IAM Policies

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:

    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

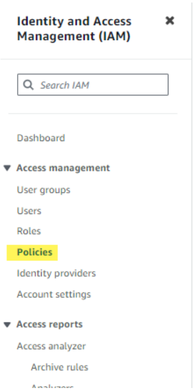
    b. Can only list EC2 and S3 resources

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

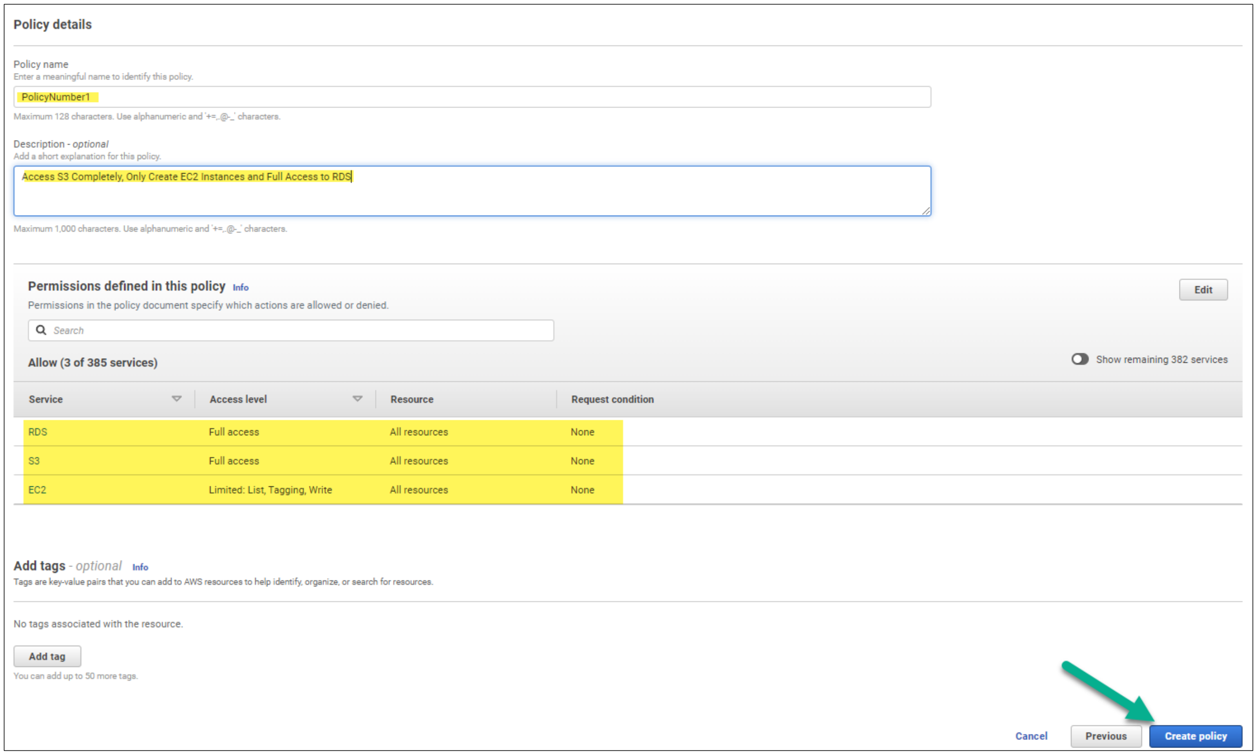
4. Attach policy number 2 to the Ops Team from task 1

Answer

Log in to the AWS Management Console and navigate to the IAM service



Click on **Policies → Create Policy**



Policy details

Policy name
Enter a meaningful name to identify this policy.
PolicyNumber1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
Access S3 Completely, Only Create EC2 Instances and Full Access to RDS
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info
Permissions in the policy document specify which actions are allowed or denied.

Allow (3 of 385 services)

