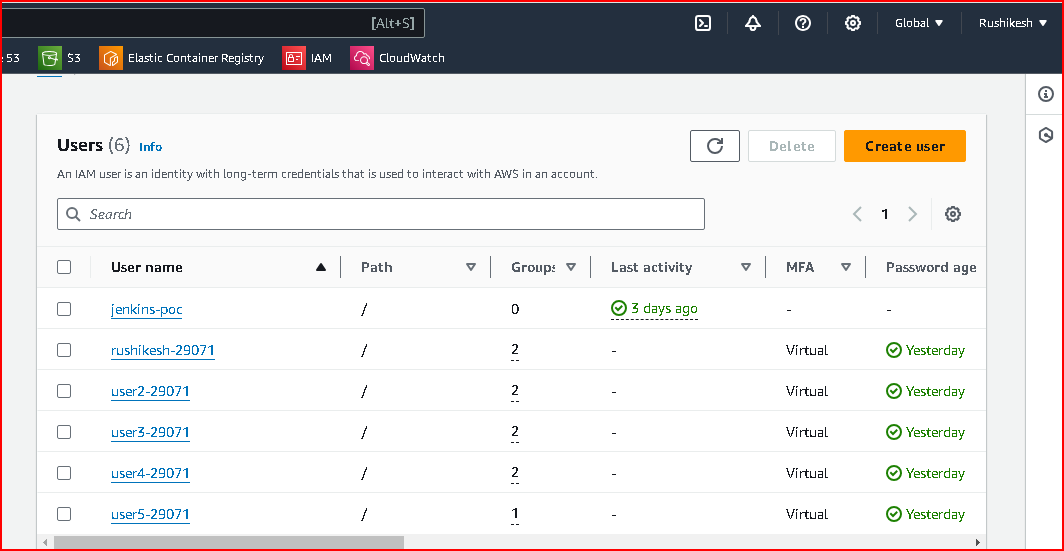
**Tasks on IAM**

**a. Create 5 IAM users:**

User 1: Rushikesh-29071

User2-29071, User3-29071, User4-29071, User5-29071



**b. For all users, enable MFA using a virtual MFA device.**

Go to the IAM Management Console.

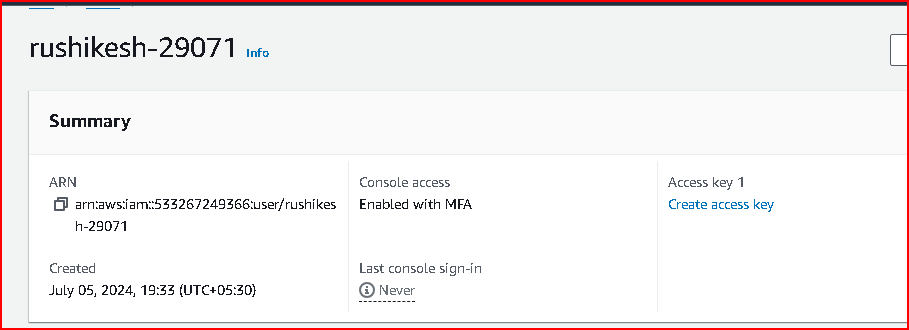
Click on Users in the left navigation pane.

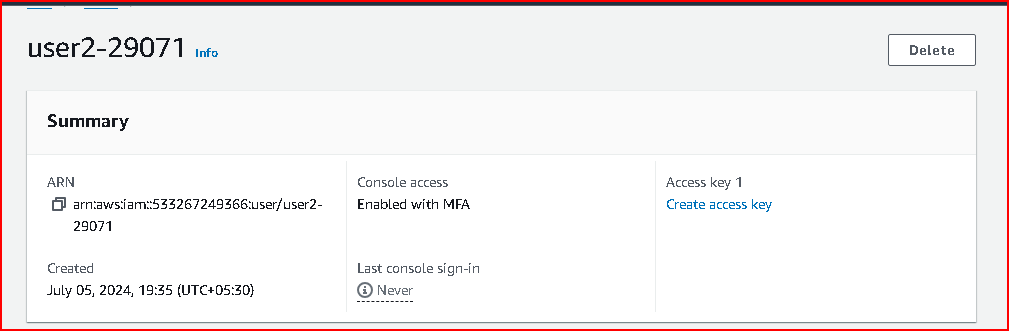
Click on the username of the first user (e.g., name1-your\_empid).

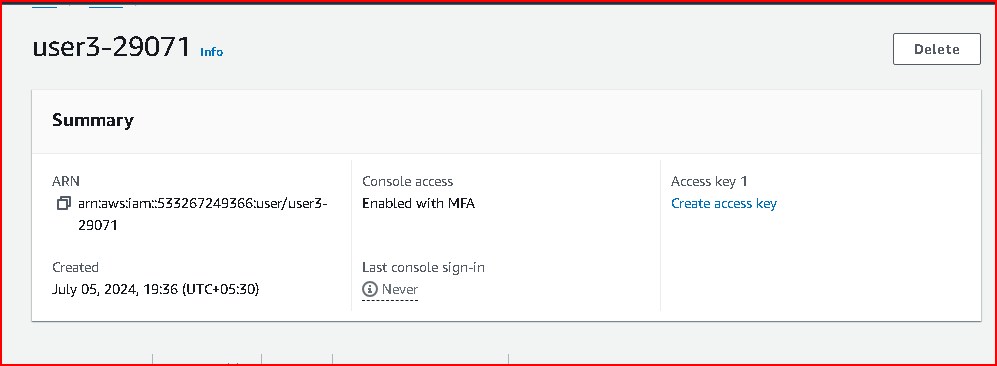
Scroll down to the Security credentials tab.

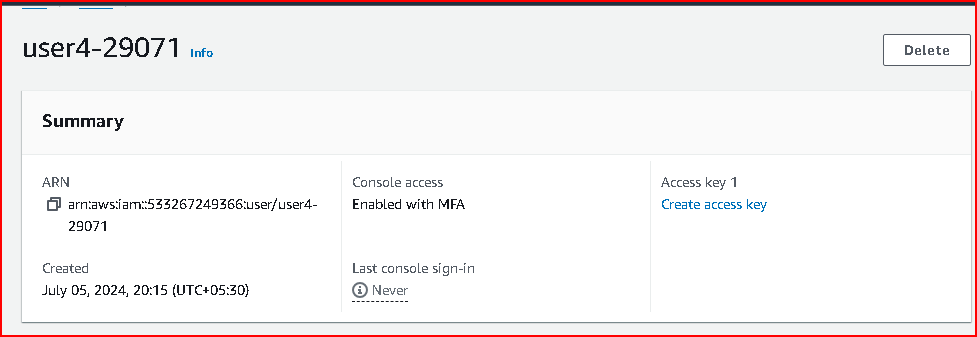
Click Manage next to Assigned MFA device.

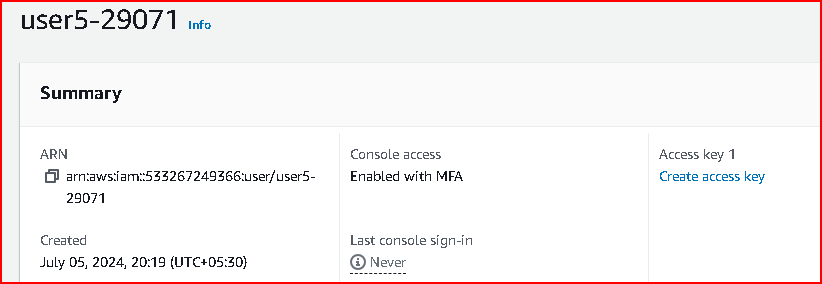
Choose Virtual MFA device and click Continue.

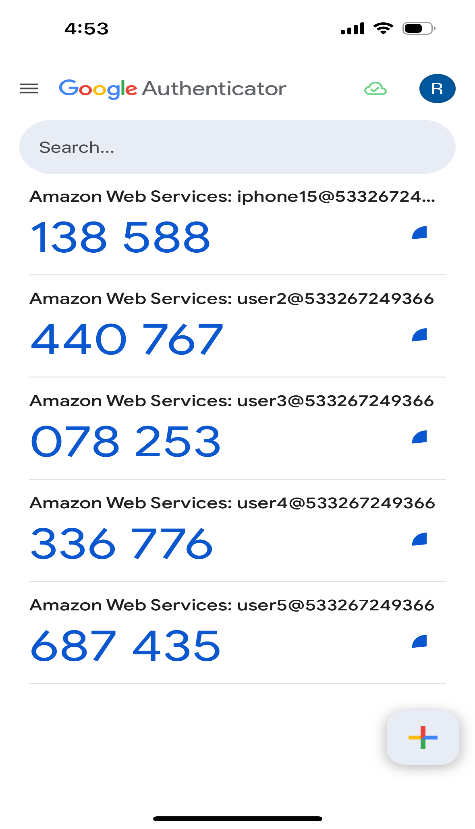
****

****

****

****

****

****

**c. Create an IAM group named "EC2Management", “VPCManagement”.**

Go to the IAM Management Console.

