

## Module 2: Security Management in AWS

---

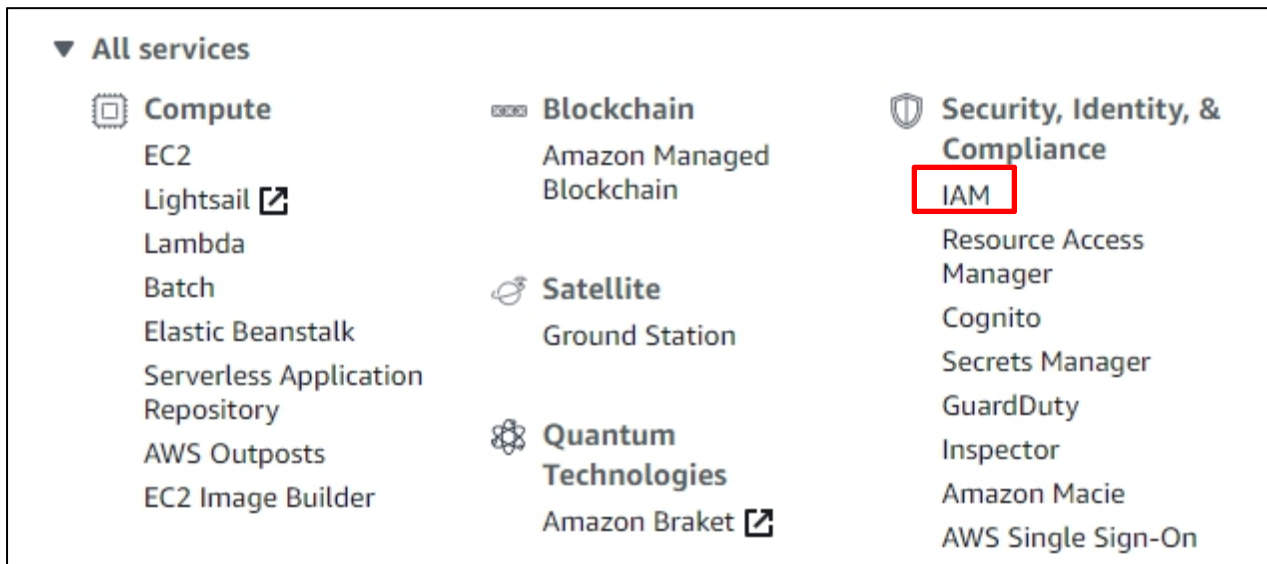
### Demo Document 2

**edureka!**

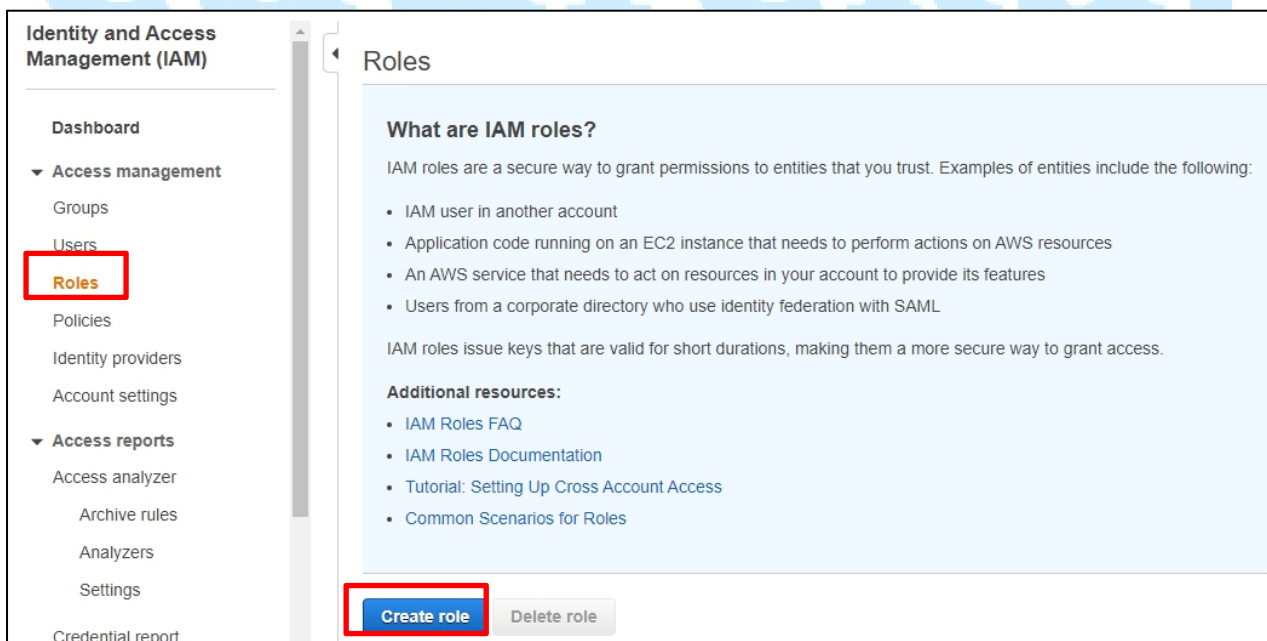
© Brain4ce Education Solutions Pvt. Ltd.

