

# CLOUD WATCH

Amazon CloudWatch is a monitoring and observability service provided by Amazon Web Services (AWS) that offers real-time insights into your AWS resources and applications. It enables you to collect and track metrics, monitor log files, set alarms, and automatically respond to changes in your AWS environment.

## Key Features of Amazon CloudWatch:

- **Metrics Collection:** CloudWatch collects and tracks metrics from various AWS services, such as Amazon EC2, providing visibility into resource utilization, application performance, and operational health.
- **Alarms:** You can set alarms to automatically initiate actions based on predefined thresholds for your metrics.
- **Logs Monitoring:** CloudWatch allows you to monitor, store, and access log files from various sources, providing a unified view of your logs.
- **Events:** It detects and responds to changes in your AWS resources, allowing you to react promptly to operational changes.

## How Amazon CloudWatch Works:

1. **Data Collection:** AWS services, such as Amazon EC2, automatically send metrics to CloudWatch. You can also publish your own custom metrics to CloudWatch.
2. **Monitoring and Visualization:** CloudWatch enables you to monitor your complete stack (applications, infrastructure, network, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR).
3. **Automated Actions:** Based on the alarms set, CloudWatch can trigger actions like sending notifications or executing automated responses to manage your AWS resources effectively.

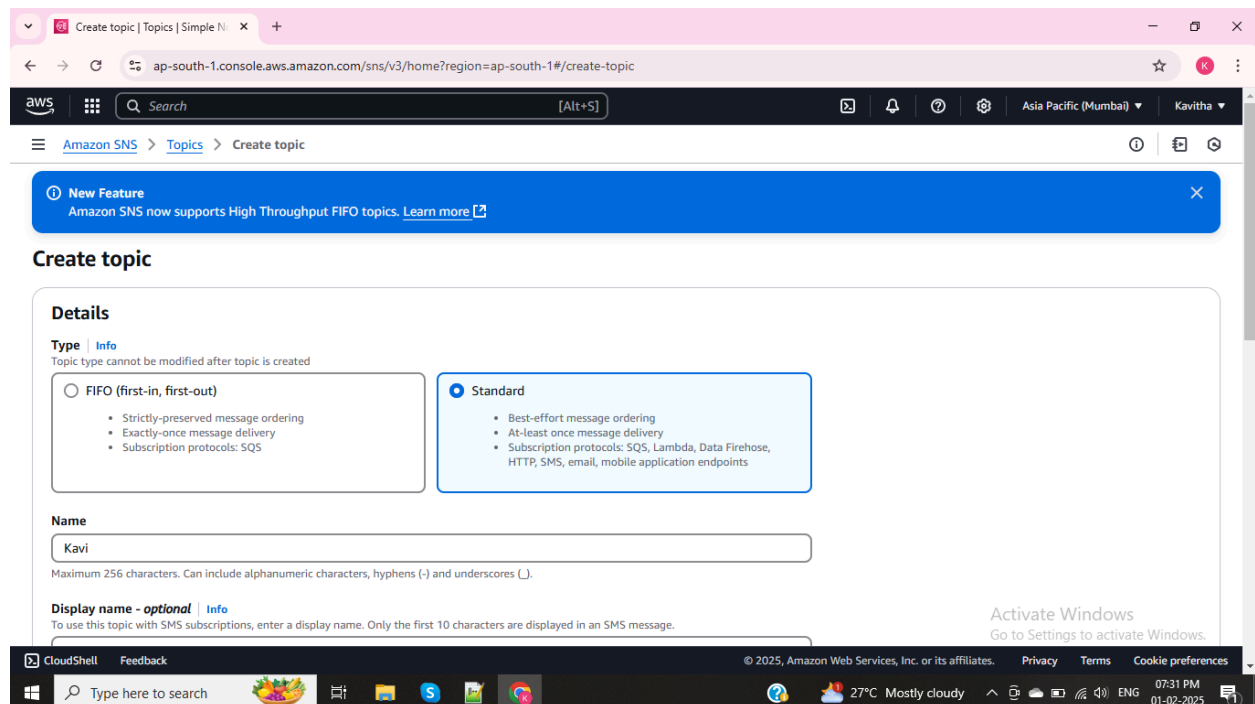
Amazon Cloud watch is a Gatekeeper of my AWS cloud which is capable to do:

