


*) Go to <https://console.aws.amazon.com/>

eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Aiam%3Aeu-north-1%3Aroot%3Aassumed-role%3A...

 You are currently using the improved sign in UI. The [improved sign in](#) experience will launch in the dropdown in the upper right corner.

IAM user sign in

Account ID (12 digits) or account alias

IAM username

Password

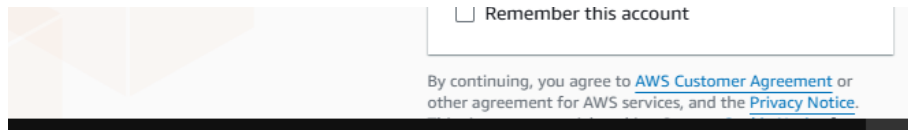
☐ Show Password [Having trouble?](#)

Sign in

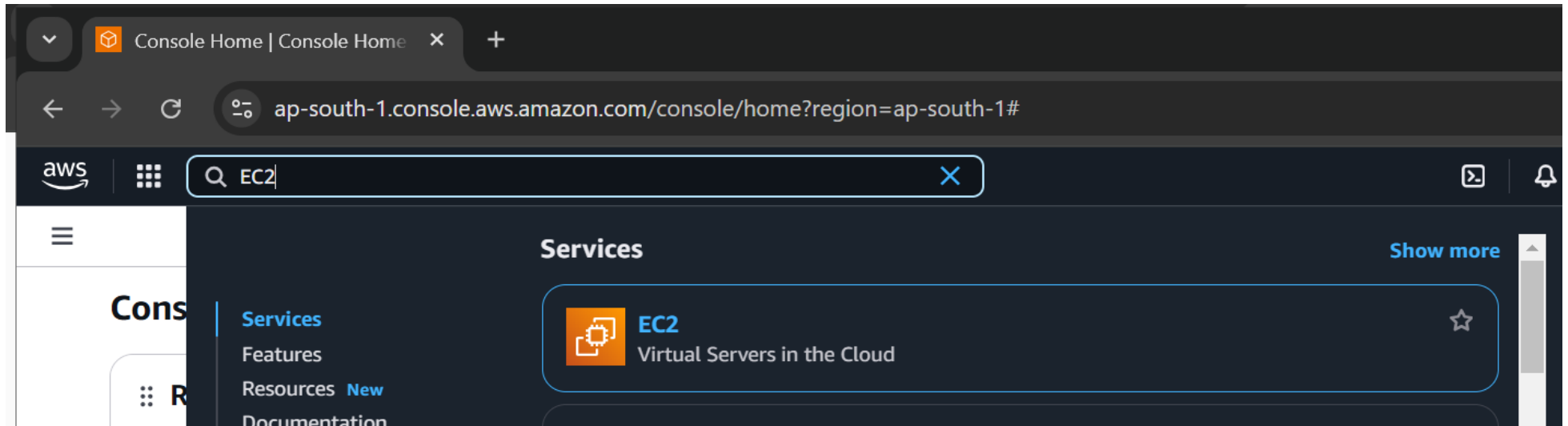
Sign in using root user email

[Create a new AWS account](#)

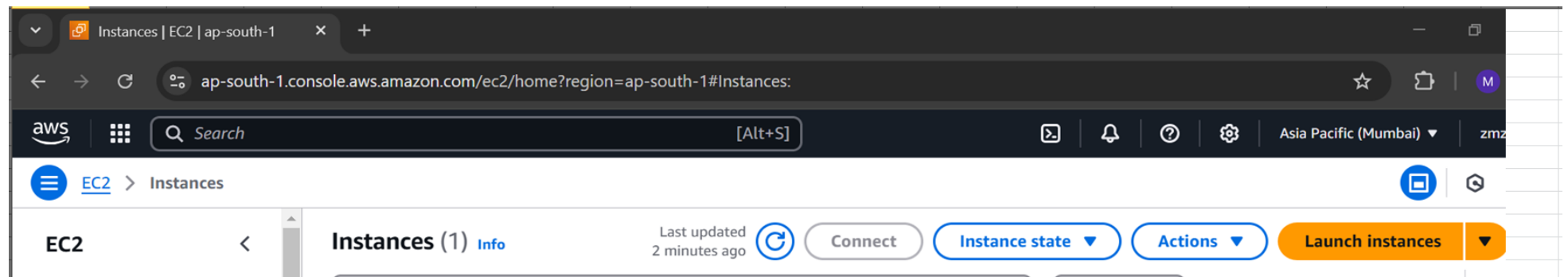
☐ Sign in with...



