IAM-Roles-Assignment—-3

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.

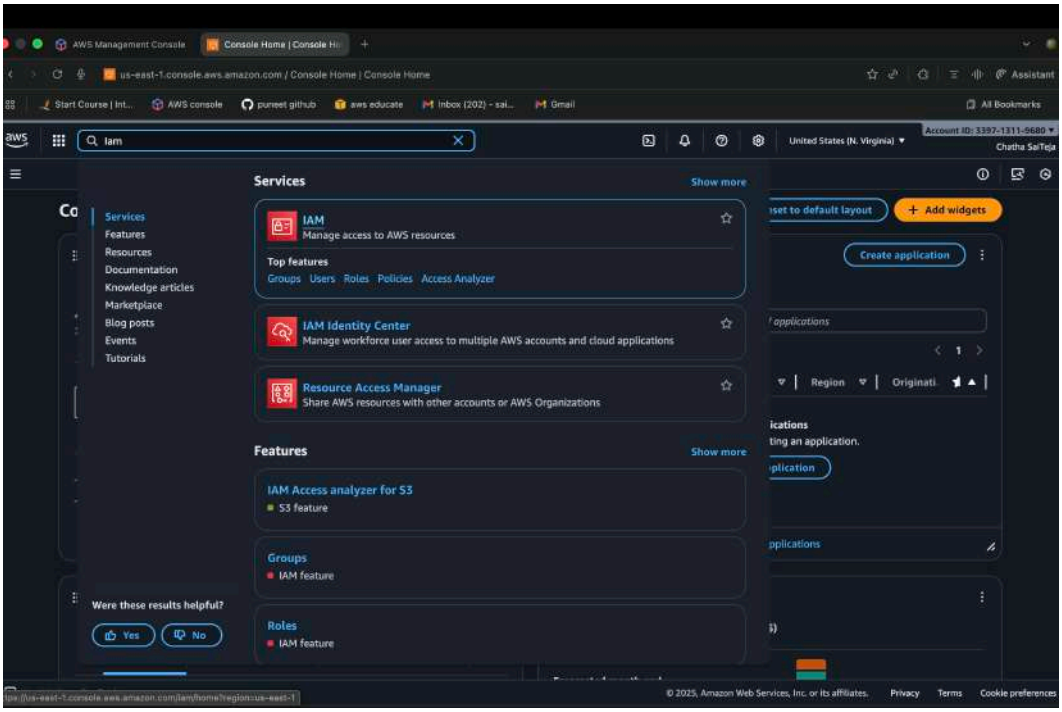
Tasks To Be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature

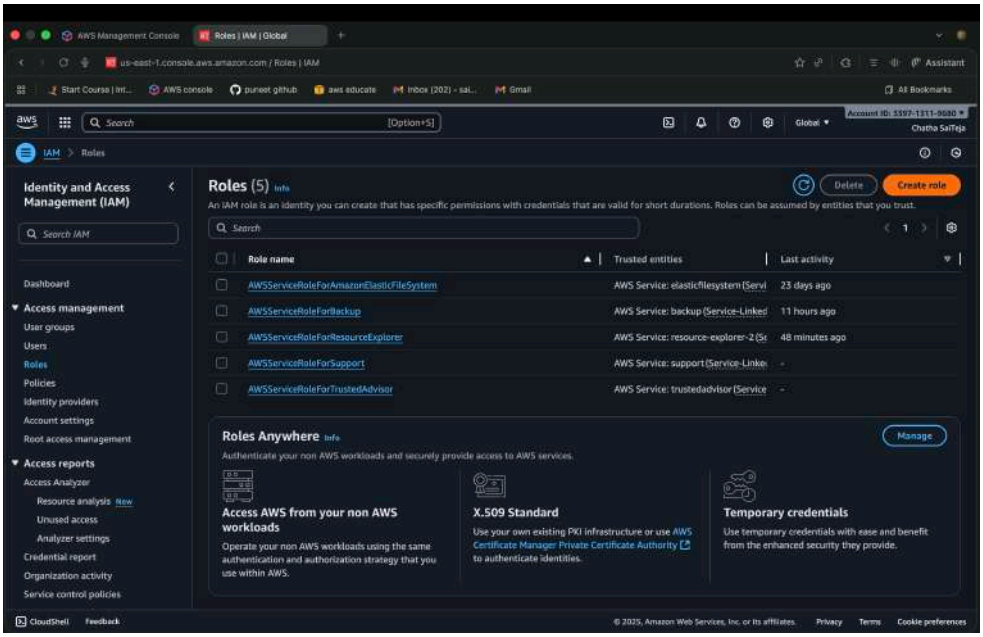
Step-By-Step Procedure:-

Step 1:-Create an IAM role for user1 and user2, where user1 refers to Dev1 and user2 refers to Dev2 as specified in Task 1.

Step 2:- To create an IAM role search IAM in search bar and open the service and go to role in the dashboard.