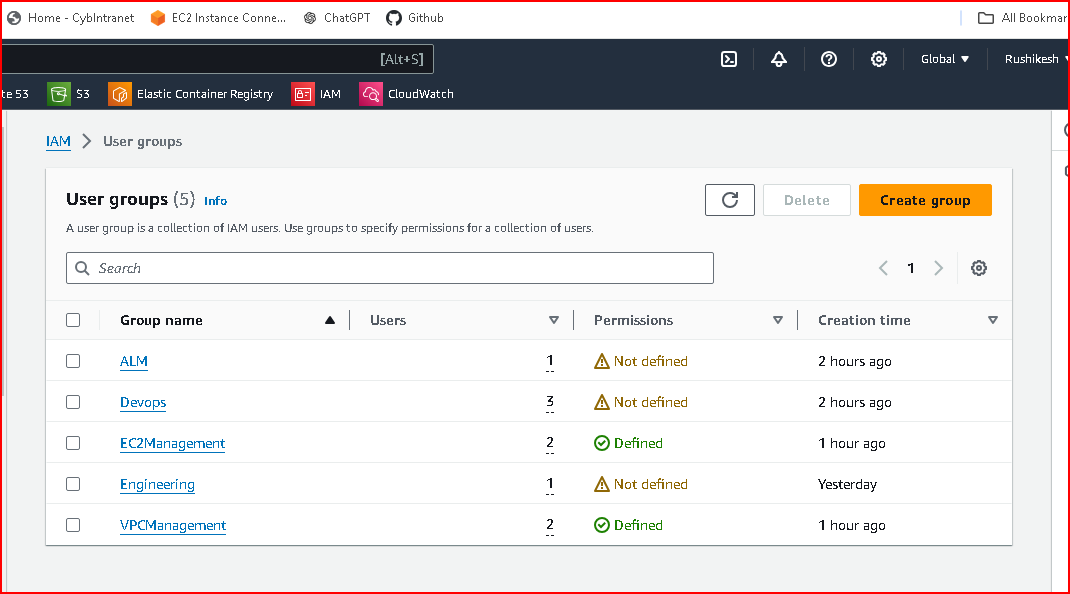
Click on Groups in the left navigation pane.

Click Create group.

Enter EC2Management as the Group name.

Click Next Step.

Review and click Create group

****

**d. After creating "EC2Management" group, add User 1 & User 2 to this group.**

Go to the IAM Management Console.

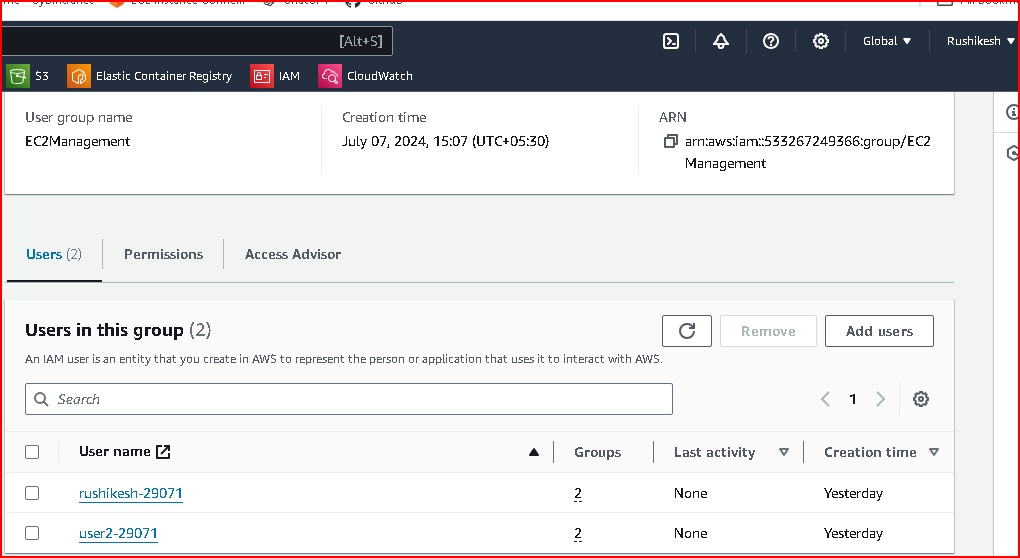
Click on Groups in the left navigation pane.

Click on the EC2Management group.

Click on the Add users to group button.

Check the boxes next to rushikesh\_29071 and user2-29071

Click Add users.



**e. User 3 and User 4 in “VPCManagement” group.**

Go to the IAM Management Console.

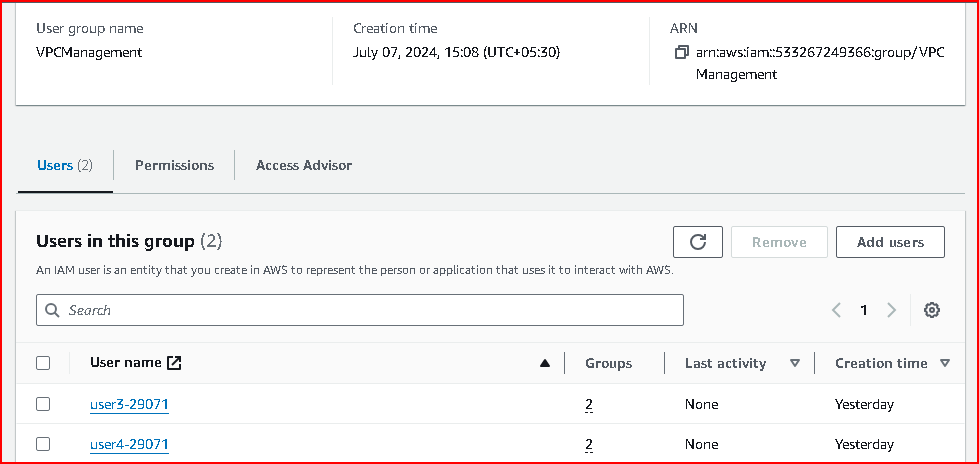
Click on Groups in the left navigation pane.

Click on the EC2Management group.

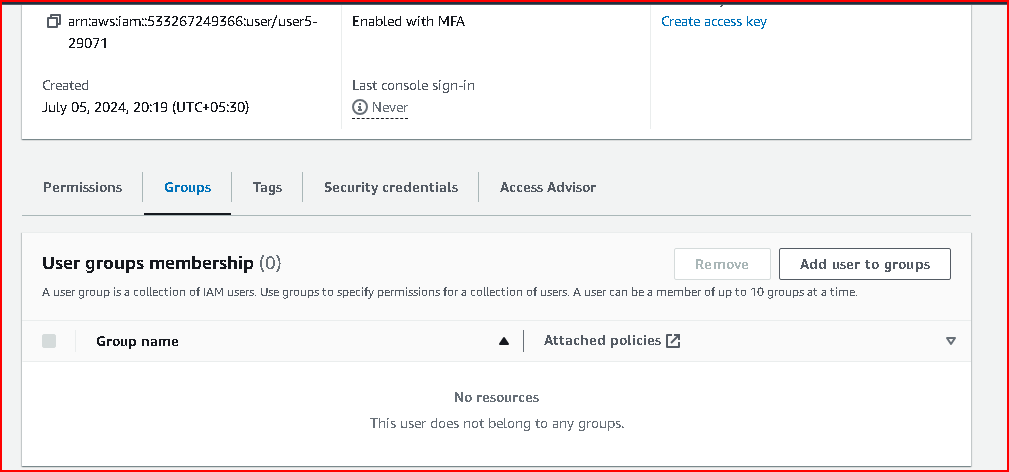
Click on the Add users to group button.

Check the boxes next to user3-29071 and user4-29071

Click Add users.



**f. User 5 will not be part of any group.**

****

**g. Create a policy for "EC2Management” group for creating & terminating EC2 instances**

Go to the IAM Management Console: IAM Console.

Click on Policies in the left navigation pane.

Click Create policy.

Choose the visual editor tab.

Click Review policy.

Provide a name for the policy, e.g., EC2ManagementPolicy.

Optionally, add a description.

Click Create policy.

Attaching the Policy to the "EC2Management" Group

Go to the IAM Management Console.

