Name: Mayur Dhotre

Batch: B33

<u>IAM Service:-</u> (Identity And Access Management)

Four main components:-

1. **Users :-** IAM users in AWS are used to represent individuals, applications, or services that need to interact with AWS resources.

2. **User Groups :-** It consists the collection of IAM users.

3. **Policies:-** IAM policies are JSON documents that define permissions. Policies can be attached to users, groups, or roles to grant or deny access to AWS resources. They specify what actions are allowed or denied and which resources those actions can be performed on.

4. **Roles:-** IAM roles are similar to users but are not associated with a specific person. Roles are meant to be assumed by entities such as AWS services, applications, or other AWS accounts. Roles define a set of permissions, and when a role is assumed, it temporarily inherits those permissions.

What is ARNs:- (Amazon Resource Name)

It is a identifier that is used in Amazon Web Services (AWS) to uniquely identify and name AWS resources. ARNs are used across various AWS services to specify resources, such as EC2 instances, S3 buckets, Lambda functions, and more.

ARN FORMATE:- arn:partition:service:region:account-id:resource

EXAMPLE:- arn:aws:s3:::my-bucket-name

arn: This is a constant that indicates it's an Amazon Resource Name.

partition: Represents the partition in which the resource is located (e.g., aws, aws-cn, or aws-us-gov).

service: Specifies the service that manages the resource (e.g., s3, ec2, lambda).
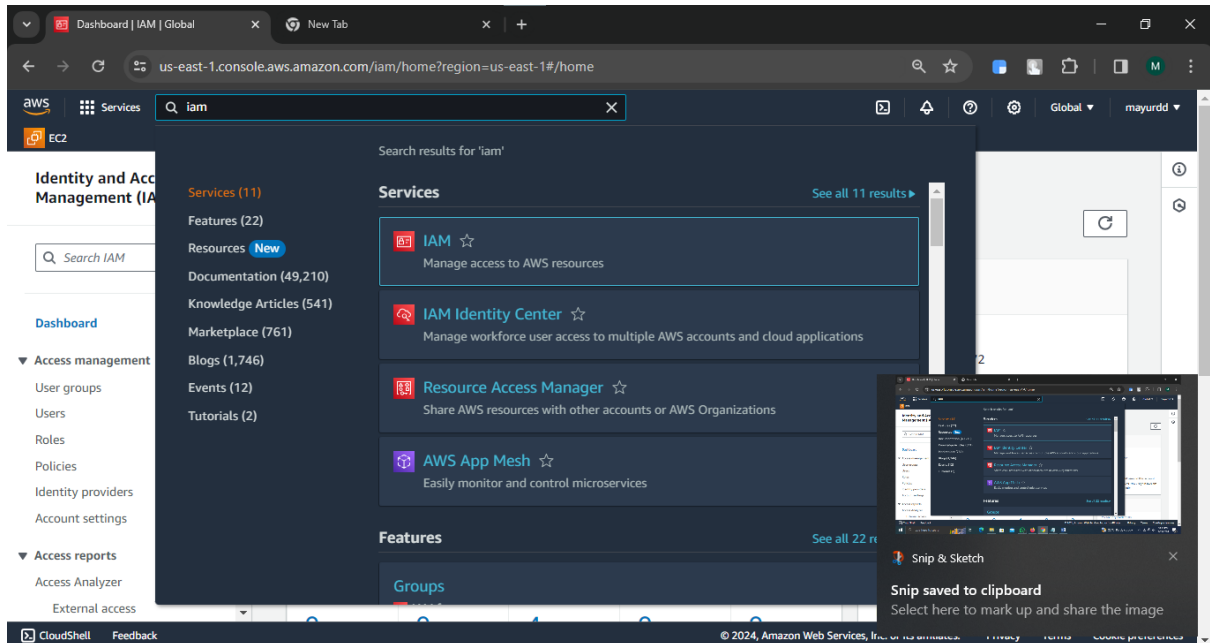
region: Specifies the AWS region where the resource is located. This part is optional and may be omitted for some global services or resources.

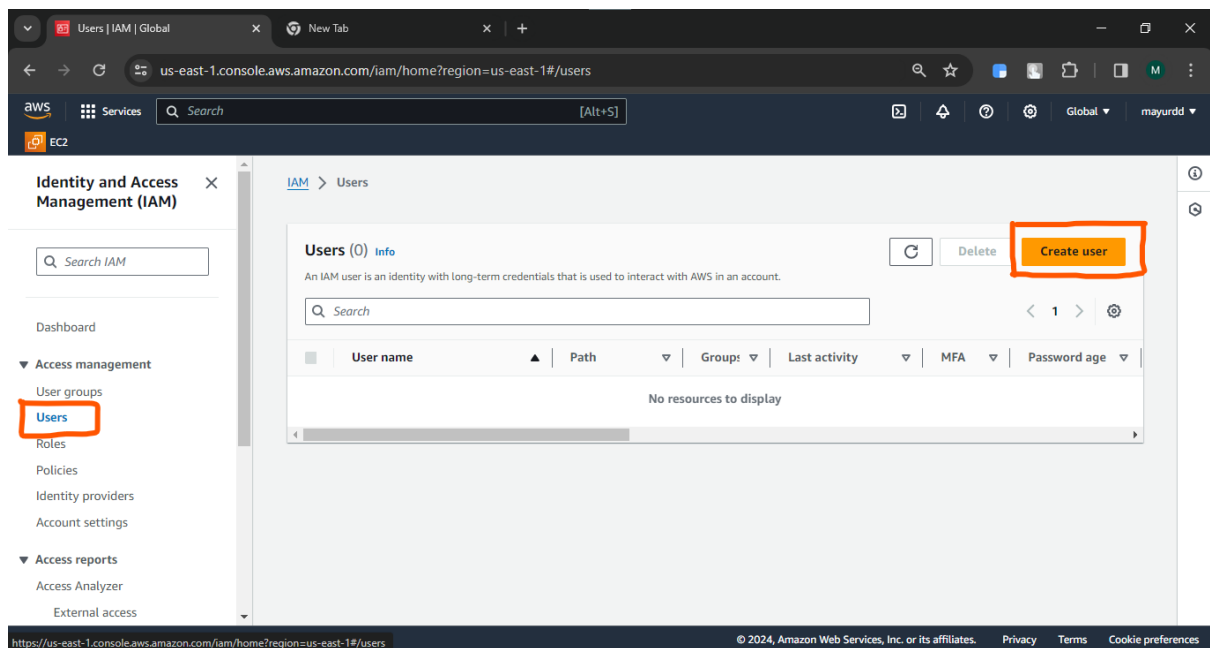account-id: Represents the AWS account ID that owns the resource.

