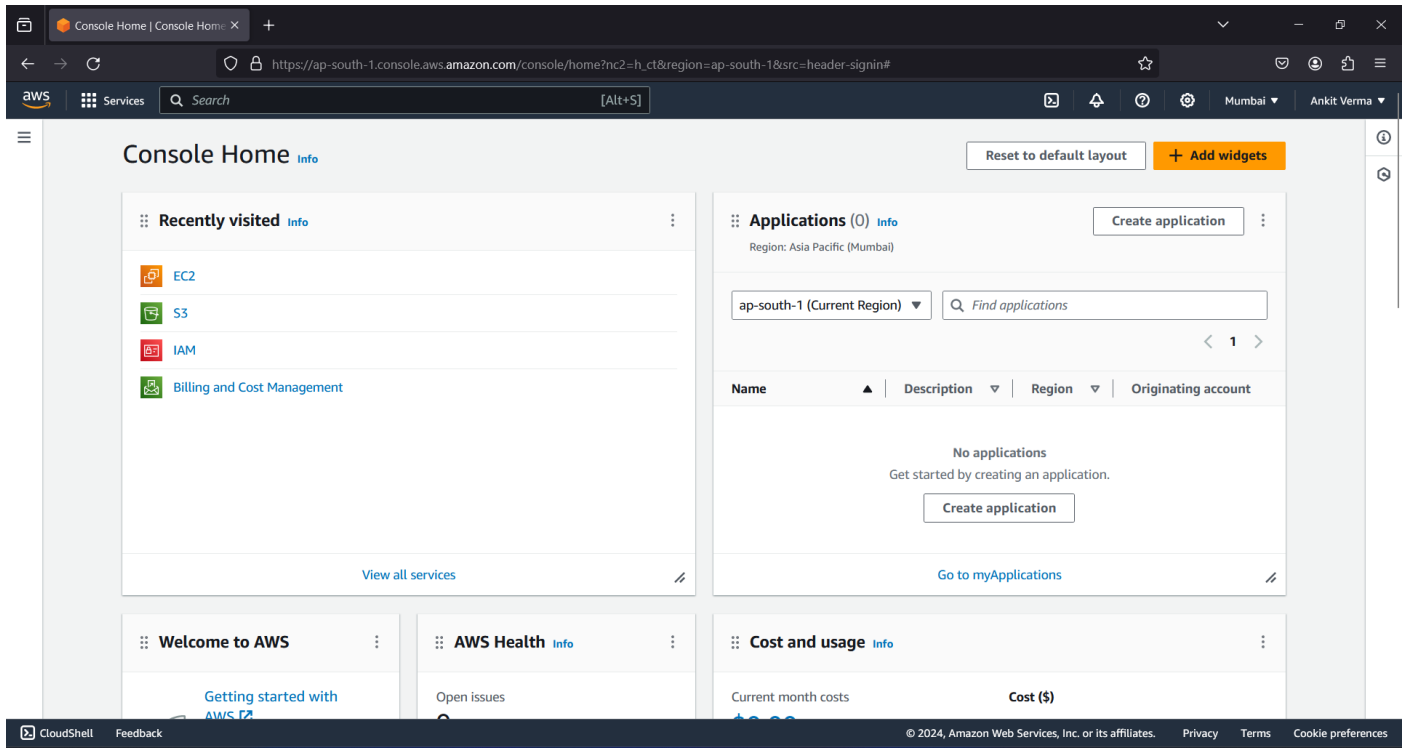


# Assignment: 10

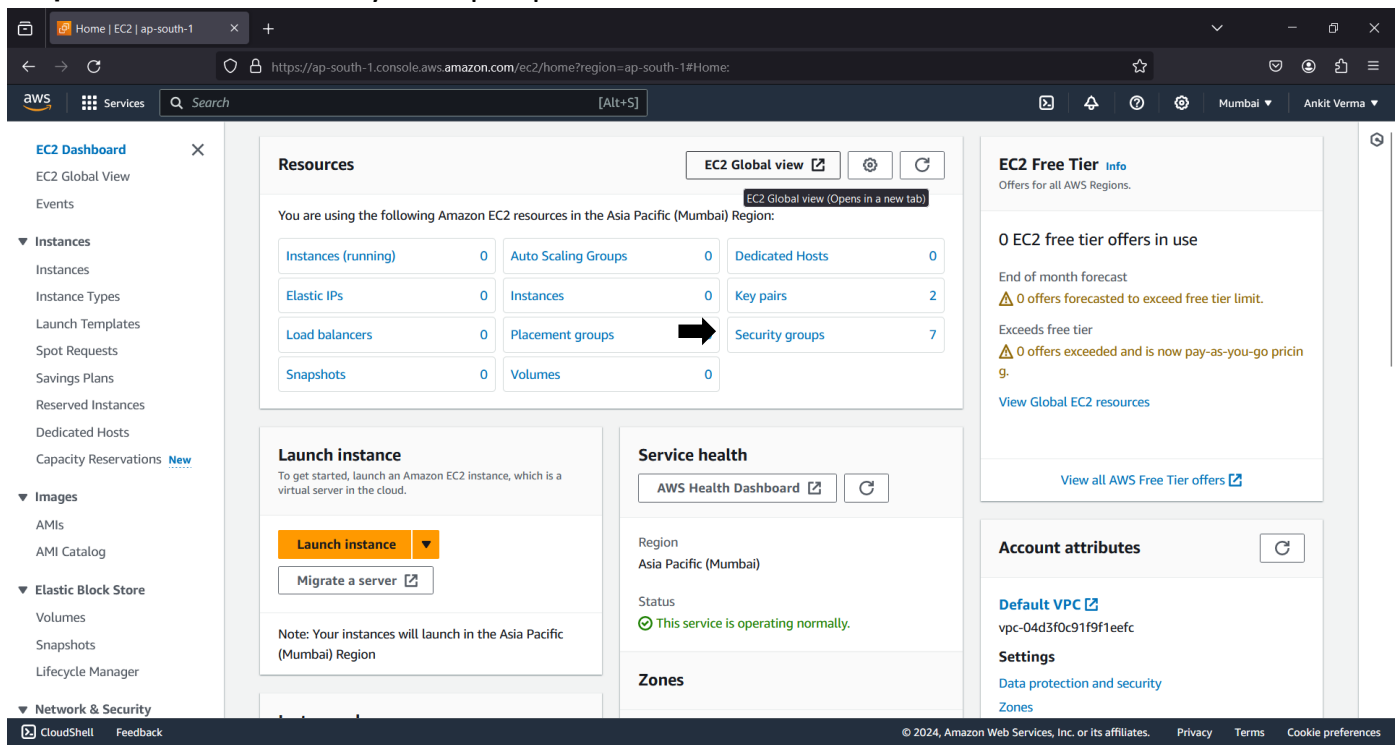
**Problem Statement:** Deploy a project from GitHub to EC2 by creating a new security group and user data.

» The steps to Deploy the Project from GitHub to EC2 by creating a new Security Group:-

