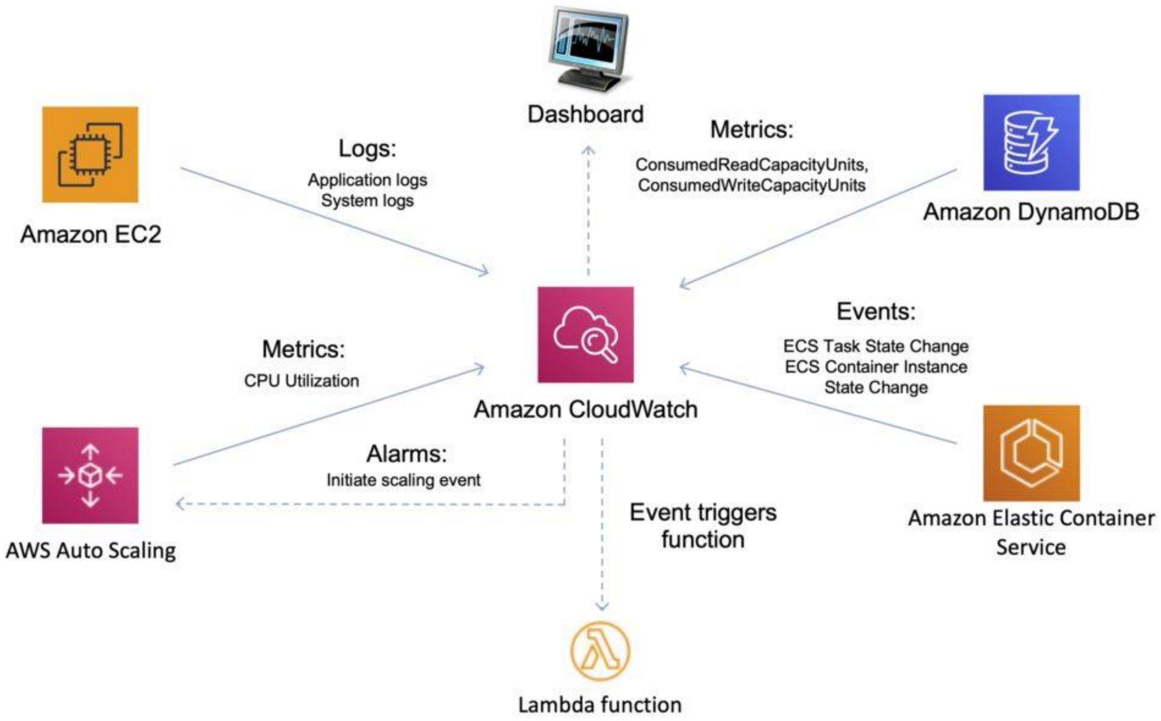
CLOUD WATCH

Amazon CloudWatch is a monitoring service for Amazon Web Services cloud resources and the applications you run on Amazon Web Services. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your Amazon Web Services resources. Amazon CloudWatch can monitor Amazon Web Services resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

With CloudWatch you can:

- Gain system-wide visibility into resource utilization.
- Monitor application performance.
- Monitor operational health.



1. CloudWatch alarms monitor metrics and can be configured to automatically initiate actions.
2. CloudWatch Logs centralizes logs from systems, applications, and AWS services.
3. CloudWatch Events delivers a stream of system events that describe changes in AWS resources.
4. CloudWatch is accessed via API, command-line interface, AWS SDKs, and the AWS Management Console.
5. CloudWatch integrates with AWS IAM.
6. CloudWatch can automatically react to changes in your AWS resources.

With CloudWatch you can monitor resources such as:

- EC2 instances.
- DynamoDB tables.
- RDS DB instances.
- Custom metrics generated by applications and services.
- Any log files generated by your applications.

CloudWatch retains metric data as follows:

- Data points with a period of less than 60 seconds are available for 3 hours. These data points are high-resolution custom metrics.
- Data points with a period of 60 seconds (1 minute) are available for 15 days.
- Data points with a period of 300 seconds (5 minute) are available for 63 days.
- Data points with a period of 3600 seconds (1 hour) are available for 455 days (15 months).

Key Features of CloudWatch

Metrics Collection:

- CloudWatch collects and tracks metrics for AWS services like EC2, RDS, S3, Lambda, and many others.
- Custom metrics can also be created for your applications and infrastructure.

Alarms:

- You can set alarms to automatically react to changes in your metrics, such as CPU utilization, memory usage, or custom metrics.
- Alarms can trigger actions like sending notifications, executing Auto Scaling policies, or invoking AWS Lambda functions.

Logs Management:

- CloudWatch Logs allows you to monitor, store, and access log files from AWS services and custom applications.
- You can set up log group filters and metrics to analyze log data and create dashboards.

Events:

- CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources.
- You can configure rules to match events and route them to targets like Lambda functions, Kinesis streams, or other AWS services.

Dashboards:

- CloudWatch Dashboards allow you to create customizable visualizations of your metrics and logs.
- Dashboards can be shared and provide an at-a-glance view of the health and performance of your resources.

Application Insights:

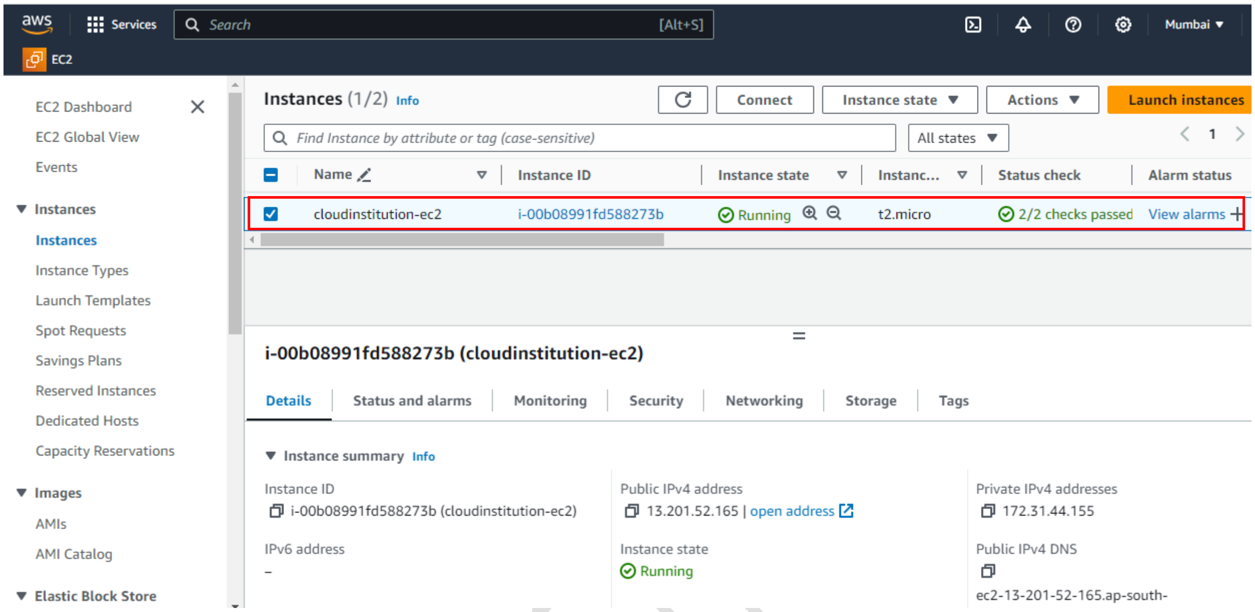
- CloudWatch Application Insights provides automated monitoring for your applications, helping to detect common problems like memory leaks, misconfigurations, and other issues.