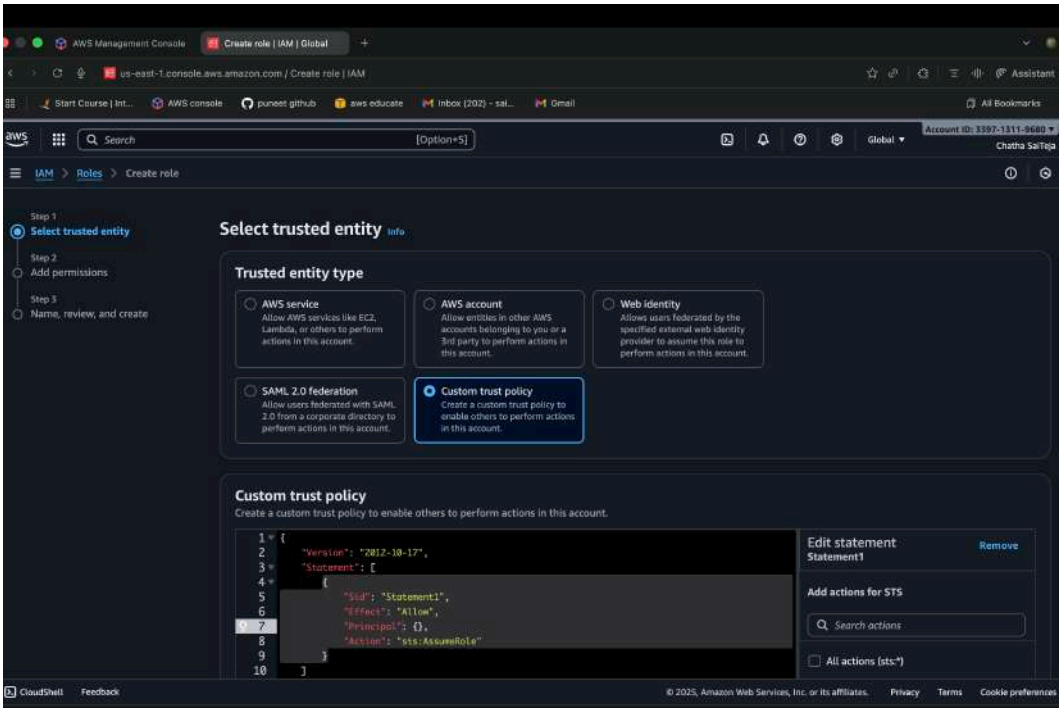


Search for IAM



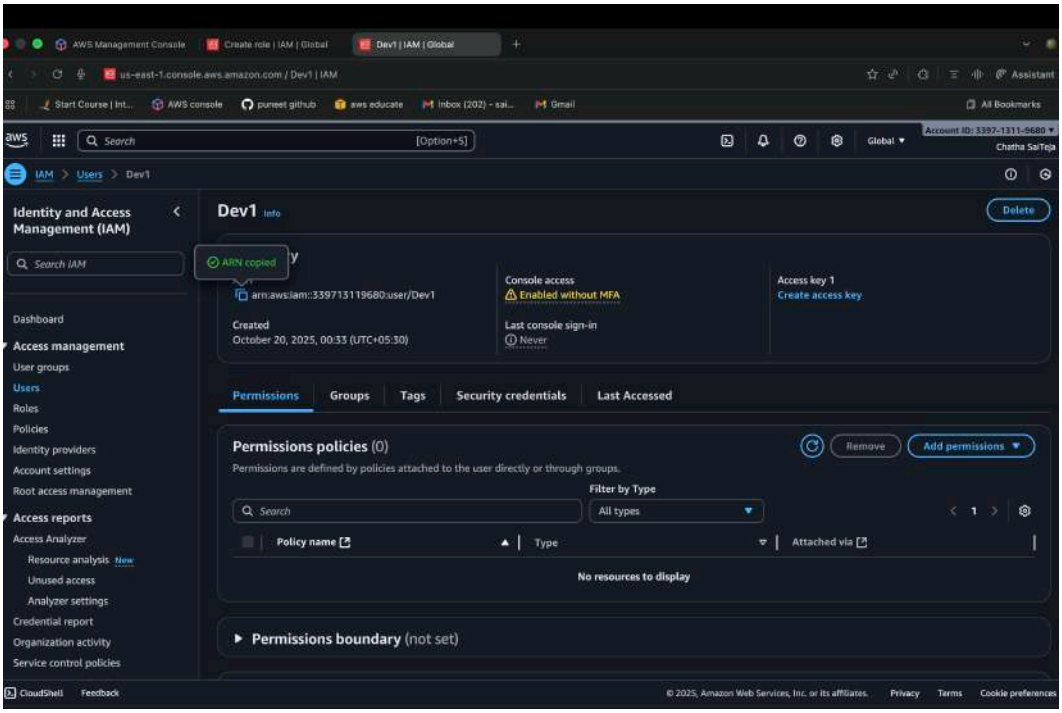
Click roles In dashboard

Step3 :- Click on Create Role, then we have too select the trusted entity(it means for which we creating a role it can be AWS service, account or other resources) where we have “AWS service”,”AWS account”and “Custom Trust policy”, we select Custom Trust Policy because we are creating role especially for user1(Dev1) and user2(Dev2)

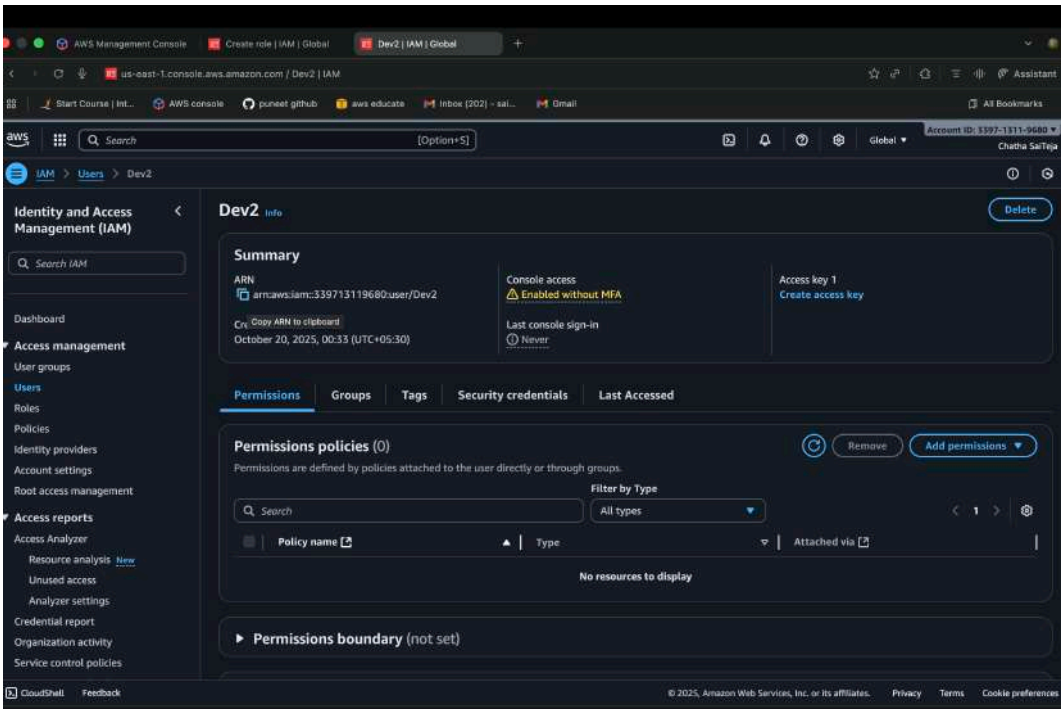


Select Custom Trust Policy

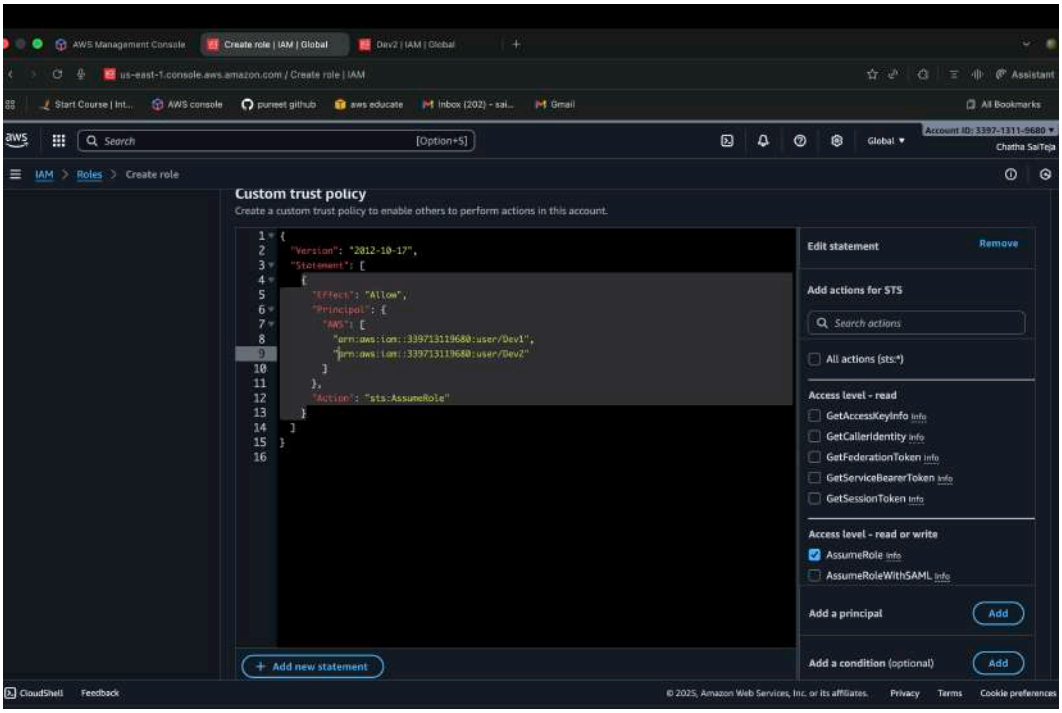
Step 4:- In trust policy we have to edit JSON where we have to copy the ARN's of user1(Dev1) and user2(Dev2) then we have to mention the ARN's Of users in principal of Custom Trust Policy and then allow all actions for "STS Assume Role"



