

IAM Service:- (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`

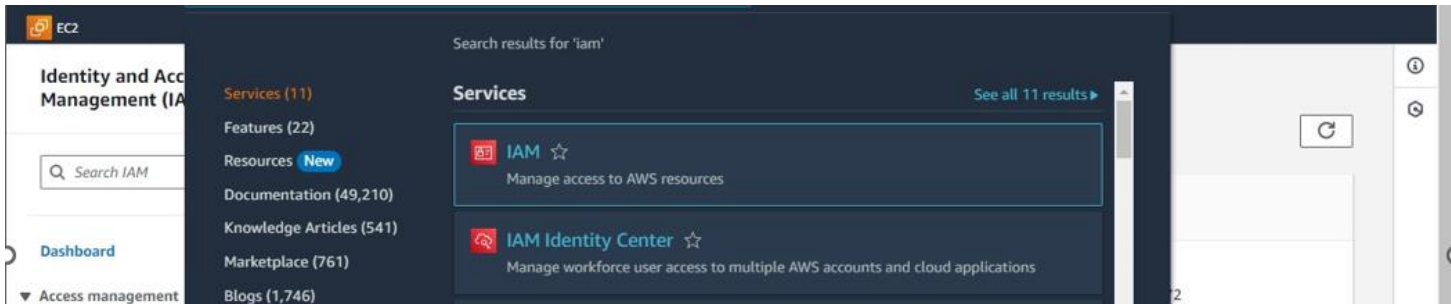
EXAMPLE:- `arn:aws:s3::my-bucket-name` `arn:` This is a constant that indicates it's an Amazon Resource Name.

`partition:` Represents the partition in which the resource is located (e.g., `aws`, `aws-cn`, or `awsus-gov`). `service:` Specifies the service that manages the resource (e.g., `s3`, `ec2`, `lambda`).

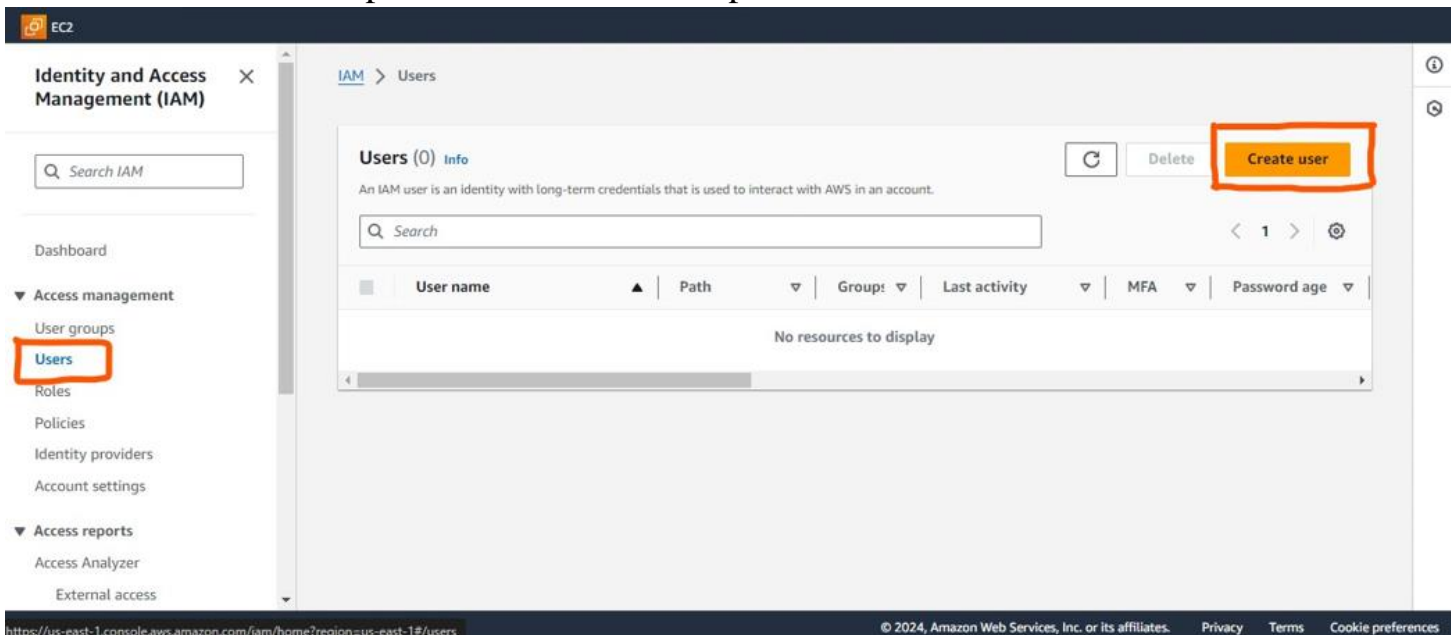
`region:` Specifies the AWS region where the resource is located. This part is optional and may be omitted for some global services or resources. `account-id:` Represents the AWS account ID that owns the resource. `resource:` Specifies the specific resource within the service.

❖ 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

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


Specify user details

User details

User name

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

☒ 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)

Search

< 1 >

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	developer	2	AmazonEC2FullAccess	2024-02-22 (14 hours ago)
<input type="checkbox"/>	HR	1	AmazonVPCFullAccess	2024-02-22 (14 hours ago)
<input type="checkbox"/>	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
mayur-temp

Console password type
Autogenerated

Require password reset
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)

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL
https://412832919872.signin.aws.amazon.com/console

