Amazon Web Services

Dikshitha Chawan

13.11.2023
Maintaining the security of AWS Account

INTRODUCTION

AWS provides cloud computing platforms and API's to individuals and companies on pay-as-you-go basis.

It offers reliable, scalable and inexpensive cloud services.

AMAZON SECURITY

IAM

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access.

TASK GIVEN

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
3. Attach policy number 1 to the Dev Team from task6.
4. Attach policy number 2 to the Ops team from task6.

TASK :

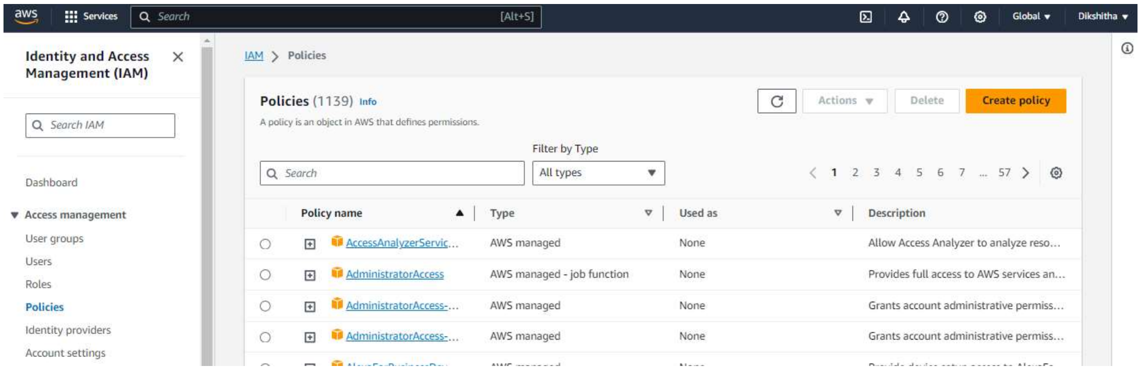
1. Create policy number 1 which lets the users to:

a. Access S3 completely

b. Only create EC2 instances

c. Full access to RDS

- From the IAM dashboard, go to policies section→create policy

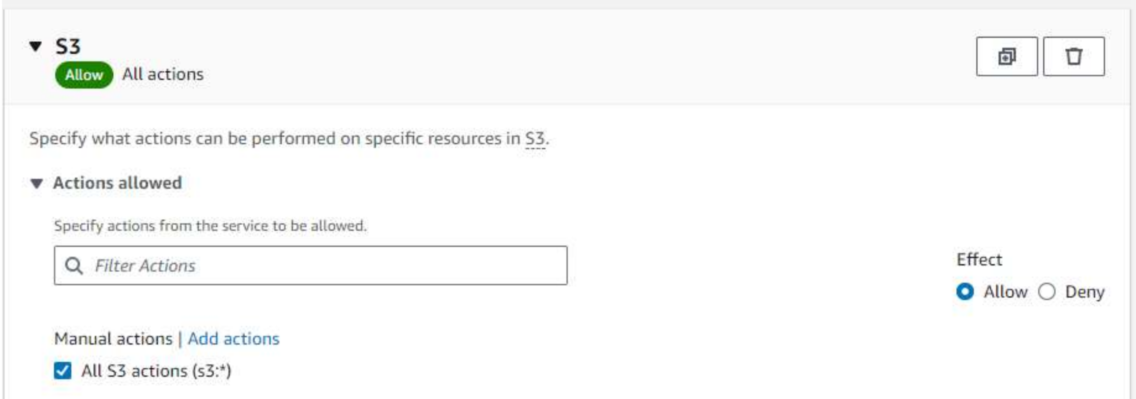


Policies (1139) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AccessAnalyzerServic...	AWS managed	None	Allow Access Analyzer to analyze reso...
○	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permiss...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permiss...