Show remaining 382 services

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

Add tags - *optional* Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

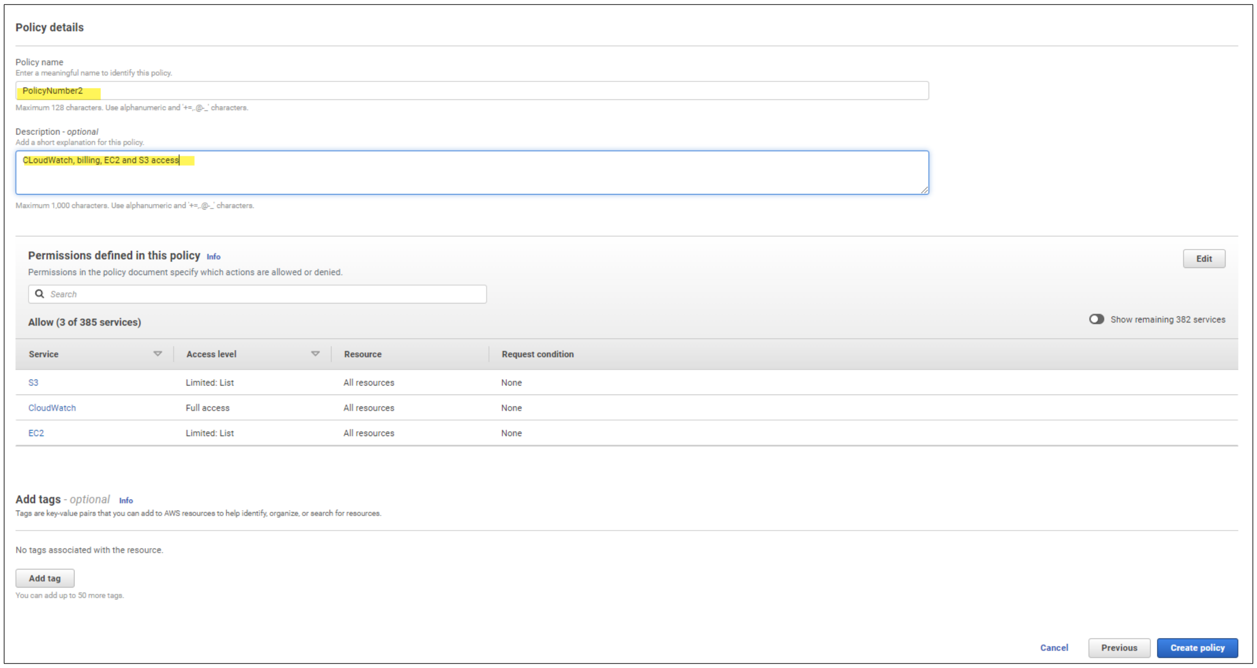
You can add up to 50 more tags.

Create Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "rds:*",
                "s3:*",
                "ec2:CreateTags",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeInstanceTypes",
                "ec2:RunInstances",
                "ec2:AssociateAddress",
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

JSON Format Policy details

Now create PolicyNumber2



Policy details

Policy name
Enter a meaningful name to identify this policy.
PolicyNumber2
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
CLoudWatch, billing, EC2 and S3 access
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info
Permissions in the policy document specify which actions are allowed or denied.

Allow (3 of 385 services)

Show remaining 382 services

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

Add tags - *optional* Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

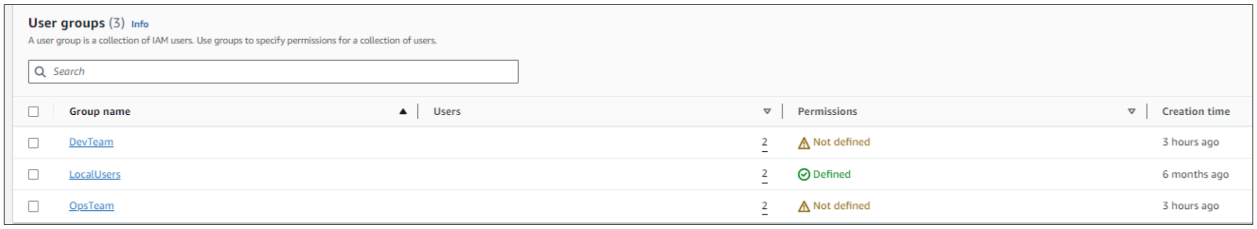
No tags associated with the resource.

You can add up to 50 more tags.

