

Module 3: IAM Policies
Assignment

SUBMITTED BY :-HITESH CHAUHAN

COURSES OFFERED:ADVANCED CLOUD COMPUTING AND DEVELOPS

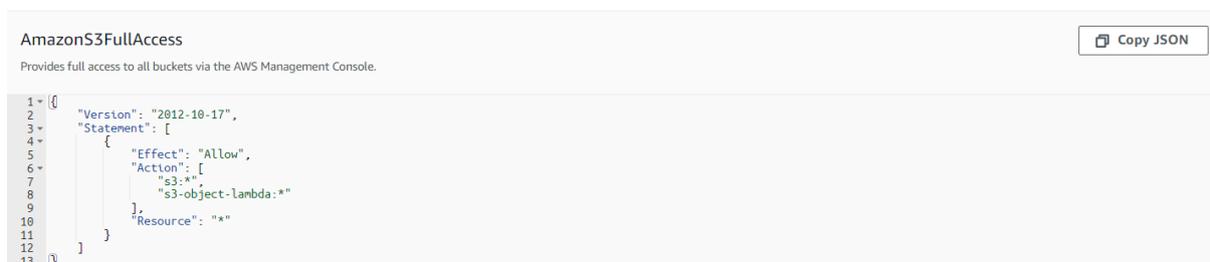
Problem Statement:

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:

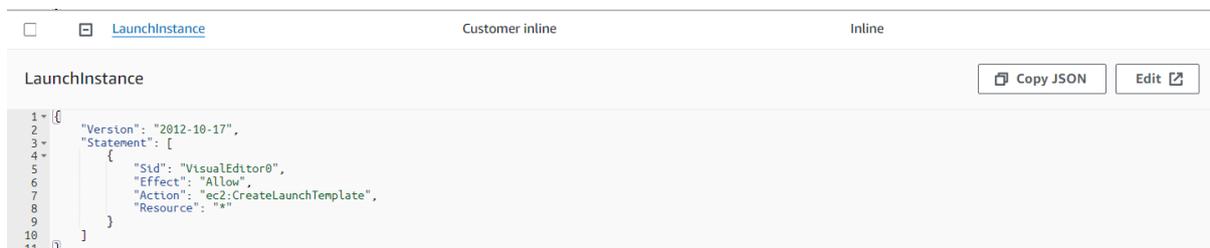
a. Access S3 completely



The screenshot shows the AWS IAM console page for the **AmazonS3FullAccess** policy. It includes a description: "Provides full access to all buckets via the AWS Management Console." and a "Copy JSON" button. The JSON policy document is displayed in a code editor with line numbers 1 through 13. The policy allows all actions on all resources in the S3 service namespace.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:*",
8         "s3-object-lambda:*"
9       ],
10      "Resource": "*"
11    }
12  ]
13 }
```

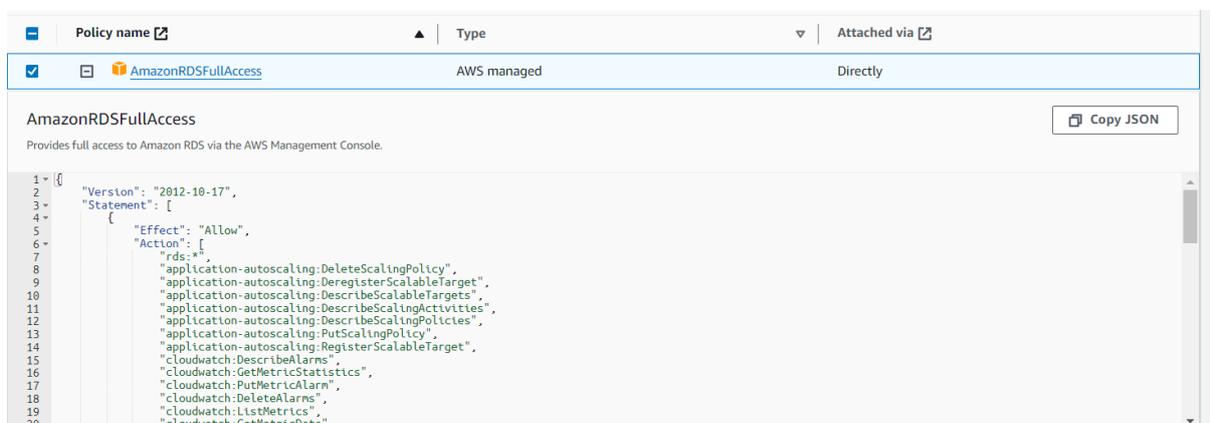
b. Only create EC2 instances



The screenshot shows the AWS IAM console page for the **LaunchInstance** policy. It includes a description: "Customer inline" and "Inline". There are "Copy JSON" and "Edit" buttons. The JSON policy document is displayed in a code editor with line numbers 1 through 11. The policy allows the `ec2:CreateLaunchTemplate` action on all resources.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:CreateLaunchTemplate",
8       "Resource": "*"
9     }
10  ]
11 }
```

