



## Guidelines for creating Roles in AWS

**Case:** Creating a role for accessing S3 bucket from EC2 instance

### Prerequisites:

- S3 bucket and EC2 instance should be the same region - **N. Virginia.**
- S3 bucket should be available in your account.

1. Edit the security group with my IP before starting the EC2 instance.

2. Select EC2 and click on the security group - **ml-sec**

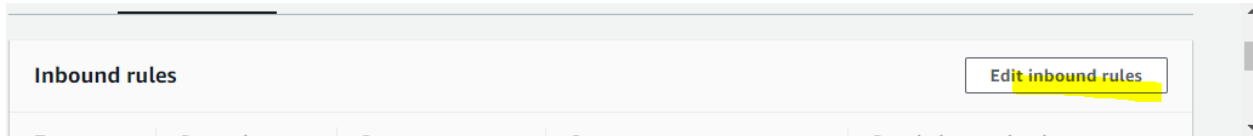
The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a user profile 'ta8@upgrad.com'. The left sidebar shows the 'EC2 Dashboard' and various navigation links. The main content area displays the 'Launch Instance' page for an instance named 'Ubuntu' with ID 'i-0b2e2c6140683d09e'. The instance is a 't2.micro' type in the 'us-east-1d' availability zone, currently in a 'stopped' state. Below the instance details, there is a section for 'Security groups' which lists 'ml-sec' with a link to 'view inbound rules. view outbound rules'.

3. Next, click on **Inbound rules**:

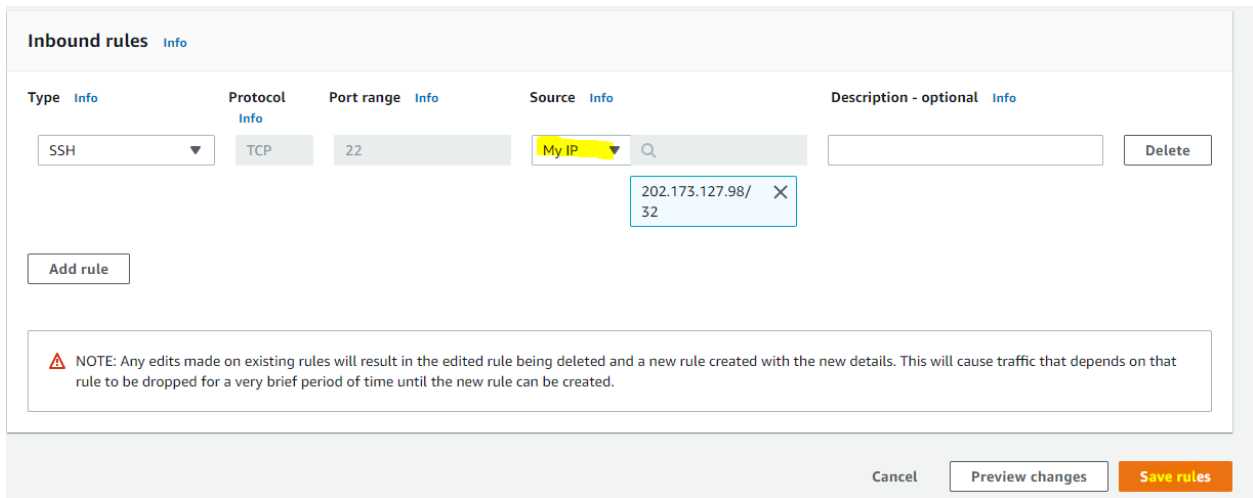
The screenshot shows the 'Security Groups (1/1) Info' page in the AWS Management Console. The 'Inbound rules' tab is selected, showing a table with one rule. The rule has a 'Security group ID' of 'sg-03fc94c28aba725cf', a 'Security group name' of 'ml-sec', a 'VPC ID' of 'vpc-810955fb', a 'Description' of 'ml-sec-group', and an 'Owner' of '5230231083'. The 'Details' tab is also visible at the bottom of the page.



