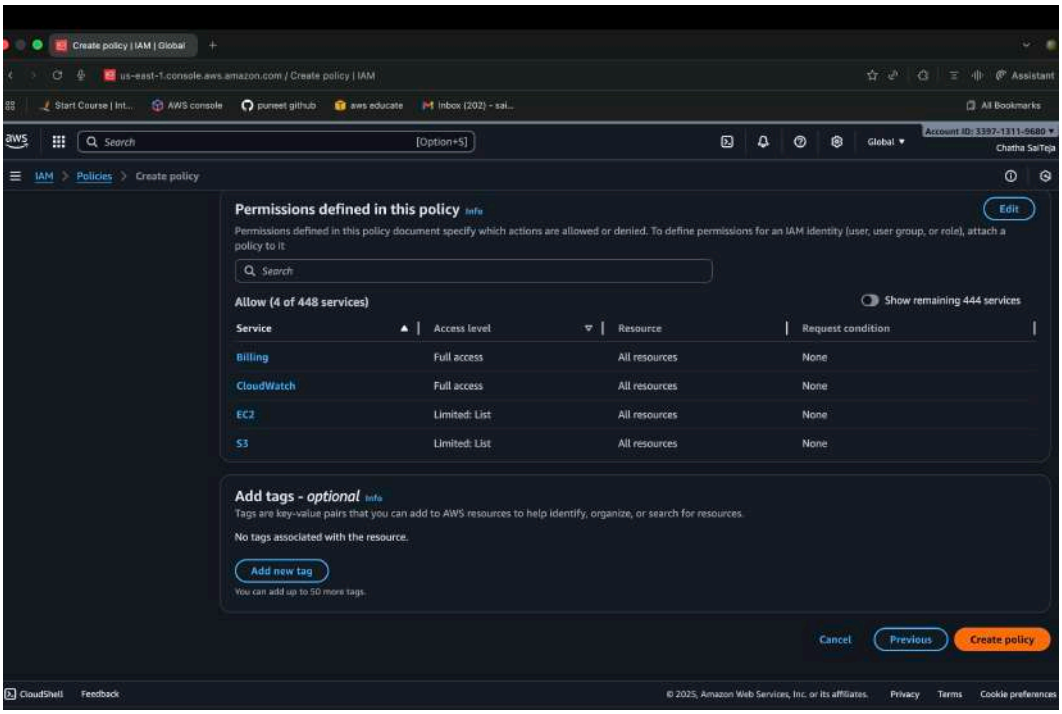
B) Can only list EC2 and S3 resources:- to provide these permissions we have to specify the service Ec2 and enable actions “DescribeInstance” to list all instances for s3 we have to enable “ListAllMyBuckets”