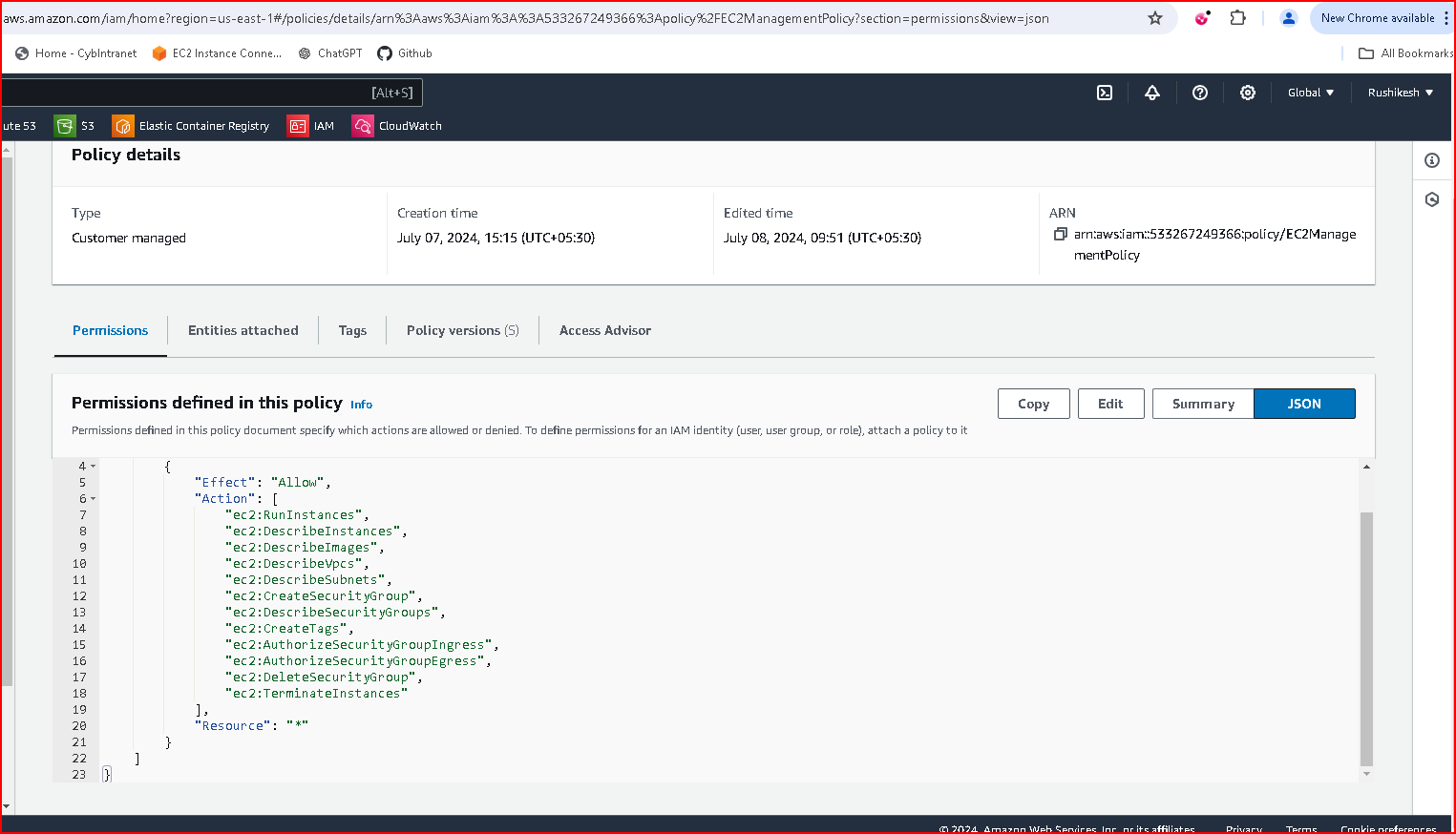
Click on Groups in the left navigation pane.

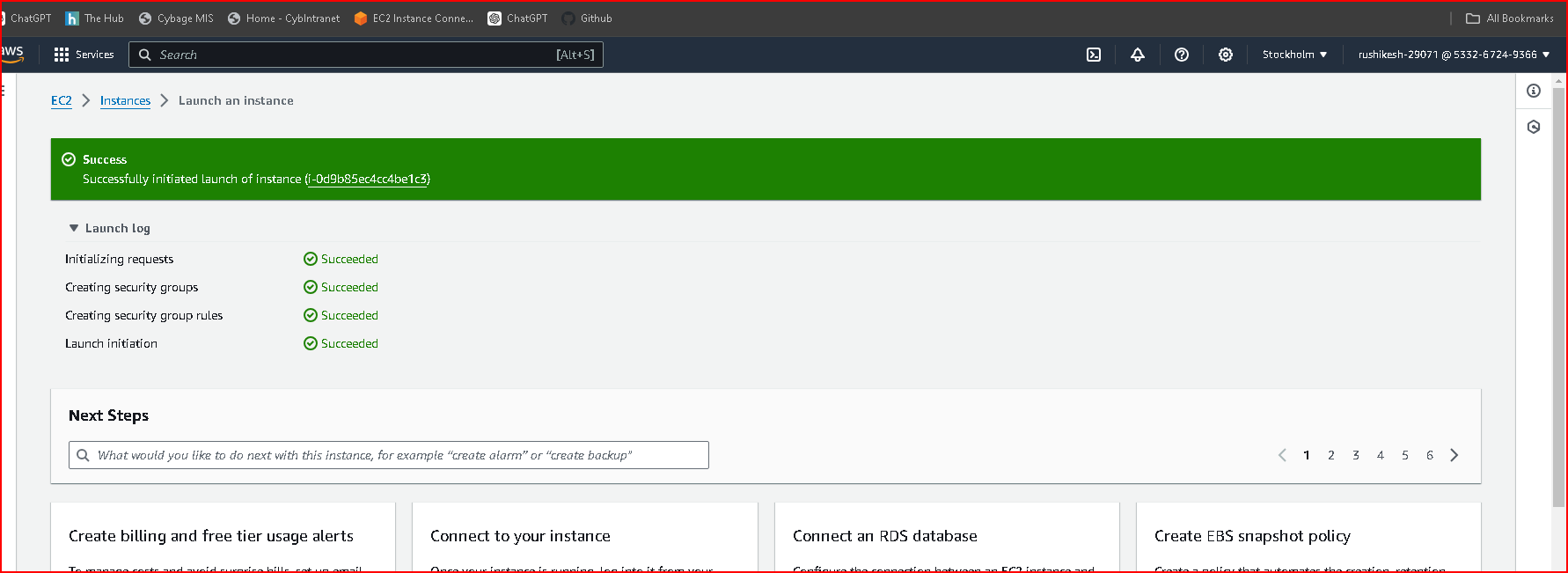
Click on the EC2Management group.

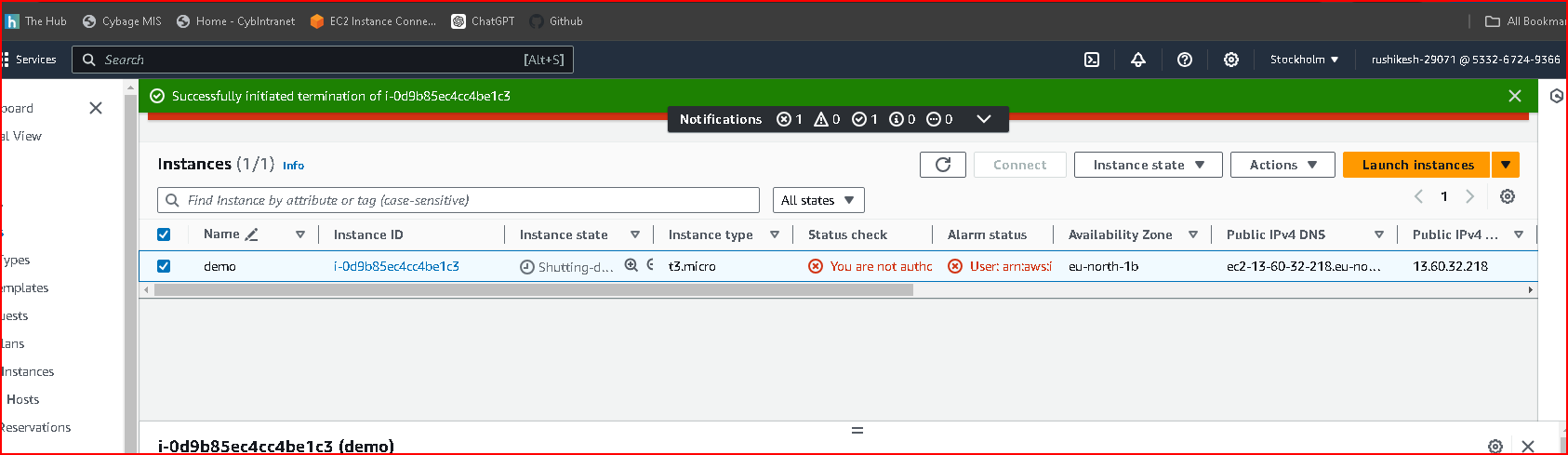
In the Permissions tab, click Attach policies.

Search for the policy you created (EC2ManagementPolicy).

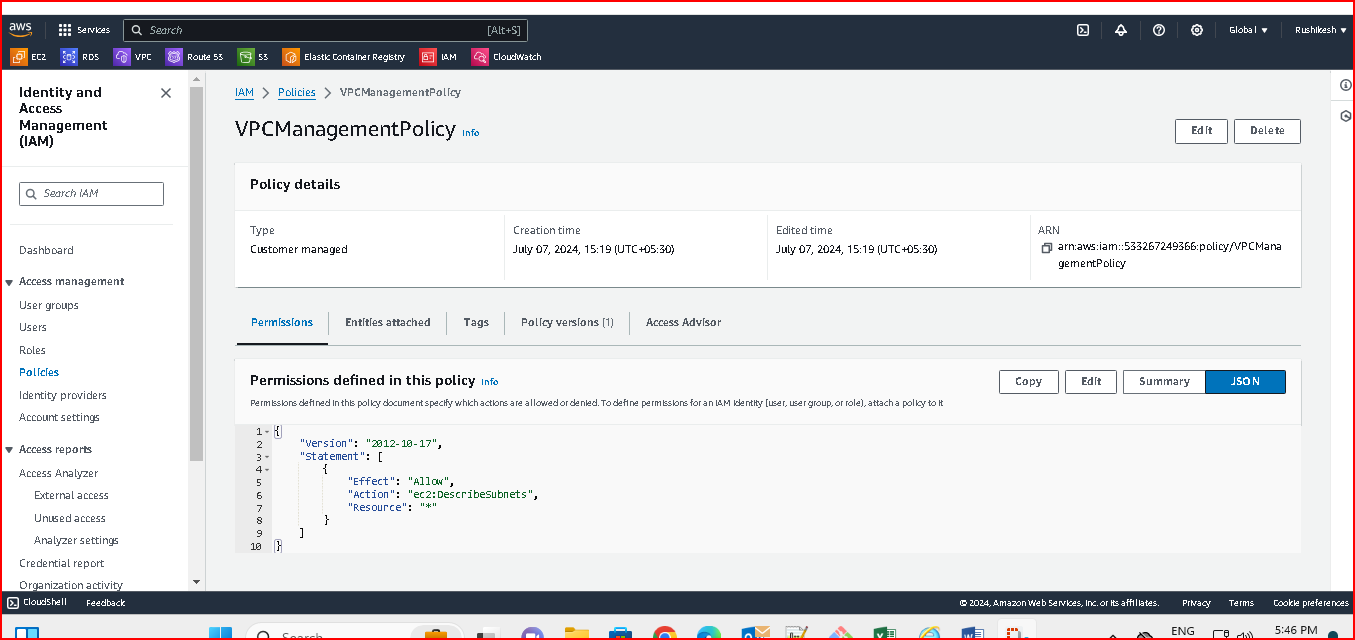
Click Attach policy.