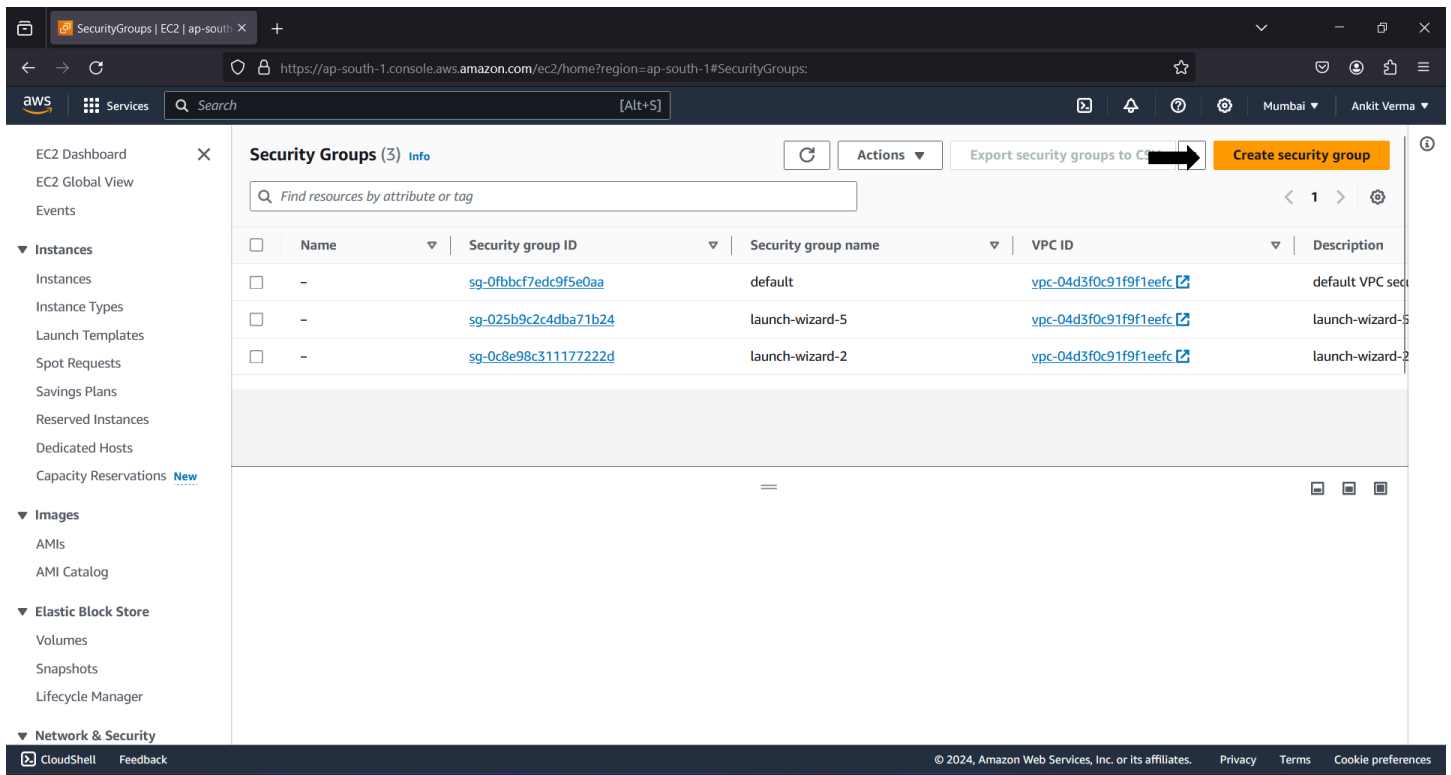
**Step 1: Select EC2.**



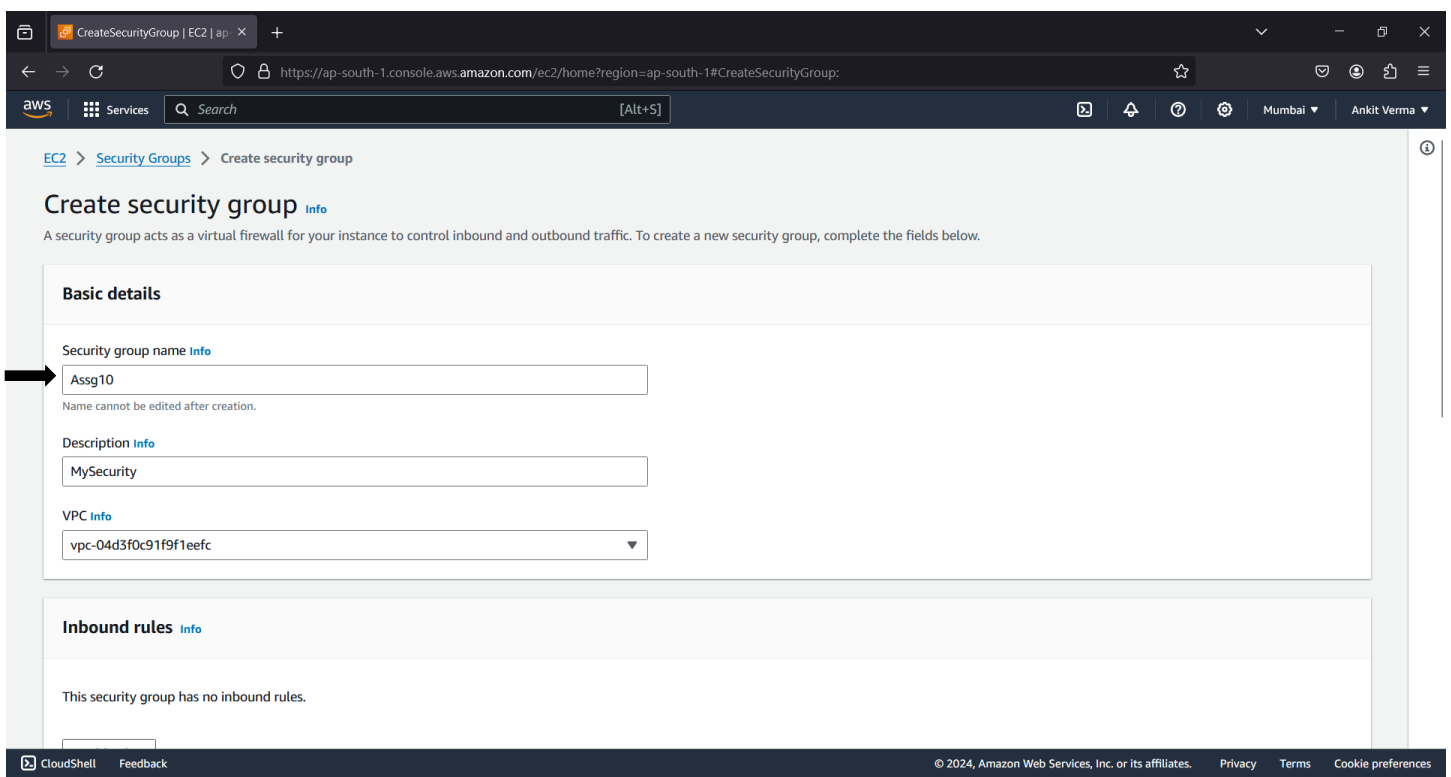
**Step 2: Go to the Security Groups option.**



### Step 3: Click on Create Security Group.



### Step 4: Give a name and Description to the Security Group. Then click on Add Rule under the Inbound Rules tab.



**Step 5:** Add the following 4 rules. Give all the rules the source address of 0.0.0.0/0 & and Port range of 4000 to Custom TCP.