*) Login with your credentials



*) Type EC2 and select EC2 services



*) Click Launch Instances

Launch an instance | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws Search [Alt+S]

Asia Pacific (Mumbai)

[EC2](#) > [Instances](#) > Launch an instance

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

[Add additional tags](#)

▼ 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

[Recents](#) | [Quick Start](#)

▼ Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0ddfba243cbee3768

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)

[Cancel](#) [Launch instance](#) [Preview code](#)

*) Give an instance name

Launch an instance | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws Search [Alt+S]

Asia Pacific (Mumbai)

EC2 > Instances > Launch an instance

▼ 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

RecentsQuick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

ami-00bb6a80f01f03502 (64-bit (x86)) / ami-09773b29dffbf1f2 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...read more

ami-00bb6a80f01f03502

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

Cancel

Launch instance

Preview code

*) Select Ubuntu Server Image (Free tier)

Launch an instance | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

aws Search [Alt+S]

Asia Pacific (Mumbai)

EC2 > Instances > Launch an instance

▼ 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

▼

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ 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

Select

Create new key pair

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...read more

ami-00bb6a80f01f03502

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

Cancel

Launch instance

Preview code

*) Select t2.micro instance type (free tier) and click Create new key pair(for any future server access)

Create key pair

✕

Key pair name
Key pairs allow you to connect to your instance securely.

kp11

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

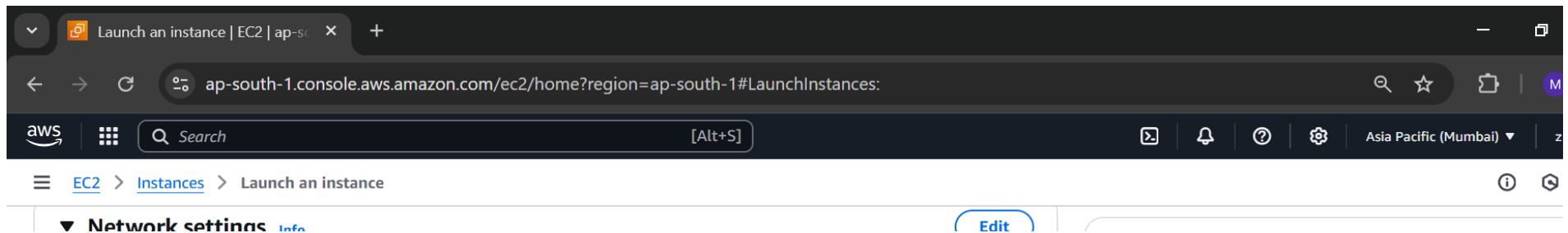
☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel

Create key pair

*) give a key pair name and keep rest as it is and click create key pair



Network settings

Network

Info

vpc-0a4306b149c2e022a

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

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒

Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☒

Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒

Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

Summary

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd6...read more

ami-00bb6a80f01f03502

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Preview code

*) Click Launch Instance and your Server is ready

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd6...read more

ami-00bb6a80f01f03502

Virtual server type (instance type)

t2.micro

Firewall (security group)

firewall (security group)

New security group

Cancel

Launch instance

 Preview code

☰ [EC2](#) > [Instances](#) > Launch an instance

✓ Success

Successfully initiated launch of instance ([i-0a476749238d4ea8c](#))

► Launch log

Next Steps

🔍 What would you like to do next with this instance, for example "create alarm" or "create backup"



Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create

Create a creation, EBS snap

*) Click connect to your instance to log into server

Connect to instance [Info](#)

Connect to your instance i-0a476749238d4ea8c (inst2) using any of these options


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console


Instance ID

 i-0a476749238d4ea8c (inst2)

Connection Type

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



☐ Connect using VPC endpoint.
Connect using a VPC endpoint.