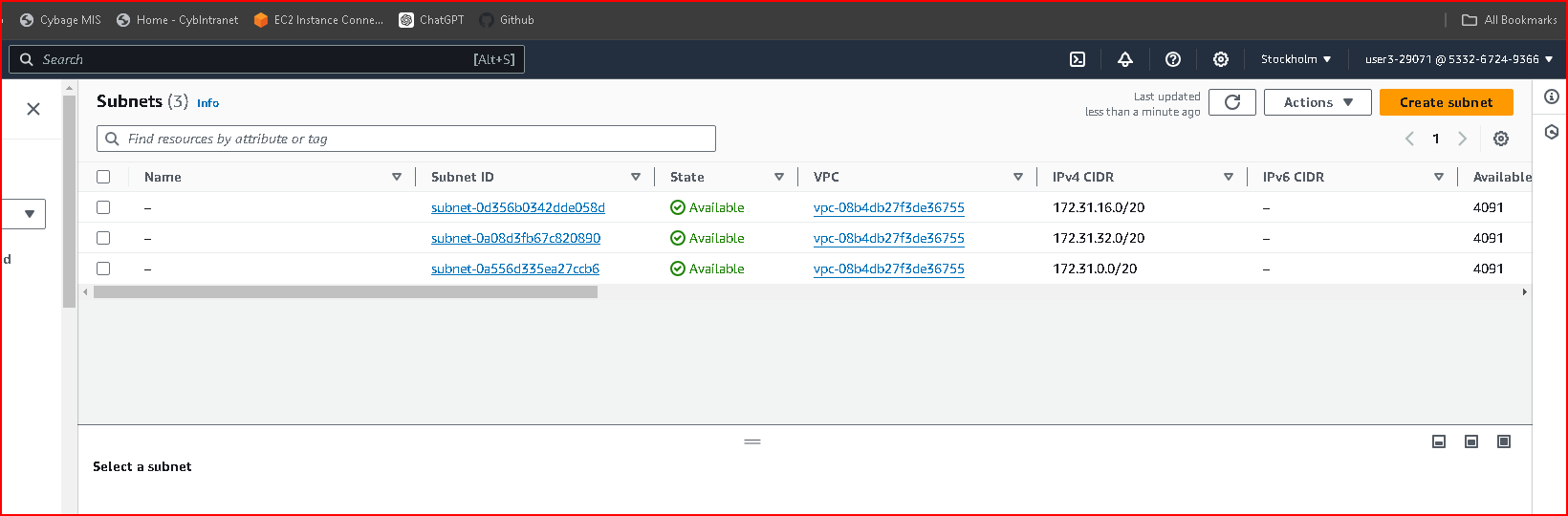






**h. Create a policy for " VPCManagement” group for only listing the Subnets in your account**

****

****

1. **Create 1 Role for EC2 instance for accessing data from ECR(read-only)**

A.

1. Navigate to the IAM Console:

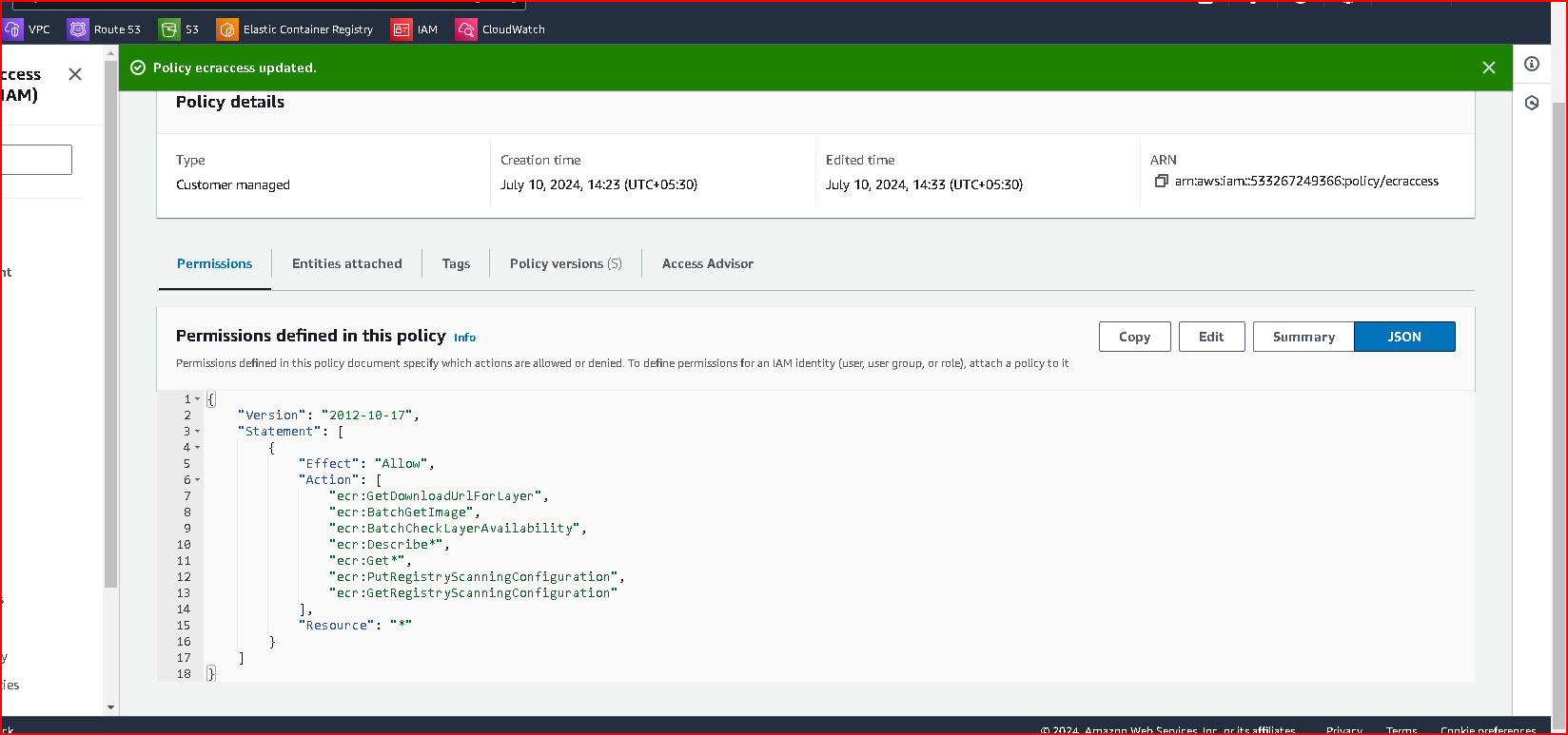
2. Create Policy:

Click on "Policies" in the left sidebar.

Click on "Create policy", then select the "JSON" tab.

3. Policy JSON:

Use the following JSON as a template for your policy



Click Next: Review.

Click "Create policy".

B. Create an IAM Role for EC2 Instance

Now, create an IAM role that the EC2 instance will assume, with the policy you just created attached.

1. Navigate to Roles:

In the IAM Console, click on "Roles" in the left sidebar.

Click on Create role

2. Choose the service that will use this role:

Select "EC2" as the service that will use this role.

Click "Next: Permissions"

