Module 3: IAM Users Assignment

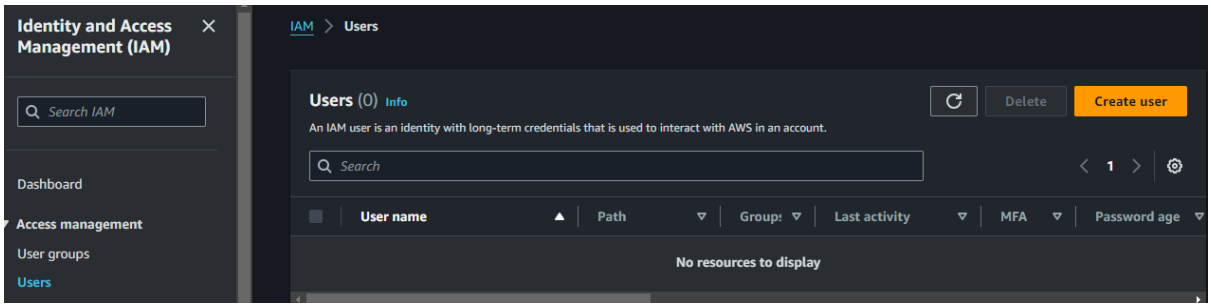
Problem Statement:

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.

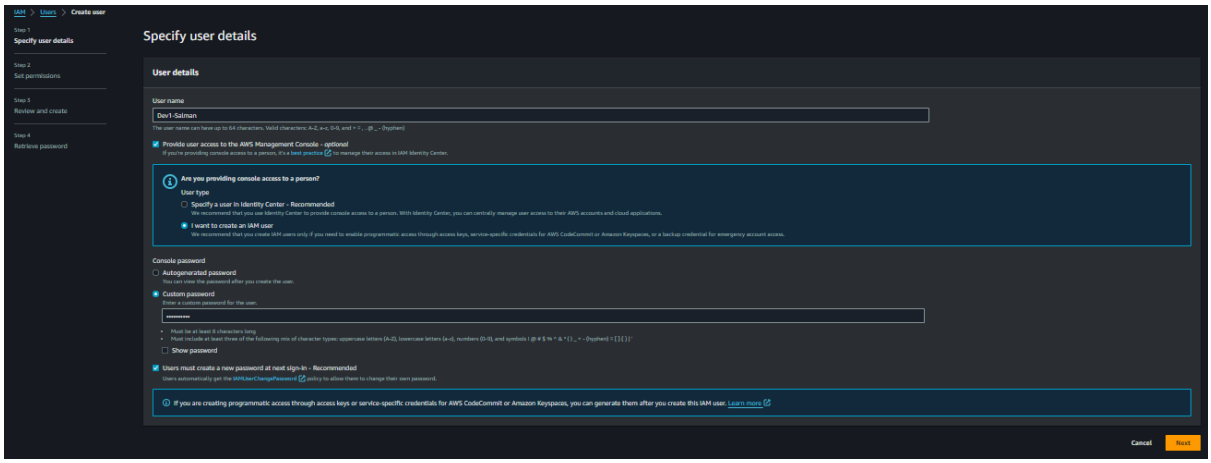
Tasks To Be Performed:

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.
2. Create 2 groups named “Dev Team” and “Ops Team”.
3. Add Dev1 and Dev2 to the Dev Team.
4. Add Dev1, Test1 and Test2 to the Ops Team.

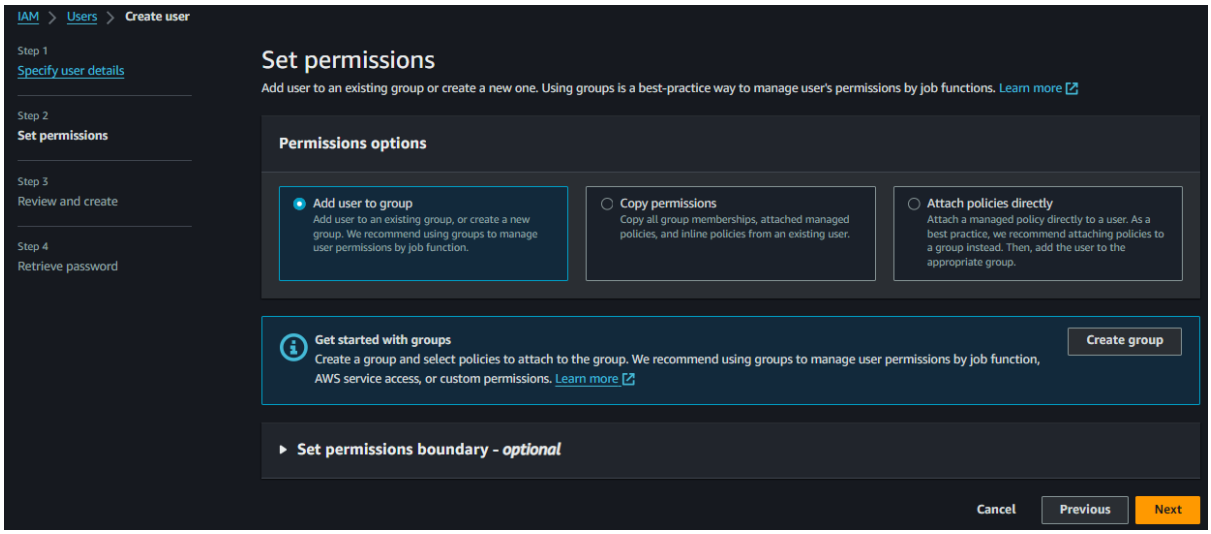
1. Creating 4 IAM Users So Need to go IAM Console > Users > Create User



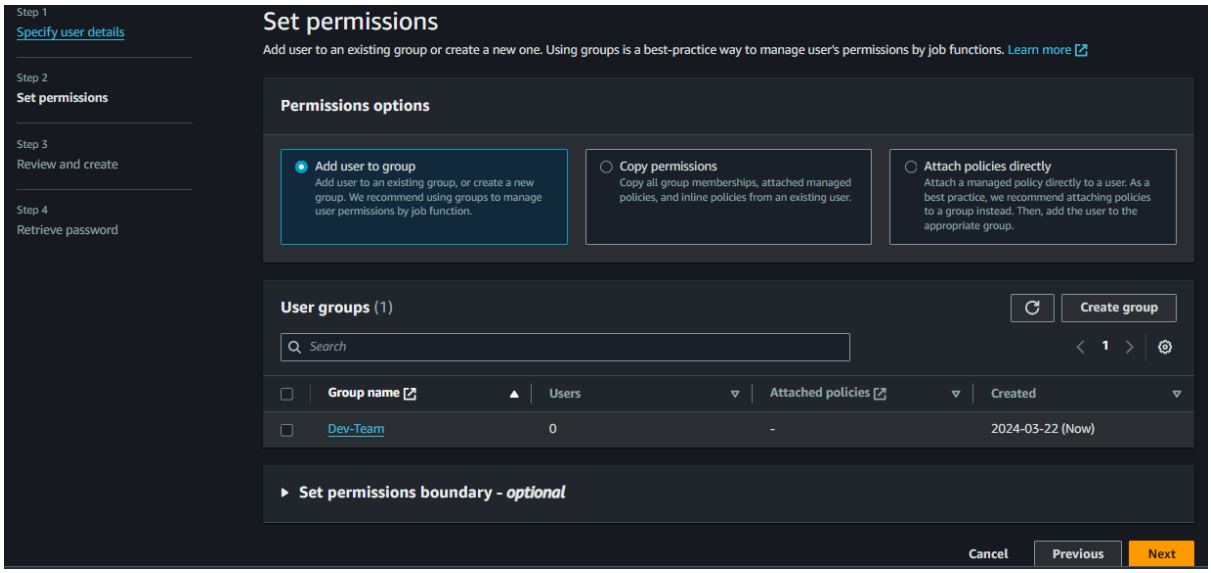
2. Select Name As per the Assignment and Provide Console Access and Select Custom or Autogenerated Password as your wish.



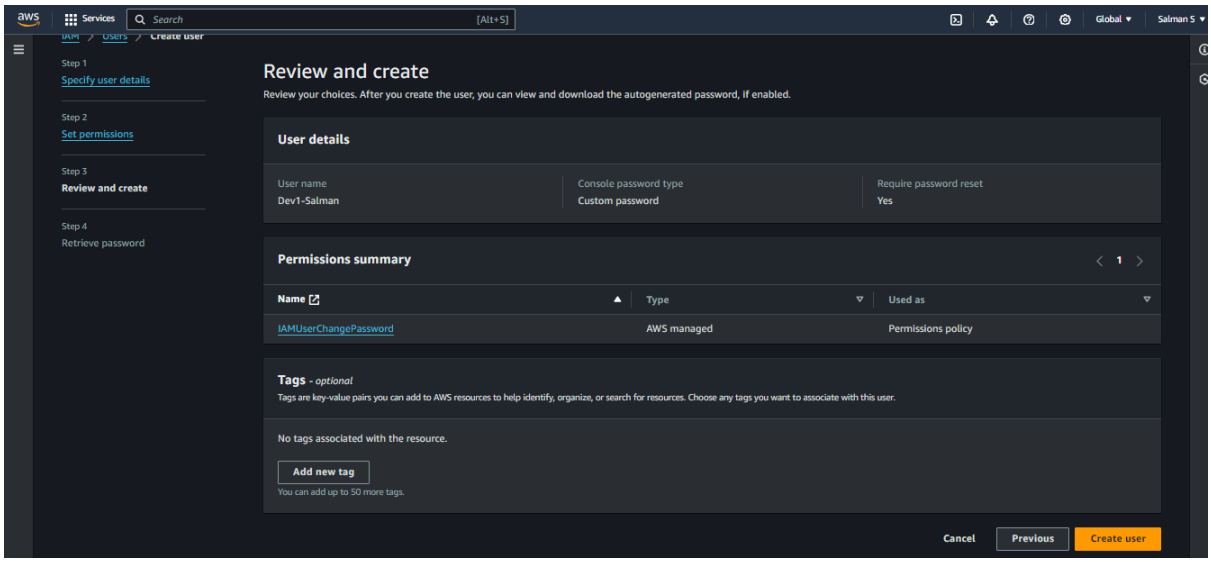
3. Add User to Group and Create Group From Here Or Click Next, later also can Add in Group