User name
mayur-temp

Console password
***** Show

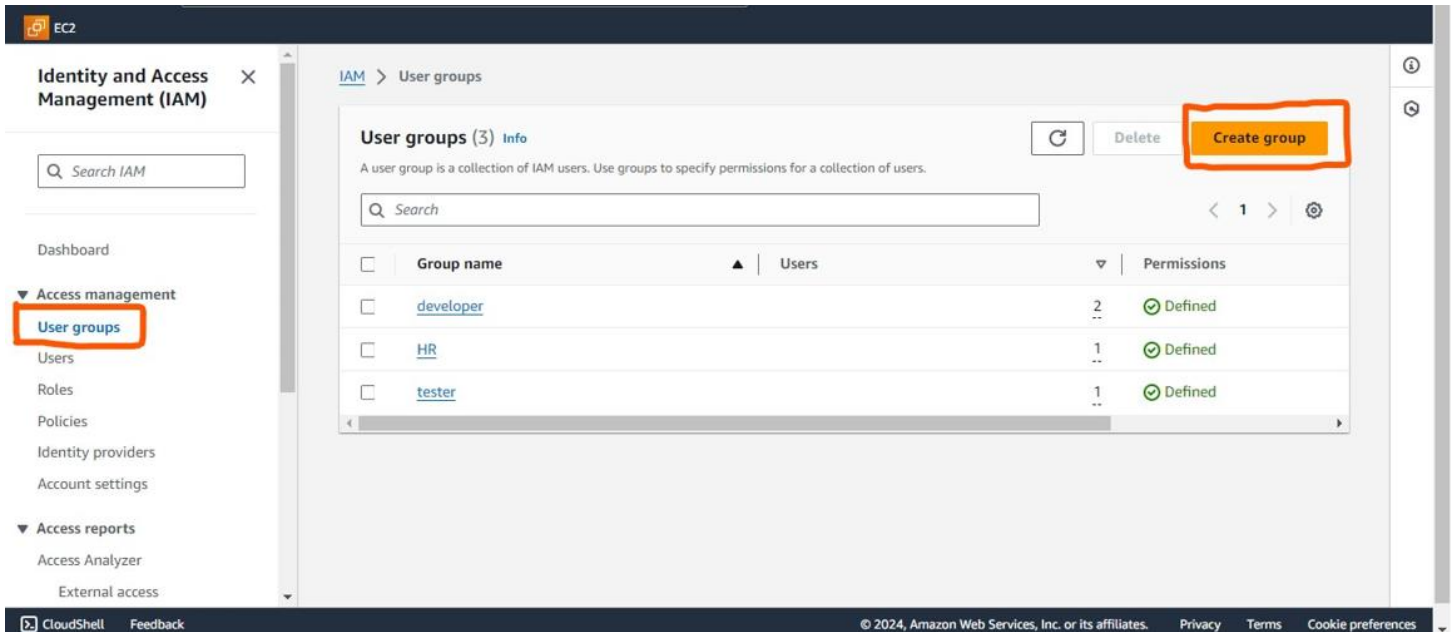
Cancel

Download .csv file

Return to users list

❖ Creating a group And assigning Aws policy:-

1. Click on user group and create group in IAM Service Dashboard



2. Assign a group name as per your choice

IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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

3. Add existing user to group (optional)

Add users to the group - Optional (7) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

<input type="checkbox"/>	User name ↗	Groups	Last activity	Creation time
<input type="checkbox"/>	mayur	0	None	11 hours ago
<input type="checkbox"/>	mayur-temp	0	None	12 minutes ago
<input type="checkbox"/>	mayur1	1	14 hours ago	14 hours ago
<input type="checkbox"/>	mayur2	1	None	14 hours ago
<input type="checkbox"/>	mayur3	1	None	14 hours ago
<input type="checkbox"/>	mayur4	0	13 hours ago	14 hours ago
<input type="checkbox"/>	mayur5	1	None	14 hours ago

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

Attach permissions policies - Optional (1/911) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Search: Filter by Type: 4 matches

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AWSAccountActivityAccess	AWS managed	None	Allows users to access the Account Act...
<input type="checkbox"/>	AWSAccountManagementFullAccess	AWS managed	None	Provides full access to AWS Account M...
<input type="checkbox"/>	AWSAccountManagementReadOnlyAccess	AWS managed	None	Provides read-only access to AWS Acco...
<input type="checkbox"/>	AWSAccountUsageReportAccess	AWS managed	None	Allows users to access the Account Usa...

5. Group created successfully

group1 user group created. [View group](#)

User groups (4) [Info](#)

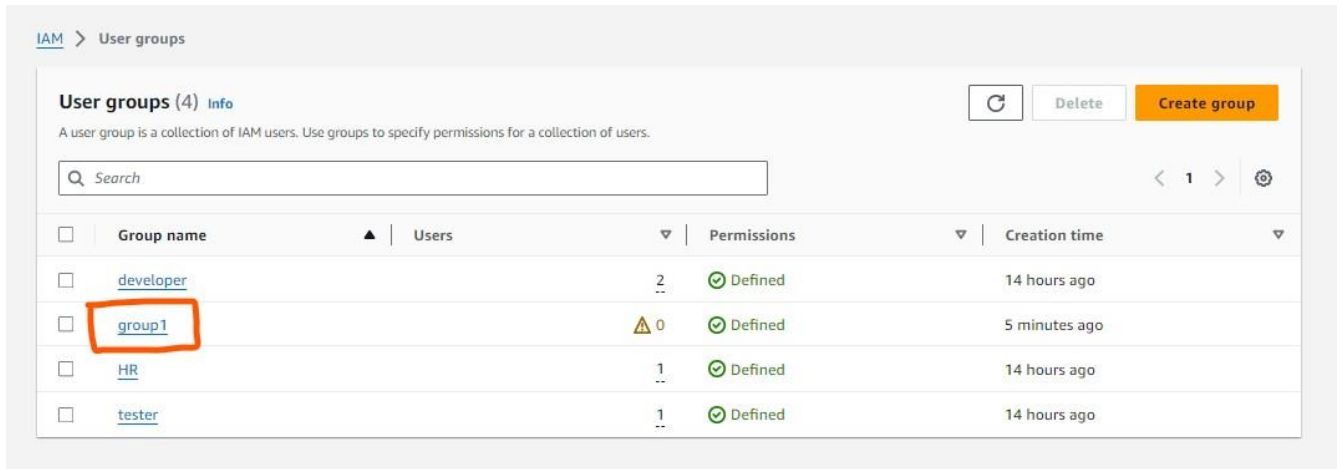
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

