

**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**PRN:** 20220801024

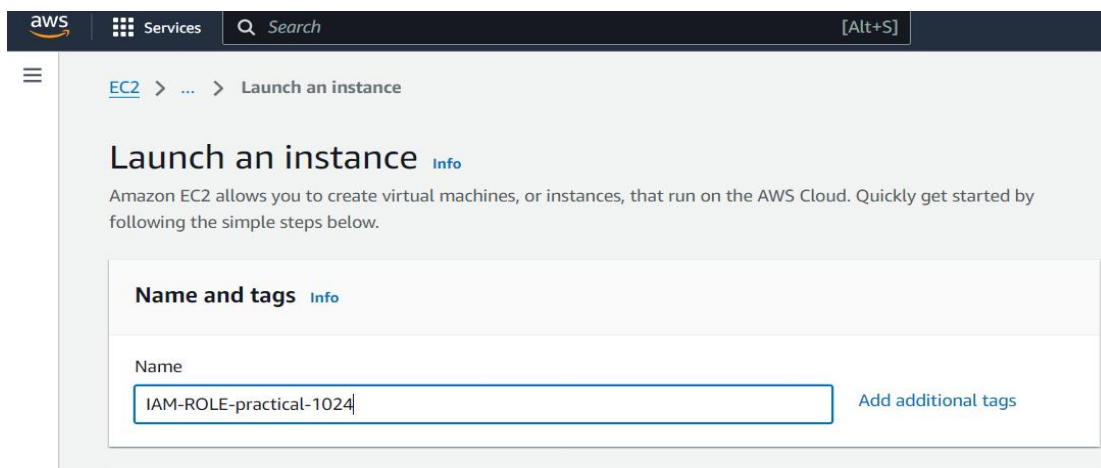
**Title of Practicle :**

Access S3 bucket through EC2 using IAM role

**STEP1: LOG IN AND create one ec2 instance**

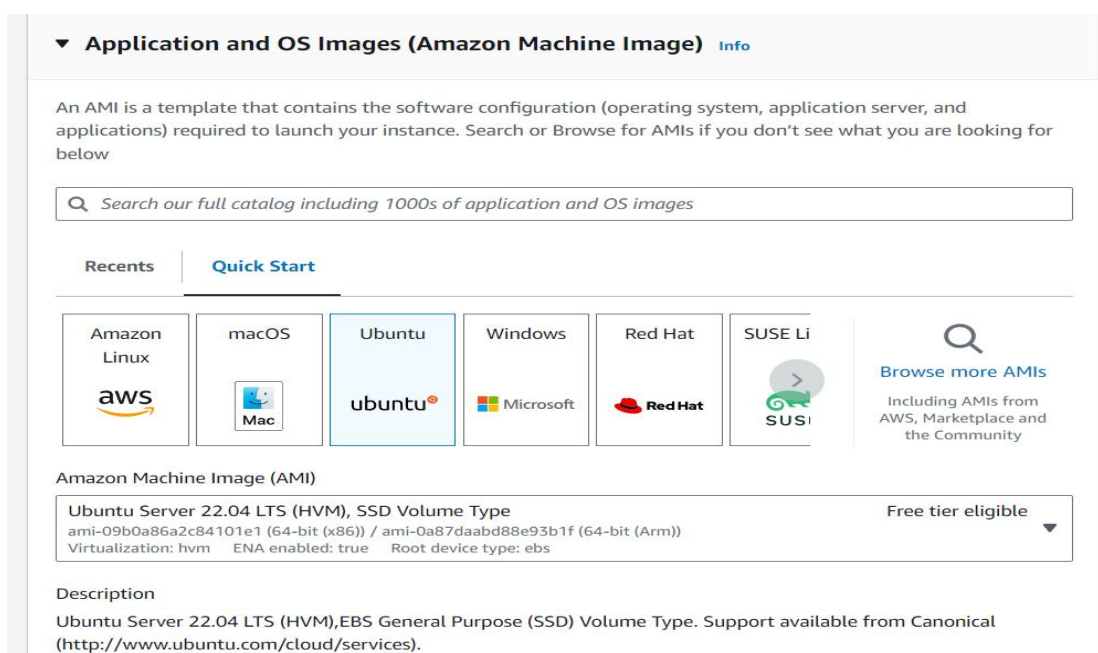
Go to EC2 service and launch one instance