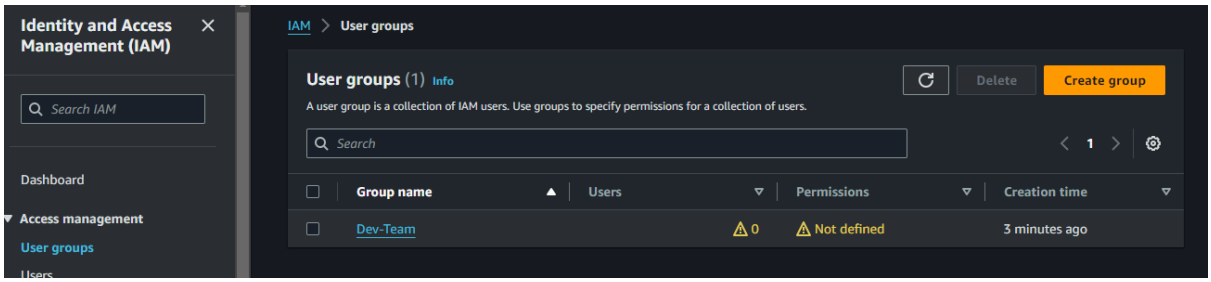
4. Created a Group As Per Assignment Dev-Team and Click Next



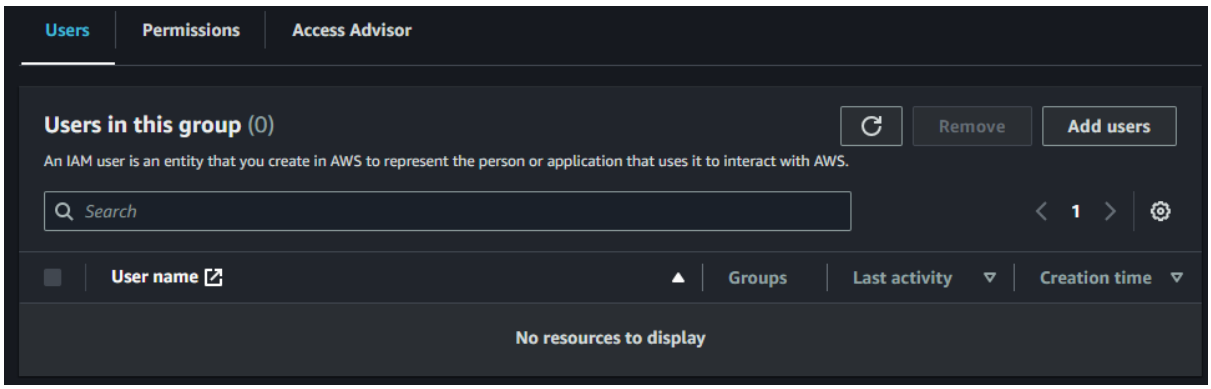
5. Review and Click Create User



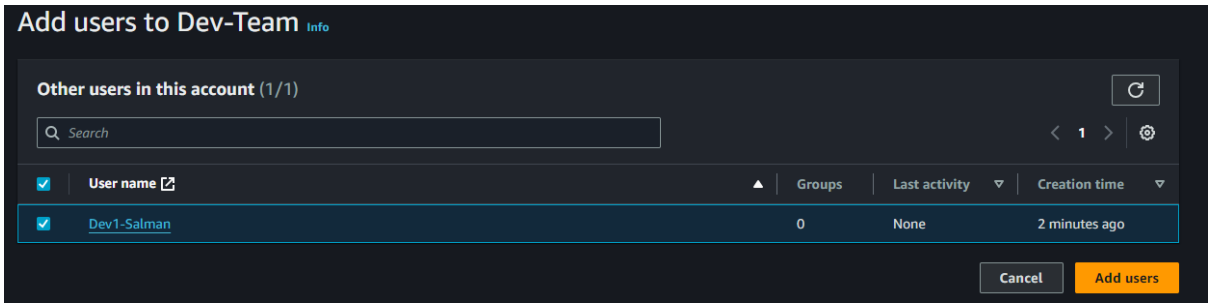
6. I Created Group while Creating Users



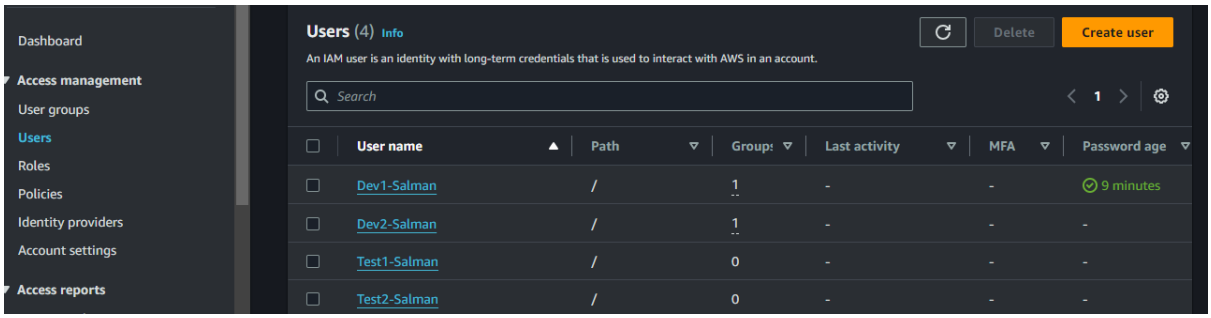
7. Click Dev-Team and Go Users > Add Users on right side end



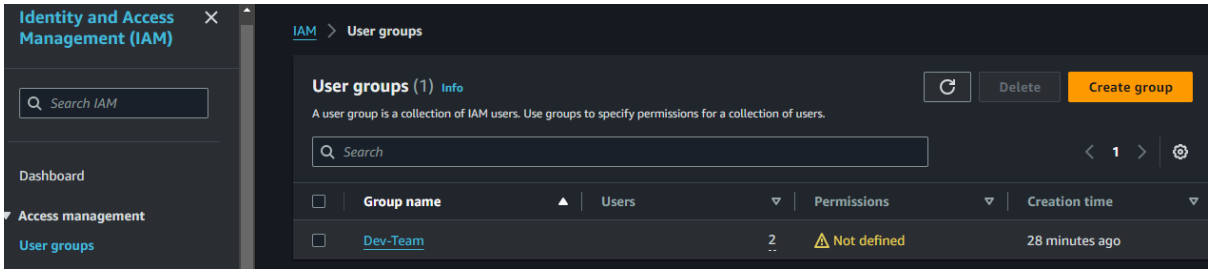
8. And Add Dev1-Salman in Dev-Team



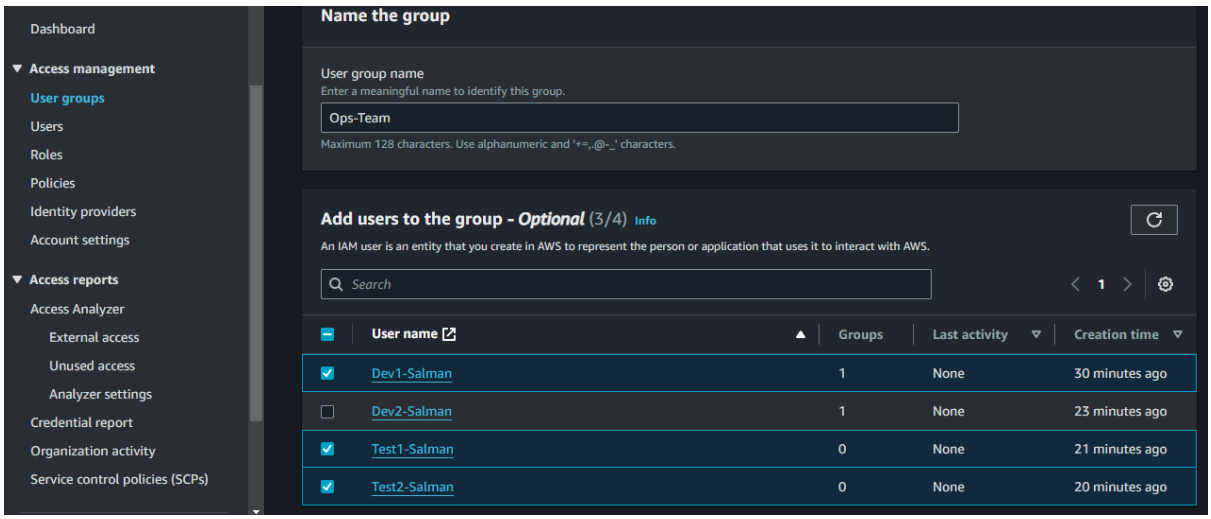
9. Create another 3 Users From Following Above the Steps and also Create Another Group



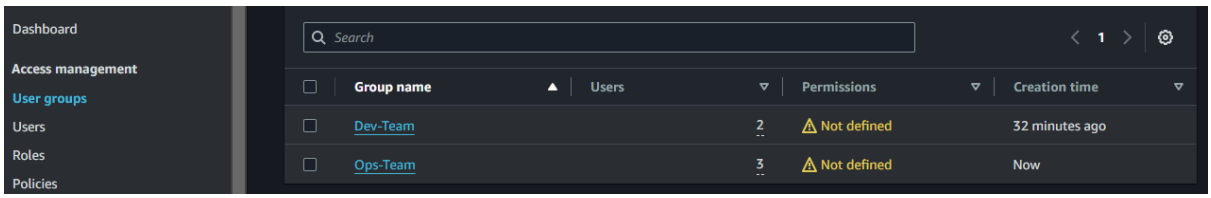
10. Add Dev2-Salman in Dev-Team



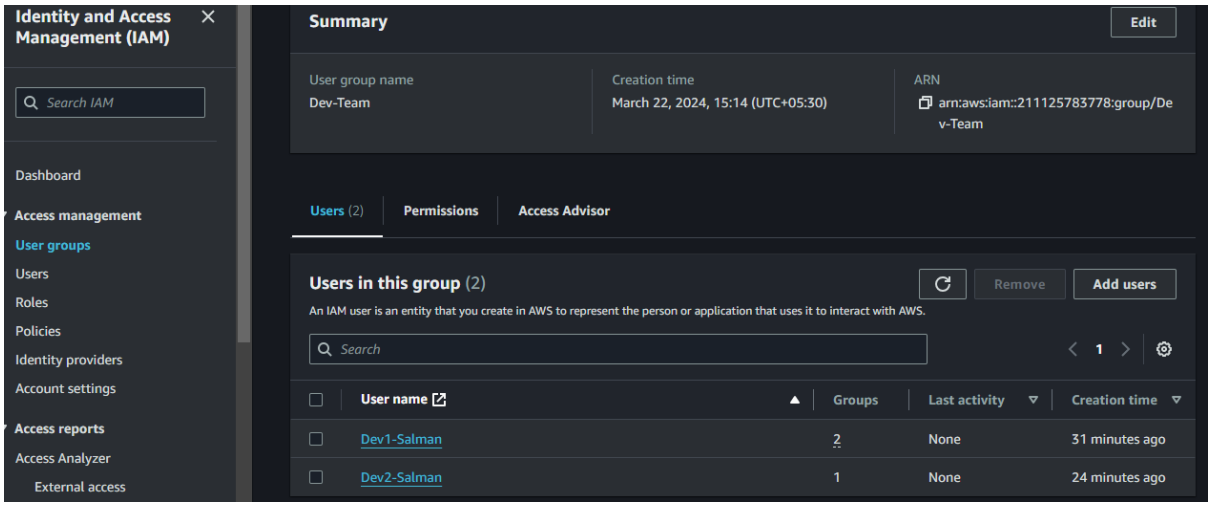
11. Now I'm Adding 3 Users in Ops-Team As per the Assignment



