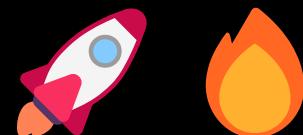


PROJECT DOCUMENTATION: CREATING A STRESS ENVIRONMENT ON EC2 AND ENABLING CLOUDWATCH ALARM WITH SNS NOTIFICATION



INTRODUCTION

This project demonstrates how to create a stress environment on an AWS EC2 instance, set up CloudWatch alarms to monitor CPU utilization, and use Amazon SNS (Simple Notification Service) to trigger alerts. By following these steps, you will learn how to monitor EC2 performance, receive alerts when CPU usage exceeds a defined threshold, and effectively use AWS services for infrastructure monitoring.

PREREQUISITES

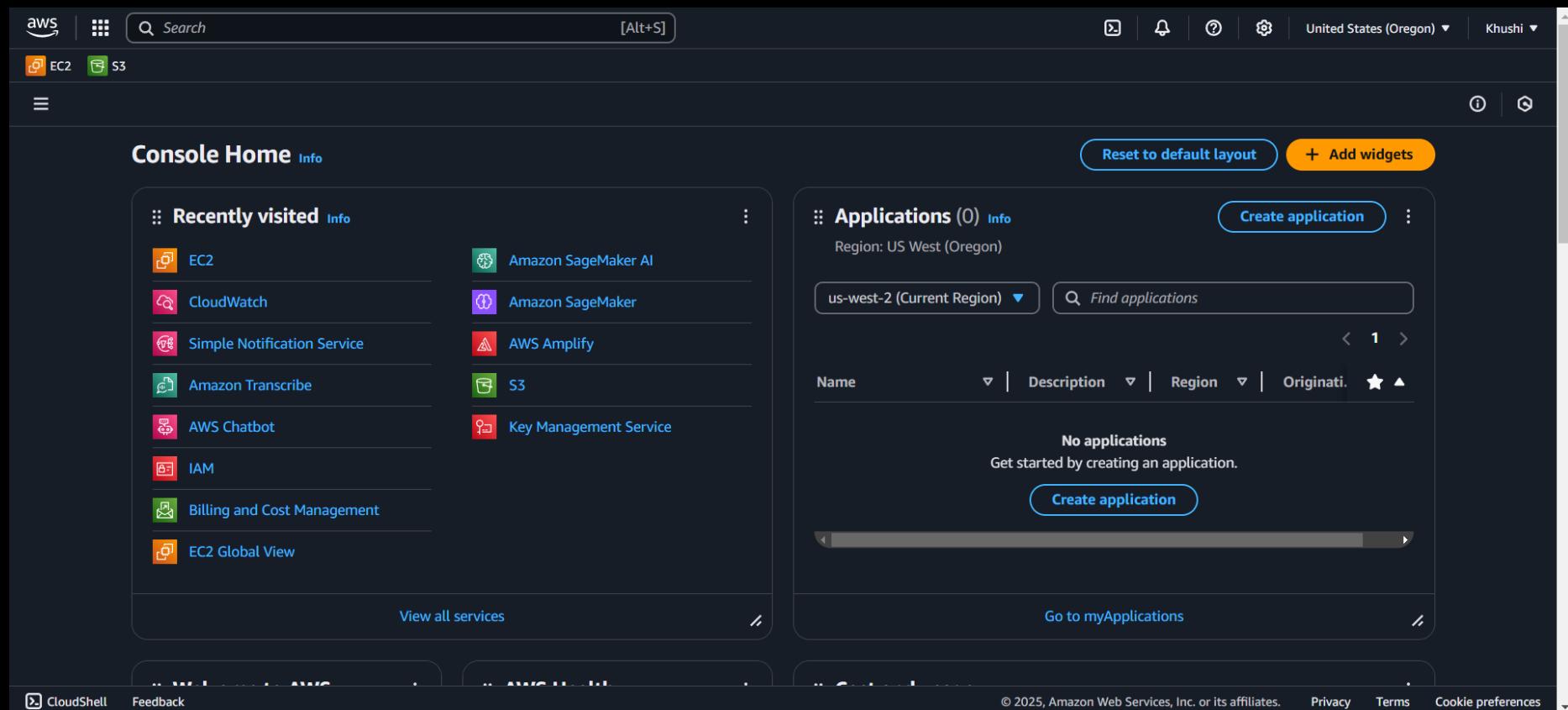
Before starting, ensure you have the following:

-  An AWS account
-  Access to the AWS Management Console
-  Basic understanding of AWS services (EC2, CloudWatch, SNS)
-  Familiarity with Linux commands

🚀 IMPLEMENTATION STEPS

I. SETTING UP THE EC2 INSTANCE 🖥️

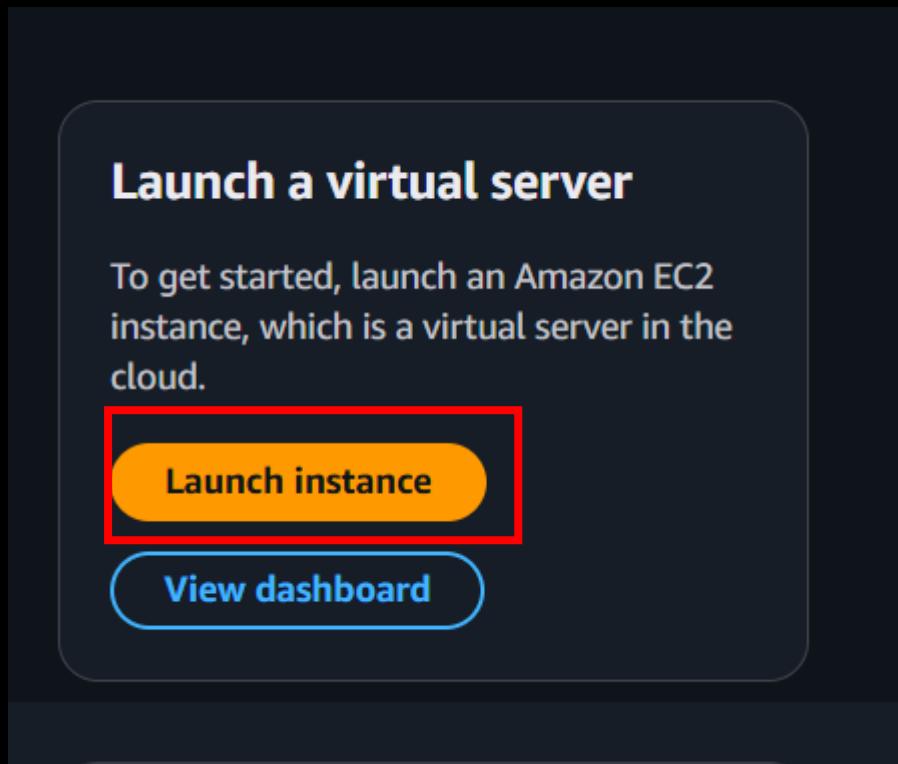
1. Open AWS Management Console.



2. Search for EC2 and navigate to the EC2 dashboard.

The screenshot shows the EC2 dashboard with a dark theme. The left sidebar has a navigation menu with 'EC2' selected. The main content area features the heading 'Amazon Elastic Compute Cloud (EC2)' and the sub-headline 'Create, manage, and monitor virtual servers in the cloud.' Below this, there's a brief description of EC2's capabilities and a section titled 'Benefits and features' with a sub-section 'EC2 offers ultimate scalability and control'. On the right side, there are two callout boxes: 'Launch a virtual server' (with 'Launch instance' and 'View dashboard' buttons) and 'Get started' (with a 'Get started walkthroughs' button). The footer includes copyright information and links for 'Privacy', 'Terms', and 'Cookie preferences'.

3. Click on Launch Instance.



4. Assign a **name** to your instance.

The screenshot shows the 'Launch an instance' step in the AWS EC2 console. The navigation bar at the top shows 'EC2 > Instances > Launch an instance'. The main heading is 'Launch an instance' with an 'Info' link. Below it, a sub-section titled 'Name and tags' also has an 'Info' link. A 'Name' label is followed by a text input field containing the value 'linux-instance-in-stress-env'. To the right of the input field is a blue 'Add additional tags' button. The background of the page is dark grey.

5. Choose Amazon Linux 2 AMI (HVM)

The screenshot shows the AWS Lambda console interface. A red box highlights the 'Amazon Linux' option in the list of available AMIs. The list includes: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. To the right is a search bar with a magnifying glass icon and a link to 'Browse more AMIs'. Below the list, a section titled 'Amazon Machine Image (AMI)' displays the selected AMI details: 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type'. The AMI ID is 'ami-000089c8d02060104 (64-bit (x86)) / ami-0b16505c55f9802f9 (64-bit (Arm))'. It is marked as 'Free tier eligible'. Below this, the 'Description' section provides information about the AMI: 'Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.' At the bottom, there are fields for 'Architecture' (set to '64-bit (x86)'), 'AMI ID' ('ami-000089c8d02060104'), 'Username' ('ec2-user'), and a green button labeled 'Verified provider'.

6. Select **t2.micro** or **t3.micro** as the instance type (whichever is available under free tier).

The screenshot shows the 'Instance type' section of the AWS CloudFormation configuration. The 't2.micro' option is selected, and its details are displayed: Family: t2, 1 vCPU, 1 GiB Memory, Current generation: true. Pricing includes On-Demand Linux base pricing at 0.0116 USD per Hour, On-Demand SUSE base pricing at 0.0116 USD per Hour, On-Demand Windows base pricing at 0.0162 USD per Hour, On-Demand RHEL base pricing at 0.026 USD per Hour, and On-Demand Ubuntu Pro base pricing at 0.0134 USD per Hour. A red box highlights the 'Free tier eligible' status. To the right, there's a radio button for 'All generations' and a link to 'Compare instance types'. A note at the bottom states: 'Additional costs apply for AMIs with pre-installed software'.

7. Proceed without a key pair.

The screenshot shows the 'Key pair (login)' section. It includes a note: '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.' Below is a dropdown menu for 'Key pair name - required'. The 'Proceed without a key pair (Not recommended)' option is selected, and a red box surrounds this entire section. To the right, there's a 'Default value' dropdown and a 'Create new key pair' button.