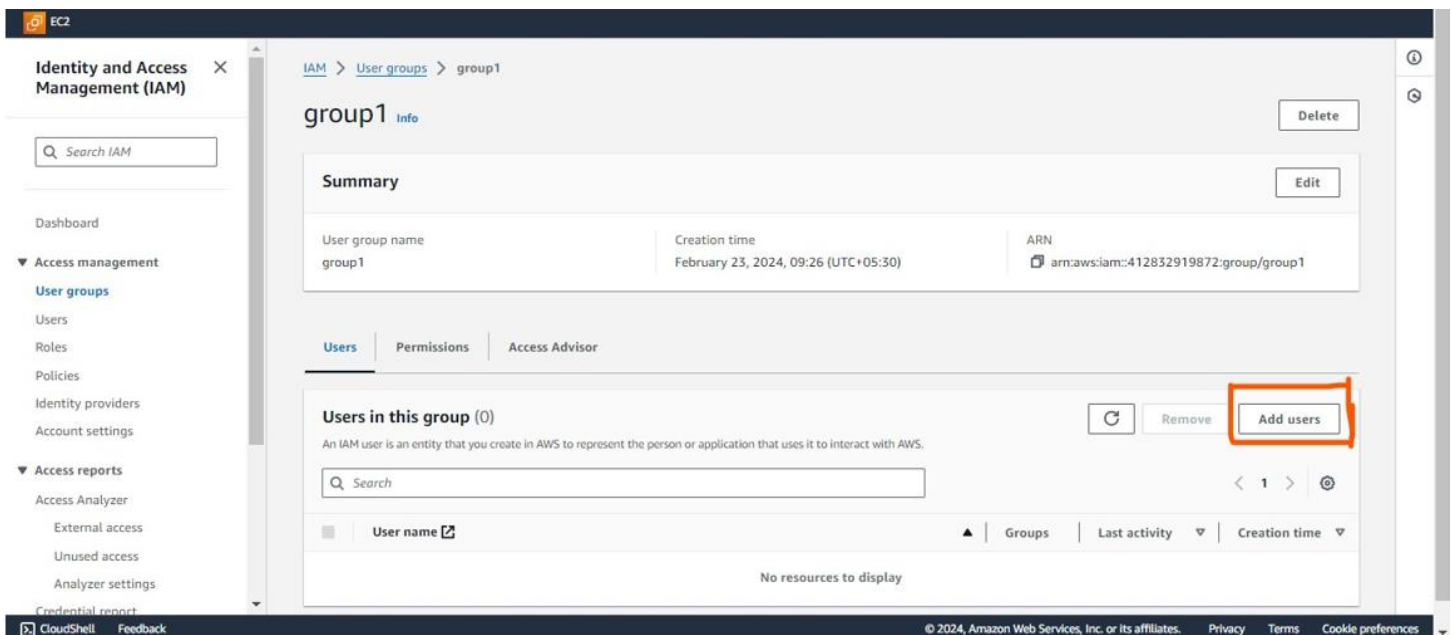
<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	developer	2	Defined	14 hours ago
<input type="checkbox"/>	group1	0	Defined	Now

❖ Adding user into group :-

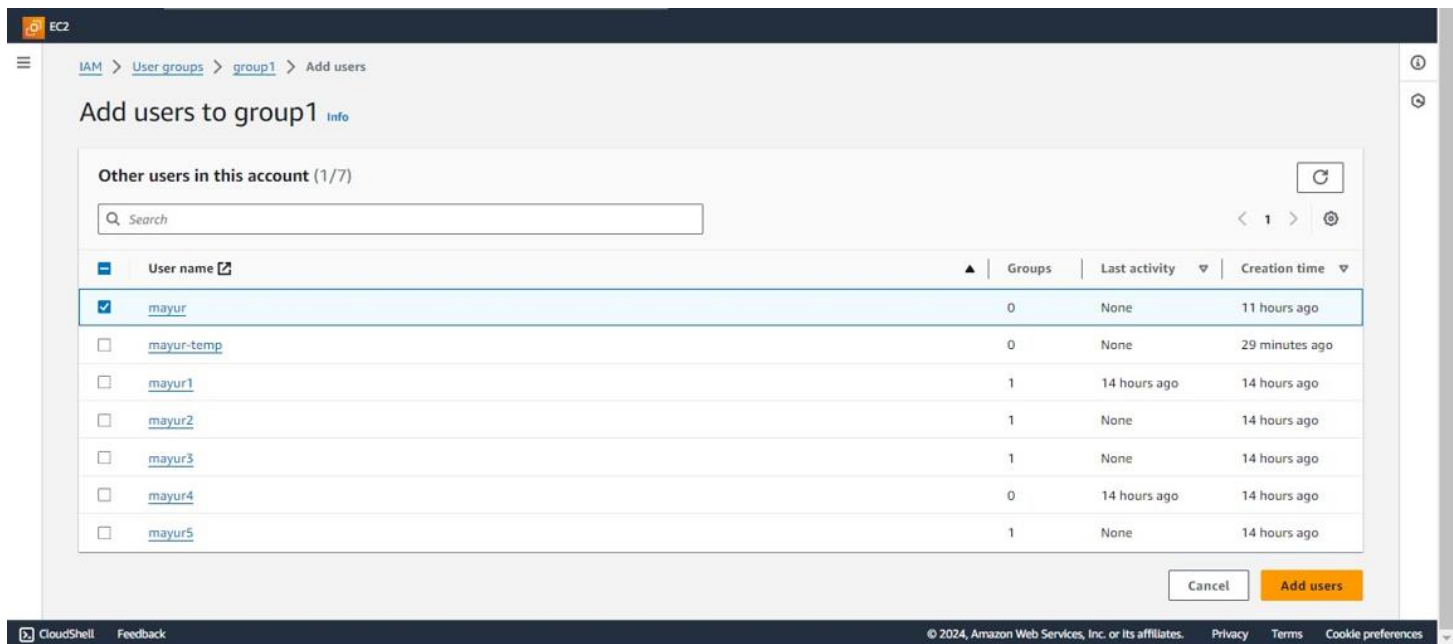
1. Select a group (in our case group1)