- Select the services you want to give access(S3, creating instances and RDS)



▾ S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

▾ Actions allowed

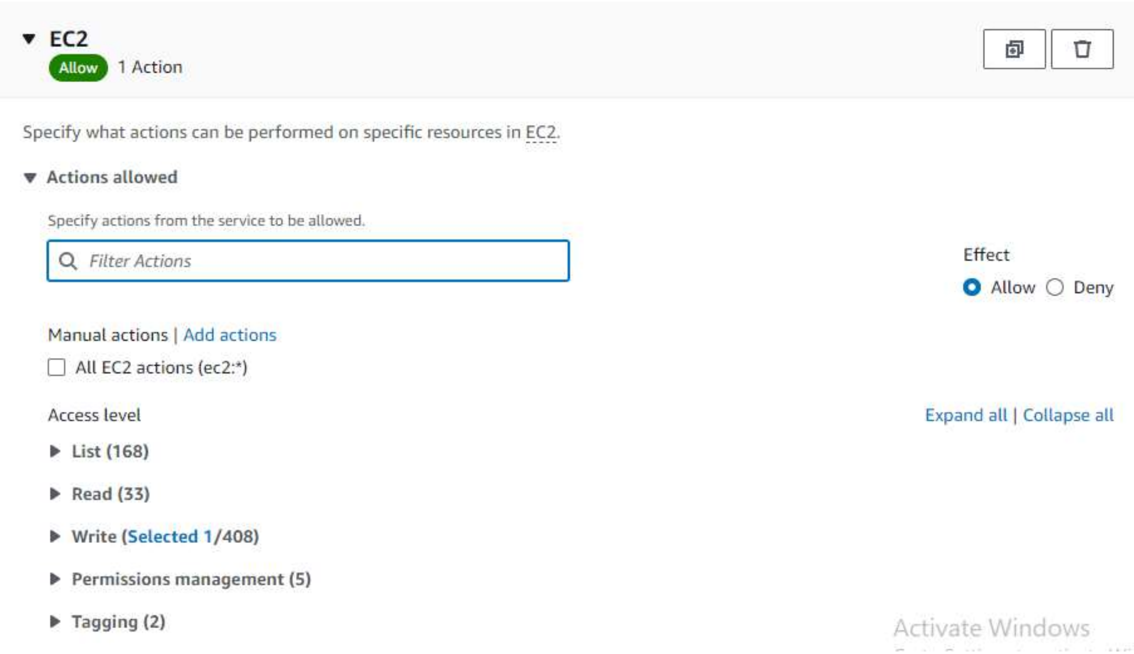
Specify actions from the service to be allowed.

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All S3 actions (s3:*)



▾ EC2

Allow 1 Action

Specify what actions can be performed on specific resources in EC2.

▾ Actions allowed

Specify actions from the service to be allowed.

Effect

● Allow ○ Deny

Manual actions | Add actions

□ All EC2 actions (ec2:*)

Access level

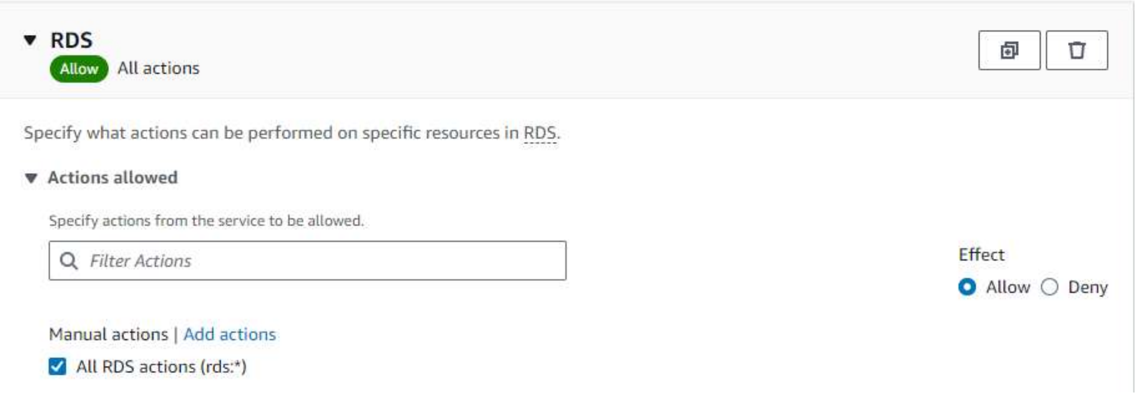
▸ List (168)