CloudWatch Vs CloudTrail:

CloudWatch	CloudTrail
Performance monitoring	Auditing
Log events across AWS Services – think operations	Log API activity across AWS services – think activities, or who to blame
Higher-level comprehensive monitoring and event service	More low-level, granular
Log from multiple accounts	Log from multiple accounts
Logs stored indefinitely	Logs stored to S3 or CloudWatch indefinitely
Alarms history for 14 days	No native alarming; can use CloudWatch alarms

Set Up an Alarm to Terminate an Instance Using Amazon CloudWatch

Step 1 : Create a EC2 instance



Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

☑	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status
☑	cloudinstitution-ec2	i-00b08991fd588273b	Running	t2.micro	2/2 checks passed	View alarms +

i-00b08991fd588273b (cloudinstitution-ec2)

▼ Instance summary Info

Instance ID: i-00b08991fd588273b (cloudinstitution-ec2)

Public IPv4 address: 13.201.52.165 | open address

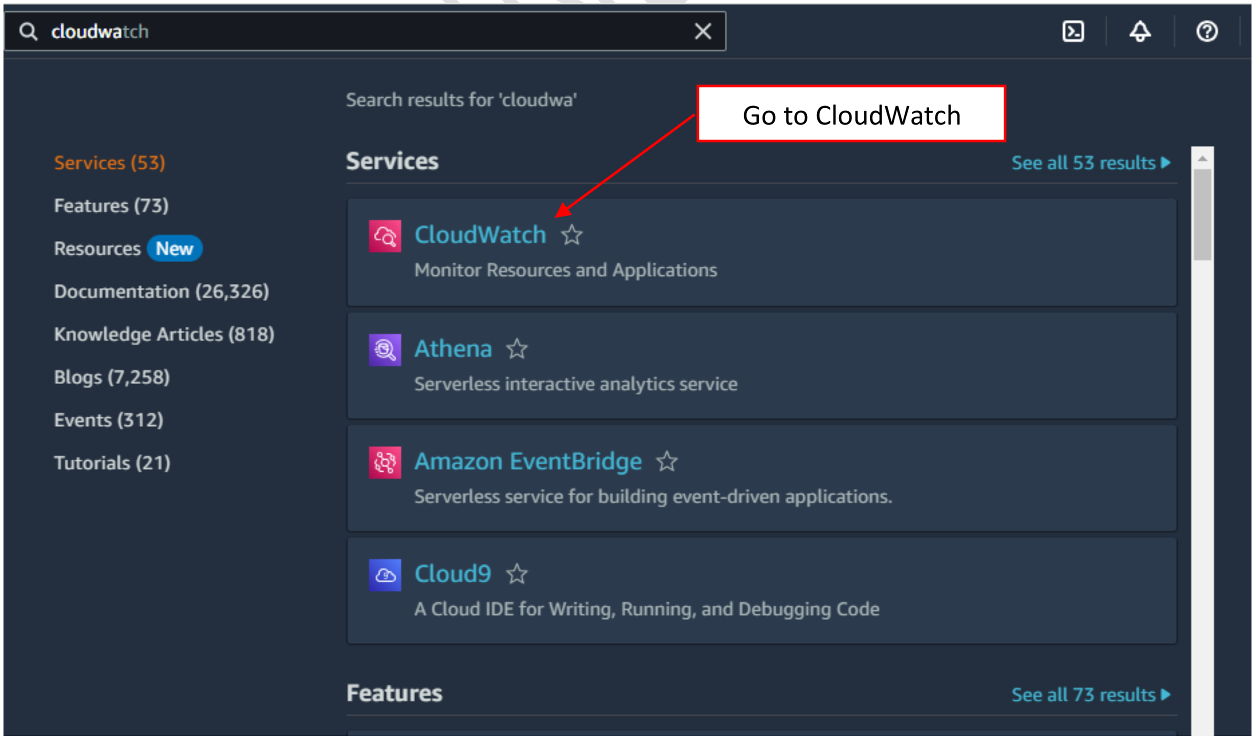
Private IPv4 addresses: 172.31.44.155

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-13-201-52-165.ap-south-

Step 2 : Create a Alarm in cloud watch to monitor the CPU utilization in EC2 instance



Search results for 'cloudwa'

Services

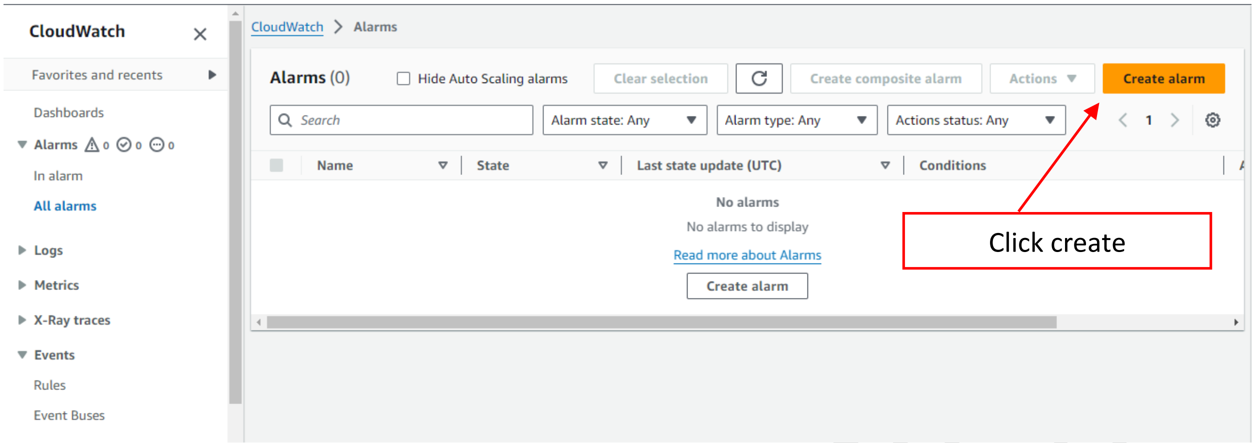
CloudWatch ☆
Monitor Resources and Applications

Athena ☆
Serverless interactive analytics service

Amazon EventBridge ☆
Serverless service for building event-driven applications.

Cloud9 ☆
A Cloud IDE for Writing, Running, and Debugging Code

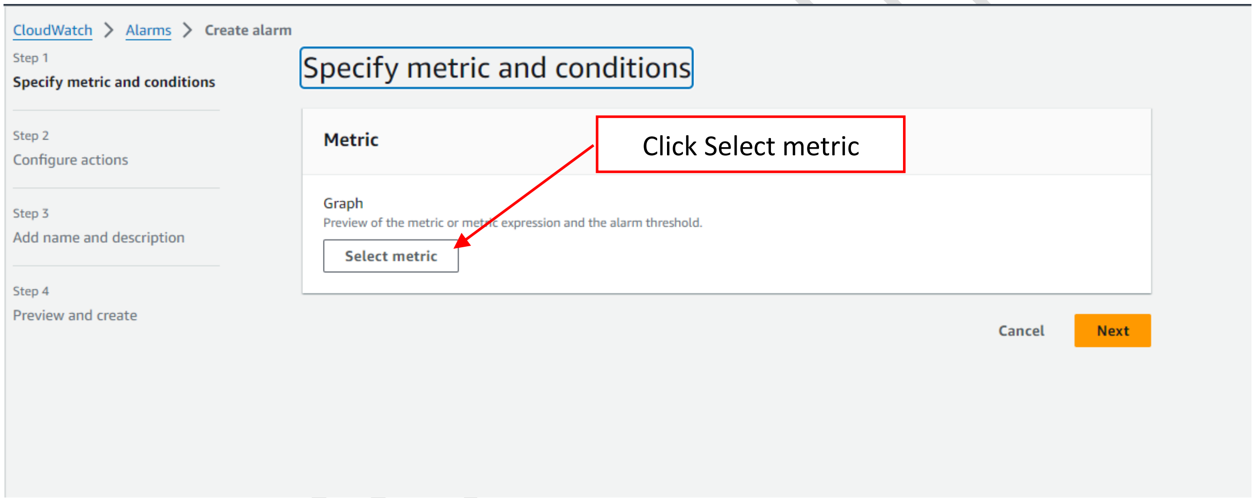
Features



No alarms

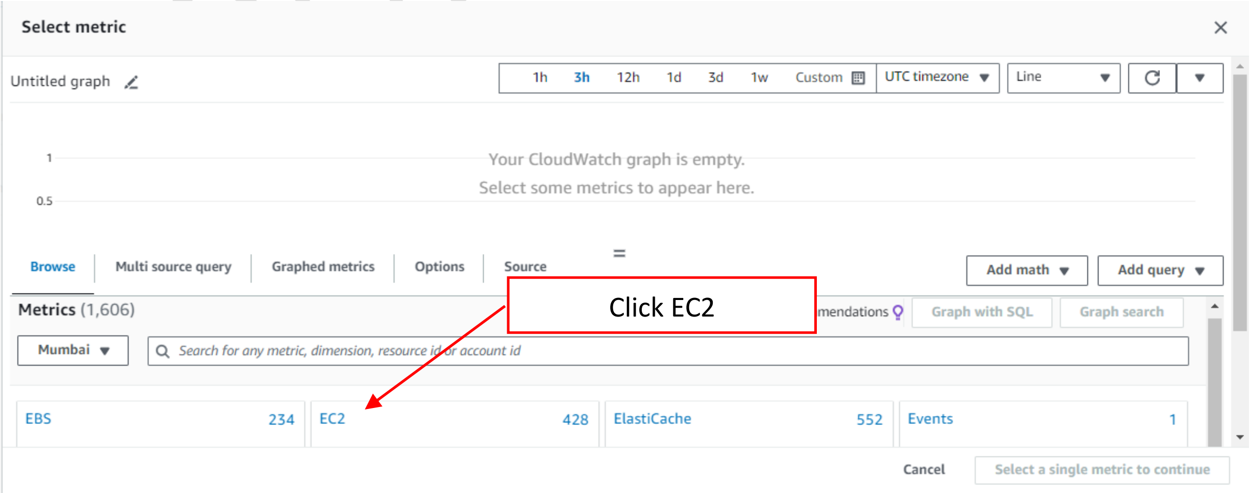
No alarms to display

Click create



Preview of the metric or metric expression and the alarm threshold.