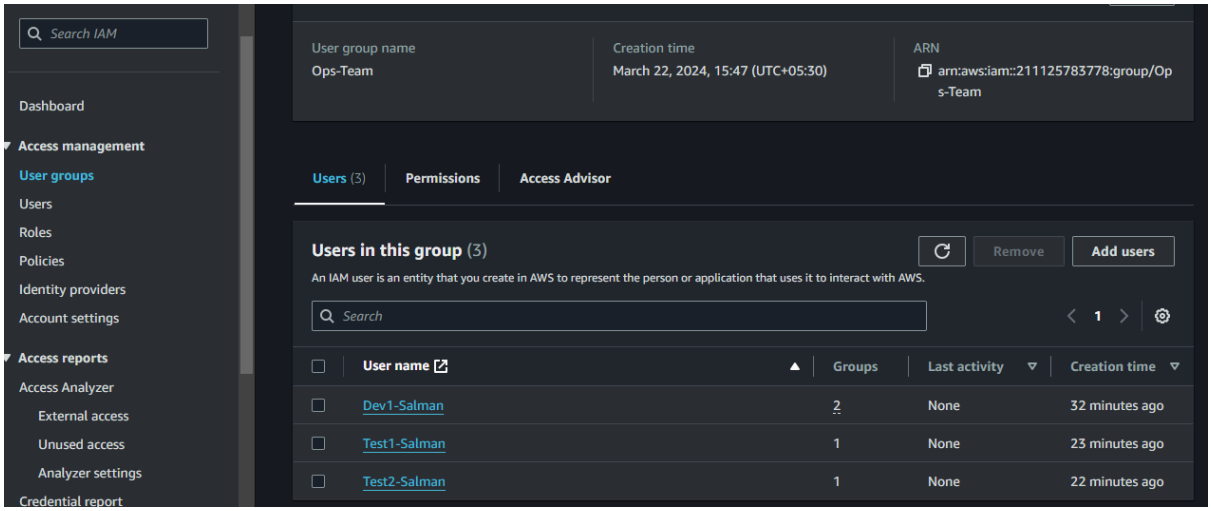
12. Now in the Dev-Team Having 2 Users and Ops-Team Having 3 users



13. Now we can see As per the Assignment Dev1 in 2 Groups and This Dev-Team



14. Now this is Ops-Team Creating and Adding the Users in Groups Successfully Completed



Module 3: IAM Policies Assignment

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.

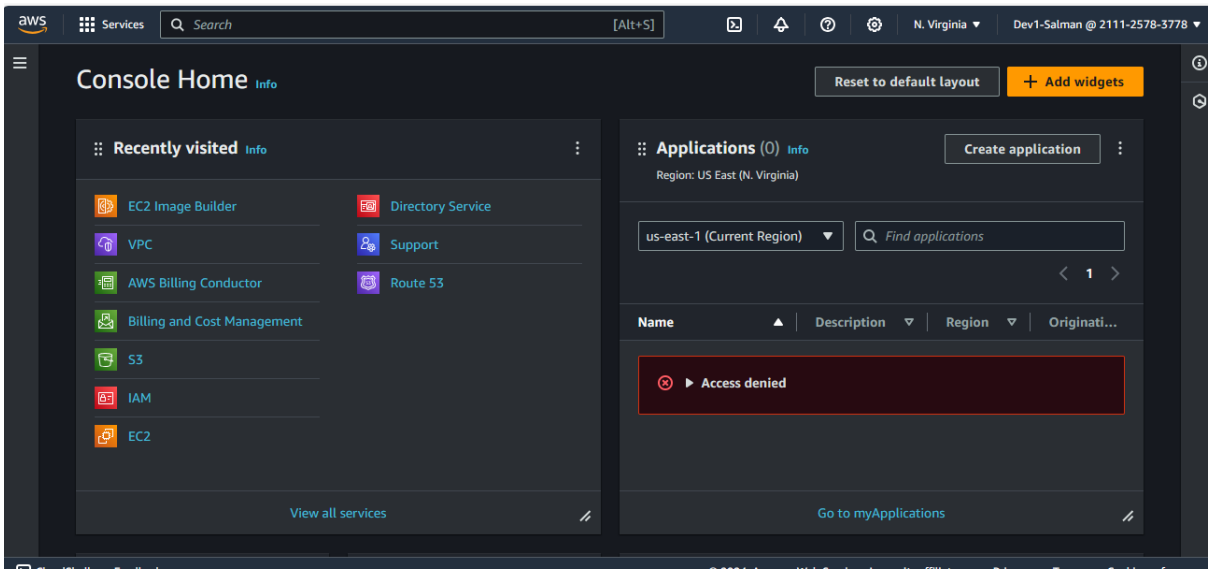
Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
    a. Access S3 completely
    b. Only create EC2 instances
    c. Full access to RDS

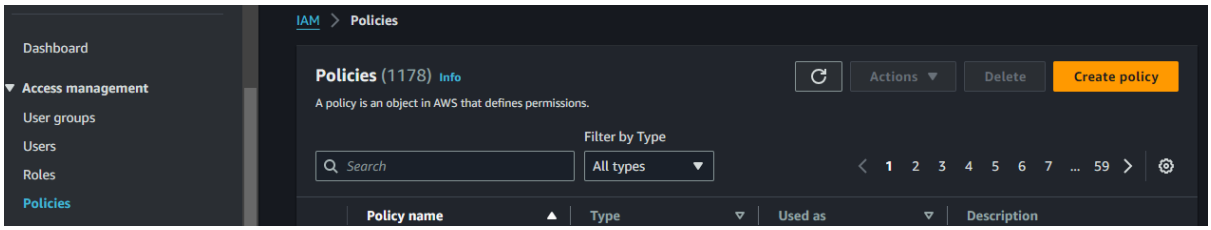
2. Create a policy number 2 which allows the users to:
    a. Access CloudWatch and billing completely
    b. Can only list EC2 and S3 resources

3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

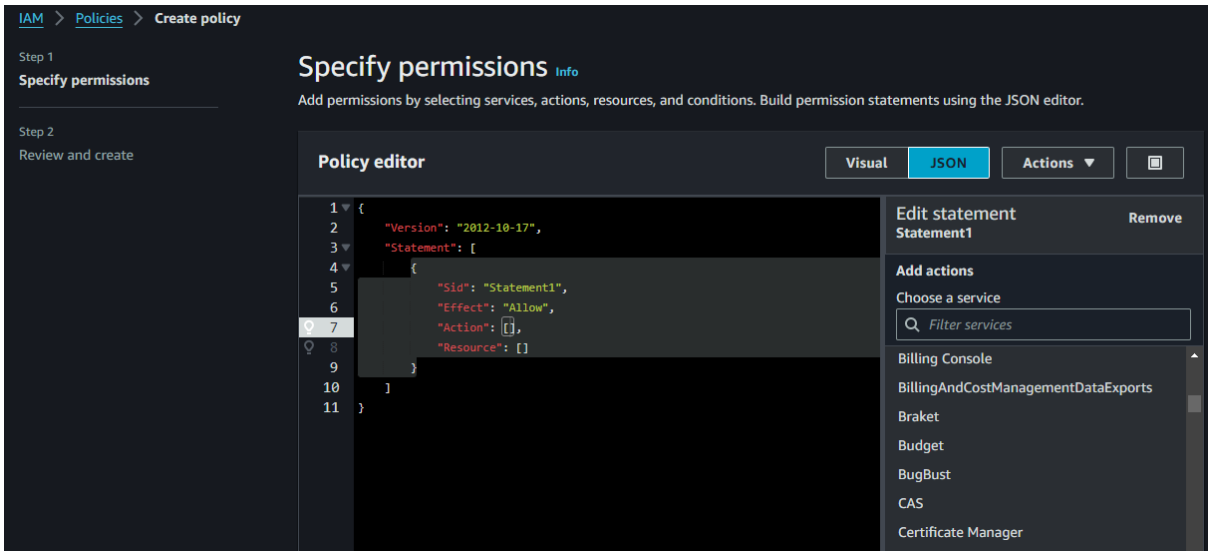
15. Now I am Loged in as Dev1-User Checking that have Permission to Use? Now we see No Permission



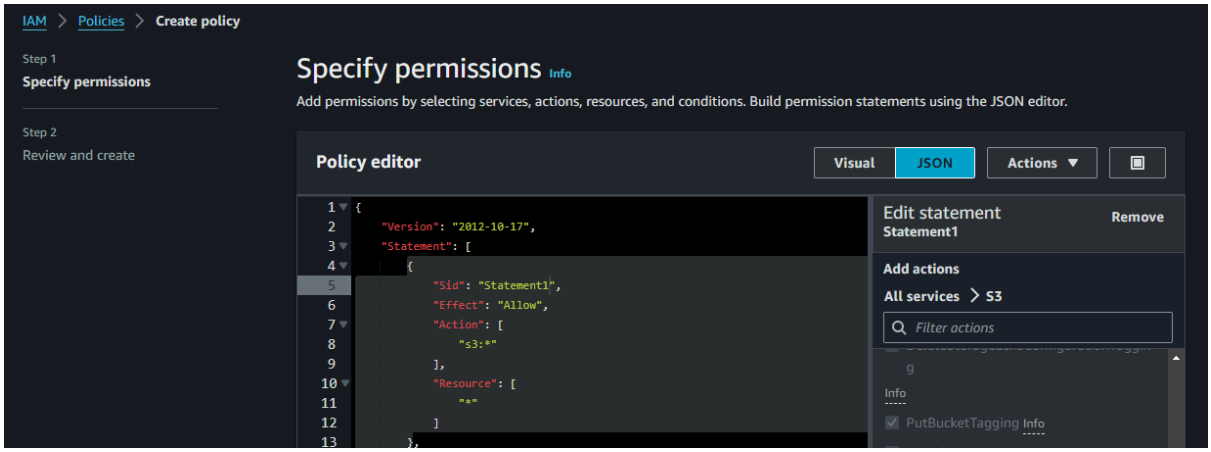
16. Now Assignment-2 Create Policies Go to IAM Dashboard > Polices > Create Policy



