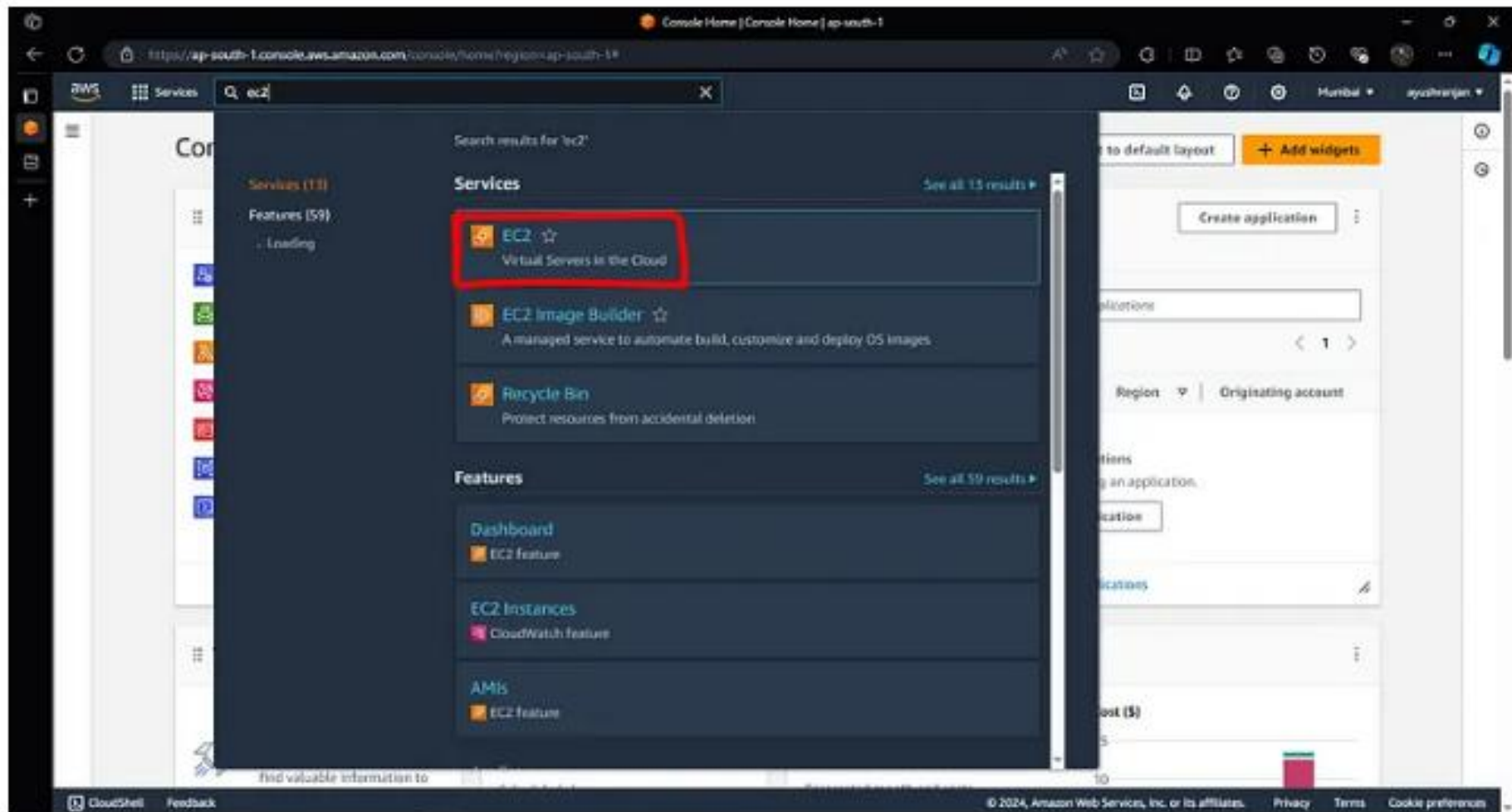


# 1. Login to AWS Management Console

- Go to the [AWS Management Console](#)
- Search for EC2 and click on the service.



## 2. Launch an Instance

- In the EC2 Dashboard, click on the **Launch Instance** button.

The screenshot displays the AWS Management Console for the EC2 service in the Asia Pacific (Mumbai) region. The left-hand navigation pane lists various EC2-related services, with 'Instances' currently selected. The main content area is divided into several sections: 'Resources' showing a summary of EC2 resources (Instances, Auto Scaling Groups, Capacity Reservations, etc.), 'Launch instance' with a prominent orange 'Launch Instance' button highlighted by a red rectangle, 'Service health' indicating the service is operating normally, and 'Instance alarms'. The right-hand sidebar contains information about the 'EC2 Free Tier', 'Account attributes', 'Settings', and 'Additional information'.

**Resources**

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

|                     |   |                     |   |                       |   |
|---------------------|---|---------------------|---|-----------------------|---|
| Instances (running) | 0 | Auto Scaling Groups | 0 | Capacity Reservations | - |
| Dedicated Hosts     | 0 | Elastic IPs         | 0 | Instances             | 0 |
| Key pairs           | 2 | Load balancers      | 3 | Placement groups      | 0 |
| Security groups     | 3 | Snapshots           | 0 | Volumes               | 0 |

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Launch Instance** (highlighted)

Migrate a server

Note: Your instances will launch in the Asia Pacific (Mumbai) Region.

**Service health**

AWS Health Dashboard

Region: Asia Pacific (Mumbai)

Status: This service is operating normally.

**Instance alarms**

View in CloudWatch

**EC2 Free Tier**

Offers for all AWS Regions.

View all AWS Free Tier offers

**Account attributes**

**Settings**

Data protection and security  
Zones  
EC2 Serial Console  
Default credit specification  
EC2 console preferences

**Additional information**

Getting started guide  
Documentation  
All EC2 resources  
Regions

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Launch an instance | EC2 | ap-south-1

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

Services Search [Alt+F]

Mumbai ayushranjan

Name and tags info

Name

AyushRanjanCloudWatchDemo

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.

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0e3db6f3757e58c7 (64-bit (x86), x86\_64-preferred) / ami-0e3db6f3757e58c7 (64-bit (x86), x86\_64)

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

Free tier eligible

Description

Summary

Number of instances info

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.5.2...read more

ami-0e3db6f3757e58c7

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 tier AMIs per month. 750 hours of public IPv4 addresses include per month. 8 GiB

Cancel

Launch instance

Review commands

CloudShell Feedback

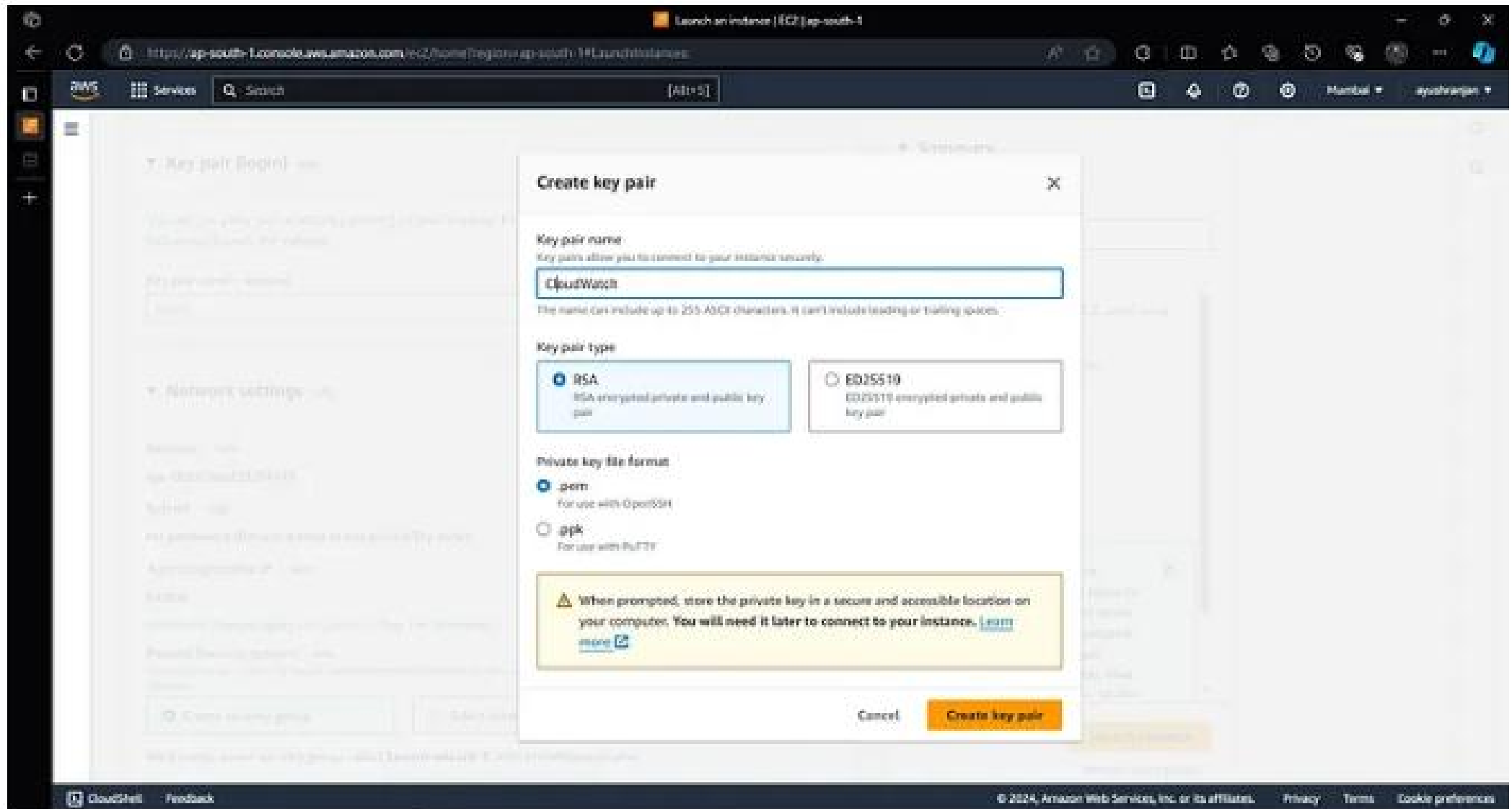
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Choose **Instance Type**:

Select **t2.micro** (Free Tier eligible) which provides 1 vCPU and 1 GB of memory.