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



The screenshot shows the AWS Management Console interface for the 'Launch an instance' page. The breadcrumb navigation shows 'EC2 > ... > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. Below the heading, a brief description states: '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.' A section titled 'Name and tags' contains a text input field for 'Name' with the value 'IAM-ROLE-practical-1024' and a button labeled 'Add additional tags'.

AMI---ubuntu linux



The screenshot shows the 'Application and OS Images (Amazon Machine Image)' page in the AWS Management Console. It includes a search bar with the placeholder text 'Search our full catalog including 1000s of application and OS images'. Below the search bar are tabs for 'Recents' and 'Quick Start'. A grid of image cards is displayed, including 'Amazon Linux', 'macOS', 'Ubuntu' (which is highlighted), 'Windows', 'Red Hat', and 'SUSE Li'. To the right of the grid is a link 'Browse more AMIs' with a magnifying glass icon. Below the grid, the details for the selected 'Ubuntu Server 22.04 LTS (HVM), SSD Volume Type' AMI are shown, including the AMI ID 'ami-09b0a86a2c84101e1' and a 'Free tier eligible' status. A description at the bottom states: 'Ubuntu Server 22.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).'



## School of Computer Science, Engineering and Applications(SCSEA)

### B.C.A. TY (SCSEA)

### Subject: Advance Cloud Computing(ACC)

Name of the Student: Shrushti Krishna Shrivastav

PRN: 20220801024

Title of Practicle : Access S3 bucket through EC2 using IAM role

Instance type--- t2.micro

**▼ Instance type** [Info](#) | [Get advice](#)

Instance type

t2.micro

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

Free tier eligible

☐ All generations

[Compare instance types](#)

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

[Create new key pair](#)

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

**▼ Network settings** [Info](#) [Edit](#)

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 X

VPC: vpc-0662aa9456cd34d0a

[Compare security group rules](#)

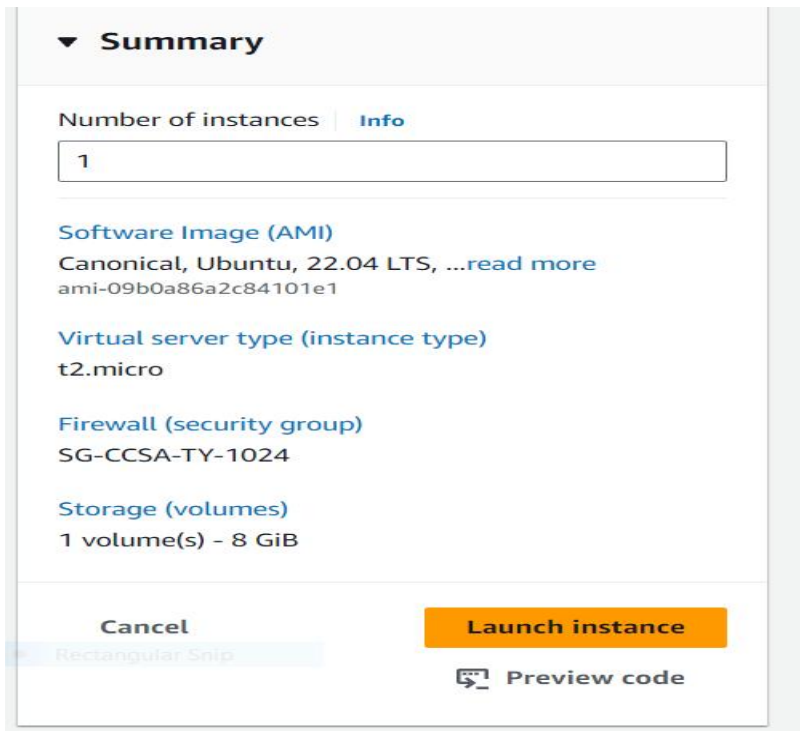
Security groups that you add or remove here will be added to or removed from all your network interfaces.