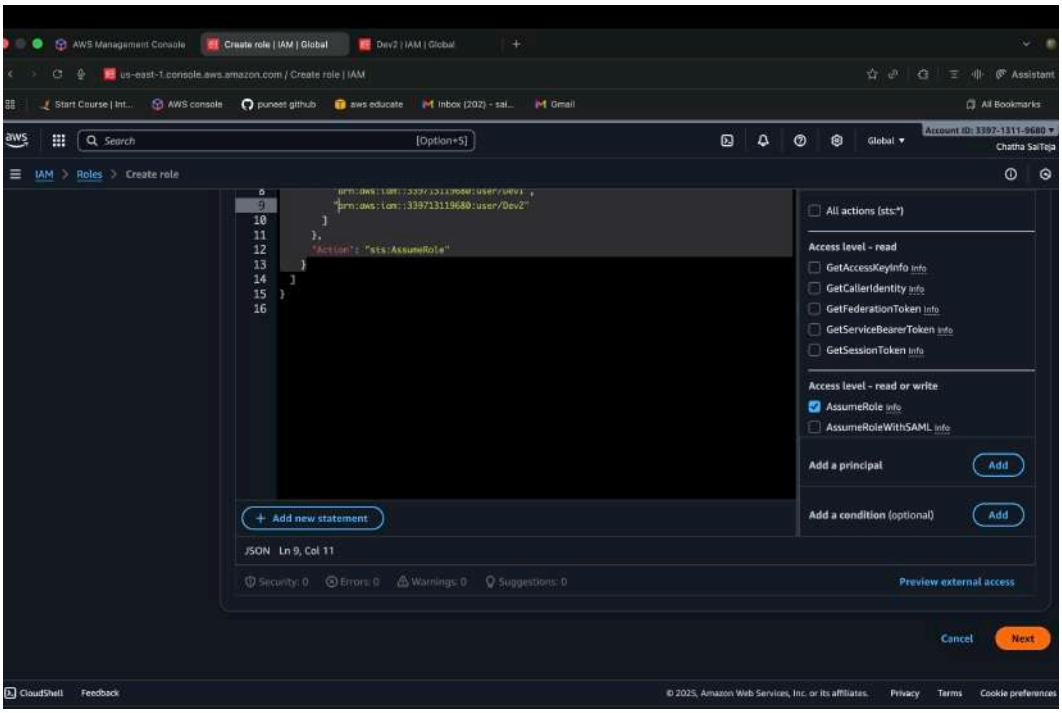
Copy Dev1(user1) ARN



Copy Dev2 (user2) ARN

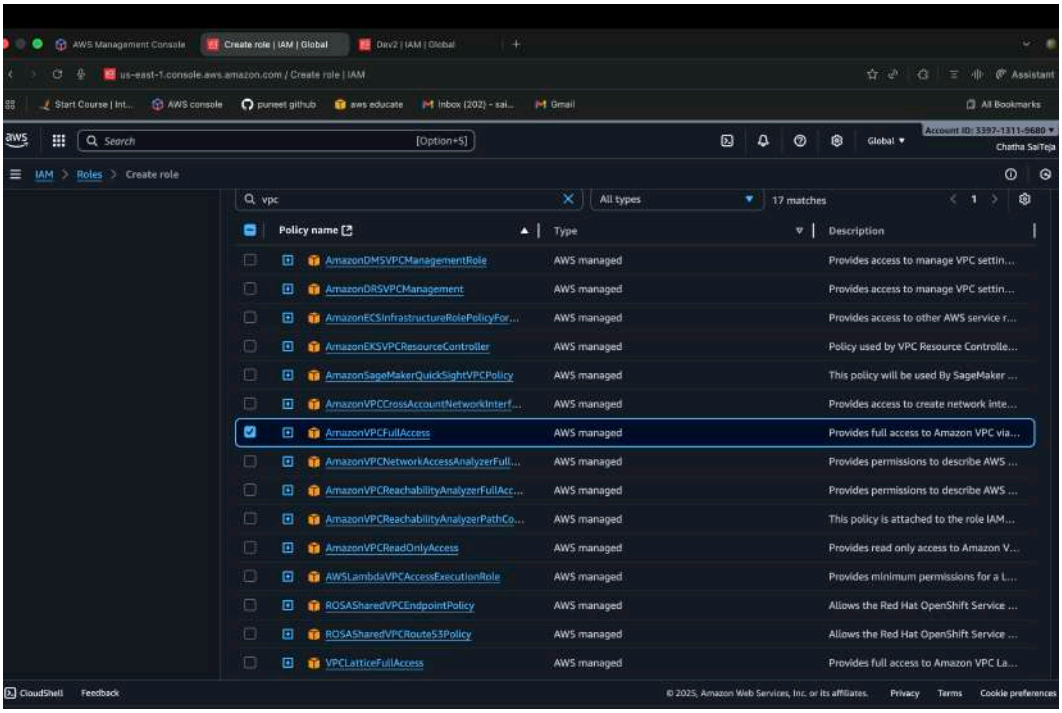


Add ARNs of user1&2 in principal of Custom Trust Policy

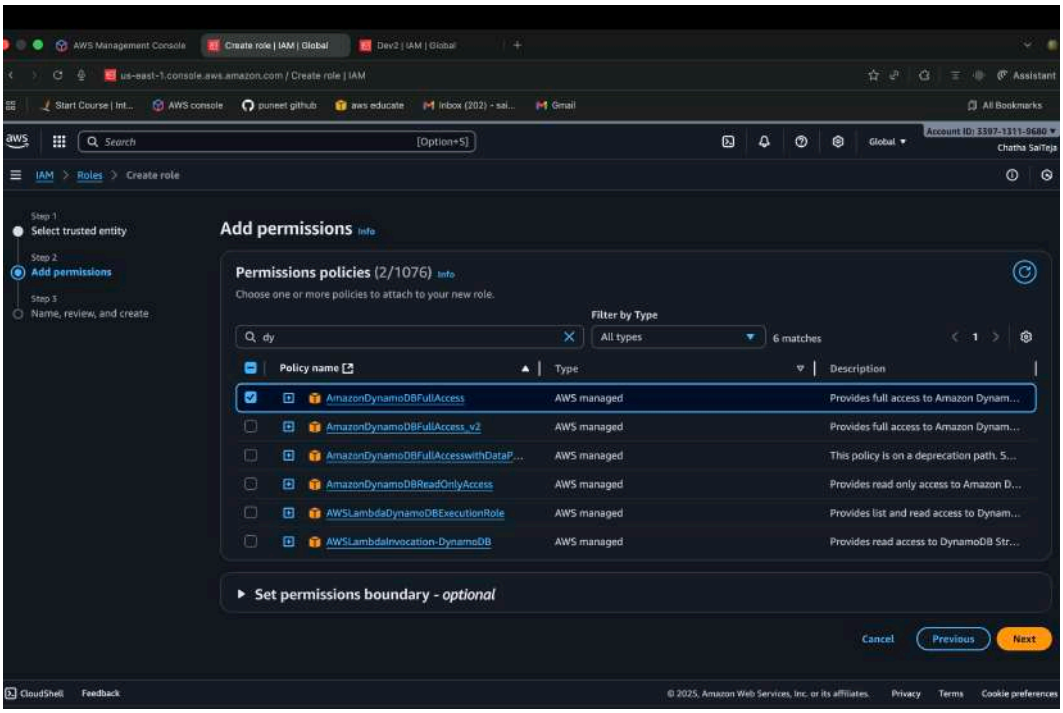


Click on next

Step 5:- After Clicking on next ,we have to specify the permission to the role ,here we have to give two permissions to the role that is full access to VPC & DynamoDb(as mentioned in the question).