resource: Specifies the specific resource within the service.

❖ Creating A user :-

1. Search IAM service and click on it.

2. Click on **users** option and **Create user** option

3. Specify the username as per your choice

Specify user details

User details

User name

mayur-temp

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

4. Click on the checkbox (It provide the AWS console to the user) , And also click on **I want to create user**

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice ☑ to manage their access in IAM Identity Center.

ⓘ **Are you providing console access to a person?**

User type

◯ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

◉ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

5. Create a password and click on next

Console password
◉ Autogenerated password
You can view the password after you create the user.

◯ Custom password
Enter a custom password for the user.

- Must be at least 10 characters long
- Must include at least one uppercase letter (A-Z)
- Must include at least one lowercase letter (a-z)
- Must include at least one number (0-9)
- Must include at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

☐ Show password

☐ Users must create a new password at next sign-in - Recommended

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more ☑

Cancel   **Next**

6. Assign the permissions as per your requirement

Permissions options

◉ **Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ **Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (3)

[Create group]

Q Search

< 1 >

	Group name ↗ ▲	Users ▽	Attached policies ↗ ▽	Created ▽
☐	developer	2	AmazonEC2FullAccess	2024-02-22 (14 hours ago)
☐	HR	1	AmazonVPCFullAccess	2024-02-22 (14 hours ago)
☐	tester	1	AmazonRDSFullAccess	2024-02-22 (14 hours ago)

▶ **Set permissions boundary - optional**

Cancel   Previous   Next

7. Review and create (summary of your user details)

Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
mayur-temp	Autogenerated	No

Permissions summary

< 1 >

Name ↗ ▲	Type ▽	Used as ▽
	No resources	

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag]
You can add up to 50 more tags.

Cancel   Previous   Create user

8. User is created (download the **.csv** file which consist the username and password and user id)

❖ Creating a group And assigining Aws policy:-

1. Click on **user group** and **create group** in IAM Service Dashboard
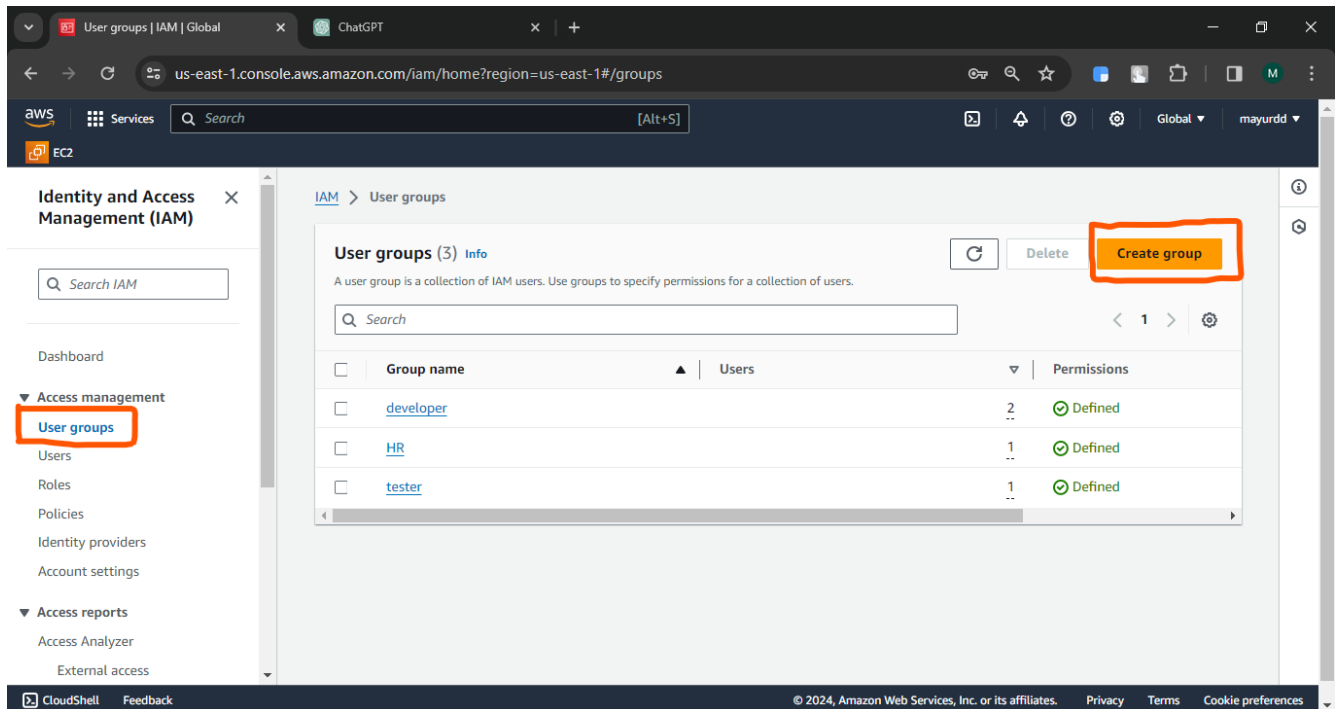
2. Assign a group name as per your choice

