D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Infrastructure Orchestration (P)

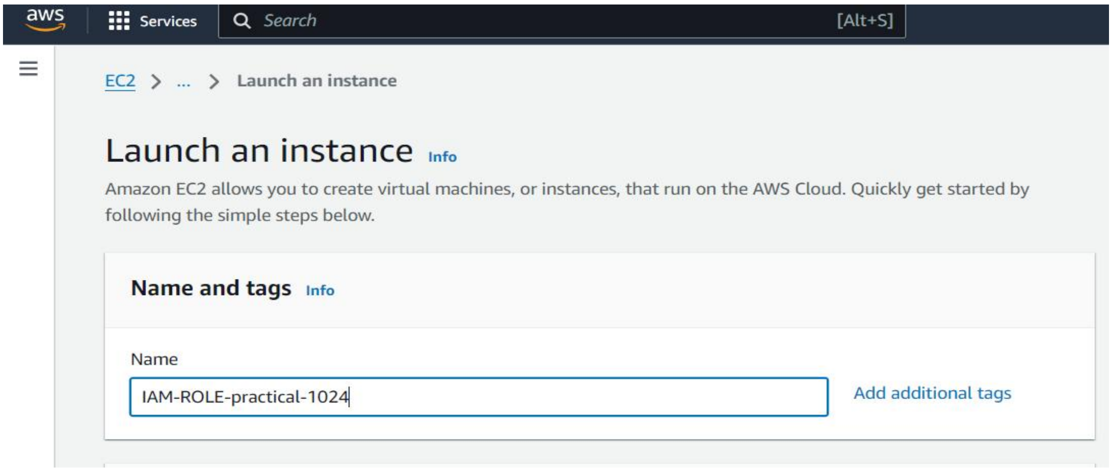
Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practical: **Enabling EC2 Instance Access to S3 Buckets**

STEP1: LOG IN AND create one ec2 instance

Go to EC2 service and launch one instance

Name--(IAM-ROLE-practical-1024)



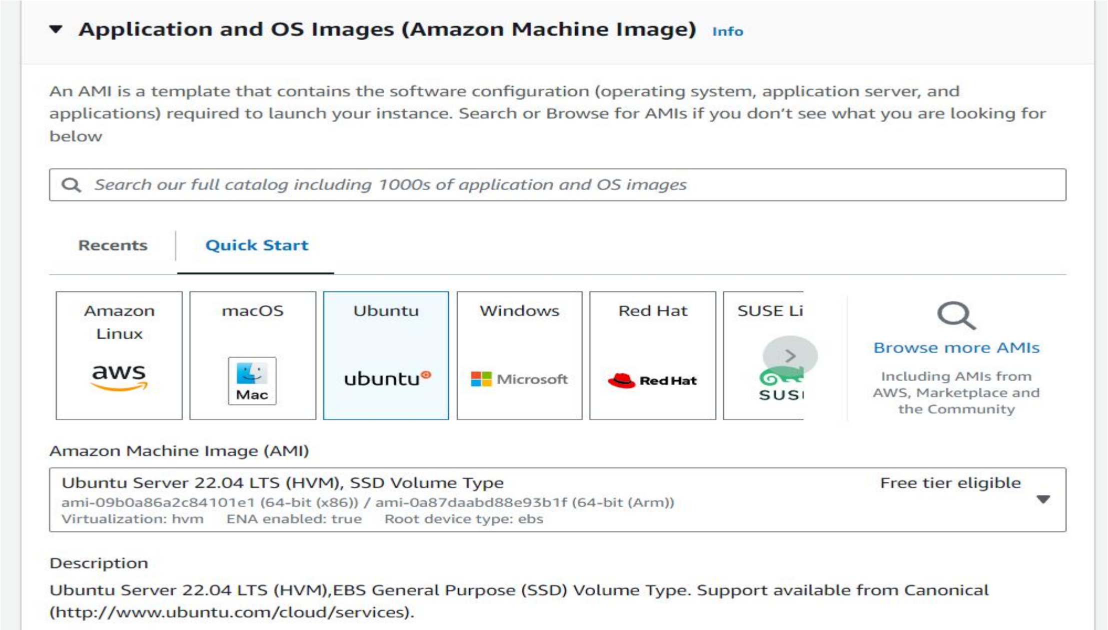
Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: IAM-ROLE-practical-1024

AMI---ubuntu linux


Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUSE
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

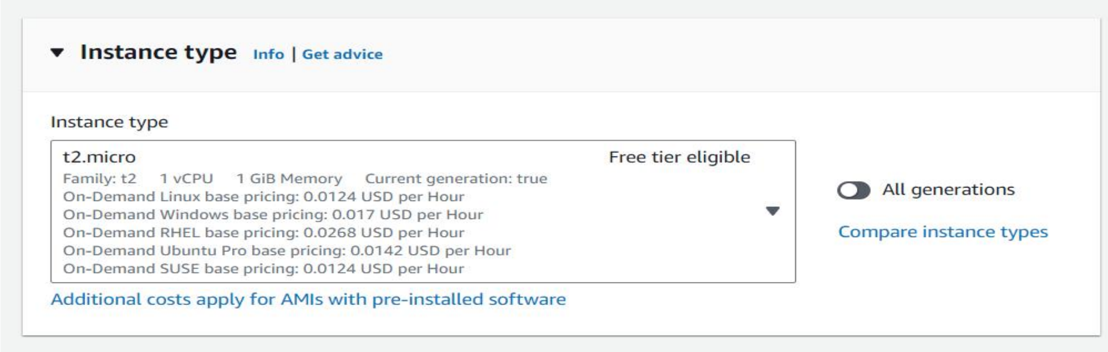
Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-09b0a86a2c84101e1 (64-bit (x86)) / ami-0a87daabd88e93b1f (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 22.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Instance type--- t2.micro



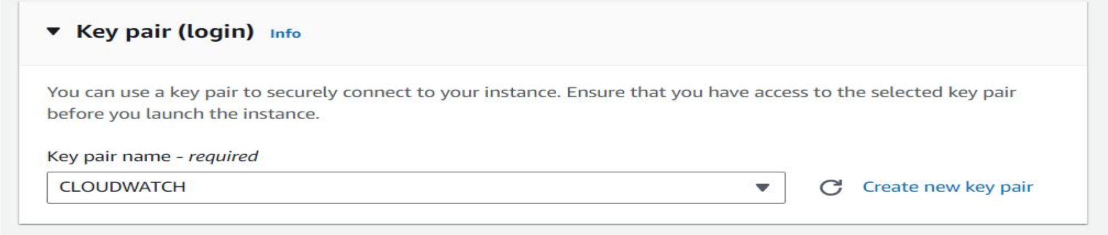
▾ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

Attach keypair or create new one.



