



St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119



Placement Empowerment Program

Cloud Computing and DevOps Centre

Creating an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Esly Abro

Department: IT



Setting Up IAM Roles and Permissions

Introduction

In this POC, we will demonstrate how to create an IAM role on a cloud platform, assign the role to a virtual machine (VM), and restrict/allow specific actions (e.g., accessing an S3 bucket). This is a

fundamental aspect of cloud security, ensuring that resources are accessed only by authorized entities with appropriate permissions.

Overview

This POC covers the basics of setting up and managing IAM roles, including role creation, permission assignment, and testing access. By the end of this POC, you'll understand how to control access to cloud resources using IAM roles and test access to ensure security policies are enforced.

Objectives

- Create an IAM role with custom permissions (e.g., access to S3)
- Assign the IAM role to a VM (EC2 in AWS)
- Verify the role's permissions by testing both allowed and denied actions

Step-by-Step Process

Step 1: Create an IAM Role

1. **Login to AWS Console:**
 - a. Go to [AWS Management Console](#).
2. **Navigate to IAM:**
 - a. From the Services menu, select **IAM**.

The screenshot shows the AWS IAM console 'Create role' page. The left sidebar contains a navigation menu with 'IAM' and 'Roles' selected. The top navigation bar shows the AWS logo, a search bar, and user information. The main content area is titled 'Create role' and shows the 'Select trusted entity' step. The 'Trusted entity type' section has five options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'Use case' section has a dropdown menu with 'EC2' selected. The footer contains the text '© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

3. **Create New Role:**
 - a. Click on **Roles** in the left sidebar, then click **Create Role**.
 - b. Choose **AWS Service** as the trusted entity, and select **EC2** (for VM).
 - c. Click **Next**.
4. **Attach Policies:**
 - a. In the **Permissions** section, attach a managed policy (e.g., AmazonS3ReadOnlyAccess) to give read access to S3.
 - b. Click **Next: Tags**, and then **Next: Review**.

aws Search [Alt+S]

IAM > Roles > Create role

Step 1 Select trusted entity
Step 2 **Add permissions**
Step 3 Name, review, and create

Add permissions [Info](#)

Permissions policies (1/1023) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type: All types 13 matches

	Policy name	Type	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings ...
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permi...
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
<input checked="" type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
<input type="checkbox"/>	AmazonS3TablesFullAccess	AWS managed	Provides full access to all S3 table buc...
<input type="checkbox"/>	AmazonS3TablesReadOnlyAccess	AWS managed	Provides read only access to all S3 tabl...

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5. Review and Create:

- Name the role (e.g., S3ReadOnlyRole) and click **Create Role**.

aws Search [Alt+S]

IAM > Roles > Create role

Step 1 Select trusted entity
Step 2 Add permissions
Step 3 **Name, review, and create**

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
s3readonly
Maximum 64 characters. Use alphanumeric and '+,=, @, -, _' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/\[\]!#\$%^&*~'`"

Step 1: Select trusted entities [Edit](#)

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::123456789012:role/S3ReadOnlyRole"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 2: Assign Role to an EC2 Instance

1. Launch or Select an EC2 Instance:

- Navigate to **EC2** under Services and either create or select an existing EC2 instance.

2. Modify IAM Role:

- Select the instance, click on **Actions**, choose **Security**, then **Modify IAM Role**.
- Assign the newly created IAM role (e.g., S3ReadOnlyRole) to the instance.
- Save the changes.

The image shows two screenshots of the AWS Management Console. The top screenshot displays the 'Instances' page for the 'i-Of51ad15f88fd5a2a' instance (30jan). The instance is in a 'Running' state. A context menu is open over the instance, showing options like 'Connect', 'View details', 'Manage instance state', 'Instance settings', 'Networking', 'Security', 'Image and templates', and 'Monitor and troubleshoot'. The 'Security' option is highlighted. Below the instance list, the 'Security' tab is selected, showing 'Security details' with 'IAM Role' set to '-', 'Owner ID' as '779846806994', and 'Launch time' as 'Thu Jan 30 2025 17:47:57 GMT+0530 (India Standard Time)'. The bottom screenshot shows the 'Modify IAM role' page for the same instance. It displays the 'Instance ID' as 'i-Of51ad15f88fd5a2a (30jan)' and the 'IAM role' as 's3readonly'. There is a 'Create new IAM role' button and an 'Update IAM role' button.

Step 3: Verify Permissions

1. SSH into the EC2 Instance:

- Connect to the instance via SSH (or EC2 Instance Connect).

2. Install AWS CLI (if not installed):

```
sudo apt-get update
sudo apt-get install awscli
```

3. Test Allowed Actions:

- Run the following command to list S3 buckets (allowed by the assigned role):

```
aws s3 ls
```

You should see a list of S3 buckets because the role has read-only access.

4. Test Denied Actions:

- a. Try to upload a file to an S3 bucket:

```
aws s3 cp testfile.txt s3://bucket-name/
```

This should result in an "Access Denied" error, as the role does not have permission to upload files.

```
login as: ec2-user
Authenticating with public key "jan30"

#_
~\####_      Amazon Linux 2023
~~\#####\
~~\####|
~~\#/      https://aws.amazon.com/linux/amazon-linux-2023
~~V~' '->
~~~
~~.
~~/_/m/' '->

Last login: Thu Jan 30 12:18:52 2025 from 125.17.180.42
[ec2-user@ip-172-31-89-179 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-172-31-89-179 ~]$
```

```
login as: ec2-user
Authenticating with public key "jan30"

#_
~\####_      Amazon Linux 2023
~~\#####\
~~\####|
~~\#/      https://aws.amazon.com/linux/amazon-linux-2023
~~V~' '->
~~~
~~.
~~/_/m/' '->

Last login: Thu Jan 30 12:18:52 2025 from 125.17.180.42
[ec2-user@ip-172-31-89-179 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-172-31-89-179 ~]$ aws s3 ls
[ec2-user@ip-172-31-89-179 ~]$
```

Step 4: Clean Up

1. **Terminate the EC2 Instance** (if no longer needed):
 - a. Navigate to EC2, select the instance, and terminate it.
2. **Delete the IAM Role** (if no longer needed):
 - a. Go to **IAM Roles**, select the created role, and click **Delete Role**.

Outcomes

- Successfully created an IAM role (S3ReadOnlyRole) with restricted permissions.
- Assigned the role to an EC2 instance and verified that it can access permitted resources (S3 read-only) and was denied other actions (uploading to S3).