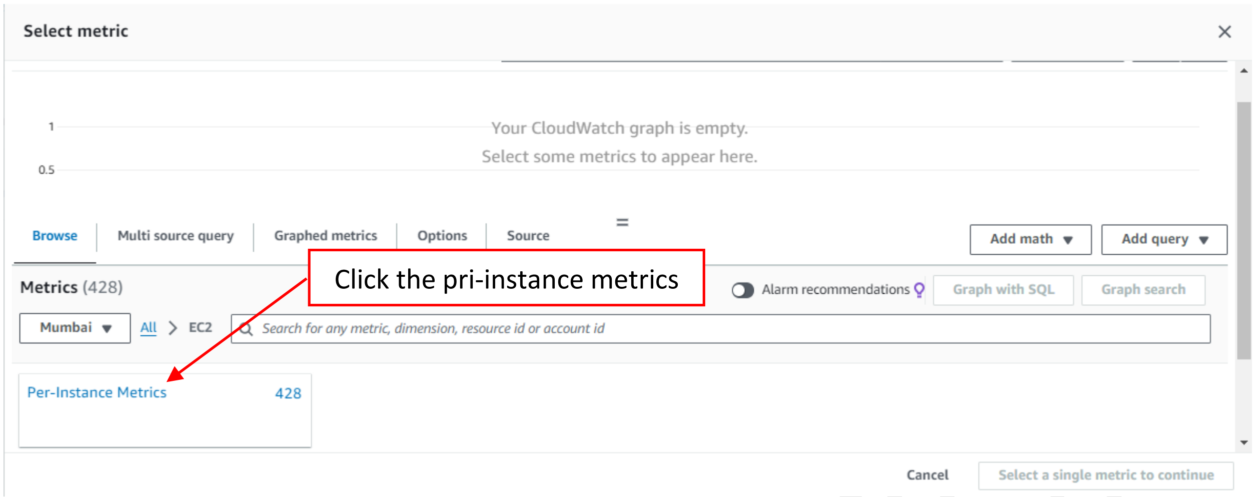
Click Select metric



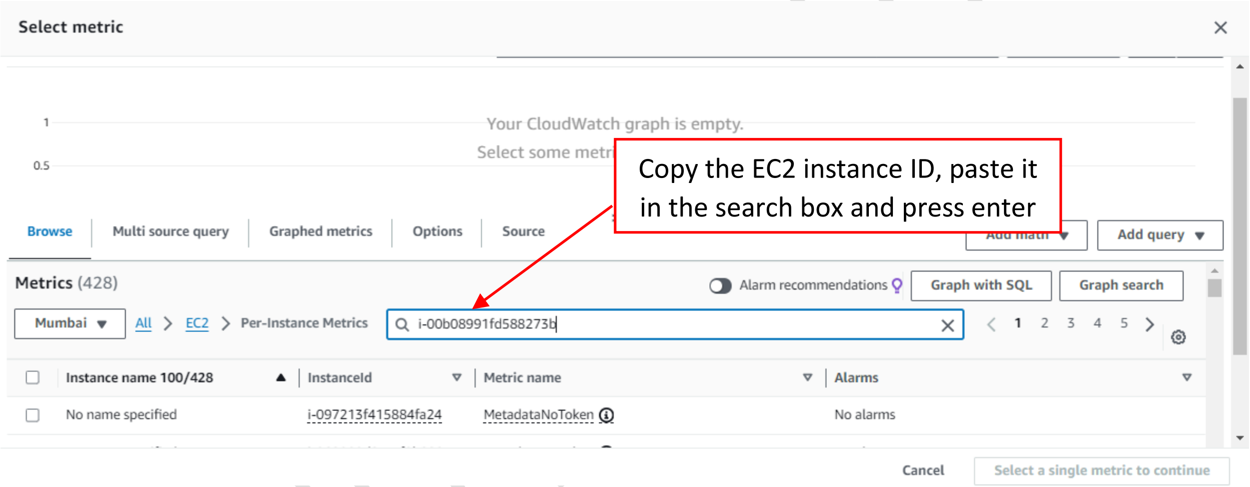
Your CloudWatch graph is empty.

Select some metrics to appear here.

Click EC2



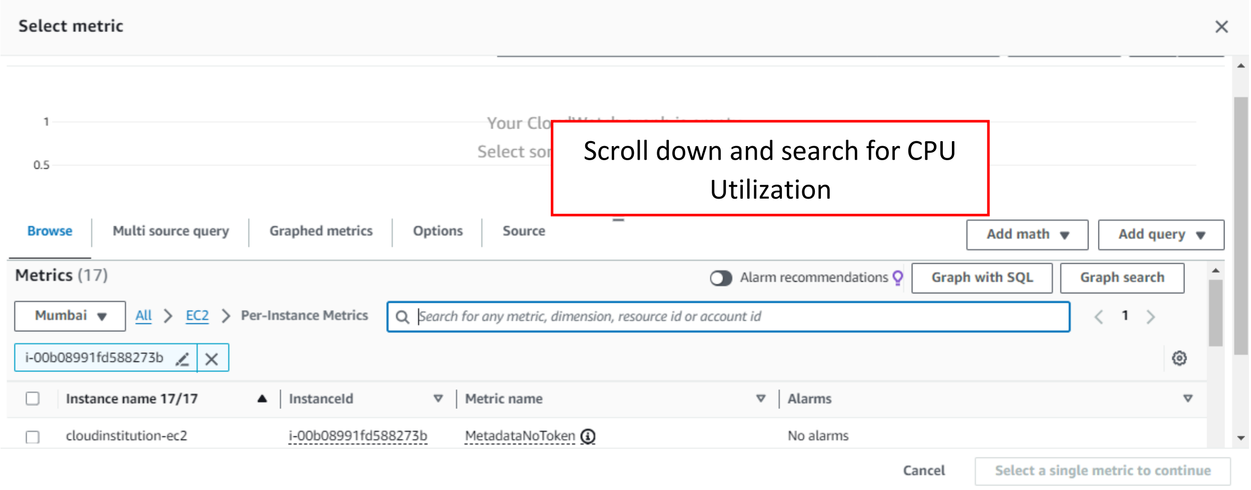
Click the pri-instance metrics



Copy the EC2 instance ID, paste it in the search box and press enter

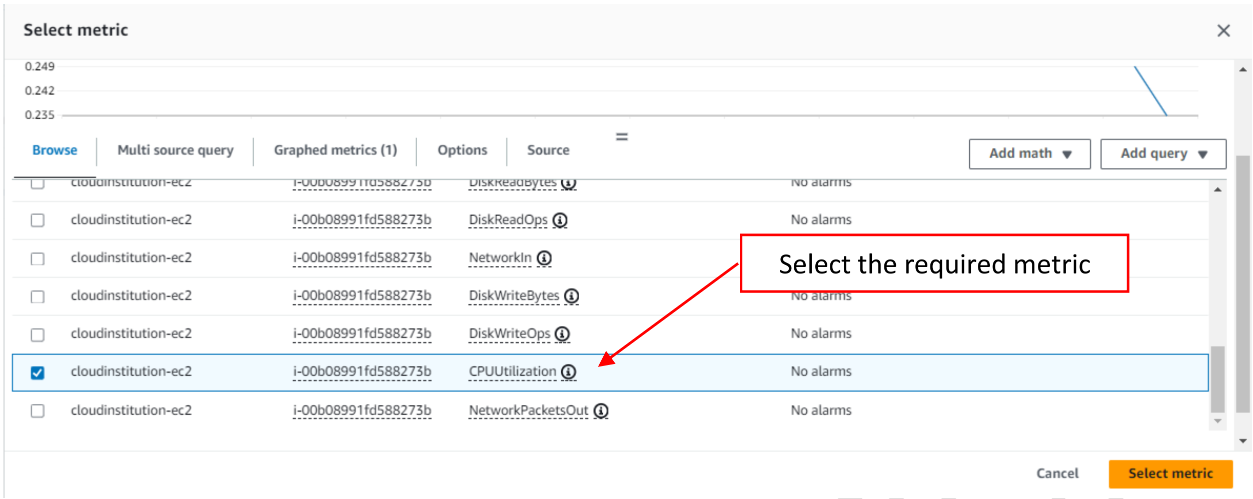
i-00b08991fd588273b

Instance name 100/428	InstanceId	Metric name	Alarms
No name specified	i-097213f415884fa24	MetadataNoToken	No alarms