**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

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

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

### 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

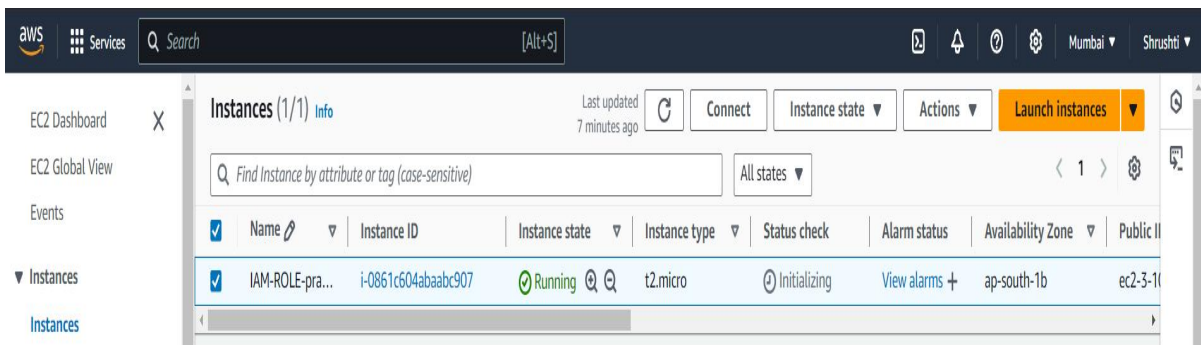
**Firewall (security group)**  
SG-CCSA-TY-1024

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

**Cancel** **Launch instance**

[Preview code](#)

### Our instance is created



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
IAM-ROLE-pra...	i-0861c604abaabc907	Running	t2.micro	Initializing	<a href="#">View alarms</a>	ap-south-1b	ec2-3-1...



**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**PRN:** 20220801024

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

**STEP2: Now create one s3 bucket--**

Name--iam-role-bkt-1024

**Ownership--- ACLs disabled**



## School of Computer Science, Engineering and Applications(SCSEA)

### B.C.A. TY (SCSEA)

### Subject: Advance Cloud Computing(ACC)

Name of the Student: Shrushti Krishna Shrivastav

PRN: 20220801024

Title of Practicle : Access S3 bucket through EC2 using IAM role

### 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 same bucket. Every version of every object stored in your Amazon S3 bucket. With versioning, you can recover deleted objects and versions of an object if you have deleted the wrong one. [Learn more](#)

#### Bucket Versioning

☒ Disable

☐ Enable





**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**PRN:** 20220801024

**Title of Practicle :**

Access S3 bucket through EC2 using IAM role

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.**

[Cancel](#) [Create bucket](#)

Create bucket

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

[Amazon S3](#) > **Buckets**



**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

**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---

Connect Type

☒ Connect using EC2 Instance Connect  
Connect using the EC2 Instance Connect browser-based client, 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

