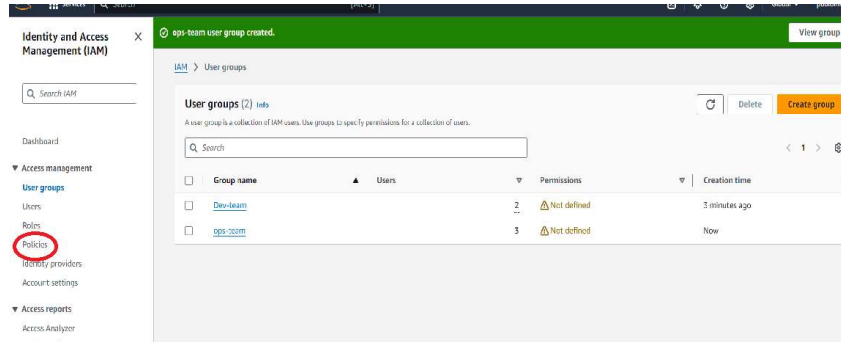


## Tasks To Be Performed:

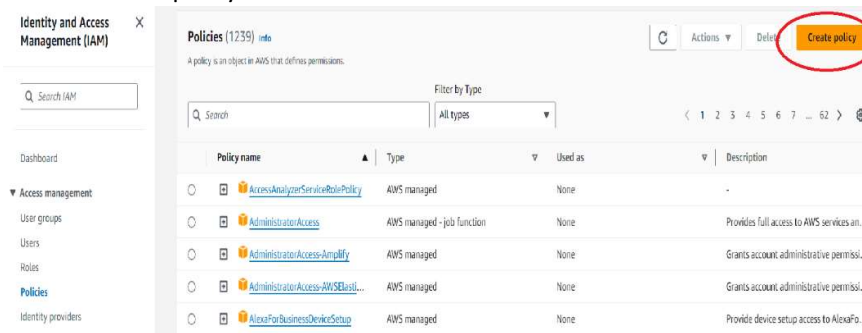
1. Create policy number 1 which lets the users to:
  - a. Access S3 completely
  - b. Only create EC2 instances
  - c. Full access to RDS

## Solution:

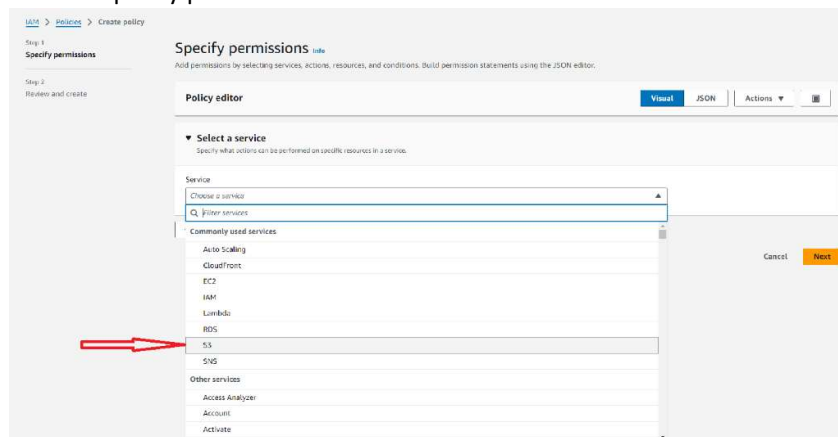
1. On the right side of IAM dashboard click on policies.



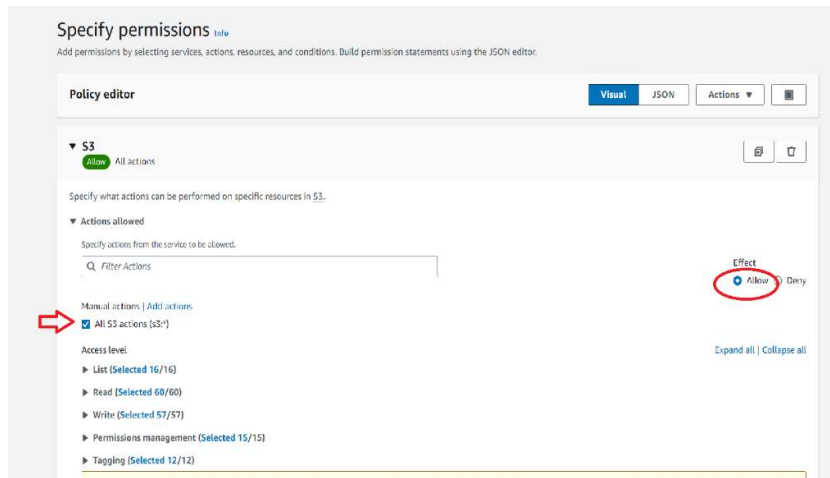
2. Click on create policy.