8. In Networking settings, allow SSH traffic.

The screenshot shows the 'Network settings' section of the AWS CloudFormation console. A red box highlights the 'Network settings' header. Below it, the 'Network' tab is selected, showing the VPC ID: vpc-095d5ffaad02ac091. The 'Subnet' tab shows 'No preference (Default subnet in any availability zone)'. The 'Auto-assign public IP' tab is set to 'Enable'. A note about additional charges applies when outside of free tier allowance. The 'Firewall (security groups)' tab is selected, showing a note that a security group controls traffic for the instance. It offers two options: 'Create security group' (selected) and 'Select existing security group'. A red box highlights the 'Allow SSH traffic from' checkbox, which is checked and enables connecting to the instance. The dropdown menu next to it shows 'Anywhere' and the IP range '0.0.0.0/0'.

▼ **Network settings** Info

Network Info

vpc-095d5ffaad02ac091

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.

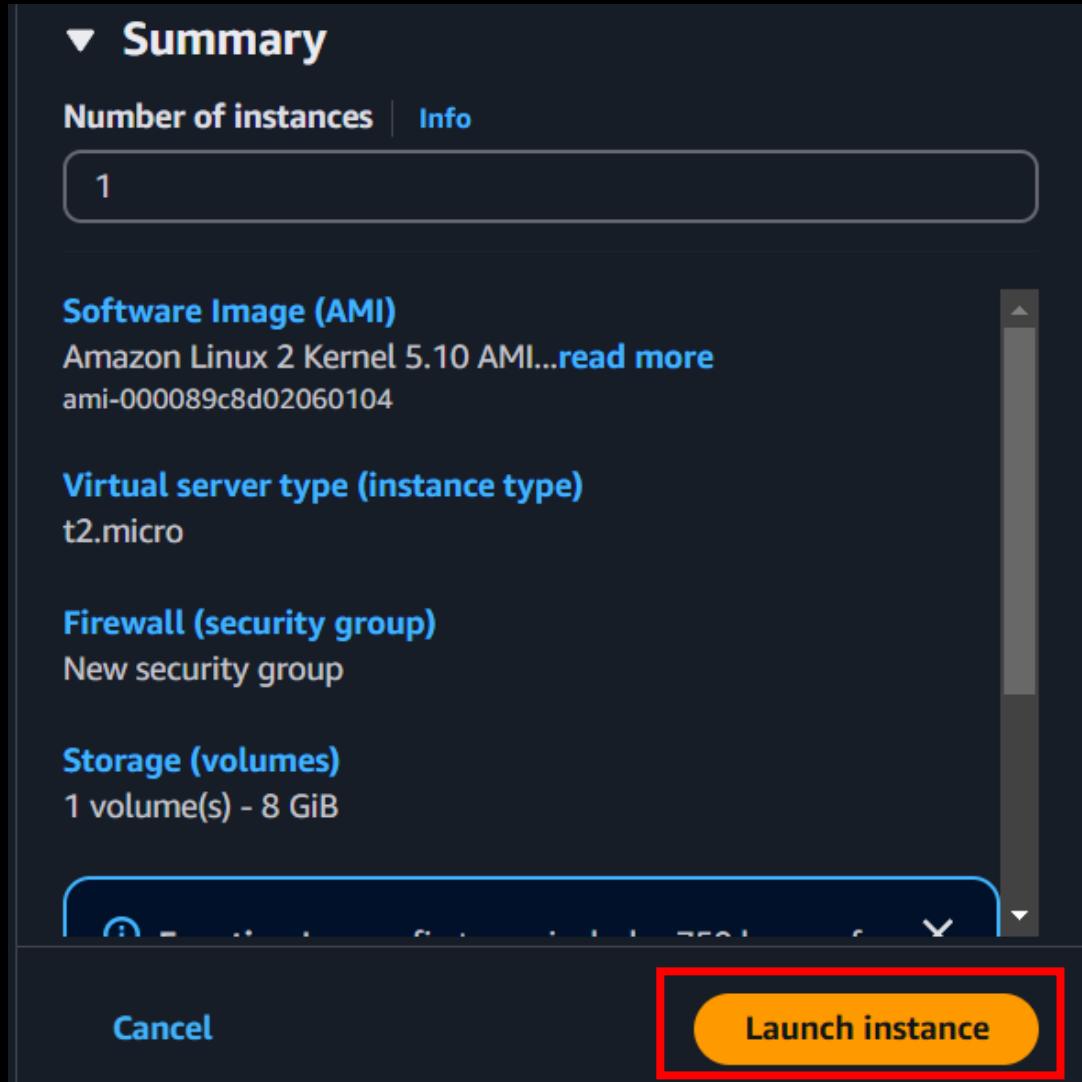
Create security group Select existing security group

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

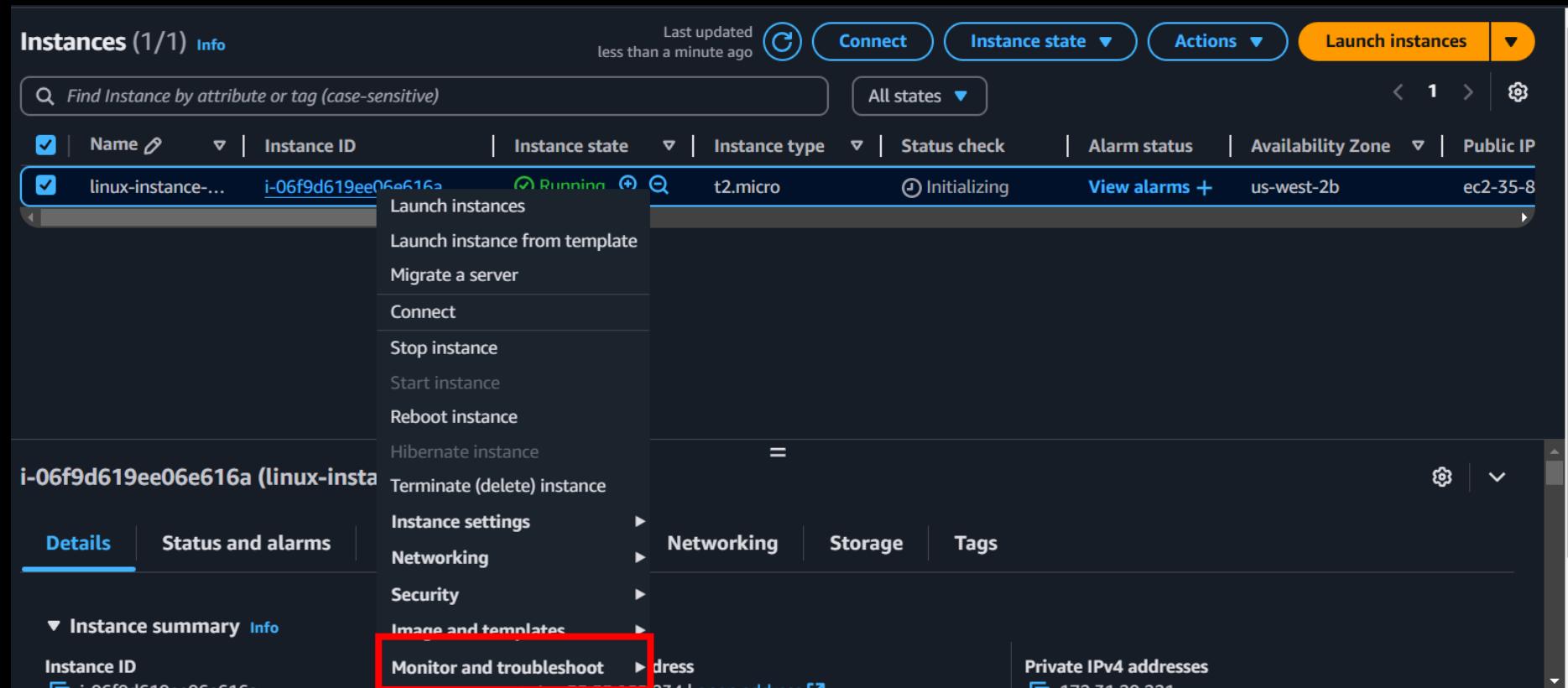
Anywhere
0.0.0.0/0

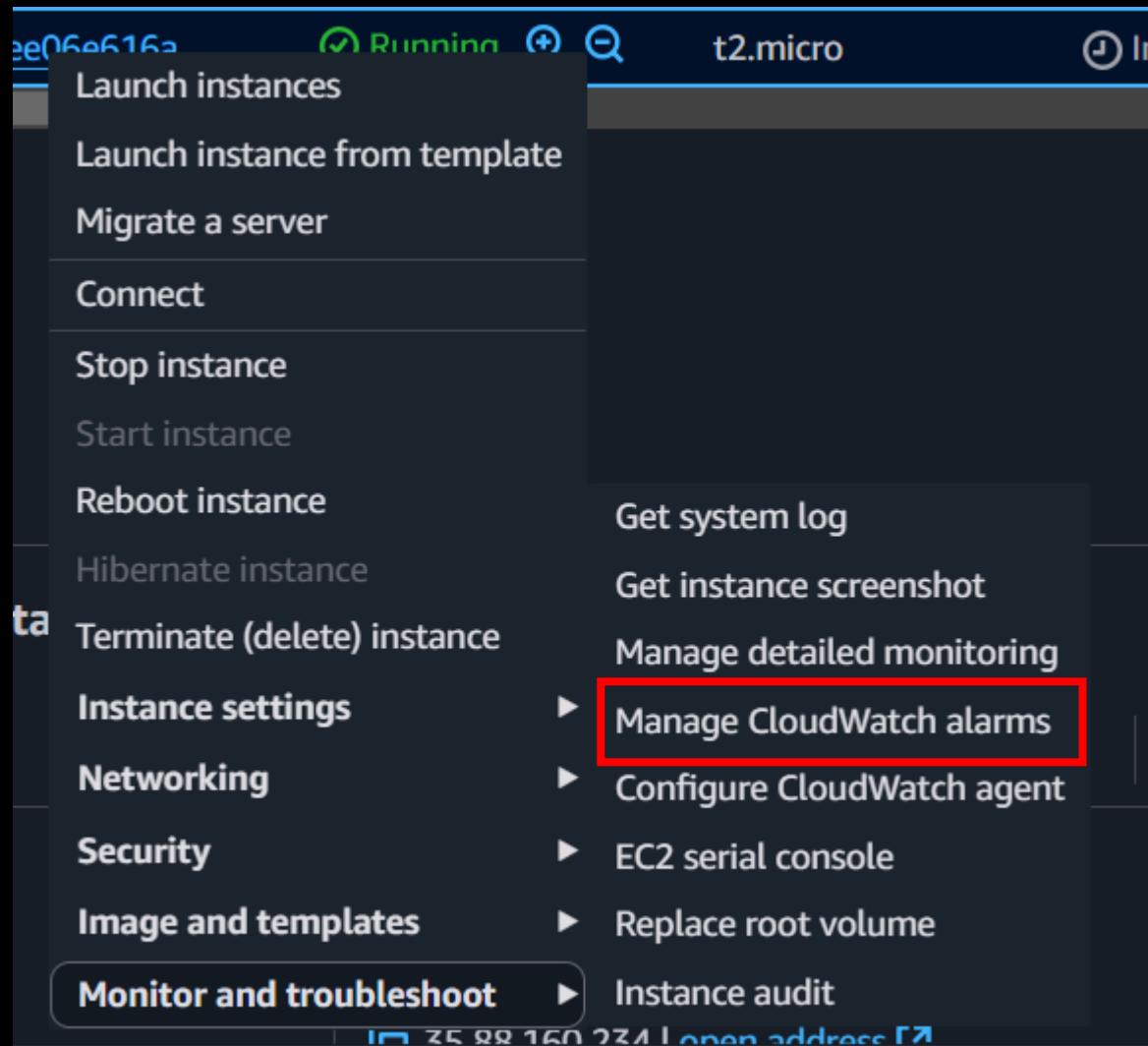
9. Click on Launch Instance.