2. Click on Add user option



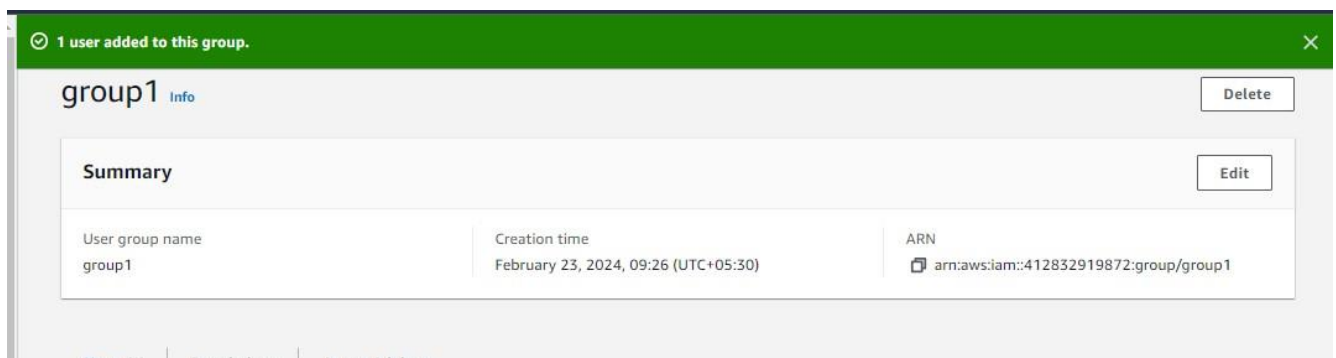
3. Select any user you want to add and click on **Add user** option



The screenshot shows the AWS IAM console interface for adding users to a group. The breadcrumb navigation is IAM > User groups > group1 > Add users. The main heading is 'Add users to group1' with an 'Info' link. Below this, there's a section 'Other users in this account (1/7)' with a search bar and a refresh button. A table lists the users with columns for selection, user name, groups, last activity, and creation time. The user 'mayur' is selected. At the bottom right, there are 'Cancel' and 'Add users' buttons.

	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	mayur	0	None	11 hours ago
<input type="checkbox"/>	mayur-temp	0	None	29 minutes ago
<input type="checkbox"/>	mayur1	1	14 hours ago	14 hours ago
<input type="checkbox"/>	mayur2	1	None	14 hours ago
<input type="checkbox"/>	mayur3	1	None	14 hours ago
<input type="checkbox"/>	mayur4	0	14 hours ago	14 hours ago
<input type="checkbox"/>	mayur5	1	None	14 hours ago

4. User added successfully

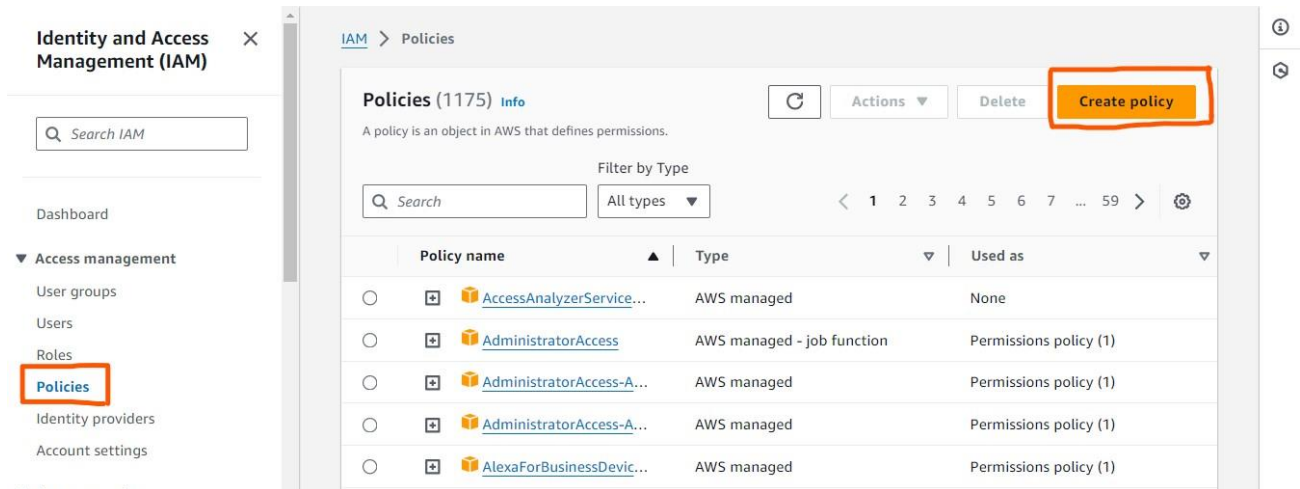


The screenshot shows the AWS IAM console interface for the 'group1' page. A green banner at the top indicates '1 user added to this group.' with a close button. The page title is 'group1' with an 'Info' link. There are 'Delete' and 'Edit' buttons. Below this is a 'Summary' section with a table showing the group details.