Scroll down and search for CPU Utilization

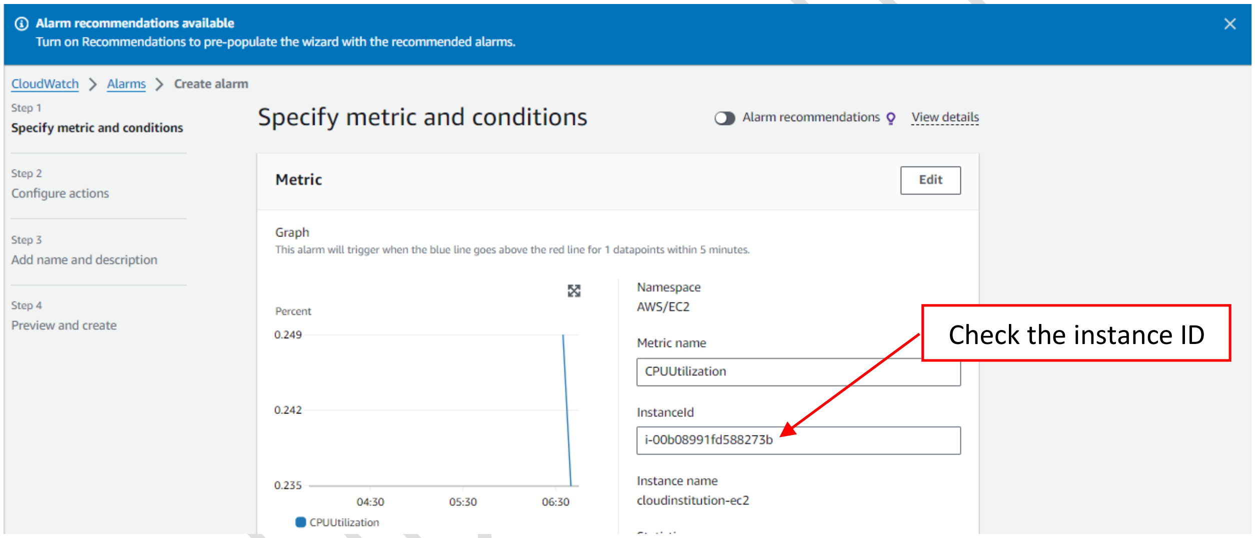
Instance name 17/17	InstanceId	Metric name	Alarms
cloudinstitution-ec2	i-00b08991fd588273b	MetadataNoToken	No alarms



Select metric

□	cloudinstitution-ec2	i-00b08991fd588273b	DiskReadBytes	No alarms
□	cloudinstitution-ec2	i-00b08991fd588273b	DiskReadOps	No alarms
□	cloudinstitution-ec2	i-00b08991fd588273b	NetworkIn	No alarms
□	cloudinstitution-ec2	i-00b08991fd588273b	DiskWriteBytes	No alarms
□	cloudinstitution-ec2	i-00b08991fd588273b	DiskWriteOps	No alarms
☑	cloudinstitution-ec2	i-00b08991fd588273b	CPUUtilization	No alarms
□	cloudinstitution-ec2	i-00b08991fd588273b	NetworkPacketsOut	No alarms

Select the required metric



Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.

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

Metric

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

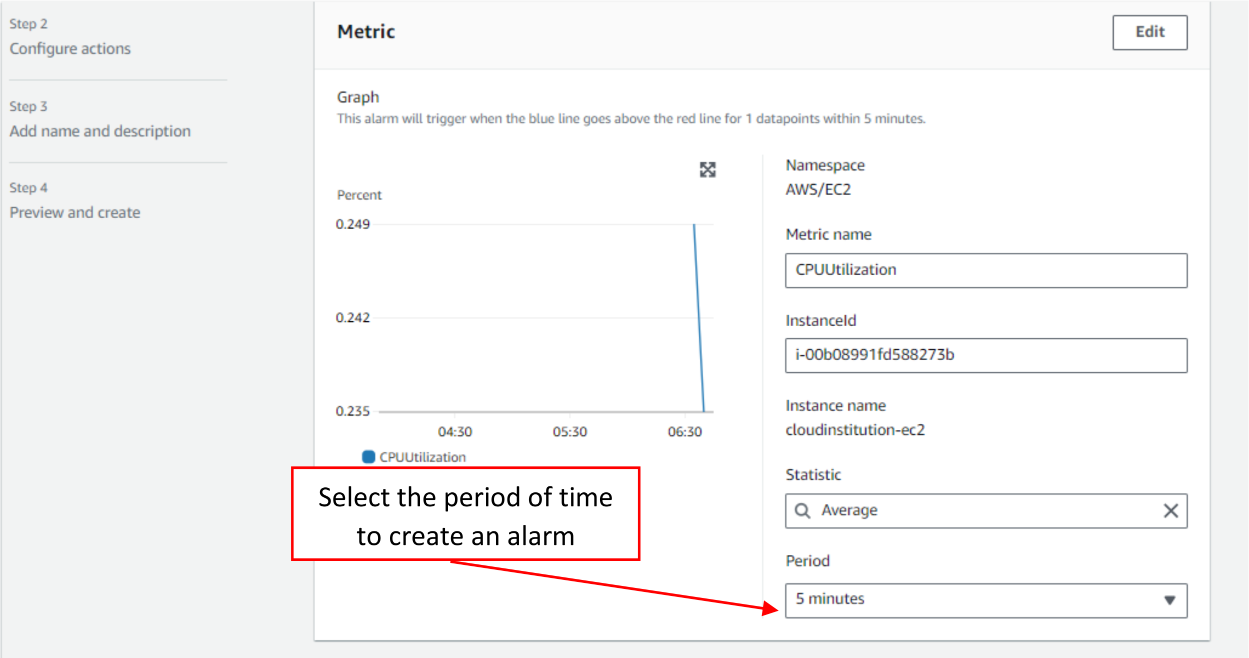
Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-00b08991fd588273b

Instance name
cloudinstitution-ec2

Check the instance ID



Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Metric Edit

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

Namespace
AWS/EC2

Metric name
CPUUtilization

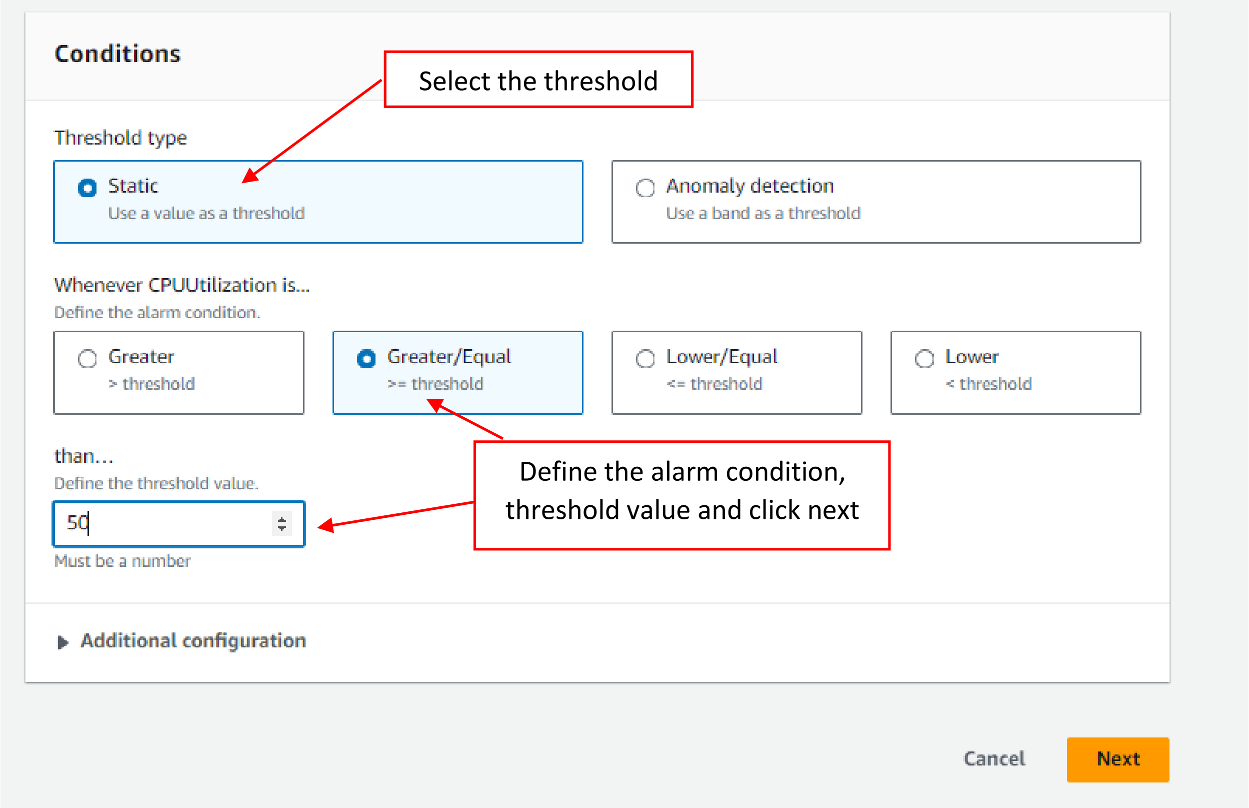
InstanceId
i-00b08991fd588273b

Instance name
cloudinstitution-ec2

Statistic
Average

Period
5 minutes

Select the period of time to create an alarm



Conditions

Select the threshold

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

than...
Define the threshold value.

