Guidelines for creating Roles in AWS

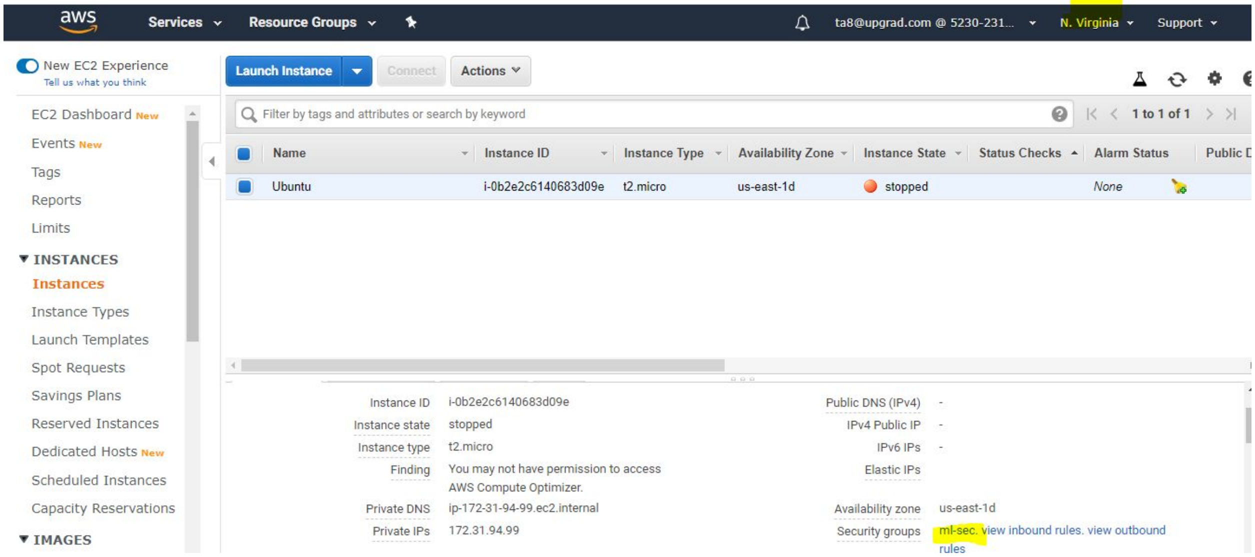
Case: Creating a role for accessing S3 bucket from EC2 instance

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.

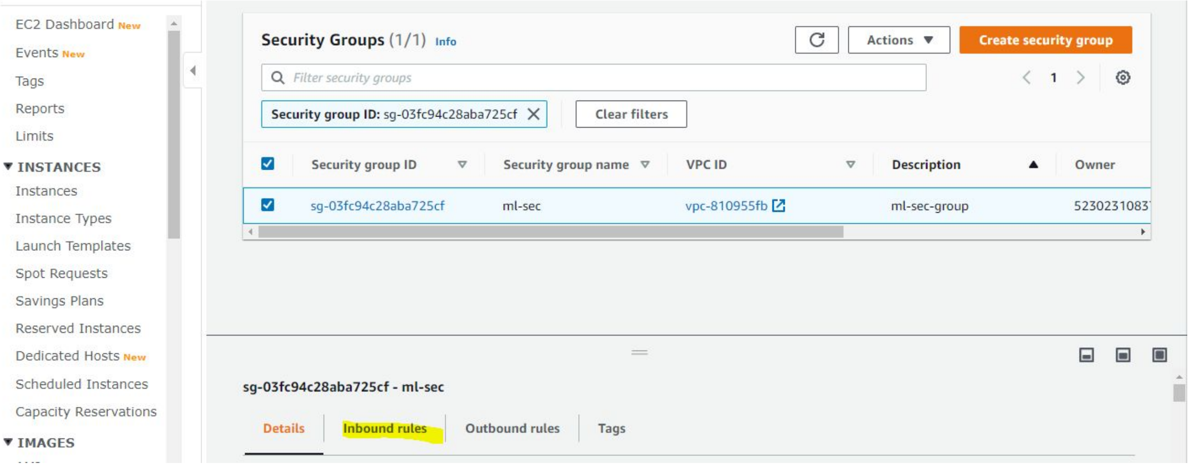
2. Select EC2 and click on the security group - **ml-sec**



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public D
Ubuntu	i-0b2e2c6140683d09e	t2.micro	us-east-1d	stopped		None	