▸ Read (33)

▸ Write (Selected 1/408)

▸ Permissions management (5)

▸ Tagging (2)



Specify what actions can be performed on specific resources in RDS.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

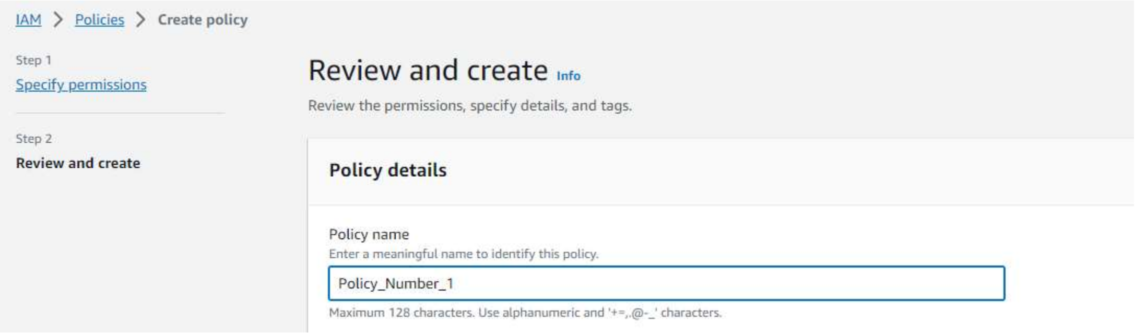
Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All RDS actions (rds:*)

- Next, give a name to you policy



Review and create

Review the permissions, specify details, and tags.

Policy details

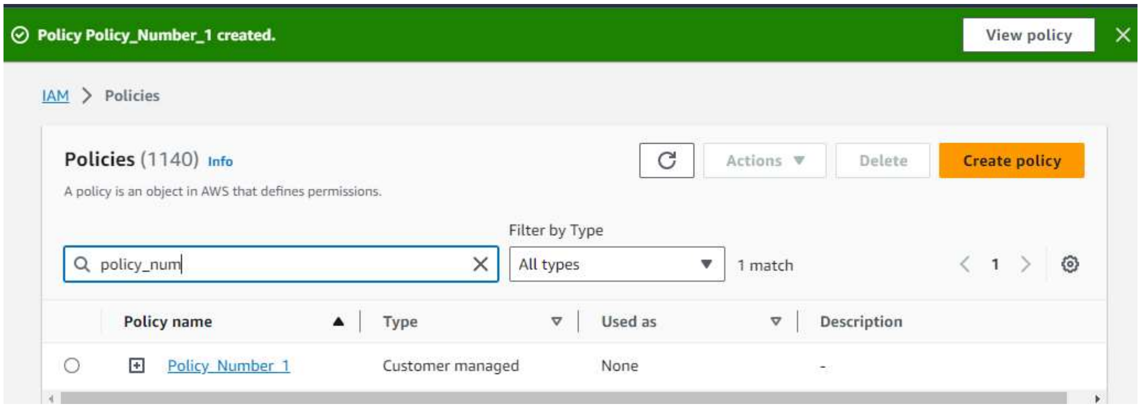
Policy name

Enter a meaningful name to identify this policy.

Policy_Number_1

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

- Policy created.



Policy Policy_Number_1 created.

Policies (1140)

A policy is an object in AWS that defines permissions.