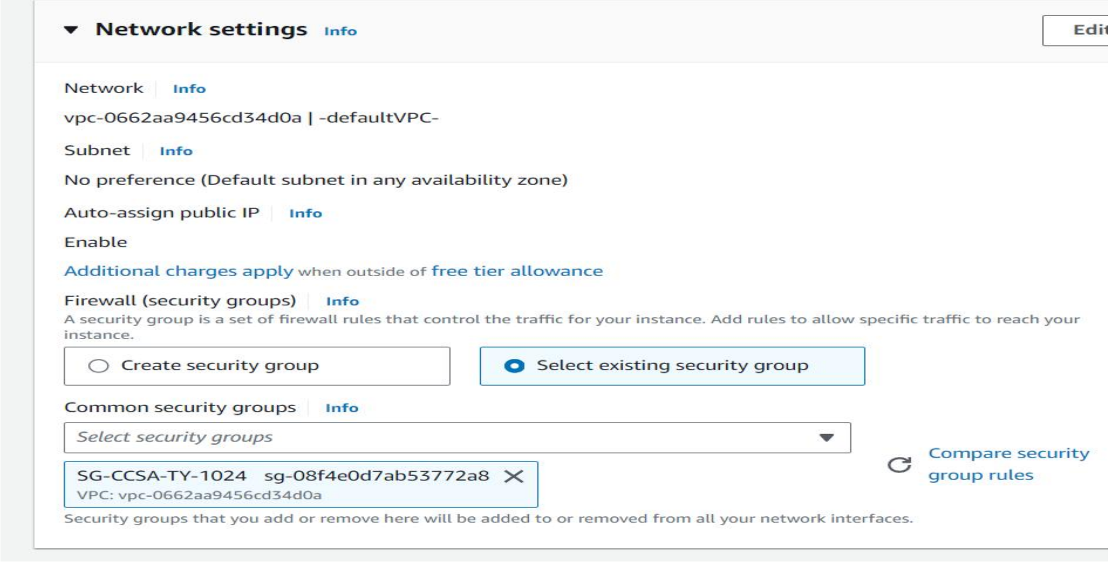
▾ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

CLOUDWATCH

Attach or create new security group(allow ssh and http)



▾ Network settings Info

Network Info
vpc-0662aa9456cd34d0a | -defaultVPC-

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info
Select security groups

SG-CCSA-TY-1024 sg-08f4e0d7ab53772a8 ✕
VPC: vpc-0662aa9456cd34d0a

Security groups that you add or remove here will be added to or removed from all your network interfaces.

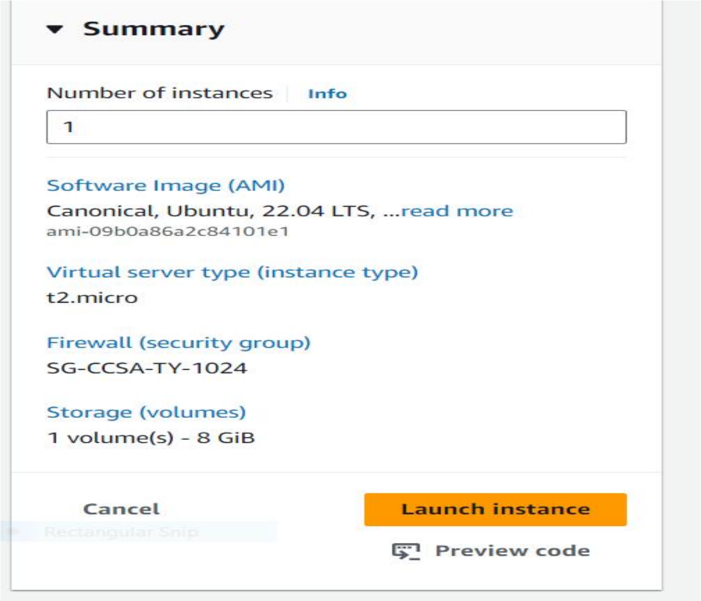
D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Infrastructure Orchestration (P)

Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practical: **Enabling EC2 Instance Access to S3 Buckets**

Launch instance



▼ Summary

Number of instances Info

1

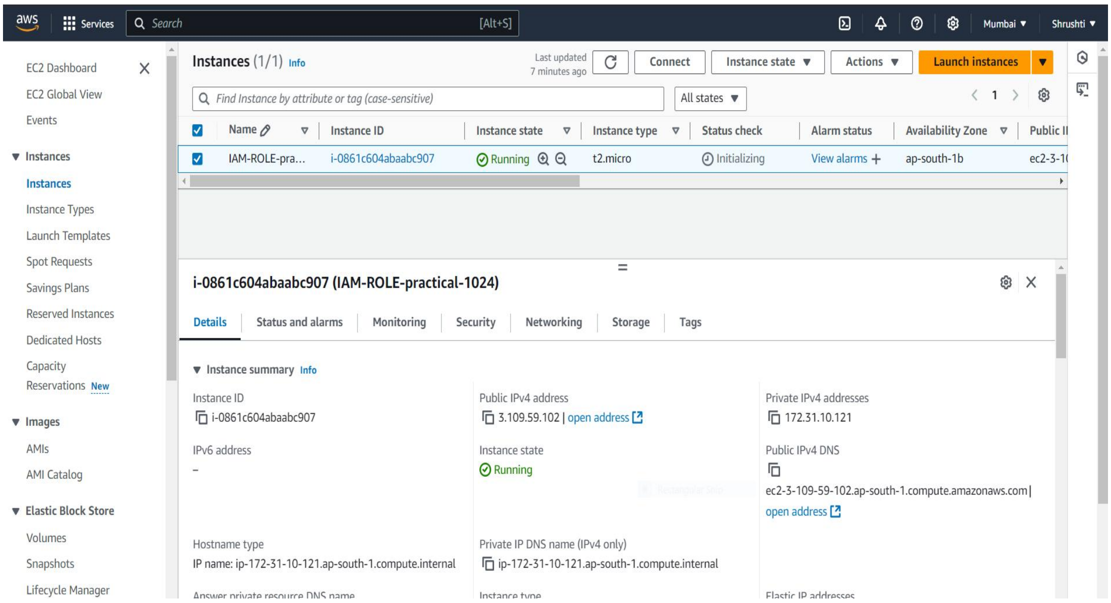
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-09b0a86a2c84101e1