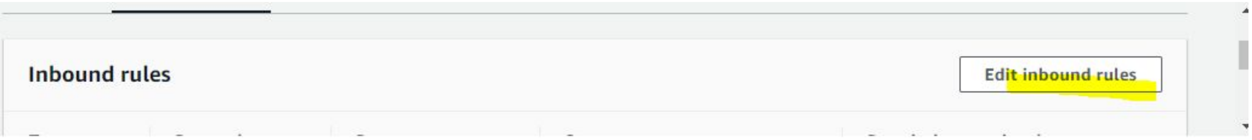
Instance ID	i-0b2e2c6140683d09e	Public DNS (IPv4)	-
Instance state	stopped	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	
Private DNS	ip-172-31-94-99.ec2.internal	Availability zone	us-east-1d
Private IPs	172.31.94.99	Security groups	ml-sec. view inbound rules. view outbound rules

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

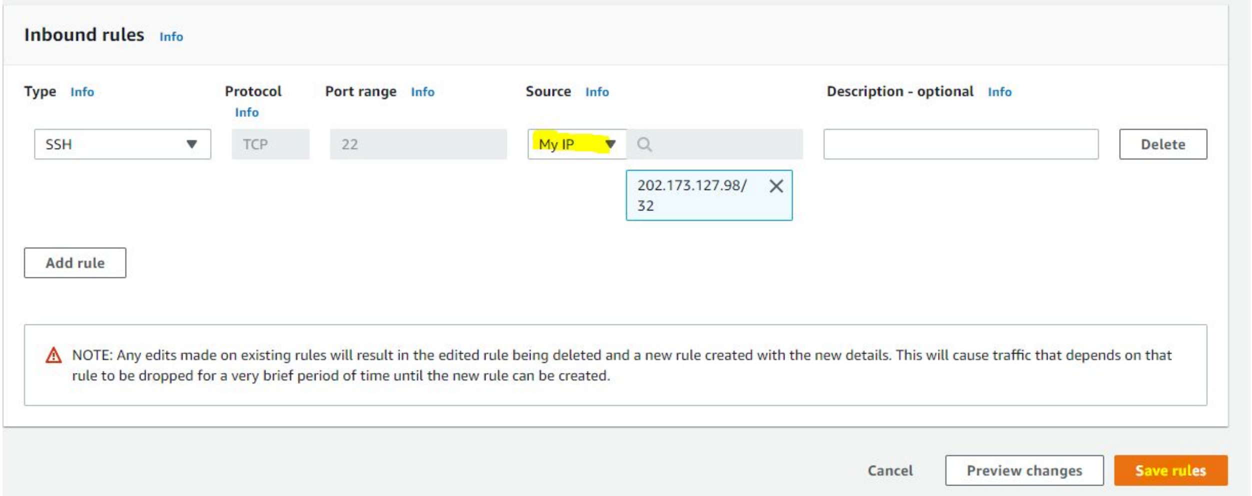


	Security group ID	Security group name	VPC ID	Description	Owner
☑	sg-03fc94c28aba725cf	ml-sec	vpc-810955fb	ml-sec-group	5230231083

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



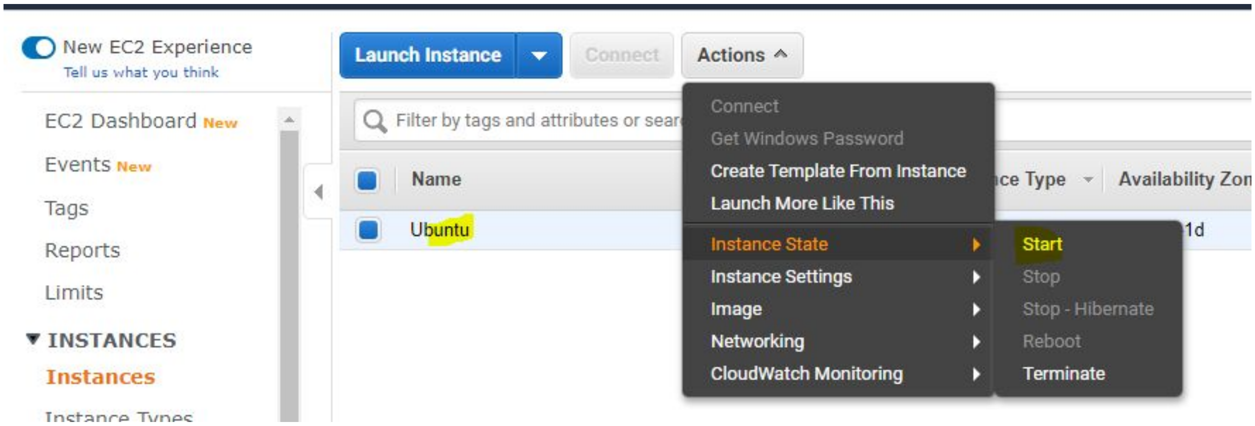
5. Edit source with My IP and click on **Save rules**.