Filter by Type

policy_num

All types

1 match

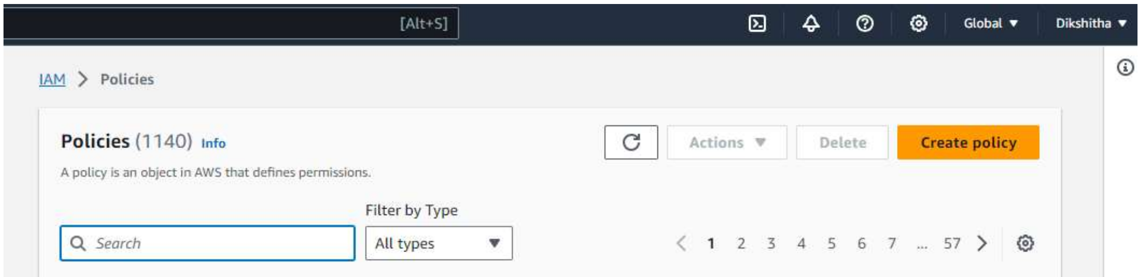
	Policy name	Type	Used as	Description
○	Policy_Number_1	Customer managed	None	-

2. Create a policy number 2 which allows the users to:

a. Access CloudWatch and billing completely

b. Can only list EC2 and S3

- Similarly, go to policy section and create policy



Policies (1140)

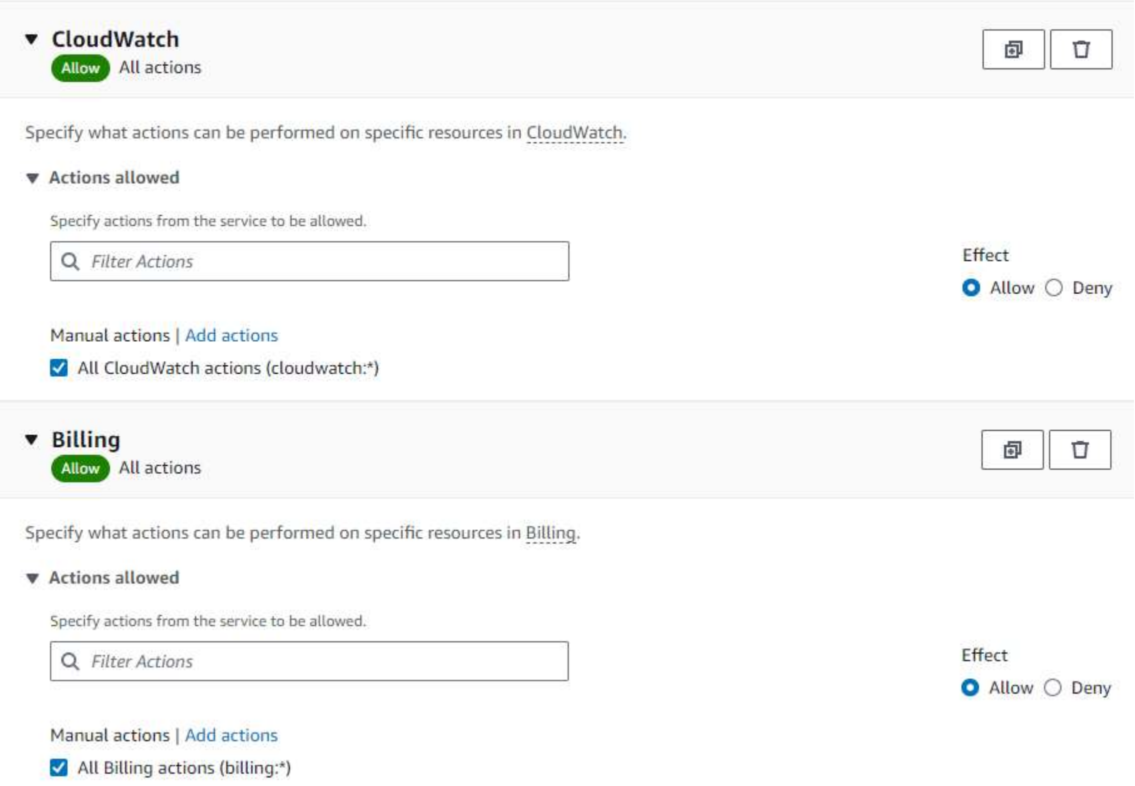
A policy is an object in AWS that defines permissions.