The screenshot shows the 'Create Security Group' page in the AWS Management Console. The 'Inbound rules' section is active, displaying a table with four rules. Each rule has a 'Type' dropdown, a 'Protocol' dropdown, a 'Port range' input, a 'Source' dropdown, and a 'Description - optional' input. The 'Source' dropdown for each rule is set to 'Anywh...' and has a search box with '0.0.0.0/0' entered. The 'Port range' for each rule is set to a specific port: 22 for SSH, 80 for HTTP, 443 for HTTPS, and 4000 for Custom TCP. The 'Type' dropdown for each rule is set to the corresponding protocol: SSH, HTTP, HTTPS, and Custom TCP. The 'Protocol' dropdown for each rule is set to TCP. The 'Description - optional' input is empty for all rules. There is a 'Delete' button next to each rule. At the bottom of the table is an 'Add rule' button. A yellow warning banner at the bottom of the page states: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	Anywh... 0.0.0.0/0	
HTTP	TCP	80	Anywh... 0.0.0.0/0	
HTTPS	TCP	443	Anywh... 0.0.0.0/0	
Custom TCP	TCP	4000	Anywh... 0.0.0.0/0	

**Step 6:** Click on Create Security Group

The screenshot shows the 'Create Security Group' page in the AWS Management Console. The 'Outbound rules' section is active, displaying a table with one rule. The rule has a 'Type' dropdown set to 'All traffic', a 'Protocol' dropdown set to 'All', a 'Port range' input set to 'All', a 'Destination' dropdown set to 'Anywh...', and a 'Description - optional' input. The 'Destination' dropdown has a search box with '0.0.0.0/0' entered. There is a 'Delete' button next to the rule. At the bottom of the table is an 'Add rule' button. A yellow warning banner at the bottom of the page states: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Anywh... 0.0.0.0/0	

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

**Add new tag**  
You can add up to 50 more tags

**Create security group**

## Step 7: Now click on “Launch Instance”.

The screenshot shows the AWS Management Console EC2 Dashboard for the Asia Pacific (Mumbai) region. The left sidebar contains navigation links for EC2 Dashboard, Instances, Images, Elastic Block Store, and Network & Security. The main content area is divided into several sections: Resources (showing usage of EC2 resources), Launch instance (with a prominent orange 'Launch instance' button), Service health (showing AWS Health Dashboard), and EC2 Free Tier (showing 0 offers in use). The bottom of the dashboard includes a footer with 'CloudShell', 'Feedback', and copyright information.

## Step 8: Give a unique name to the instance and select Ubuntu.

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The 'Name and tags' step is active, with a text input field containing 'Ag10'. A black arrow points to this field. The 'Application and OS Images (Amazon Machine Image)' step is also visible, showing a search bar and a grid of AMIs including Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. The 'Summary' section on the right shows the configuration: 1 instance, Canonical, Ubuntu, 24.04 LTS, ami-0f58b397bc5c1f2e8, t2.micro, New security group, and 1 volume(s) - 8 GiB. A 'Free tier' notification is displayed at the bottom right, stating that 750 hours of t2.micro (or t3.micro) are included in the first year. The bottom of the wizard includes 'Cancel' and 'Launch instance' buttons, along with a 'Review commands' link.

**Step 9:** Under key pair (login) select an existing key from the drop-down menu or create a new key.

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: 0.0724 USD per Hour  
On-Demand SUSE base pricing: 0.0124 USD per Hour

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

key2

Proceed without a key pair (Not recommended) Default value

key1  
Type: rsa

key2  
Type: rsa

vp-04d3f0c91f9f1eefc

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

**Summary**

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more  
ami-0f58b397bc5c1f2e8

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free

Cancel Launch instance

Review commands

**Step 10:** Select the Select Existing Security Group, then select the newly created security group.

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

Assg10  
VPC: vpc-04d3f0c91f9f1eefc sg-0e8da184778a43395

default  
VPC: vpc-04d3f0c91f9f1eefc sg-0fbcf7edc9f5e0aa

launch-wizard-5  
VPC: vpc-04d3f0c91f9f1eefc sg-025b9c2c4dba71b24

launch-wizard-2  
VPC: vpc-04d3f0c91f9f1eefc sg-0c8e98c311177222d

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store

**Summary**

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more  
ami-0f58b397bc5c1f2e8

Virtual server type (instance type)

t2.micro

Firewall (security group)

-

Storage (volumes)