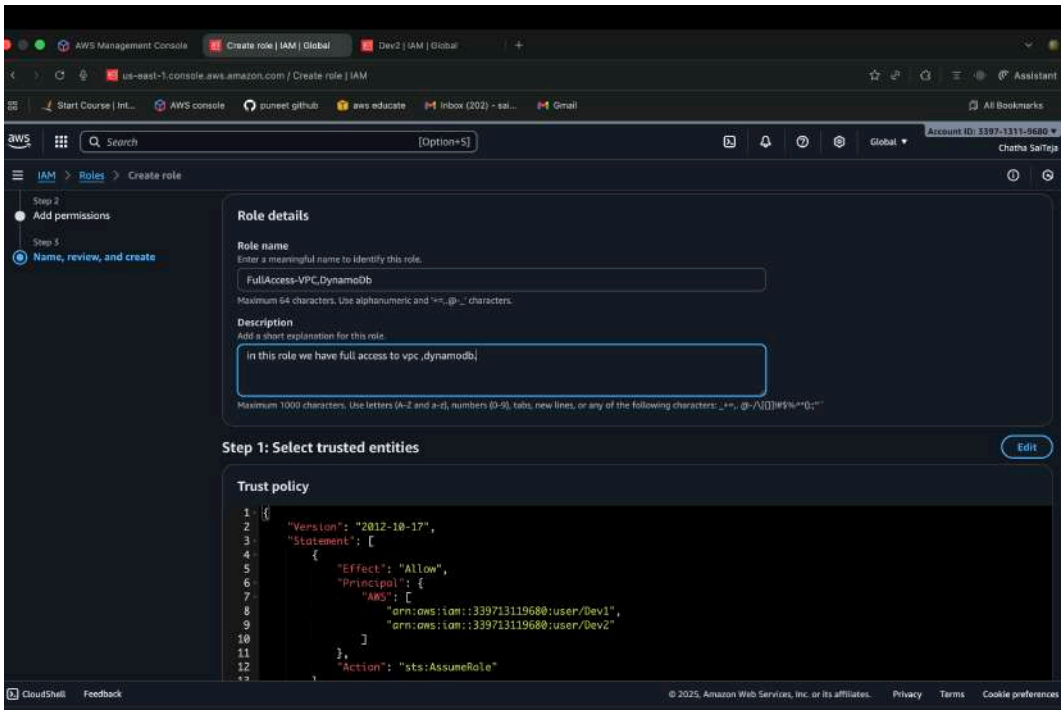


Giving full access to VPC

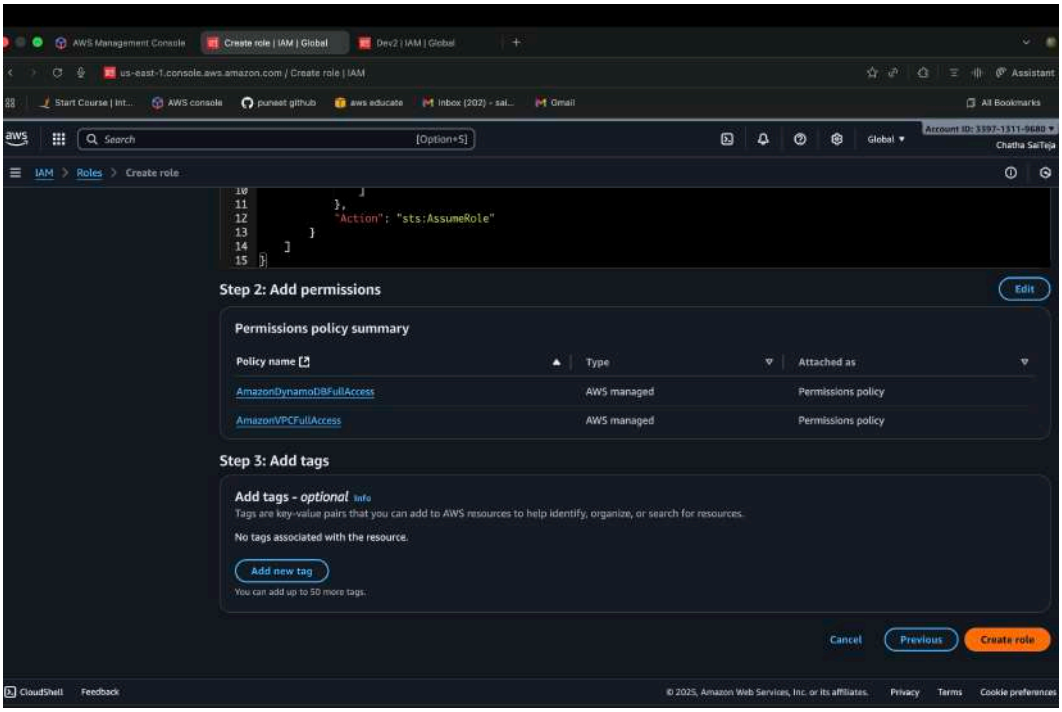


Giving Full Access to DynamoDB

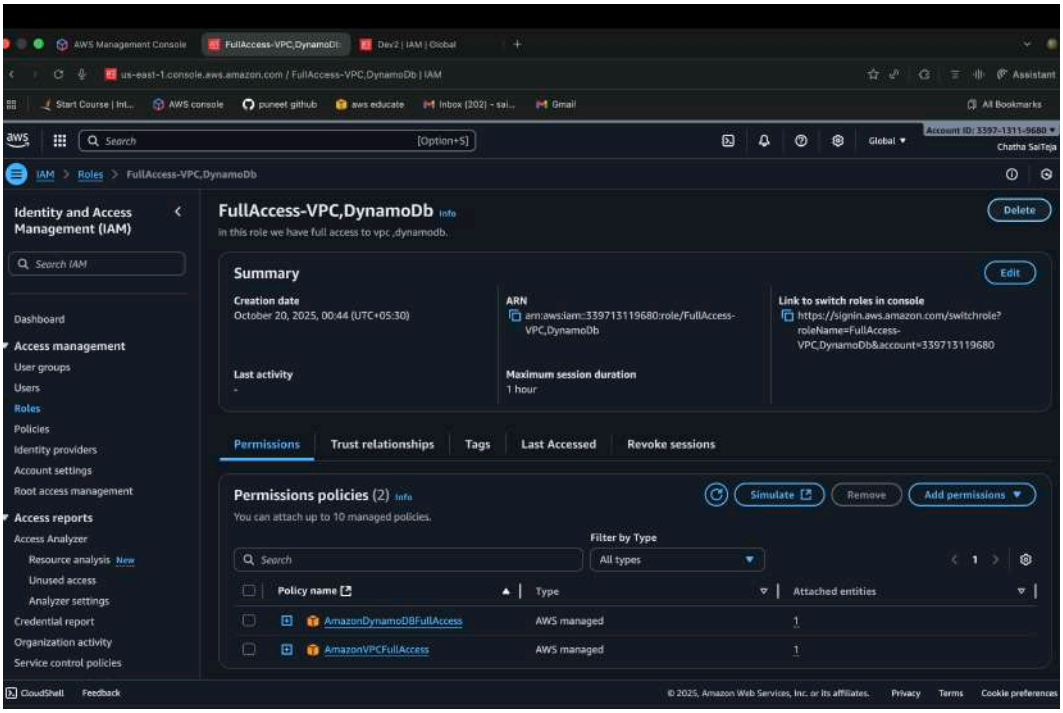
Step 6:- In next step, we can review the total configurations of a role and we specify the name (FullAccess-VPC,DynamoDb) and description for a role then click on create role.



Specifying the role details

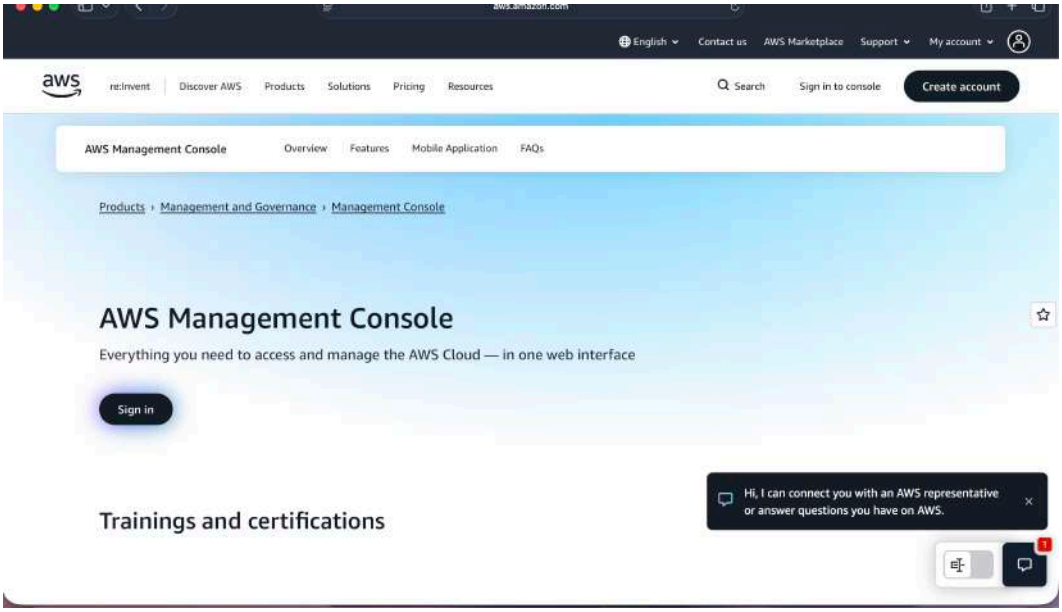


Click on create role

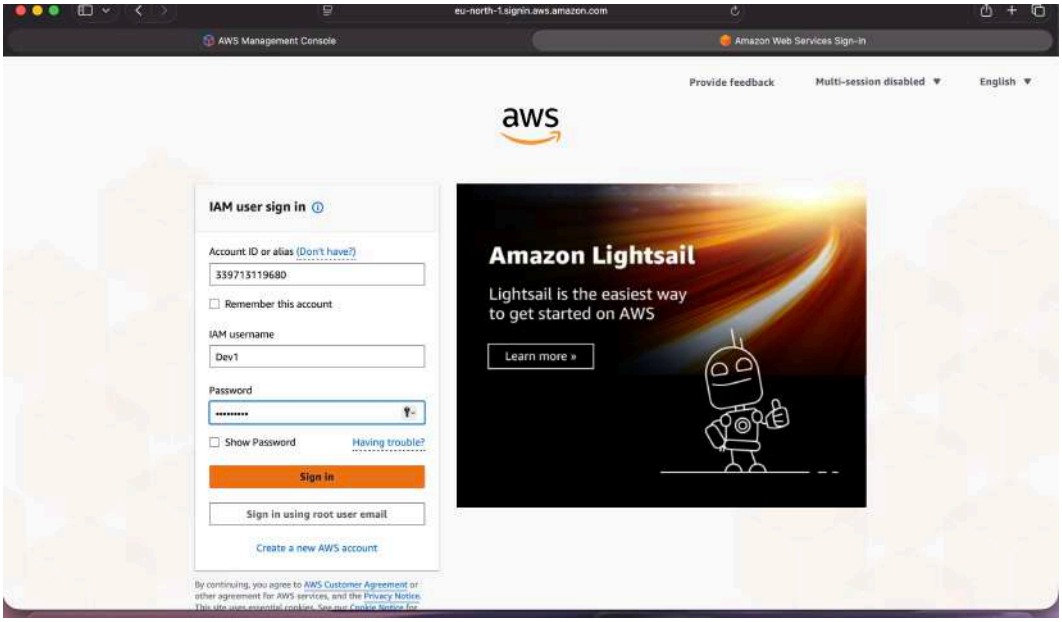


Summary of Role(FullAccess-VPC,DynamoDb)