Filter by Type

Search

All types

- Select the services you want to give access(CloudWatch and Billing)



▼ **CloudWatch**

Allow All actions

Specify what actions can be performed on specific resources in CloudWatch.

▼ **Actions allowed**

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All CloudWatch actions (cloudwatch:*)

▼ **Billing**

Allow All actions

Specify what actions can be performed on specific resources in Billing.

▼ **Actions allowed**

Specify actions from the service to be allowed.

Filter Actions

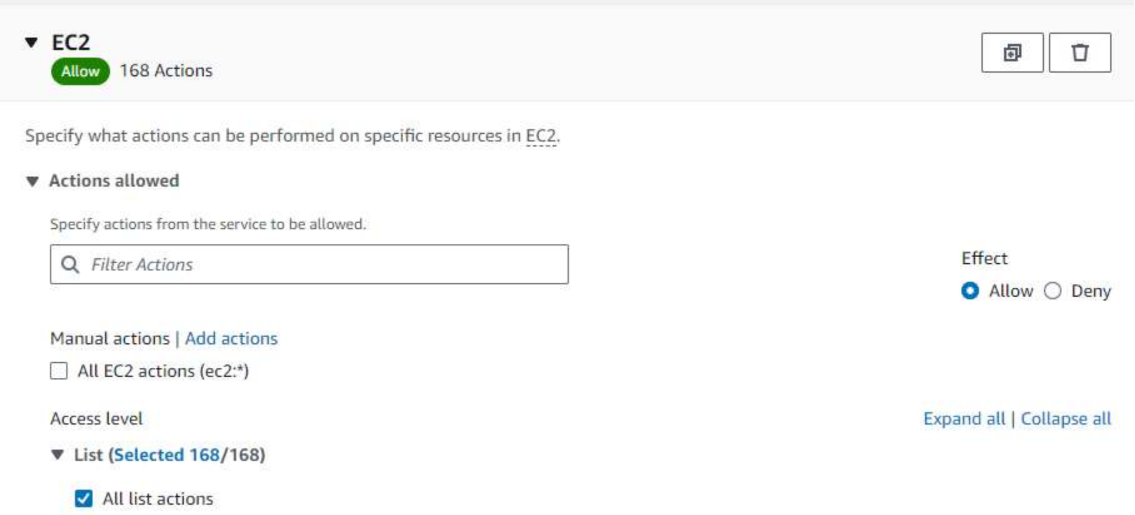
Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All Billing actions (billing:*)

- Can only list EC2 and S3



▼ **EC2**

Allow 168 Actions

Specify what actions can be performed on specific resources in EC2.

▼ **Actions allowed**

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

□ All EC2 actions (ec2:*)

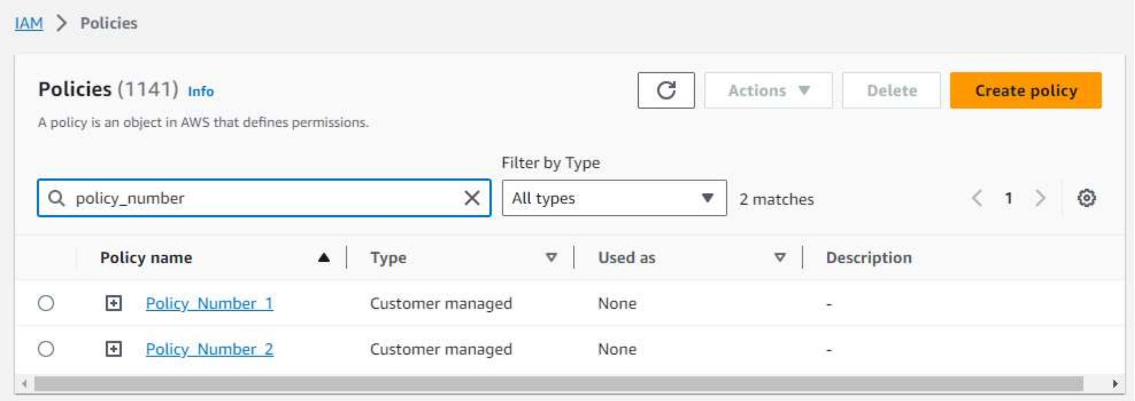
Access level

Expand all | Collapse all

▼ List (Selected 168/168)