c. Full access to RDS



The screenshot shows the AWS IAM console page for the **AmazonRDSFullAccess** policy. It includes a description: "Provides full access to Amazon RDS via the AWS Management Console." and a "Copy JSON" button. The JSON policy document is displayed in a code editor with line numbers 1 through 20. The policy allows all actions on all resources in the RDS service namespace.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "rds:*",
8         "application-autoscaling:DeleteScalingPolicy",
9         "application-autoscaling:DeregisterScalableTarget",
10        "application-autoscaling:DescribeScalableTargets",
11        "application-autoscaling:DescribeScalingActivities",
12        "application-autoscaling:DescribeScalingPolicies",
13        "application-autoscaling:PutScalingPolicy",
14        "application-autoscaling:RegisterScalableTarget",
15        "cloudwatch:DescribeAlarms",
16        "cloudwatch:GetMetricStatistics",
17        "cloudwatch:PutMetricAlarm",
18        "cloudwatch:DeleteAlarms",
19        "cloudwatch:ListMetrics",
20        "cloudwatch:GetMetricData"
21      ],
22      "Resource": "*"
23    }
24  ]
25 }
```

2. Create a policy number 2 which allows the users to:
 - a. Access CloudWatch and billing completely

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": "cloudwatch:*",
8-       "Resource": "*"
9-     }
10-  ]
11- ]

```

Policies (1/1227) Info Actions Delete Create policy

A policy is an object in AWS that defines permissions.

Filter by Type: 3 matches

| Policy name | Type | Used as | Description |
|-----------------------------|------------------|---------|-------------|
| CloudWatchFullAccess | Customer managed | None | - |
| BillingFullAccess | Customer managed | None | - |

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": "billing:*",
8-       "Resource": "*"
9-     }
10-  ]
11- ]

```

- b. Can only list EC2 and S3 resources

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": [
8-         "ec2:DescribeImages",
9-         "ec2:DescribeInstances",
10-        "ec2:DescribeTags",
11-        "ec2:DescribeInstanceTypes",
12-        "ec2:DescribeSnapshots"
13-       ],
14-       "Resource": "*"
15-     }
16-  ]
17- ]

```

```

4- [
5-   "Sid": "VisualEditor0",
6-   "Effect": "Allow",
7-   "Action": [
8-     "s3:ListAccessPointsForObjectLambda",
9-     "s3:ListBucketMultipartUploads",
10-    "s3:ListAccessPoints",
11-    "s3:ListBucketVersions",
12-    "s3:ListJobs",
13-    "s3:ListBucket",
14-    "s3:ListMultiRegionAccessPoints",
15-    "s3:ListStorageLensGroups",
16-    "s3:ListAccessGrantsLocations",
17-    "s3:ListMultipartUploadParts",
18-    "s3:ListStorageLensConfigurations",
19-    "s3:ListTagsForResource",
20-    "s3:ListAllMyBuckets",
21-    "s3:ListAccessGrantsInstances",
22-    "s3:ListAccessGrants"
23-  ],

```

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

DevTeam [Info](#) Delete

Summary Edit

| | | |
|----------------------------|--|--|
| User group name DevTeam | Creation time September 01, 2024, 23:27 (UTC+05:30) | ARN arn:aws:iam::381492076809:group/DevTeam |
|----------------------------|--|--|

Users (2) | **Permissions** | Access Advisor

Permissions policies (3) [Info](#) Refresh Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type All types < 1 > Settings

| <input type="checkbox"/> | Policy name ↗ | Type | Attached entities |
|--------------------------|---|------------------|-------------------|
| <input type="checkbox"/> | AmazonS3FullAccess | AWS managed | 2 |
| <input type="checkbox"/> | EC2FastLaunchFullAccess | AWS managed | 1 |
| <input type="checkbox"/> | rds_fullaccess | Customer managed | 1 |

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

OpsTeam [Info](#) Delete

Summary Edit

| | | |
|----------------------------|--|--|
| User group name OpsTeam | Creation time September 01, 2024, 23:28 (UTC+05:30) | ARN arn:aws:iam::381492076809:group/OpsTeam |
|----------------------------|--|--|

Users (5) | **Permissions** | Access Advisor

Permissions policies (4) [Info](#) Refresh Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type All types < 1 > Settings

| <input type="checkbox"/> | Policy name ↗ | Type | Attached entities |
|--------------------------|--------------------------------------|------------------|-------------------|
| <input type="checkbox"/> | BillingFullAccess | Customer managed | 1 |
| <input type="checkbox"/> | CloudWatchFullAccess | Customer managed | 1 |
| <input type="checkbox"/> | EC2_RESOURCES | Customer managed | 1 |
| <input type="checkbox"/> | S3RESOURCES | Customer managed | 1 |

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

a. Access S3 completely

b. Only create EC2 instances

c. Full access to RDS