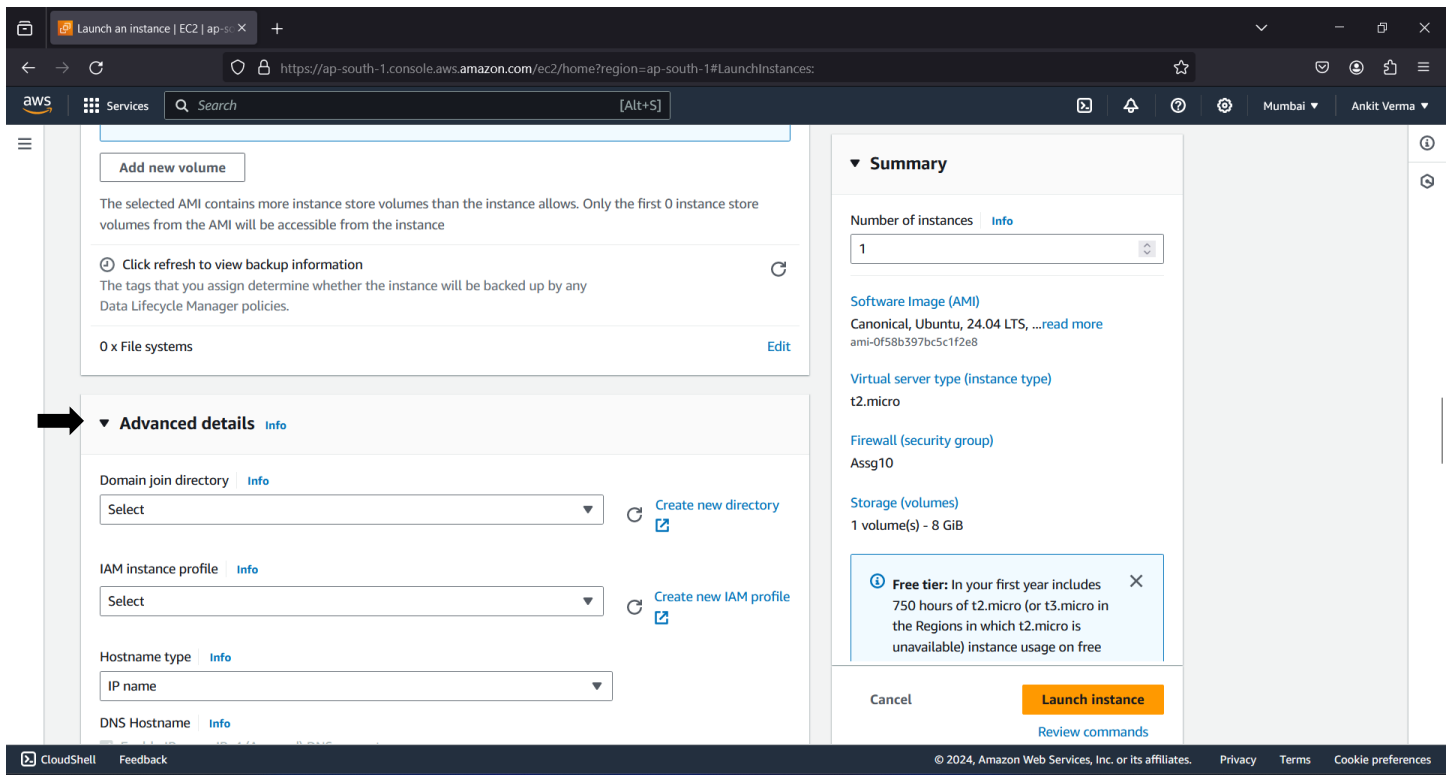
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free