3. Attach Policies:

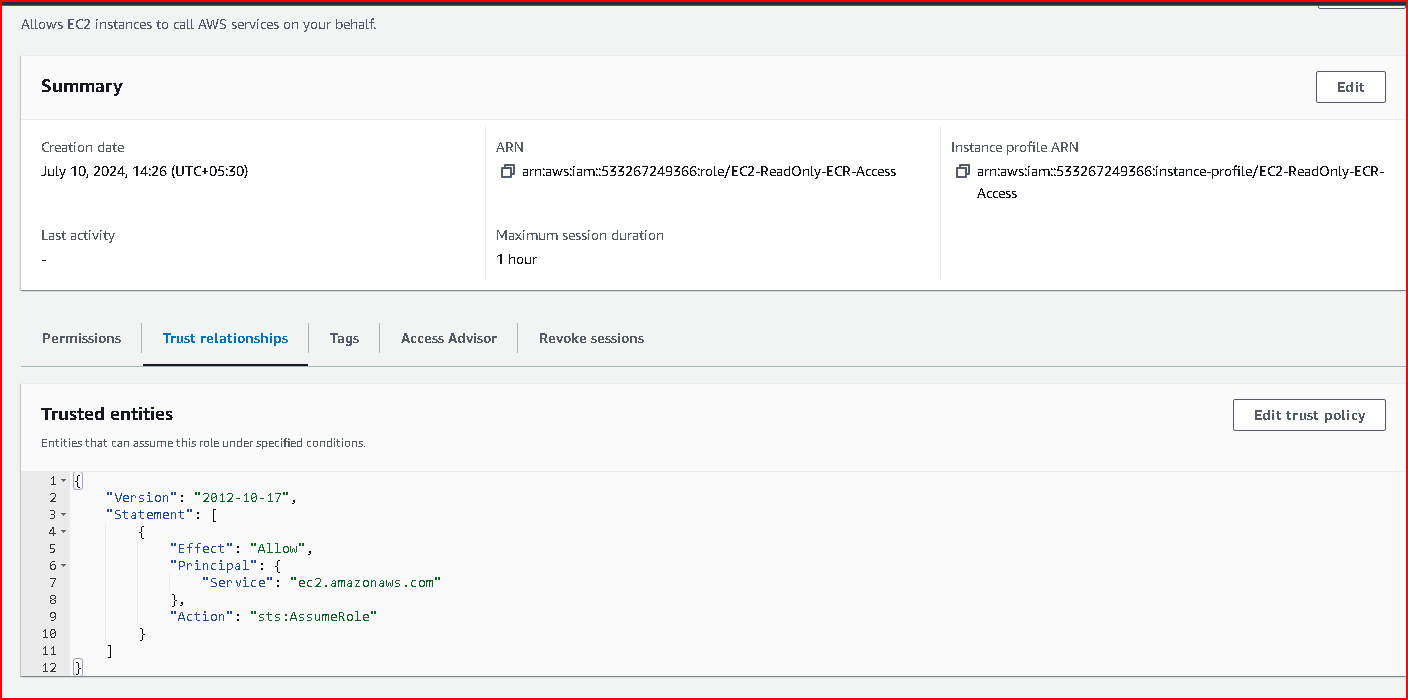
Search for and select the policy you created earlier

Click "Next: Tags" if you need to add tags. Otherwise, click "Next: Review".

4. Review and Create Role:

Provide a name and description for your role (e.g., `EC2-ReadOnly-ECR-Access`).

Click "Create role".



C. Attach Role to EC2 Instance

Finally, attach the IAM role you created to your EC2 instance.

1. Navigate to EC2 Instances:

Go to the [EC2 Console](https://console.aws.amazon.com/ec2/).

2. Select Instance:

Select the instance to which you want to attach the role.

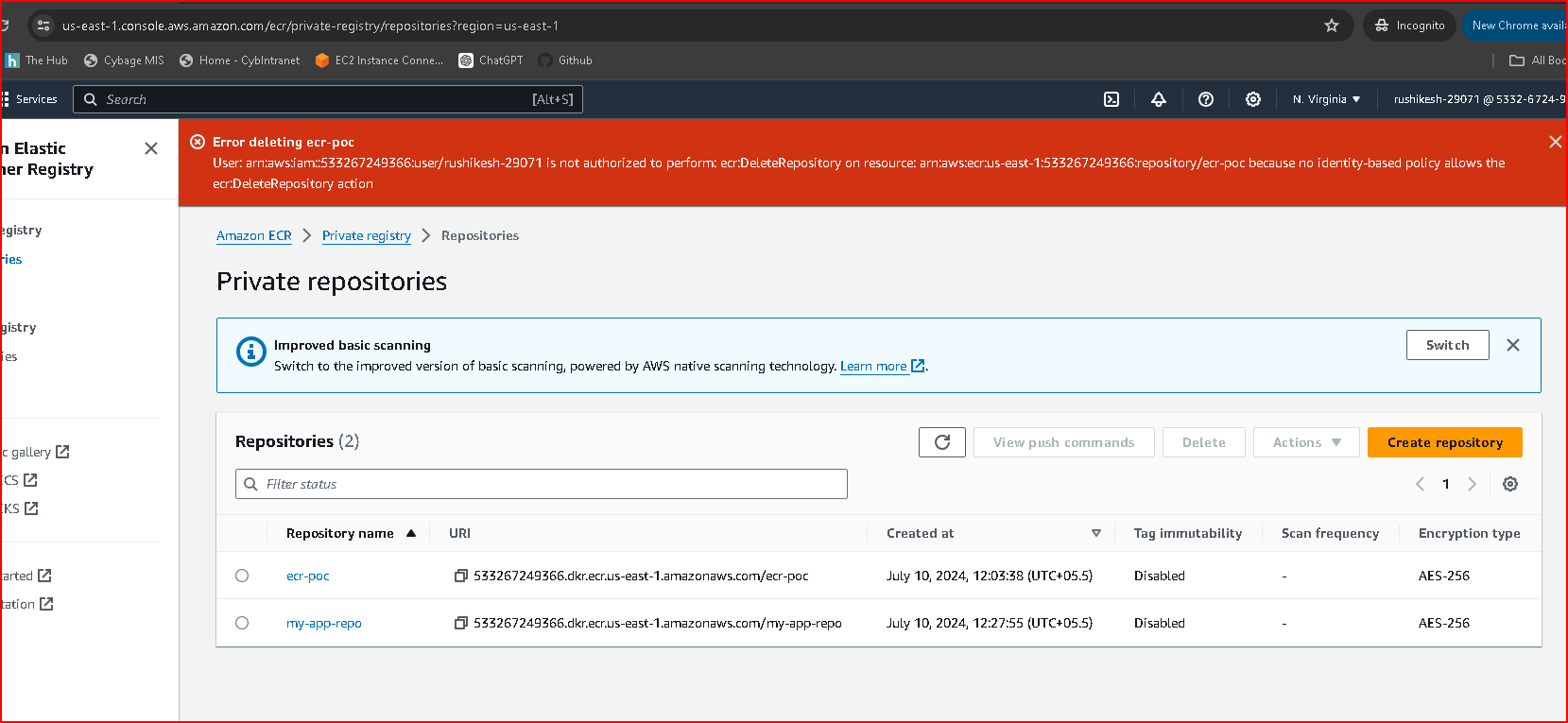
3. Attach IAM Role:

In the instance details pane, click on "Actions" -> "Security" -> "Modify IAM role".

Choose the IAM role you created (e.g., `EC2-ReadOnly-ECR-Access`).

Click "Apply".

We have read only access I cannot delete or edit the ecr repo created in root account.



**j. Assume role for test-user and give read-only access to S3**

Create an IAM Policy for Read-Only Access to S3

Navigate to IAM Policies:

Go to the AWS Management Console.

Search for and click on "IAM" under "Security, Identity, & Compliance".

Create Policy:

Click on "Policies" in the left-hand menu.

Click on "Create policy".

Policy Configuration:

Choose the "JSON" tab.

Review Policy:

Click on "Review policy".

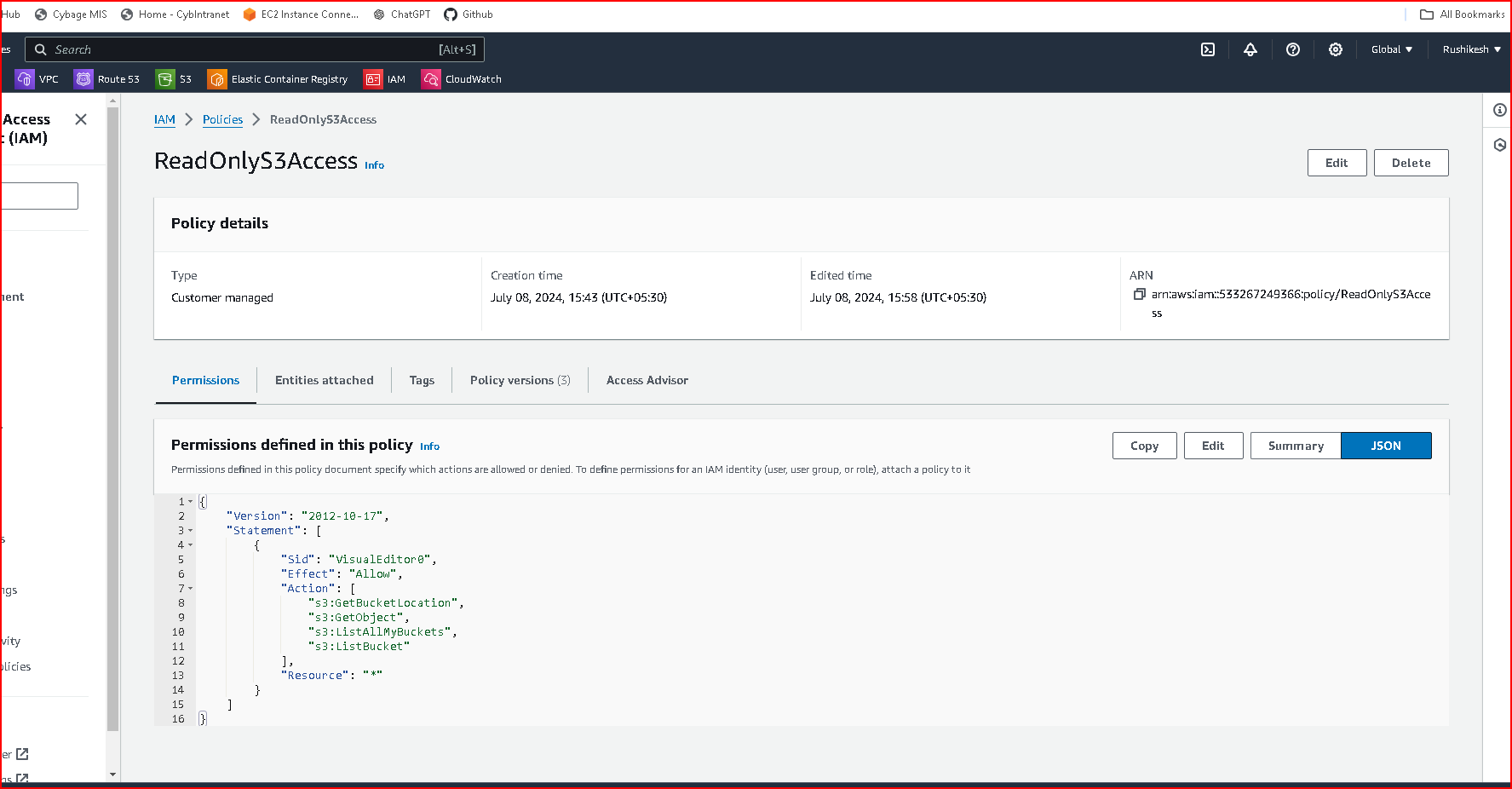
Name your policy (e.g., ReadOnlyS3AccessPolicy).