## To Create an IAM Role for Applications on EC2 Instance to Access the S3 Service

**Step 1:** Go to the AWS Management Console and click on the **IAM** service.



**Step 2:** In the left navigation column, select **Roles**, and click on Create Roles.





**Step 3:** Select the service to which you want to attach the Role and click on **Next: Permission** option displayed on the bottom. For the demo, we have selected the EC2 service.


## Create role


1234

### Select type of trusted entity

**AWS service**  
EC2, Lambda and others

**Another AWS account**  
Belonging to you or 3rd party

**Web identity**  
Cognito or any OpenID provider

**SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

### Choose a use case

**Common use cases**

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

**Or select a service to view its use cases**

API Gateway

CodeGuru

ElastiCache

Kinesis

RoboMaker

AWS Backup

CodeStar Notifications

Elastic Beanstalk

Lake Formation

S3

\* Required

Cancel

Next: Permissions

Step 4: Attach the policy and click on **Next Review**.

## Create policy

Filter policies Search Showing 781 results

	Policy name	Used as
<input type="checkbox"/>	AmazonRoute53ReadOnlyAccess	None
<input type="checkbox"/>	AmazonRoute53ResolverFullAccess	None
<input type="checkbox"/>	AmazonRoute53ResolverReadOnlyAccess	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	Permissions policy (3)
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	Permissions policy (1)
<input type="checkbox"/>	AmazonSageMaker-ExecutionPolicy-20180928T161943	Permissions policy (1)
<input type="checkbox"/>	AmazonSageMaker-ExecutionPolicy-20181001T122903	Permissions policy (1)

\* Required

Cancel

Previous

Next: Tags

You can skip the create role optional page by clicking on the Next: Review

## Create role

1234

### Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel Previous Next: Review

**Step 5:** Write a unique name and click on **Create Role**.

## Create role

### Review

Provide the required information below and review this role before you create it.

Role name\*

Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.