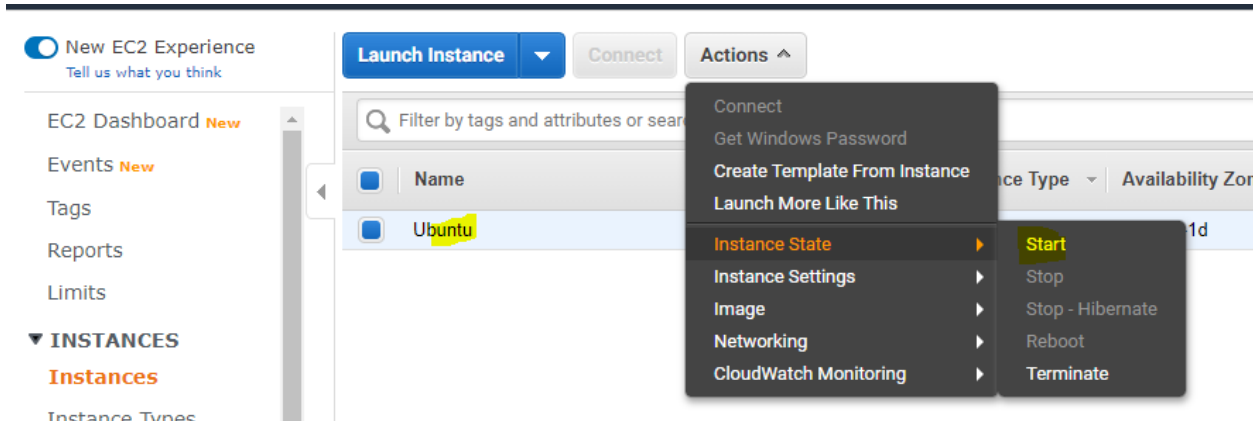
4. Click on **Edit inbound rules**:



5. Edit source with My IP and click on **Save rules**.



6. Navigate back to the EC2 dashboard and **start** the EC2 instance.





New EC2 Experience  
Tell us what you think

Launch Instance Connect Actions

EC2 Dashboard New

Events New

Tags

Reports

Limits

INSTANCES

Instances

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Ubuntu	i-0b2e2c6140683d09e	t2.micro	us-east-1d	running	2/2 checks ...	None	ec2-54-91

7. Then, access the EC2 instance from PuTTY or Linux/MAC shell.

```
ubuntu@ip-172-31-94-99: ~  
login as: ubuntu  
Authenticating with public key "imported-openssh-key"  
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information disabled due to load higher than 1.0  
  
* Kubernetes 1.18 GA is now available! See https://microk8s.io for docs or  
install it with:  
  
    sudo snap install microk8s --channel=1.18 --classic  
  
* Multipass 1.1 adds proxy support for developers behind enterprise  
firewalls. Rapid prototyping for cloud operations just got easier.  
  
    https://multipass.run/  
  
49 packages can be updated.  
22 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-94-99:~$
```

8. Run below command and access s3 bucket from instance.

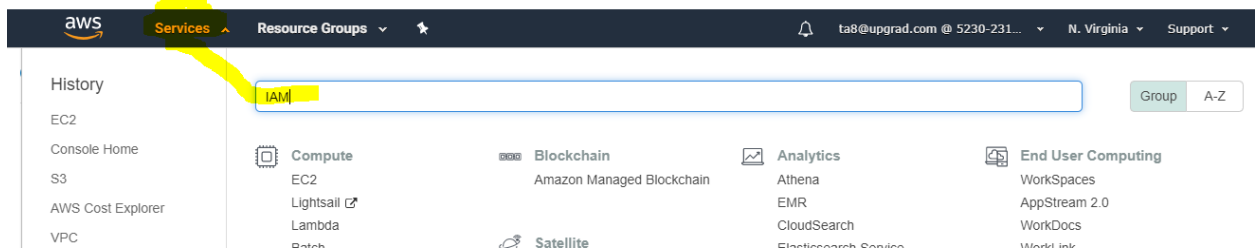
```
sudo apt-get update  
sudo apt-get install awscli
```