Address

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

ubuntu

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

Cancel Connect



**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**PRN:** 20220801024

**Title of Practicle :**

Access S3 bucket through EC2 using IAM role

```
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.





**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**PRN:** 20220801024

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

**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 federated with specified external provider to assume perform actions in

☐ **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

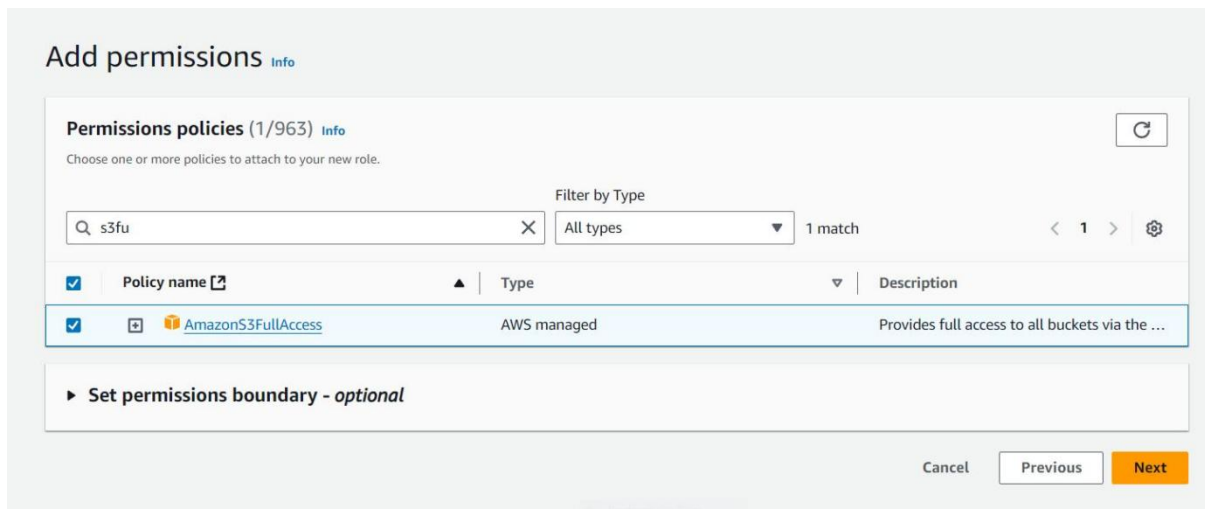
☒ **EC2**  
Allows EC2 instances to call AWS services on your behalf.

**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

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

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

- 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