17. Now to Add Permissions using visual or Json and I am Using Json



18. So In the Statement1, I Add s3 and Allow All Services for s3 and Click All Resources and Allow it



19. We can Add New statement and Add a Resource Option and Add a Condition Option too

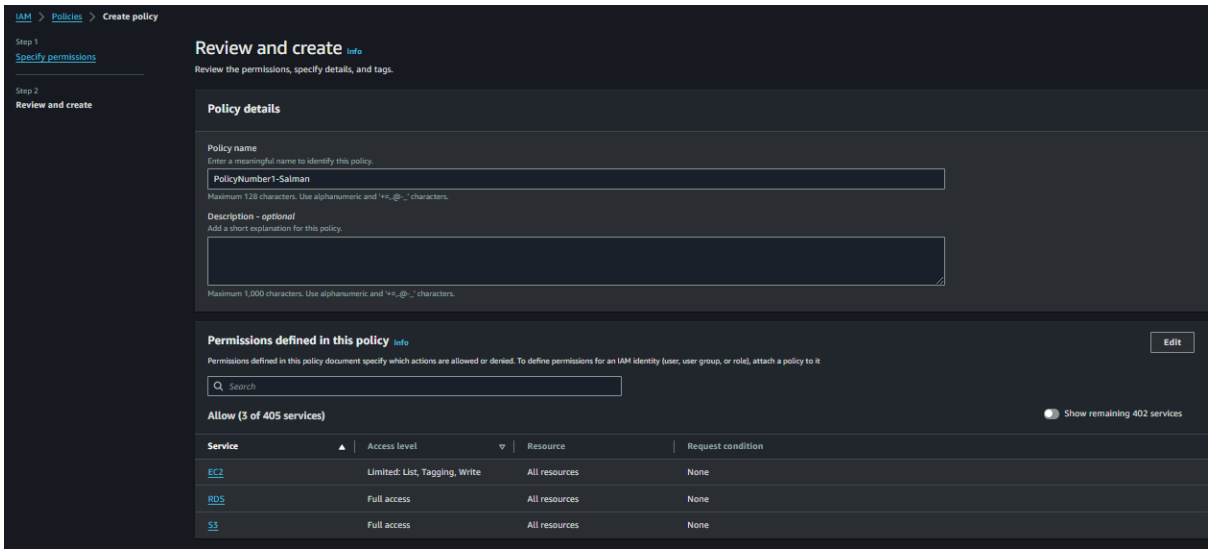
20. Added Statement2 and Allowed RDS All Services and Allowed All Resources

```
    "Sid": "Statement2",
    "Effect": "Allow",
    "Action": [
        "rds:*"
    ],
    "Resource": [
        "*"
    ]
},
```

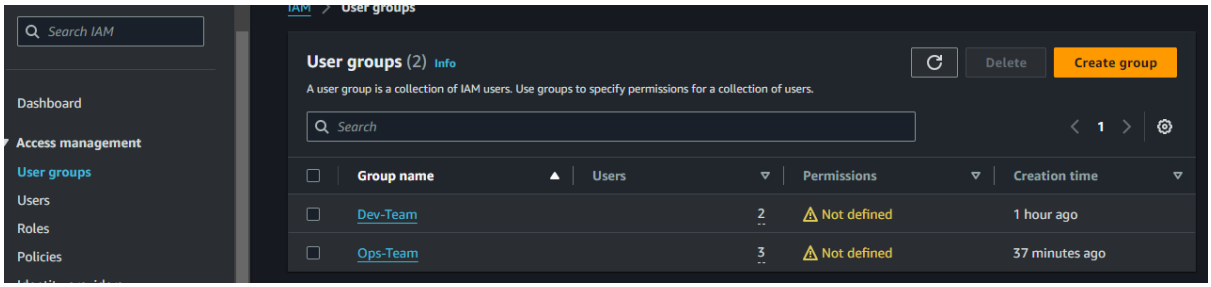
21. Adding Statement 3 only Allow to Create EC2 Instances EC2 but, find Below the Services which allowed to EC2 as per the task

```
{
    "Sid": "Statement3",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeKeyPairs",
        "ec2:CreateKeyPair",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVolumes",
        "ec2:CreateVolume",
        "ec2:AttachVolume",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
    ],
    "Resource": [
        "*"
    ]
```

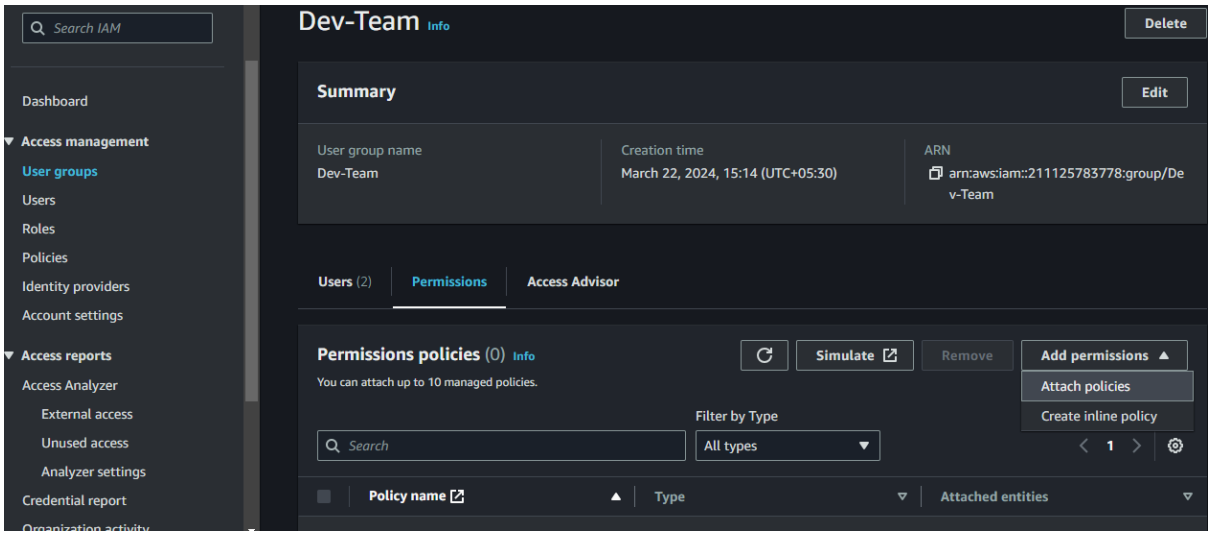
22. Give a Policy Name and Check your Permissions which defined to policy



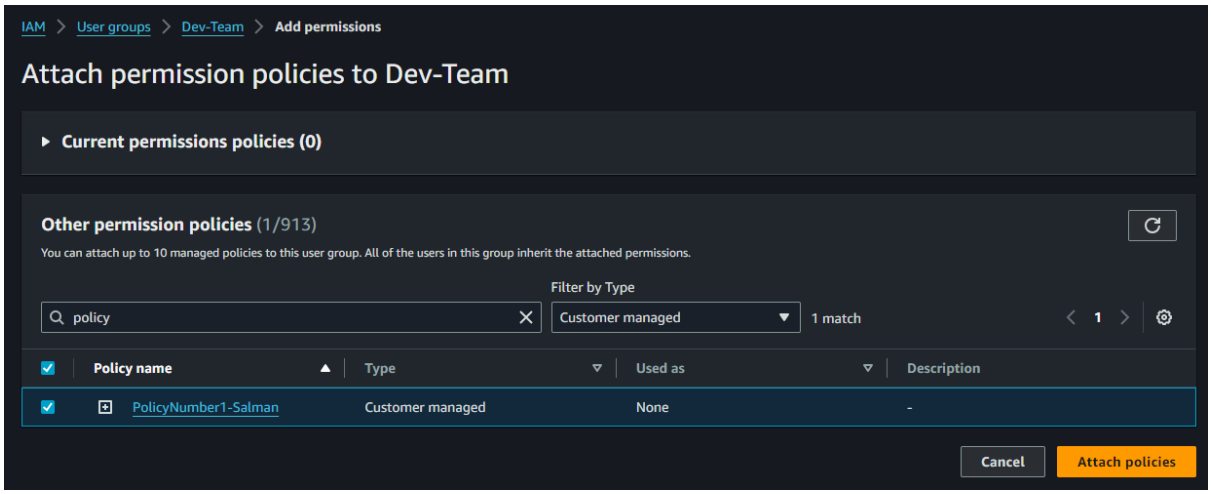
23. Now go to Groups Section and Go To Dev Team



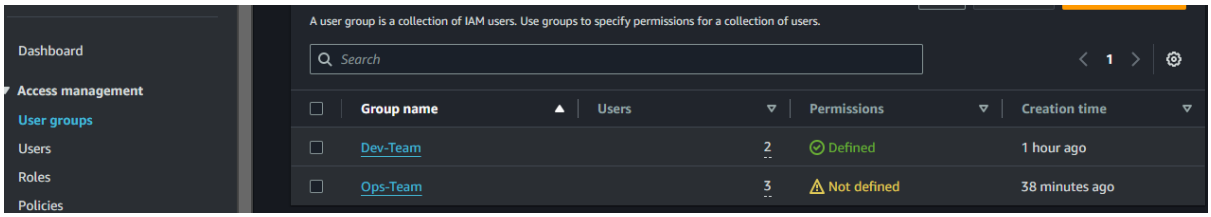
24. As per Task Click on Dev-Team > Permissions > Right Side Add Permissions > Attach Policies



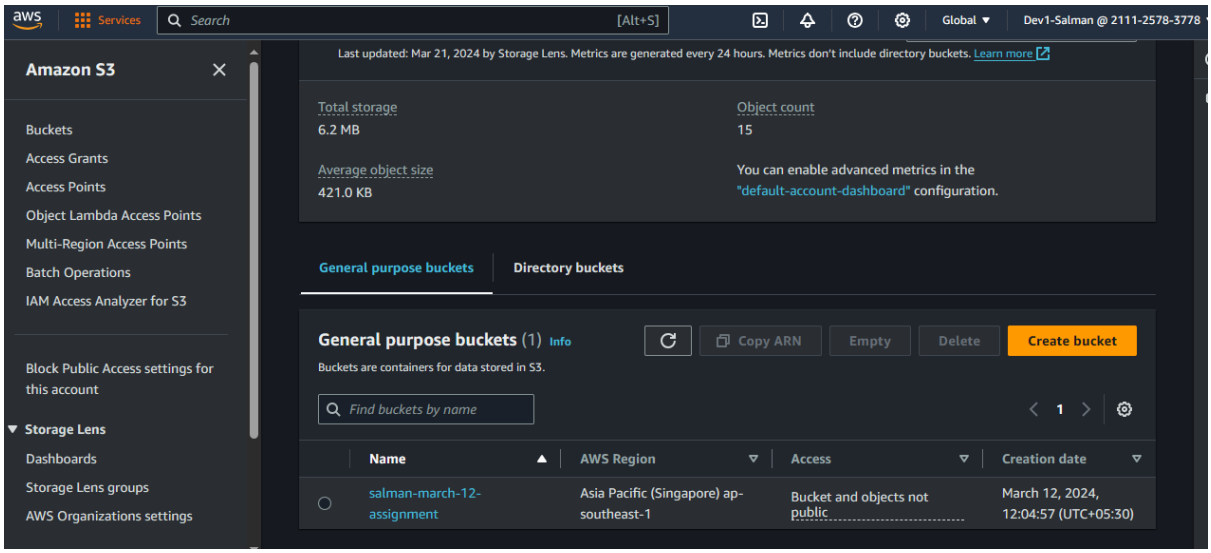
25. Select Your Created Policy and Attach Policies