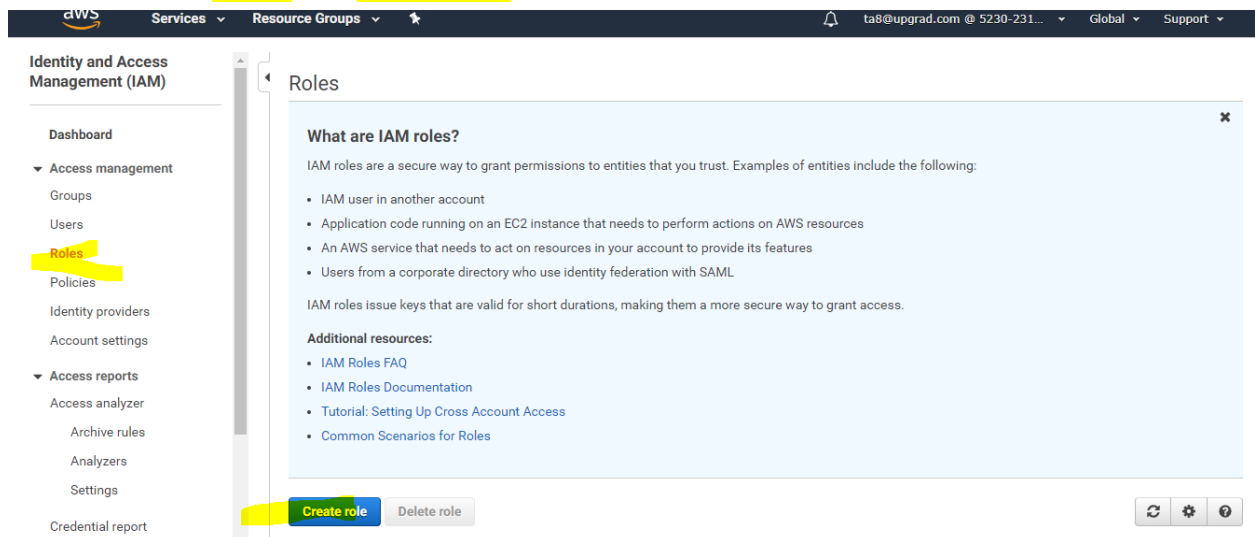
9. Enter **aws s3 ls**

```
ubuntu@ip-172-31-94-99:~$ aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
ubuntu@ip-172-31-94-99:~$
```

10. Presently, you are not able to access the bucket. Go back to the AWS management console and search for the **IAM** service.



11. Click on **Roles** and **Create role**.








12. Select **EC2** in the use case list and click on **Next Permissions**.


Create role 1 2 3 4

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

CodeDeploy

EMR

KMS

RoboMaker

AWS Backup

CodeGuru

ElastiCache

Kinesis

S3

\* Required Cancel Next: Permissions

13. In the search tab, search policy **s3full** and select the checkbox for **AmazonS3full access**.

Policy- AmazonS3FullAccess

Create role 1 2 3 4

▼ Attach permissions policies

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

Create policy ↺

Filter policies  Showing 1 result

	Policy name	Used as
<input checked="" type="checkbox"/>	AmazonS3FullAccess	None

14. Click on Next numbered tab



## Create role

1 2 3 4

### 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.

15. Give the role name: **s3\_access\_role** and click on create role.

## Create role

1 2 3 4

### 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

No tags were added.

\* Required

Cancel

Previous

Create role

16. Navigate back to the EC2 service.

aws

Services

Resource Groups

ta8@upgrad.com @ 5230-231...