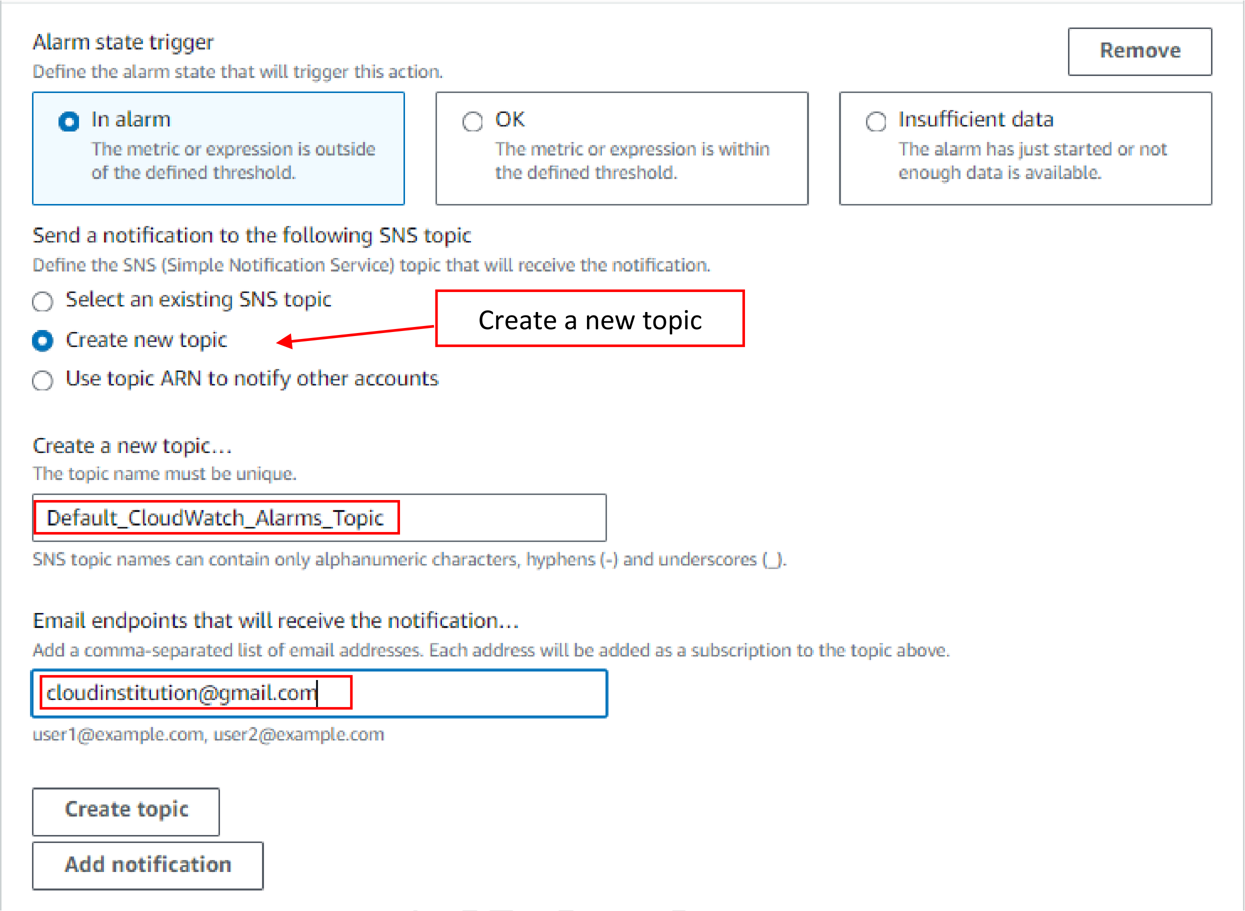
50

Must be a number

Define the alarm condition, threshold value and click next

▸ Additional configuration

Cancel Next



Alarm state trigger

Define the alarm state that will trigger this action.

● In alarm
The metric or expression is outside of the defined threshold.

○ OK
The metric or expression is within the defined threshold.

○ Insufficient data
The alarm has just started or not enough data is available.

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

○ Select an existing SNS topic

● Create new topic

○ Use topic ARN to notify other accounts

Create a new topic

Create a new topic…

The topic name must be unique.

Default_CloudWatch_Alarms_Topic

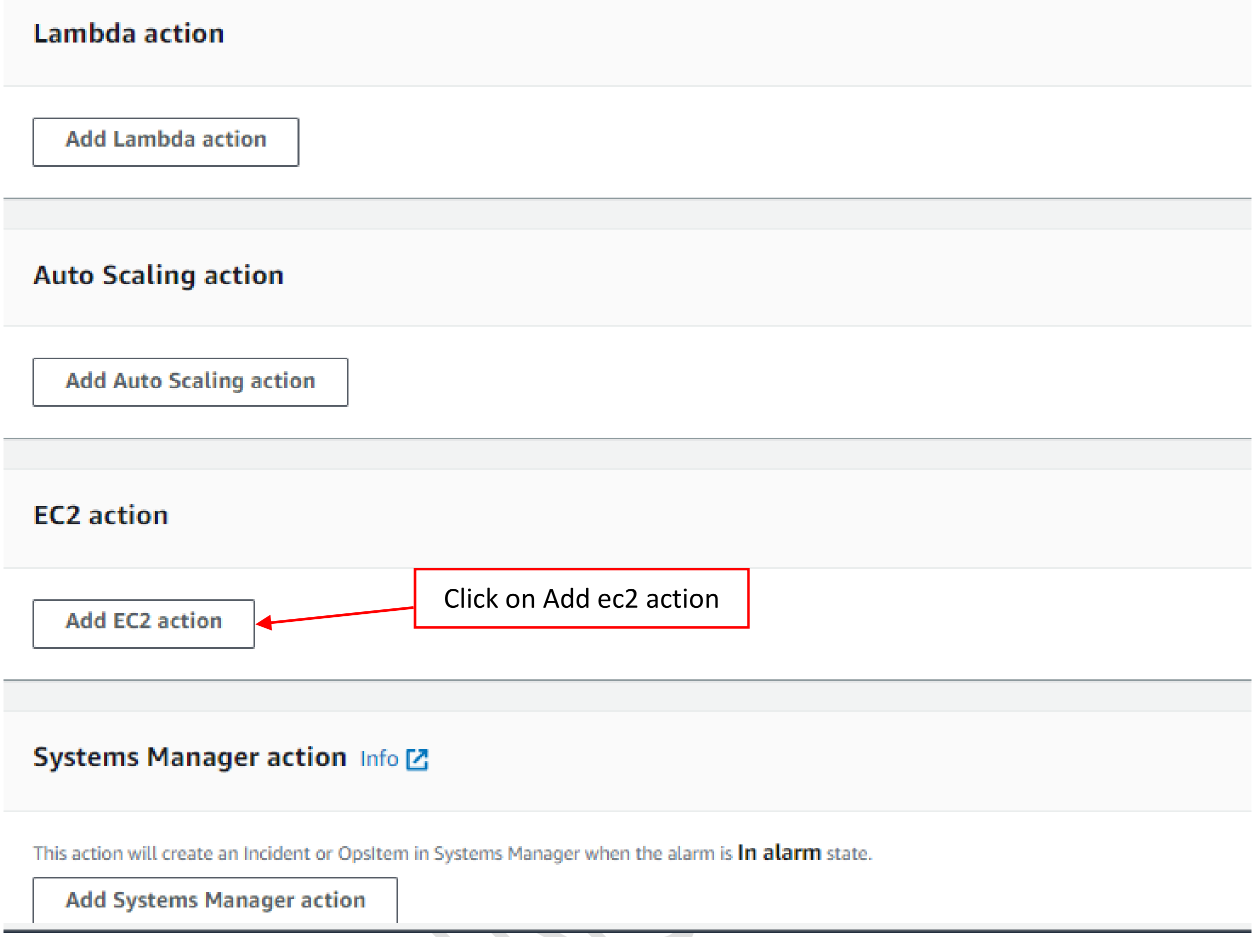
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification…