☒ Public IPv4 address
 52.66.249.247

☐ IPv6 address
—

Username

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

 ubuntu 

*) choose Connect using EC2 instance connect as Connection Type

```
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status
```

```
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
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-172-31-13-65:~$
```

i-0a476749238d4ea8c (inst2)

PublicIPs: 52.66.249.247 PrivateIPs: 172.31.13.65

*) You will see a terminal connected to server

*) Type the following commands to update/install the libraries in the server and activate Mlflow server

to update the server, python and virtual environment library

sudo apt update

sudo apt install python3-pip

sudo apt install python3-virtualenv

to create the virtual environment

virtualenv env1

go to the bin folder in the newly created virtual environment

cd env1/bin

activate the virtual environment

source activate

install MLFlow library

pip install mlflow

***) With the instance created click Security Groups , choose create security group and check the three Allow boxes**

The screenshot shows the AWS Management Console interface for the 'Security Groups' page. The left sidebar shows the 'EC2' menu with options like Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main content area displays 'Security Groups (1/2)' with a search bar and a table of security groups. The 'launch-wizard-1' security group is selected, and its inbound rules are shown below. The inbound rules table has columns for Group rule ID, IP version, Type, Protocol, Port range, and Source. Two rules are listed: one for SSH (TCP, port 22) and one for HTTPS (TCP, port 443), both with a source of 0.0.0.0/0.

| Group rule ID | IP version | Type | Protocol | Port range | Source |
|---------------|------------|-------|----------|------------|-----------|
| c65dda80f06 | IPv4 | SSH | TCP | 22 | 0.0.0.0/0 |
| 4b43a4f6c43 | IPv4 | HTTPS | TCP | 443 | 0.0.0.0/0 |

*) Choose launch-wizard-1 group, under the Inbound rules tab, and click Edit Inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

| Inbound rules Info | | | | | | |
|------------------------------------|---------------------------|-------------------------------|---------------------------------|-----------------------------|---|--|
| Security group rule ID | Type Info | Protocol Info | Port range Info | Source Info | Description - optional Info | |
| sgr-01ca8f60beb261e68 | SSH ▼ | TCP | 22 | Cus... ▼ | <input type="text" value="0.0.0.0/0"/> ✕ | <input type="text" value=""/> Delete |
| sgr-0f7946253c8532355 | Custom TCP ▼ | TCP | 5000 | Cus... ▼ | <input type="text" value="0.0.0.0/0"/> ✕ | <input type="text" value=""/> Delete |
| sgr-09c3011e8702f6952 | HTTP ▼ | TCP | 80 | Cus... ▼ | <input type="text" value="0.0.0.0/0"/> ✕ | <input type="text" value=""/> Delete |
| sgr-06cf30bba1c699660 | HTTPS ▼ | TCP | 443 | Cus... ▼ | <input type="text" value="0.0.0.0/0"/> ✕ | <input type="text" value=""/> Delete |