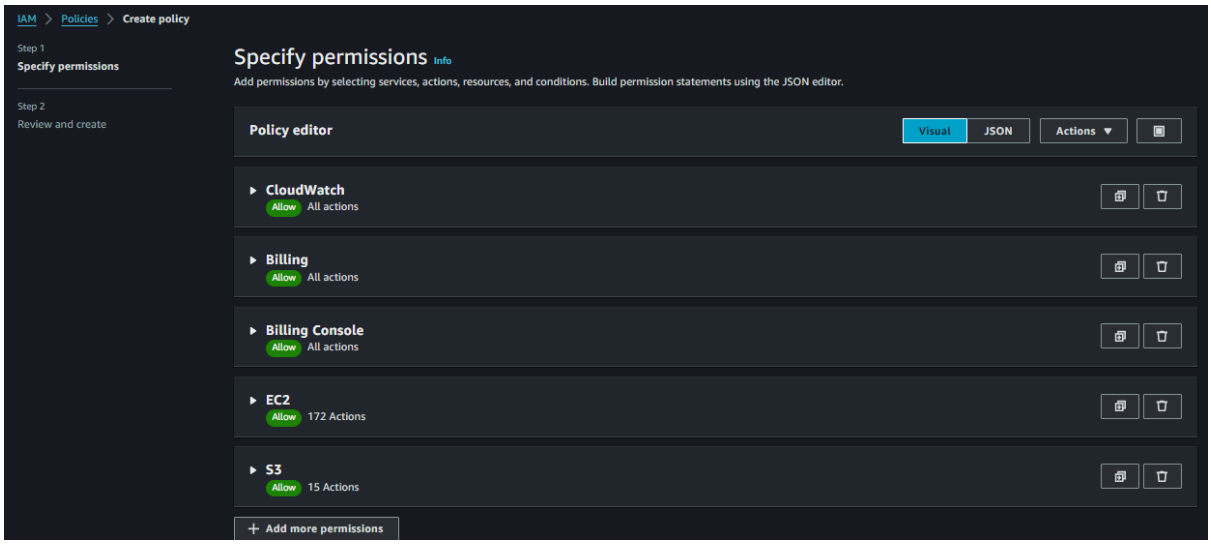
26. Now See that Permssions Defined



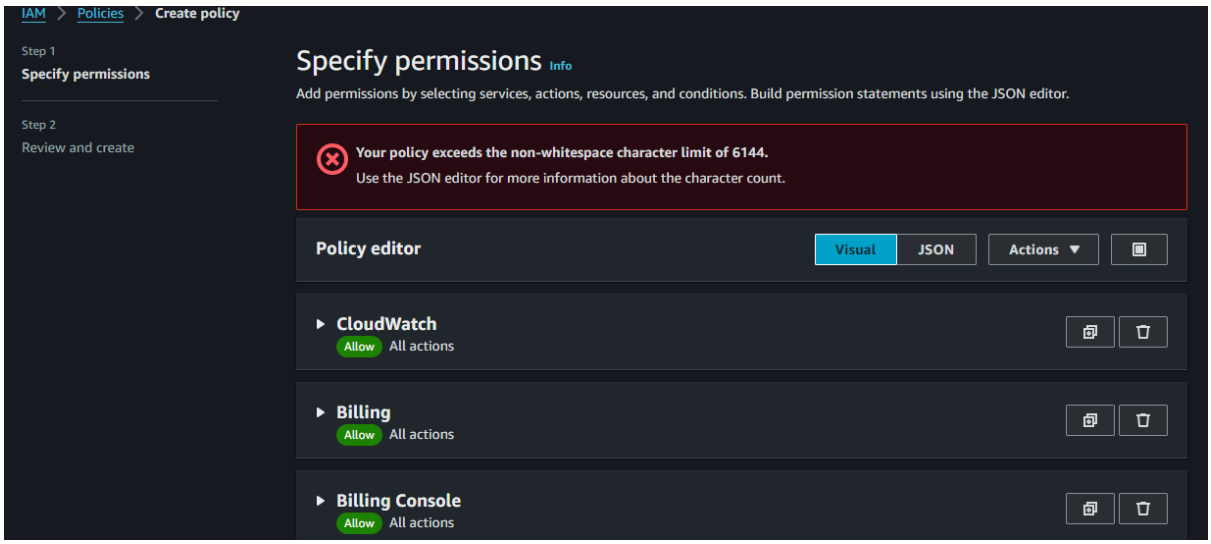
27. Now Check with Dev1-User use to see and edit s3 bucket because permission defined



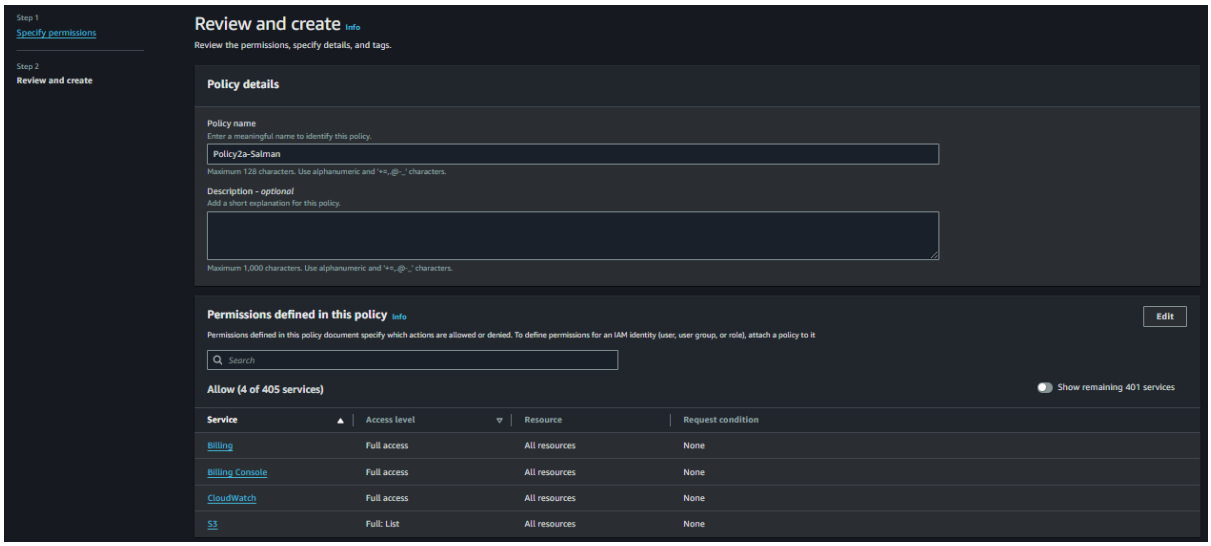
28. Now to go Polices and Create another Policies add Services as per the Task and Go Ahead



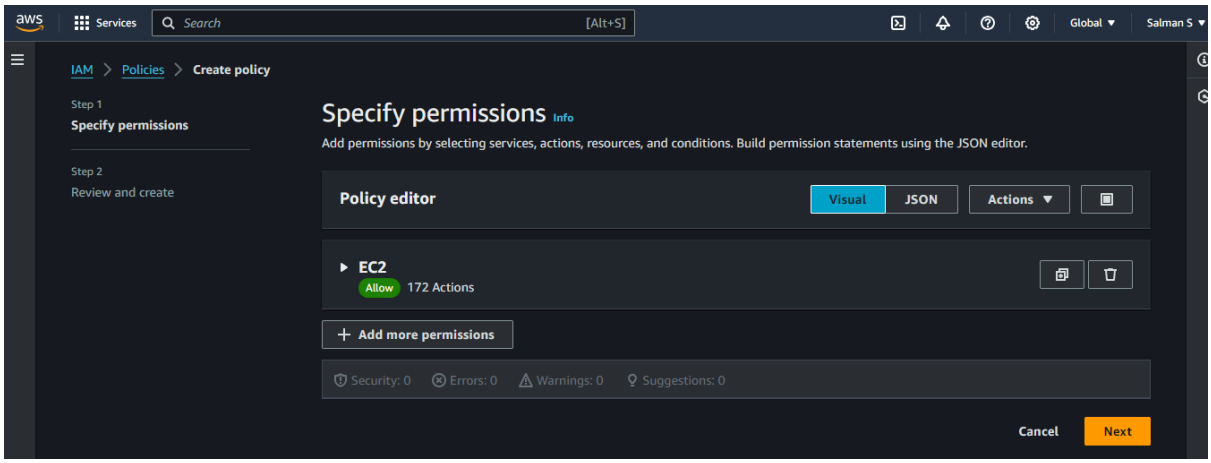
29. Triggered Error Because Non-Whitespace Character Limit of 6144