The screenshot displays the AWS Management Console interface for launching an instance. The 'Instance type' section is highlighted with a red box, showing 't2.micro' as the selected instance type, which is 'Free tier eligible'. The 'Summary' section on the right provides a overview of the configuration: 1 instance, Amazon Linux 2023 AMI 2023.5.2, t2.micro instance type, New security group, and 1 volume(s) - 8 GiB. A 'Free tier' notification box is also visible, stating '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 tier AMIs per month, 750 hours of public IPv4 address, 1500 hours of public IPv6 address, 1500 hours of public IPv4 address, 1500 hours of public IPv6 address'. The 'Launch instance' button is highlighted in orange.

- Create a key pair



### **3. Configure Instance Settings**

- **Network:** Use the default VPC and subnet.
- **Auto-assign Public IP:** Ensure it is set to “Enable”.
- **IAM Role:** Leave this empty for now, as it’s optional for this project.

## 4. Configure Storage

- Leave the default of 8 GB SSD (General Purpose), as this is free-tier eligible.

The screenshot displays the AWS Management Console interface for launching an EC2 instance. The 'Configure storage' section is active, showing the following configuration:

- Source type:** My IP
- Name:** Add ODR prefix (if security)
- Description - optional:** e.g. SSH for admin desktop
- IP address:** 87.19.104.205/32
- Configure storage:** 8 GB gp3 Root volume (Not encrypted)
- Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.**
- Add new volume:** Button to add additional volumes.
- Click refresh to view backup information:** The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
- On File systems:** Edit
- Advanced details:** Edit

The **Summary** section on the right shows the following details:

- Number of instances:** 1
- Software image (AMI):** Amazon Linux 2023 AMI 2023.5.2
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 8 GB

A **Free tier** notification states: "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 tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GB".

At the bottom, there are buttons for **Cancel**, **Launch instance**, and **Review commands**.

## **5. Add Tags**

- Tags can help organize your resources, but you can skip this for now.



## 6. Configure Security Group

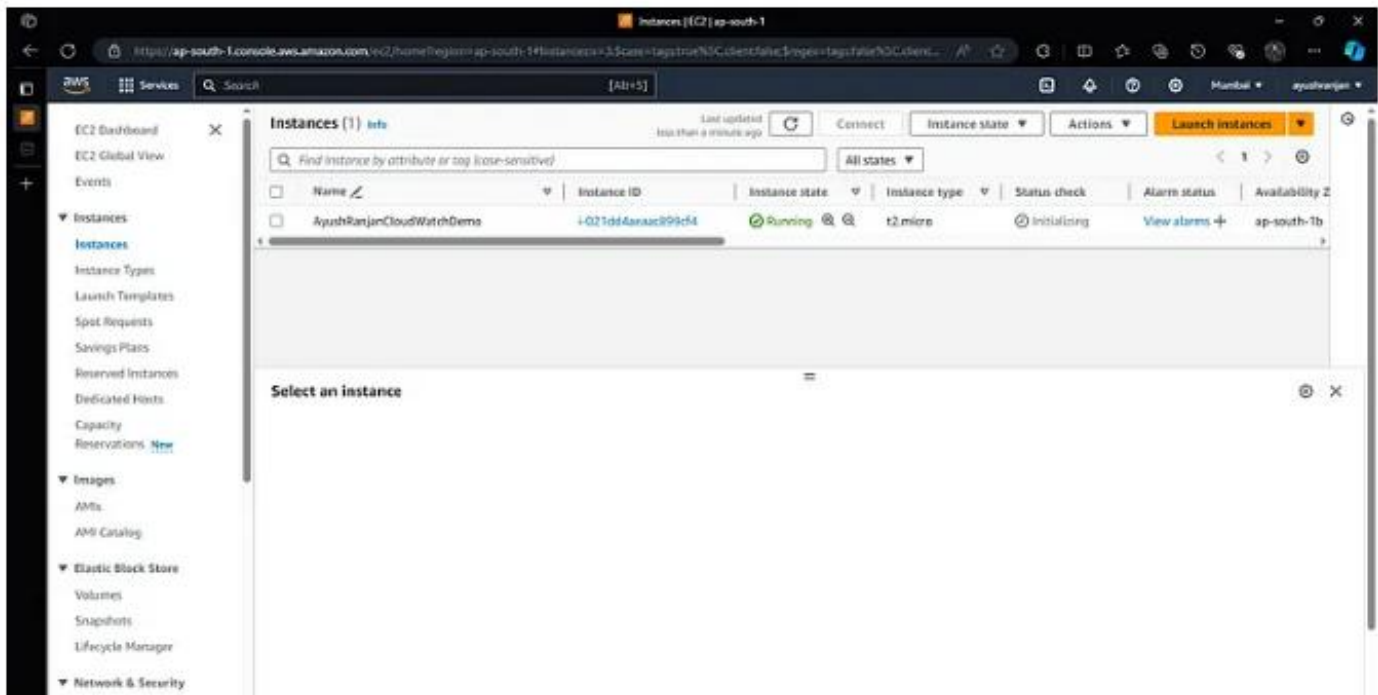
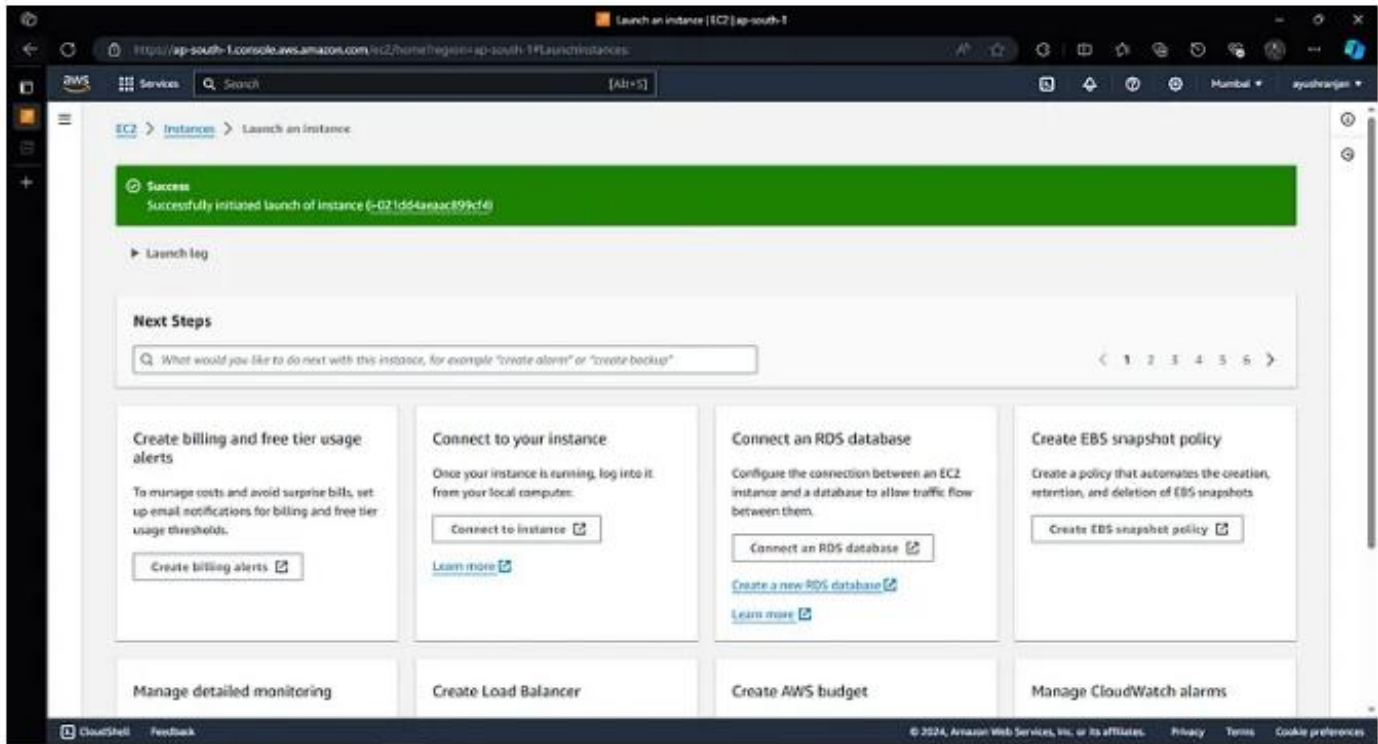
- Create a new security group and allow SSH (port 22) from your IP address.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The 'Network settings' tab is active. In the 'Firewall (security groups)' section, the 'Create security group' button is selected. The 'Security group name' is 'launch-wizard-3' and the 'Description' is 'launch-wizard-3 created 2024-09-15T03:31:33.741Z'. Under 'Inbound Security Group Rules', a rule is added with 'Type' set to 'ssh', 'Protocol' set to 'TCP', and 'Port range' set to '22'. The 'Source type' is set to 'My IP'. A red circle highlights the 'Type', 'Protocol', 'Port range', and 'Source type' fields. A red box highlights the 'Add CIDR, prefix list or security group' button.

