Assignment: IAM Policies Creation and Attachment

Name: *Vikram*

Course: AWS DevOps

🧩 Problem Statement

You work for **XYZ Corporation**.

To maintain the security of the AWS account and resources, you have been asked to implement a solution that helps easily **recognize and monitor different users** by assigning proper **IAM policies** to user groups.

🎯 Tasks to Be Performed

1. **Create Policy 1** which allows users to:
   a. Access **S3 completely**
   b. **Only create EC2 instances**
   c. Have **full access to RDS**
2. **Create Policy 2** which allows users to:
   a. Access **CloudWatch and Billing completely**
   b. **Only list EC2 and S3 resources**
3. **Attach Policy 1** to the **Dev Team** (from the previous task).
4. **Attach Policy 2** to the **Ops Team** (from the previous task).

⚙️ Implementation Steps (Using AWS Management Console)

Step 1 — Open IAM

1. Sign in to the **AWS Management Console**.
2. In the top search bar, type **IAM** → open the **IAM service**.
3. You will see the IAM Dashboard.

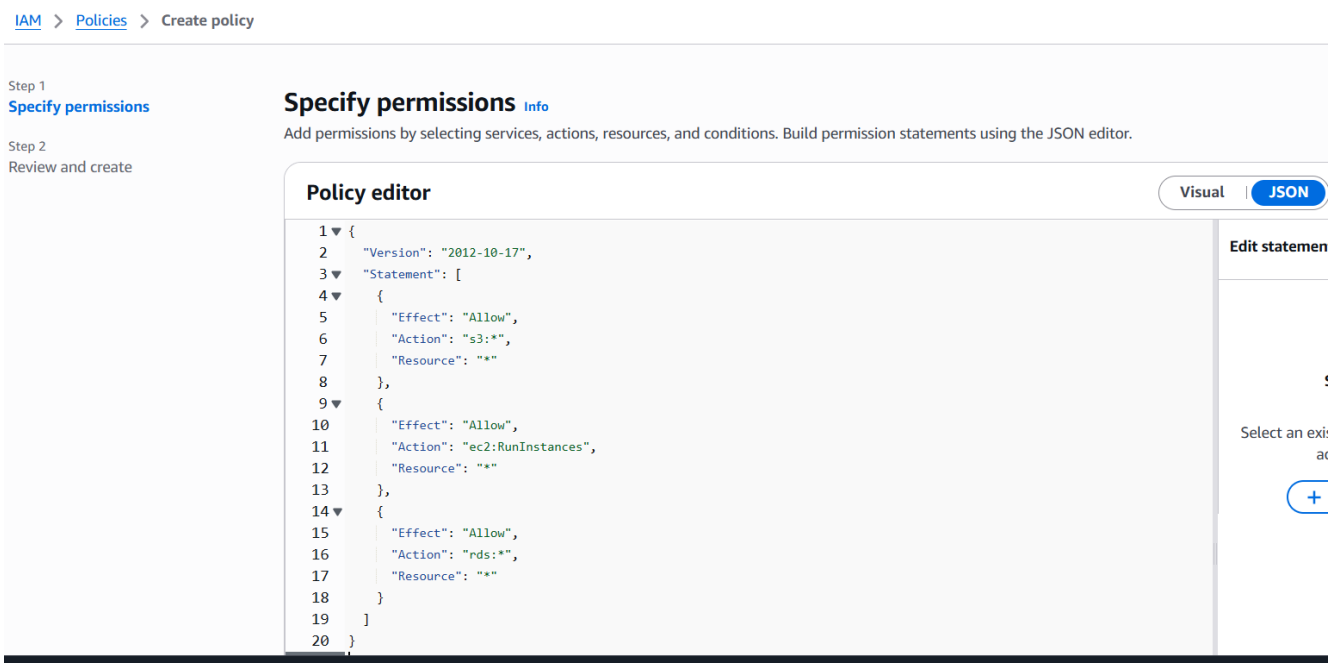
Step 2 — Create Policy 1

1. In the left sidebar, click **Policies** → **Create policy**.
2. Select the **JSON** tab and paste the following policy:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "ec2:RunInstances",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "rds:*",
   "Resource": "*"
  }
 ]
}
```

3. Click **Next**, give the policy a name: Policy-1
4. Add description: *Allows full S3 and RDS access, and EC2 creation only*
5. Click **Create policy**.

☑ *Result:* Policy-1 is created successfully.



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.

Allows full S3 and RDS access and EC2 creation only

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

Permissions defined in this policy Info — Edit

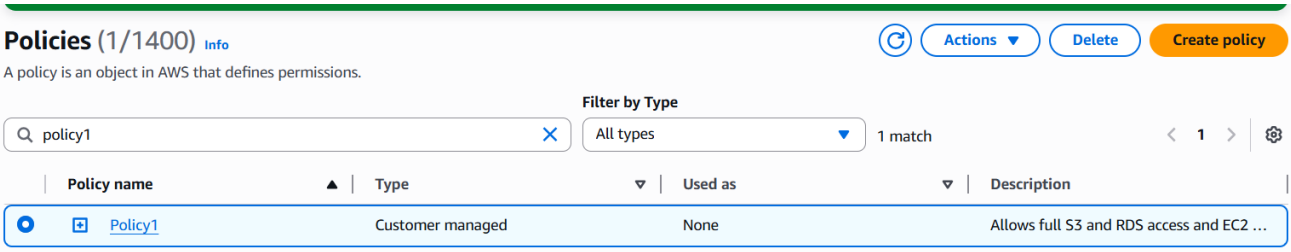
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (3 of 449 services) — Show remaining 446 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