II. CONFIGURING CLOUDWATCH ALARM AND SNS

10. Click on the Instance ID, right-click, and navigate to Monitor and Troubleshoot → Manage CloudWatch Alarms.





11. You will be redirected to the CloudWatch Alarms dashboard.

The screenshot shows the 'Manage CloudWatch alarms' section of the AWS CloudWatch Alarms dashboard. A red box highlights the title 'Manage CloudWatch alarms' and the sub-instruction 'Create or edit a CloudWatch alarm that monitors CloudWatch metrics for the instance.' Below this, there are two main options: 'Create an alarm' (selected) and 'Edit an alarm'. The 'Create an alarm' section includes a sub-instruction 'Create an alarm for i-06f9d619ee06e616a'. To the right, there are sections for 'Search for alarm' (with a search bar), 'Alarm notification' (with a search bar and a toggle switch set to 'On'), and 'Alarm action' (with a search bar and a toggle switch set to 'Off'). The top navigation bar shows the path: EC2 > Instances > i-06f9d619ee06e616a > Manage CloudWatch alarms.

12. Click **Create Alarm** → In **Alarm Notification**, select or search for **SNSTopicEC2**.

The screenshot shows the 'Manage CloudWatch alarms' page. At the top, there's a heading 'Add or edit alarm' with a sub-instruction: 'You can create a new alarm or edit an existing alarm'. Below this, there are two main options: 'Create an alarm' (selected) and 'Edit an alarm'. The 'Create an alarm' section has a sub-instruction: 'Create an alarm for i-06f9d619ee06e616a'. A red box highlights this entire section. Below it is a 'Search for alarm' section with a sub-instruction: 'Find an alarm to modify' and a search bar containing 'Select an existing alarm to edit'. A second red box highlights the 'SNSEC2TOPIC' entry in the search results list. The search results also include a 'Create an SNS topic' option. Further down, under 'Alarm notification', there's a sub-instruction: 'Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.' Another red box highlights the 'SNSEC2TOPIC' entry in the search bar here.

13. Under Alarm Threshold, change the CPU utilization percentage to 50%.

The screenshot shows the 'Alarm thresholds' configuration page. The 'Type of data to sample' is set to 'CPU utilization'. The 'Percent' field is highlighted with a red box and contains the value '50'. Other fields include 'Group samples by' (Average), 'Alarm when' (>=), 'Consecutive period' (1), 'Period' (5 Minutes), 'Alarm name' (awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization), and 'Alarm description' (Alarm on instance i-06f9d619ee06e616a: Triggered when CPUUtilization >= 50 for 1 consecutive 5-minute periods.).

14. Scroll down and click **Create Alarm**.



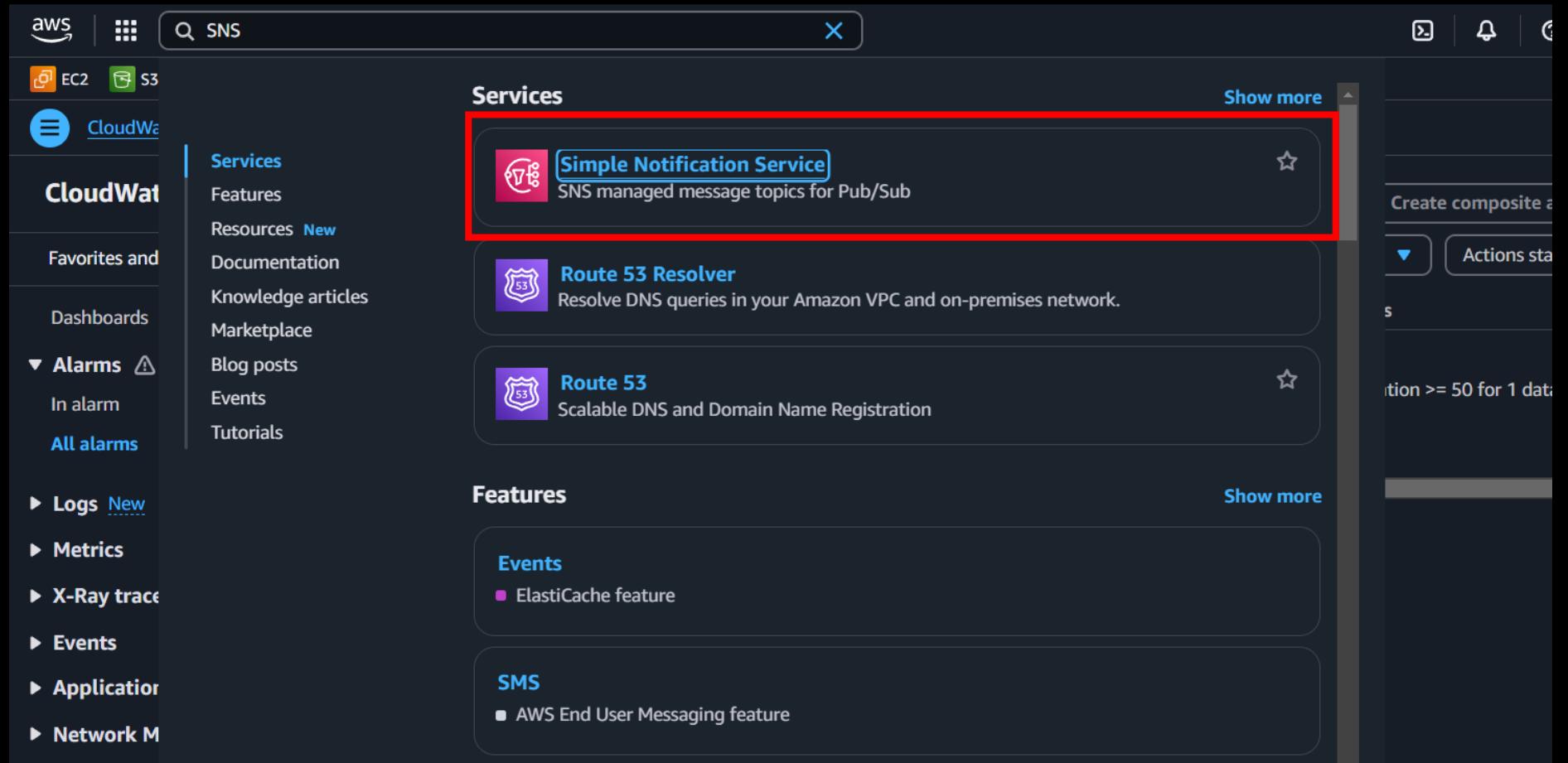
15. Verify that the alarm has been created successfully.

The screenshot shows the AWS CloudWatch Alarms interface. On the left, there's a sidebar with 'CloudWatch' selected, followed by 'Favorites and recents', 'Dashboards', and a expanded 'Alarms' section with 'In alarm' and 'All alarms' options. Below the sidebar is a 'Logs' section. The main area is titled 'Alarms (1)' and contains a table with one row. The table columns are 'Name', 'State', 'Last state update (UTC)', 'Conditions', and 'Actions'. The single alarm listed is 'awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualTo', which is currently in an 'Insufficient data' state. It was last updated on 2025-02-17 13:43:42. The condition is 'CPUUtilization >= 50 for 1 datapoints within 5 minutes'. The 'Actions' column shows a green checkmark next to 'Actions enabled'.

Name	State	Last state update (UTC)	Conditions	Actions
awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualTo	Insufficient data	2025-02-17 13:43:42	CPUUtilization >= 50 for 1 datapoints within 5 minutes	Actions enabled

III. CONFIGURING SNS FOR NOTIFICATIONS

16. Search for SNS service and open it in a new tab.



17. Navigate to the SNS Dashboard, where you will see one SNS topic.

The screenshot shows the Amazon SNS Dashboard. On the left, there's a navigation sidebar with links for EC2, S3, Amazon SNS (which is highlighted), Dashboard, Topics, Subscriptions, Mobile (Push notifications, Text messaging (SMS)), CloudShell, and Feedback. The main content area has a blue header bar with a 'New Feature' message: 'Amazon SNS now supports High Throughput FIFO topics. Learn more'. Below this is a section titled 'Dashboard' with a red box around the 'Resources for us-west-2' box. Inside this box, there's a 'Topics' section showing 1 topic, a 'Platform applications' section showing 0, and a 'Subscriptions' section showing 1. Below the dashboard, there's an 'Overview of Amazon SNS' section with a 'Application-to-application (A2A)' subsection. This subsection describes Amazon SNS as a managed messaging service for decoupling publishers from subscribers, useful for microservices, distributed systems, and serverless applications. It includes a 'Learn more' link. To the right of this is a diagram showing a flow from a document icon to a central hub, then to a dead-letter queue icon (with a note: 'If an endpoint is unavailable, messages can be held in a dead-letter queue for analysis or reprocessing'), and finally to a database icon. To the right of the queue is a list of supported platforms: AWS Lambda, Amazon SQS, Amazon Kinesis Data Firehose, and HTTP/HTTPS. At the bottom of the page are copyright information ('© 2025, Amazon Web Services, Inc. or its affiliates.'), privacy links ('Privacy', 'Terms', 'Cookie preferences'), and a dropdown menu.