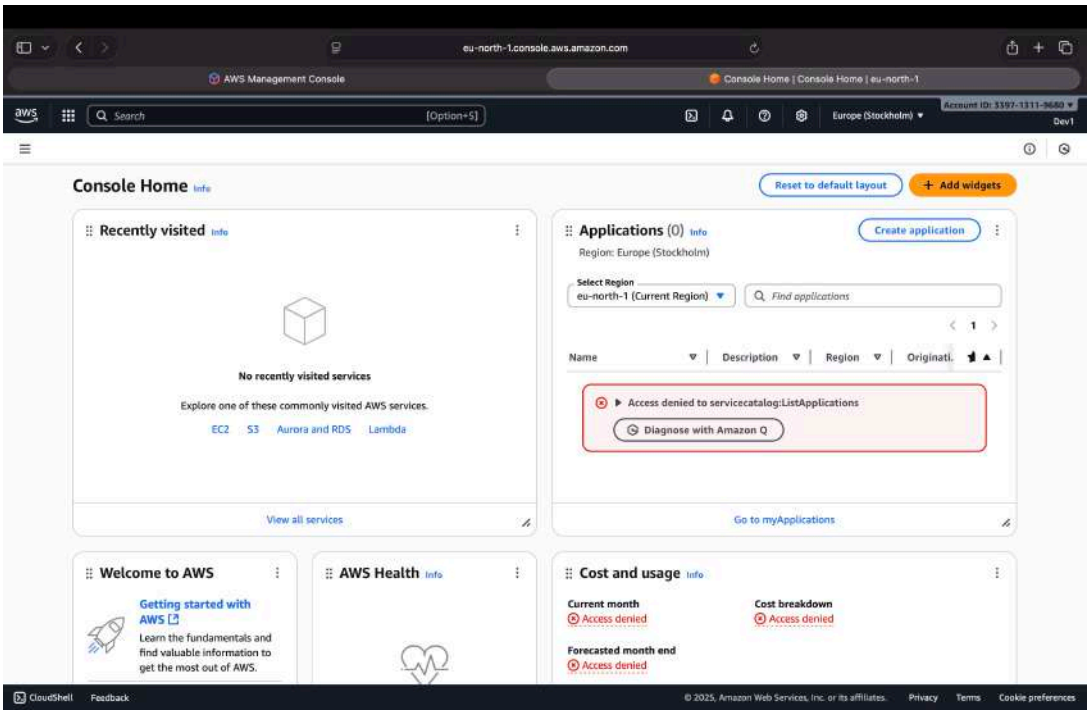
Step 7:-As role is created we have to try out the role by signing into user1(Dev1) it should be done in other browser by providing the account id, username and password.