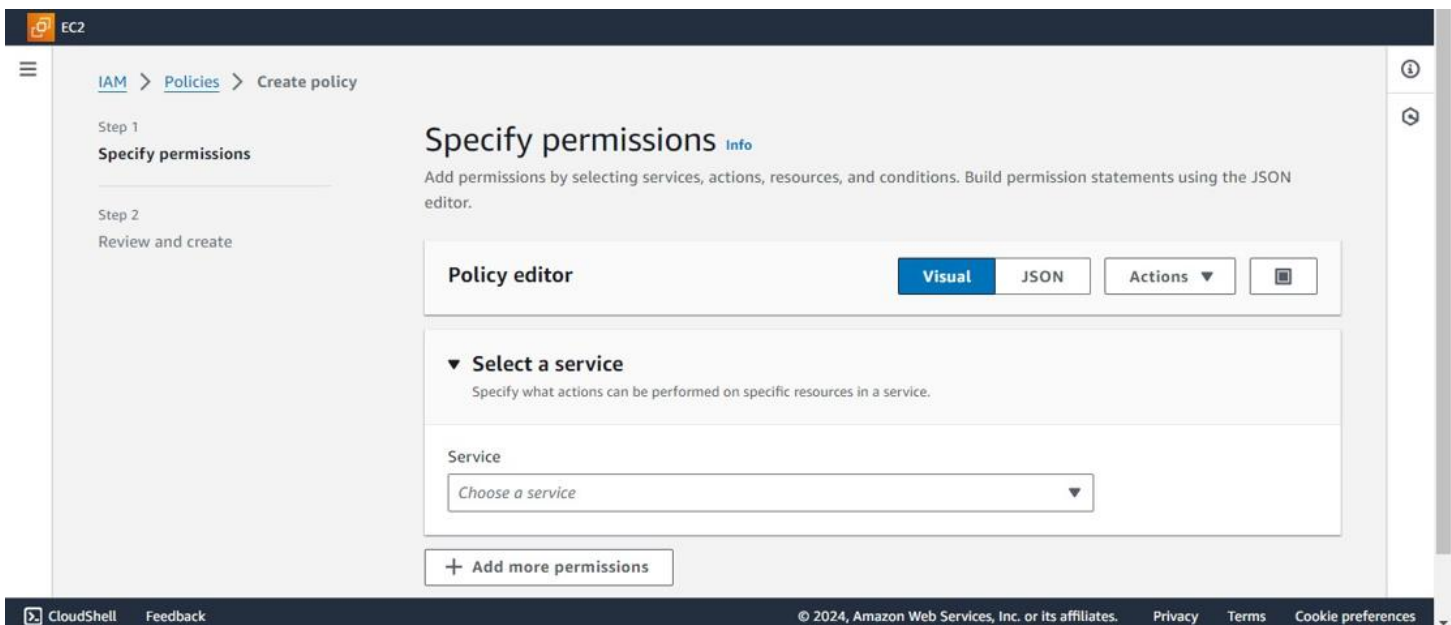
Summary		
User group name	Creation time	ARN
group1	February 23, 2024, 09:26 (UTC+05:30)	arn:aws:iam::412832919872:group/group1

❑ Creating custom policy :-

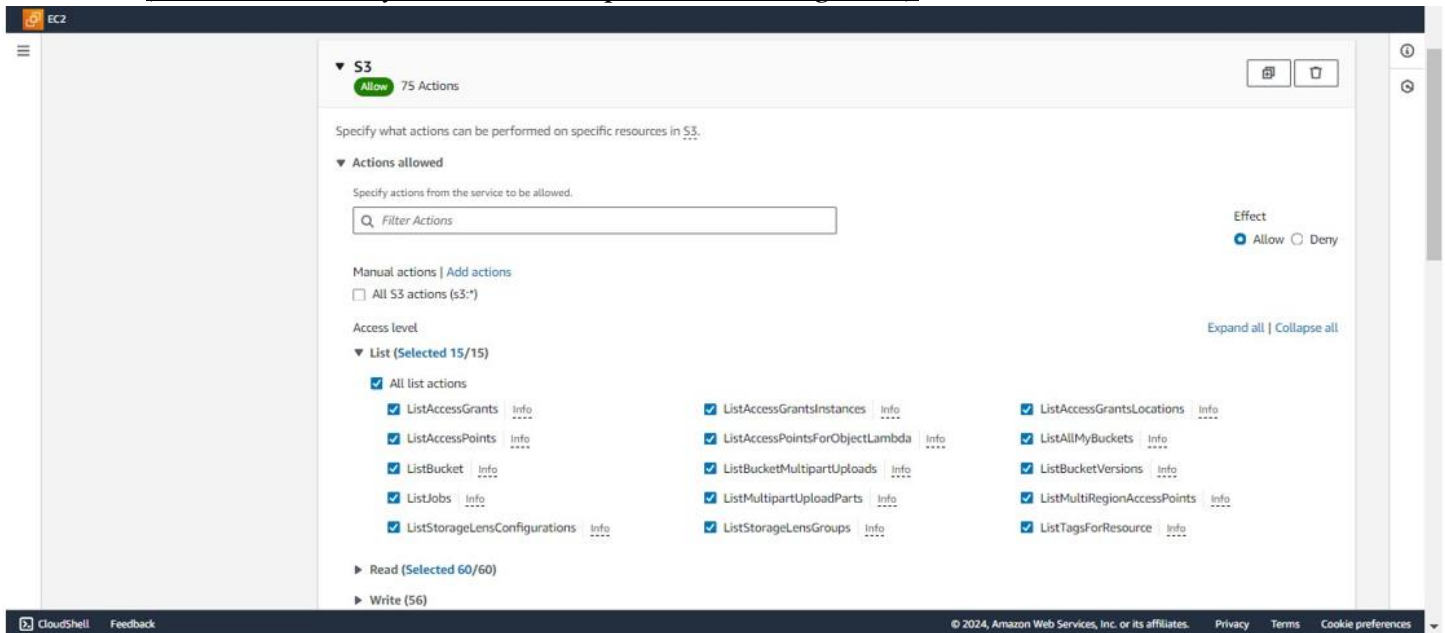
1. Click on **Policies** and **Create policy** option.