18. Click on the topic, scroll down, and click **Create Subscription**.

The screenshot shows the Amazon SNS Topics page for a topic named 'SNSEC2TOPIC'. The left sidebar includes links for Dashboard, Topics (which is selected), Subscriptions, Mobile (Push notifications and Text messaging (SMS)), CloudShell, and Feedback. The main content area displays the topic's ARN (arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC), Topic owner (971422709086), and Type (Standard). Below this, the 'Subscriptions' tab is active, showing a table with columns for ID, Endpoint, Status, and Protocol. A message states 'No subscriptions found' and 'You don't have any subscriptions to this topic.' A prominent yellow 'Create subscription' button is located at the bottom right of the table area, which is highlighted with a red box.

19. Choose Email as the protocol.

The screenshot shows the AWS SNS console interface. At the top, there are tabs for EC2 and S3. Below the tabs, a sidebar lists various protocols: Amazon Kinesis Data Firehose, Amazon SQS, AWS Lambda, Email (which is selected and highlighted with a blue border), Email-JSON, HTTP, HTTPS, Platform application endpoint, SMS, and Email again at the bottom. In the main area, there's a 'Details' section with a 'Topic ARN' input field containing 'arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC'. Below it is a 'Protocol' section, which is also highlighted with a red box. The 'Protocol' section contains the text 'The type of endpoint to subscribe' and a dropdown menu with 'Email' selected. A small blue arrow icon is visible to the right of the dropdown.

20. Enter your **email address** in the **Endpoint** field.

The screenshot shows the 'Protocol' section with 'Email' selected. Below it is the 'Endpoint' section, which contains the email address 'youremail@gmail.com'. A red box highlights the 'Endpoint' input field. At the bottom, a note says 'After your subscription is created, you must confirm it.' with a blue 'Info' link.

21. Scroll down and click **Create Subscription**.

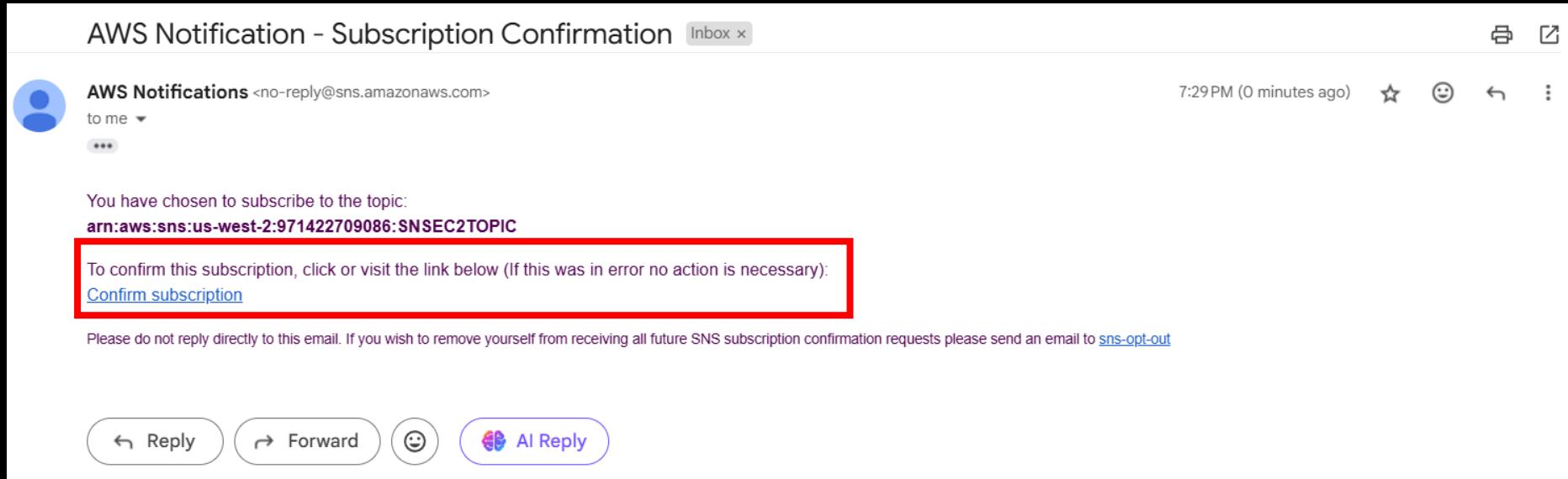
The screenshot shows the 'Subscription filter policy - optional' and 'Redrive policy (dead-letter queue) - optional' sections. At the bottom right are 'Cancel' and 'Create subscription' buttons, with 'Create subscription' highlighted by a red box. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

22. Verify that your subscription appears in the SNS Dashboard.

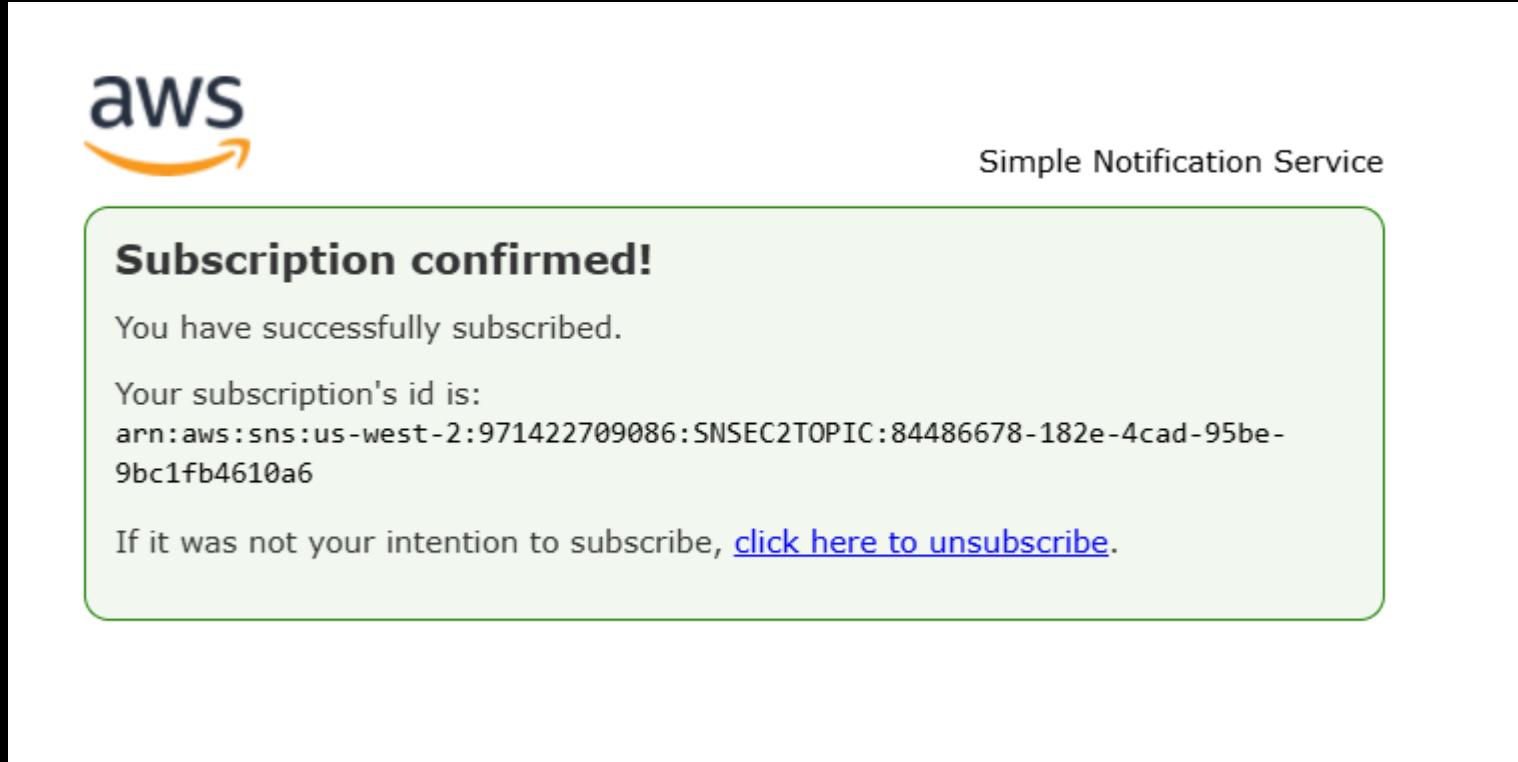
The screenshot shows the Amazon SNS console. In the top navigation bar, 'Amazon SNS' is selected. Below it, the path is 'Topics > SNSEC2TOPIC > Subscription: 6d74ee6a-e41c-4ddf-80d3-712842d0329f'. On the left sidebar, 'Subscriptions' is highlighted. The main content area displays a green success message: 'Subscription to SNSEC2TOPIC created successfully.' followed by the ARN: 'arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC:6d74ee6a-e41c-4ddf-80d3-712842d0329f'. Below this, the subscription details are listed:

Details	
ARN	arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC:6d74ee6a-e41c-4ddf-80d3-712842d0329f
Endpoint	youremail@gmail.com
Topic	SNSEC2TOPIC
Subscription Principal	arn:aws:iam::971422709086:root
Status	Pending confirmation
Protocol	EMAIL

23. Open your email and confirm the AWS Notification Subscription.



24. Upon confirmation, you will be redirected to a page that says **Subscription Confirmed**.



25. Refresh the SNS dashboard and verify that the subscription status is confirmed.

The screenshot shows the AWS SNS Subscription Details page for a specific subscription. The subscription ARN is listed as arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC:73fc19c3-a23f-4f48-8bf1-a741f73e8bd5. The endpoint is set to @gmail.com and the topic is SNSEC2TOPIC. The subscription principal is arn:aws:iam::971422709086:root. The status is shown as 'Confirmed' with a green checkmark icon, which is highlighted with a red box. The protocol is listed as EMAIL. There are 'Edit' and 'Delete' buttons at the top right of the card.