1. Monitoring
2. Real life Metrics
3. Alarms
4. Log insights
5. Custom metrics
6. Cost optimisation
7. Scaling

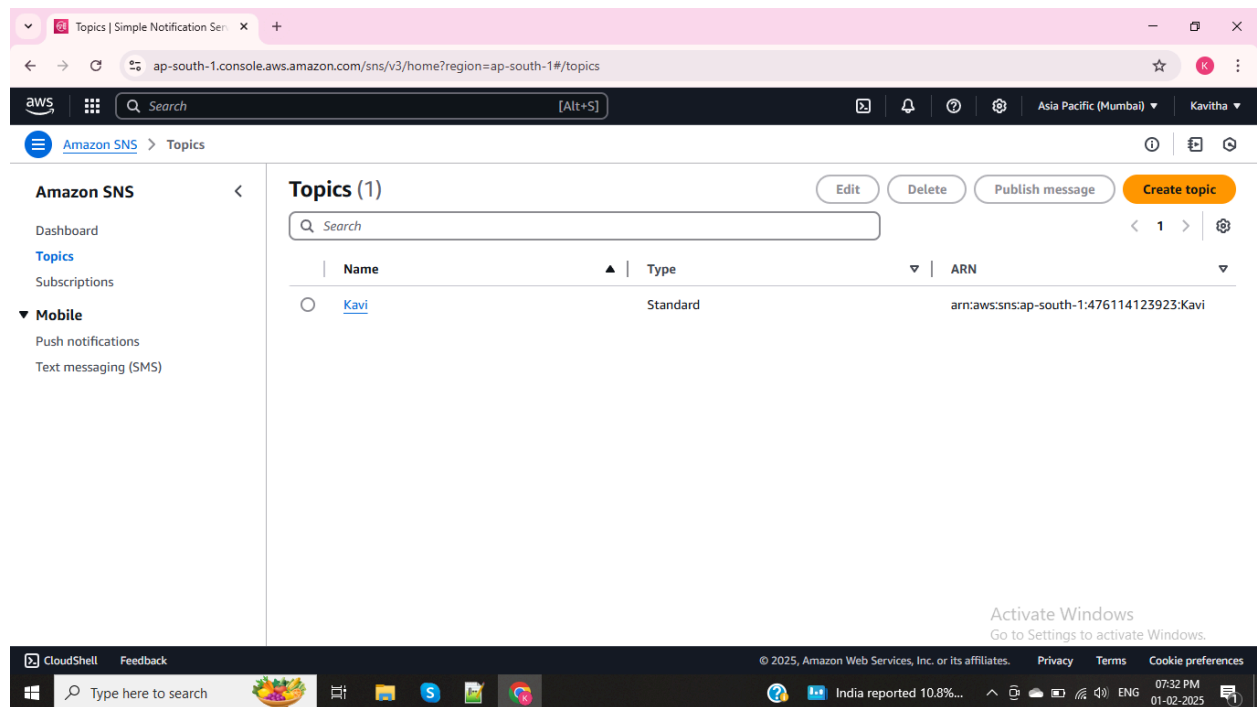
**TASK :** Configure Amazon CloudWatch to monitor EC2 instance's Metrics and send an email notification when it exceeds. This involves creating a CloudWatch alarm linked to an Amazon Simple Notification Service (SNS) topic.

