

Module-8 Assignment – 2 IAM

You have been asked to:

1. Create a policy number 1 which lets the users to:
 - a) Access S3 completely
 - b) Only create EC2 instances
 - c) And full access to RDS
2. Create a policy number 2 which allows the users to:
 - a) Access CloudWatch and Billing completely
 - b) And can only list EC2 and S3 resources
3. Attach policy number 1 to Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Policies (919) info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

Policy name	Type	Used as	Description
m8a2_policies_1	Customer managed	None	Policy number 1 which lets the users to...
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access to AWS Dire...

1

Visual editor

JSON

3

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:DisassociateAddress",
9         "ec2:DescribeInstances",
10        "ec2:DescribeAddresses",
11        "ec2:TerminateInstances",
12        "rds:*",
13        "s3:*",
14        "ec2:DescribeRegions",
15        "ec2:RunInstances",
16        "ec2:StopInstances",
17        "ec2:StartInstances",
18        "ec2:DescribeAvailabilityZones",
19        "ec2:AssociateAddress",
20        "ec2:DescribeInstanceStatus"
21      ],
22      "Resource": "*"
23    }
24  ]
25 }
```

4

2

1. Open Policies in IAM console
2. Click on create policy
3. Click on JSON
4. Enter this JSON and finish all remaining steps to create policy

▼ CloudWatch (All actions)

► Service CloudWatch

► Actions Manual actions *

▼ Resources ☐ Specific ☒ All resources close

As a best practice, define permissions using condition keys. [Learn more](#)

► Request conditions Specify request conditions (optional)

5

6

▼ Billing (All actions)

► Service Billing

▼ Actions Specify the actions allowed in Billing ? close

Filter actions

Manual actions (add actions)

☒ All Billing actions (aws-portal:*)

Access level

► ☒ Read (4 selected)

► ☒ Write (3 selected)

Resources All resources have been selected for you because you selected All resources

► Request conditions Specify request conditions (optional)

7

▼ S3 (10 actions)

► Service S3

▼ Actions Specify the actions allowed in S3 ? close

Filter actions

Manual actions (add actions)

☐ All S3 actions (s3:*)

Access level

► ☒ List (10 selected)

► ☐ Read

► ☐ Tagging

► ☐ Write

► ☐ Permissions management

Resources All resources

► Request conditions Specify request conditions (optional)

8

▼ EC2 (137 actions)

► Service EC2

▼ Actions Specify the actions allowed in EC2 ? close

Filter actions

Manual actions (add actions)

☐ All EC2 actions (ec2:*)

Access level

► ☒ List (137 selected)

► ☐ Read

► ☐ Tagging

► ☐ Write

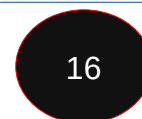
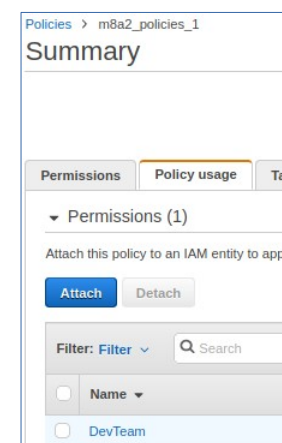
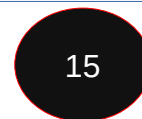
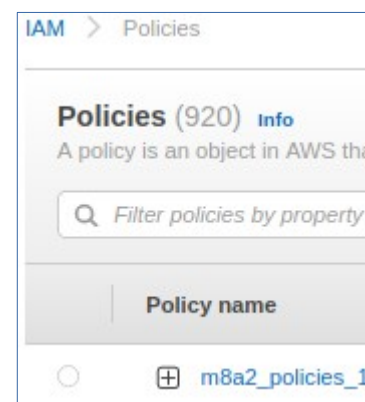
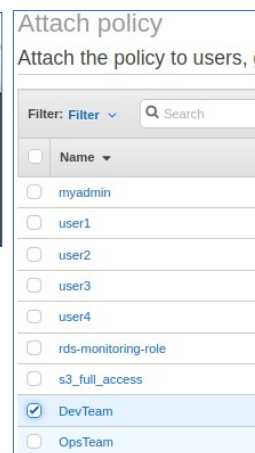
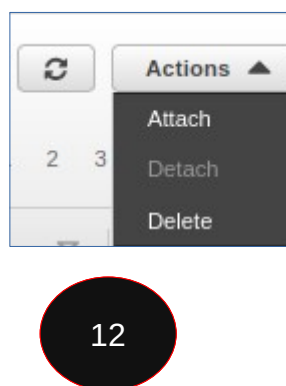
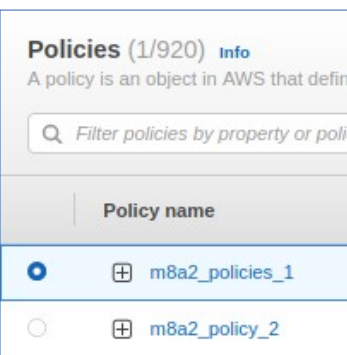
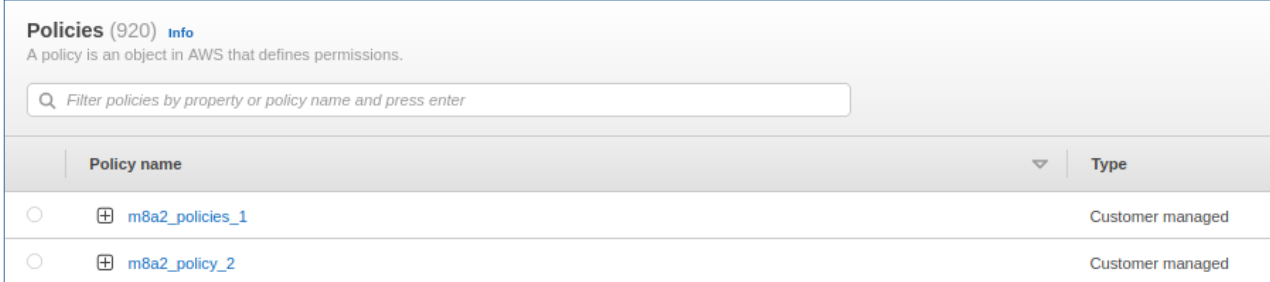
► ☐ Permissions management

Resources All resources

► Request conditions Specify request conditions (optional)

9

5. Repeat steps 1 & 2
 6. Search for service coudwatch and add all actions
 7. Search for service billing and add all actions
 8. Search for service S3 and add only List actions
 9. Search for service EC2 and add only List actions.
- Also, finish all remaining steps to create policy



10. Verify that both policies are created in IAM Policies console
11. Select policy 1
12. Select Actions-->Attach
13. Select DevTeam
14. Click on Attach policy
15. In IAM Policy Console, click on m8a2_policies_1
16. Click on Policy usage to verify that DevTeam is attached
17. Repeat steps 10-16 to attach m8a2_policies_2 to OpsTeam and verify