IAM Policies Assignment

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

First open the IAM POLICES

CREATE NEW [POLICES]
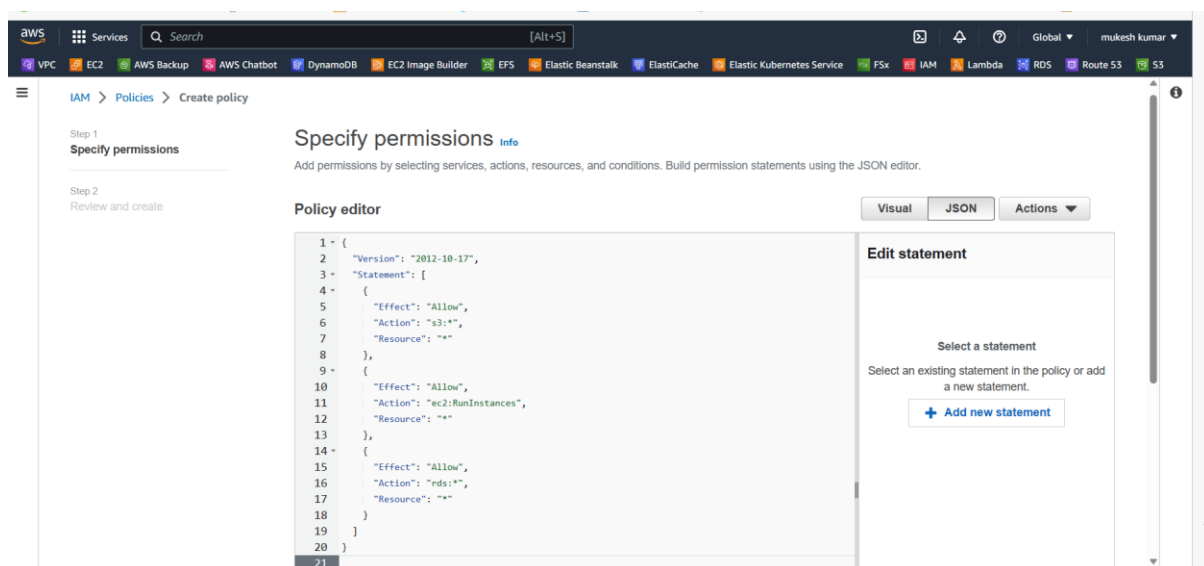
NEXT

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

policy1

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - optional
Add a short explanation for this policy.

new police

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info   Edit

Permissions in the policy document specify which actions are allowed or denied.

Q Search

THEN

NEXT

aws   Services   Q Search   [Alt+S]   Global ▼   mukesh kuma

Q Search

Allow (3 of 380 services)   Show remaining 377 services

Service ▽	Access level ▽	Resource	Request condition
RDS	Full access	All resources	None
S3	Full access	All resources	None
EC2	Limited: Write	All resources	None

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

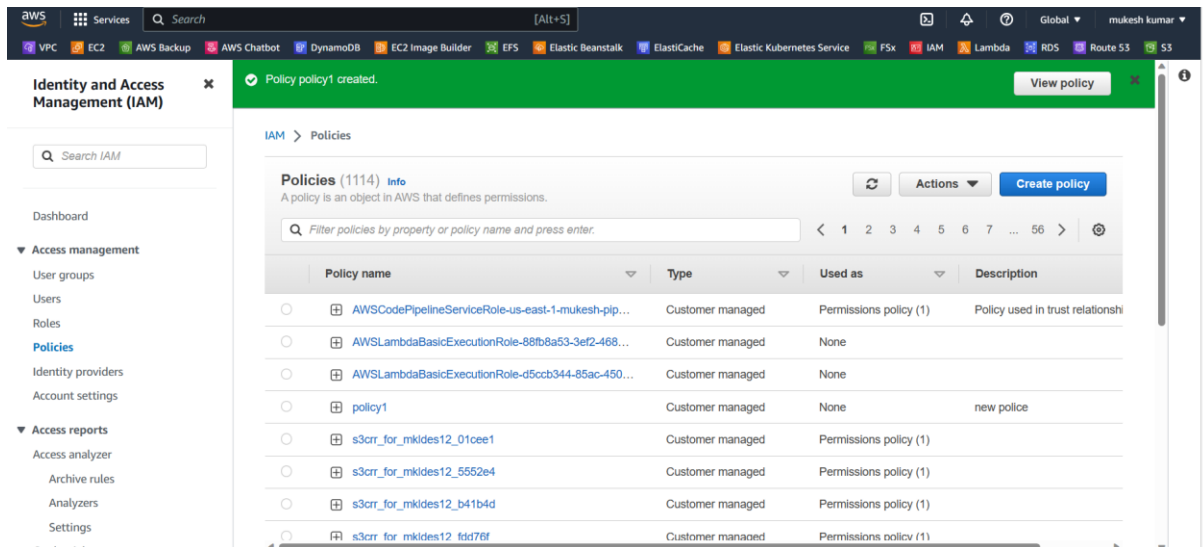No tags associated with the resource.