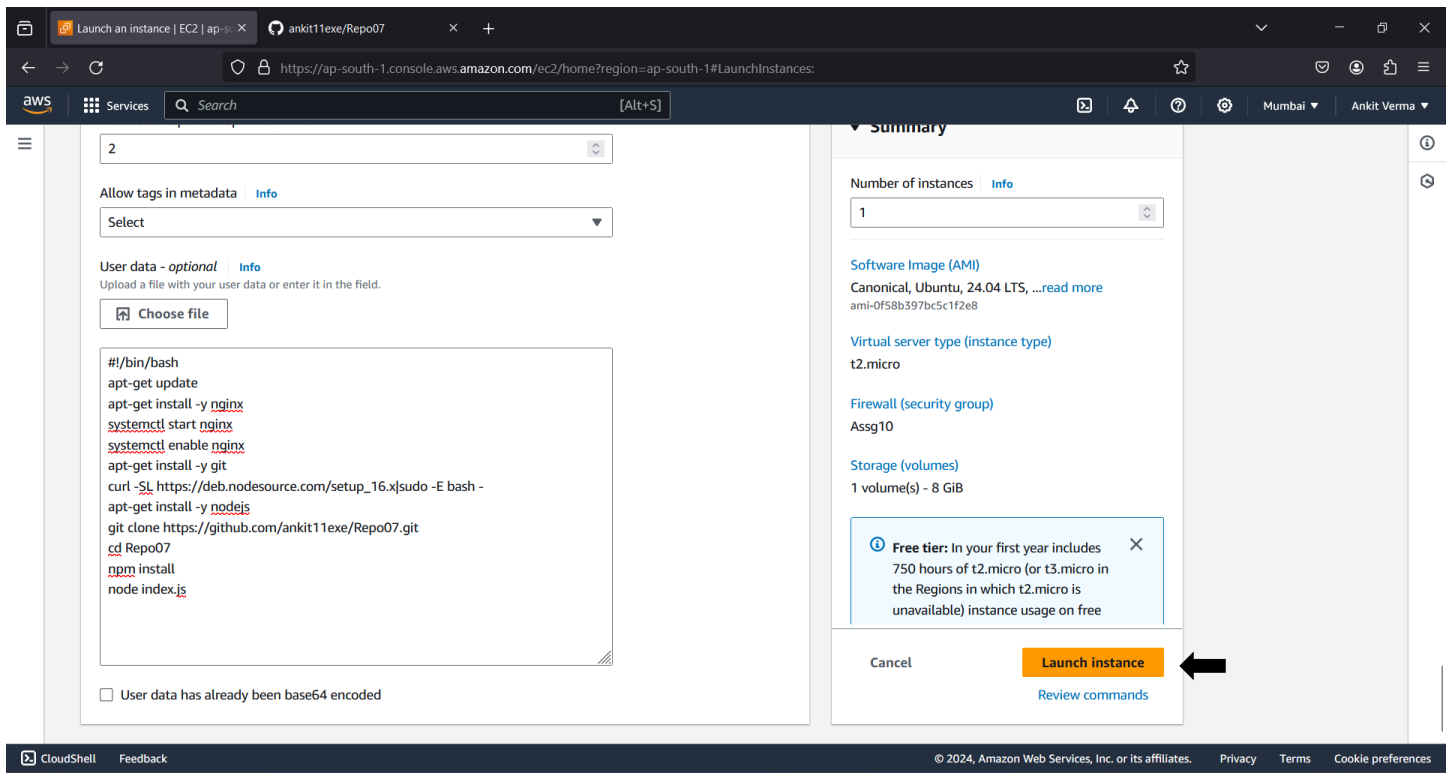
Cancel Launch instance

Review commands

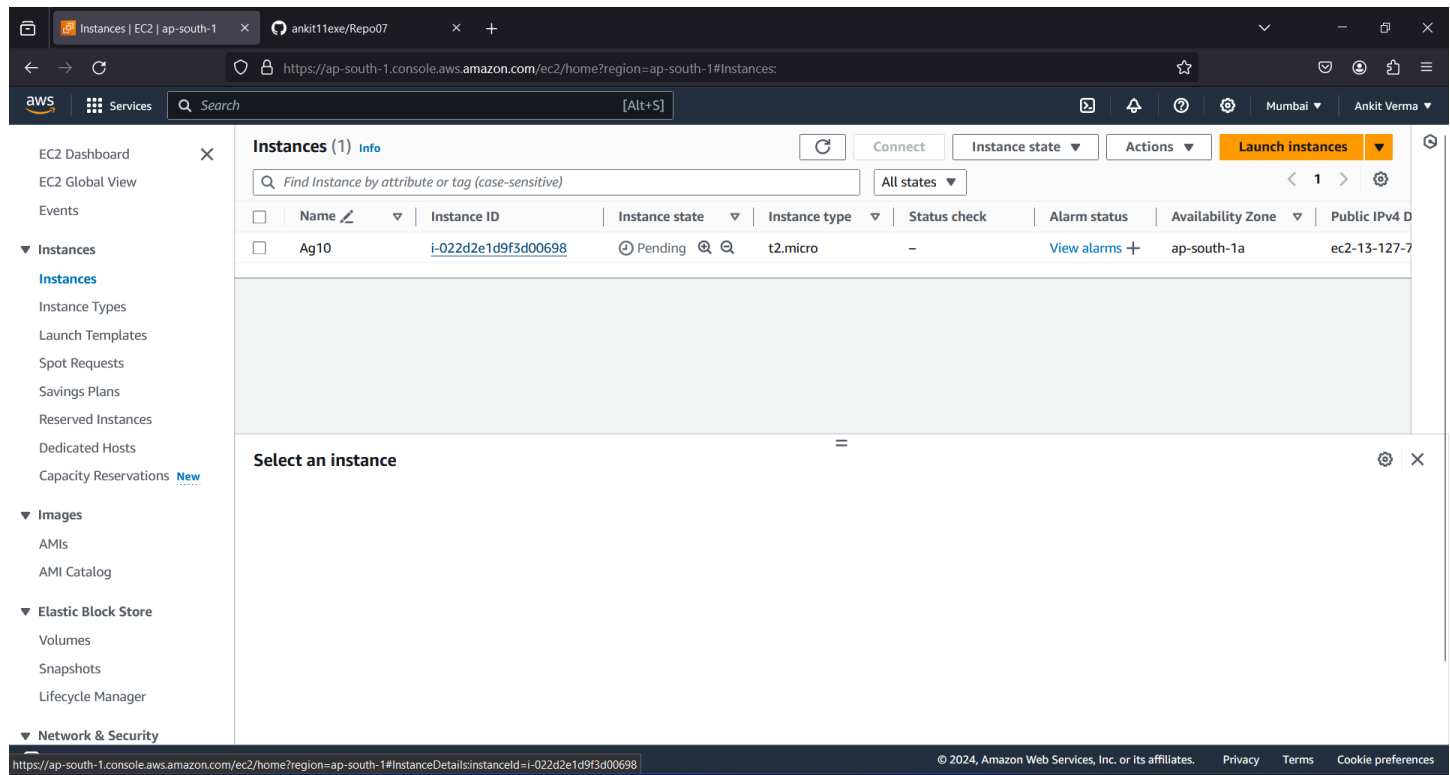
## Step 11: Expand the Advanced Details tab.