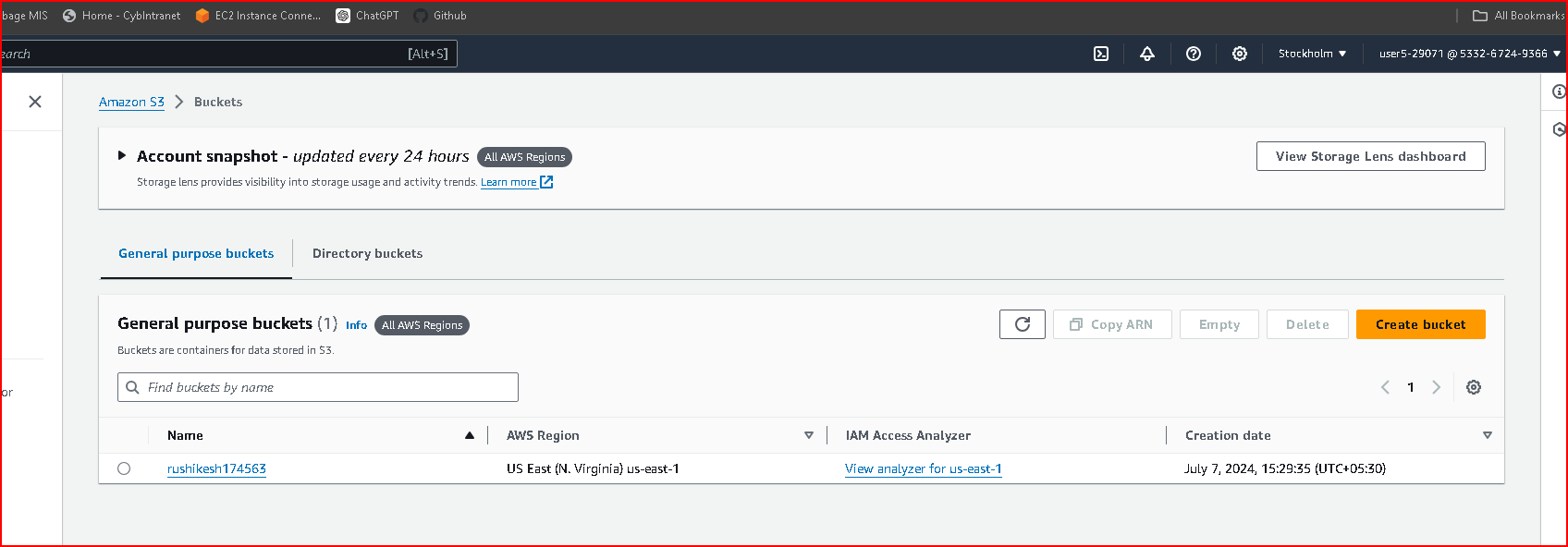
Optionally, provide a description.

Click on "Create policy".

Attach this policy to user5

login using user5 and check the list of buckets





Session has been expired after 1 hour

1. **Write a policy to restrict EC2 instance creation to t2.micro and t2.medium instances**

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: ec2:RunInstances is denied.

Resource: All EC2 instance resources (arn:aws:ec2:\*:\*:instance/\*).

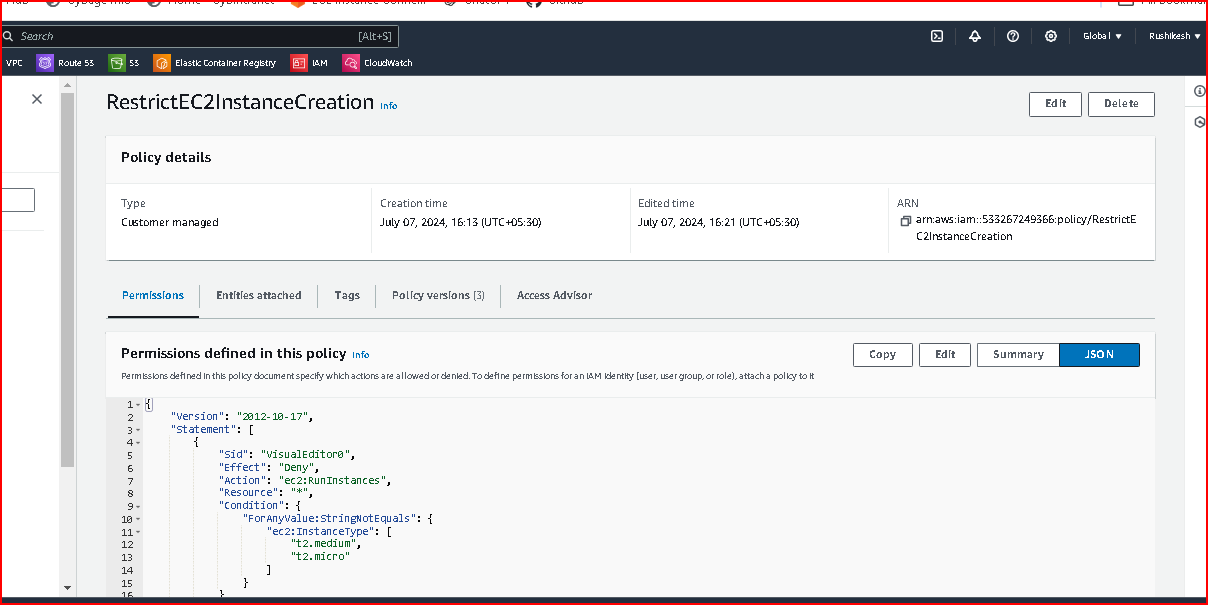
Condition: Allows only t2.micro and t2.medium instance types.

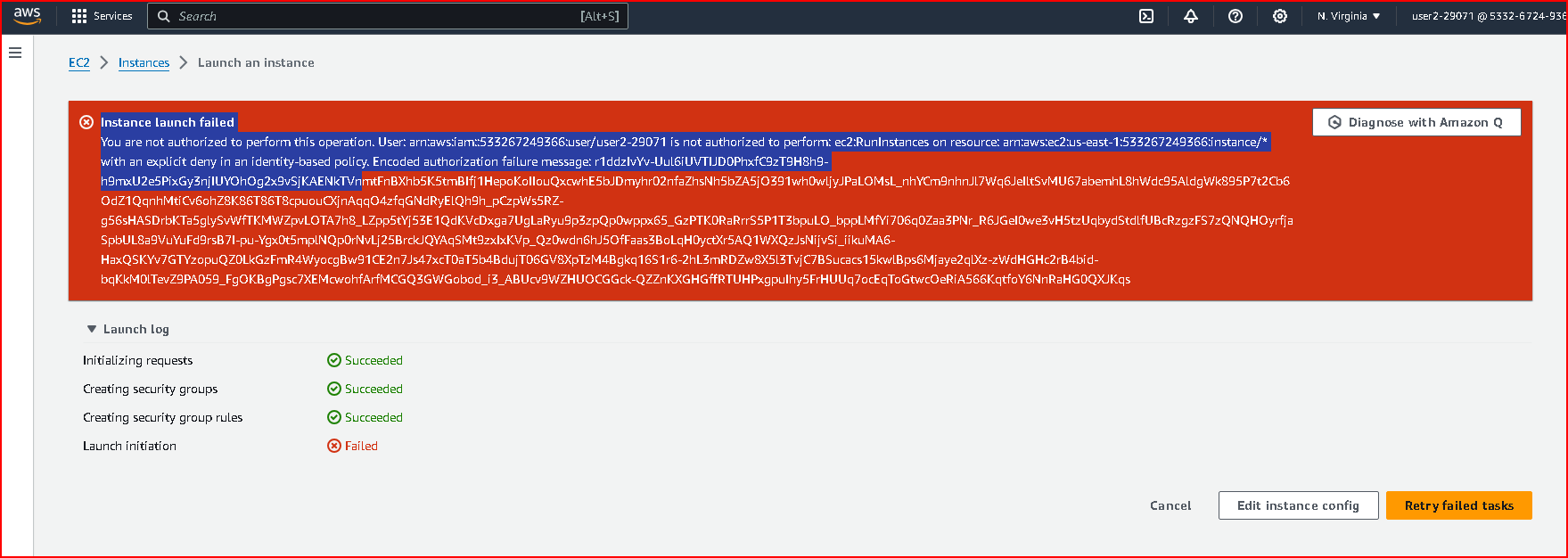
Click on the "Review policy" button.

Provide a name for the policy (e.g., RestrictEC2InstanceCreationToT2MicroAndT2Medium).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.





1. **Write an IAM Policy to Restrict EKS Node Creation to t3.medium Instances**

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: eks:CreateNodegroup is denied.

Resource: All EKS Nodegroup resources (\*).