3. Add existing user to group (optional)

4. Attach policies As per your requirement and click on **Create group**

5. Group created successfully

❖ Adding user into group :-

1. Select a group (in our case group1)
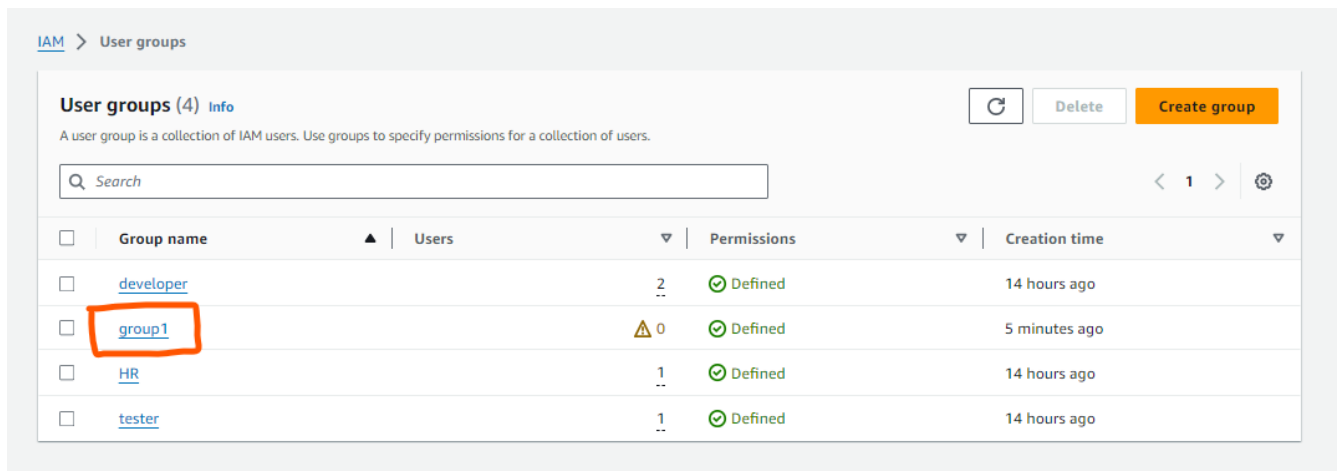
