

**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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

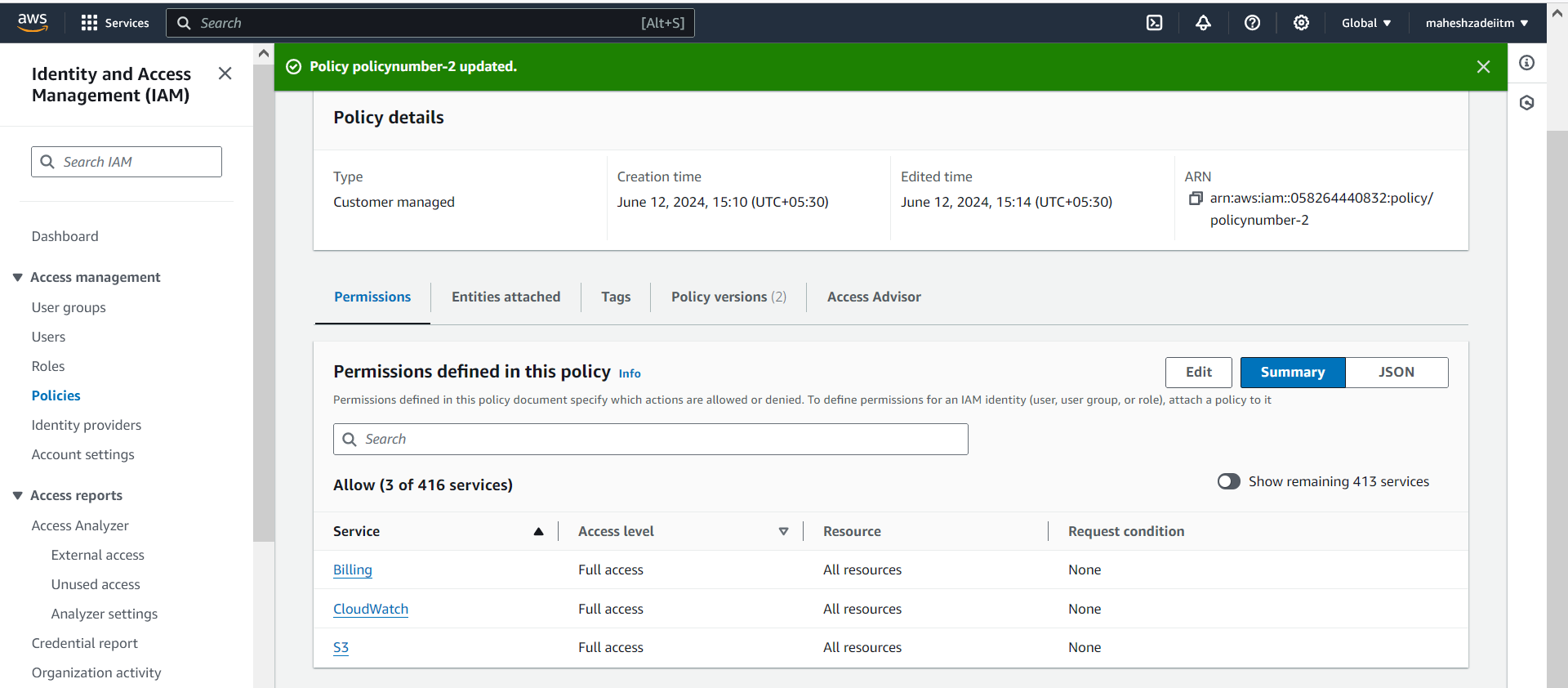
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