- Add HTTP (port 80) if you plan to host a web application, but this isn't necessary for our CloudWatch project.

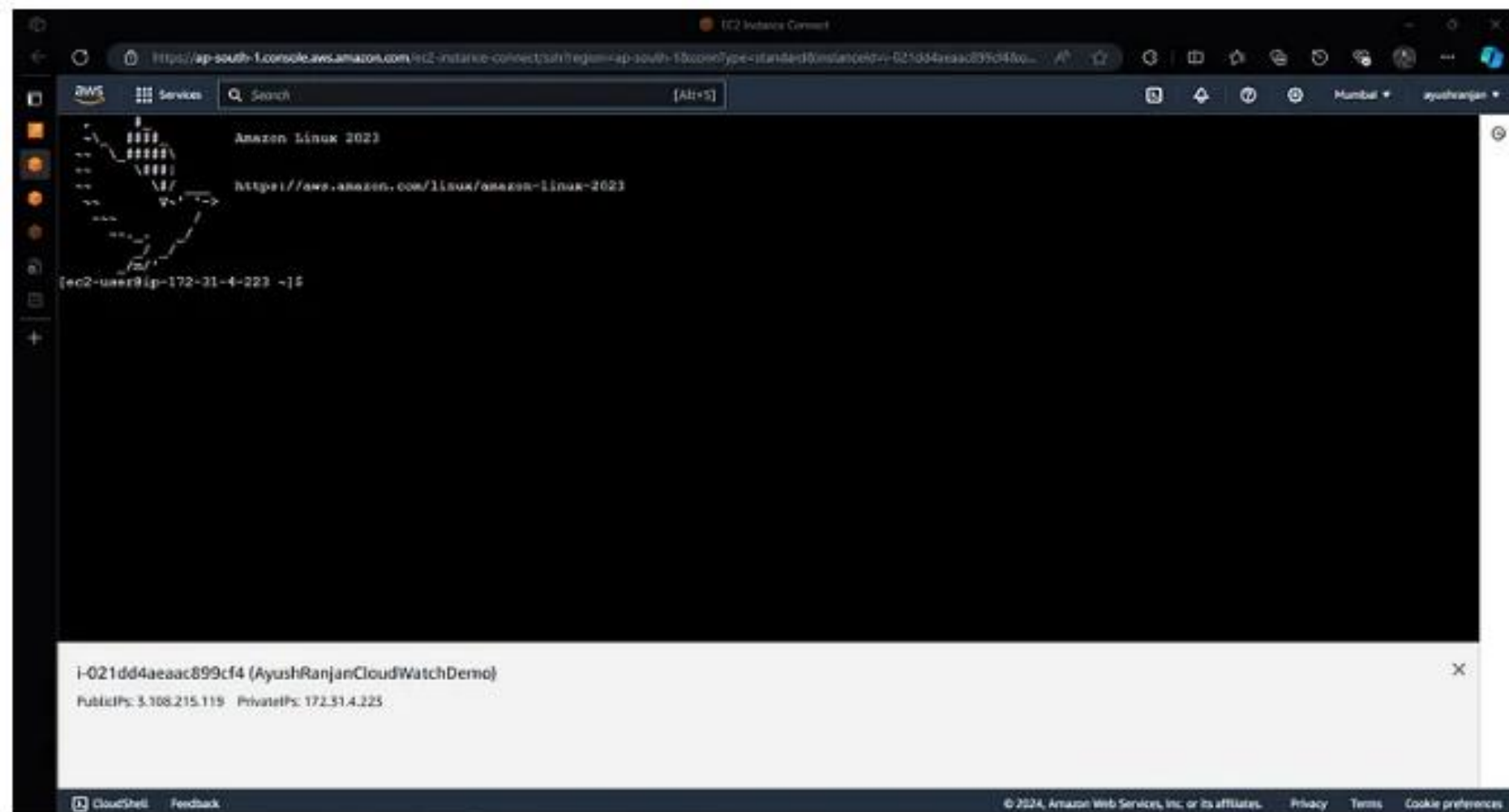
## 7. Launch Instance

- Finally, click on Launch Instance.



## 8. Access Your EC2 Instance

- Once the instance is running, you can SSH or connect to instance using EC2 Instance Connect

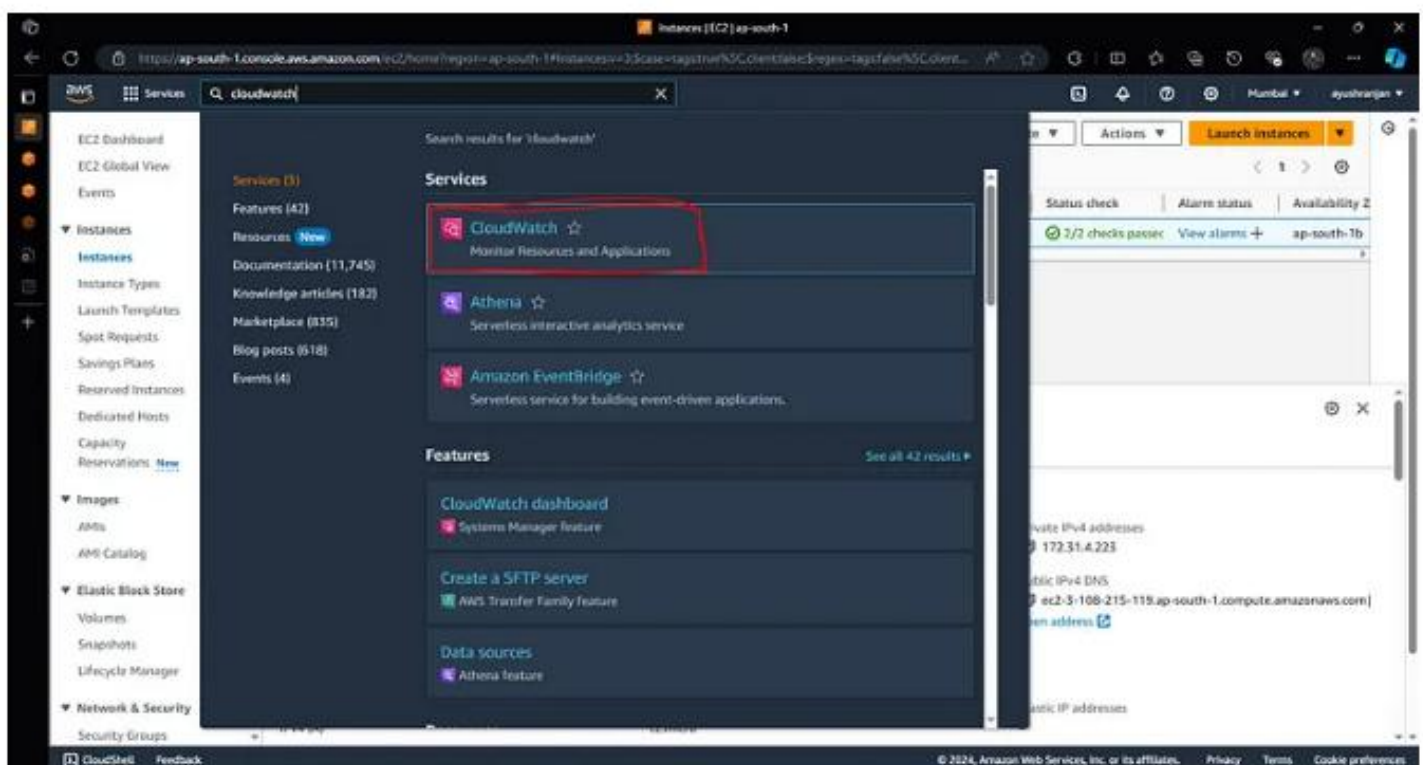


## Step 2: Enable Basic CloudWatch Monitoring

By default, CloudWatch provides basic monitoring for EC2 instances, including metrics like CPU utilization, network in/out, and disk I/O. This data is collected at 5-minute intervals and is completely free within the AWS Free Tier.

### 1. Navigate to the CloudWatch Console

- In the AWS Management Console, search for **\*\*CloudWatch\*\*** and click on the service.





## 2. Check Default Metrics

- On the CloudWatch Dashboard, click on **Metrics** in the left-hand menu. In the **Browse** tab, click on **EC2** under the list of services.

The screenshot shows the AWS CloudWatch Metrics console interface. The left-hand navigation menu is visible, with the 'Metrics' section expanded and 'All metrics' highlighted. The main area displays the 'Browse' tab, showing a search for 'ec2' in the 'Metrics (246)' section. The search results are displayed in a grid of service tiles, including EBS, EC2, Events, Lambda, Logs, RDS, and Usage. The EC2 tile is highlighted with a red rectangle, indicating it is the selected service. The top of the console shows the 'Untitled graph' section with various time range and action options.