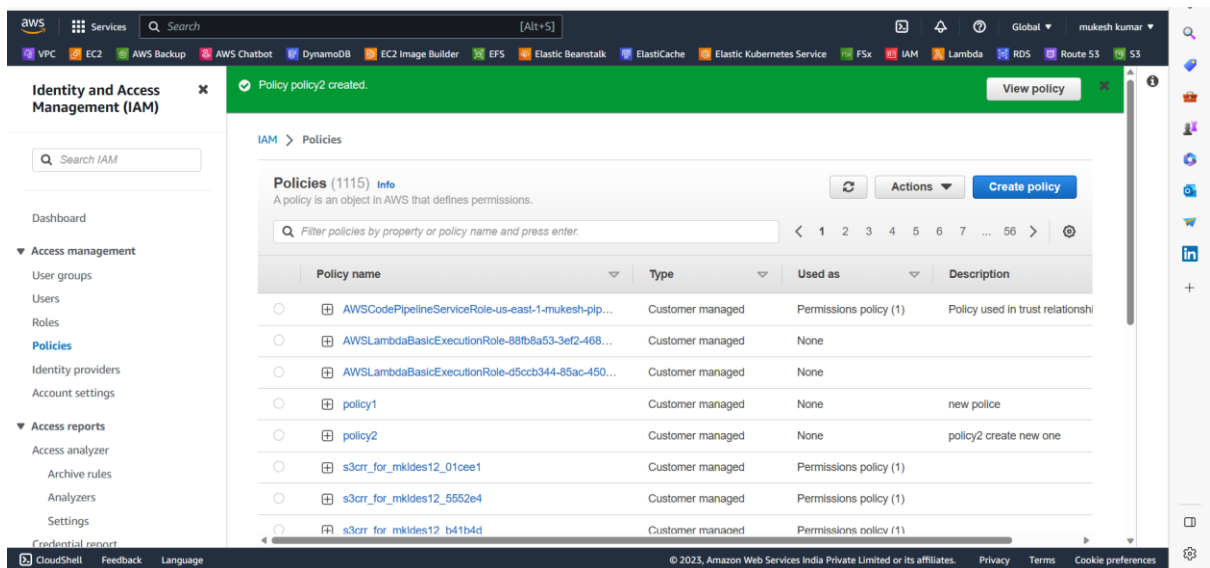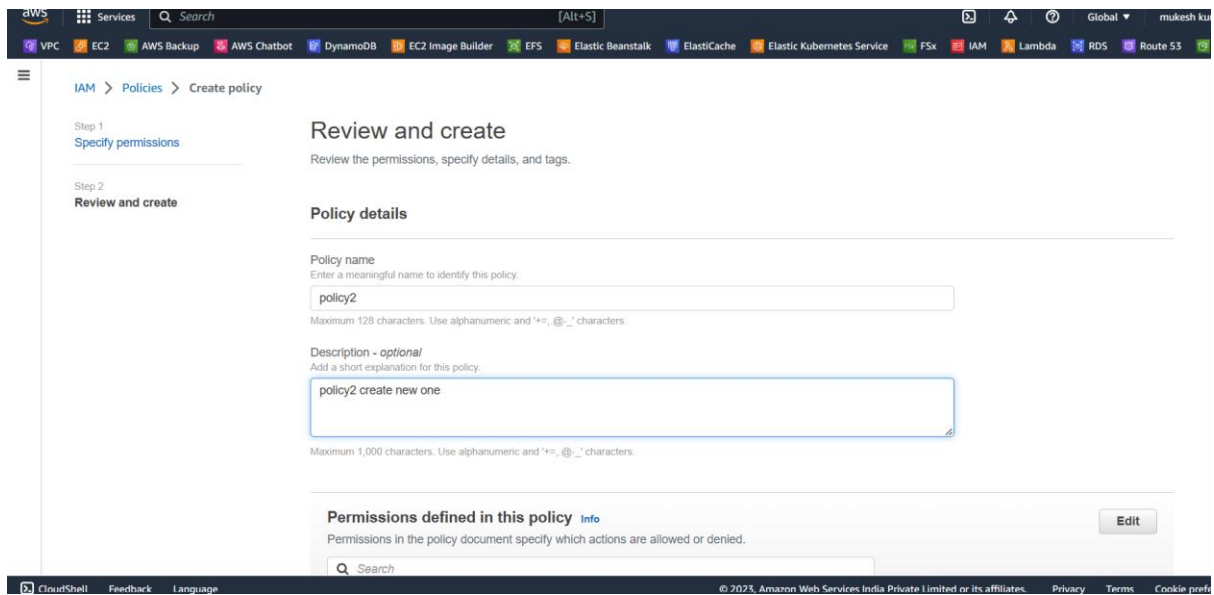Add tag