☑ All list actions

- The second policy has been created



IAM > Policies

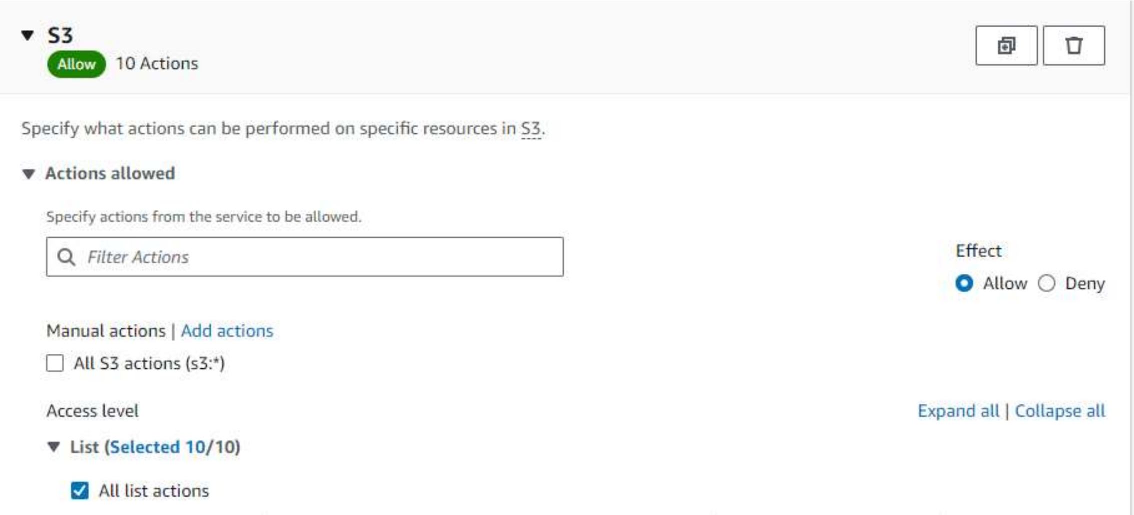
Policies (1141) Info

A policy is an object in AWS that defines permissions.

Filter by Type

policy_number ✕ | All types ▼ | 2 matches | < 1 >

	Policy name ▲	Type	Used as	Description
○	Policy_Number_1	Customer managed	None	-
○	Policy_Number_2	Customer managed	None	-



▼ S3

Allow 10 Actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

□ All S3 actions (s3:*)