CloudWatch Metrics (246) Info

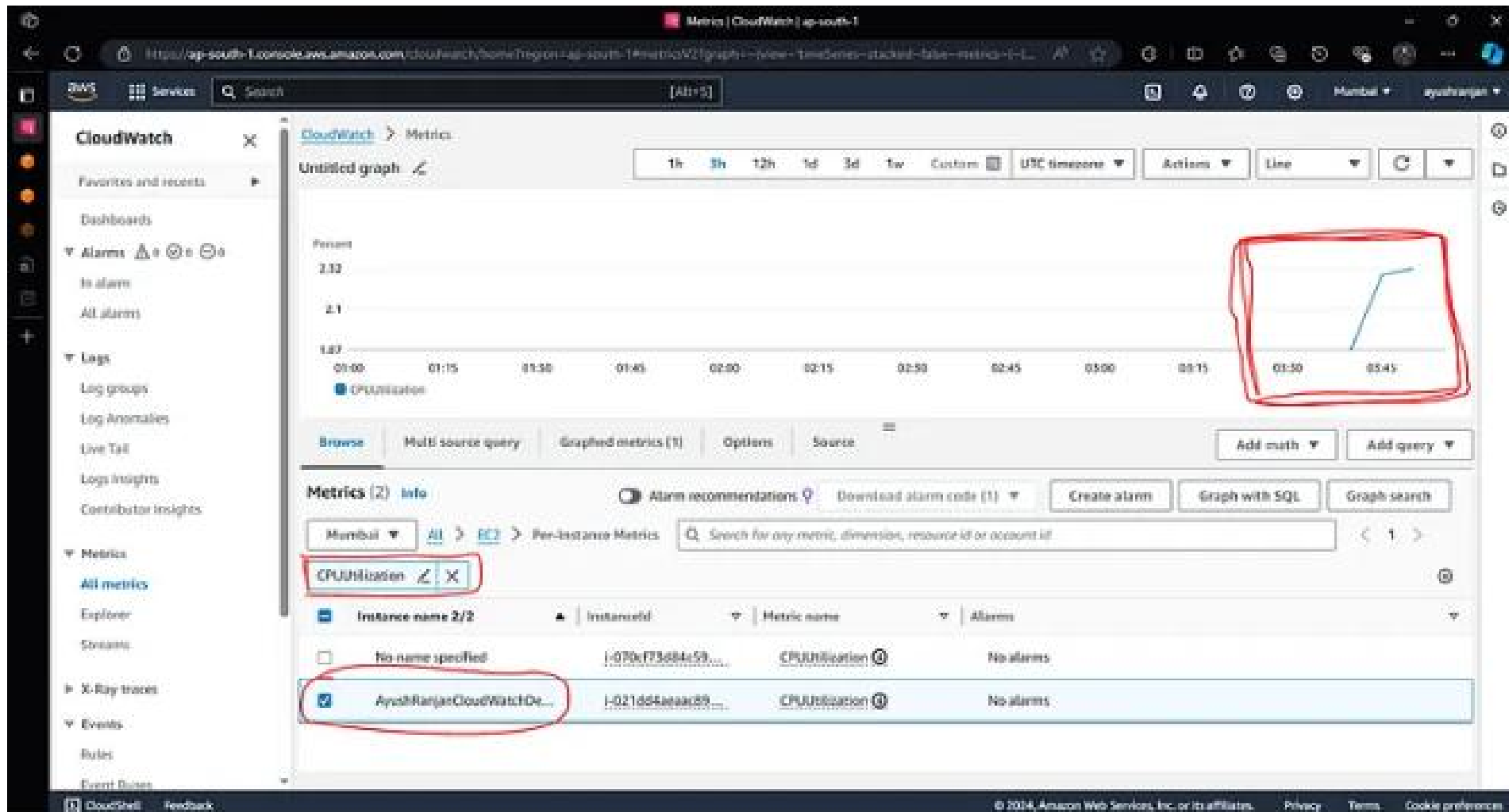
Alarm recommendations Download alarm code Create alarm Graph with SQL Graph search

Mumbai ec2

|                                       |                                      |   |   |
|---------------------------------------|--------------------------------------|---|---|
| EBS 17<br>• View automatic dashboard  | EC2 36<br>• View automatic dashboard | Events 1<br>• View automatic dashboard  | Lambda 17<br>• View automatic dashboard |
| Logs 14<br>• View automatic dashboard | RDS 4<br>• View automatic dashboard  | Usage 157<br>• View automatic dashboard |   |

© 2024 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- You will see metrics for your running EC2 instance, including CPUUtilization, NetworkIn, and NetworkOut.