Subscription: 73fc19c3-a23f-4f48-8bf1-a741f73e8bd5

Details

ARN
arn:aws:sns:us-west-2:971422709086:SNSEC2TOPIC:73fc19c3-a23f-4f48-8bf1-a741f73e8bd5

Endpoint
@gmail.com

Topic
SNSEC2TOPIC

Subscription Principal
arn:aws:iam::971422709086:root

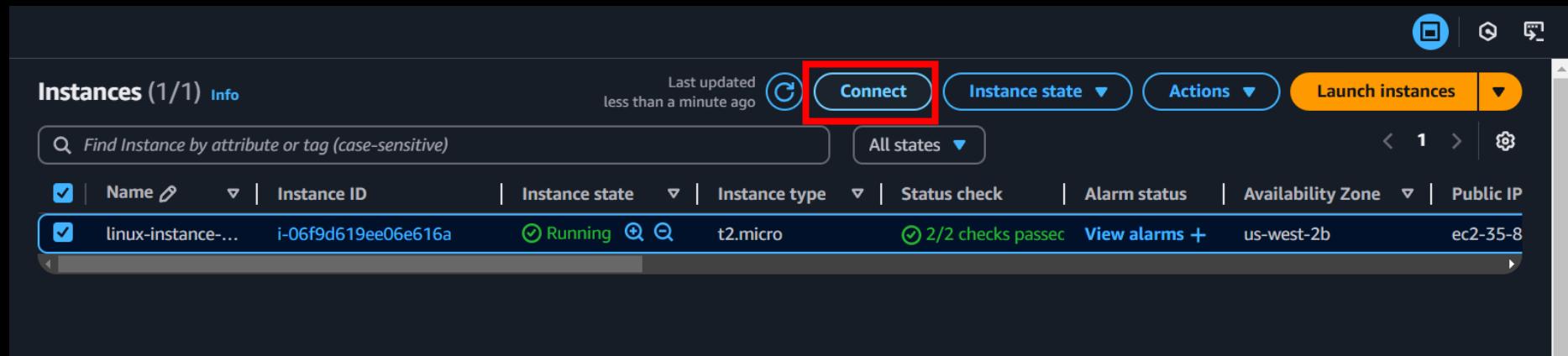
Status
Confirmed

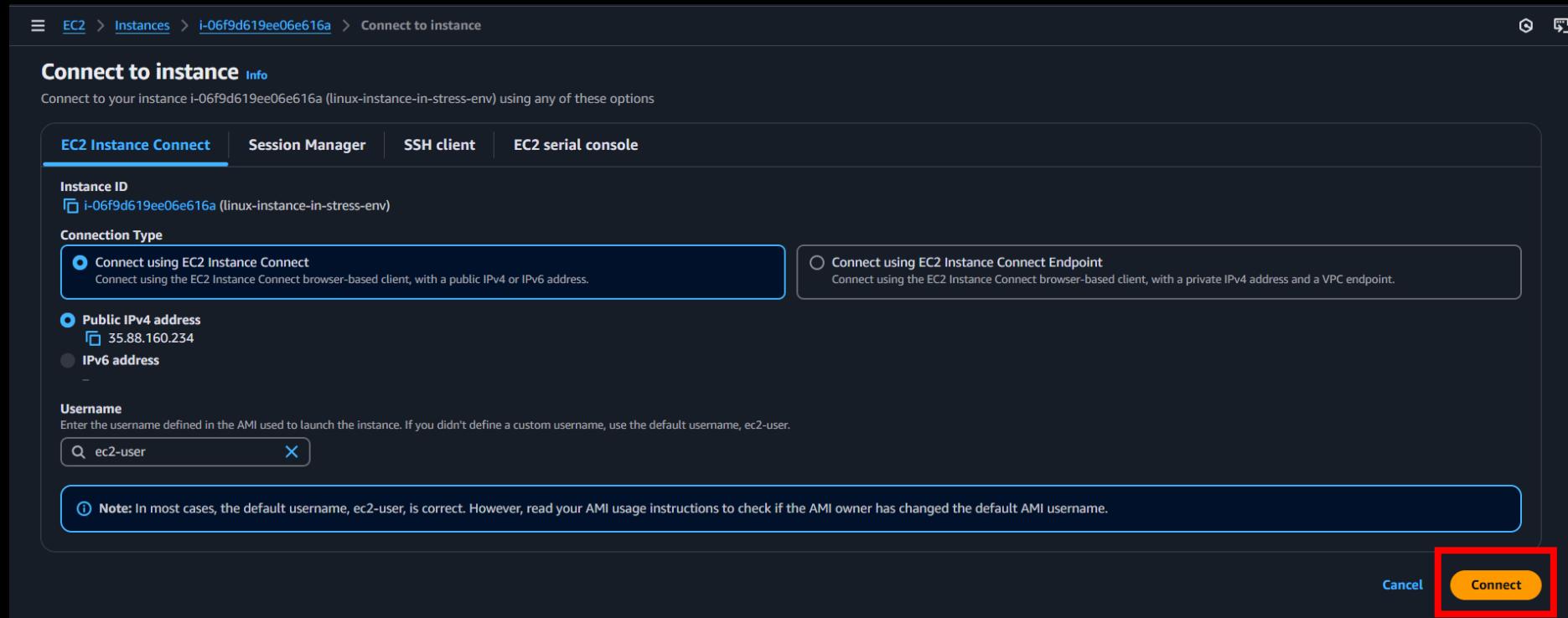
Protocol
EMAIL

Edit **Delete**

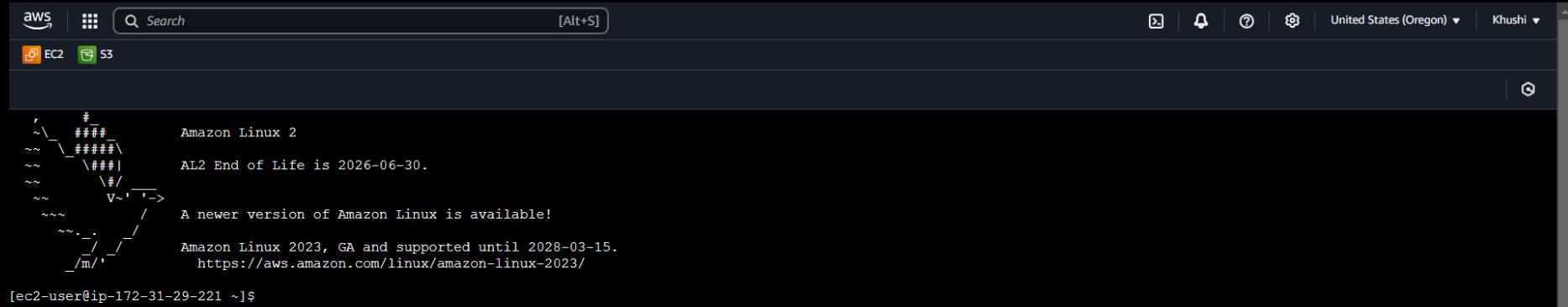
IV. CREATING A STRESS ENVIRONMENT ON EC2

26. Navigate back to your EC2 instance, select it, and click Connect.





27. Once the Linux server is ready, execute the following commands to install the stress tool:



The screenshot shows a terminal window within the AWS CloudWatch interface. The title bar includes the AWS logo, a search bar, and navigation icons. The main area displays a stylized welcome message for Amazon Linux 2, which includes a URL to the latest version. The message is as follows:

```
'\#\#\#'
~~\_#\#\#\#
~~ \#\#\#
~~ \#/ 
~~ V~'-->
~~ / 
~~ A newer version of Amazon Linux is available!
~~ / 
~~ Amazon Linux 2023, GA and supported until 2028-03-15.
~~ /m/ https://aws.amazon.com/linux/amazon-linux-2023/'
```

[ec2-user@ip-172-31-29-221 ~]\$

- **sudo yum update -y:** Updates all installed packages.

```
'          #
~\_\#\#\# Amazon Linux 2
~~ \_\#\#\#\#
~~  \#\#\| AL2 End of Life is 2026-06-30.
~~   \#/ 
~~   V~' '-->
~~~      / A newer version of Amazon Linux is available!
~~~_._. / 
~/\_/ / Amazon Linux 2023, GA and supported until 2028-03-15.
/_m/' / https://aws.amazon.com/linux/amazon-linux-2023/
```

```
[ec2-user@ip-172-31-29-221 ~]$ sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
           | 3.6 kB  00:00:00
No packages marked for update
[ec2-user@ip-172-31-29-221 ~]$ 
```

- **sudo amazon-linux-extras install epel -y:** Enables the Extra Packages for Enterprise Linux (EPEL) repository.

```
[ec2-user@ip-172-31-29-221 ~]$ sudo amazon-linux-extras install epel -y
Installing epel-release
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Cleaning repos: amzn2-core amzn2extra-docker amzn2extra-epel amzn2extra-kernel-5.10
17 metadata files removed
6 sqlite files removed
0 metadata files removed
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
    | 3.6 kB  00:00:00
amzn2extra-docker
    | 2.9 kB  00:00:00
amzn2extra-epel
    | 3.0 kB  00:00:00
amzn2extra-kernel-5.10
    | 3.0 kB  00:00:00
(1/9): amzn2-core/2/x86_64/group_gz
    | 2.7 kB  00:00:00
(2/9): amzn2-core/2/x86_64/updateinfo
    | 1.0 MB   00:00:00
(3/9): amzn2extra-epel/2/x86_64/primary_db
    | 1.8 kB  00:00:00
```

- **sudo yum install stress -y:** Installs the **stress** tool for generating high CPU usage.

```
[ec2-user@ip-172-31-29-221 ~]$ sudo yum install stress -v
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
230 packages excluded due to repository priority protections
Resolving Dependencies
--> Running transaction check
--> Package stress.x86_64 0:1.0.4-16.el7 will be installed
--> Finished Dependency Resolution
```