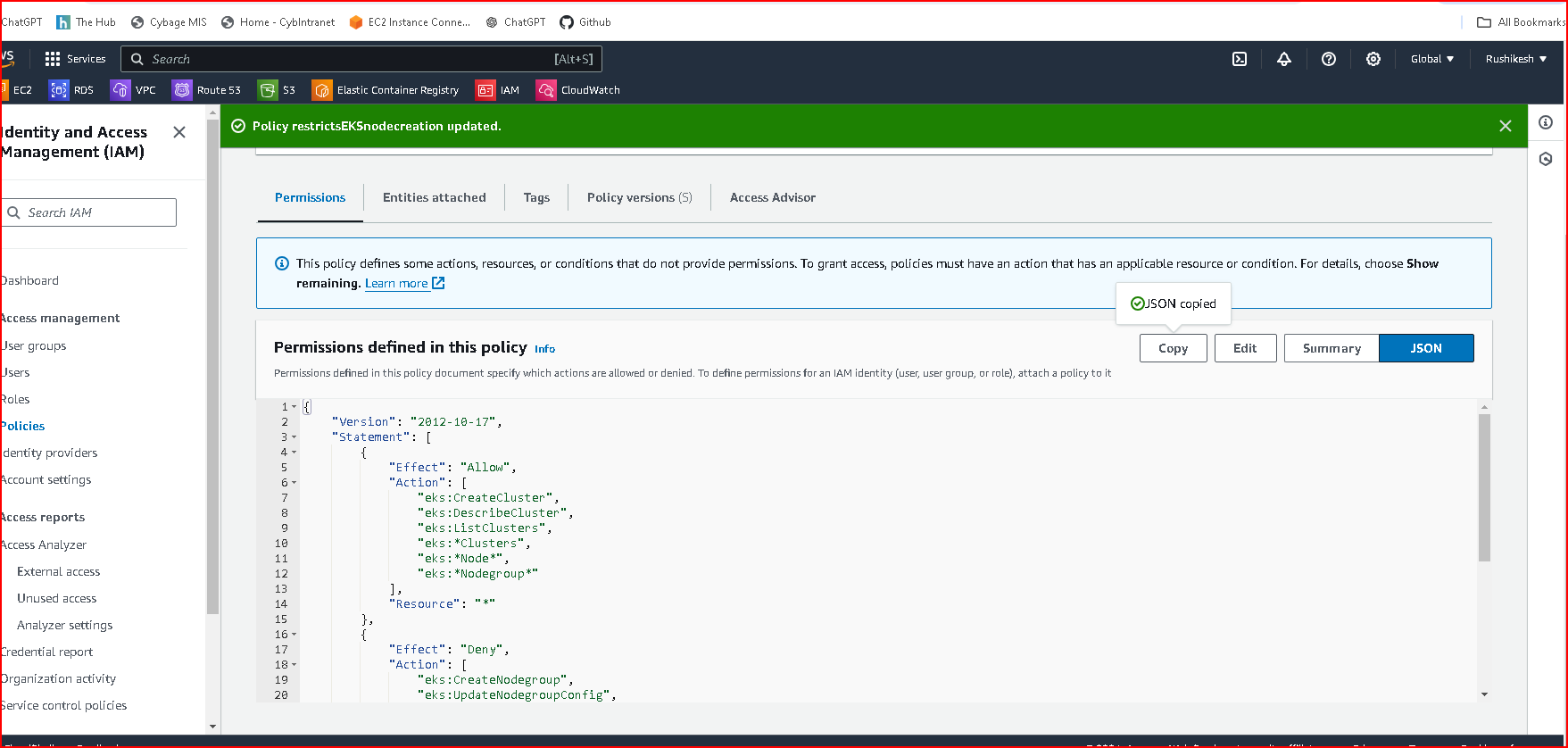
Condition: Allows only t3.medium instance types.

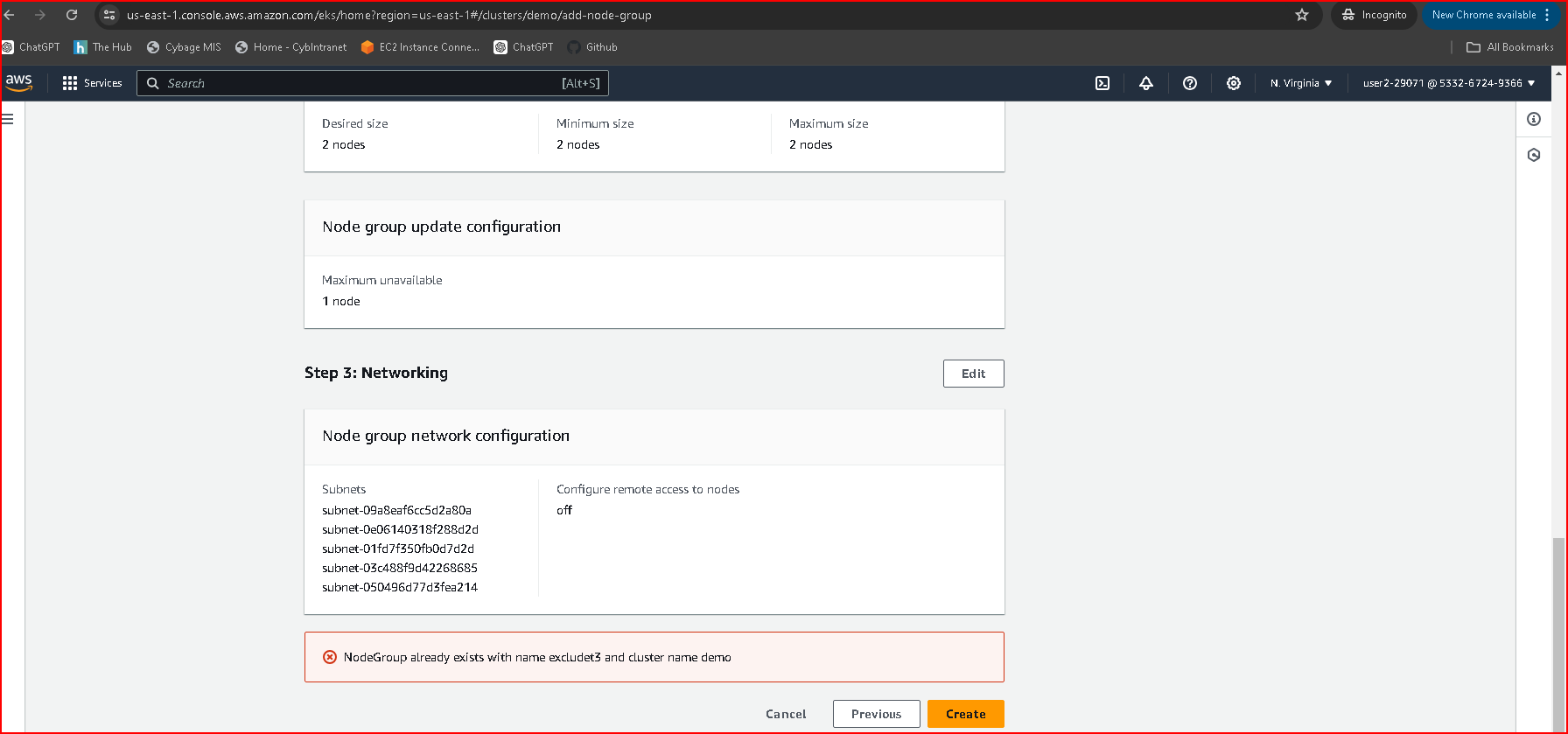
Click on the "Review policy" button.

Provide a name for the policy (e.g., RestrictEKSNodeCreationToT3Medium).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.





1. **Write an IAM Policy to Limit RDS Database Creation to db.t3.micro Instances**

Go to the AWS Management Console and navigate to the IAM service.

In the left sidebar, click on "Policies" and then click on the "Create policy" button.

Select the "visual editor" tab to switch to the visual editor mode.

Action: rds:CreateDBInstance is denied.

Resource: All RDS DB instance resources (\*).