Add tags - *optional* Info



Step 3 — Create Policy 2

1. Go to **IAM → Policies → Create policy**.
2. Choose **JSON** tab and paste the following:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudwatch:*",
    "aws-portal:*"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:Describe*",
    "s3:ListAllMyBuckets",
    "s3:ListBucket"
   ],
   "Resource": "*"
  }
 ]
}
```

3. Click **Next**, give the policy a name: Policy-2
4. Add description: *Allows full CloudWatch & Billing access and list permissions for EC2 and S3*
5. Click **Create policy**.

☑ *Result:* Policy-2 is created successfully.

Policies > Create policy

Policy1 created.

Policy editor

Visual | JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:*",
        "aws-portal:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

Edit statement

Create policy

Policy details

Policy name

Enter a meaningful name to identify this policy.

Policy2

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

Description - *optional*

Add a short explanation for this policy.

Allows full CloudWatch and Billing access and list permissions for EC2 and S3

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

Permissions defined in this policy Info

Edit

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

Search

Allow (4 of 449 services)

Show remaining 445 services

Service	Access level	Resource	Request condition
Billing Console	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
S3	Limited: List	All resources	None

Policy Policy2 created.

View policy

Policies (1/1401) Info

Actions | Delete | Create policy

A policy is an object in AWS that defines permissions.

Filter by Type

policy2

All types

1 match

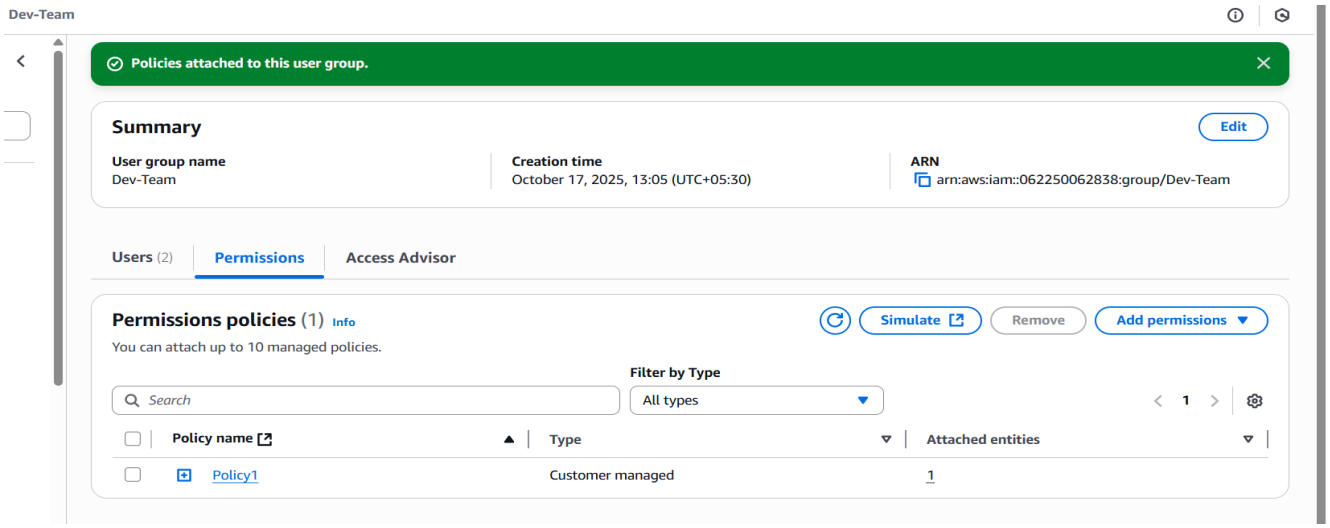
1

Policy name	Type	Used as	Description
Policy2	Customer managed	None	Allows full CloudWatch and Billing acc...