List Ec2 Instances

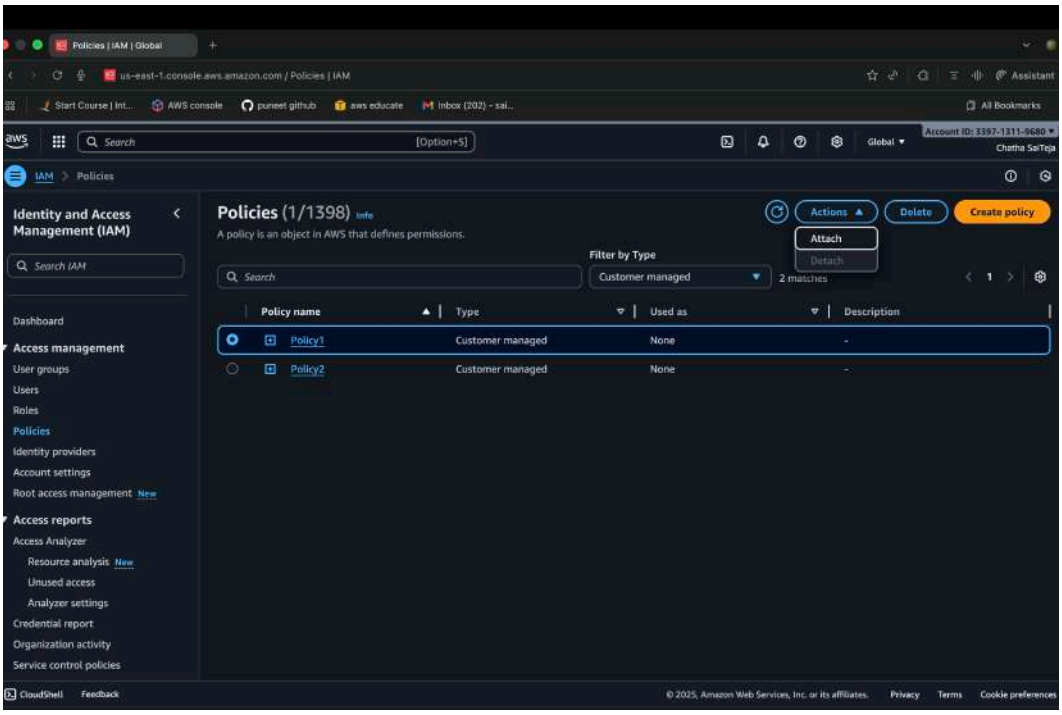


List S3 resources

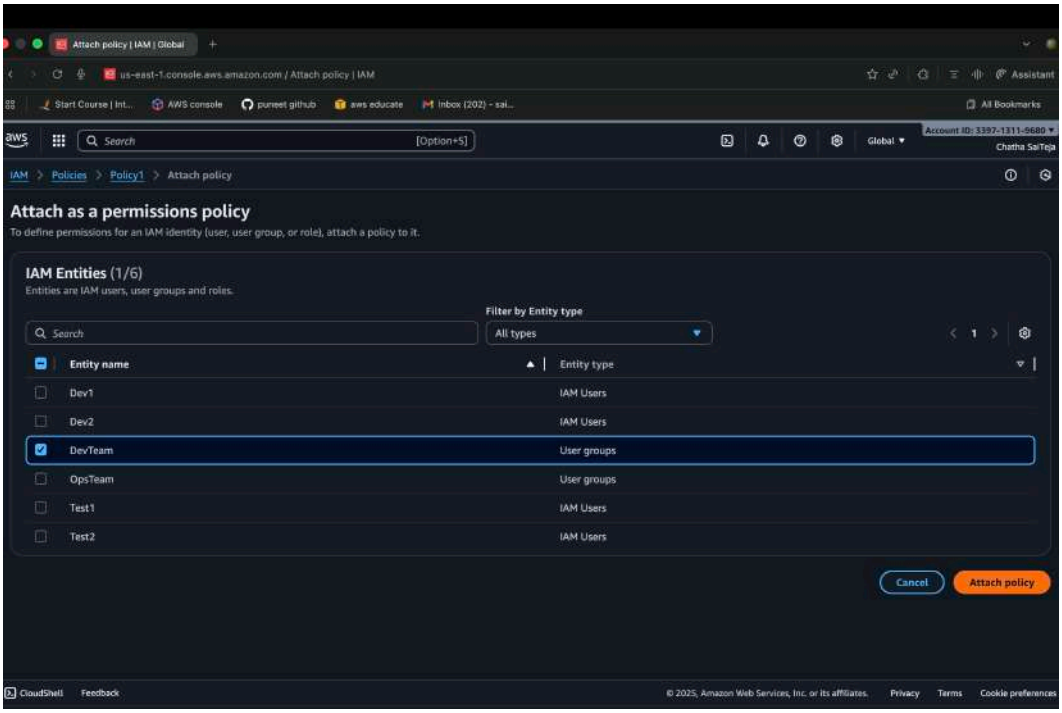


Policy 2 summary

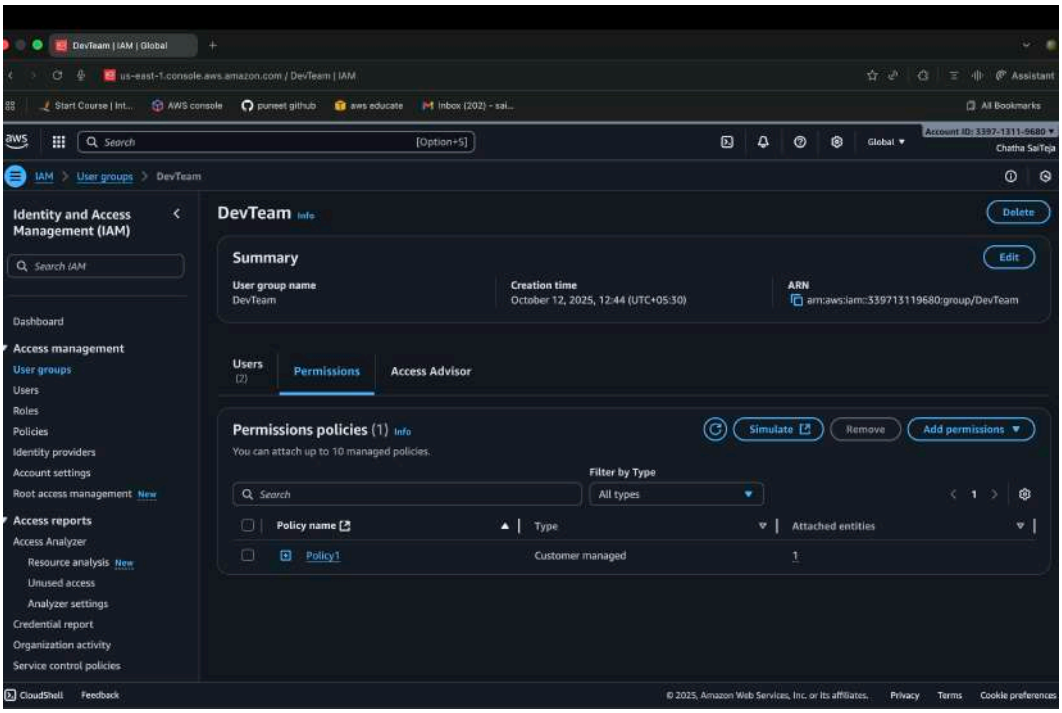
Step 4:- Now we have to attach the policy 1 to DevTeam which we created in previous assignment ,now we select the policy 1, go to actions then click on attach then we can see the user group we created.