Click on SignIn

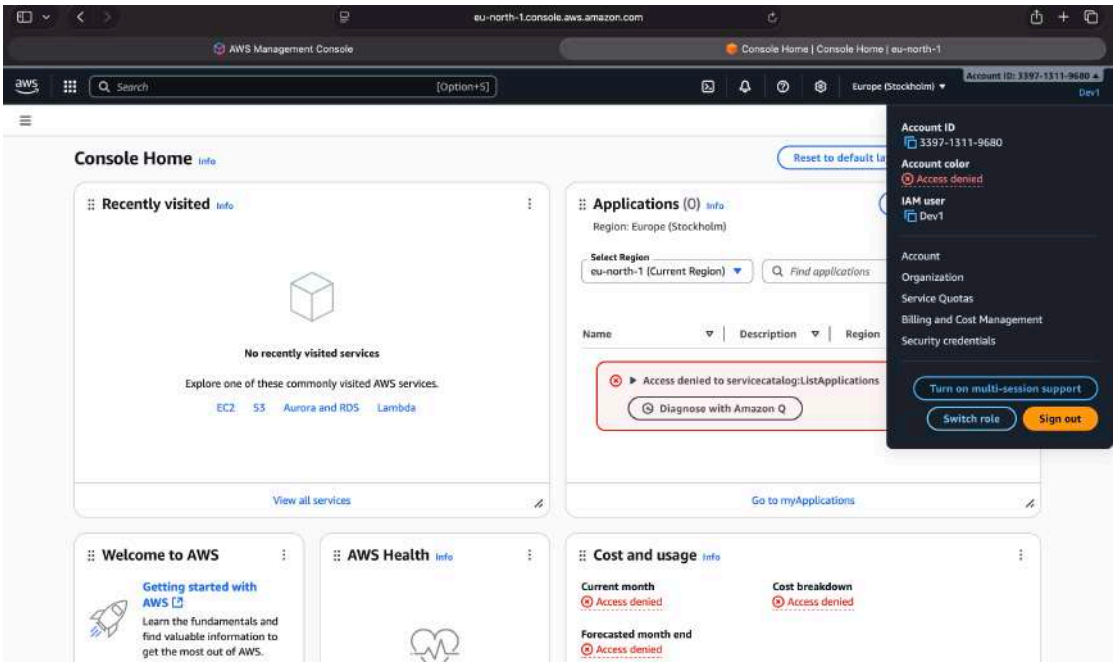


Signing into Dev1

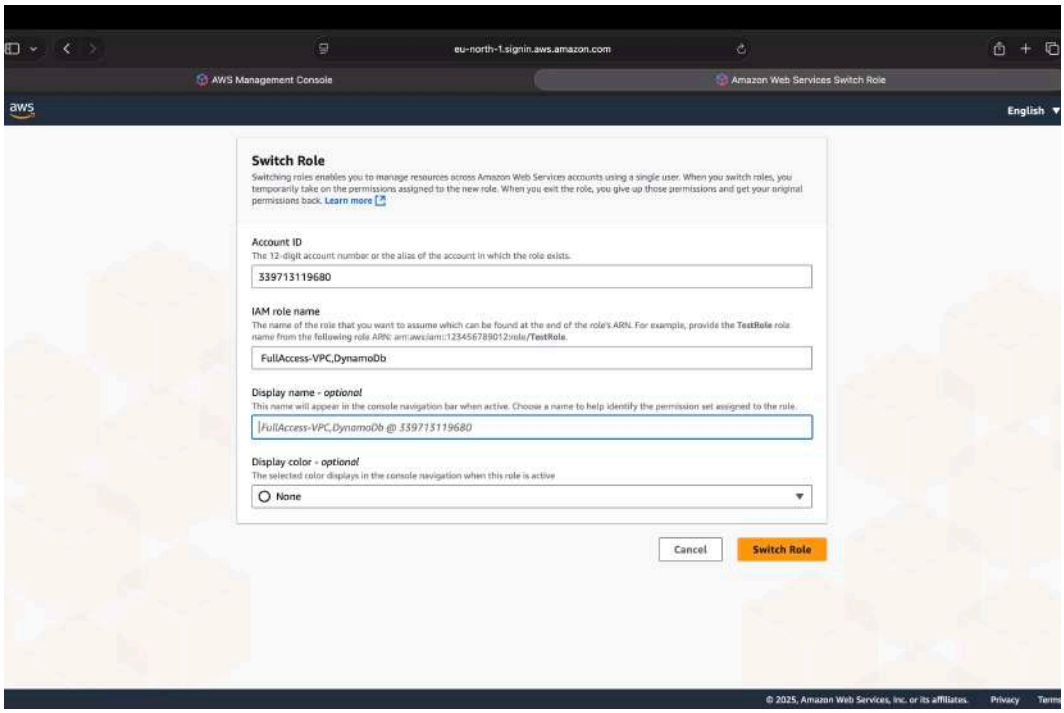


Management Console of Dev1

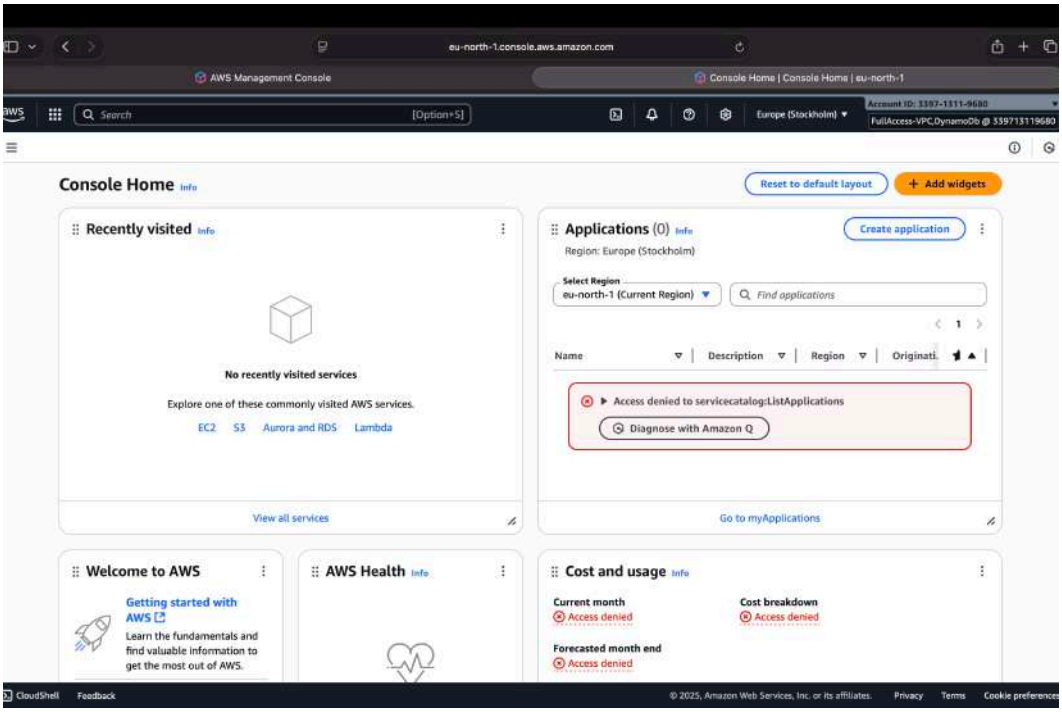
Step 8:- In right corner of Dev1(user1) console we have account related information in that there is an option of " Switch Role",after clicking on