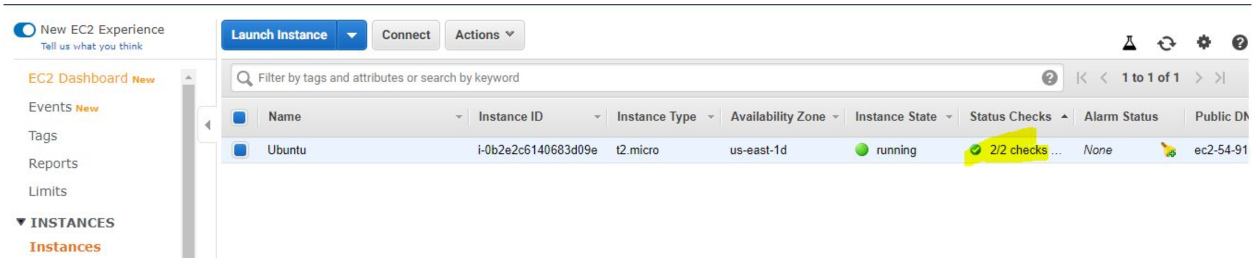


Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	My IP 202.173.127.98/32	

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

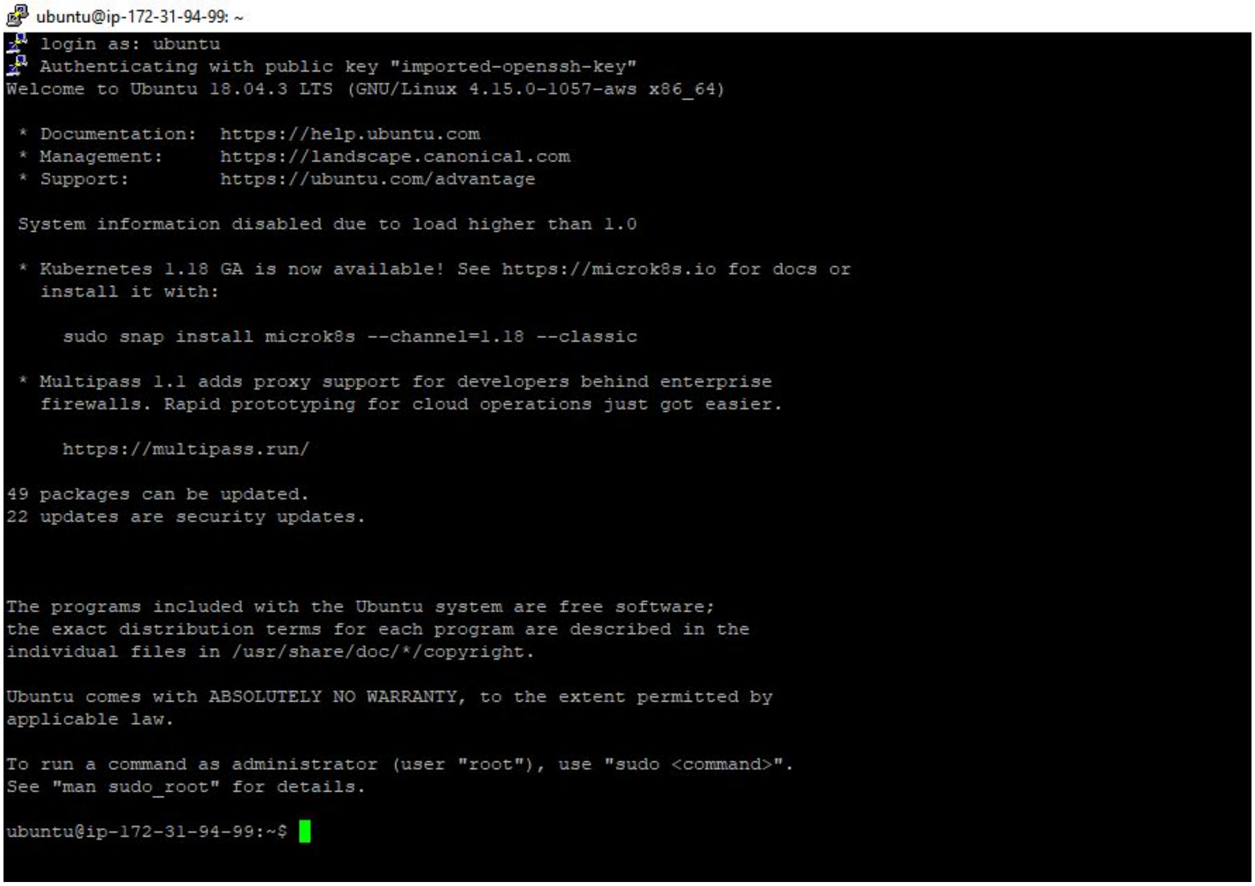
6. Navigate back to the EC2 dashboard and **start** the EC2 instance.