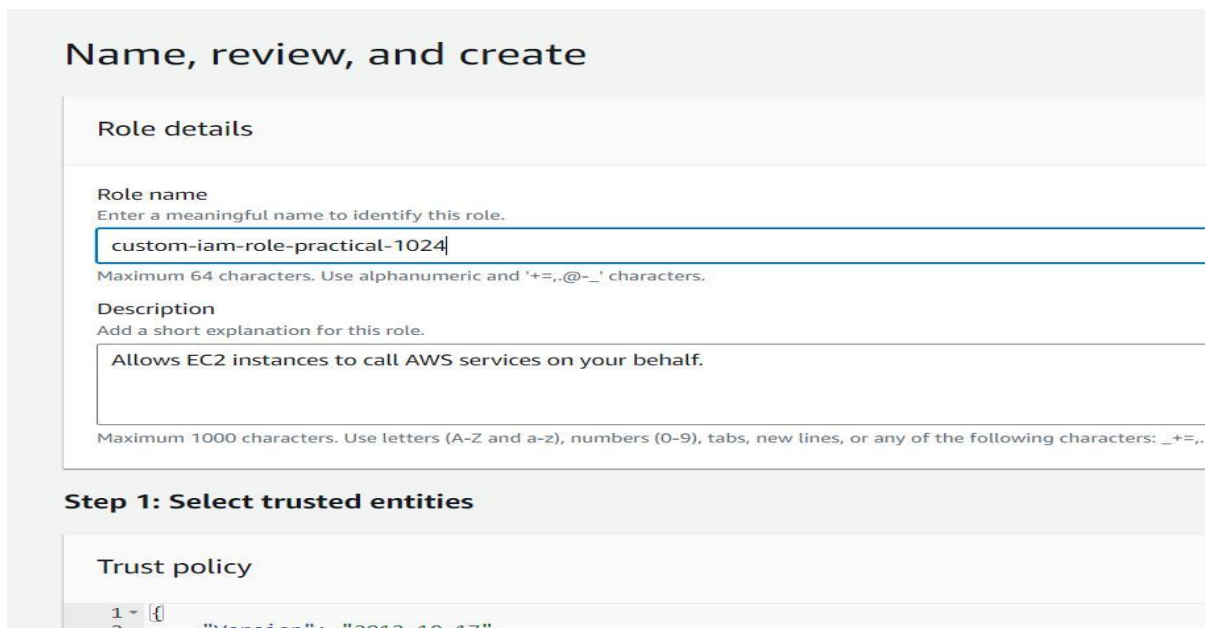
Q s3fu X All types 1 match < 1 > ⚙

<input checked="" type="checkbox"/>	Policy name <a href="#">?</a>	Type	Description
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the ...

▶ Set permissions boundary - optional

Cancel Previous Next

- 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**

1 - {  
2 "Version": "2012-10-17".

## School of Computer Science, Engineering and Applications(SCSEA)

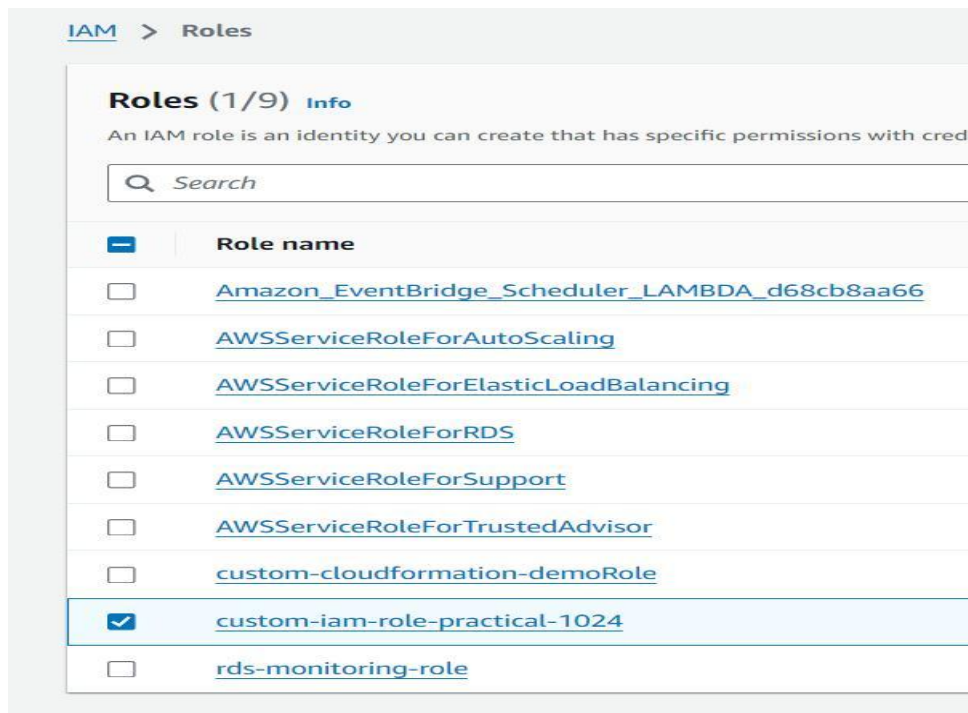
### B.C.A. TY (SCSEA)

### Subject: Advance Cloud Computing(ACC)

Name of the Student: Shrushti Krishna Shrivastav

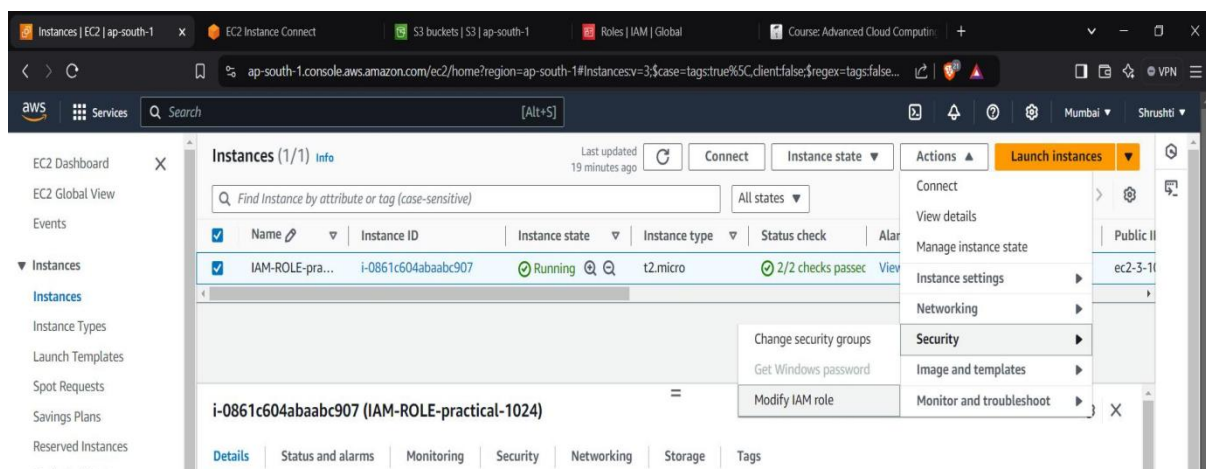
PRN: 20220801024

Title of Practicle : Access S3 bucket through EC2 using IAM role



### Step5: Modify EC2 Instance Role

- Go back to the EC2 dashboard.

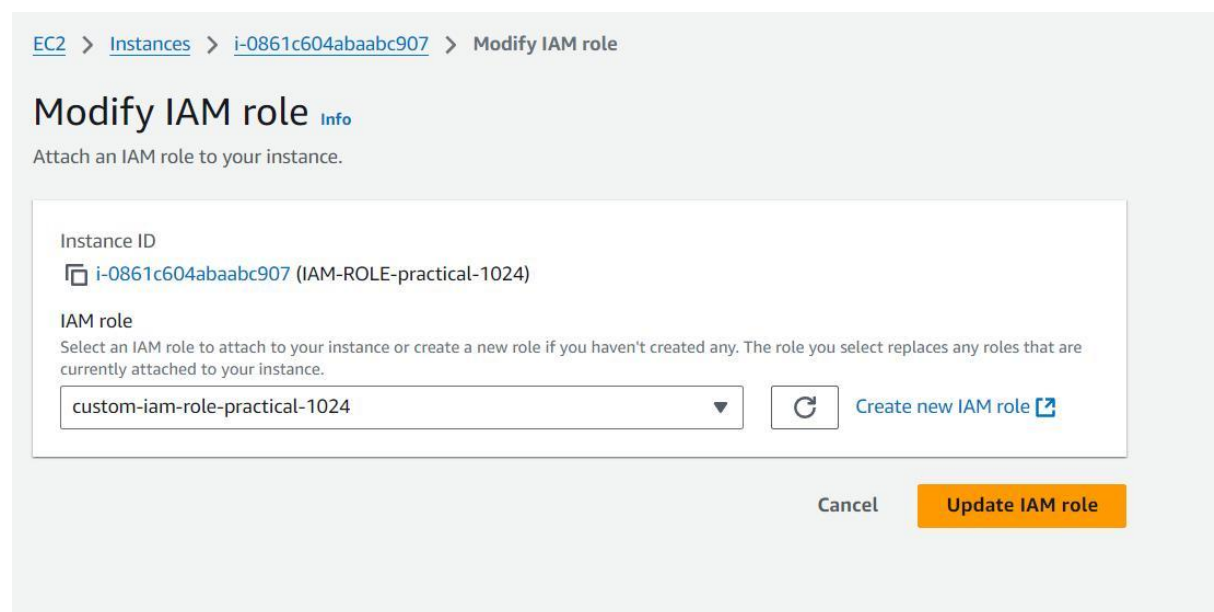


**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

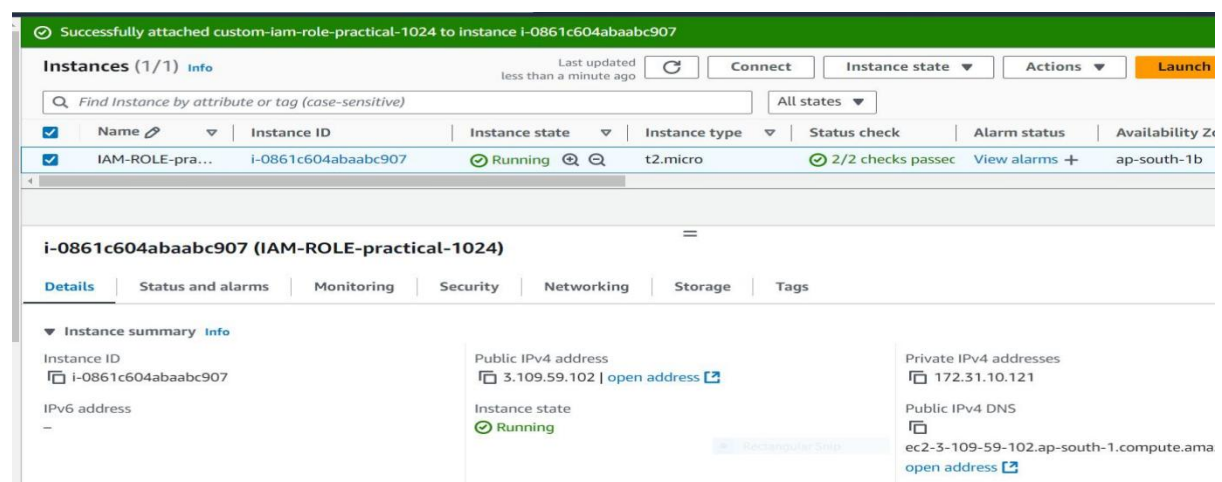
**Name of the Student:**      Shrushti Krishna Shrivastav      **PRN:** 20220801024

**Title of Practicle :**      Access S3 bucket through EC2 using IAM role

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