Role description

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities

AWS service: ec2.amazonaws.com

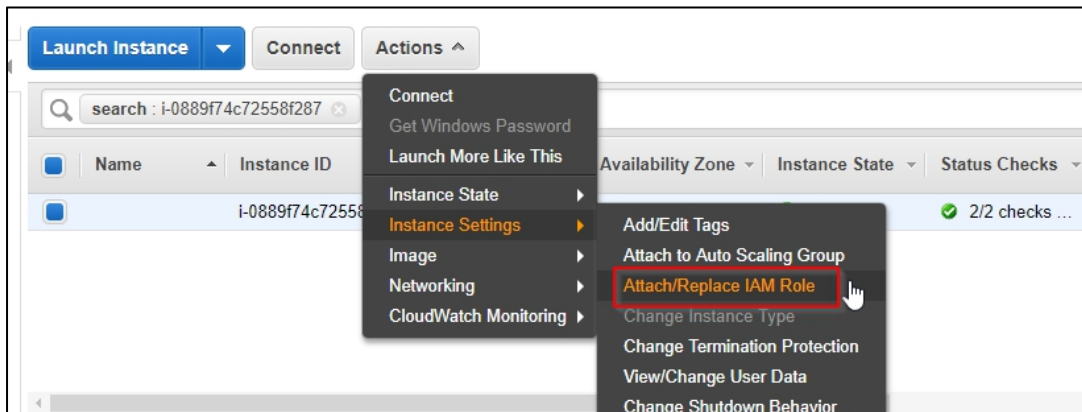
Policies

 [AmazonS3FullAccess](#)

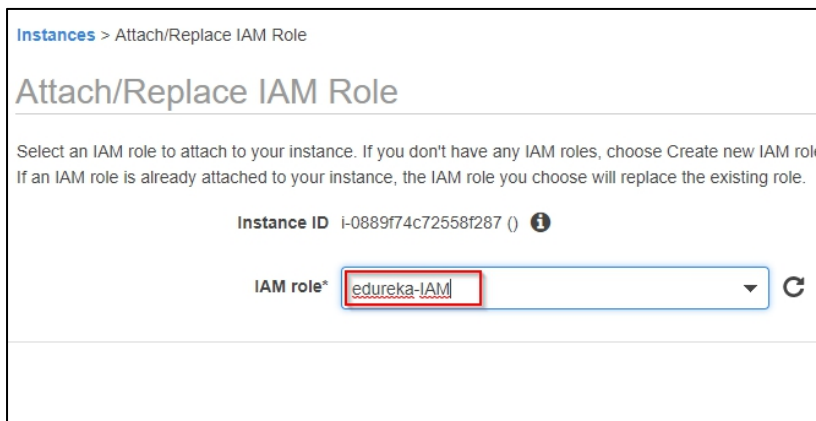
Permissions boundary

Permissions boundary is not set

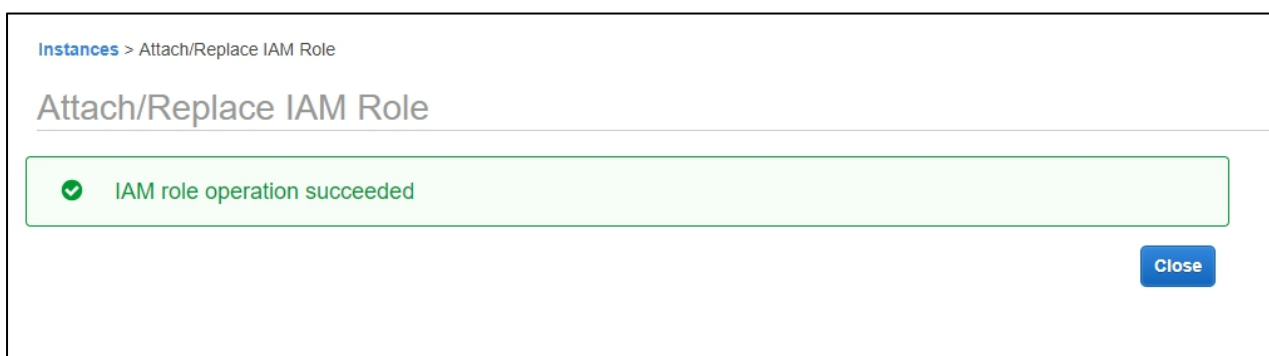
**Step 6:** Go back to the EC2 Instance where your application is running. Select **Actions**, then **Instance Settings**, and click on **Attach IAM Role**.



**Step 7:** From the list of the available Roles, select the Role that you have created. In this case, we have named it as edureka-IAM.



**Step 8:** Once you are done with all your demo steps, you will get to witness the below notification on your screen.



**Conclusion:** You have successfully created an **IAM Role** so that your application can access the S3 service.

edureka!