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

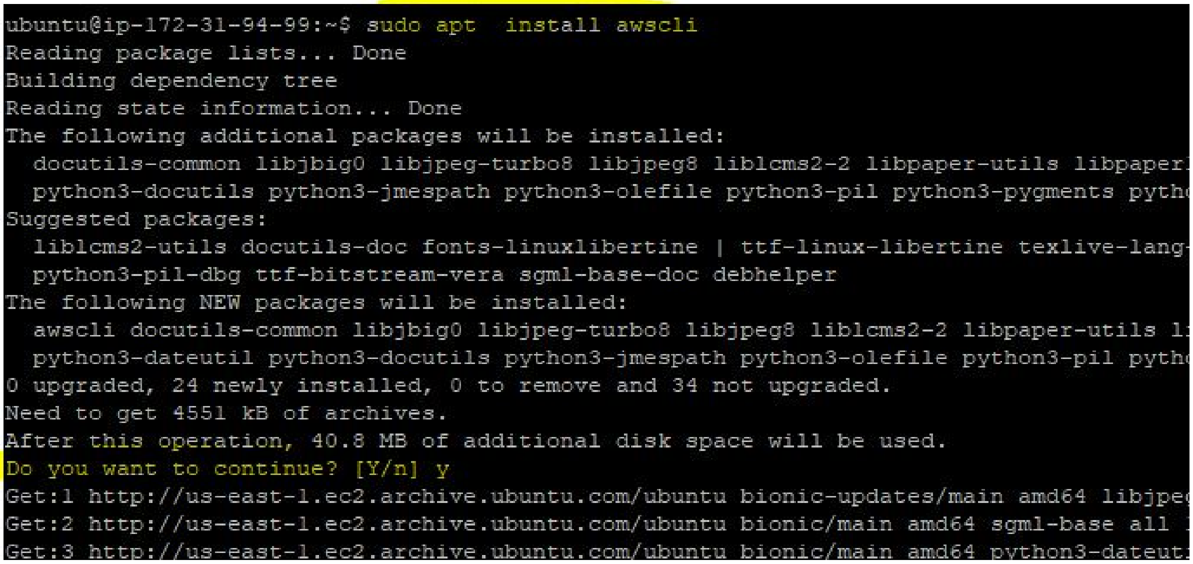
7. Then, access the EC2 instance from PuTTy or Linux/MAC shell.



```
 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:~$
```

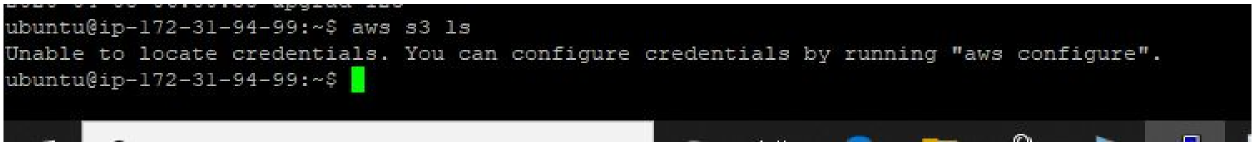
8. Run below command and access s3 bucket from instance.