You can add up to 50 more tags.

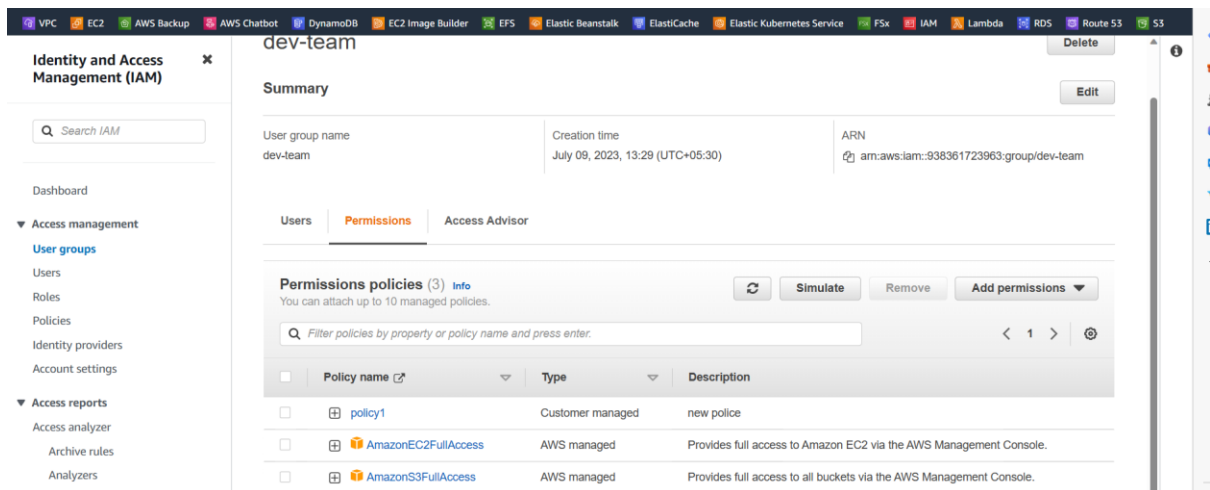Cancel   Previous   Create policy

CREATE IT

AGAIN CREATE Again policy 2

U can see policy 1 and policy 2

Devteam create policy1

Ops team add policy2

U can attach the police in every group

Complete assignment