### 1. Create an SNS Topic for Email Notifications:

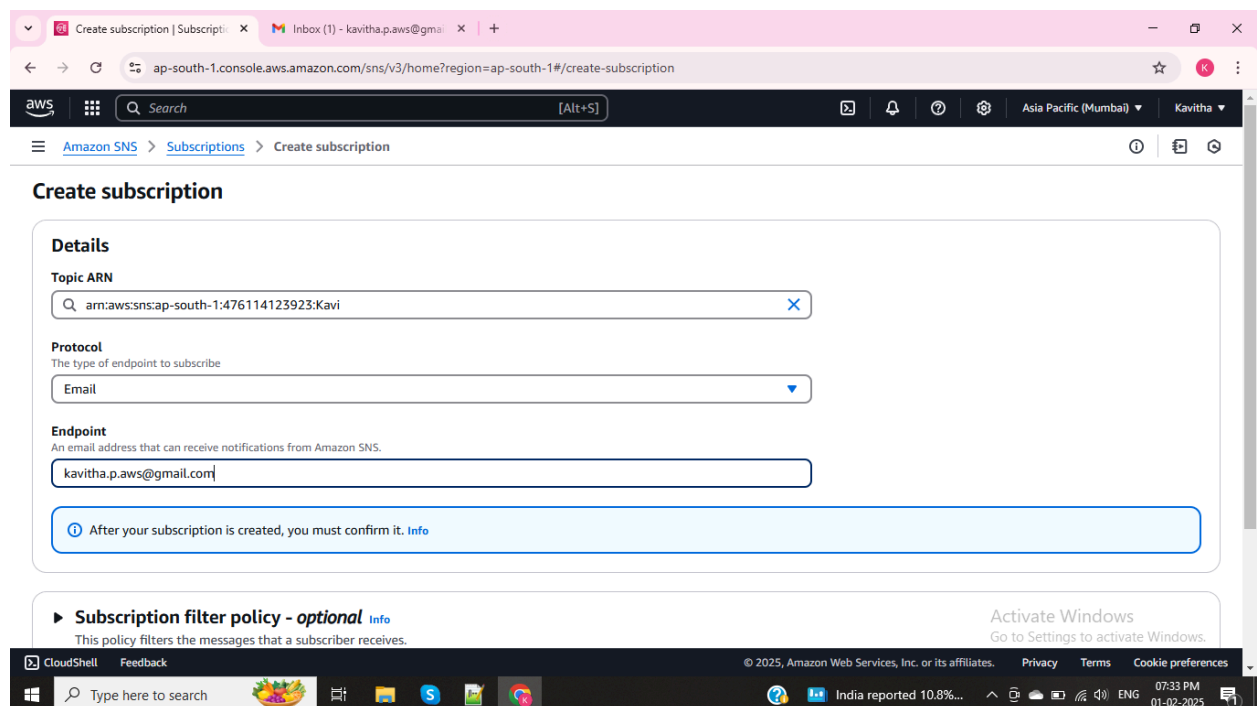
- Open the [Amazon SNS console](#).
- In the navigation pane, select **Topics**, then choose **Create topic**.
- For **Type**, select **Standard**.
- Enter a name for the topic.
- Choose **Create topic**.