Dependencies Resolved

```
=====
Package           Arch      Version       Repository
Size
=====
Installing:
stress            x86_64   1.0.4-16.el7    epel
39 k
```

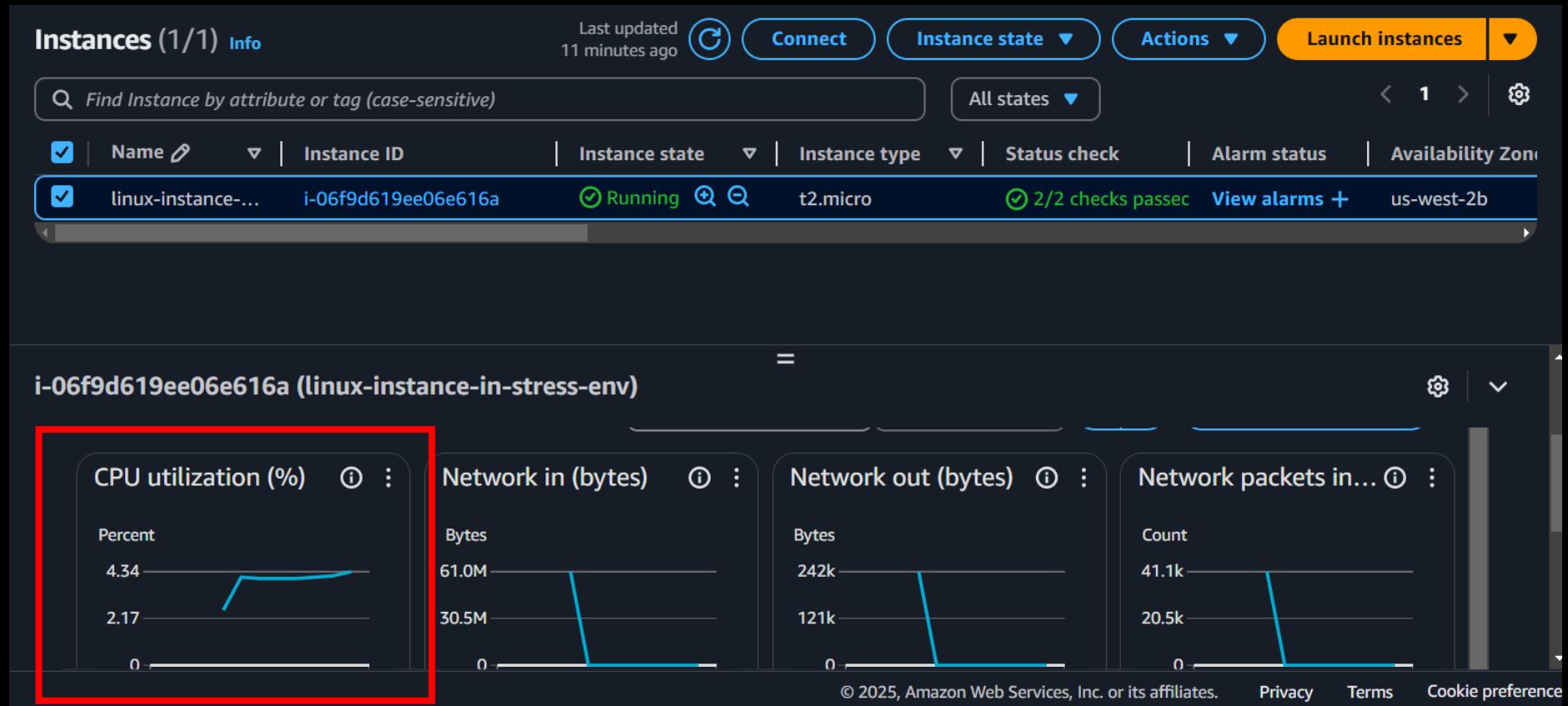
Transaction Summary

Install 1 Package

Total download size: 39 k
Installed size: 94 k

V. GENERATING STRESS AND MONITORING CLOUDWATCH

28. Go to the EC2 instance → Monitoring tab, scroll down, and enlarge the CPU Utilization graph.



29. Run the following command in your Linux terminal to generate stress on the CPU:

```
stress --cpu 9
```

```
          1/1  
Verifying : stress-1.0.4-16.el7.x86_64  
          1/1
```

Installed:

```
stress.x86_64 0:1.0.4-16.el7
```

Complete!

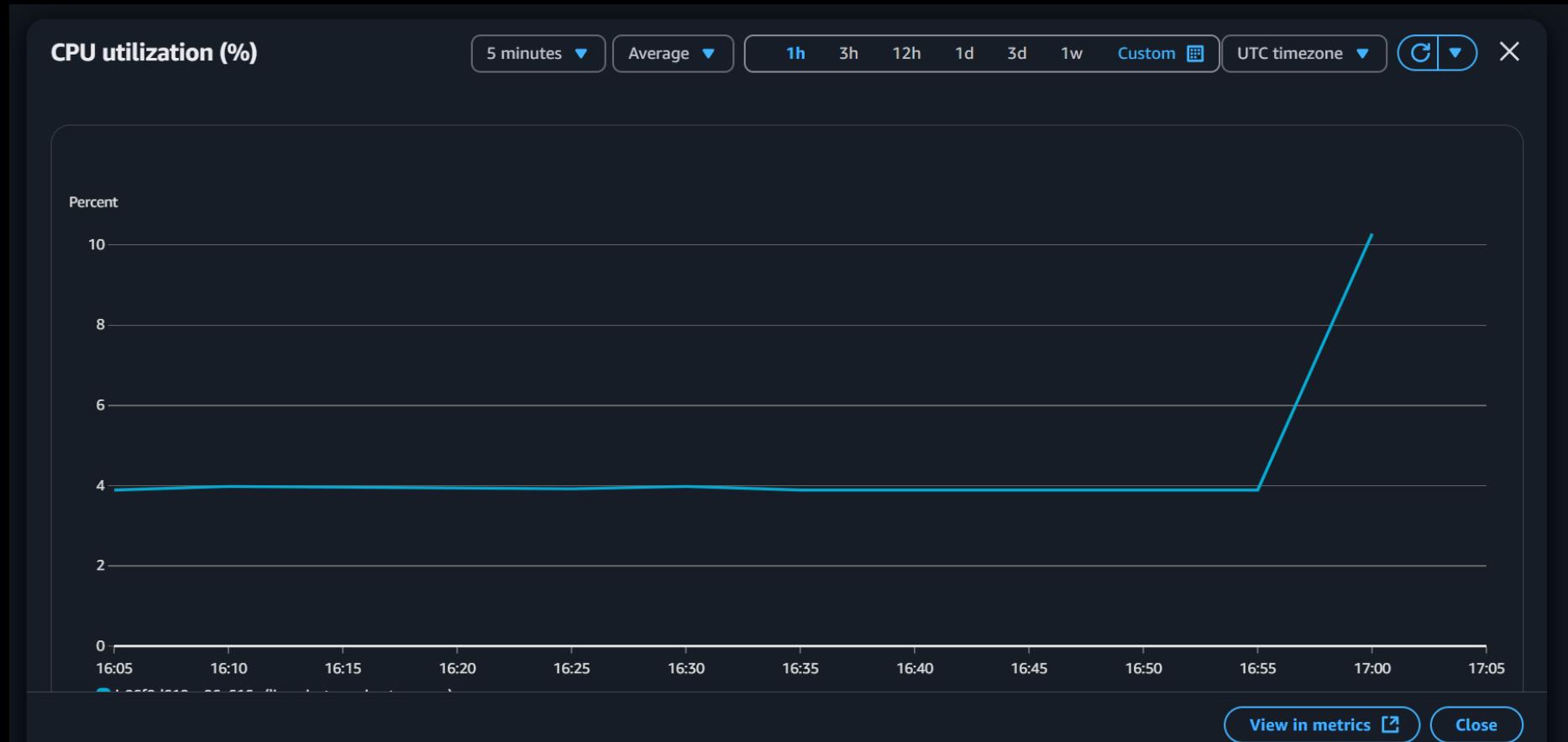
```
[ec2-user@ip-172-31-29-221 ~]$ stress --cpu 9  
stress: info: [32665] dispatching hogs: 9 cpu, 0 io, 0 vm, 0 hdd
```

30. Go back to the **CloudWatch dashboard**, click **All Alarms**, and you will see your alarm

The screenshot shows the AWS CloudWatch Alarms page with the following details:

- Alarms (1)**: Shows there is one alarm.
- Actions** button is highlighted in orange.
- Search bar**: Contains the placeholder "Search".
- Filter buttons**: "Hide Auto Scaling alarms", "Clear selection", "Create composite alarm", "Actions", and "Create alarm".
- Table Headers**: Name, State, Last state update (UTC), Conditions, Actions.
- Table Data**:
 - Name**: awsec2-i-06f9d619ee06e616a
 - State**: In alarm (indicated by a yellow exclamation mark icon)
 - Last state update (UTC)**: 2025-02-17 17:07:16
 - Conditions**: CPUUtilization >= 50 for 1 datapoints within 5 minutes
 - Actions**: A checkbox labeled "Action" with a green checkmark is checked.

31. Wait a few minutes and observe the increase in CPU utilization.



32. You will receive an **email notification** when CPU utilization crosses the threshold.

ALARM: "awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization" in US West (Oregon) Inbox ×

 AWS Notifications <no-reply@sns.amazonaws.com> 10:37 PM (3 minutes ago) to me ▾ ...

You are receiving this email because your Amazon CloudWatch Alarm "awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization" in the US West (Oregon) region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [72.15875312675482 (17/02/25 17:02:00)] was greater than or equal to the threshold (50.0)." at "Monday 17 February, 2025 17:07:16 UTC".

View this alarm in the AWS Management Console:
<https://us-west-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-2#alarmsV2:alarm/awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization>

Alarm Details:

- Name: awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization
- Description: Alarm on instance i-06f9d619ee06e616a: Triggered when CPUUtilization >= 50 for 1 consecutive 5-minute periods.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [72.15875312675482 (17/02/25 17:02:00)] was greater than or equal to the threshold (50.0).
- Timestamp: Monday 17 February, 2025 17:07:16 UTC
- AWS Account: 971422709086
- Alarm Arn: arn:aws:cloudwatch:us-west-2:971422709086:alarm:awsec2-i-06f9d619ee06e616a-GreaterThanOrEqualToThreshold-CPUUtilization

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 50.0 for at least 1 of the last 1 period(s) of 300 seconds.