sudo apt install awscli



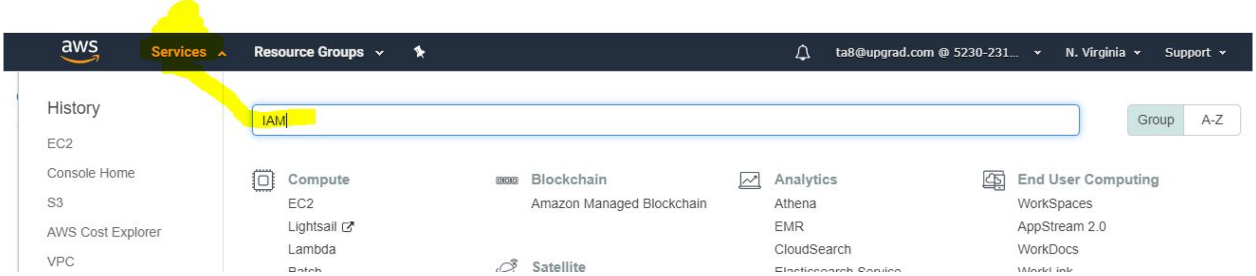
```
ubuntu@ip-172-31-94-99:~$ sudo apt  install awscli
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docutils-common libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2 libpaper-utils libpaper
  python3-docutils python3-jmespath python3-olefile python3-pil python3-pygments pytho
Suggested packages:
  liblcms2-utils docutils-doc fonts-linuxlibertine | ttf-linux-libertine texlive-lang-
  python3-pil-dbg ttf-bitstream-vera sgml-base-doc debhelper
The following NEW packages will be installed:
  awscli docutils-common libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2 libpaper-utils li
  python3-dateutil python3-docutils python3-jmespath python3-olefile python3-pil pytho
0 upgraded, 24 newly installed, 0 to remove and 34 not upgraded.
Need to get 4551 kB of archives.
After this operation, 40.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libjpeg
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/main amd64 sgml-base all 1
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic/main amd64 python3-dateut
```

9. Enter **aws s3 ls**



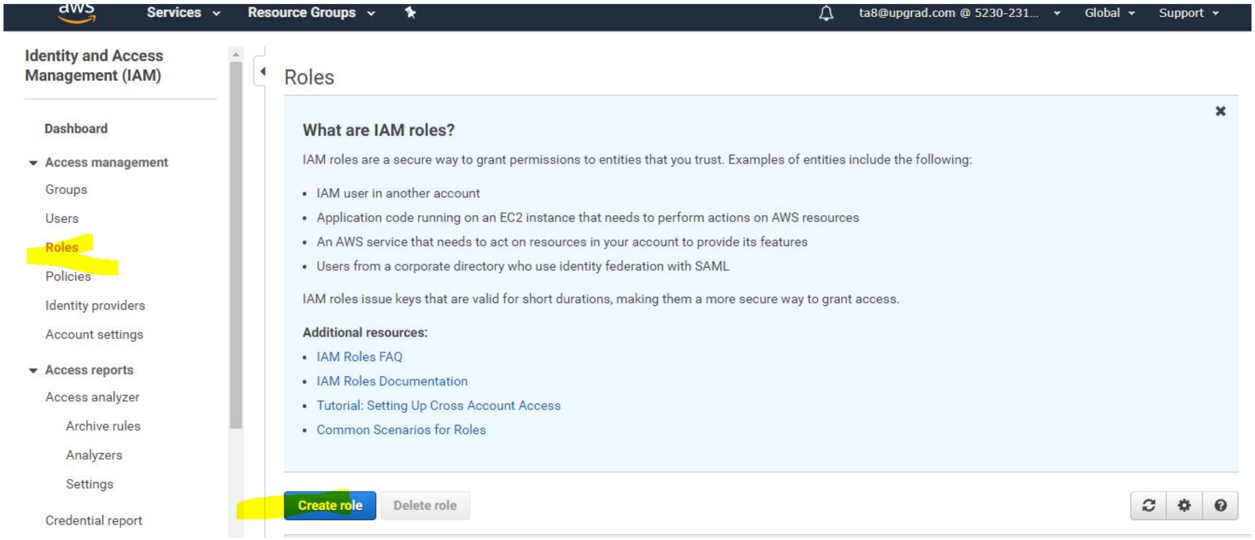
```
ubuntu@ip-172-31-94-99:~$ aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
ubuntu@ip-172-31-94-99:~$
```

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



IAM

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



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

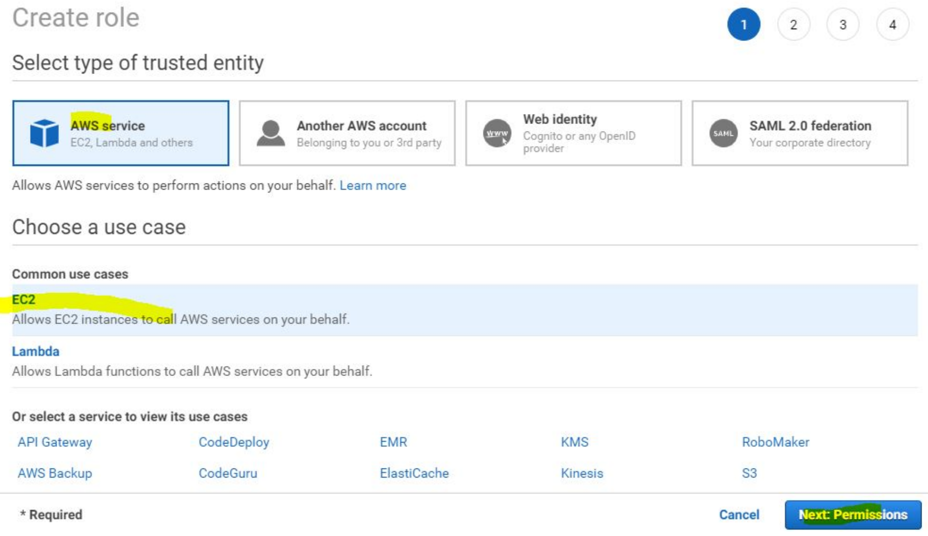
- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