Virtual server type (instance type)
t2.micro

Firewall (security group)
SG-CCSA-TY-1024

Storage (volumes)
1 volume(s) - 8 GiB

Our instance is created



Instances (1/1) Info

Last updated 7 minutes ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public I
☑	IAM-ROLE-pra...	i-0861c604abaabc907	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-3-1

i-0861c604abaabc907 (IAM-ROLE-practical-1024)

▼ Instance summary Info

Instance ID
i-0861c604abaabc907

Public IPv4 address
3.109.59.102 | open address

Private IPv4 addresses
172.31.10.121

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-109-59-102.ap-south-1.compute.amazonaws.com | open address

Hostname type
IP name: ip-172-31-10-121.ap-south-1.compute.internal

Private IP DNS name (IPv4 only)
ip-172-31-10-121.ap-south-1.compute.internal

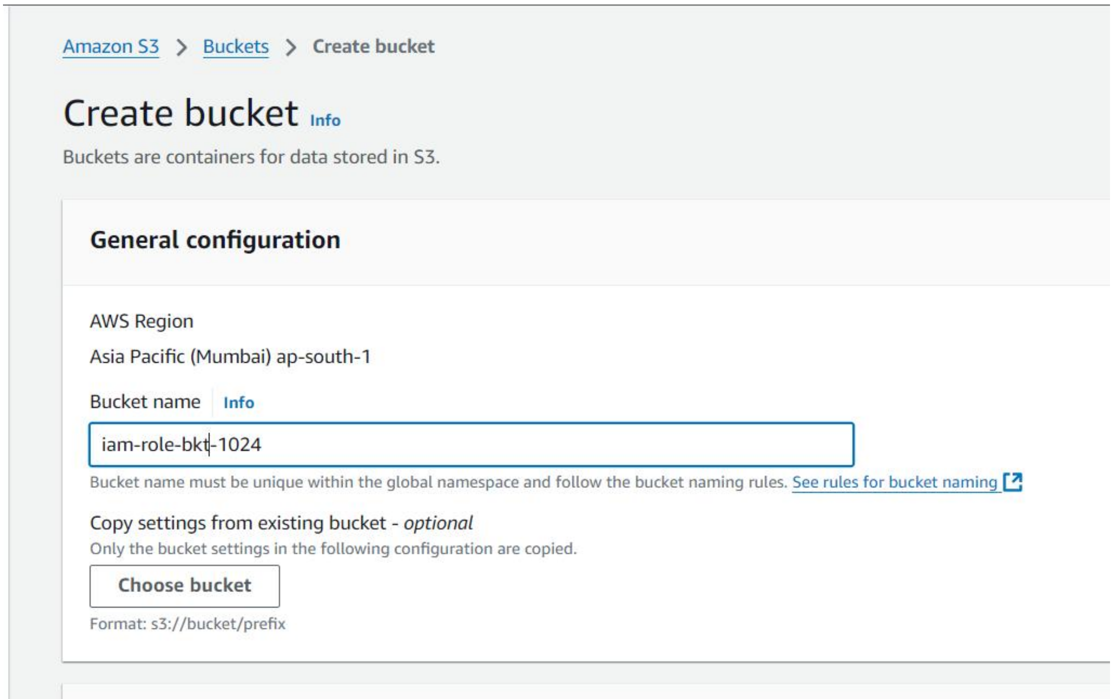
Answer private resource DNS name

Instance type

Elastic IP addresses

STEP2: Now create one s3 bucket--

Name--iam-role-bkt-1024



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name Info
iam-role-bkt-1024

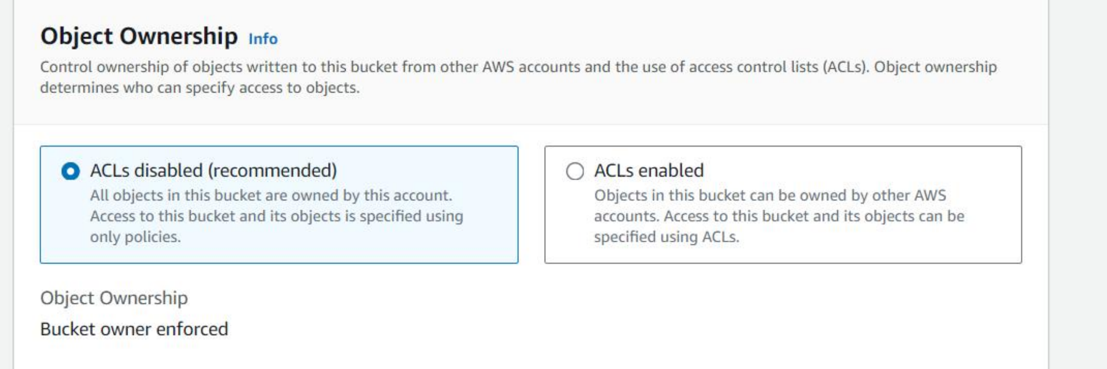
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