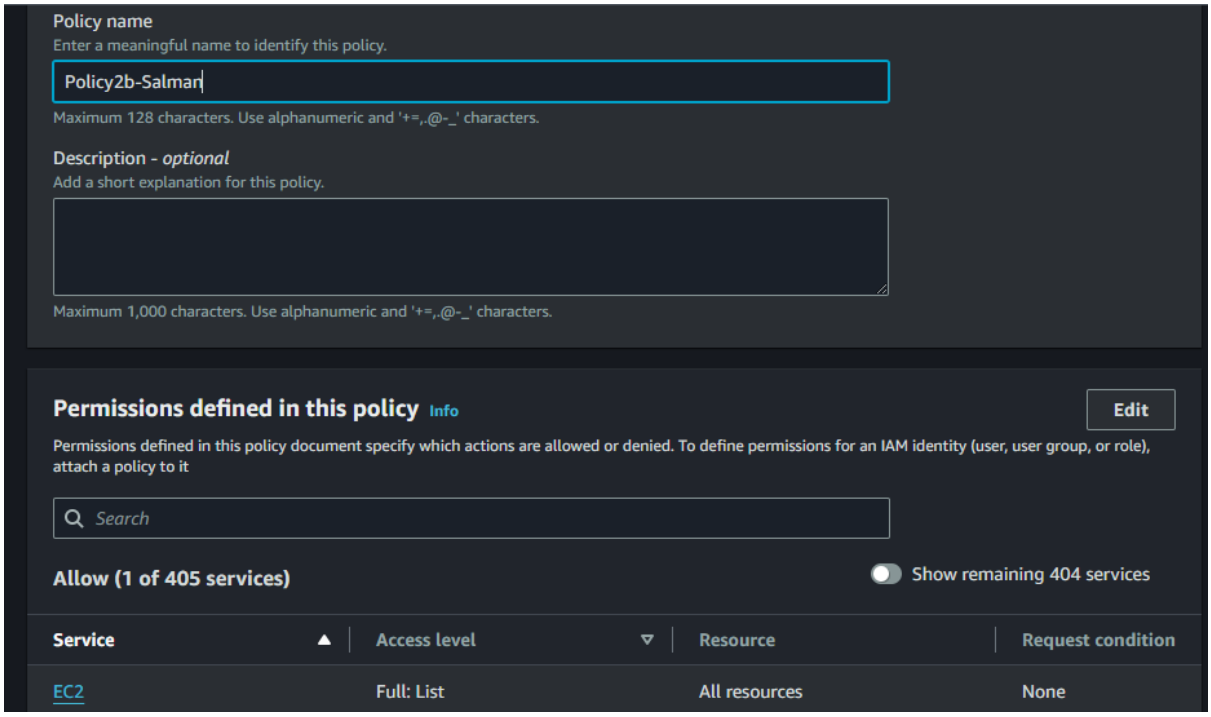
30. So Removed EC2 All Lists and Creating a Policy2a-Salman



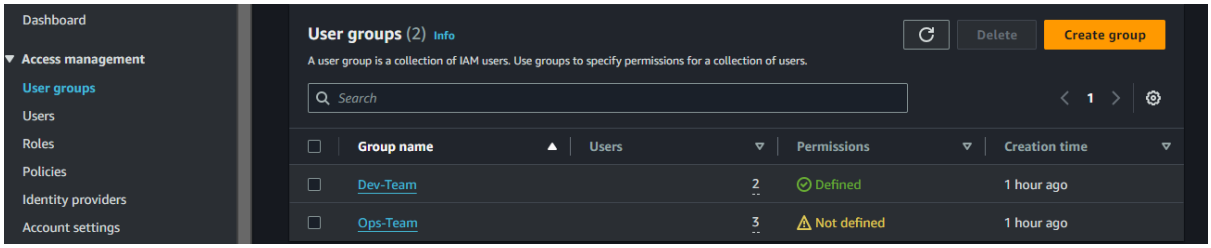
31. Now Again Creating Another Policies added EC2 All Lists and Click Next



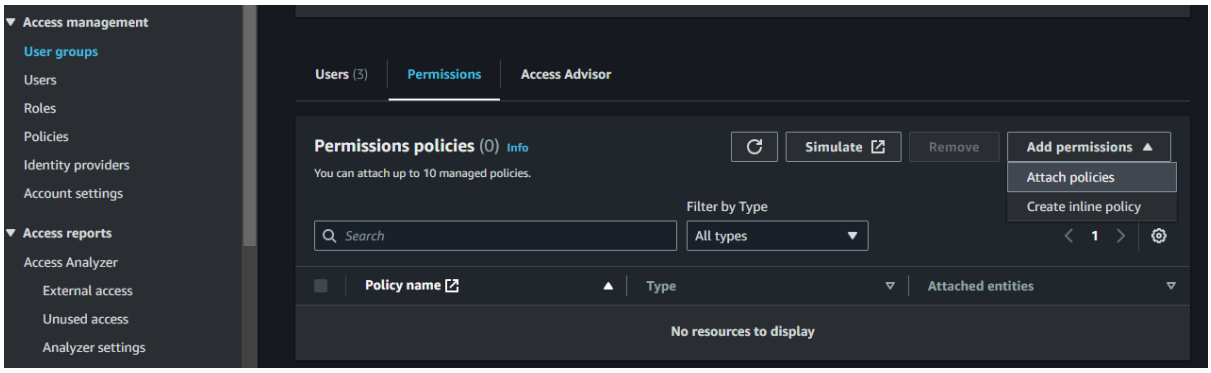
32. Policy2b-Salman



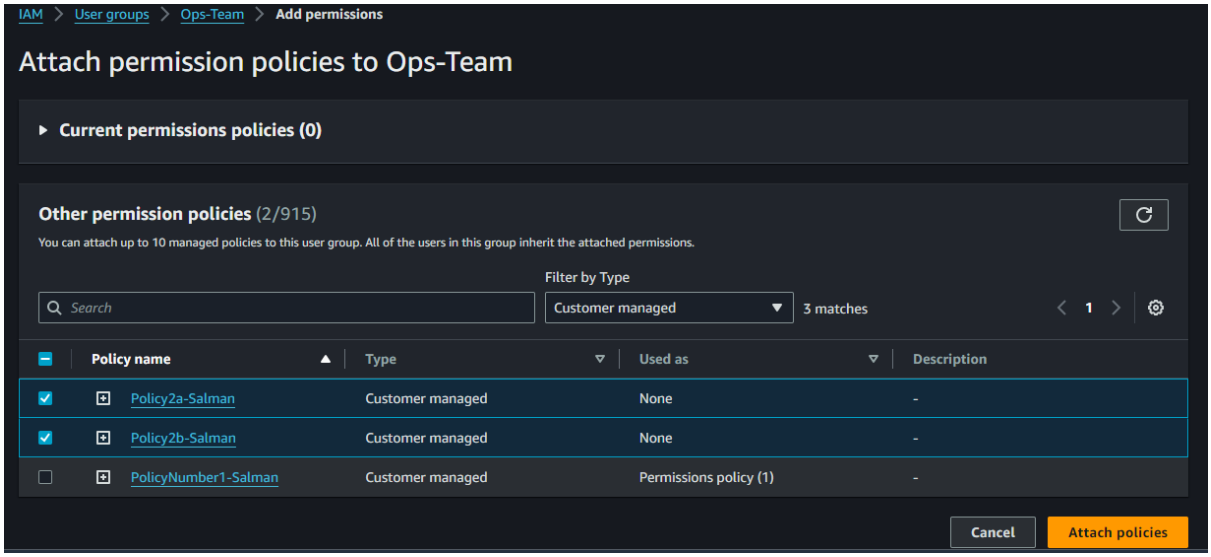
33. Now This Time go to Ops-Team As per the Task and Click



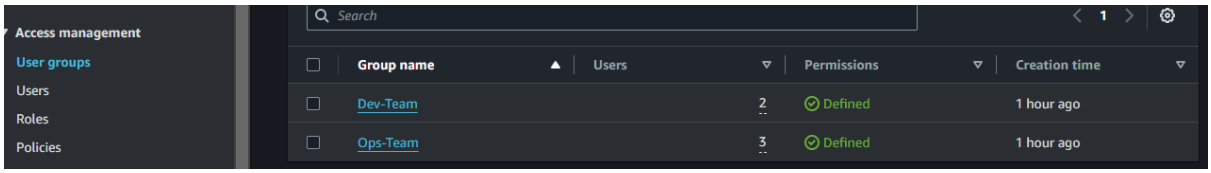
34. Same Click Attach Polices



35. Select 2 policies which we created for Ops-Team and Attach it



36. Now its Defined to Ops-Team and we Created Successfully Users and Policies



Module 3: IAM Roles Assignment

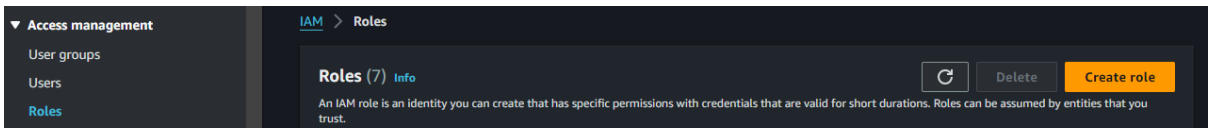
Problem Statement:

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.

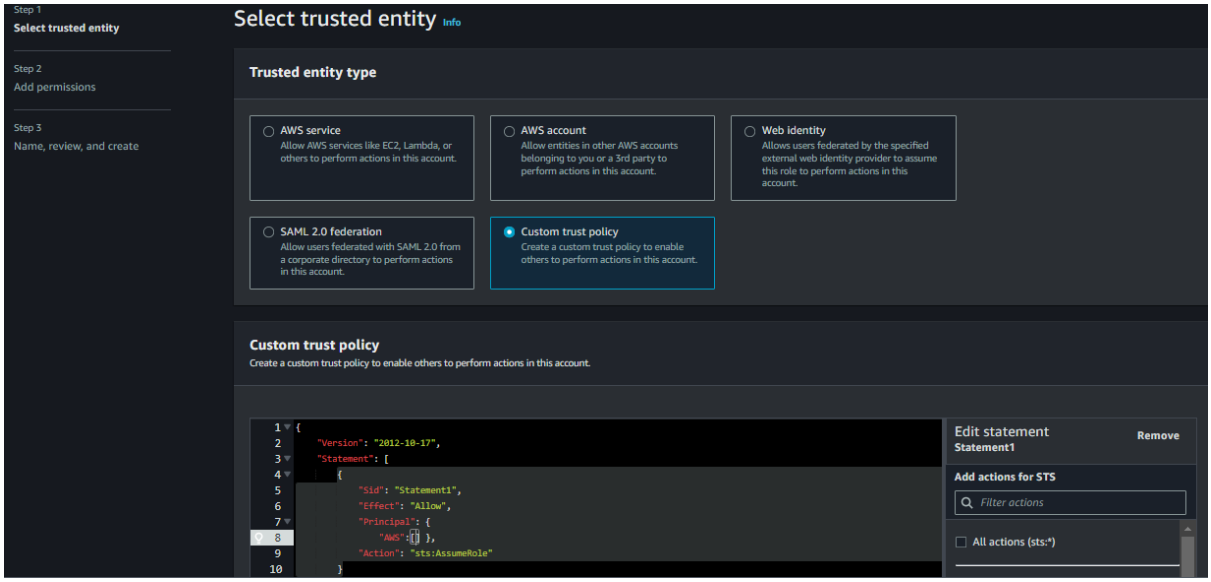
Tasks To Be Performed:

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.