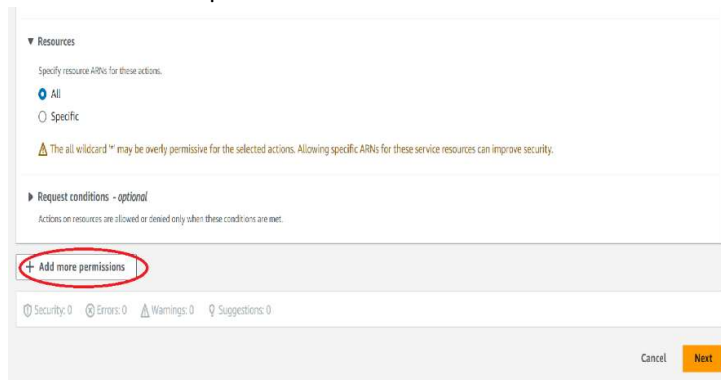
3. Here we specify permissions . so under service choose s3.



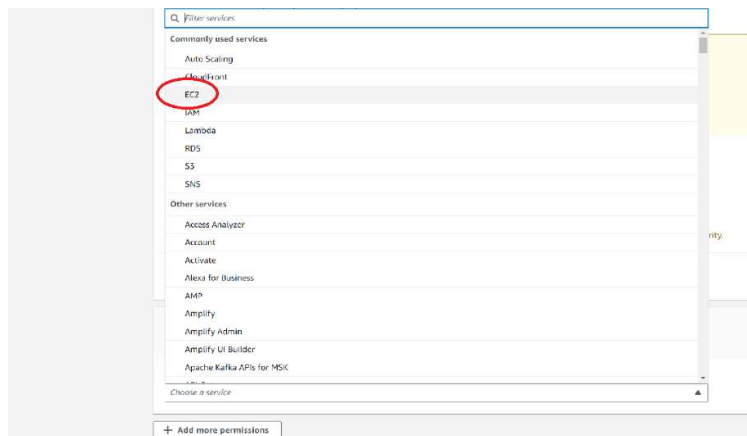
4. So under effect click allow. Under actions allowed enable all s3 actions. So S3 full access done



5. Click on add more permissions.



6. Under service choose EC2.



7. Effect = allow. Action is start instance. Click on add more permissions.

**EC2** 1 Action

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

**Actions allowed**

Specify actions from the service to be allowed.

Q start

**Effect**  
☒ Allow ☐ Deny

**Write**

☐ ModifyInstanceEventStartTime ☒ StartInstances ☐ StartNetworkInsightsAccessScopeAnalysis ☐ StartNetworkInsightsAnalysis ☐ StartTypeEndpointServicePrivateDnsVerification

**Resources**

Specify resource ARNs for these actions:

☒ All ☐ Specific

⚠ The all wildcard "\*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

**Request conditions - optional**

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

8. Under service choose RDS. So under effect click allow. Under actions allowed enable all RDS actions. So RDS full access done.

**RDS** All actions

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

**Actions allowed**

Specify actions from the service to be allowed.

Q Filter Actions

Manual actions | Add actions

☒ All RDS actions (rds:\*)

**Access level**

- List (Selected 45/45)
- Read (Selected 5/5)
- Write (Selected 115/115)
- Permissions management (Selected 1/1)
- Tagging (Selected 2/2)

**Effect**  
☒ Allow ☐ Deny

Expand all | Collapse all

9. Under review and create give policy name . Add description and it shows permission allowed in this policy. Policy number 1 created.

**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.

**Description - optional**  
 Add a short explanation for this policy.  
 Access S3 completely  
 Only create EC2 instances  
 Full access to RDS  
 Maximum 1,000 characters. Use alphanumeric and "-", "@", "." characters.