Go to Actions click on attach

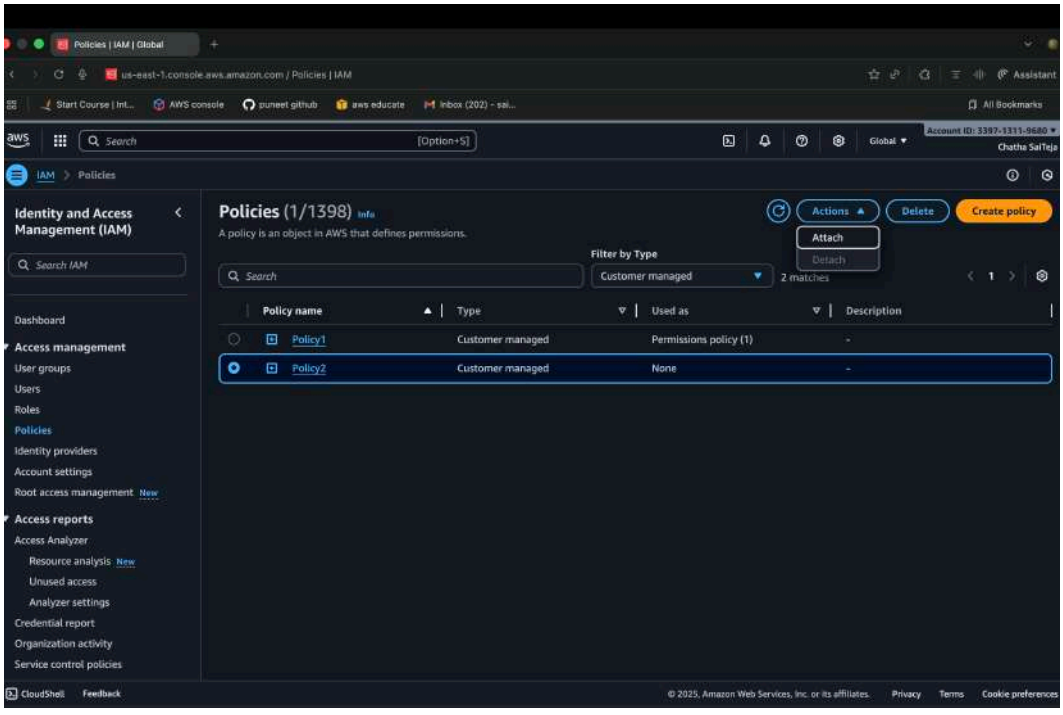


Selecting Dev Team

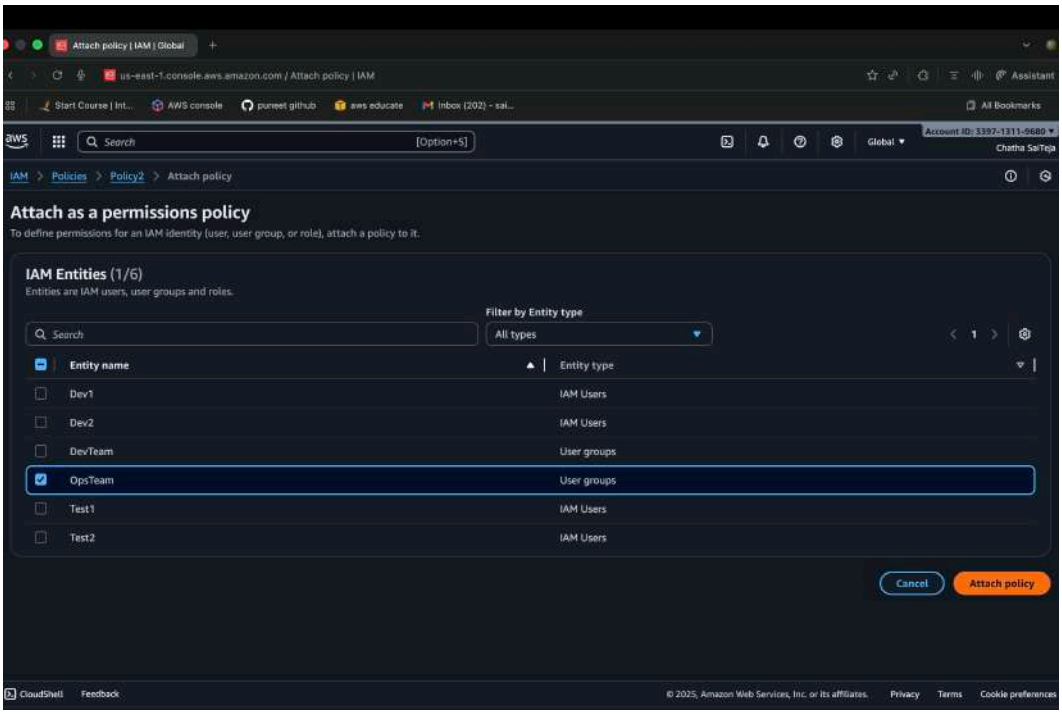


Policy1 added to DevTeam

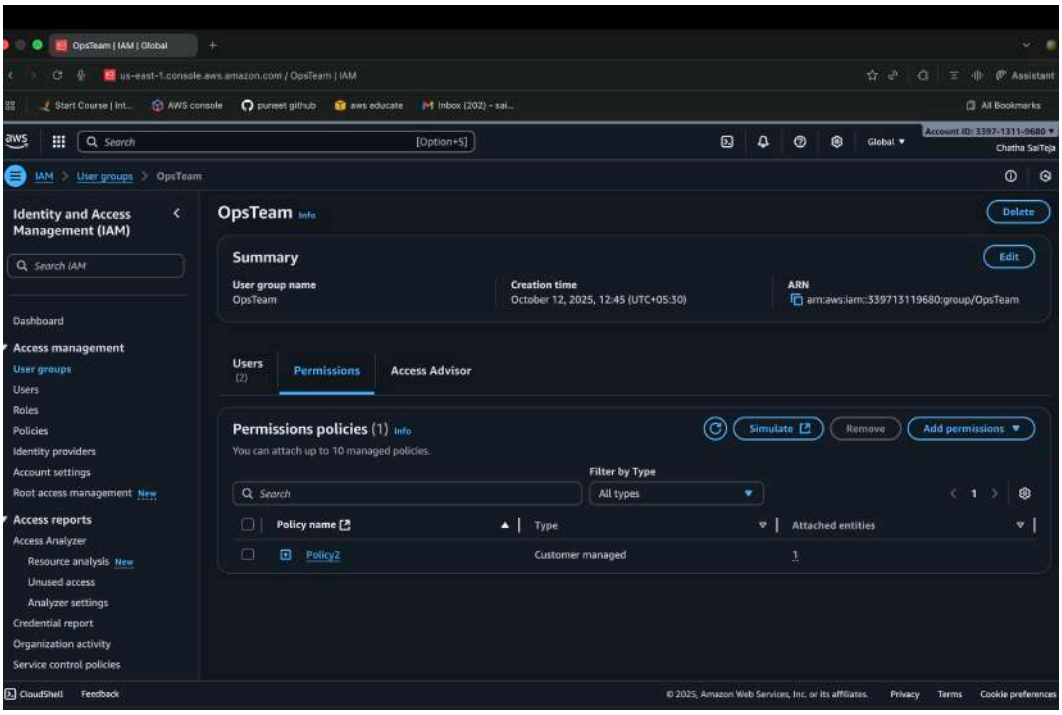
Step 5:- now we have to attach the policy2 to OpsTeam ,select the policy2 click on action then attach it.



Go to Actions click on attach



Selecting OpsTeam



Policy 2 added to OpsTeam