*) Add rule, Custom TCP(Type), 5000(port range) and 0.0.0.0/0(Source) and Save

*) go back to the EC2 instance window and start the MLFlow server

mlflow server -h 0.0.0.0 --port 5000

```
(env1) ubuntu@ip-172-31-13-65:~/env1/bin$ mlflow server -h 0.0.0.0 --port 5000
[2025-02-14 17:13:35 +0000] [5103] [INFO] Starting gunicorn 23.0.0
[2025-02-14 17:13:35 +0000] [5103] [INFO] Listening at: http://0.0.0.0:5000 (5103)
[2025-02-14 17:13:35 +0000] [5103] [INFO] Using worker: sync
[2025-02-14 17:13:35 +0000] [5104] [INFO] Booting worker with pid: 5104
```

```
[2025-02-14 17:13:35 +0000] [5105] [INFO] Booting worker with pid: 5105
[2025-02-14 17:13:35 +0000] [5106] [INFO] Booting worker with pid: 5106
[2025-02-14 17:13:35 +0000] [5107] [INFO] Booting worker with pid: 5107
```

*) server is started and you can copy the public ip of the server and start using in your code for experiment tracking

*) you can retrieve public ip address from various ways(below is one of them)

Connect to instance [Info](#)


Connect to your instance i-0a476749238d4ea8c (inst2) using any of these options

EC2 Instance Connect

Session Manager

SSH client


EC2 serial console

Instance ID
 i-0a476749238d4ea8c (inst2)

Connection Type


☒ **Connect using EC2 Instance Connect**
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

☐ **Connect using VPC endpoint**
Connect using VPC endpoint.

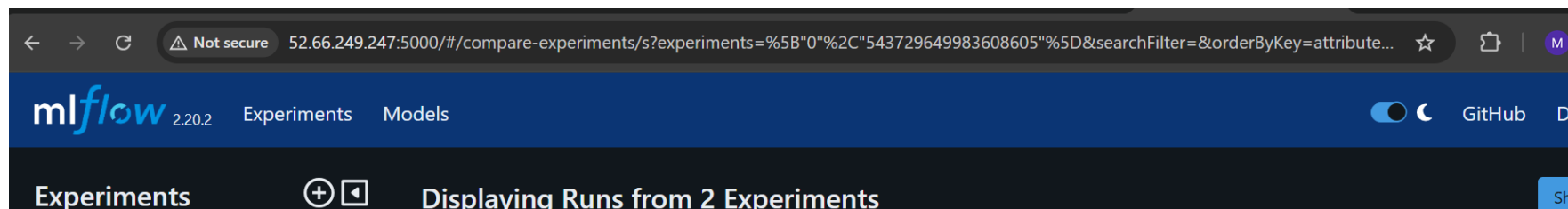
☒ **Public IPv4 address**
 52.66.249.247

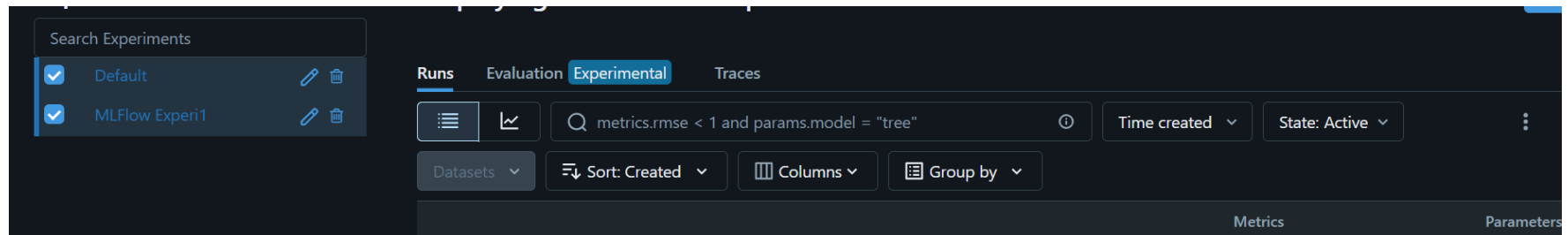
☐ **IPv6 address**
—

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



*) access MLFlow Dashboard from browser like <http://52.66.249.247:5000>





*) use this server for experiment tracking in the code (sample)

```
mlflow.set_tracking_uri("http://52.66.249.247:5000")
```

```
exp = mlflow.set_experiment("demo1")
```