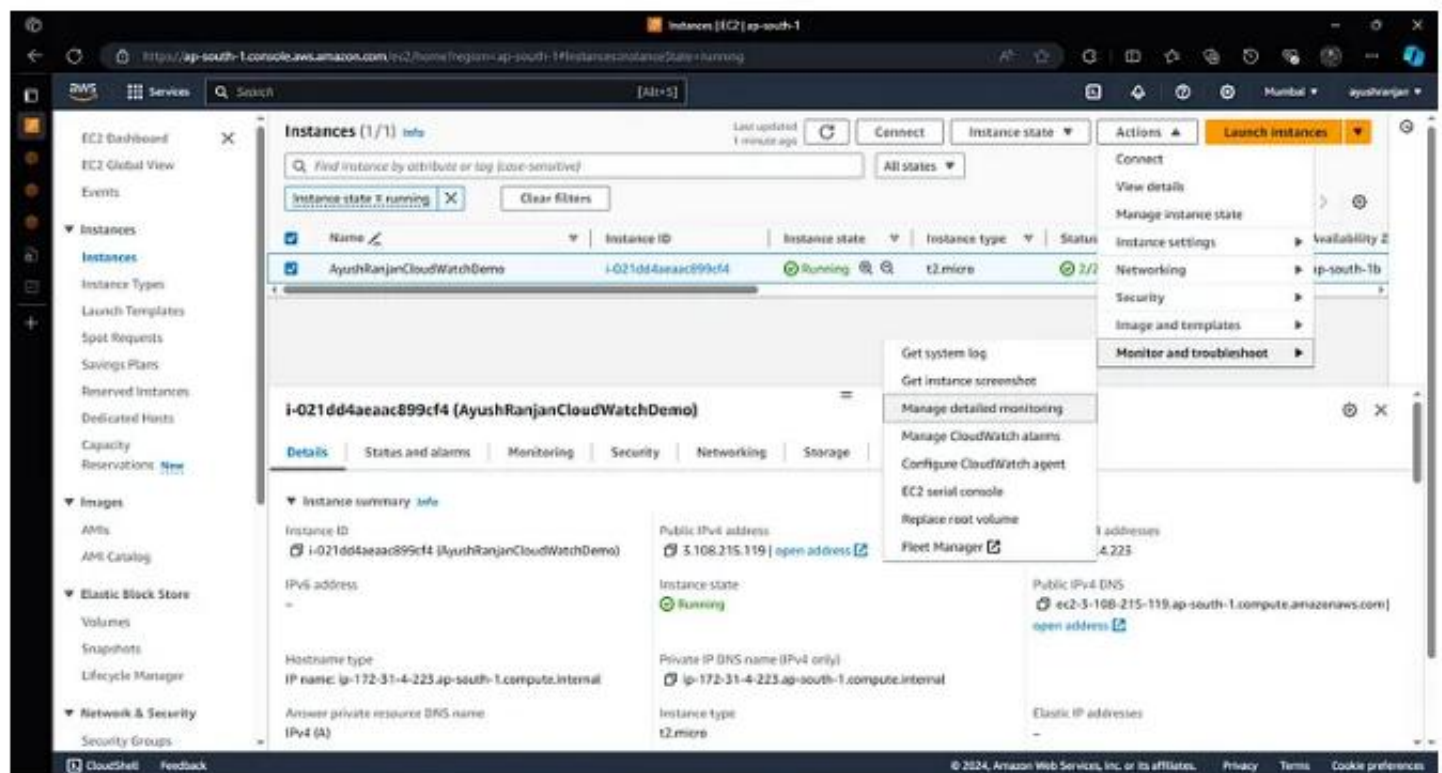
## Step 3: Enable Detailed Monitoring

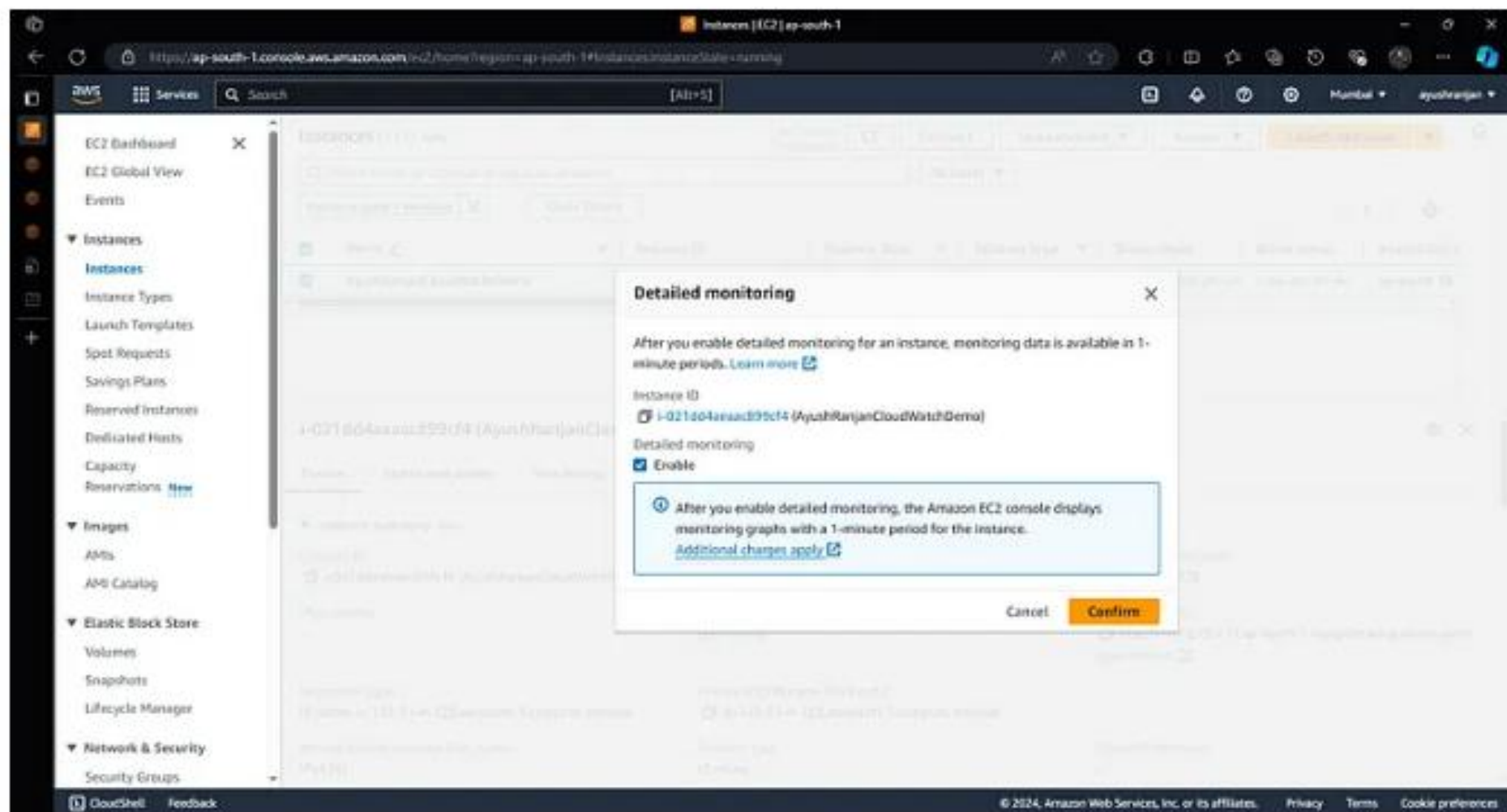
Detailed monitoring collects metrics at 1-minute intervals instead of the default 5-minute interval. While this is generally not needed for basic workloads, it can be useful for more precise monitoring.

It is not free but costs a minimal amount if you go beyond the free tier.

### 1. Enable Detailed Monitoring for EC2

- Navigate back to the EC2 Dashboard.
- Select your running instance.
- Under Actions in the top-right corner, choose **Monitor and troubleshoot** and click **Enable Detailed Monitoring**.





**Important:** Detailed monitoring is not free but is charged at around \$0.30 per instance per month if you use it beyond free-tier limits. For this guide, it's optional.

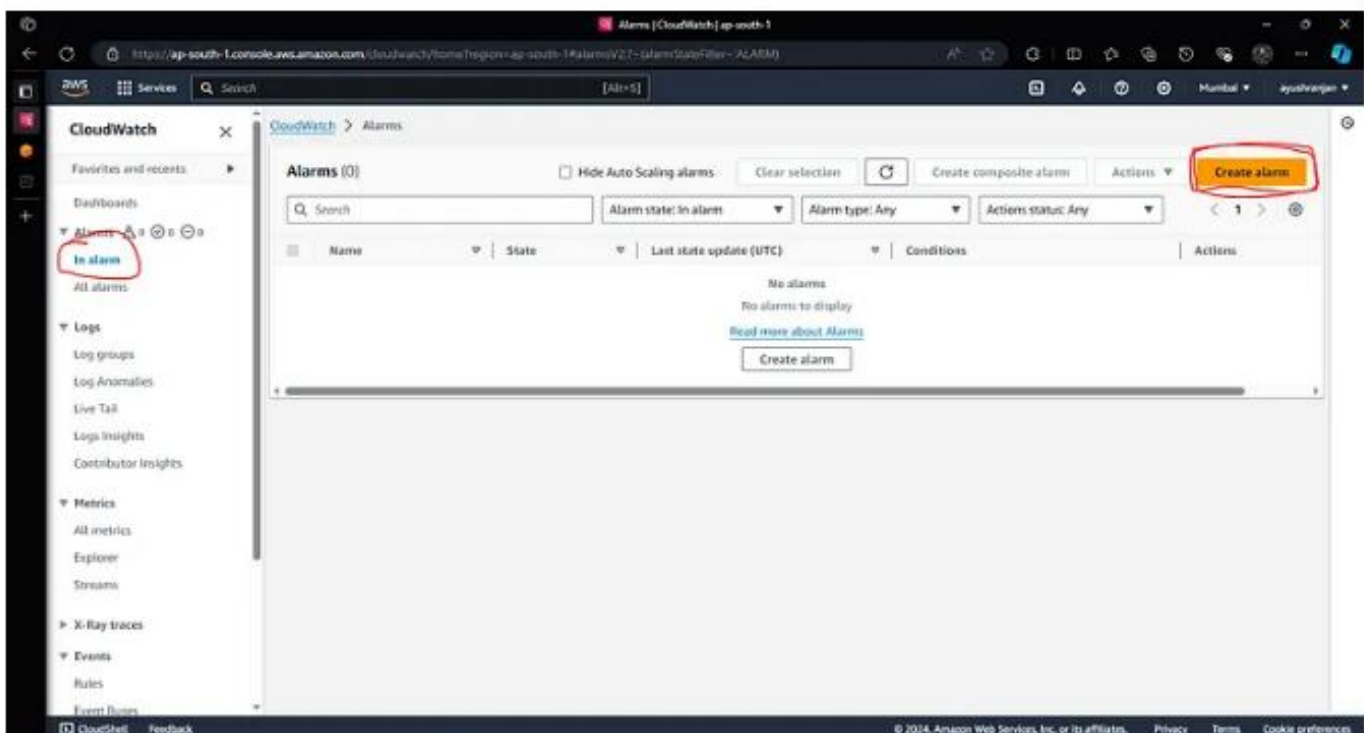


## Step 4: Set Up CloudWatch Alarms for EC2

Now, we will create a CloudWatch Alarm to notify you when the EC2 instance's CPU utilization exceeds a specific threshold (e.g., 70%). You can stay within the AWS Free Tier as alarms are included up to 10 alarms per month.

### 1. Navigate to Alarms in CloudWatch

- In the CloudWatch console, select **Alarms** from the left-hand menu.
- Click on **Create Alarm**.



## 2. Select the Metric for CPU Utilization

- Click Select metric.
- In the Browse tab, choose EC2 > Per-Instance Metrics.  
Locate your EC2 instance and select CPUUtilization as the metric to monitor.
- Click Select metric.

The screenshot shows the AWS CloudWatch 'Select metric' dialog box. The 'Browse' tab is active, displaying a breadcrumb path: Mumbai > EC2 > Per-Instance Metrics. A search filter 'ec2' is applied. A table lists metrics for instance 'i-070cf73d84c59...'. The 'CPUUtilization' metric is selected with a checkbox. The 'Select metric' button is highlighted in orange at the bottom right.

| Instance name 16/36                                   | Instance ID        | Metric name         | Alarms    |
|---|--------------------|---------------------|-----------|
| <input checked="" type="checkbox"/> No name specified | i-070cf73d84c59... | CPUUtilization ⓘ    | No alarms |
| <input type="checkbox"/> No name specified            | i-070cf73d84c59... | DiskReadOps ⓘ       | No alarms |
| <input type="checkbox"/> No name specified            | i-070cf73d84c59... | NetworkPacketsOut ⓘ | No alarms |

### 3. Set a Threshold

- In the conditions section, set the alarm threshold to notify you when CPU usage is higher than 70%.
- For **Whenever CPU utilization is**, choose **Greater/Equal to** and set the threshold value to 70.

The screenshot shows the AWS CloudWatch 'Create alarm' wizard, specifically the 'Set a Threshold' step. The 'Threshold type' is set to 'Static' (Use a value as a threshold). The condition is 'Whenever CPUUtilization is...'. The 'Define the alarm condition' section shows 'Greater/Equal to threshold' selected. The 'Define the threshold value' section shows the value '70' entered. The 'Additional configuration' section shows 'Datapoints to alarm' set to '1 out of 1' and 'Missing data treatment' set to 'Treat missing data as missing'. The 'Next' button is highlighted in orange.

Threshold type

☒ Static  
Use a value as a threshold

☐ Anomaly detection  
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition

☐ Greater  
> threshold

☒ Greater/Equal  
≥ threshold

☐ Lower/Equal  
≤ threshold

☐ Lower  
< threshold

then...

Define the threshold value

70

Must be a number

Additional configuration

Datapoints to alarm

Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

1 out of 1

Missing data treatment

How to treat missing data when evaluating the alarm.

Treat missing data as missing

Cancel Next

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 4. Set Period and Datapoints

- Set the evaluation period to 5 minutes (free tier eligible).