Step 4 — Attach Policy 1 to Dev Team

1. Go to **IAM → User groups**.
2. Click on **Dev-Team** (created in previous assignment).
3. Open the **Permissions** tab → click **Add permissions → Attach policies directly**.
4. Search for Policy-1, select it → click **Attach policy**.

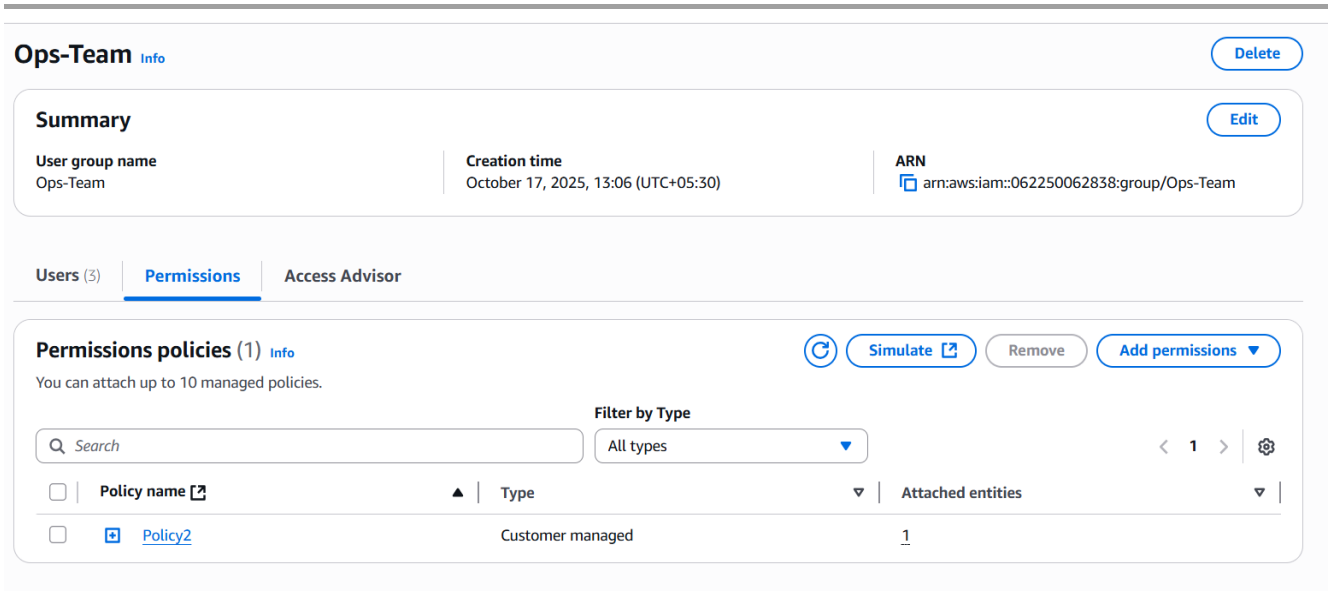
☑ *Result:* Policy-1 attached to Dev-Team.



Step 5 — Attach Policy 2 to Ops Team

1. Go to **IAM → User groups** → click **Ops-Team**.
2. Open the **Permissions** tab → **Add permissions → Attach policies directly**.
3. Search for Policy-2, select it → click **Attach policy**.

☑ *Result:* Policy-2 attached to Ops-Team.



Step 6 — Verification

- Go to **User groups → Dev-Team → Permissions tab**
    - You should see **Policy-1** attached.
- Go to **User groups → Ops-Team → Permissions tab**
    - You should see **Policy-2** attached.

☑ *Result:* Both policies are correctly attached to their respective groups.

🏁 Final Output

☑ Successfully created and attached IAM policies as per the requirements.

This ensures each team has the correct access level to AWS services, improving **security**, **resource management**, and **monitoring efficiency**.