**Permissions defined in this policy**

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, group, or role), attach a policy to it.

Q Search

**Allow (3 of 423 services)**

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

**Tasks To Be Performed:**

Create a policy number 2 which allows the users to:

- a. Access CloudWatch and billing completely
- b. Can only list EC2 and S3 resources

### Solution:

- 1) Create another policy same as above . Under service choose Cloudwatch. So under effect click allow. Under actions allowed enable all Cloudwatch actions. So Cloudwatch full access done. Add more permissions.

The screenshot shows the 'Specify permissions' console in the AWS IAM console. The 'Policy editor' tab is active. Under the 'CloudWatch' service, the 'Effect' is set to 'Allow' (circled in red). Under 'Actions allowed', 'All CloudWatch actions (cloudwatch:\*)' is selected (indicated by a red arrow). The 'Access level' section shows 'List' (6/6), 'Read' (20/20), 'Write' (25/25), and 'Tagging' (2/2) are all selected. The 'Resources' section is set to 'All'. At the bottom, there is a '+ Add more permissions' button (indicated by a red arrow).

- 2) Under service choose Billing. So under effect click allow. Under actions allowed enable all Billing actions. So Billing full access done. Add more permissions.

The screenshot shows the 'Specify permissions' console in the AWS IAM console. The 'Policy editor' tab is active. Under the 'Billing' service, the 'Effect' is set to 'Allow' (circled in red). Under 'Actions allowed', 'All Billing actions (billing:\*)' is selected (indicated by a red arrow). The 'Access level' section shows 'Read' (9/9) and 'Write' (4/4) are selected. The 'Resources' section is set to 'All resources'. At the bottom, there is a '+ Add more permissions' button (indicated by a red arrow).

- 3) Under service choose EC2. So under effect click allow. Under actions allowed enable all list actions. So only list EC2 resources access done. Add more permissions.

▼ EC2 176 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Q Filter Actions

Manual actions | Add actions

☐ All EC2 actions (ec2:\*)

Access level

▼ List (Selected 176/176)

☒ All list actions

☒ DescribeAccountAttributes info

☒ DescribeAddresses info

☒ DescribeAddressesAttribute info

Effect: ☒ Allow ☐ Deny

Expand all | Collapse all

- 4) Under service choose S3. So under effect click allow. Under actions allowed enable all list actions. So only list S3 resources access done.

▼ S3 16 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Q Filter Actions

Manual actions | Add actions

☐ All S3 actions (s3:\*)

Access level

▼ List (Selected 16/16)

☒ All list actions

☒ ListAccessGrants info

☒ ListAccessGrantsInstances info

☒ ListAccessGrantsLocations info

Effect: ☒ Allow ☐ Deny

Expand all | Collapse all

- 5) Under review and create give policy name . Add description and it shows permission allowed. Policy-number-2 created.

Policy details

Policy name

Create a meaningful name to identify this policy.

policy-number-2

Maximum 128 characters. Use alphanumeric and "-\_+=@." characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,024 characters. Use alphanumeric and "-\_+=@." characters.

Permissions defined in this policy info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, role, or group), attach a policy to it.

Q Search

Allow (4 of 423 services) Show remaining 419 services

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
IAM	Full: List	All resources	None

Finally my both policies are created.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Policy policy-number-2 created.

View policy

Policies (1241) info

A policy is an object in AWS that defines permissions.

Filter by Type

Q policy- 2 matches

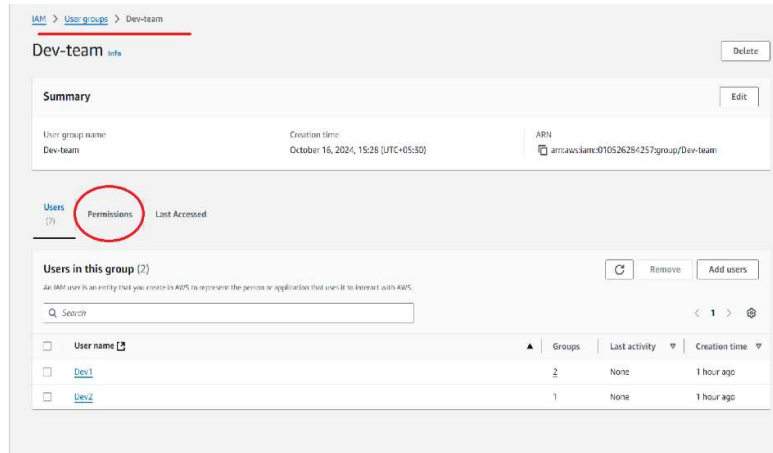
Policy name	Type	Used as	Description
policy-number-1	Customer managed	None	
policy-number-2	Customer managed	None	