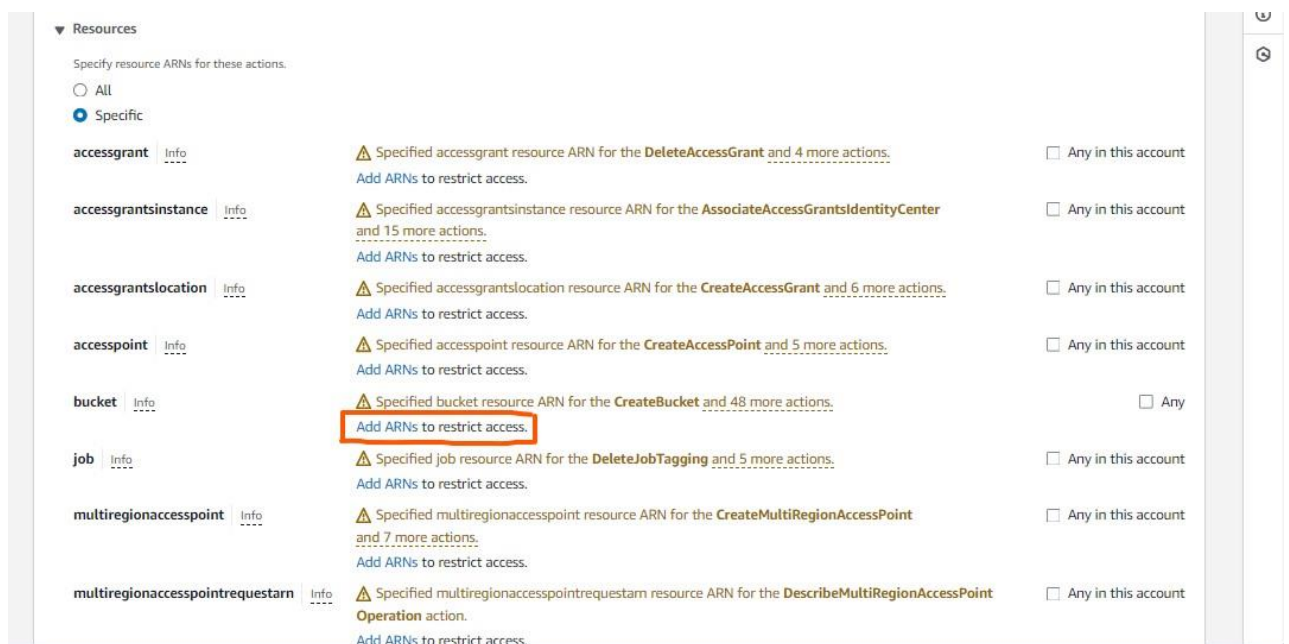
2. Select a service



3. Select the permissions or the actions you want to allow
(in this case only list and read permission is given)

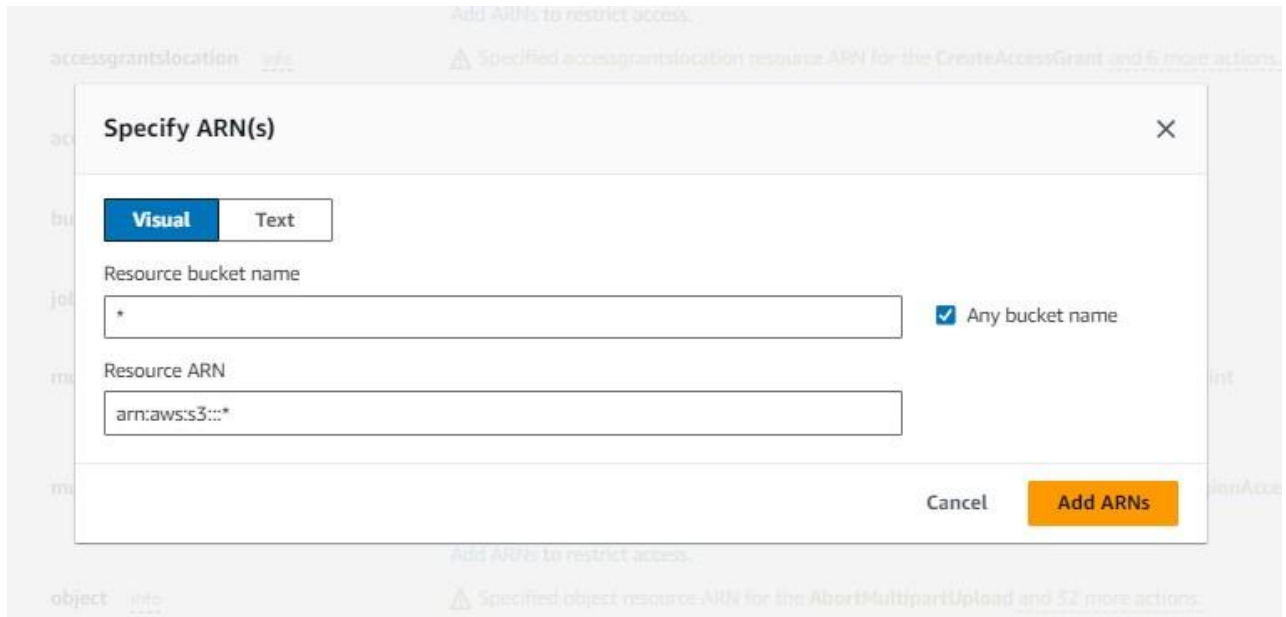


4. Click on Add ARNs option.



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



The image shows a 'Specify ARN(s)' dialog box with two tabs: 'Visual' (selected) and 'Text'. It contains two input fields: 'Resource bucket name' with a '*' character and 'Resource ARN' with 'arn:aws:s3:*'. A checkbox labeled 'Any bucket name' is checked. At the bottom right are 'Cancel' and 'Add ARNs' buttons.