2. Click on **Add user** option
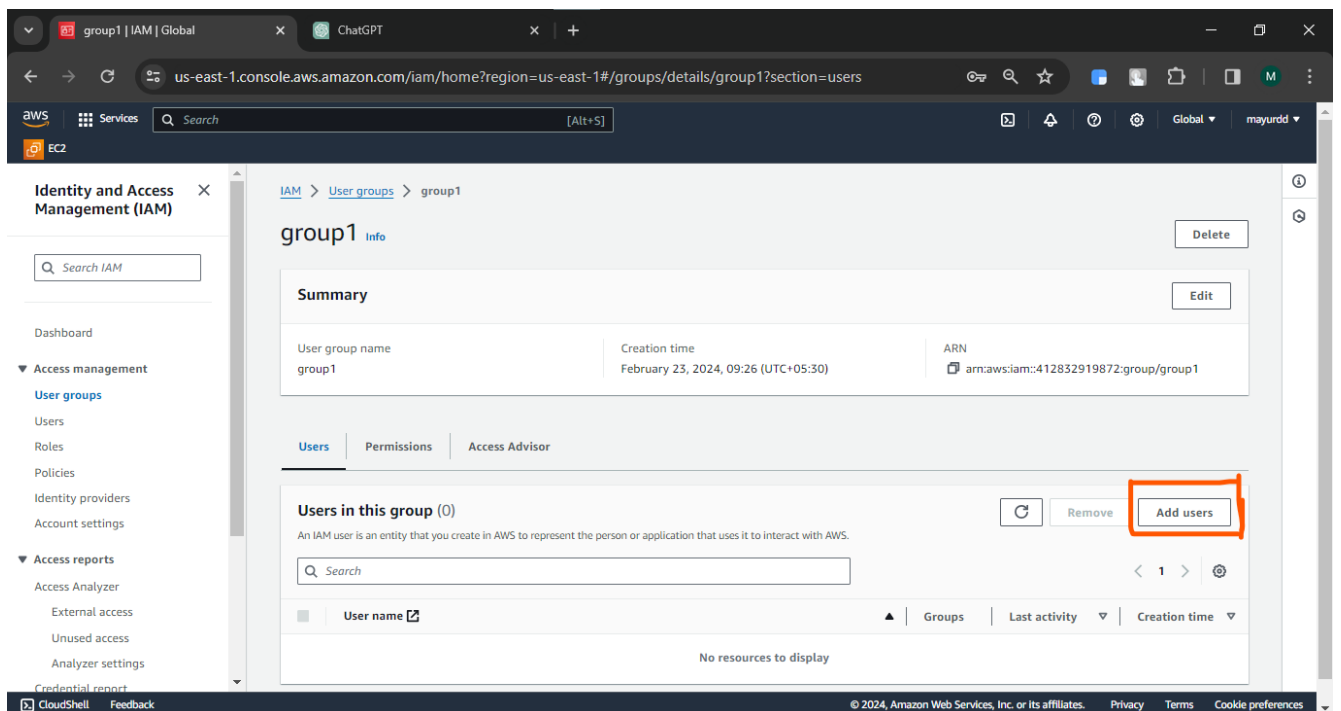
3. Select any user you want to add and click on **Add user** option
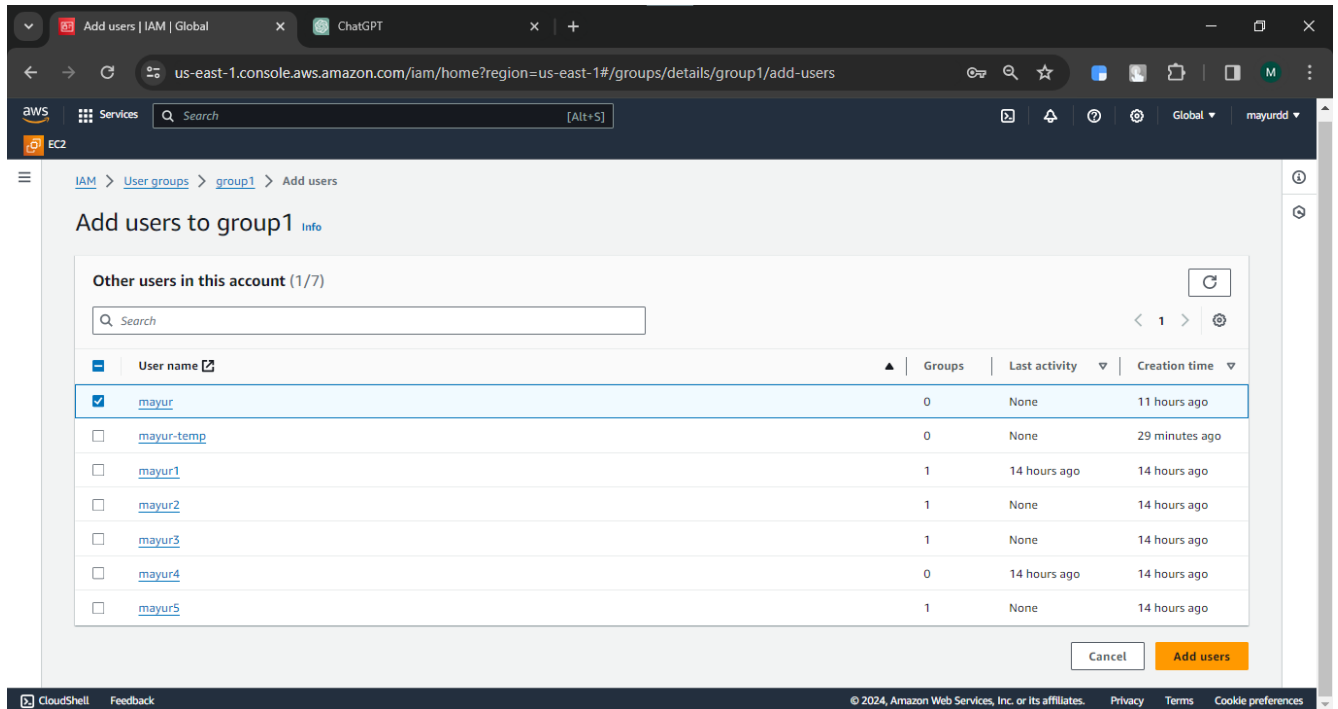
4. User added successfully
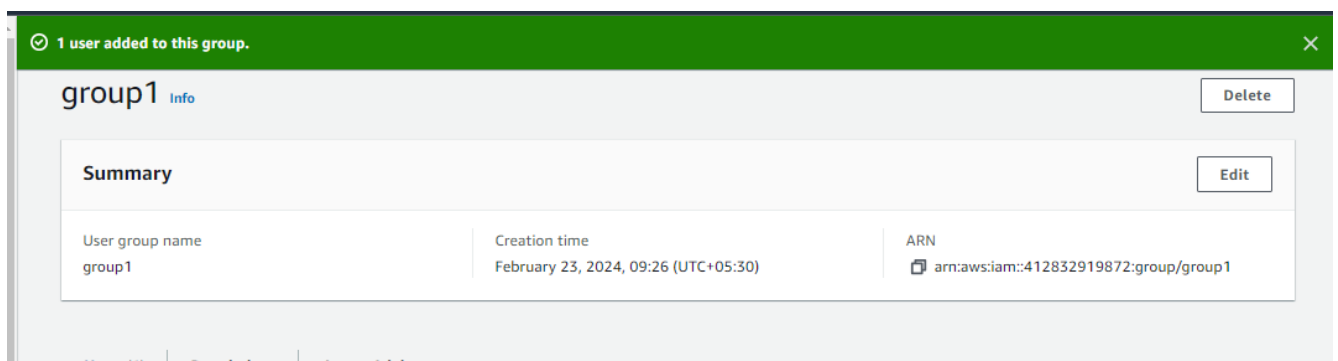
- **Creating custom policy :-**