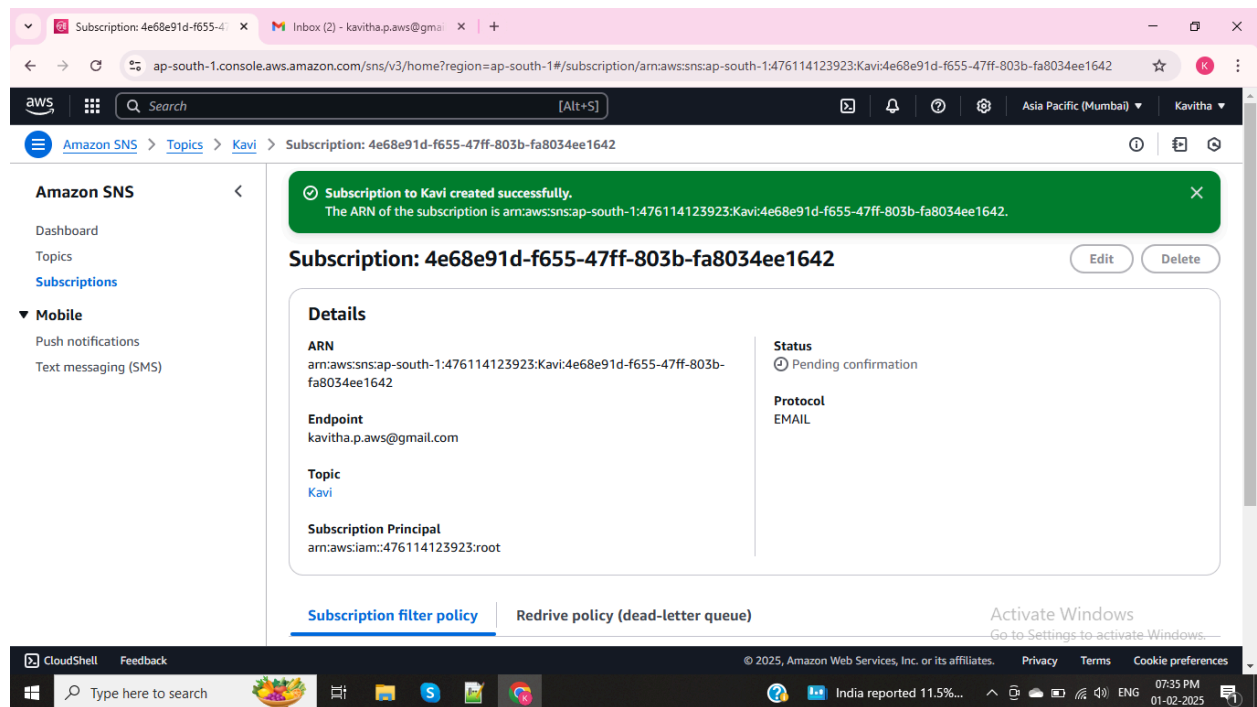
## OUTPUT



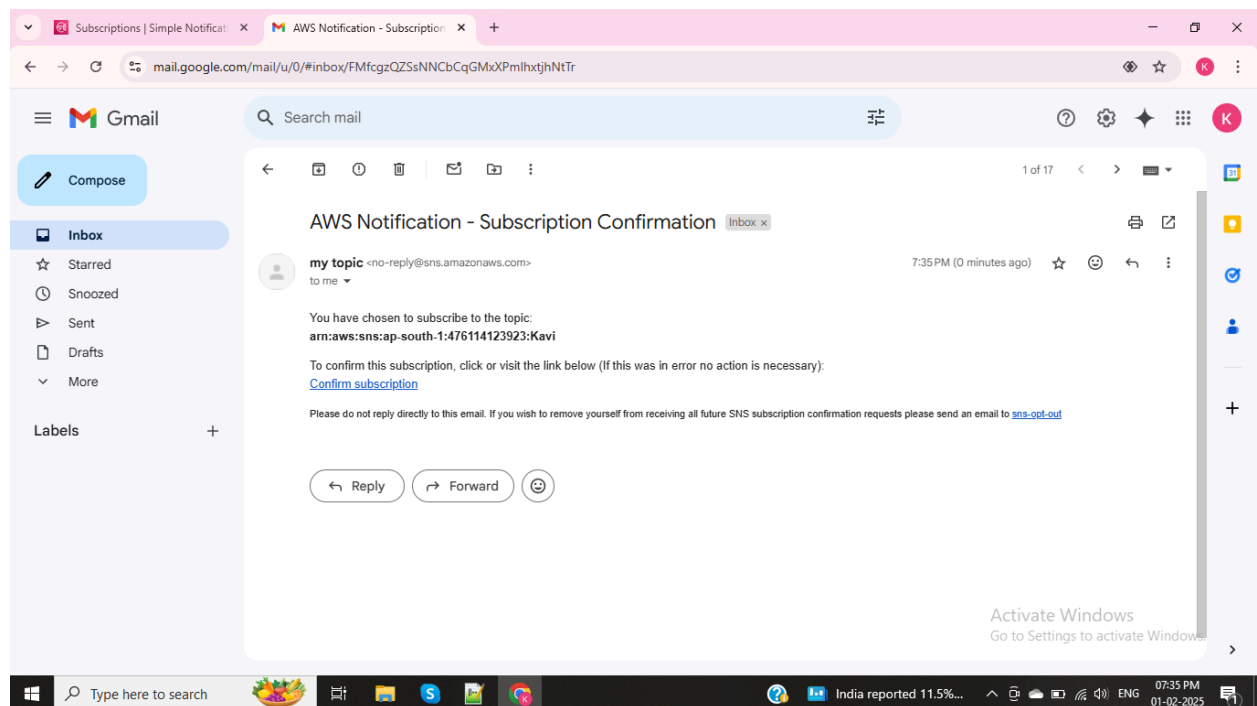
- After creating the topic, select it and choose **Create subscription**.
- Set **Protocol** to **Email** and enter email address.
- Choose **Create subscription**.