Ownership--- ACLs disabled



Object Ownership Info

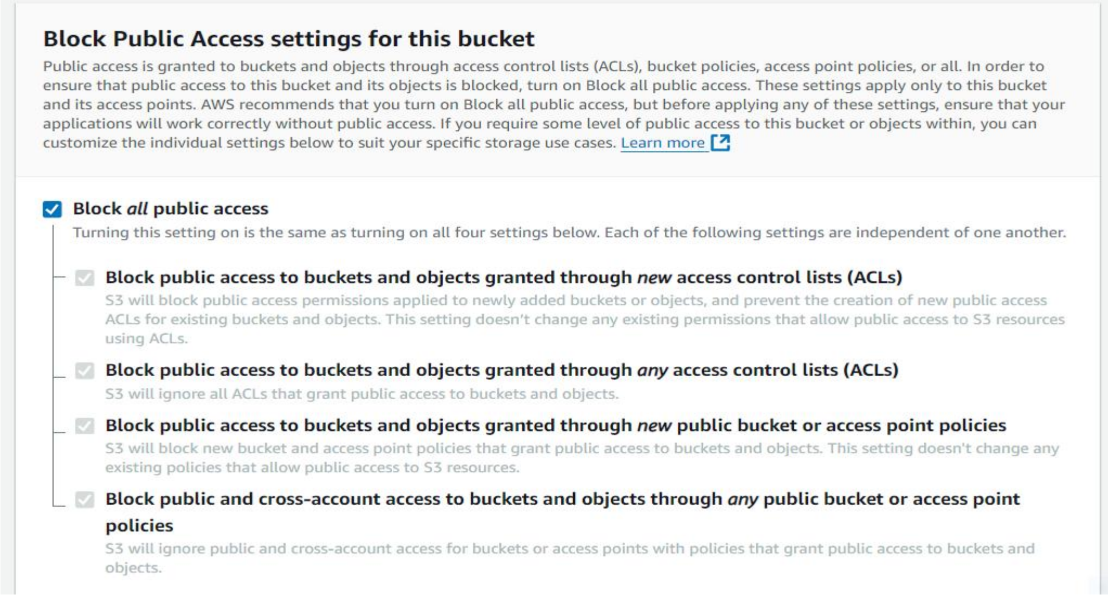
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block all public access



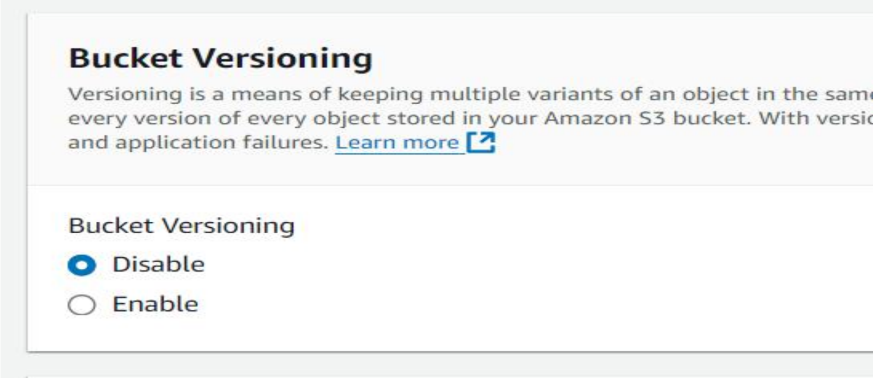
Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket versioning is disabled

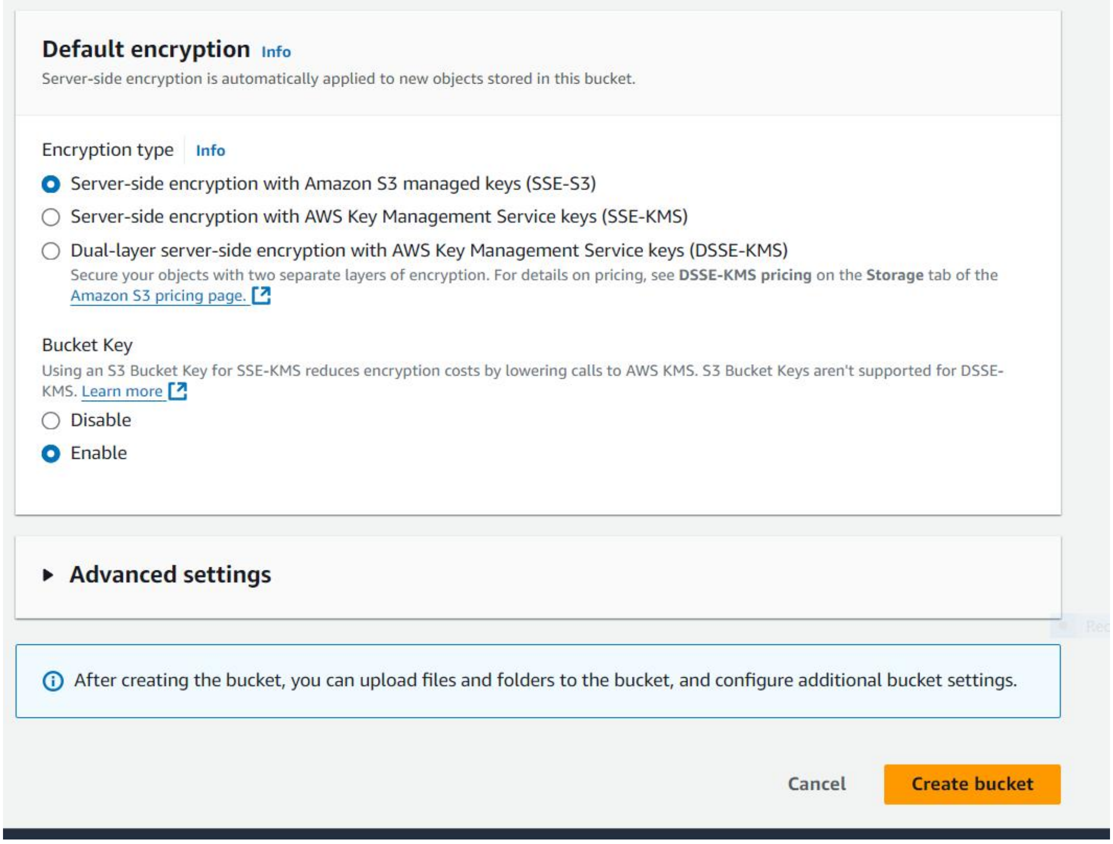


Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the sam
every version of every object stored in your Amazon S3 bucket. With versic
and application failures. Learn more

Bucket Versioning
● Disable
○ Enable

Default setting---



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | Info

- ● Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
  Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key

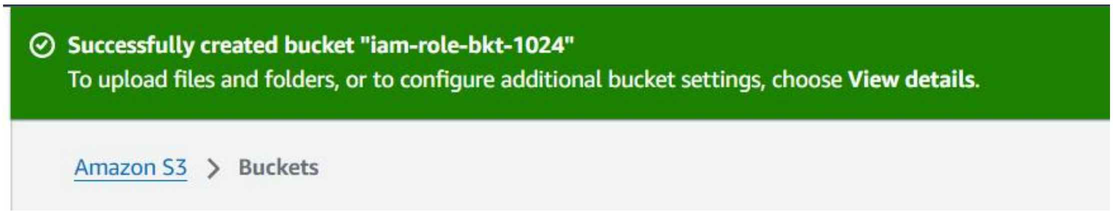
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

- ○ Disable
- ● Enable

▸ **Advanced settings**

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Bucket created.