1. Click on **Policies** and **Create policy** option.
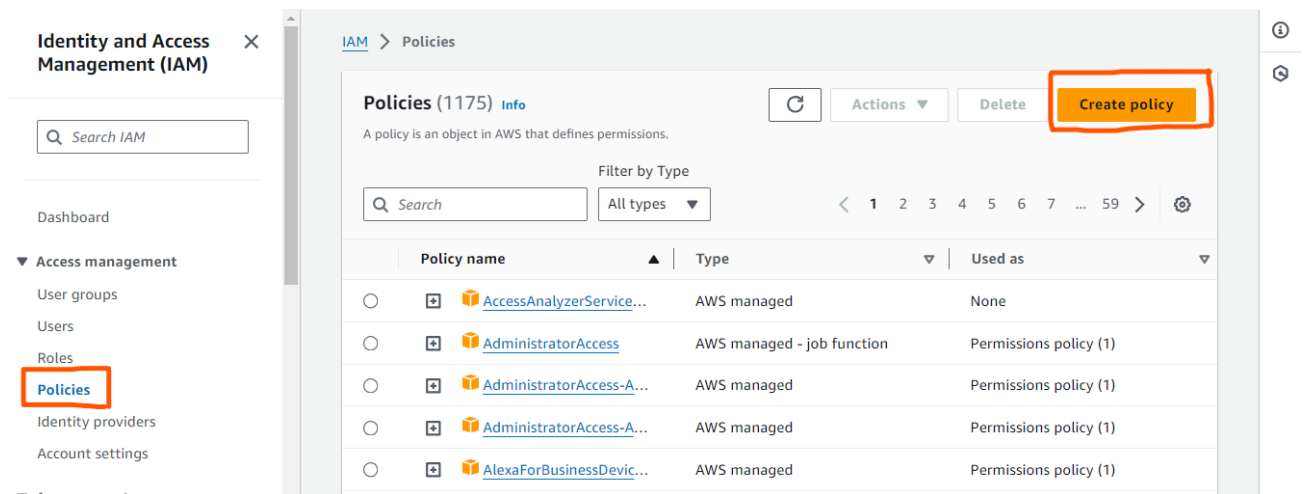
2. Select a service
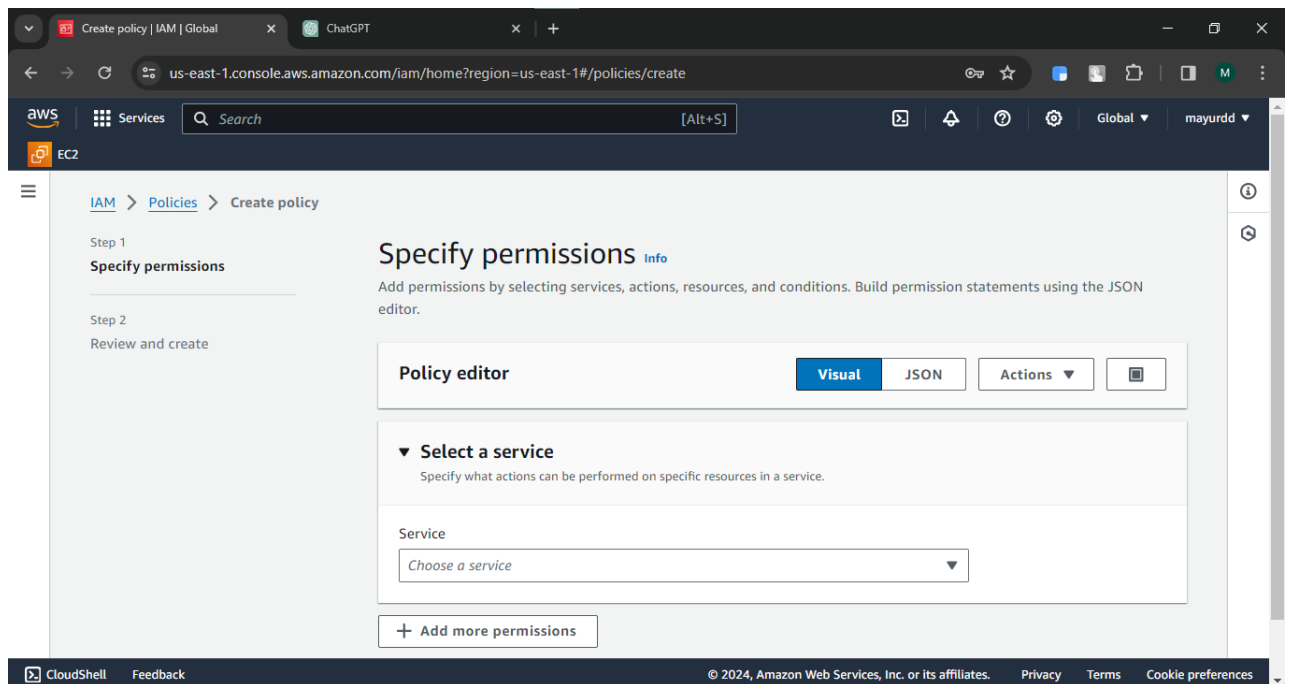
3. Select the permissions or the actions you want to allow
   (in this case only list and read permission is given)