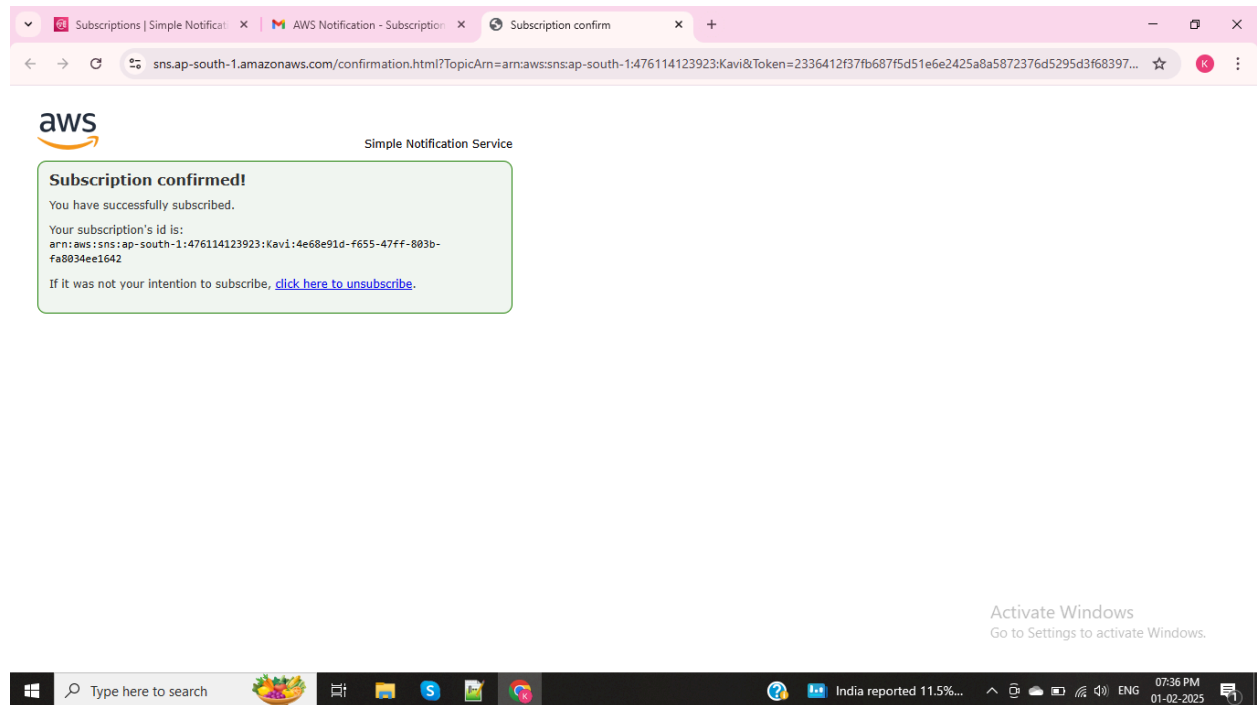
## Subscription created successfully



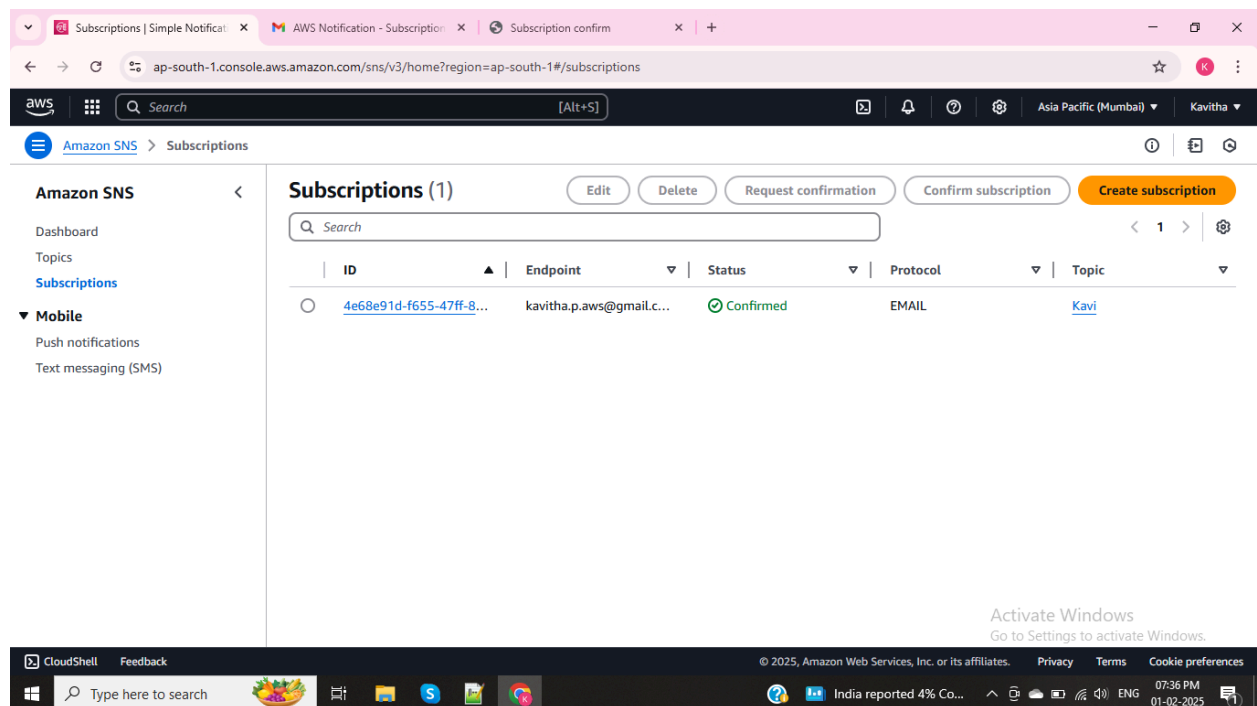
## Check email for a confirmation message