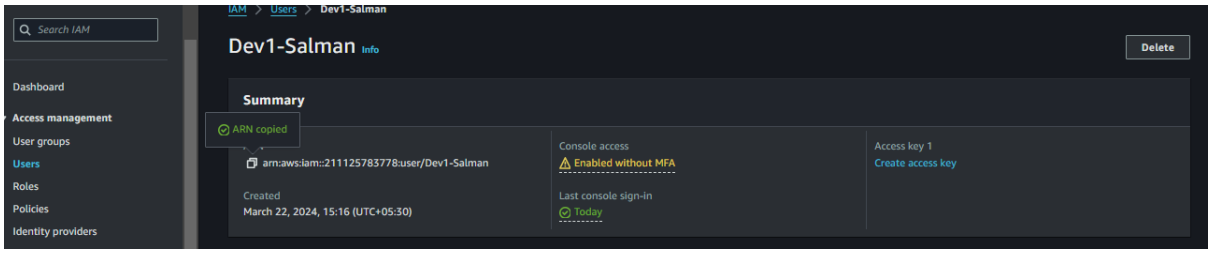
37. Go to IAM Dashboard > Roles > Create Role



38. Select Custom Trust Policy and Go to Code > Principal

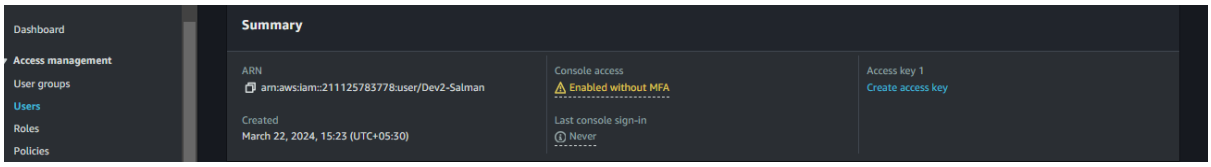


39. Go to Users Copy ARN of Dev1-Salman as User1 in the Task



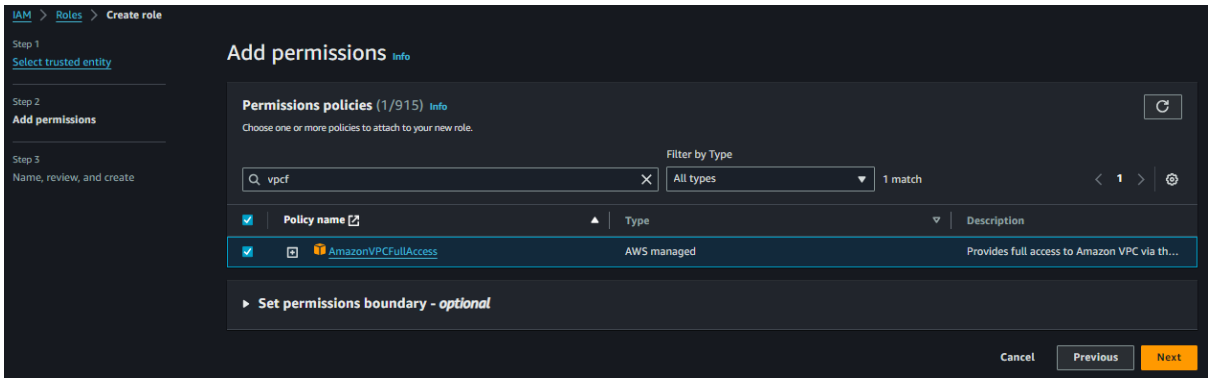
40. In the Principal part paste copied user1 ARN

41. Go to User2 and Copy ARN

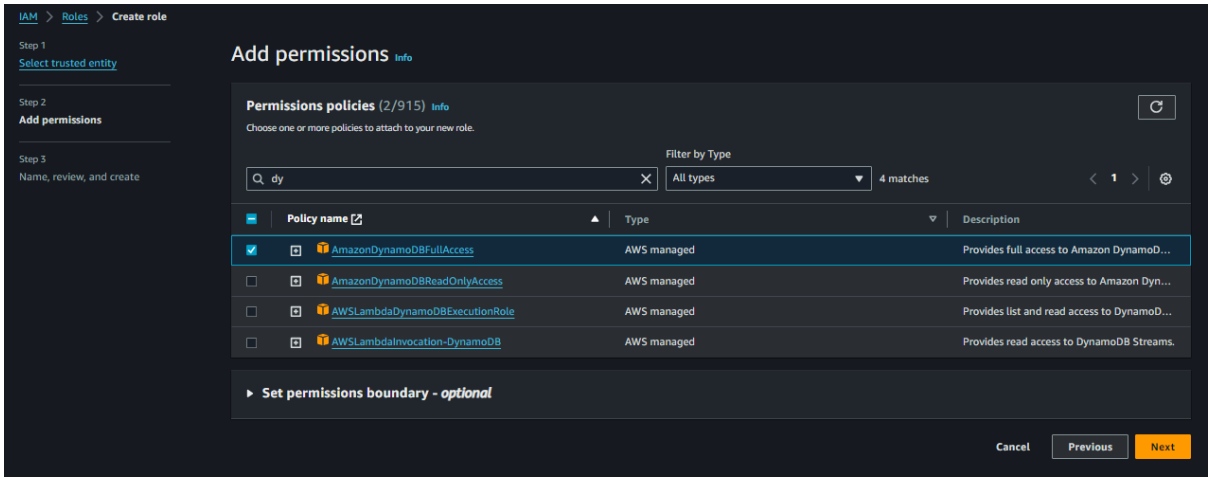


42. Again Come Paste Here

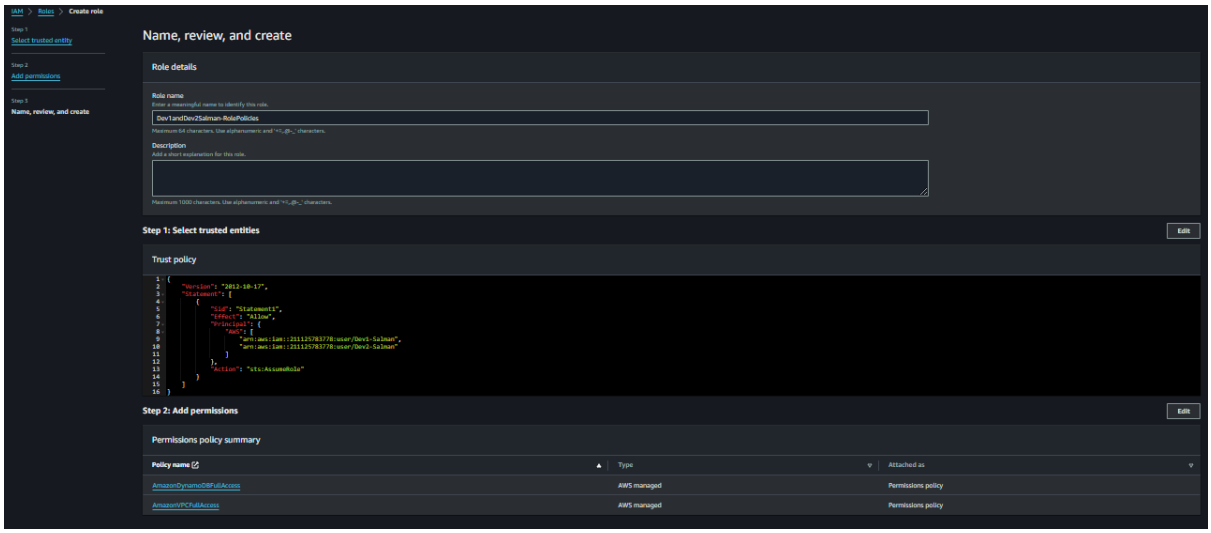
43. After Pasted the ARN and Clicking Next and finding Permissions Polices and Attach VPCfullAccess



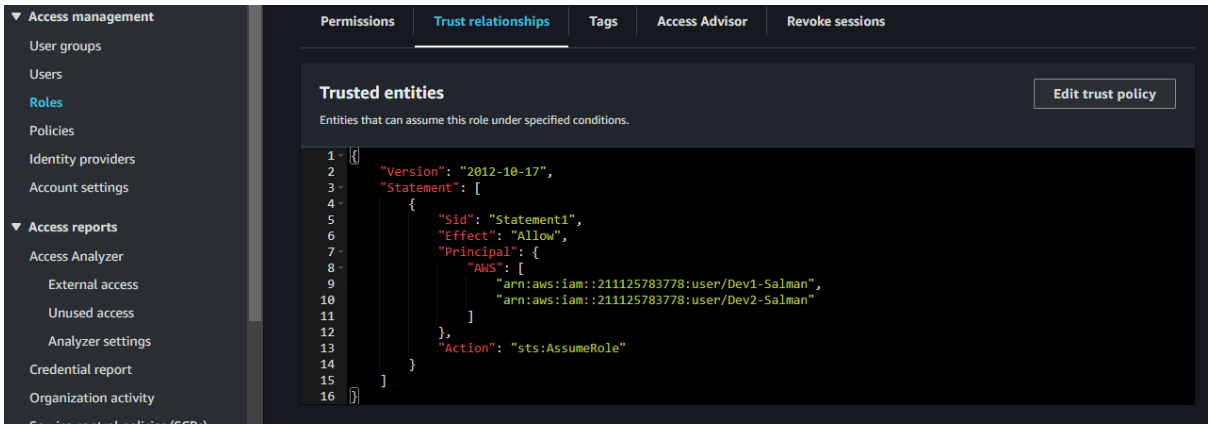
44. And Select Another Permission As per the Assignment DynamoDBFullAccess