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



Select type of trusted entity

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

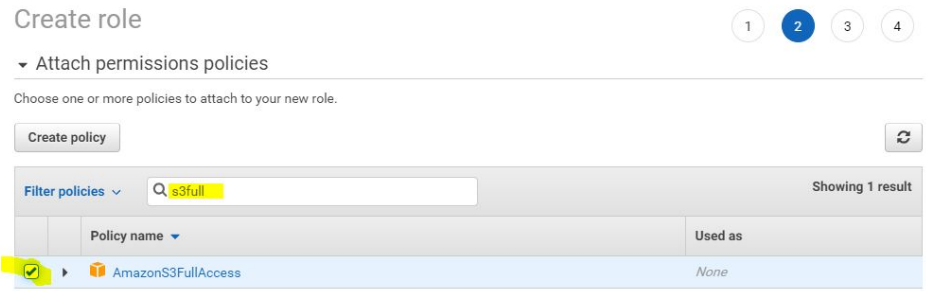
EC2
Allows EC2 instances to call AWS services on your behalf.

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

Or select a service to view its use cases

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

    Policy- AmazonS3FullAccess



Create role

Attach permissions policies

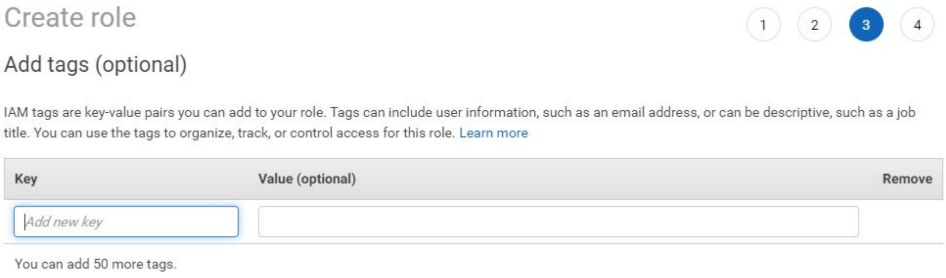
Choose one or more policies to attach to your new role.

s3full

Showing 1 result

		Policy name	Used as
☑	▸	AmazonS3FullAccess	None

14. Click on Next numbered tab



Create role

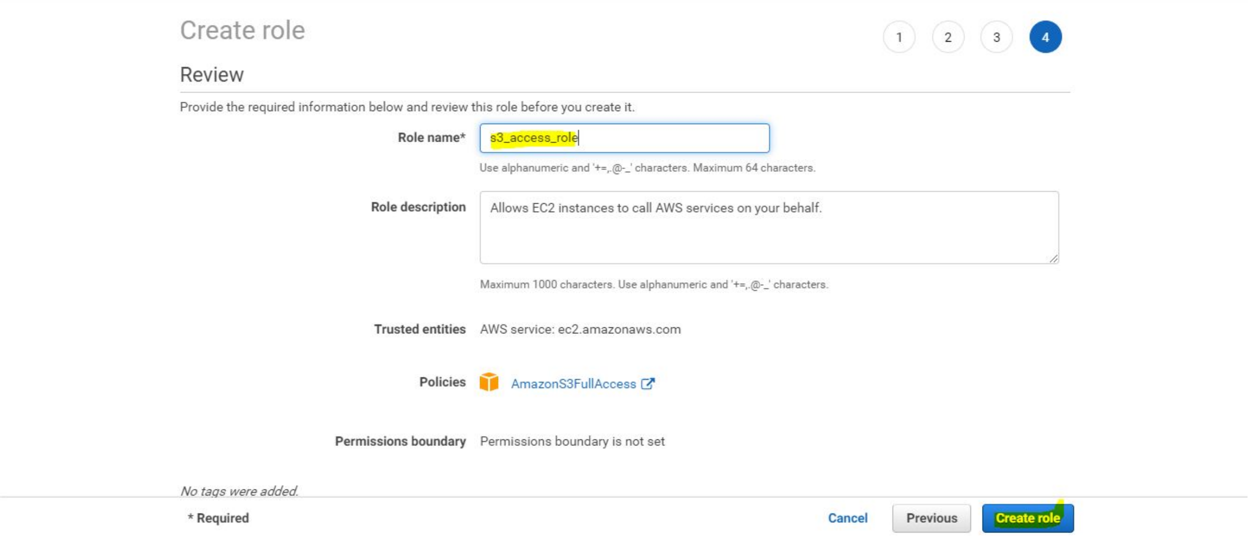
Add tags (optional)

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
Add new key		

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* s3_access_role

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

Role description Allows EC2 instances to call AWS services on your behalf.