## Step 12: Scroll down to the bottom, in the bash console type the following commands. Then click on “Launch Instance”.



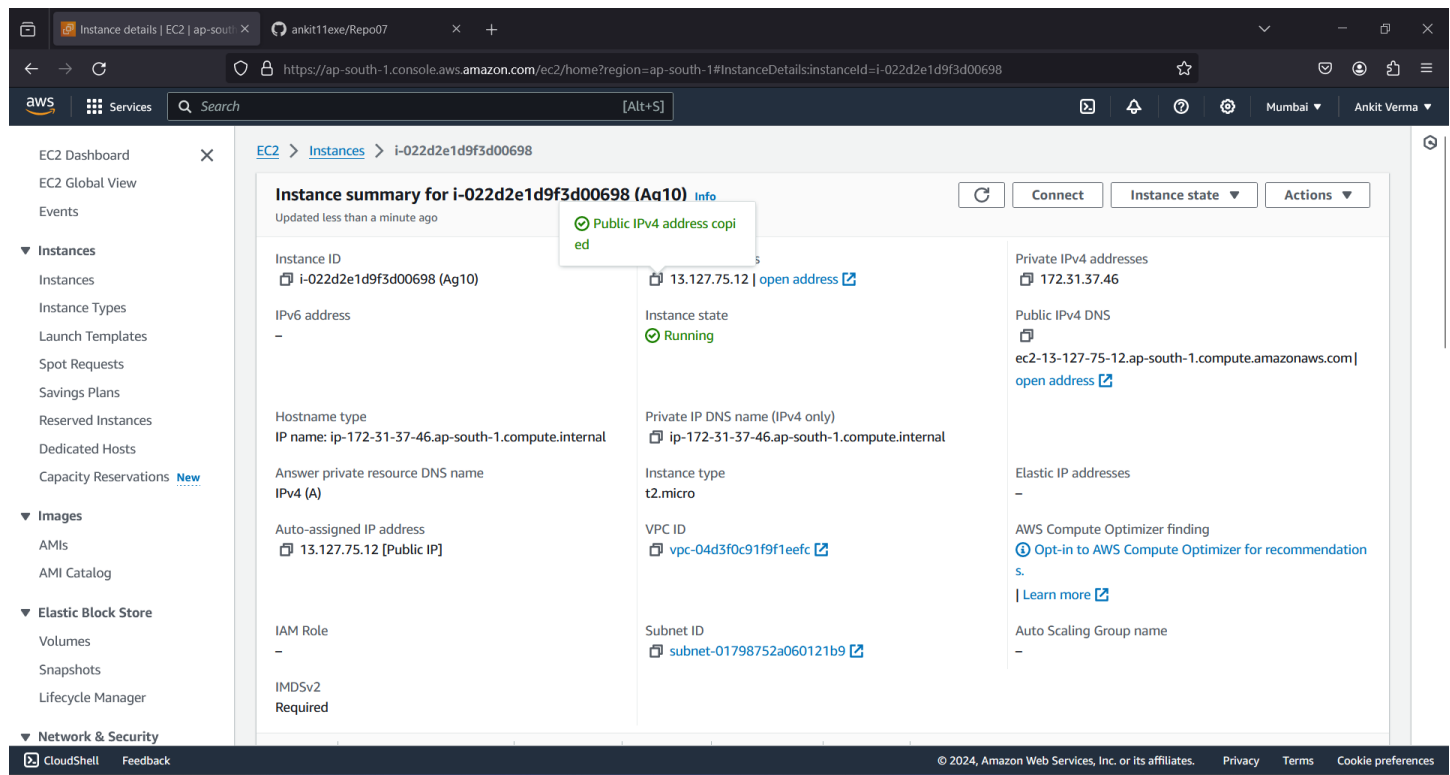
## Step 13: Click on instance id to enter into the instance.