## Tasks To Be Performed:

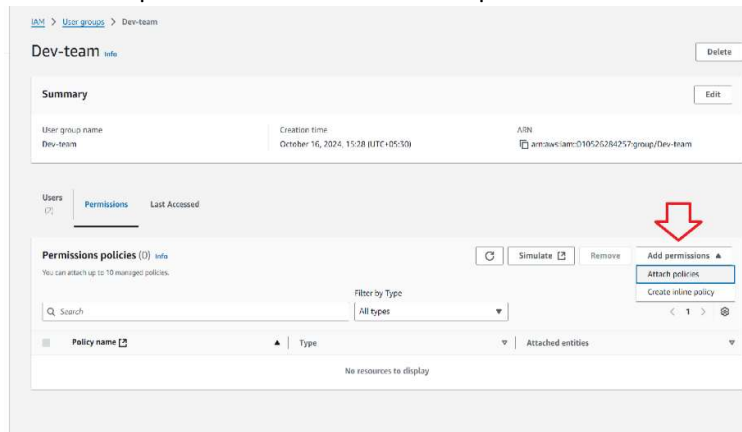
- Attach policy number 1 to the Dev Team from task 1
- Attach policy number 2 to Ops Team from task 1

### Solution:

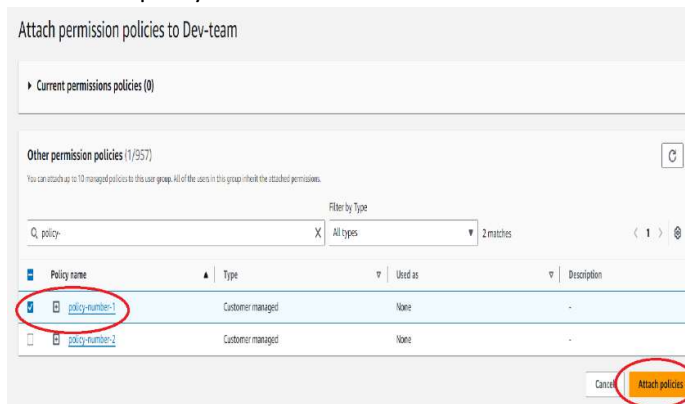
- 1) Click on user group and select Dev-team. Click on permission tab.



- 2) Click on add permission and choose attach policies.



- 3) Choose the policy we want to attach to the Dev-team and click attach policies.



- 4) Now we can see that policy-number-1 attached to Dev-team group.

iam > User groups > Dev-team

### Dev-team [info](#)

[Delete](#)

**Summary** [Edit](#)

User group name	Creation time	ARN
Dev-team	October 16, 2024, 15:28 (UTC+05:30)	arn:aws:iam::010526284257:group/Dev-team

Users (2) **Permissions** Last Accessed

**Permissions policies (1) [info](#)** [Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type: All types

<input type="checkbox"/>	Policy name <a href="#">info</a>	Type	Attached entities
<input checked="" type="checkbox"/>	<a href="#">policy-number-1</a>	Customer managed	1

5) Same steps to follow to attach policy-number-2 for Ops-team. Now we can see that policy-number-2 attached to Ops-team group.

iam > User groups > ops-team

### ops-team [info](#)

[Delete](#)

**Summary** [Edit](#)

User group name	Creation time	ARN
ops-team	October 16, 2024, 15:32 (UTC+05:30)	arn:aws:iam::010526284257:group/ops-team

Users (3) **Permissions** Last Accessed

**Permissions policies (1) [info](#)** [Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type: All types

<input type="checkbox"/>	Policy name <a href="#">info</a>	Type	Attached entities
<input checked="" type="checkbox"/>	<a href="#">policy-number-2</a>	Customer managed	1