Successfully created bucket "iam-role-bkt-1024"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

STEP3: Install AWS CLI on ec2 instance--

Note: Before running the aws S3 ls command, ensure you've created at least one empty S3 bucket via the AWS Management Console to see results.

Run the following commands to install the AWS CLI:

- sudo apt install unzip

- curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"

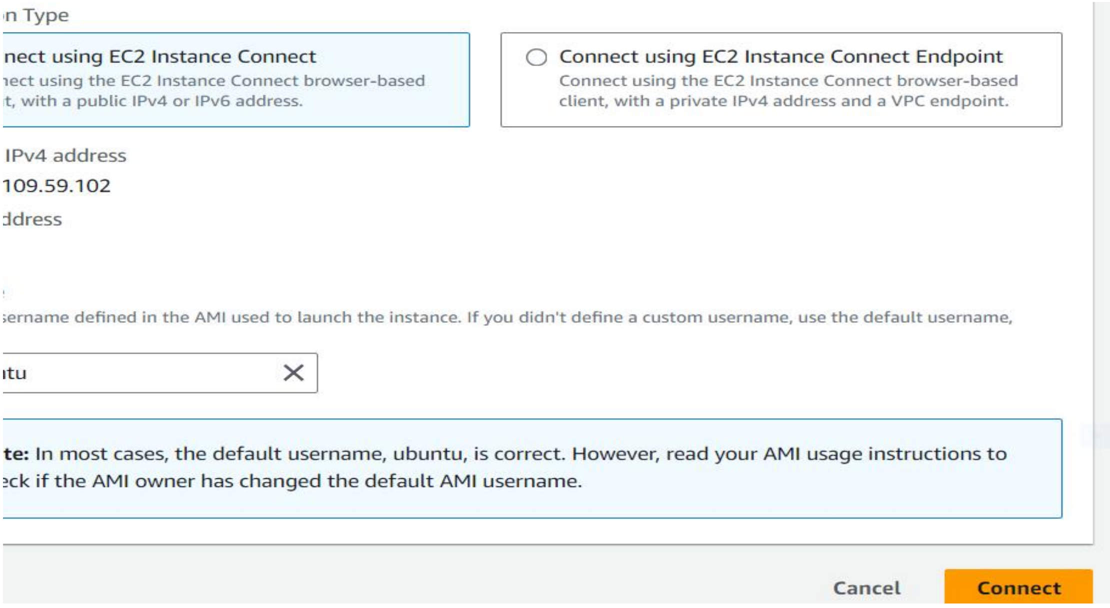
- unzip awscliv2.zip

- sudo ./aws/install

- aws --version

- aws s3 ls [To check S3 buckets (none should appear yet)] basically this command will give error because it does not have permissions to access s3.

Now connect your instance and run the above commands in terminal---



n Type

nect using EC2 Instance Connect
nect using the EC2 Instance Connect browser-based
t, with a public IPv4 or IPv6 address.

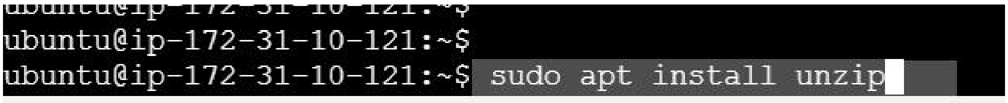
○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

IPv4 address
109.59.102
ddress

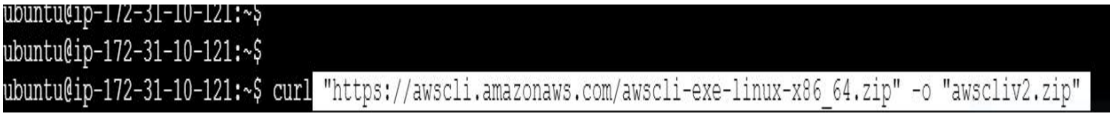
sername defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username,

itu

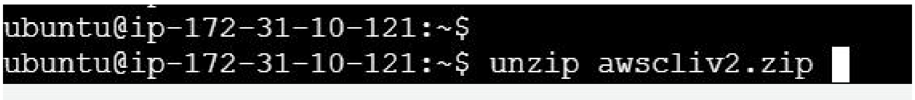
te: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to eck if the AMI owner has changed the default AMI username.



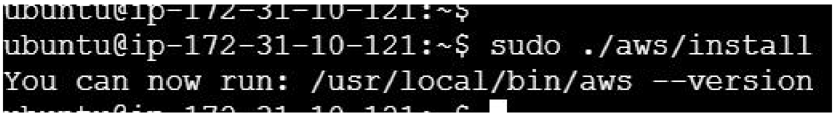
```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ sudo apt install unzip
```



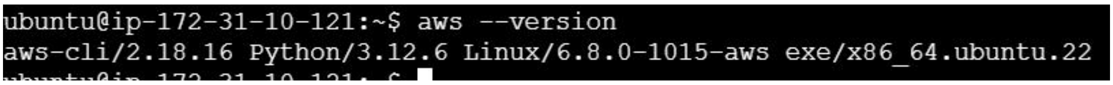
```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```



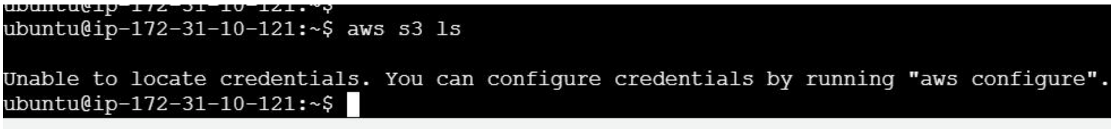
```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ unzip awscliv2.zip
```