switch role we have to mention the account id and name of the role to access the role we created, then we get the access to the role



Click on Switch Role

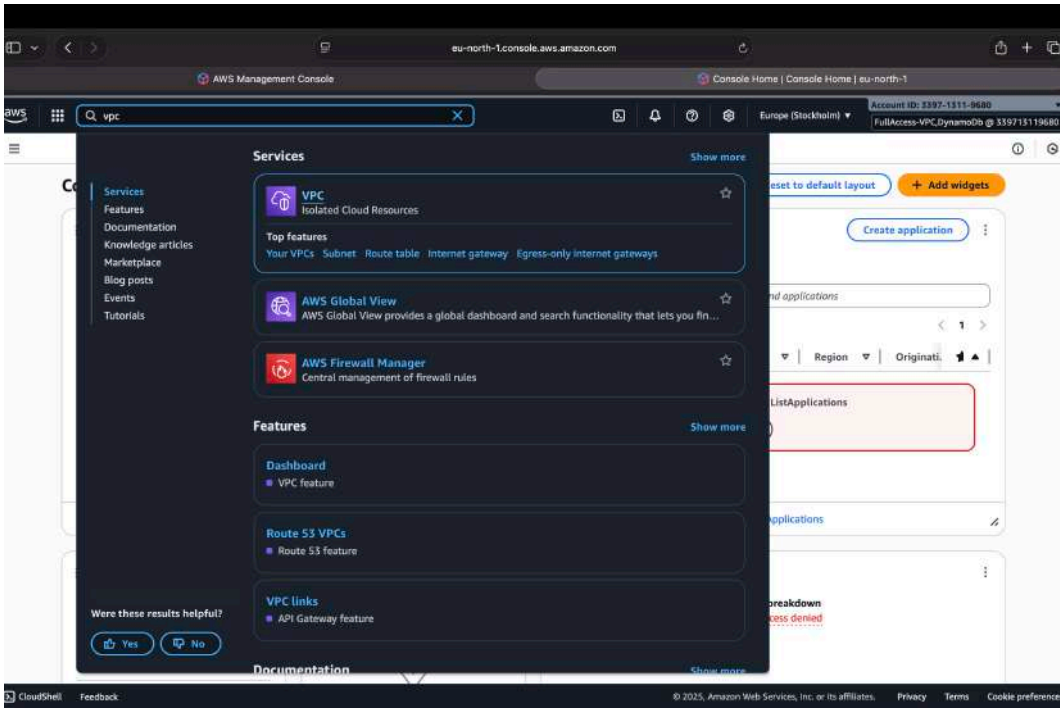


Specifying the Role details then click on switch role

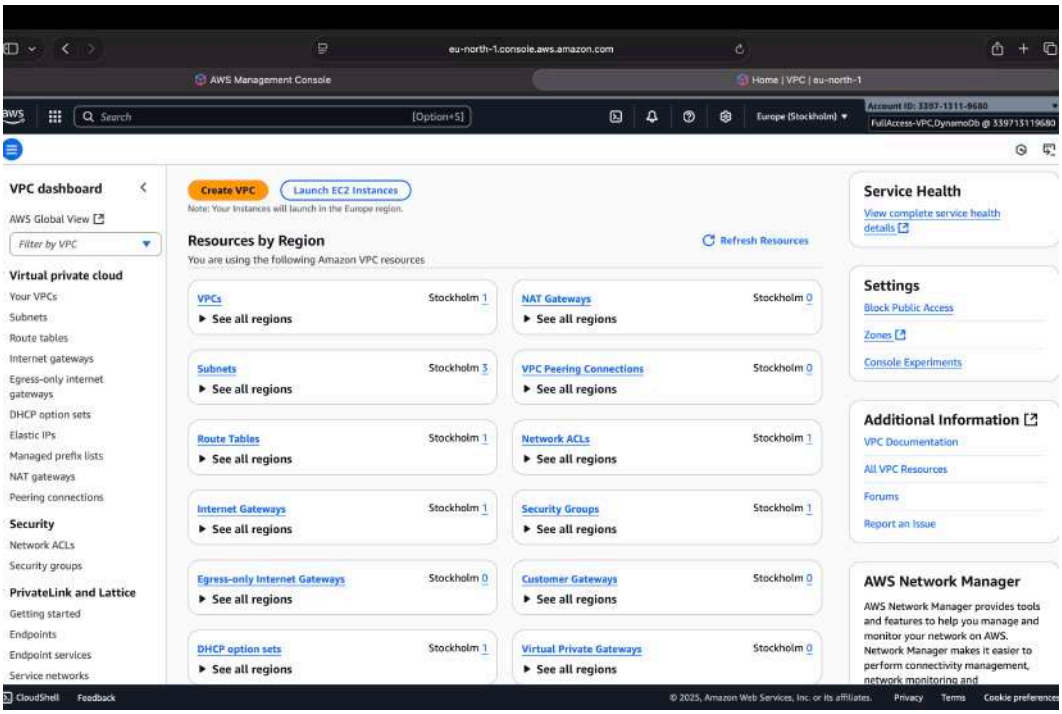


We are in FullAccess-VPC,DynamoDb (role)