The screenshot shows the 'Modify IAM role' page in the AWS IAM console. The breadcrumb trail is 'EC2 > Instances > i-0861c604abaabc907 > Modify IAM role'. The page title is 'Modify IAM role' with an 'Info' link. Below the title is the instruction 'Attach an IAM role to your instance.' The 'Instance ID' section shows 'i-0861c604abaabc907 (IAM-ROLE-practical-1024)'. The 'IAM role' section has a dropdown menu with 'custom-iam-role-practical-1024' selected and a 'Create new IAM role' link. At the bottom right are 'Cancel' and 'Update IAM role' buttons.



The screenshot shows the 'Instances' page in the AWS EC2 console. A green banner at the top states 'Successfully attached custom-iam-role-practical-1024 to instance i-0861c604abaabc907'. The 'Instances (1/1)' table has one entry: 'IAM-ROLE-pra...' with Instance ID 'i-0861c604abaabc907', state 'Running', type 't2.micro', and status '2/2 checks passed'. Below the table, the 'Details' tab for instance 'i-0861c604abaabc907 (IAM-ROLE-practical-1024)' is selected. It shows the instance is 'Running' and provides public and private IP addresses and DNS information.

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

i-0861c604abaabc907 (IAM-ROLE-practical-1024)	
<b>Instance summary</b> Instance ID: i-0861c604abaabc907 IPv6 address: —	Public IPv4 address: 3.109.59.102   open address Instance state: Running Private IPv4 addresses: 172.31.10.121 Public IPv4 DNS: ec2-3-109-59-102.ap-south-1.compute.amazonaws.com   open address

**Step6: Verify Permissions**



**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

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

**Title of Practicle :** Access S3 bucket through EC2 using IAM role

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

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

Details | Status and alarms | Monitoring | **Security** | Networking | Storage

▼ 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.

Done.