The screenshot shows the AWS CloudWatch console interface for creating a new alarm. The page title is 'Specify metric and conditions'. On the left, there is a sidebar with a navigation menu and a list of steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). The main content area is divided into two sections: 'Metric' and 'Conditions'. The 'Metric' section contains a graph showing CPU utilization over time, with a red dashed line indicating the alarm threshold at 75%. Below the graph, there are input fields for 'Namespace' (AWS/EC2), 'Metric name' (CPUUtilization), 'InstanceId' (i-070c173d84c597cb8), 'Instance name' (No name specified), and 'Statistic' (Average). The 'Period' field is highlighted with a red box and set to '5 minutes'. The 'Conditions' section is currently empty.

Create alarm | Alarms | CloudWatch | ap-south-1

http://ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#alarmsV2:create?--(Page--MetricDetection--AlarmType--MetricAlarm--)

Services Search [All+5]

Step 1: Specify metric and conditions

Step 2: Configure actions

Step 3: Add name and description

Step 4: Preview and create

### Specify metric and conditions

Alarm recommendations View details

#### Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

No unit 75

70 75

60 01:30 02:30 03:30

CPUUtilization

Namespace: AWS/EC2

Metric name: CPUUtilization

InstanceId: i-070c173d84c597cb8

Instance name: No name specified

Statistic: Average

Period: 5 minutes

#### Conditions

CloudShell Feedback

© 2014, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Set the number of datapoints to 1 out of 1.

The screenshot shows the 'Create alarm' wizard in the AWS CloudWatch console. The 'Threshold type' is set to 'Static'. The condition is 'Whenever CPUUtilization is... Greater/Equal to threshold'. The threshold value is '30'. Under 'Additional configuration', 'Datapoints to alarm' is set to '1 out of 1', and 'Missing data treatment' is set to 'Treat missing data as missing'.

Create alarm | Alarm | CloudWatch | ap-south-1

https://ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#alarms/create?--(Page--MetricSelection--AlarmType--MetricAval...

Services Search [Alt+S]

Mumbai Sydney

**Threshold type**

☒ **Static**  
Use a value as a threshold

☐ **Anomaly detection**  
Use a band as a threshold

**Whenever CPUUtilization is...**  
Before the alarm condition:

☐ Greater  
is threshold

☒ **Greater/Equal**  
is threshold

☐ Lower/Equal  
is threshold

☐ Lower  
is threshold

**then...**  
Before the threshold value:

30

Must be a number

**Additional configuration**

**Datapoints to alarm**  
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

1 out of 1

**Missing data treatment**  
How to treat missing data when evaluating the alarm.

Treat missing data as missing

Cancel Next

CloudShell Feedback

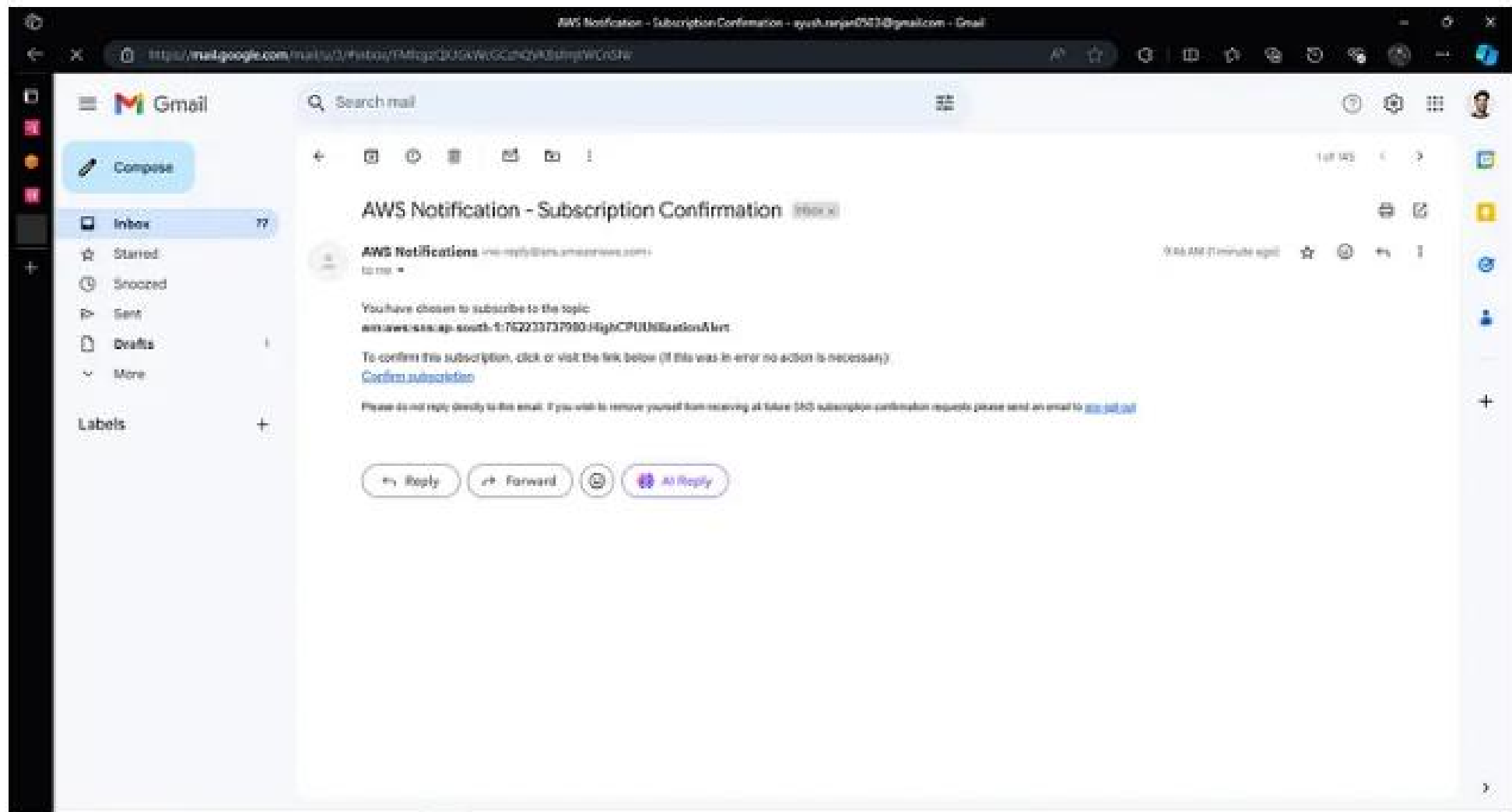
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



## 5. Configure Actions

- Choose to trigger an action when the alarm state is reached. Select **Create new topic** to send an email notification.
- Enter a name for the topic (e.g., `HighCPUUtilizationAlert`) and input your email address.
- Confirm the SNS topic by clicking on the verification link sent to your email.

The screenshot shows the AWS CloudWatch 'Create alarm' console, specifically the 'Configure actions' step. The left sidebar shows the progress: Step 1 (Add name and description), Step 2 (Configure actions), and Step 3 (Preview and create). The main content area is titled 'Configure actions' and includes a 'Remove' button. Under 'Alarm state trigger', three options are shown: 'In alarm' (selected), 'OK', and 'Insufficient data'. Below this, the section 'Send a notification to the following SNS topic' has three radio buttons: 'Select an existing SNS topic', 'Create new topic' (selected), and 'Use topic ARN to notify other accounts'. The 'Create a new topic...' section shows the topic name 'HighCPUUtilizationAlert' entered in a text field. Below this, the 'Email endpoints that will receive the notification...' section has a text field with an email address entered. At the bottom, there are two buttons: 'Create topic' and 'Add notification'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.



- Don't forget to subscribe the SNS by the link in the email.

## 6. Name and Create the Alarm

- Name your alarm (e.g., `High\_CPU\_Alarm`) for easy identification.
- Review the settings and click **Create Alarm**.

The screenshot shows the AWS CloudWatch console in the 'ap-south-1' region, specifically the 'Create alarm' wizard. The browser address bar shows the URL: `https://ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#alarm/ZoneAlert?--(Page=Details--AlarmType=MetricAlarm--Ala...`. The left sidebar shows the navigation menu with 'Alarms' selected, and the 'Create alarm' wizard steps: Step 1: Specify metric and conditions, Step 2: Configure actions, Step 3: Add name and description (current step), and Step 4: Preview and create. The main content area is titled 'Add name and description' and contains a form with the following fields:

- Name and description** section:
  - Alarm name:** A text input field containing 'High\_CPU\_Alarm'.
  - Alarm description - optional:** A text area with a 'View formatting guidelines' link. It includes a 'Preview' button and a 'Markdown' icon. The description text is: `# This is an R1`, `**double asterisks will produce strong character**`, and `This is [an example](https://example.com/) inline link.`
- Character count:** A label indicating 'Up to 1024 characters (0/1024)'.
- Warning box:** A blue box with an information icon stating: 'Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.'
- Navigation buttons:** 'Cancel', 'Previous', and 'Next' buttons at the bottom right.

The footer of the console shows 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.