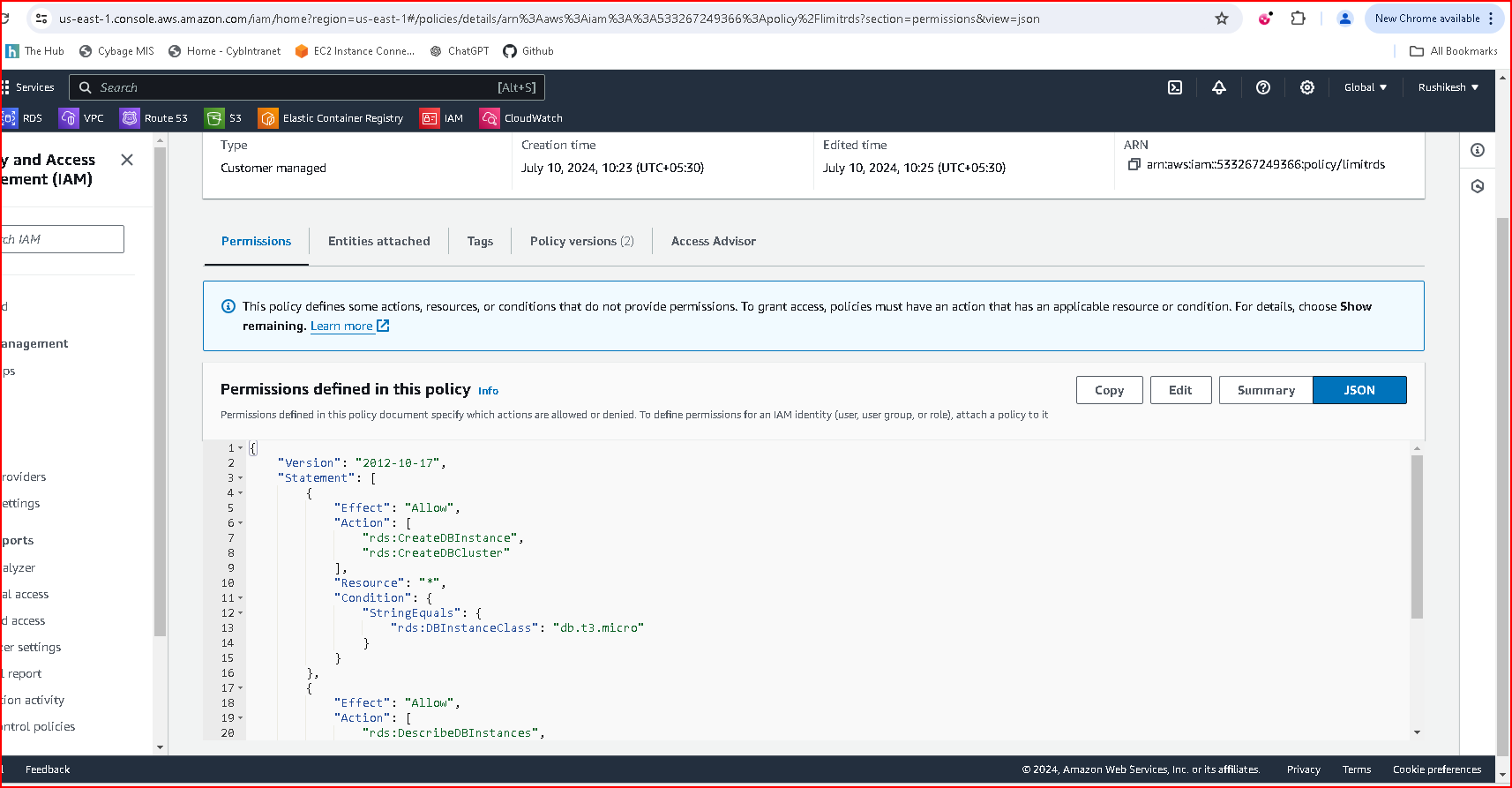
Condition: Allows only db.t3.micro database classes.

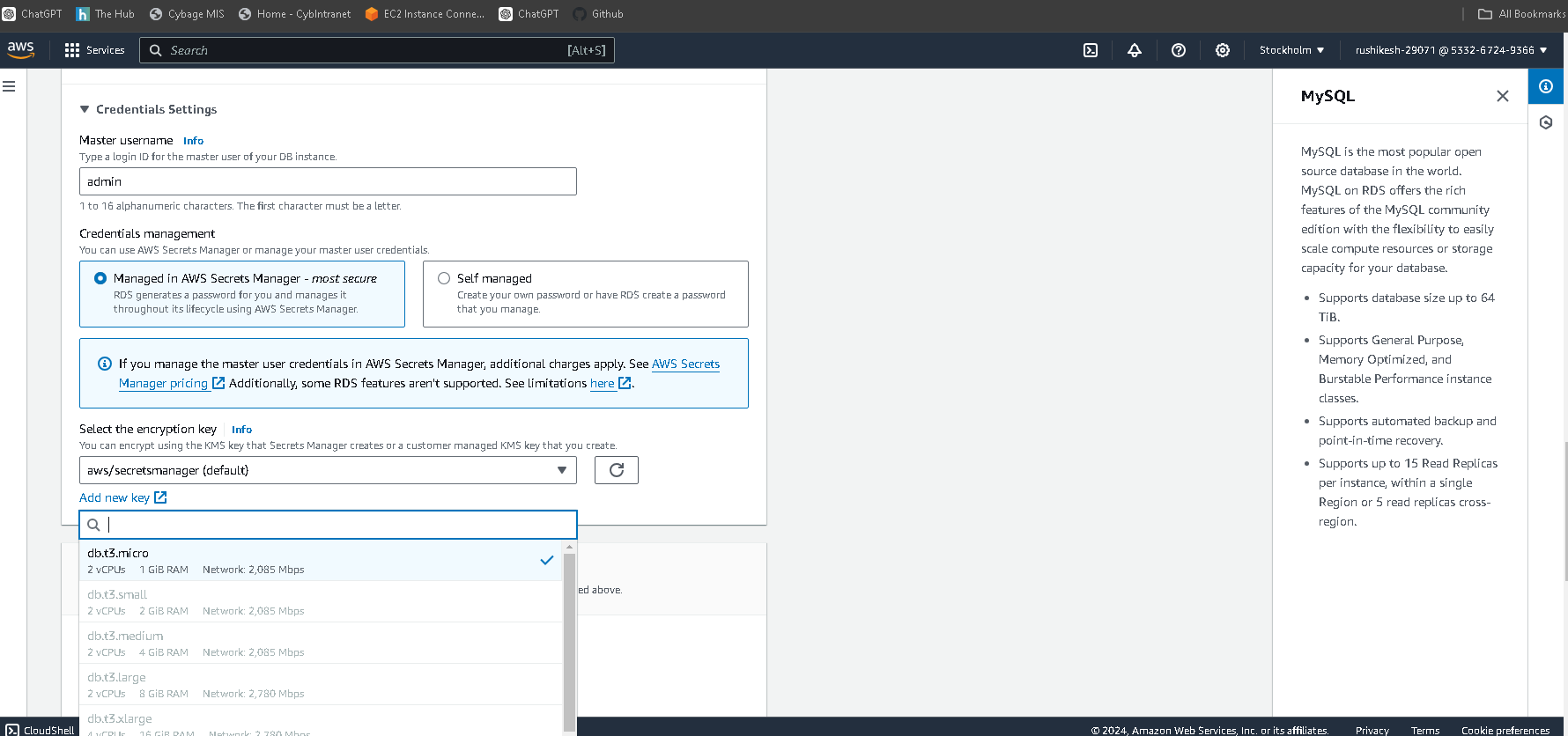
Click on the "Review policy" button.

Provide a name for the policy (e.g., LimitRDSDatabaseCreationToDbT3Micro).

Optionally, you can provide a description for the policy.

Click on the "Create policy" button to save the policy.





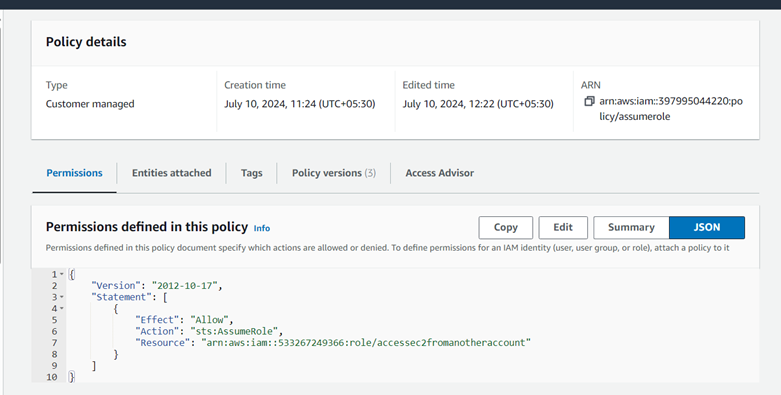
**4. Write IAM Policies for accessing EC2 instance from another account.(AssumeRole - cross account)**

Create an IAM Policy:

Click on Policies in the left navigation pane.

Click Create policy.

Choose the visual editor and enter a policy that allows assuming the role (accessEc2FromAnotherAccount) in your AWS account:



Attach the IAM Policy to the karan1\_29221 IAM User:

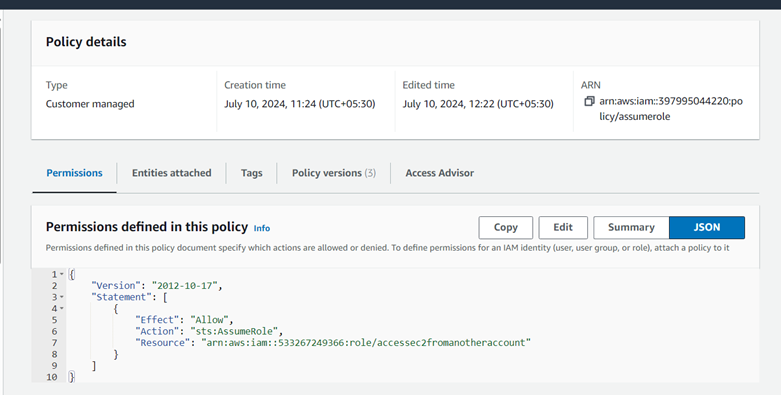
Navigate to Users in the IAM console.

Click on the karan1\_29221 user to view its details.

Click on the Add permissions button or Attach policies.

Search for and select the IAM policy you just created.

Click Attach policy to attach the policy to the karan1\_29221 IAM user.



Sign in as karan1\_29221:

Sign in to the AWS Management Console using the credentials of the karan1\_29221 IAM user.

Switch Roles:

Navigate to the IAM console: https://console.aws.amazon.com/iam/

Click on Roles in the left navigation pane.

Search for and click on the accessEc2FromAnotherAccount role.

Click Switch Role.

Enter your AWS account ID and the ARN of the role (accessEc2FromAnotherAccount) in your AWS account.

Click Switch Role.