```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ sudo ./aws/install
You can now run: /usr/local/bin/aws --version
ubuntu@ip-172-31-10-121:~$
```



```
ubuntu@ip-172-31-10-121:~$ aws --version
aws-cli/2.18.16 Python/3.12.6 Linux/6.8.0-1015-aws exe/x86_64.ubuntu.22
ubuntu@ip-172-31-10-121:~$
```



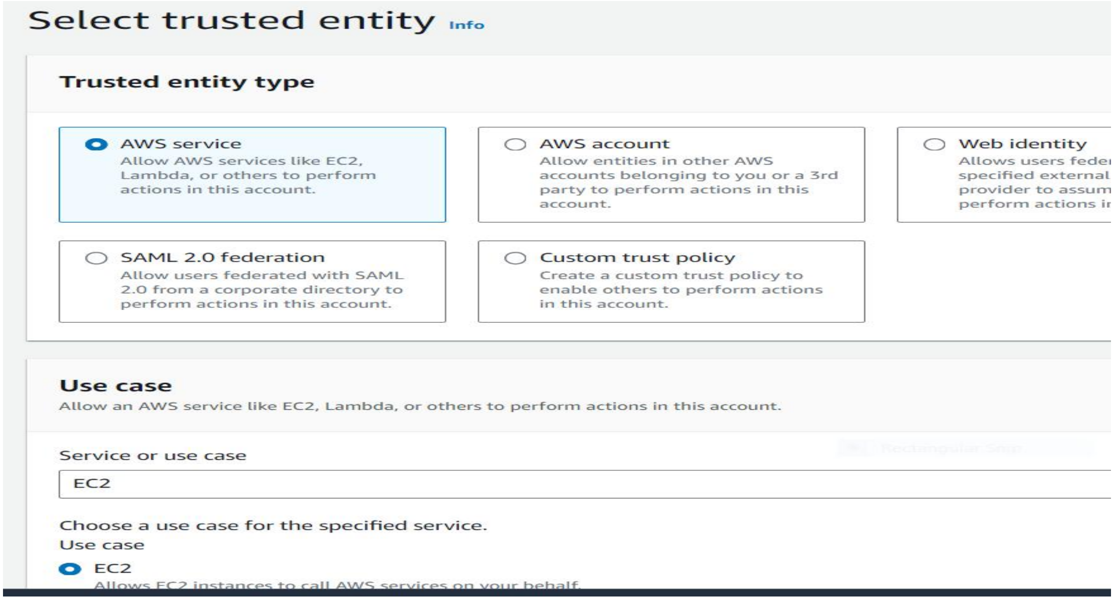
```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
ubuntu@ip-172-31-10-121:~$
```

We got the error as we don’t have permissions yet.

STEP4: Create a Role and Attach S3FullAccess Policy--

- Navigate to the IAM console, Create a new role, selecting the EC2 service as the trusted entity.



Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users fede
specified external
provider to assum
perform actions i

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

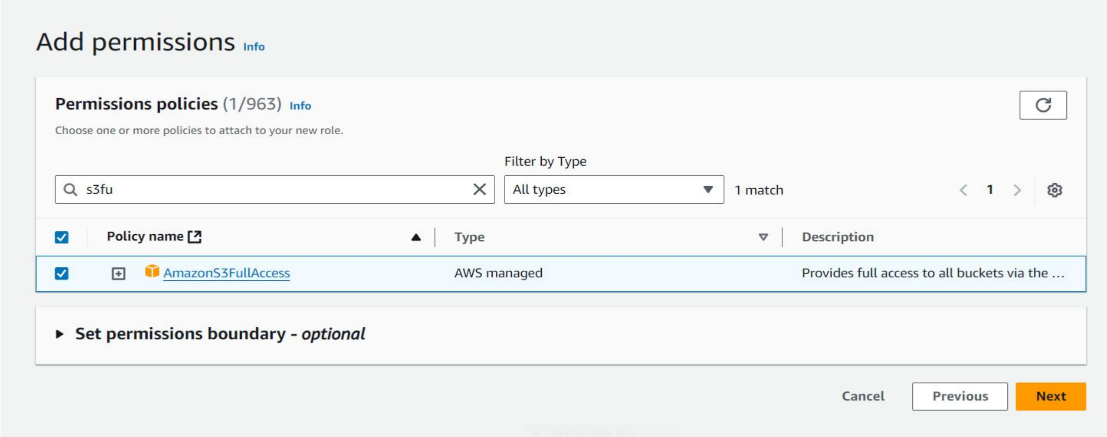
○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case
● EC2
Allows EC2 instances to call AWS services on your behalf.

- Attach the AmazonS3FullAccess policy to the role.



Add permissions Info

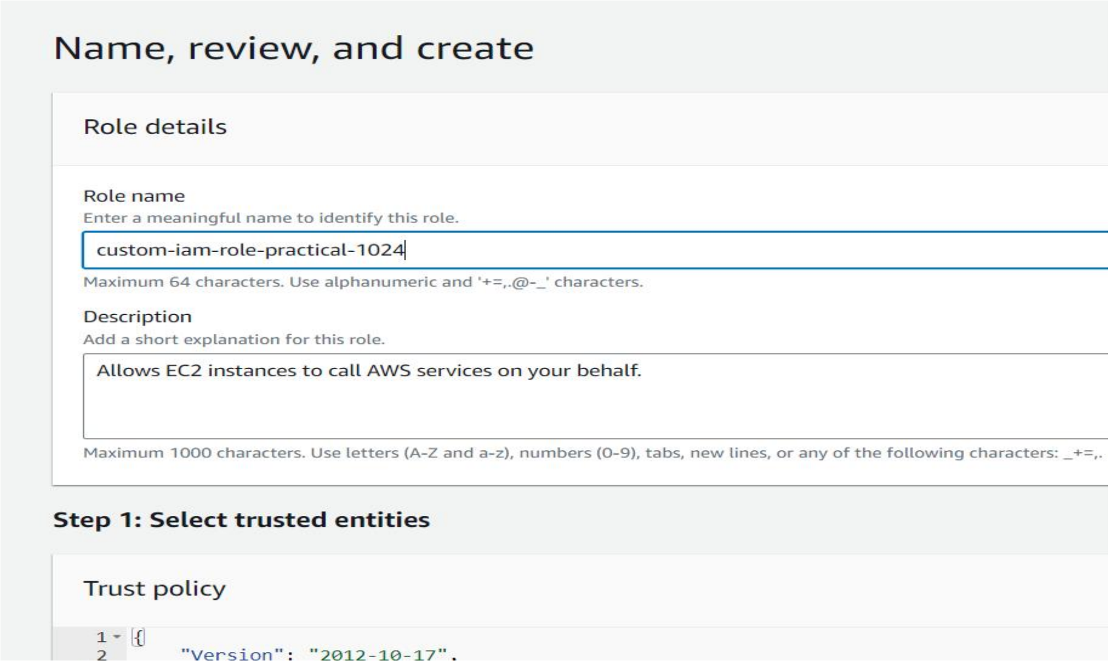
Permissions policies (1/963) Info
Choose one or more policies to attach to your new role.

Filter by Type
s3fu | All types | 1 match

☑	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the ...

▸ Set permissions boundary - *optional*

- Name your role and create it.



Name, review, and create

Role details

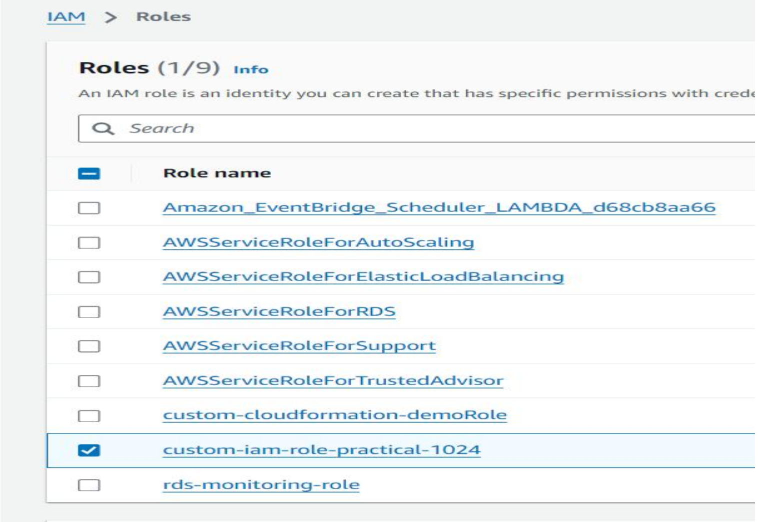
Role name
Enter a meaningful name to identify this role.
custom-iam-role-practical-1024
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

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

Trust policy