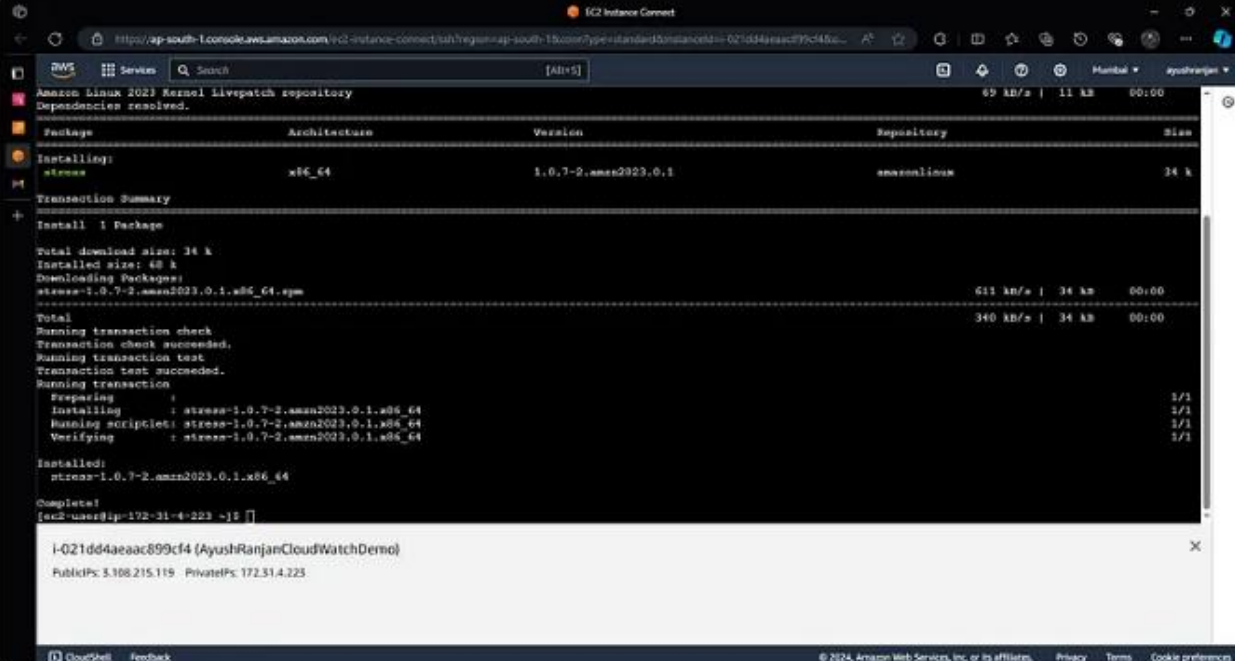
## Step 5: Test the Alarm

- To ensure everything is set up correctly, you can test the alarm by artificially increasing CPU usage on your instance.

### 1. Install Stress Tool

- On Amazon Linux 2023, install the `stress` tool, which will generate CPU load:

```
sudo yum install stress -y
```



The screenshot shows the AWS CloudShell interface with the terminal output of the command `sudo yum install stress -y`. The terminal displays the following information:

- Amazon Linux 2023 Kernel livepatch repository. Dependencies resolved.
- Package list table:

| Package            | Architecture | Version              | Repository  | Size |
|--------------------|--------------|----------------------|-------------|------|
| Installing: stress | x86_64       | 1.0.7-2.amzn2023.0.1 | amazonlinux | 34 k |

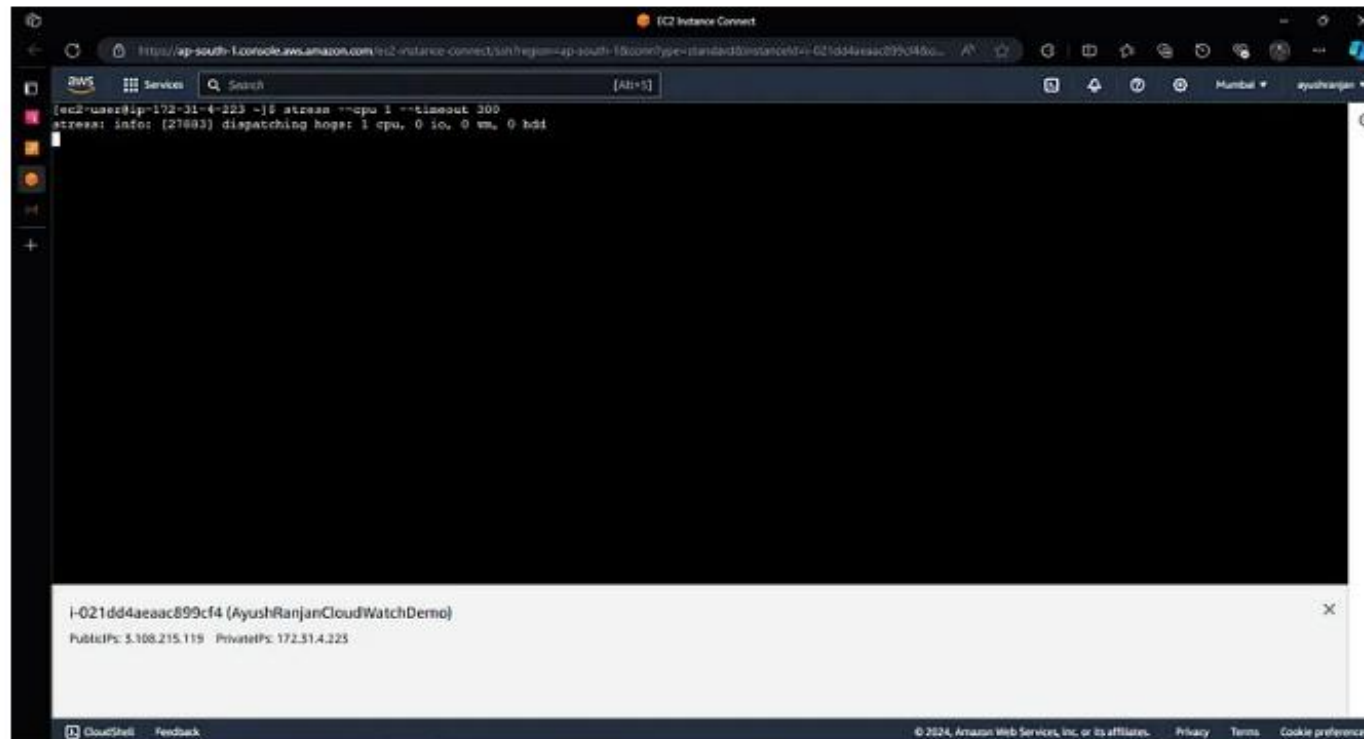
- Transaction Summary: Install 1 Package
- Total download size: 34 k, Installed size: 48 k
- Downloading Packages: stress-1.0.7-2.amzn2023.0.1.x86\_64.rpm (611 kB/s | 34 kB | 00:00)
- Total: 340 kB/s | 34 kB | 00:00
- Running transaction check, Transaction check succeeded.
- Running transaction test, Transaction test succeeded.
- Running transaction: Installing, Running scriptlet, Verifying (all 1/1)
- Installed: stress-1.0.7-2.amzn2023.0.1.x86\_64
- Complete!
- Shell prompt: [ec2-user@ip-172-31-4-223 ~]\$

At the bottom, a box displays the instance ID `i-021dd4aeac899cf4` (AyushRanjanCloudWatchDemo) and its Public IP `5.108.215.119` and Private IP `172.31.4.223`.

## 2. Generate CPU Load

- Run the following command to stress the CPU for 5 minutes:

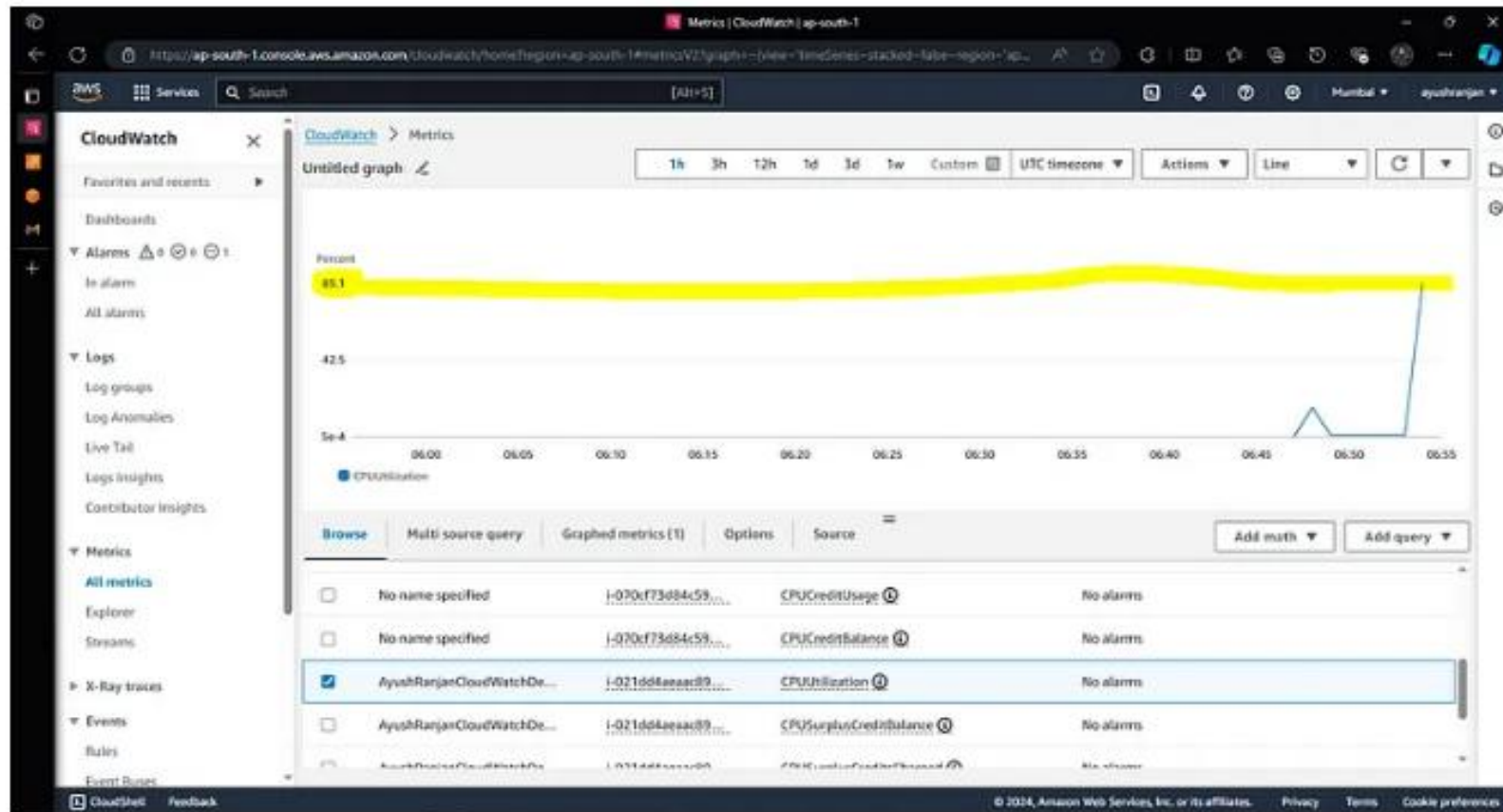
```
stress --cpu 1 --timeout 300
```



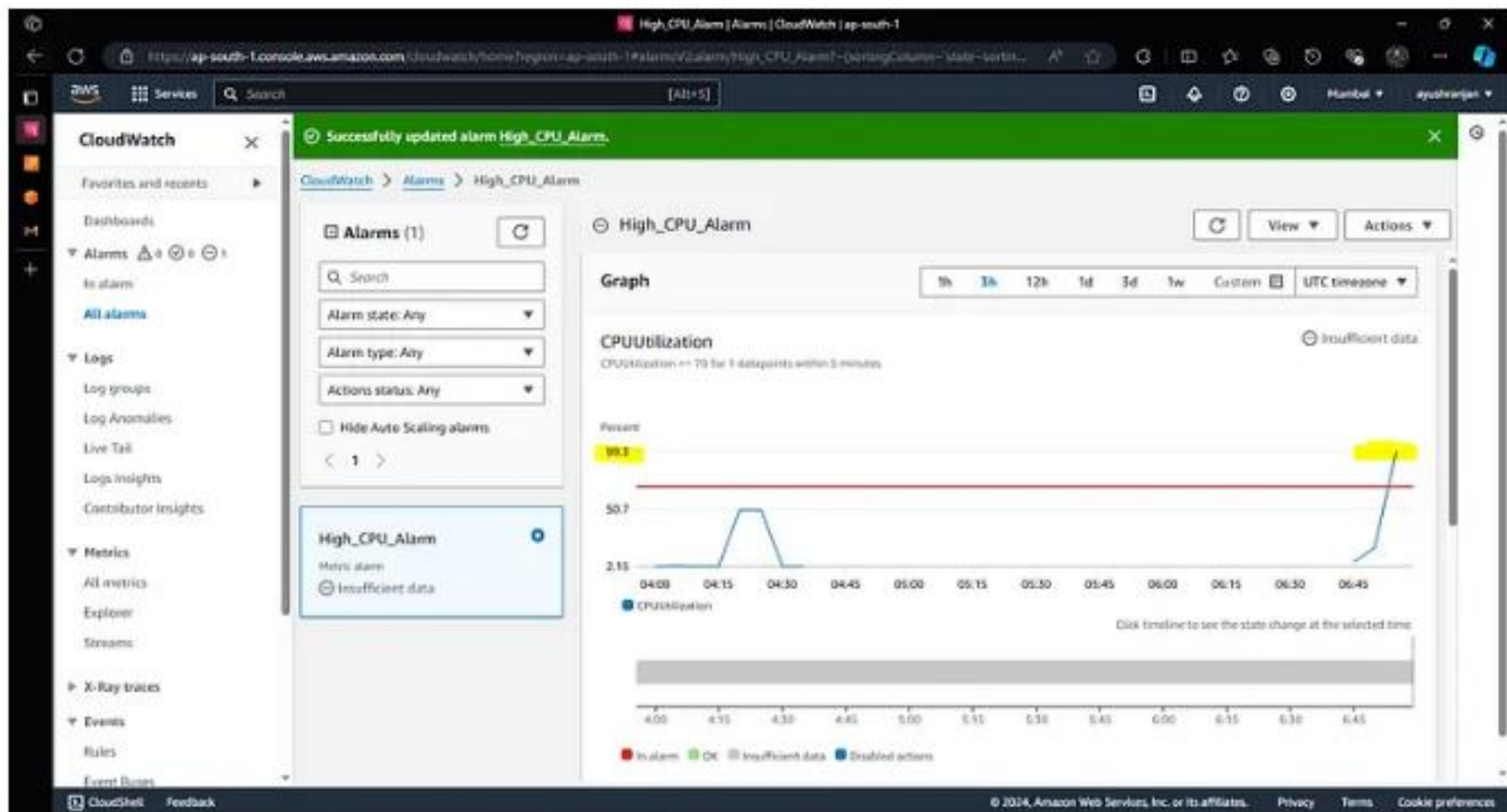
This command will use 1 CPU core for 5 minutes, increasing the CPU utilization enough to trigger the CloudWatch alarm.

## 4. Monitor CloudWatch

- Head over to the CloudWatch console and observe the CPU utilization metrics for your EC2 instance.
- Within a few minutes, you should see the CPU utilization rise and cross the **70% threshold**, triggering the alarm.

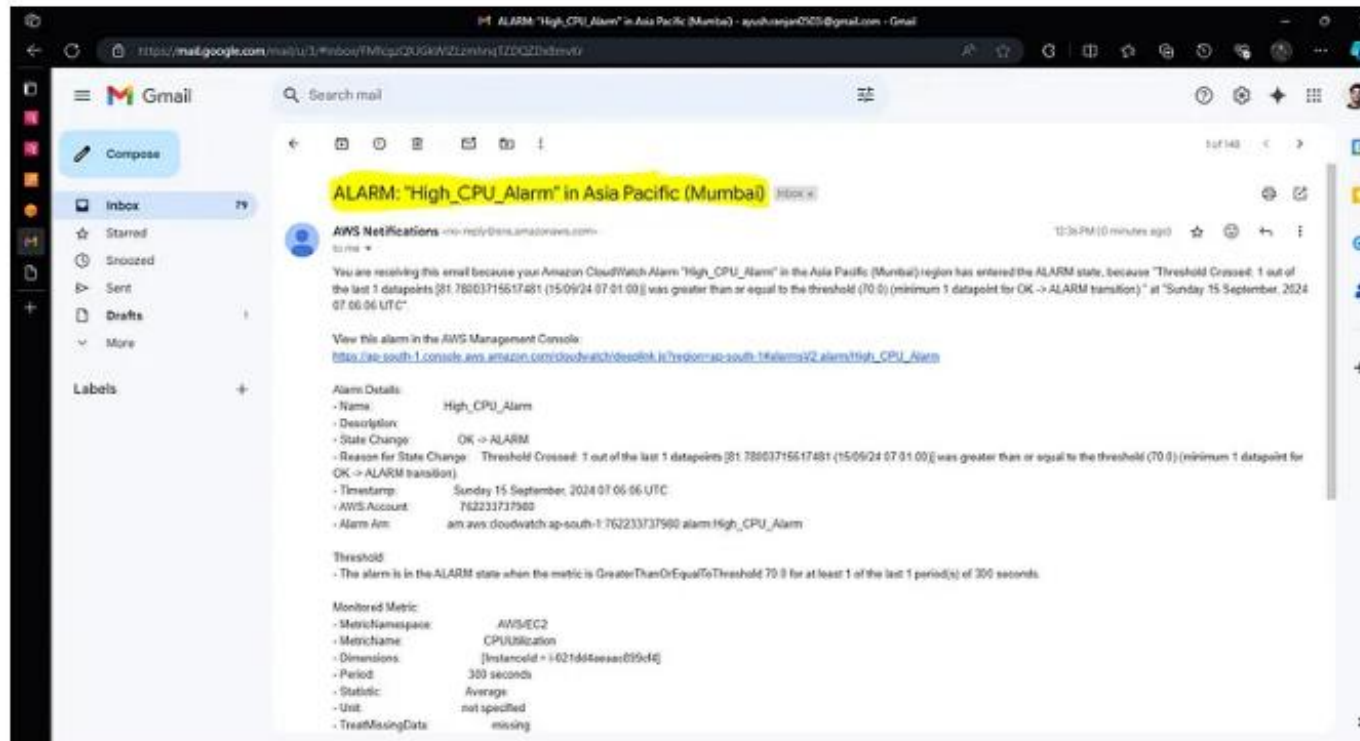


- See at the alarms section



## Step 6: Respond to the Alarm

Once the alarm is triggered, you will receive an email notification.



If the load persists, you can:

- Scale up the instance (increase the instance size to handle more traffic).
  - Investigate the process causing high CPU utilization.
  - Implement auto-scaling based on CloudWatch metrics to handle varying traffic loads.