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

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess

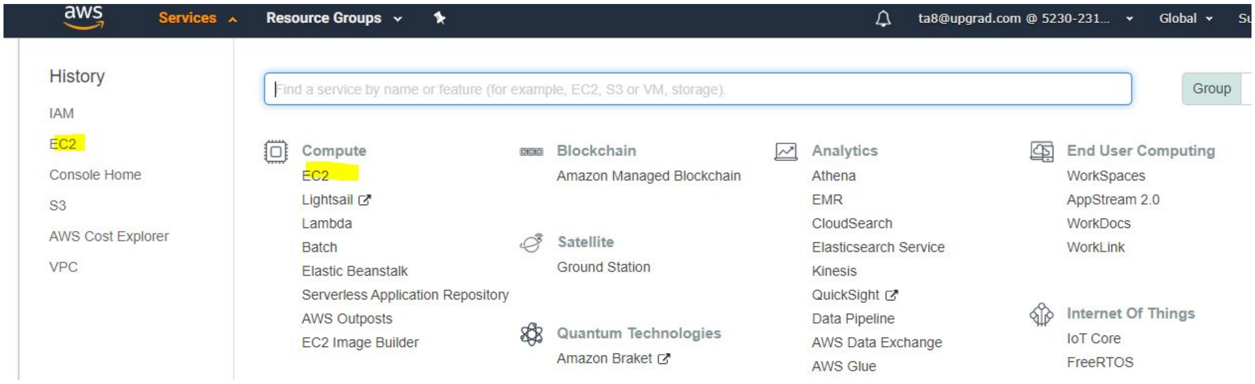
Permissions boundary Permissions boundary is not set

No tags were added.