Policy attached

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Policy attached to ops team

A screenshot of a computer

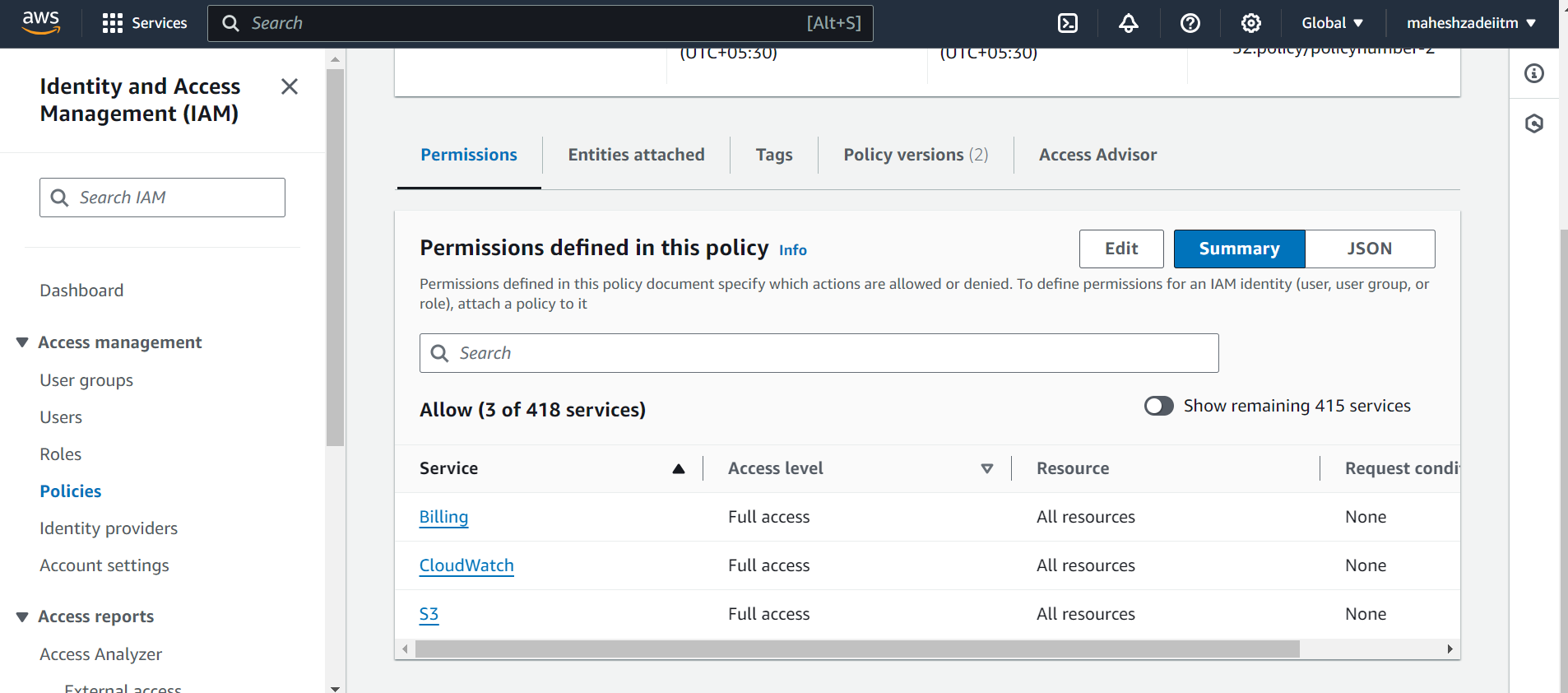
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



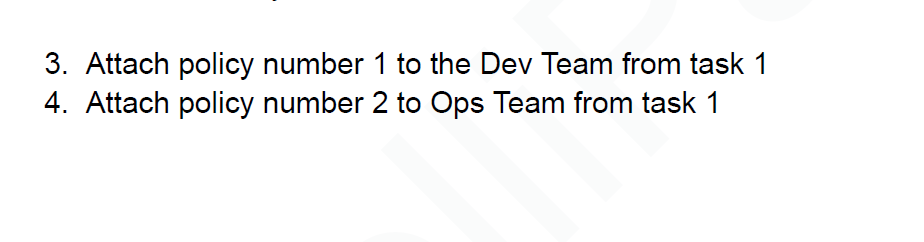
EC2 Permission added

A close up of a number

Description automatically generated

A screenshot of a computer

Description automatically generated



A close up of a button

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Click on attach policy

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

For the next task, let’s Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.

Click on Roles 🡪 Create Role

A screenshot of a computer

Description automatically generated

Click on next

Search in the policies and add **AmazonVPCFullAccess** and **AmazonDynamoDBFullAccess**. Click on Next.

Name: VPCandDynamoDBFullAccessRole 🡪 Click on Create Role

A screenshot of a computer

Description automatically generated

Search in the policies and add **AmazonVPCFullAccess** and **AmazonDynamoDBFullAccess**. Click on Next.

Name: VPCandDynamoDBFullAccessRole 🡪 Click on Create Role

A screenshot of a computer

Description automatically generated

A screenshot of a chat

Description automatically generated

Click on create Rule

A screenshot of a computer

Description automatically generated

Now we need to add users to this role.

Go to Roles 🡪 VPCandDynamoDBFullAccessRole

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Policy updated

Copy Swicth role url

A screenshot of a computer

Description automatically generated

<https://signin.aws.amazon.com/switchrole?roleName=VPCandDynmaodbfullaccess&account=maheshzade>

Paste in browser

A screenshot of a computer

Description automatically generated

Click on Switch Role

A screenshot of a computer

Description automatically generated

Also it is able to fetch the table details and showing that **there are no tables in this account** and no permission errors.

Similary navigate to VPC and see that it is fully accessible.

A screenshot of a computer

Description automatically generated

It is able to fetch the details and no permission errors

Summary

1. Created users and groups. Added those users to the appropriate groups.
2. Created 2 policies for different use cases. Attached them to the respective groups asked in the problem statement.
3. Created a role to allow 2 users to have complete VPC and DynamoDB access.
4. Logged in to User1 (Dev1) and verified that it is working as expected.

Thanks you.