```
{
    "Version": "2012-10-17",
```



IAM > Roles

Roles (1/9) Info
An IAM role is an identity you can create that has specific permissions with cred

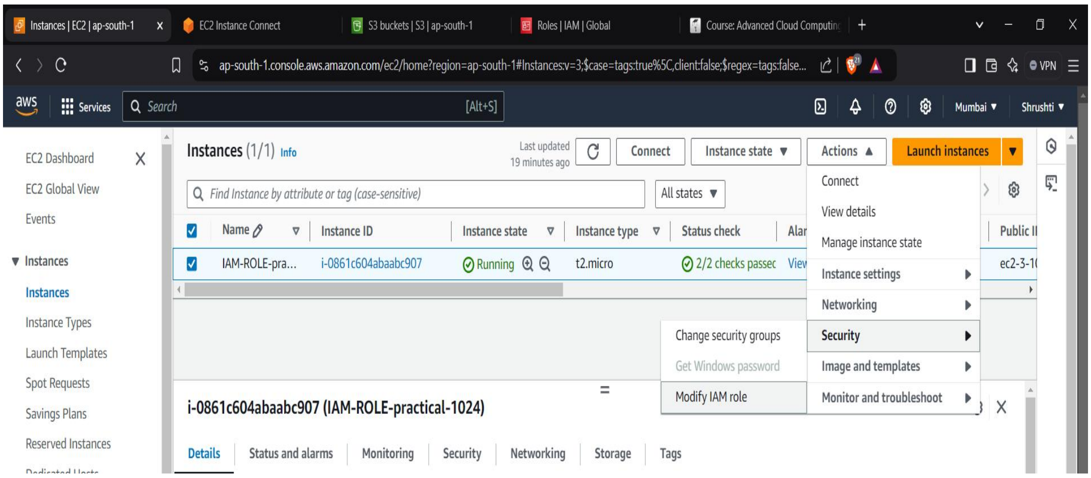
Search

⊟	Role name
☐	Amazon_EventBridge_Scheduler_LAMBDA_d68cb8aa66
☐	AWSServiceRoleForAutoScaling
☐	AWSServiceRoleForElasticLoadBalancing
☐	AWSServiceRoleForRDS
☐	AWSServiceRoleForSupport
☐	AWSServiceRoleForTrustedAdvisor
☐	custom-cloudformation-demoRole
☑	custom-iam-role-practical-1024
☐	rds-monitoring-role

role created.

Step5: Modify EC2 Instance Role

- Go back to the EC2 dashboard.



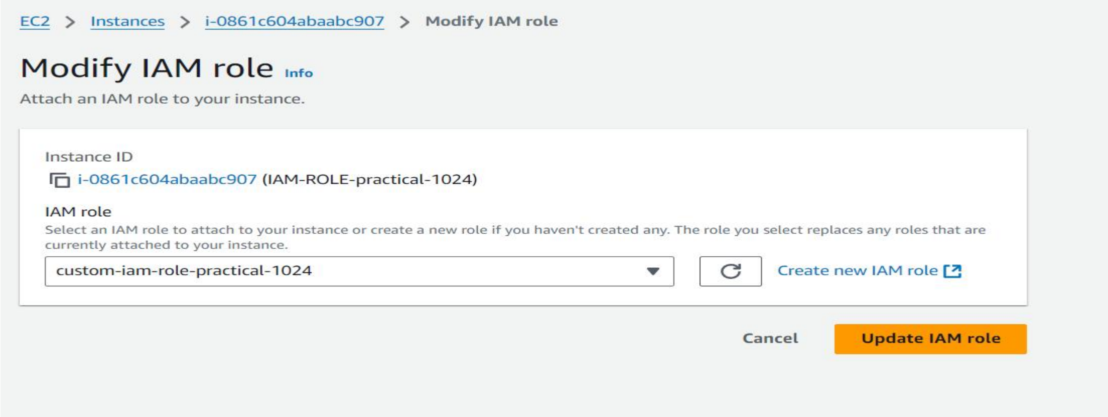
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false...

Instances (1/1) Info — Last updated 19 minutes ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alar	Public II
☑	IAM-ROLE-pra...	i-0861c604abaabc907	Running	t2.micro	2/2 checks passec	View	ec2-3-1(

i-0861c604abaabc907 (IAM-ROLE-practical-1024)

- Select your instance, then click on Actions > Security > Modify IAM Role.



EC2 > Instances > i-0861c604abaabc907 > Modify IAM role

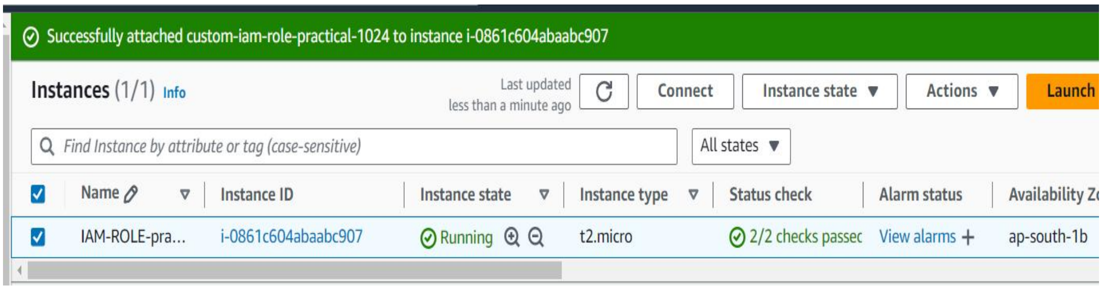
Modify IAM role Info

Attach an IAM role to your instance.

Instance ID
i-0861c604abaabc907 (IAM-ROLE-practical-1024)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