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

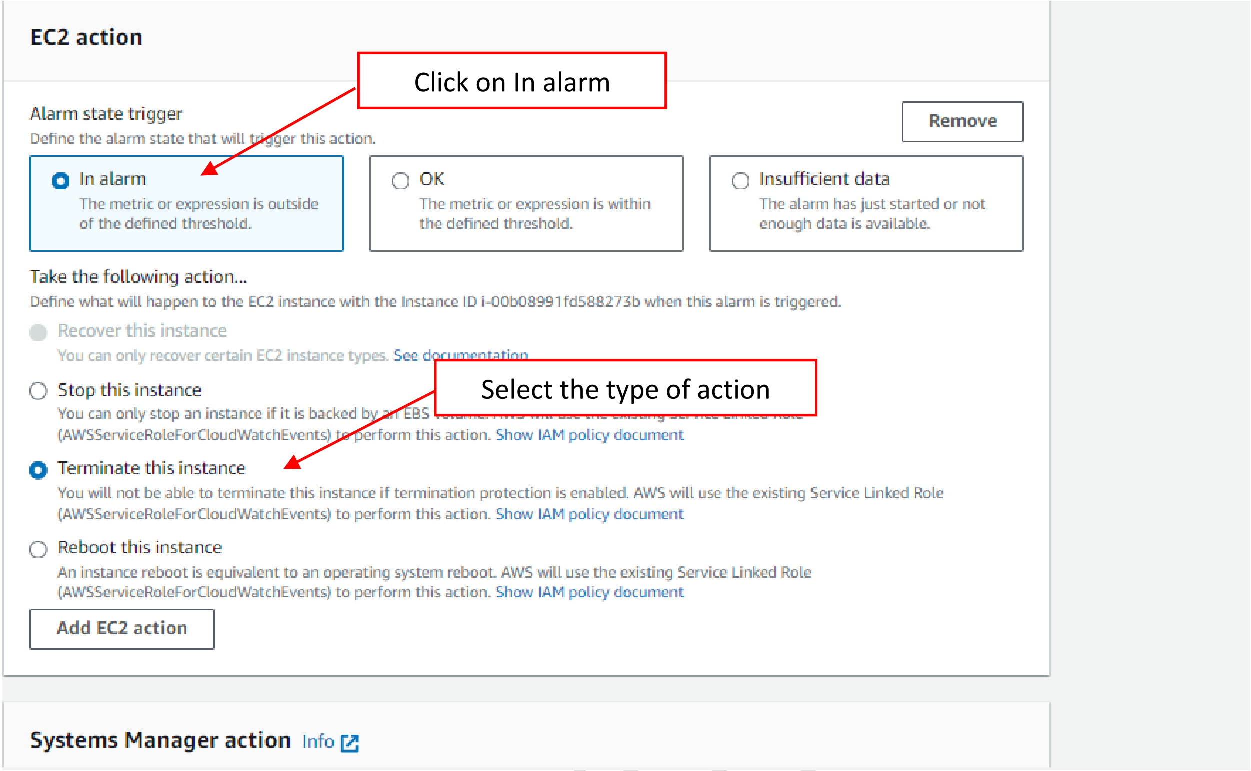
cloudinstitution@gmail.com

user1@example.com, user2@example.com



This action will create an Incident or OpsItem in Systems Manager when the alarm is **In alarm** state.

Click on Add ec2 action



EC2 action

Click on In alarm

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

● In alarm
The metric or expression is outside of the defined threshold.

○ OK
The metric or expression is within the defined threshold.

○ Insufficient data
The alarm has just started or not enough data is available.

Take the following action...

Define what will happen to the EC2 instance with the Instance ID i-00b08991fd588273b when this alarm is triggered.

● Recover this instance
You can only recover certain EC2 instance types. See documentation

Select the type of action

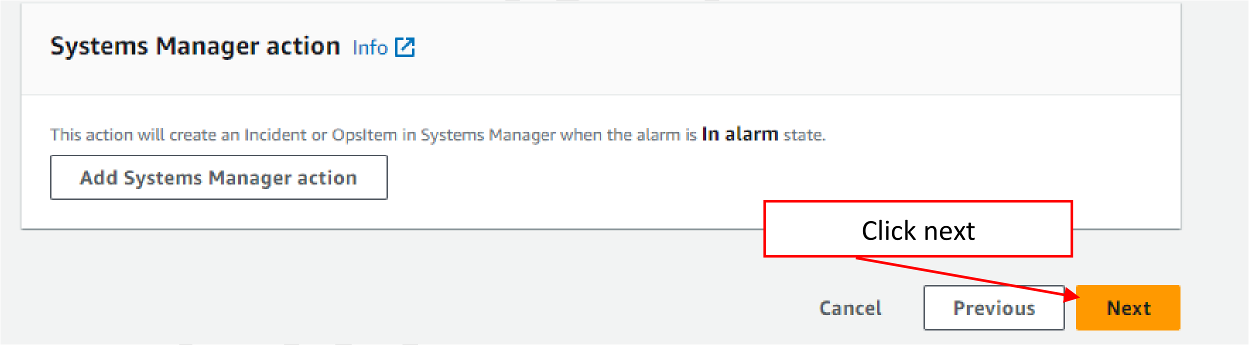
○ Stop this instance
You can only stop an instance if it is backed by an EBS volume. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document

● Terminate this instance
You will not be able to terminate this instance if termination protection is enabled. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document

○ Reboot this instance
An instance reboot is equivalent to an operating system reboot. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document

Add EC2 action

Systems Manager action Info



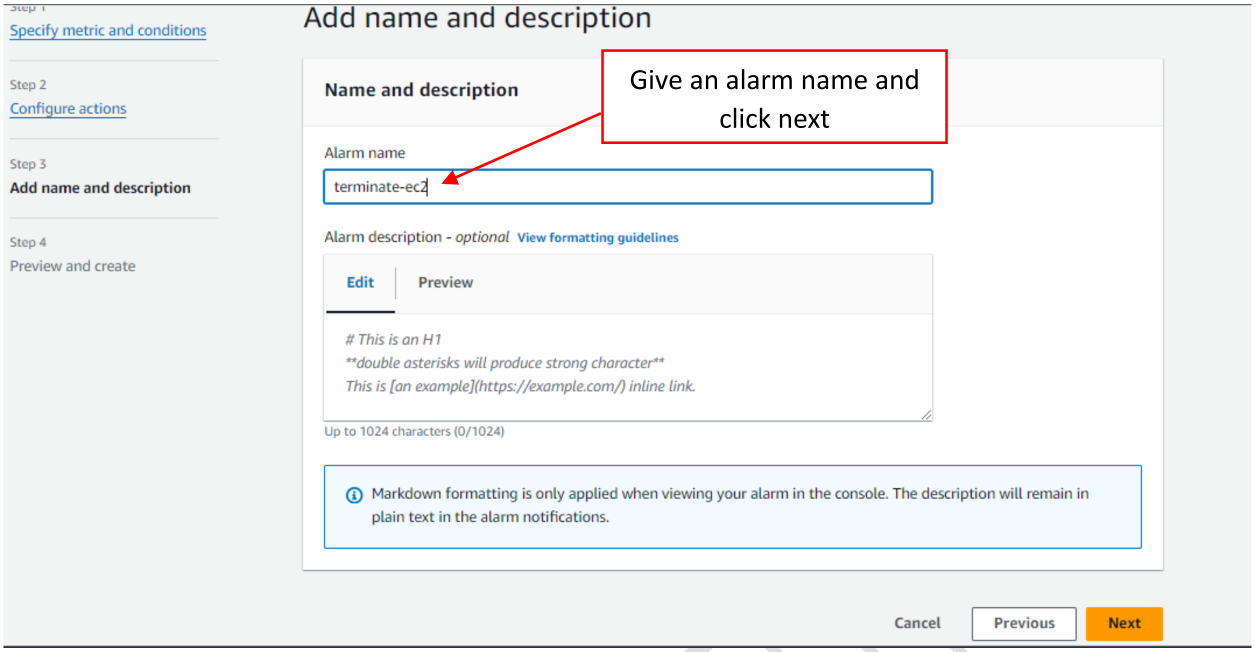
Systems Manager action Info

This action will create an Incident or OpsItem in Systems Manager when the alarm is **In alarm** state.