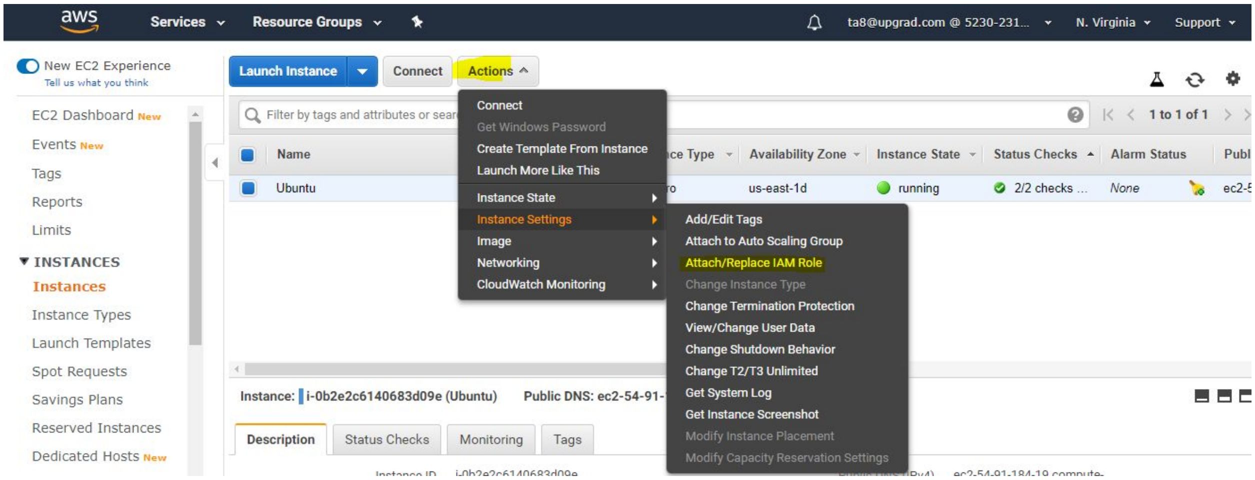
* Required

Cancel Previous Create role

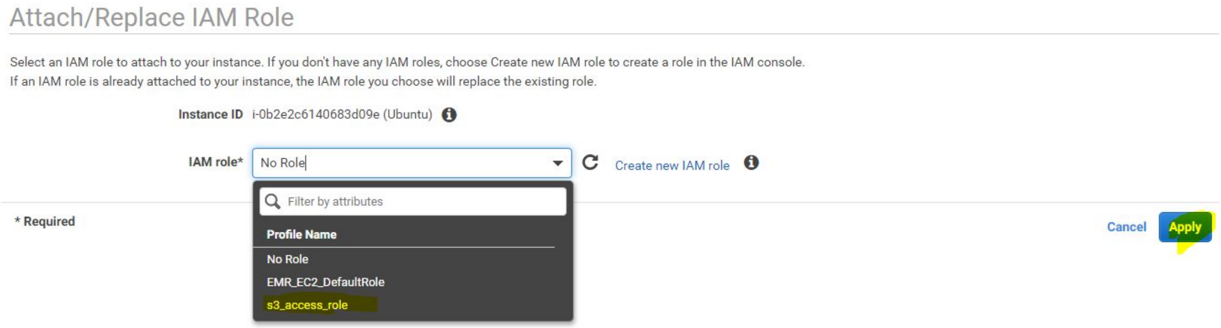
16. Navigate back to the EC2 service.



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



18. Select your role: **s3_access_role** and **Apply**.



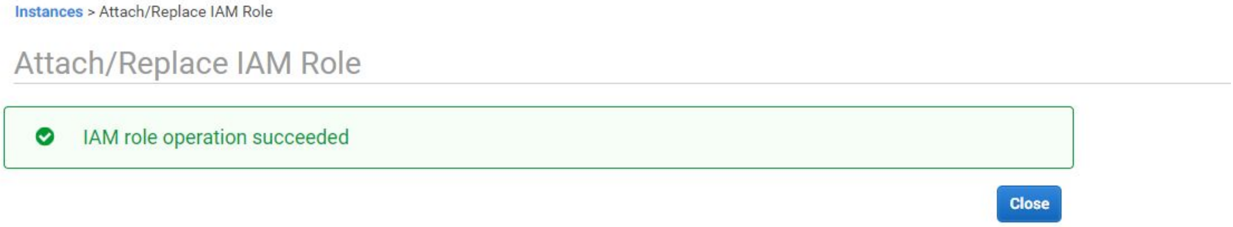
Attach/Replace IAM Role

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.

Instance ID i-0b2e2c6140683d09e (Ubuntu)

IAM role* No Role

* Required



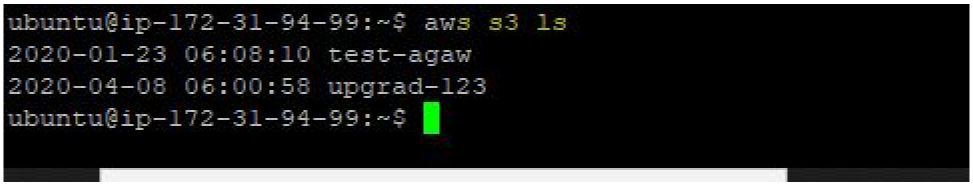
Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

IAM role operation succeeded

19. Switch back to the instance terminal.

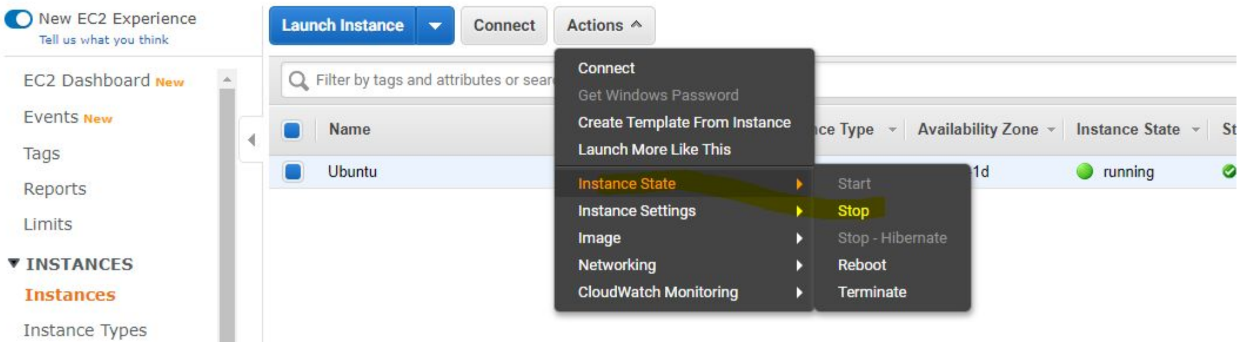
aws s3 ls



```
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.