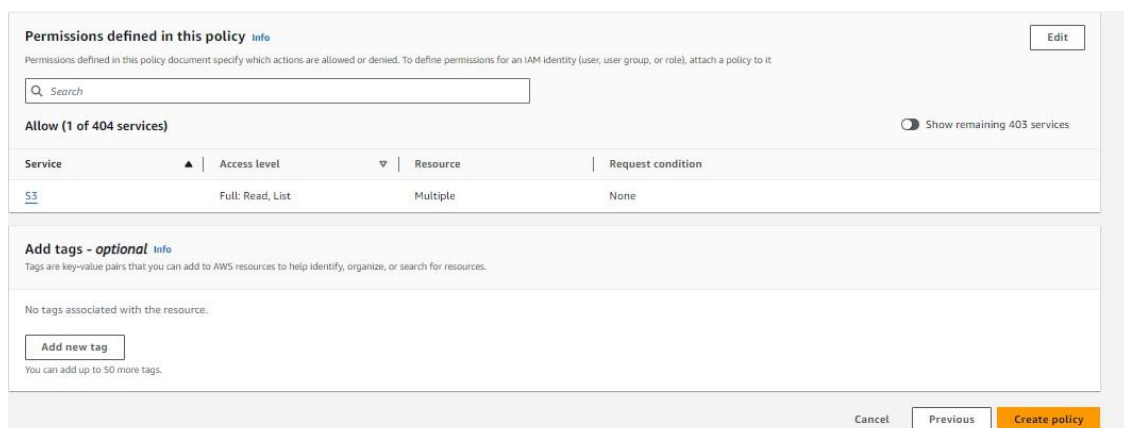
6. Click on next

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



The image shows the 'Review and create' page for an IAM policy. It includes a 'Policy details' section with a 'Policy name' field containing 'mypolicy' and a 'Description - optional' text area containing 'this policy is created for s3 bucket'. Both fields have character limits (128 for name, 1,000 for description).

8. Click on create policy



The image shows the 'Permissions defined in this policy' section. It features a search bar, a table of permissions, and an 'Add tags' section. The table has columns for Service, Access level, Resource, and Request condition. The 'Add tags' section includes an 'Add new tag' button and a note that up to 50 more tags can be added.

Service	Access level	Resource	Request condition
S3	Full: Read, List	Multiple	None

9. Policy Created successfully

Policy mypolicy created.

View policy

IAM > Policies

Policies (1176) Info

A policy is an object in AWS that defines permissions.