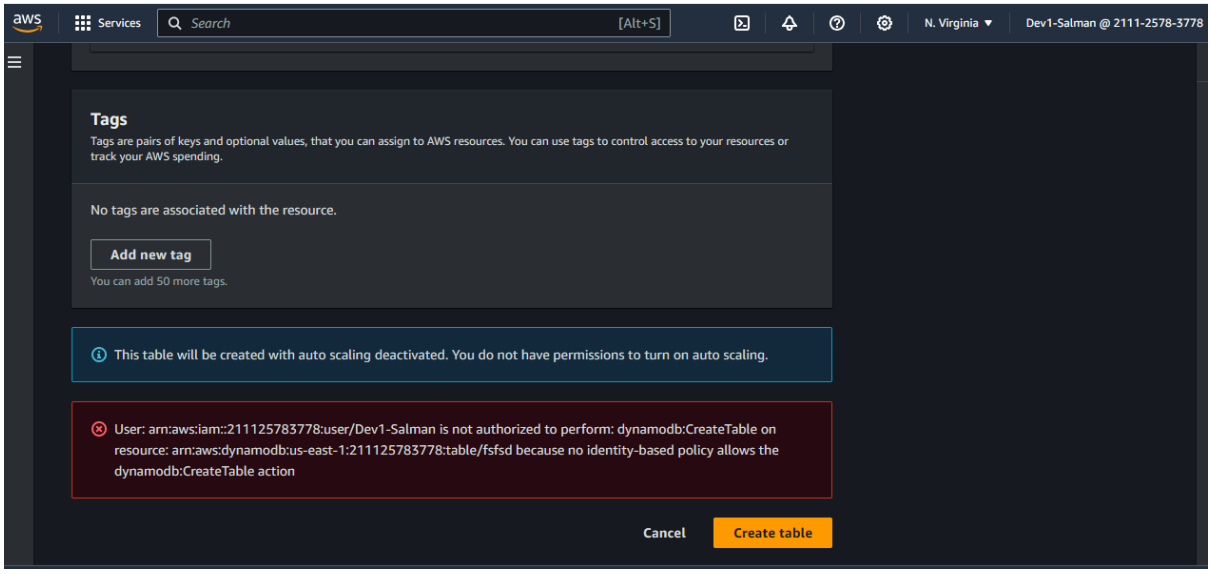
45. Name, Review and Create



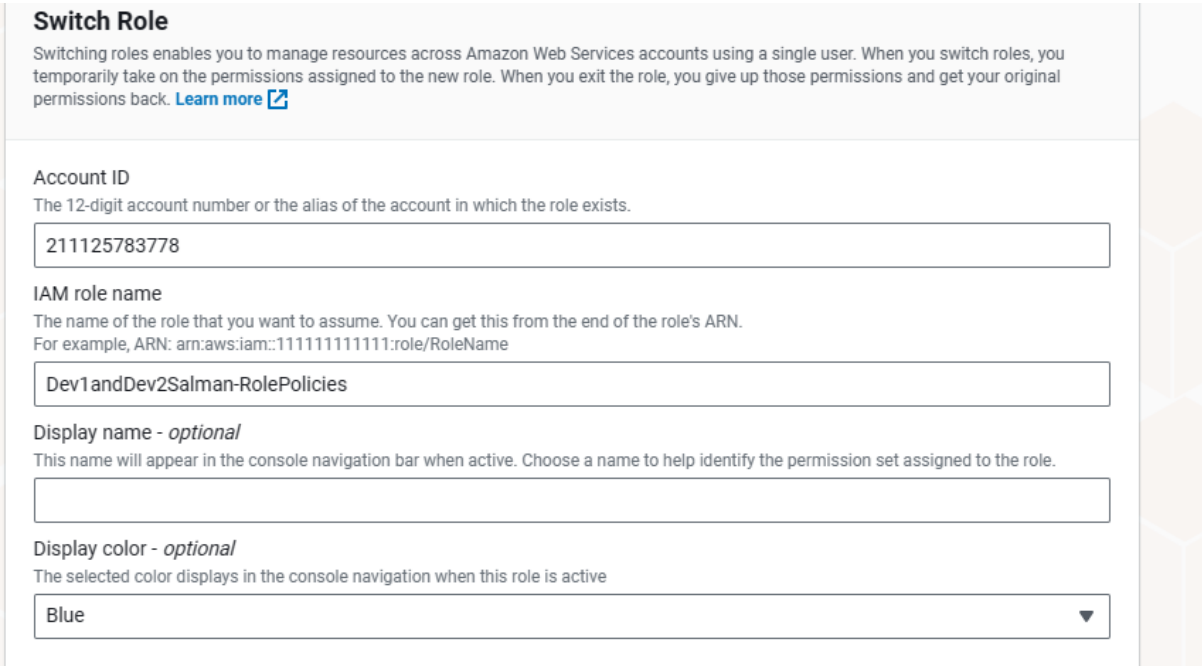
46. Created Role and Able to See the Code here and Also We can Edit it



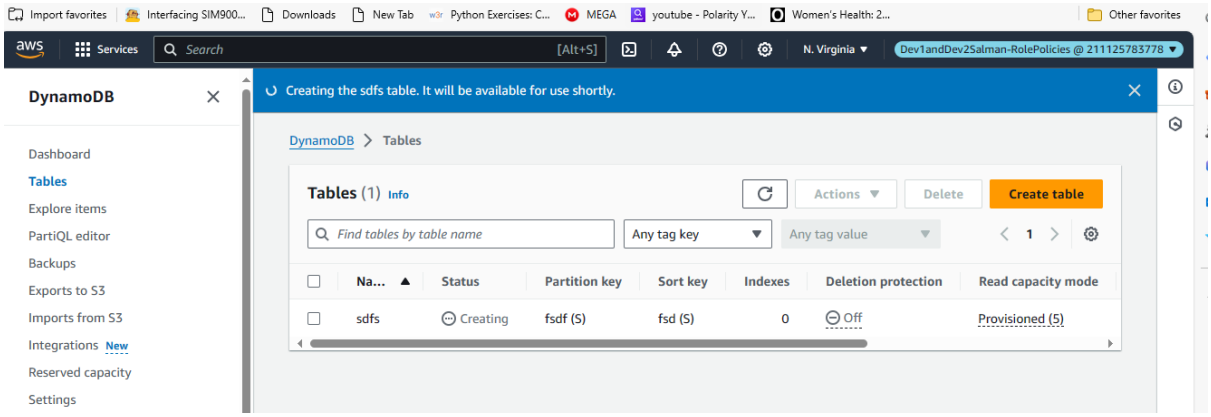
47. Check ones Login As a Dev1-Salman User able to Create DynomoDB Table see its saying your not authorized to create and Top Right Side Click on Account Id u will get a Option Switch role



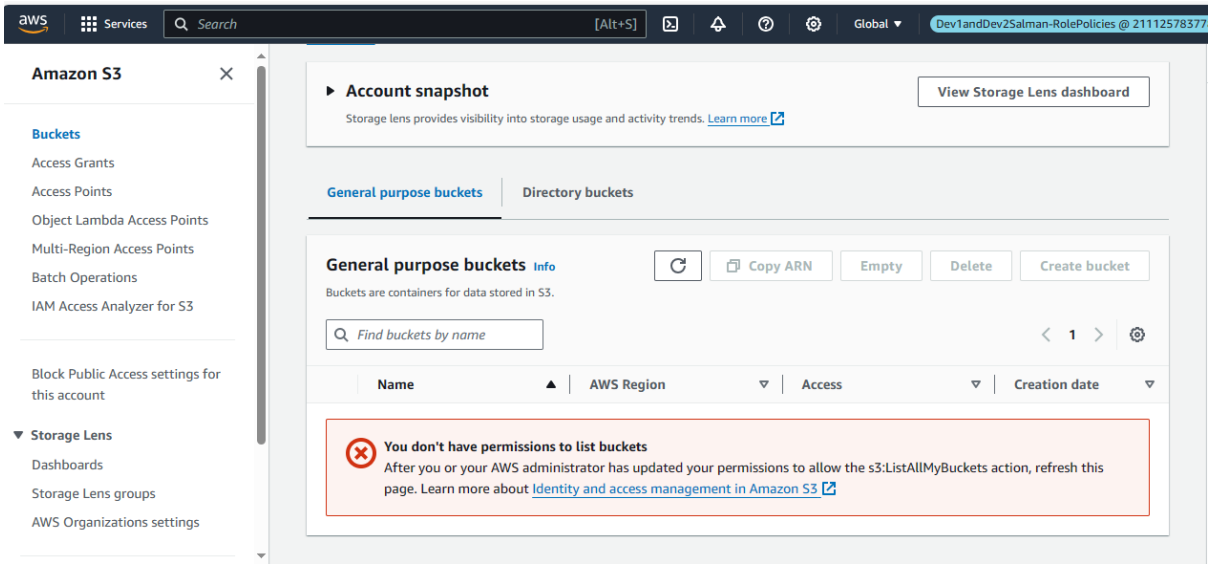
48. Paste the All Details and Role Name Which U Given and Login



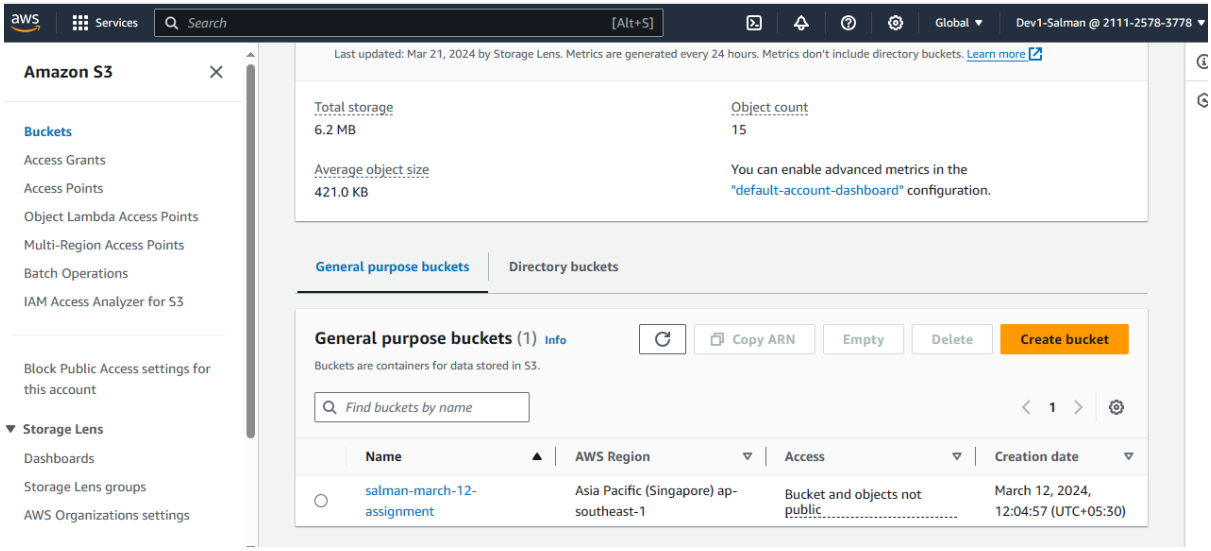
49. Now Logged as IAM-Role and See Now we able create table in Dynomodb



50. Previously As a IAM-User we Authorize to use s3 but not in IAM-Role



51. Switch Again IAM-User and Able and See and Create S3 bucket As a Dev1-user



*IAM-User :

IAM users represent individual users who can interact with AWS resources using their own long-term credentials (username and password, access keys, etc.),

*IAM-Role :

while IAM roles are a way to delegate permissions to entities within or outside your AWS account, such as applications or AWS services. Roles are temporary and can be assumed by users, services, or resources, granting them specific permissions for a limited duration.