Global

SU

History

IAM

EC2

Console Home

S3

AWS Cost Explorer

VPC

Find a service by name or feature (for example, EC2, S3 or VM, storage)

Group

Compute

EC2

Lightsail

Lambda

Batch

Elastic Beanstalk

Serverless Application Repository

AWS Outposts

EC2 Image Builder

Blockchain

Amazon Managed Blockchain

Satellite

Ground Station

Quantum Technologies

Amazon Braket

Analytics

Athena

EMR

CloudSearch

Elasticsearch Service

Kinesis

QuickSight

Data Pipeline

AWS Data Exchange

AWS Glue

End User Computing

WorkSpaces

AppStream 2.0

WorkDocs

WorkLink

Internet Of Things

IoT Core

FreeRTOS



17. Go to EC2 instance> Action> instance setting> **Attach/Replace IAM role**

The screenshot shows the AWS Management Console interface. On the left, the 'INSTANCES' section is expanded. In the center, a table lists EC2 instances, with one instance selected. A context menu is open over the instance, showing various actions. The 'Instance Settings' option is selected, and a submenu is displayed with 'Attach/Replace IAM Role' highlighted in yellow.

18. Select your role: **s3\_access\_role** and **Apply**.

### Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

The screenshot shows the 'Attach/Replace IAM Role' dialog box. The 'Instance ID' is 'i-0b2e2c6140683d09e (Ubuntu)'. The 'IAM role\*' dropdown is open, showing a list of roles: 'No Role', 'EMR\_EC2\_DefaultRole', and 's3\_access\_role'. The 's3\_access\_role' is highlighted. The 'Apply' button is highlighted in yellow.

Instances > Attach/Replace IAM Role

### Attach/Replace IAM Role

The screenshot shows a green success message box with a checkmark icon and the text 'IAM role operation succeeded'. A 'Close' button is located at the bottom right of the box.

19. Switch back to the instance terminal.

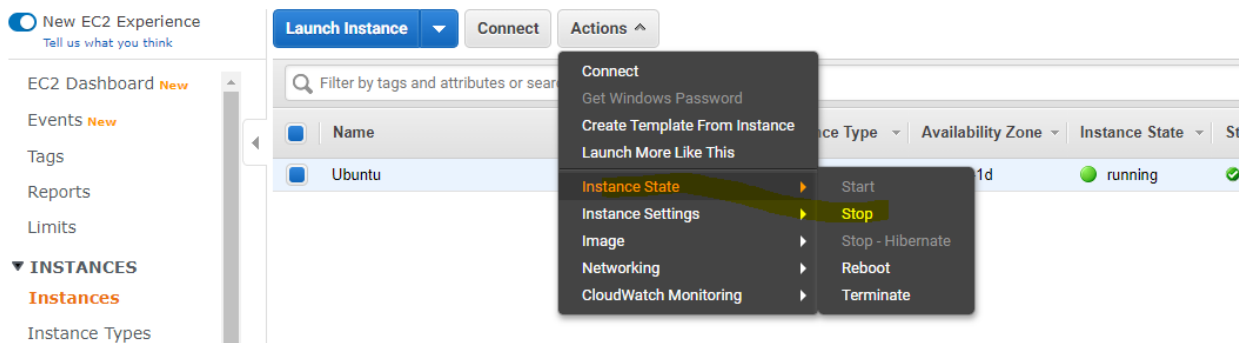
**aws s3 ls**



```
ubuntu@ip-172-31-94-99:~$ aws s3 ls
2020-01-23 06:08:10 test-agaw
2020-04-08 06:00:58 upgrad-123
ubuntu@ip-172-31-94-99:~$
```

You can view the contents of the S3 bucket now.

**Note:** Please stop the instance when not in use or save the budget. If the instance is no longer required, terminate the instance.



Please verify the instance status - **Stopped** with Red.