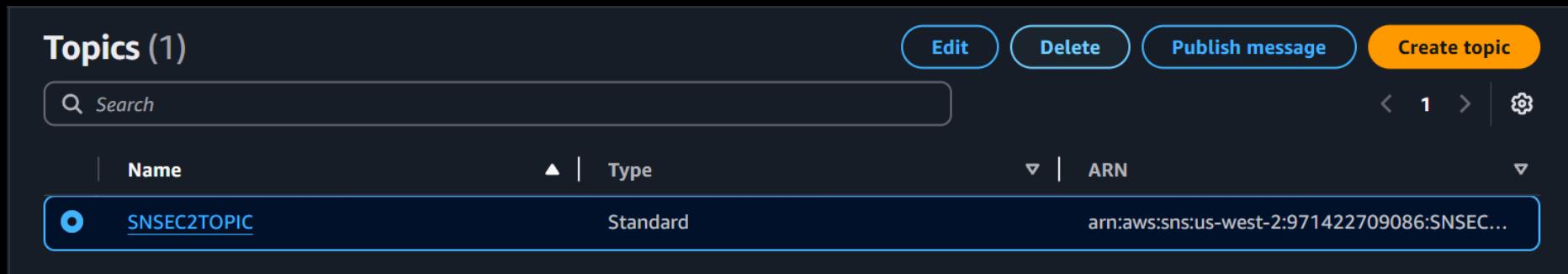
Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-06f9d619ee06e616a]
- Period: 300 seconds

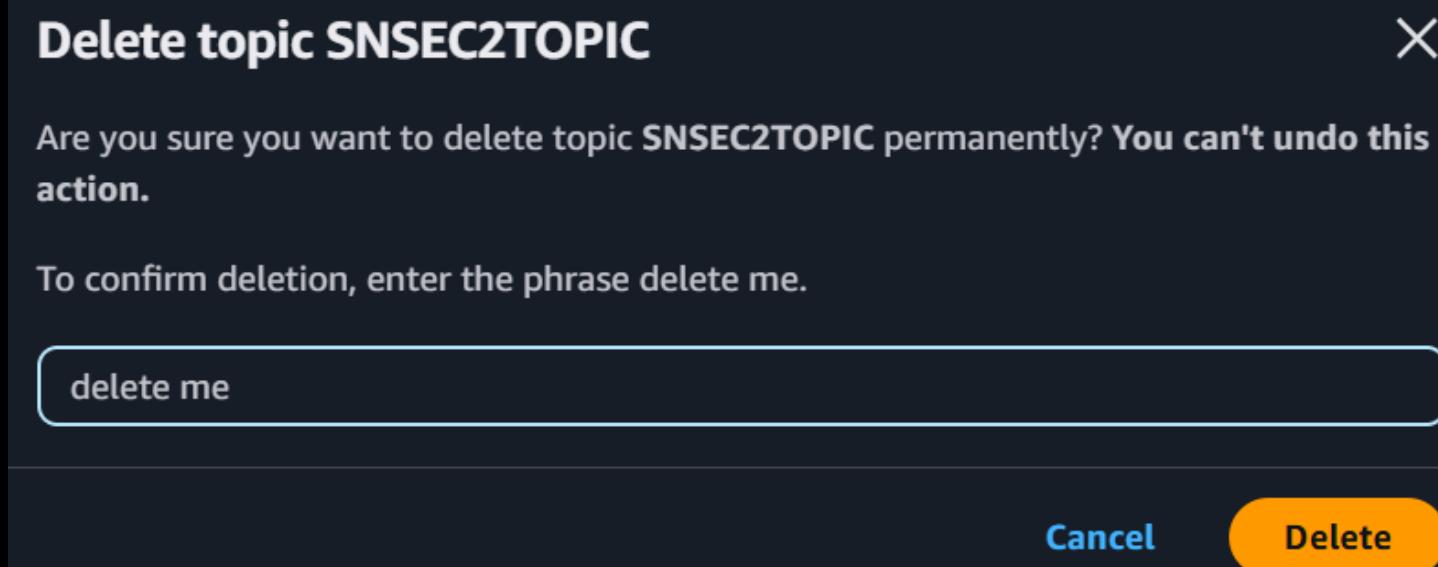
VI. CLEANING UP RESOURCES

To avoid unnecessary charges, follow these steps to delete resources:

1. Delete the SNS Topic.



The screenshot shows the AWS SNS 'Topics' list. At the top, there are buttons for 'Edit', 'Delete', 'Publish message', and 'Create topic'. Below is a search bar and a navigation bar with page numbers (1) and a gear icon. The main table has columns for 'Name', 'Type', and 'ARN'. A single row is selected, showing 'SNSEC2TOPIC' as the name, 'Standard' as the type, and a long ARN as the value. The 'Delete' button is highlighted with a blue border.

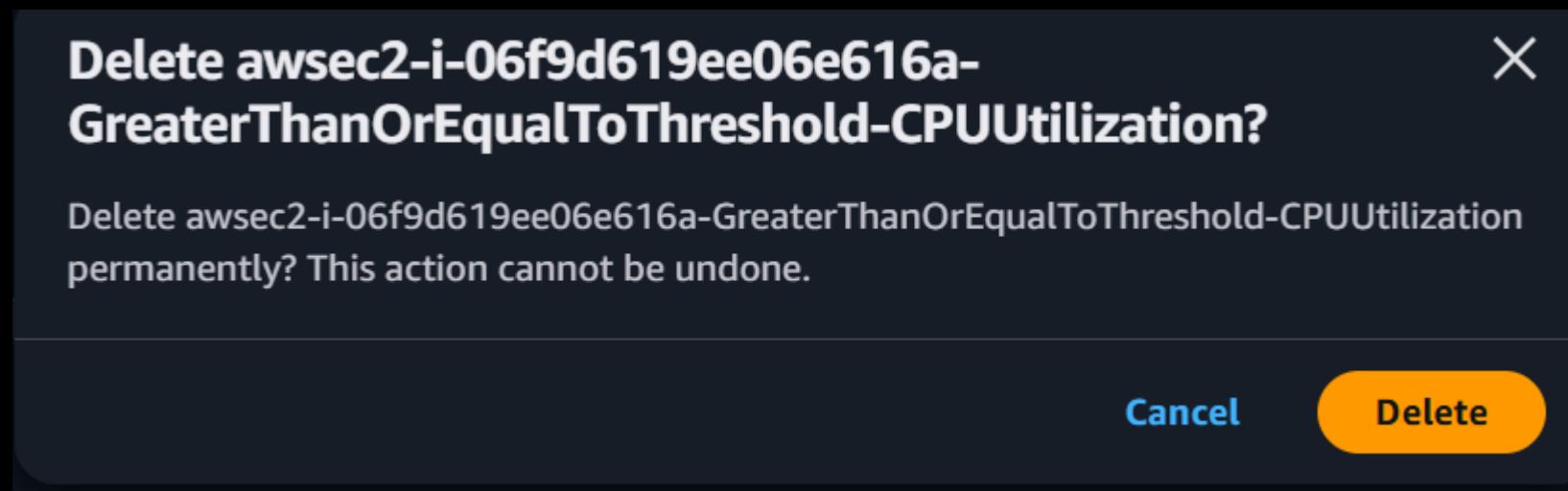
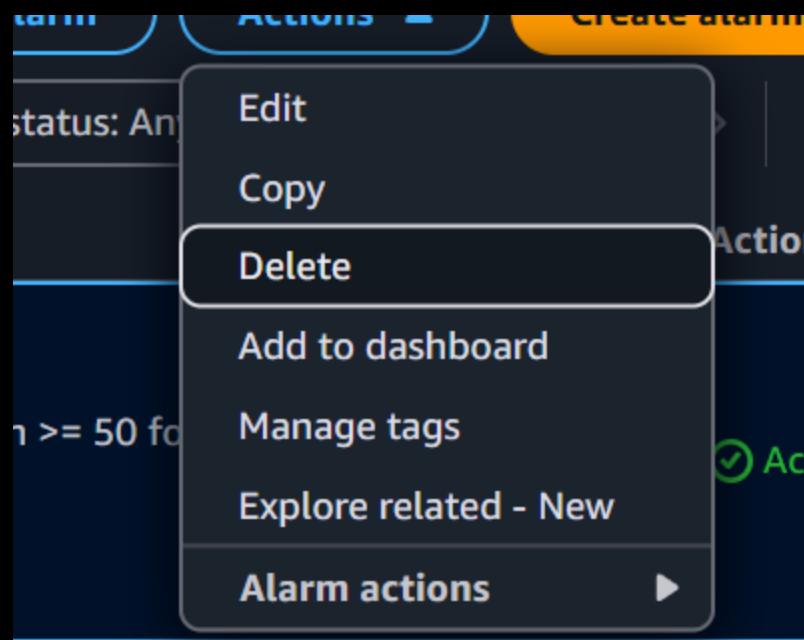