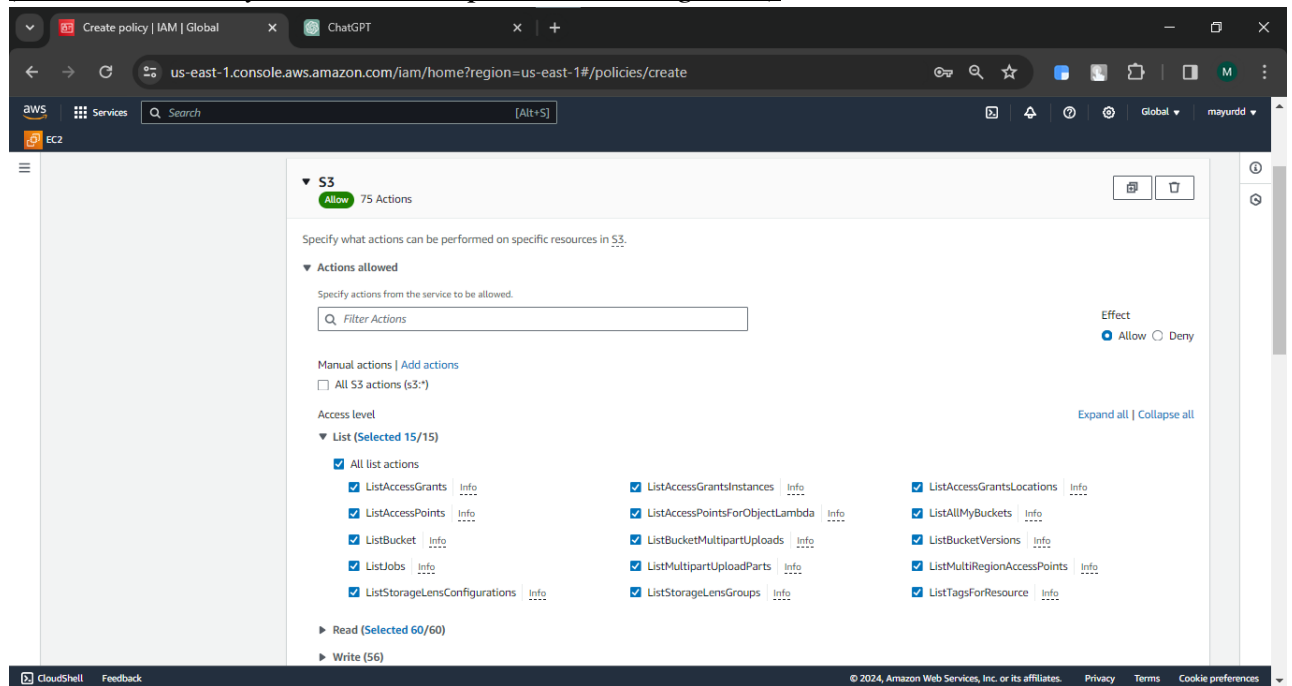
4. Click on Add ARNs option.
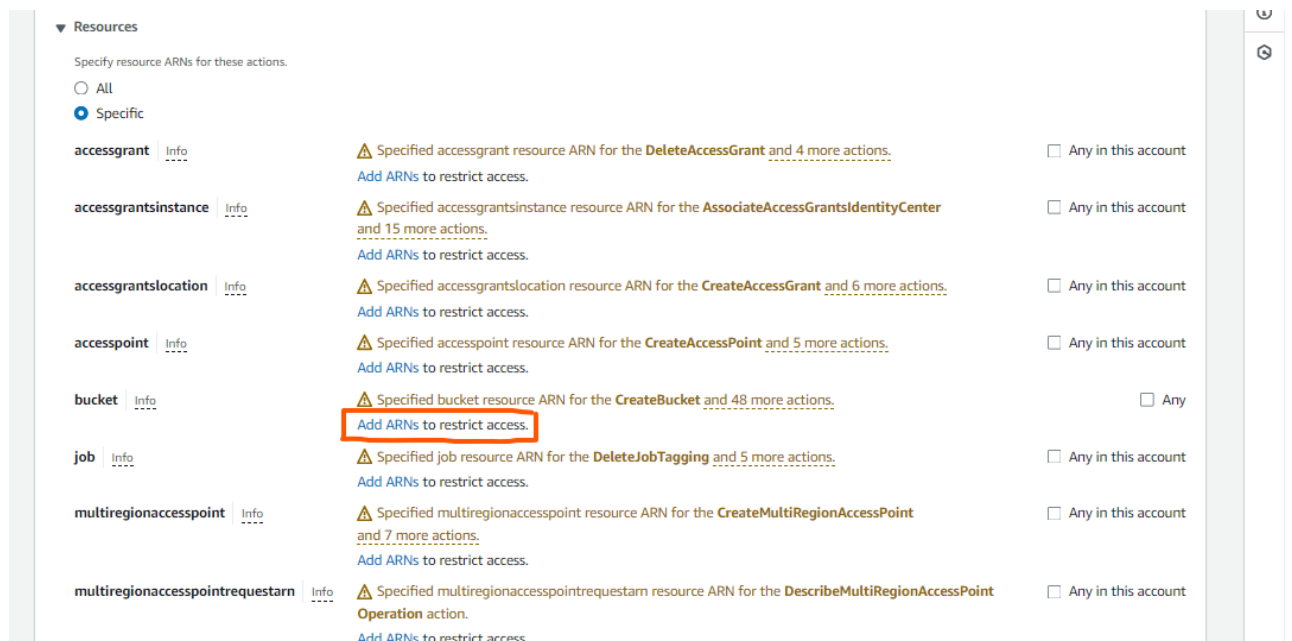
Note:- we can select ALL option also but Allowing specific ARNs for specific service resources can improve security.