Create Policy, JSON Format policy details are below

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "s3:ListAllMyBuckets",
                "cloudwatch:*",
                "s3:ListBucket"
            ],
            "Resource": "*"
        }
    ]
}
```

Attaching Policies to Groups

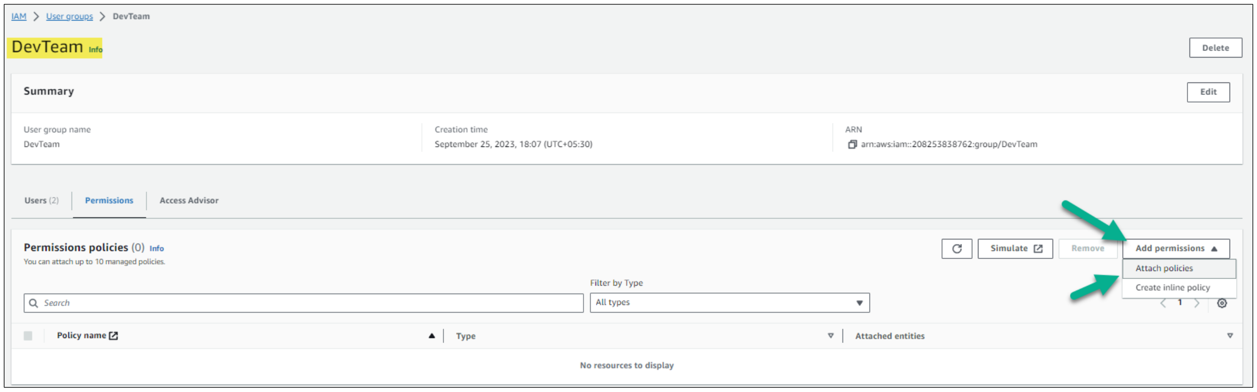


User groups (3) Info

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	⚠ Not defined	3 hours ago
☐	LocalUsers	2	✓ Defined	6 months ago
☐	OpsTeam	2	⚠ Not defined	3 hours ago

Select the group with which you want to associate a policy



IAM > User groups > DevTeam

DevTeam Info

Summary

User group name: DevTeam

Creation time: September 25, 2023, 18:07 (UTC+05:30)

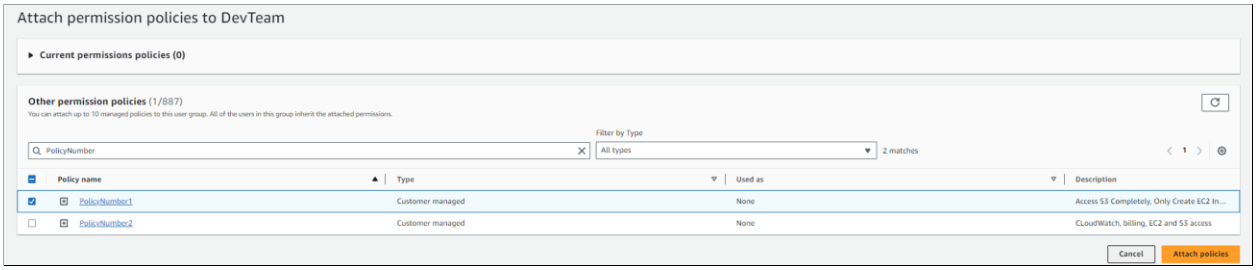
ARN: arn:aws:iam::208253838762:group/DevTeam

Permissions policies (0) Info

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
No resources to display		



Attach permission policies to DevTeam

▸ Current permissions policies (0)

Other permission policies (1/887)

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

Search: PolicyNumber

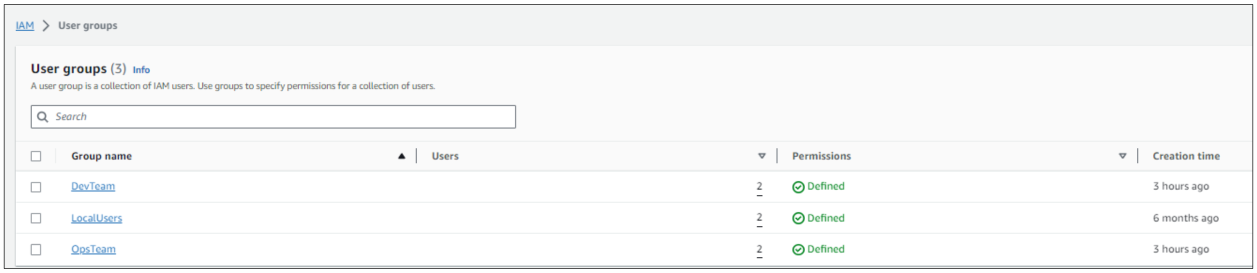
Filter by Type: All types

2 matches

☐	Policy name	Type	Used as	Description
☑	PolicyNumber1	Customer managed	None	Access S3 Completely, Only Create EC2 In...
☐	PolicyNumber2	Customer managed	None	CLoudWatch, billing, EC2 and S3 access

Select the correct policy and “**Attach the Policies**”

Similar repeat attaching policy steps to OpsTeam Group



IAM > User groups

User groups (3) 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	3 hours ago
☐	LocalUsers	2	✓ Defined	6 months ago
☐	OpsTeam	2	✓ Defined	3 hours ago

That’s all for configuring the policies.