custom-iam-role-practical-1024



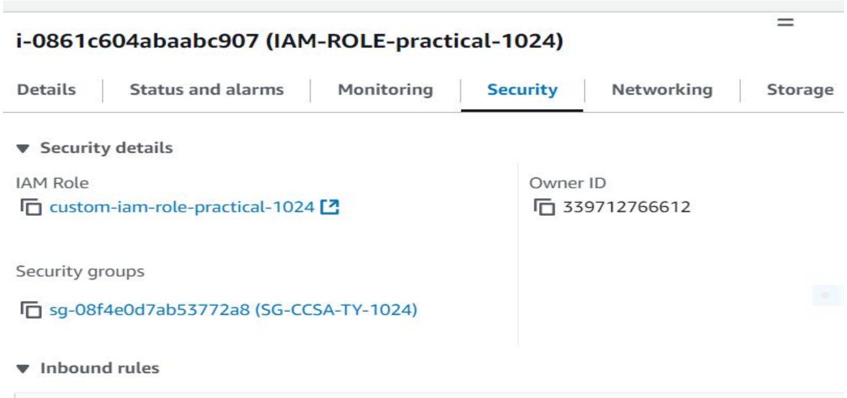
Successfully attached custom-iam-role-practical-1024 to instance i-0861c604abaabc907

Instances (1/1) Info — Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo
☑	IAM-ROLE-pra...	i-0861c604abaabc907	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1b

Step6: Verify Permissions

- With the role attached, your instance should now have permissions to access S3.



i-0861c604abaabc907 (IAM-ROLE-practical-1024)

▼ Security details

IAM Role: custom-iam-role-practical-1024

Owner ID: 339712766612

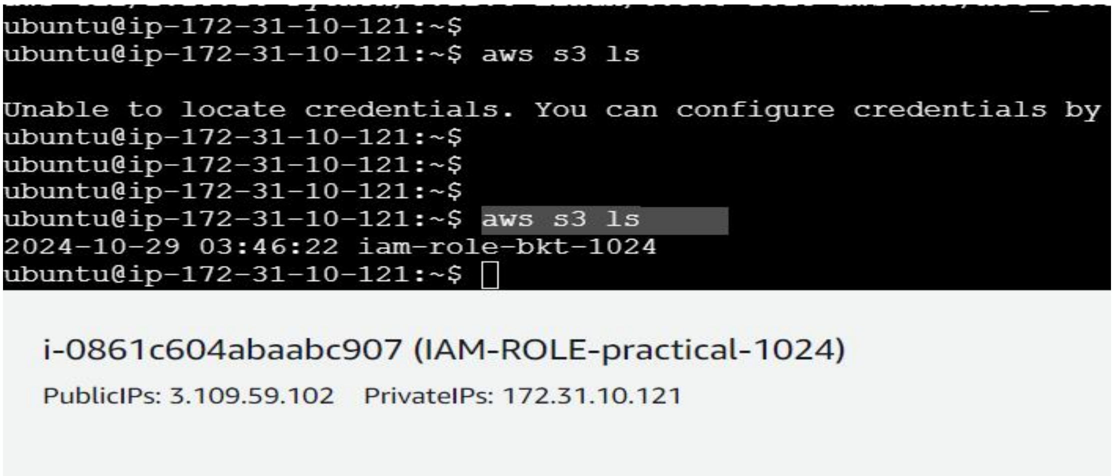
Security groups: sg-08f4e0d7ab53772a8 (SG-CCSA-TY-1024)

▼ Inbound rules

Step 7: List S3 Buckets Again

- aws s3 ls

You should now see the buckets you created.



```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ aws s3 ls

Unable to locate credentials. You can configure credentials by
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ aws s3 ls
2024-10-29 03:46:22 iam-role-bkt-1024
ubuntu@ip-172-31-10-121:~$ 
```

i-0861c604abaabc907 (IAM-ROLE-practical-1024)

PublicIPs: 3.109.59.102 PrivateIPs: 172.31.10.121

We are able to access s3 service from ec2 service using IAM role.