5. Select the bucket name and click on **Add ARNs** button

6. Click on next

7. Assign policy name and give description (description is optional)

8. Click on create policy
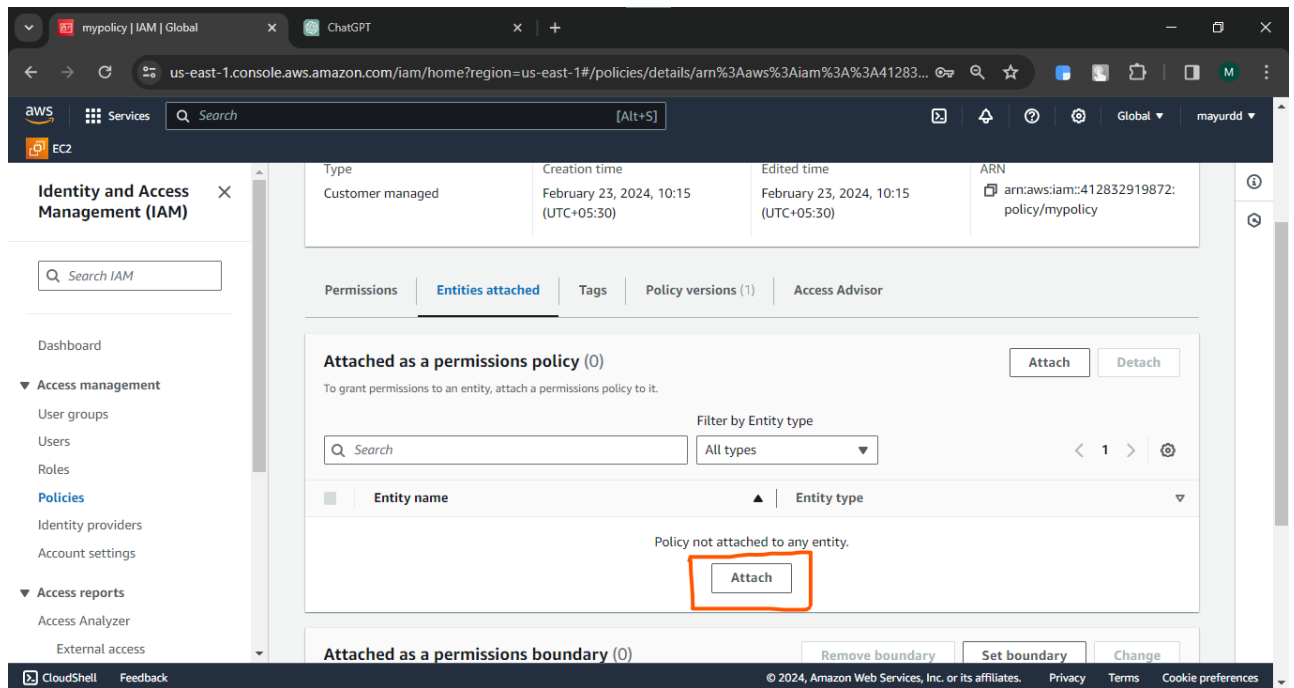
9. Policy Created successfully
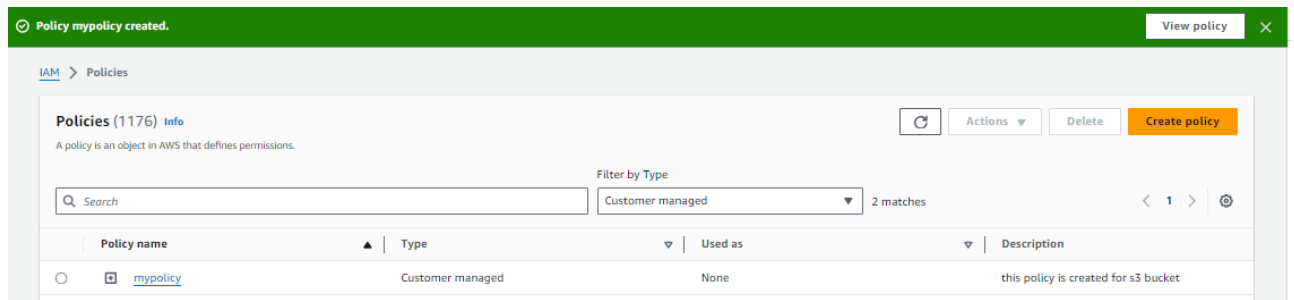
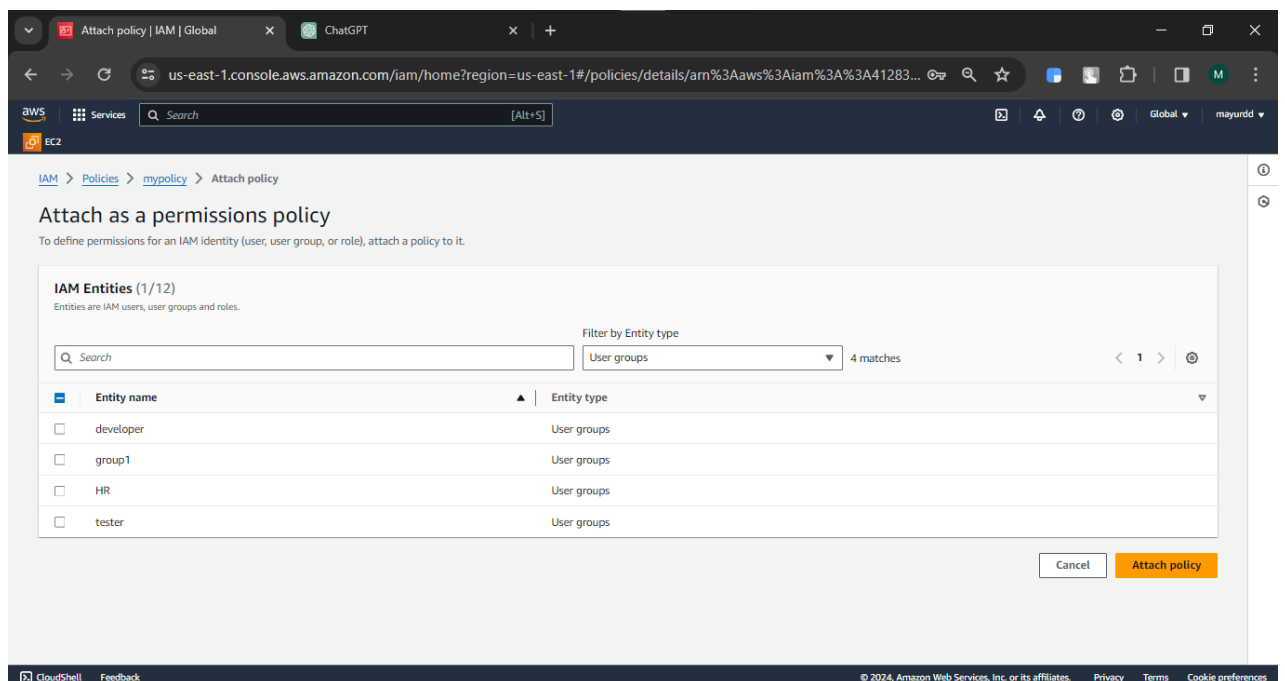- **Assigning custom policy to group and user :-**