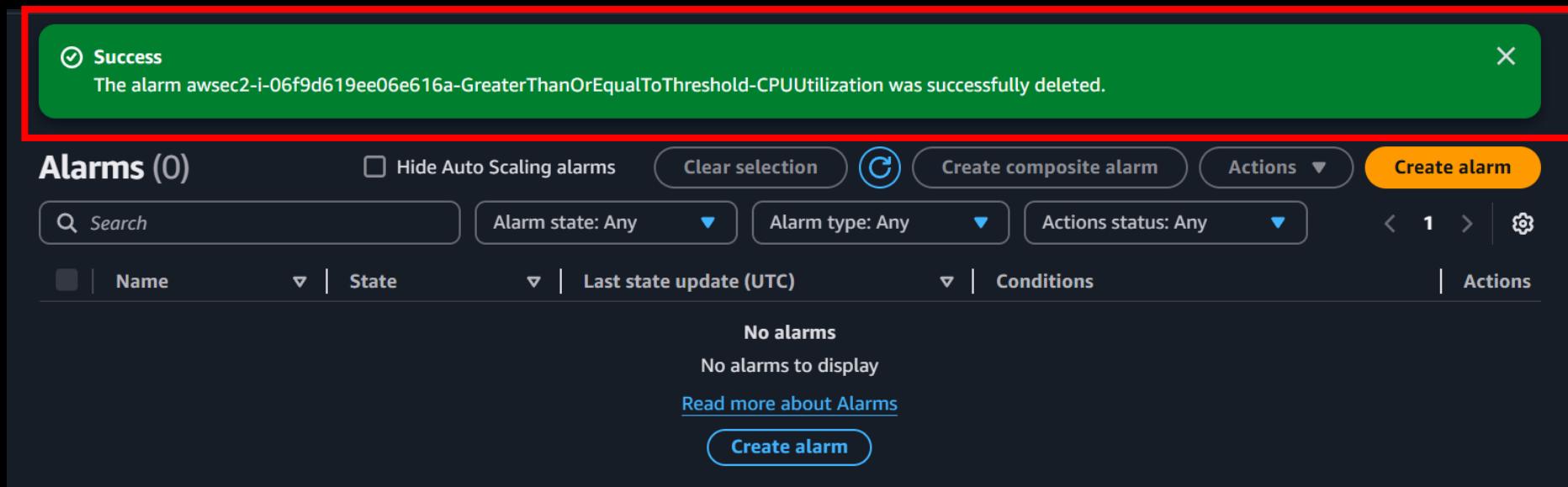
The screenshot shows a confirmation dialog box. The title is 'Delete topic SNSEC2TOPIC'. The text inside says, 'Are you sure you want to delete topic **SNSEC2TOPIC** permanently? You can't undo this action.' Below that, it says, 'To confirm deletion, enter the phrase delete me.' There is a text input field containing 'delete me'. At the bottom are 'Cancel' and 'Delete' buttons, with 'Delete' being orange.

The screenshot shows the AWS Lambda Topics page. At the top, a green notification bar displays the message "Topic SNSEC2TOPIC deleted successfully." with a red rectangular border around it. Below the notification, the page title is "Topics (0)". There are four buttons: "Edit", "Delete", "Publish message", and "Create topic". A search bar is present above the table. The table has columns for "Name", "Type", and "ARN". The message "No topics" is displayed, followed by "To get started, create a topic." and a "Create topic" button.

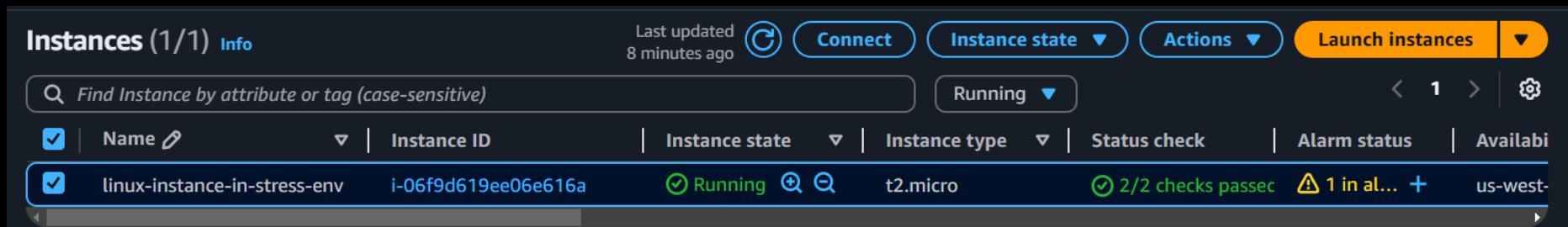
2. Delete the CloudWatch Alarm.

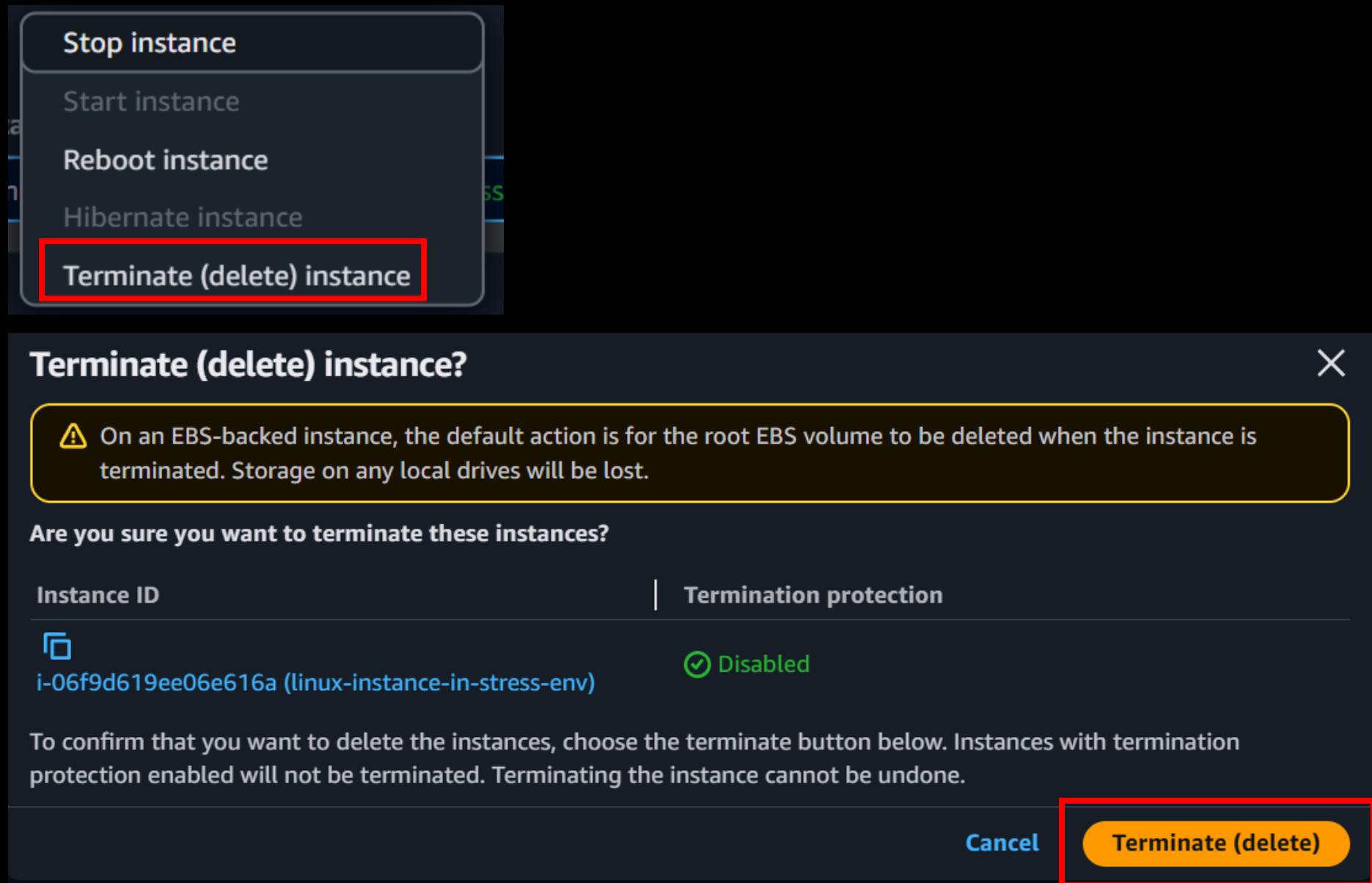
The screenshot shows the AWS CloudWatch Alarms page. The title is "Alarms (1/1)". There are several filters: "Hide Auto Scaling alarms" (unchecked), "Clear selection", "Create composite alarm", "Actions", "Create alarm", and search, alarm state, alarm type, and actions status dropdowns. The main table has columns for "Name", "State", "Last state update (UTC)", "Conditions", and "Actions". One alarm is listed: "awsec2-i-06f9d619ee06e616a" (OK, last updated 2025-02-17 17:11:16) with the condition "CPUUtilization >= 50 for 1 datapoints within 5 minutes" and an "Actions" link.

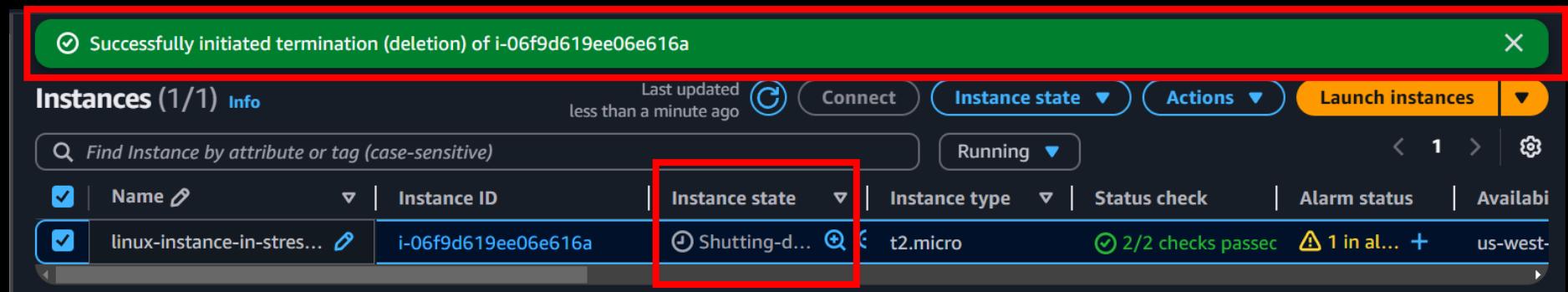




3. Terminate the EC2 Instance.







 CONCLUSION

In this project, we successfully created an EC2 instance, configured CloudWatch alarms, and set up SNS notifications to monitor CPU utilization. By inducing artificial stress using the **stress** tool, we observed real-time CPU performance monitoring and received alert notifications via email. This setup is useful for performance testing, monitoring system health, and responding to potential issues in a cloud environment.

By following these steps, you have learned the fundamentals of setting up an automated alert system using **AWS EC2, CloudWatch, and SNS**, which can be extended for production-level monitoring and response automation.

'WHAT GETS MEASURED, GETS MANAGED'

- PETER DRUCKER