Access level

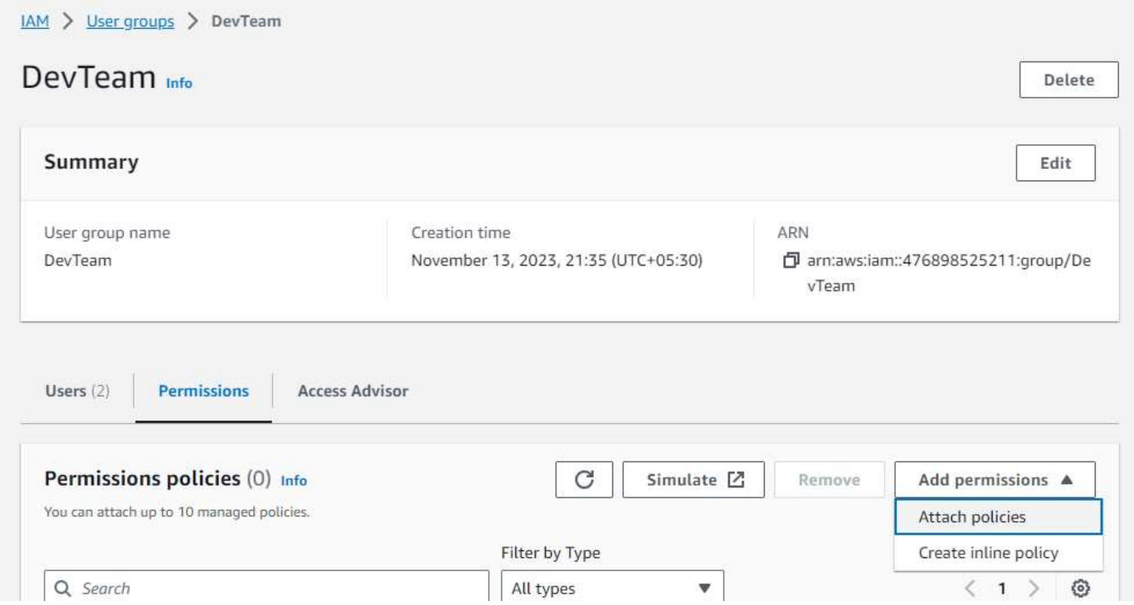
Expand all | Collapse all

▼ List (Selected 10/10)

☑ All list actions

3. Attach policy number 1 to the Dev Team from task6.

- Go to user groups and then select the group to which we need to add permission
- Next go to permission tab→Add permissions→Attach Policies



IAM > User groups > DevTeam

DevTeam Info

Delete

Summary

Edit

User group name	Creation time	ARN
DevTeam	November 13, 2023, 21:35 (UTC+05:30)	arn:aws:iam::476898525211:group/DevTeam

Users (2) | Permissions | Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Simulate | Remove | Add permissions ▲

Attach policies

Create inline policy

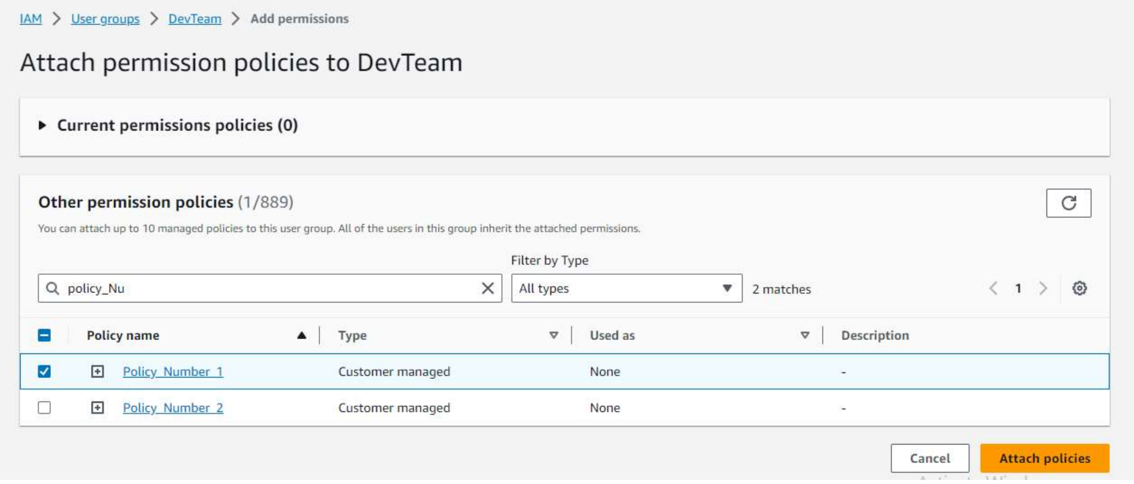
Filter by Type

Search

All types ▼

< 1 >

- Then select the permission you want to add and tap on attach policies



IAM > User groups > DevTeam > Add permissions

Attach permission policies to DevTeam

▸ Current permissions policies (0)