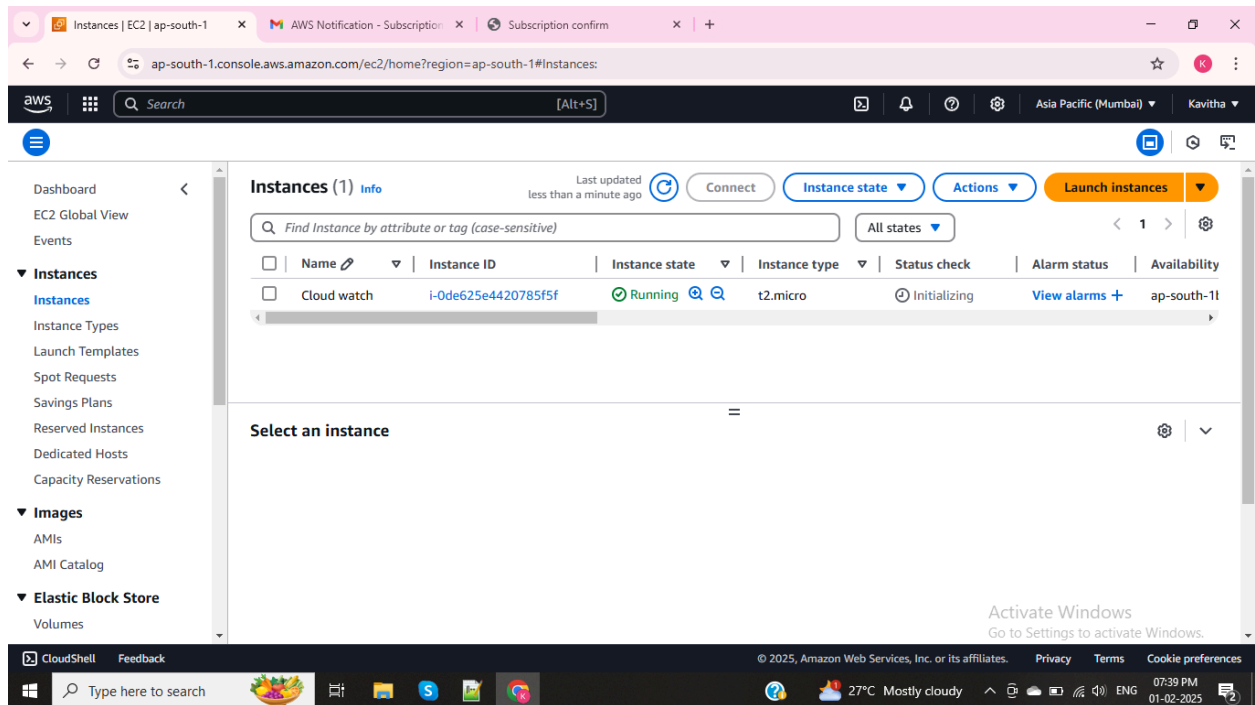
confirm the subscription



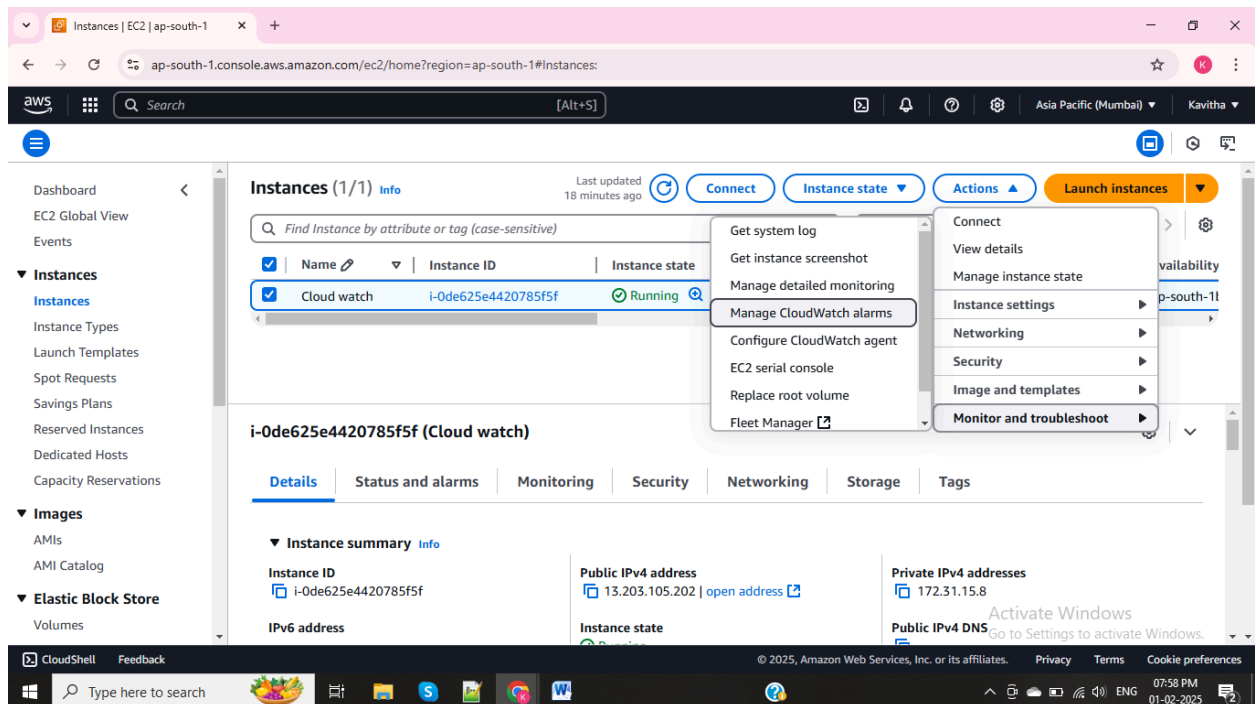
Its updated in the Amazon SNS status is **confirmed**



## 2. Creating an EC2 instance



## Configure the Cloud watch alarm with EC2 instance for Monitoring



### 3. Create a CloudWatch Alarm for an EC2 Instance:

**Create** an alarm > Alarm notification choose which created in SNS topic

The screenshot shows the 'Manage CloudWatch alarms' page in the AWS console. The breadcrumb trail is 'EC2 > Instances > i-0de625e4420785f5f > Manage CloudWatch alarms'. The page title is 'Manage CloudWatch alarms' with an 'Info' link. Below the title is a subtitle: 'Create or edit a CloudWatch alarm that monitors CloudWatch metrics for the instance.' There are two main sections: 'Add or edit alarm' and 'Alarm notification'. The 'Add or edit alarm' section has two tabs: 'Create an alarm' (selected) and 'Edit an alarm'. The 'Create an alarm' tab has a sub-label 'Create an alarm for i-0de625e4420785f5f'. Below this is a 'Search for alarm' section with a search bar containing 'Select an existing alarm to edit'. The 'Alarm notification' section has a sub-label 'Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.' and a search bar containing 'Kavi'. The 'Alarm action' section is partially visible at the bottom, with a sub-label 'Specify the action to take when the alarm is triggered'. The Windows taskbar at the bottom shows the date as 01-02-2025 and the time as 07:59 PM.