1. Select the policy
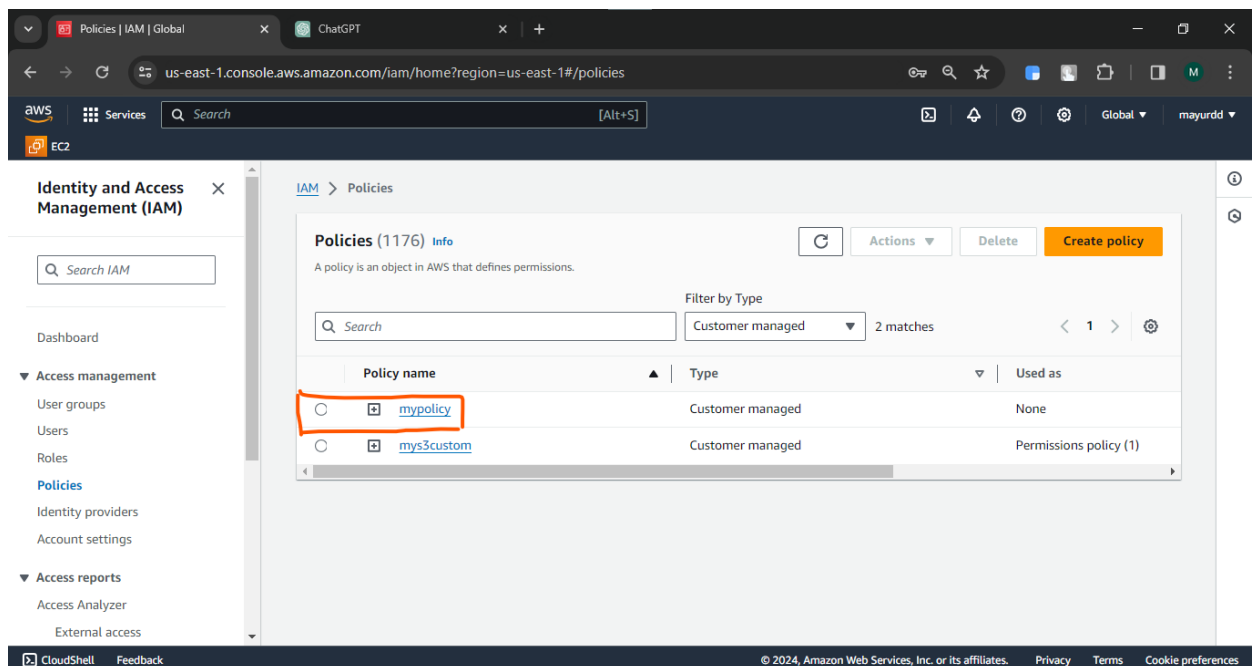
2. Click on **Entities attached** option and click on **Attach** button

3. Select the entity (user , group, and roles) you want to attach and click on **attach policy**

4. Policy attached successfully