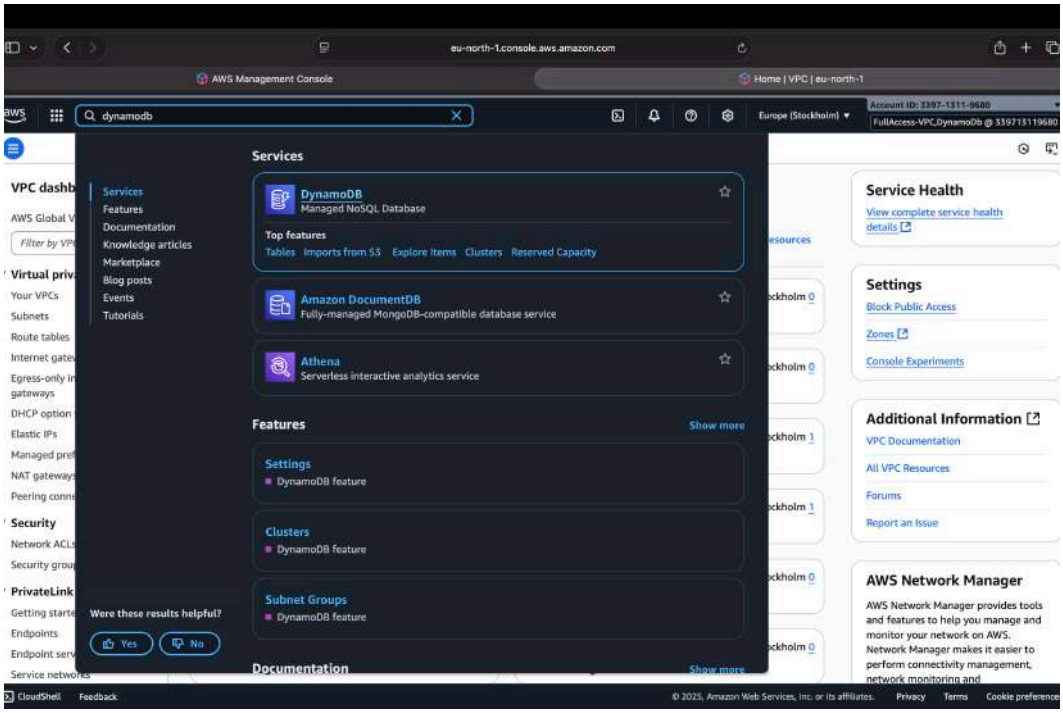
Step 9:- Now we have access to the role so we try out the VPC & DynamoDb for checking role is working or not.



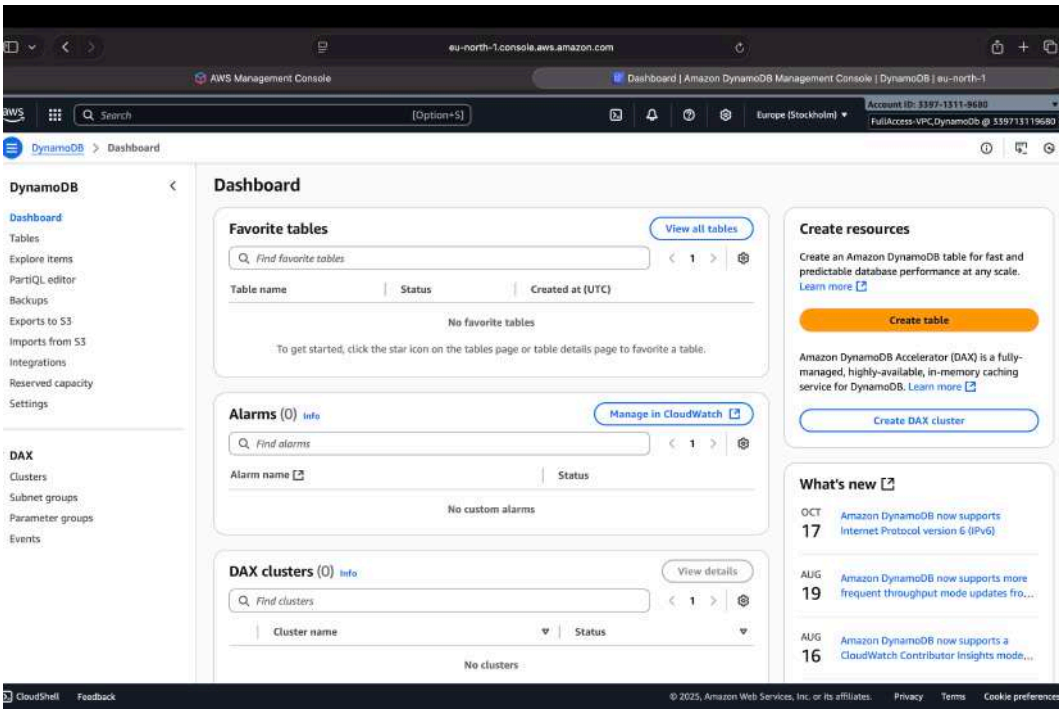
Search for VPC



VPC Dashboard

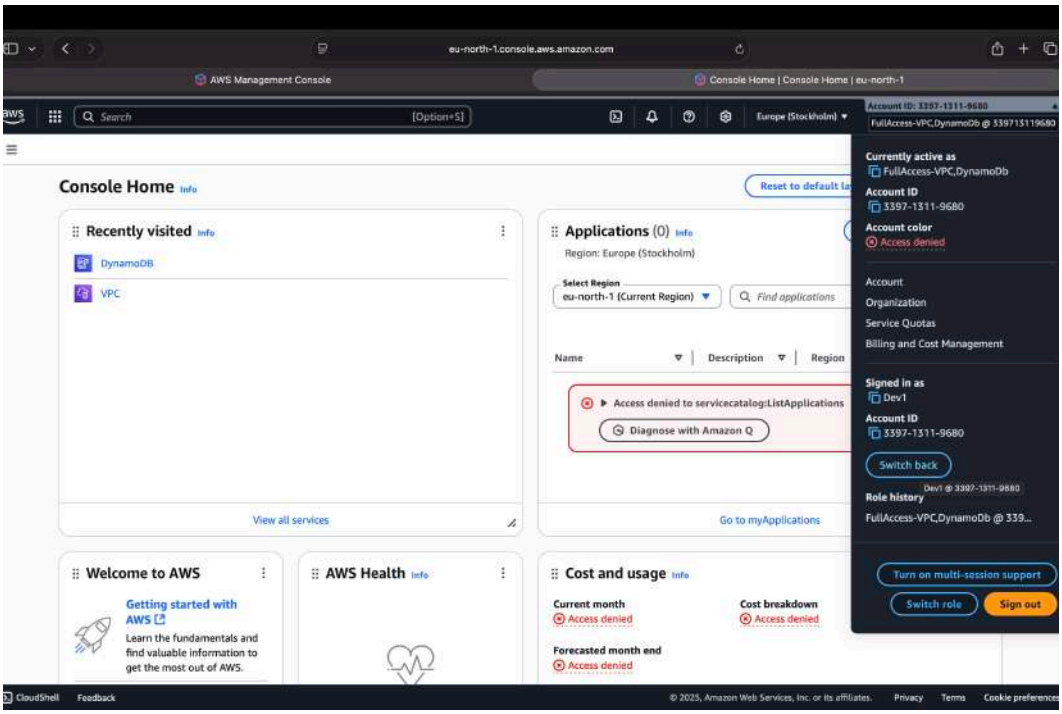


Search for Dynamo Db



DynamoDb Dashboard

Step 10:- As you can see we can access the VPC, DynamoDb then the role is working , to switch back the role click on account information and there is an option to switch back the role and sign out the user1(Dev1).



Click on Switch back and SignOut