Search

Filter by Type

Customer managed

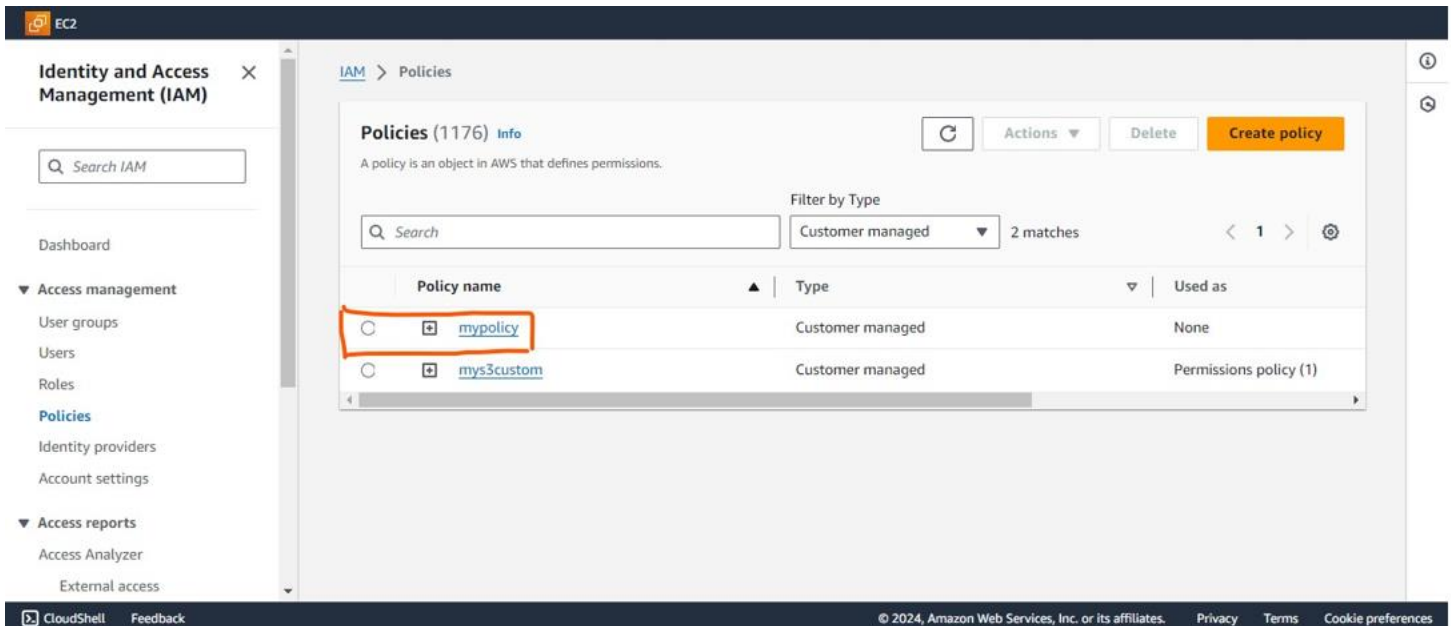
2 matches

< 1 >

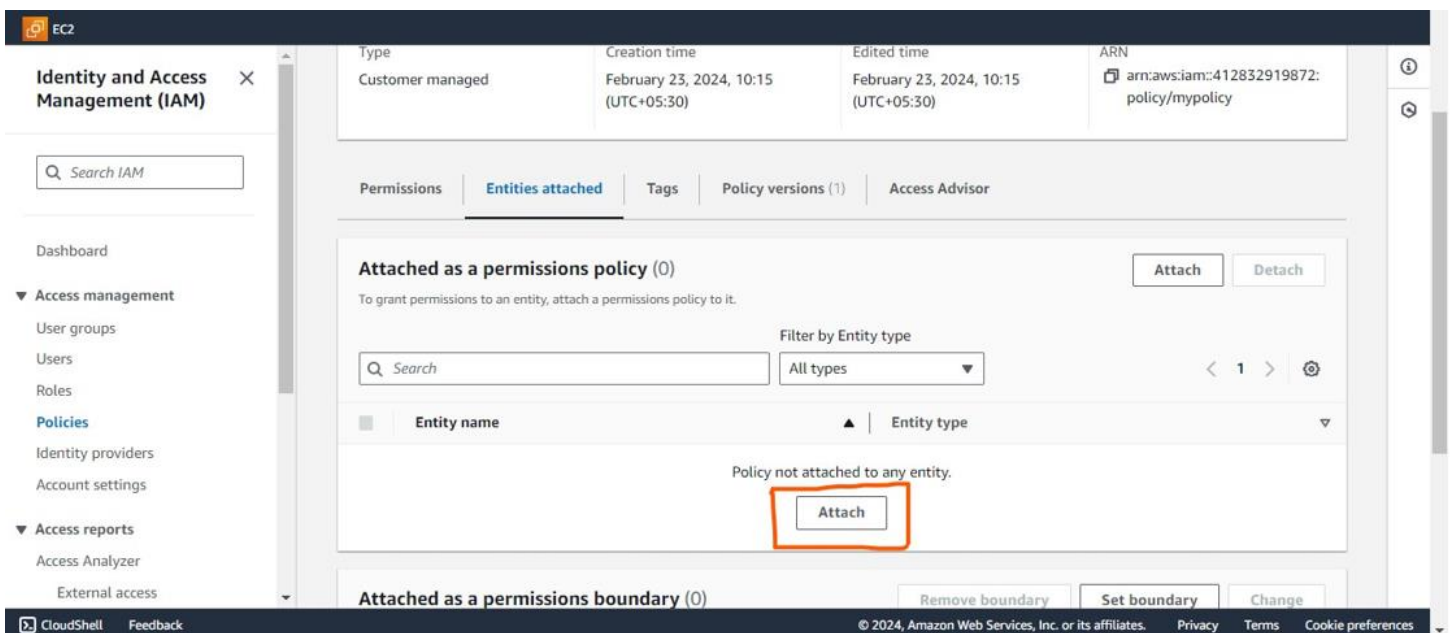
Policy name	Type	Used as	Description
 mypolicy	Customer managed	None	this policy is created for s3 bucket

□ Assigning custom policy to group and user :-

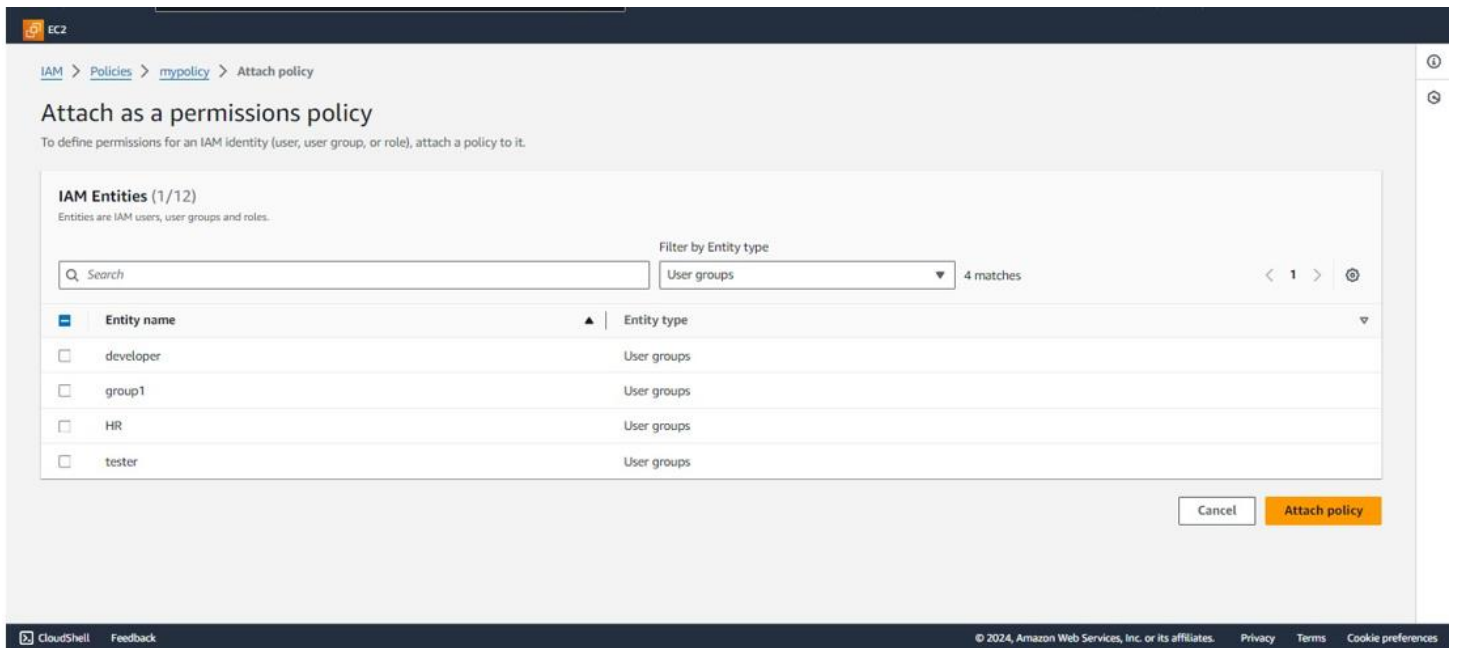
1. Select the policy



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