Add Systems Manager action

Click next

Cancel Previous Next



Step 1

Specify metric and conditions

Step 2

Configure actions

Step 3

Add name and description

Step 4

Preview and create

Add name and description

Name and description

Alarm name

terminate-ec2

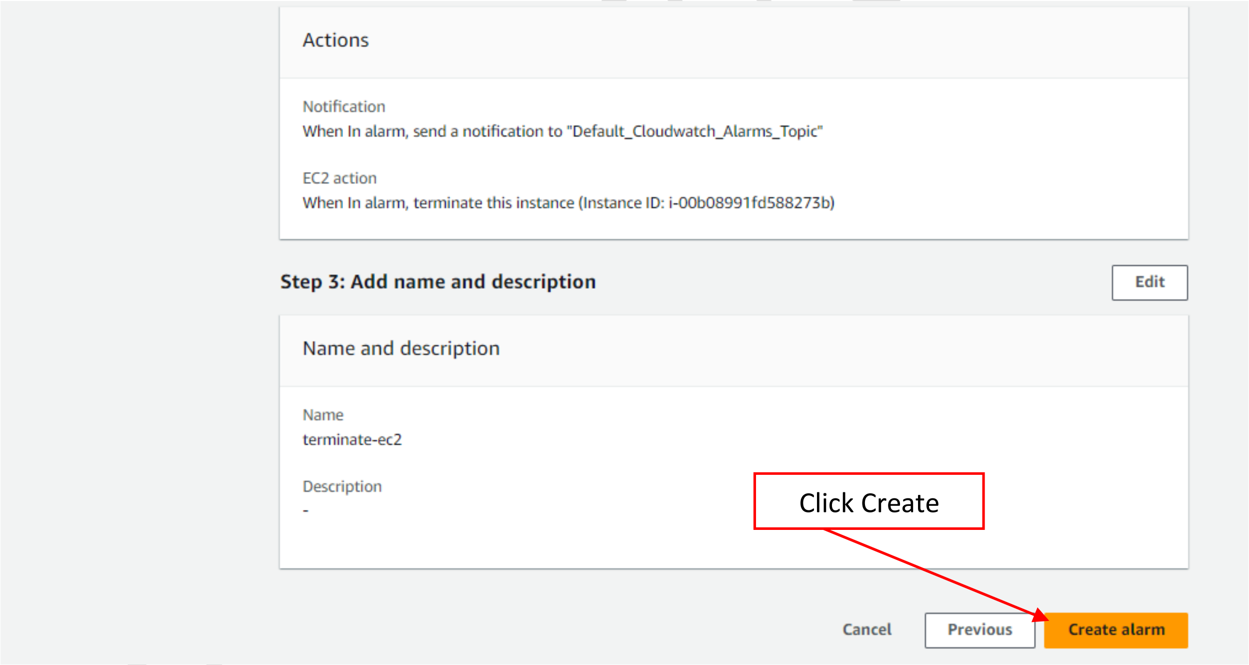
Alarm description - *optional* View formatting guidelines

# This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Give an alarm name and click next



Actions

Notification

When In alarm, send a notification to "Default_Cloudwatch_Alarms_Topic"

EC2 action

When In alarm, terminate this instance (Instance ID: i-00b08991fd588273b)

Step 3: Add name and description

Name and description

Name

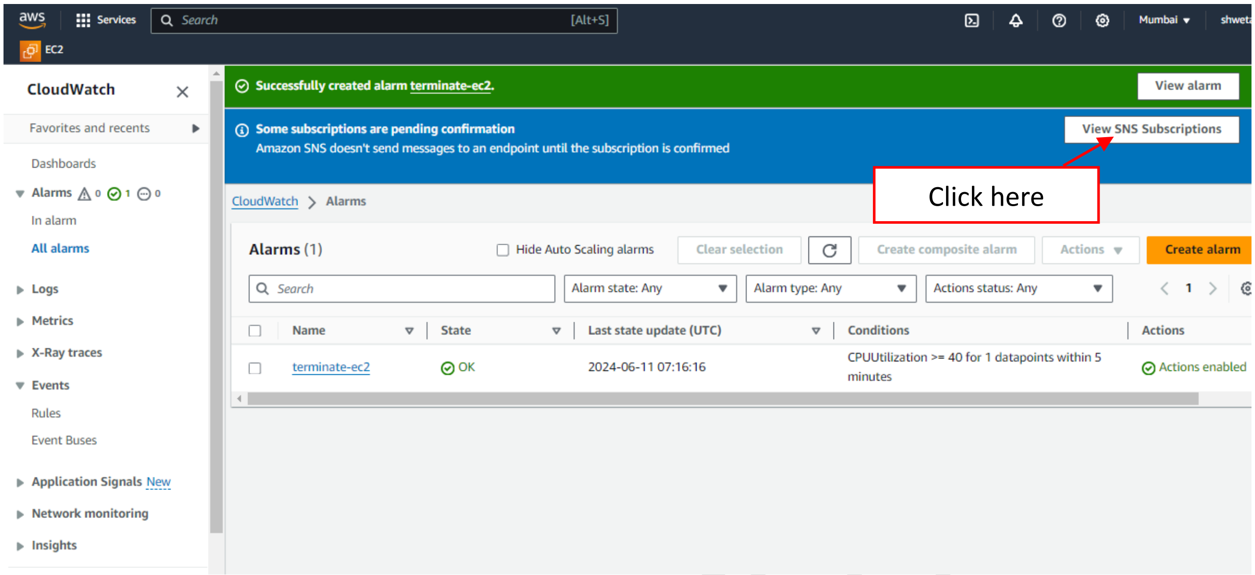
terminate-ec2

Description

-

Click Create

Alarm created successfully

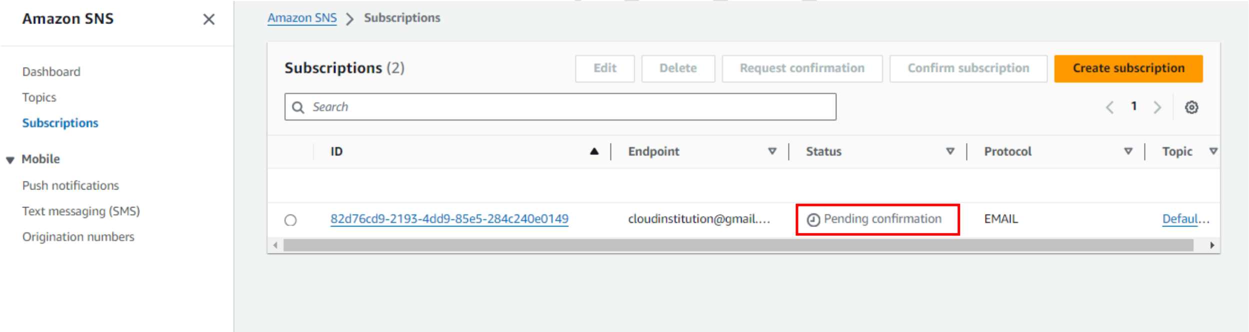


Successfully created alarm terminate-ec2.

Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

Alarms (1)

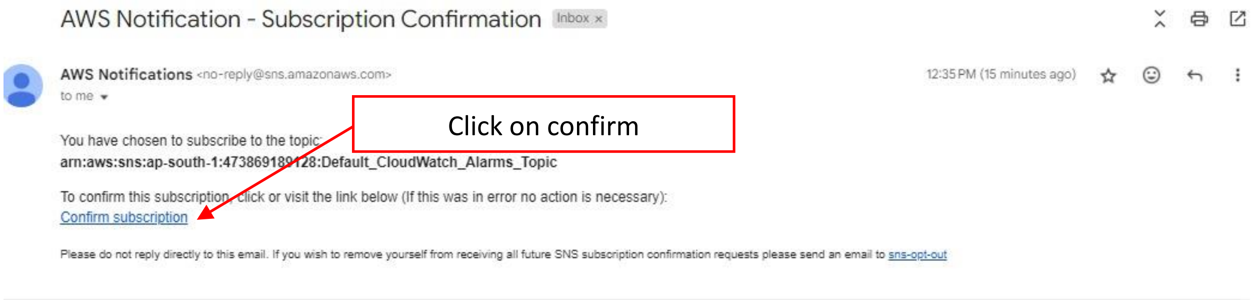
☐	Name	State	Last state update (UTC)	Conditions	Actions
☐	terminate-ec2	✓ OK	2024-06-11 07:16:16	CPUUtilization >= 40 for 1 datapoints within 5 minutes	✓ Actions enabled



Subscriptions (2)

	ID	Endpoint	Status	Protocol	Topic
○	82d76cd9-2193-4dd9-85e5-284c240e0149	cloudinstitution@gmail....	Pending confirmation	EMAIL	Defaul...