The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page is active, displaying a table with one instance: 'Ag10' (ID: i-022d2e1d9f3d00698) in a 'Pending' state. A 'Select an instance' dialog box is open, indicating that no instance is currently selected.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
Ag10	i-022d2e1d9f3d00698	Pending	t2.micro	-	View alarms +	ap-south-1a	ec2-13-127-7

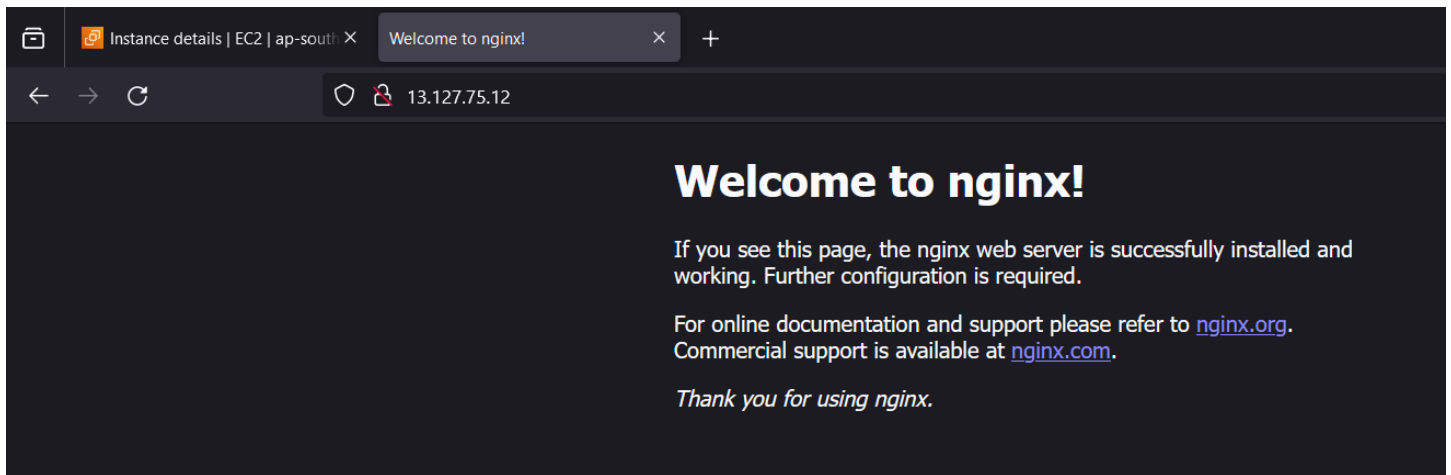
## Step 14: Copy the Public IPv4 Address.



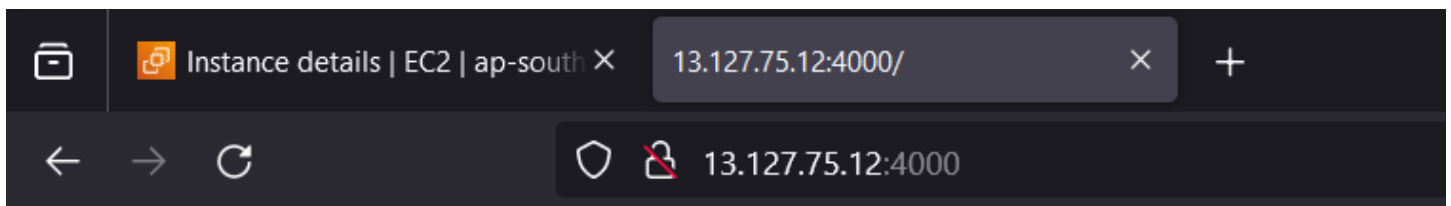
The screenshot shows the 'Instance details' page for the instance 'i-022d2e1d9f3d00698' (Ag10). The instance is in a 'Running' state. The 'Public IPv4 address' is highlighted, and a tooltip indicates it can be copied. The 'Public IPv4 address' is 172.31.37.46.

Instance ID	Instance state	Private IP DNS name (IPv4 only)	Instance type	VPC ID	Subnet ID
i-022d2e1d9f3d00698 (Ag10)	Running	ip-172-31-37-46.ap-south-1.compute.internal	t2.micro	vpc-04d3f0c91f9f1eefc	subnet-01798752a060121b9

**Step 15:** Paste the IP-Address in a new Window. Nginx window will open.



**Step 16:** The Nodejs file content will be visible. Now add “:4000” at the end of the IPv4 Address



Hello World