Other permission policies (1/889)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type

policy_Nu

All types ▼

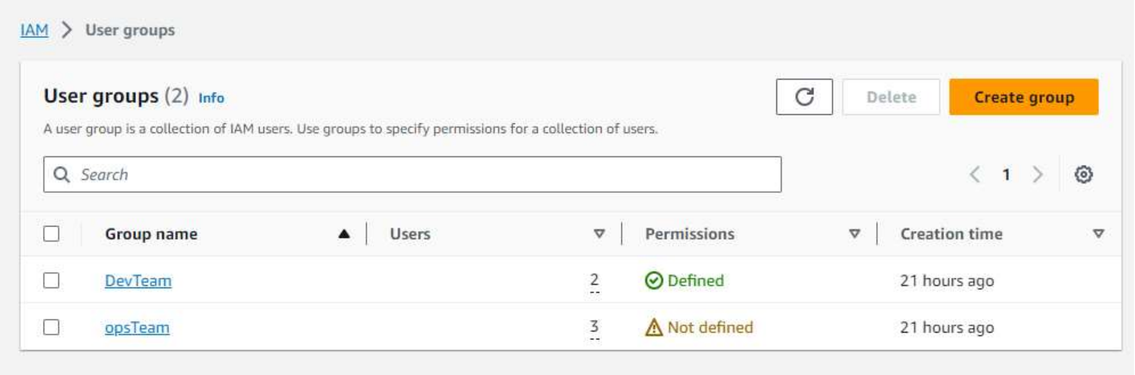
2 matches

< 1 >

	Policy name ▲	Type	Used as	Description
☑	Policy_Number_1	Customer managed	None	-
□	Policy_Number_2	Customer managed	None	-

Cancel | Attach policies

- The devteam group has policy_number_1 policy



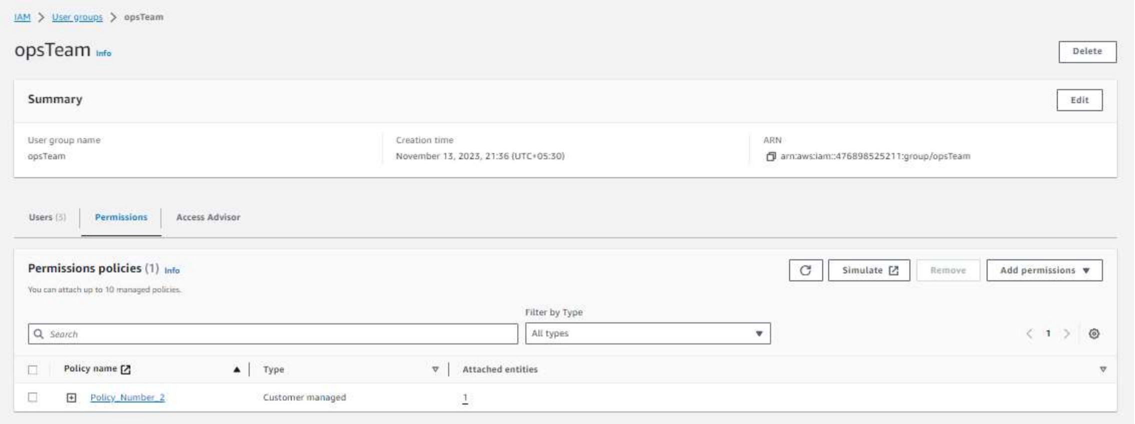
User groups (2) Info

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

□	Group name ▲	Users	Permissions	Creation time
□	DevTeam	2	✓ Defined	21 hours ago
□	opsTeam	3	⚠ Not defined	21 hours ago

4. Attach policy number 2 to the Ops team from task6.

- Similarly I have attached policy_number_2 to opsTeam



opsTeam Info

Summary

User group name	Creation time	ARN
opsTeam	November 13, 2023, 21:36 (UTC+05:30)	arn:aws:iam::476898525211:group/opsTeam

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name ▲	Type	Attached entities
□	⊞ Policy_Number_2	Customer managed	1

CONCLUSION:

Created two policies and attached them to the user group