Set Alarm thresholds as per the requirements

The screenshot shows the 'Alarm thresholds' section of the 'Manage CloudWatch alarms' page. The breadcrumb trail is 'EC2 > Instances > i-0de625e4420785f5f > Manage CloudWatch alarms'. The page title is 'Alarm thresholds' with an 'Info' link. Below the title is a subtitle: 'Specify the metric thresholds for the alarm.' There are two main sections: 'Group samples by' and 'Type of data to sample'. The 'Group samples by' section has a dropdown menu set to 'Average'. The 'Type of data to sample' section has a dropdown menu set to 'CPU utilization'. Below these are two sections: 'Alarm when' and 'Consecutive period'. The 'Alarm when' section has a dropdown menu set to '<=' and a 'Percent' input field set to '10'. The 'Consecutive period' section has an input field set to '1' and a 'Period' dropdown menu set to '5 Minutes'. The 'Alarm name' section has an input field containing 'awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshold-CPUUtilization'. The 'Alarm description' section has an input field containing 'Alarm on instance i-0de625e4420785f5f: Triggered when CPUUtilization <= 10 for 1 consecutive 5-minute periods.' The 'Sample metric data' section is partially visible at the bottom, with a sub-label 'Sample metric data for i-0de625e4420785f5f'. The Windows taskbar at the bottom shows the date as 01-02-2025 and the time as 08:00 PM.

## Cloud watch alarm set successfully

The screenshot shows the AWS Management Console for the 'ap-south-1' region. A green notification banner at the top states: 'Created CloudWatch alarm: awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshold-CPUUtilization'. Below this, the 'Instances (1/1)' page is displayed, showing a table with one instance: 'Cloud watch' with ID 'i-0de625e4420785f5f', state 'Running', type 't2.micro', and '2/2 checks passed'. The left sidebar shows navigation options like Dashboard, EC2 Global View, Events, and Instances. The bottom of the console shows the 'i-0de625e4420785f5f (Cloud watch)' details page with tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The 'Instance summary' section shows the instance ID, public IPv4 address (13.203.105.202), private IPv4 addresses (172.31.15.8), and the instance state (Running).

## Email received OUTPUT

The screenshot shows a Gmail inbox with an email from 'my topic <no-reply@sns.amazonaws.com>' received at 8:00 PM. The subject is 'ALARM: "awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshold-CPUUtiliz..." in Asia Pacific (Mumbai)'. The email body explains that the alarm was triggered because the CPU utilization threshold was crossed. It includes a link to view the alarm in the AWS Management Console and a detailed list of alarm information.

**Alarm Details:**

- Name: awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshold-CPUUtilization
- Description: Alarm on instance i-0de625e4420785f5f. Triggered when CPUUtilization <= 10 for 1 consecutive 5-minute periods.
- State Change: INSUFFICIENT\_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [3.4935047168592765 (01/02/25 14:25:00)] was less than or equal to the threshold (10.0).
- Timestamp: Saturday 01 February, 2025 14:30:48 UTC
- AWS Account: 476114123923
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:476114123923:alarm:awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshold-CPUUtilization

**Threshold:**

- The alarm is in the ALARM state when the metric is LessThanOrEqualToThreshold 10.0 for at least 1 of the last 1 period(s) of 300 seconds.



## Cloud Watch In alarms shows the alarm

The screenshot displays the AWS CloudWatch Alarms console in the Asia Pacific (Mumbai) region. The left sidebar shows the navigation menu with options like Dashboards, Alarms (1), Logs, Metrics, X-Ray traces, Events, and Application Signals. The main content area is titled 'Alarms (1/1)' and shows a single alarm in the 'In alarm' state. The alarm details are as follows:

Name	State	Last state update (UTC)	Conditions	Actions
<a href="#">awsec2-i-0de625e4420785f5f-LessThanOrEqualToThreshhold-CPUUtilization</a>	In alarm	2025-02-01 14:30:48	CPUUtilization <= 10 for 1 datapoints within 5 minutes	<a href="#">Actions</a>

At the bottom of the console, there is a Windows taskbar showing the date and time as 08:03 PM on 01-02-2025, and a system tray with weather information (27°C, Partly cloudy) and network status.