Go to the Email



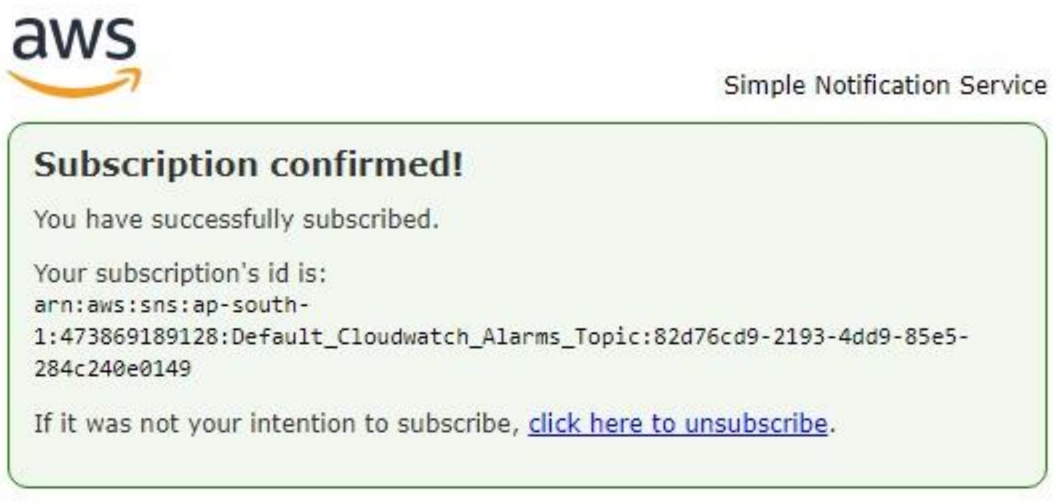
AWS Notification - Subscription Confirmation

AWS Notifications <no-reply@sns.amazonaws.com>

You have chosen to subscribe to the topic:
arn:aws:sns:ap-south-1:473869189128:Default_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out



Simple Notification Service

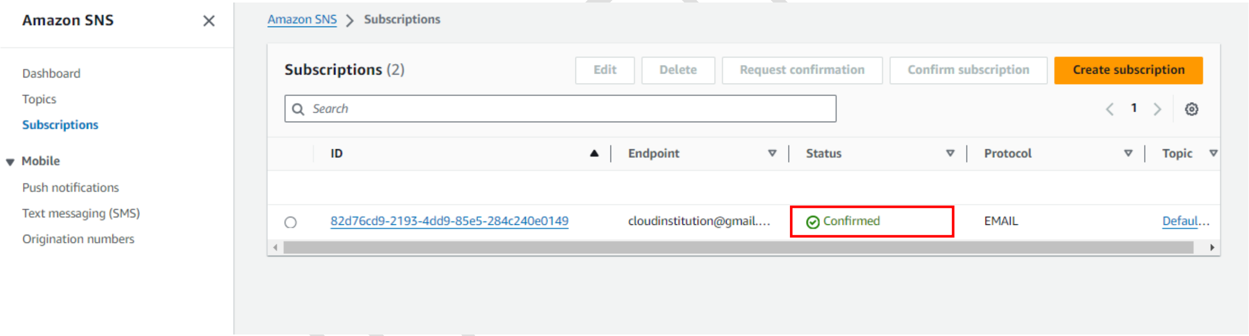
Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
```
arn:aws:sns:ap-south-1:473869189128:Default_Cloudwatch_Alarms_Topic:82d76cd9-2193-4dd9-85e5-284c240e0149
```

If it was not your intention to subscribe, click here to unsubscribe.

Subscription confirmed



Subscriptions (2)

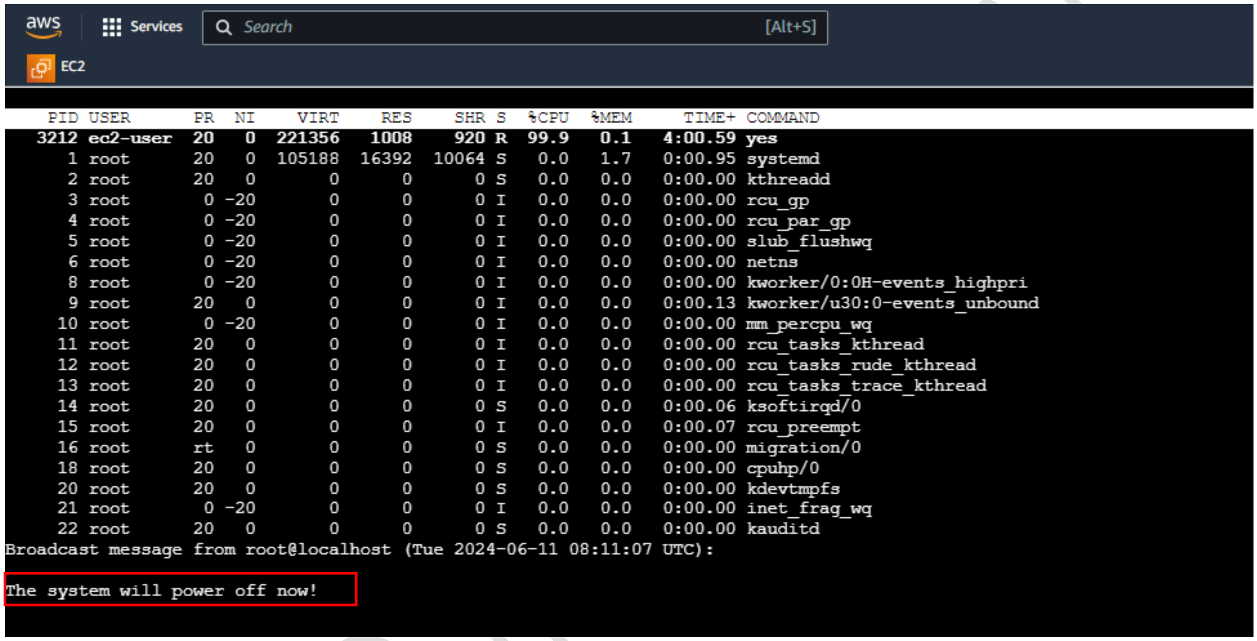
	ID	Endpoint	Status	Protocol	Topic
○	82d76cd9-2193-4dd9-85e5-284c240e0149	cloudinstitution@gmail....	✓ Confirmed	EMAIL	Defaul...

Step 3 : Now go back to the EC2 instance and connect the instance

In the instance terminal, enter the “**yes > /dev/null &”** command in the background on your EC2 instance. This command will generate CPU load, which you can monitor using various tools.

Then enter the command “**top”** and wait for few minutes until the CPU utilization reaches the mentioned threshold.

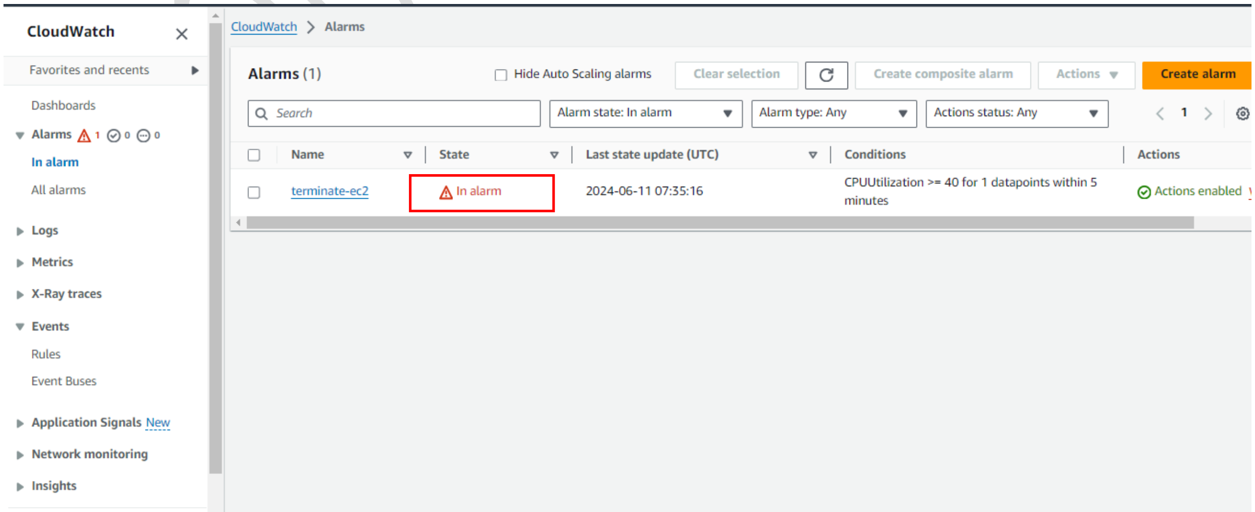
In **top**, you'll see a display of CPU usage, memory usage, and other system information. The processes consuming the most CPU will be listed at the top.



```
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 3212 ec2-user  20   0  221356   1008    920 R  99.9   0.1   4:00.59 yes
    1 root      20   0  105188  16392  10064 S   0.0   1.7   0:00.95 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
    9 root      20   0       0      0      0 I   0.0   0.0   0:00.13 kworker/u30:0-events_unbound
   10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
   11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.06 ksoftirqd/0
   15 root      20   0       0      0      0 I   0.0   0.0   0:00.07 rcu_preempt
   16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
   18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
   21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
   22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
Broadcast message from root@localhost (Tue 2024-06-11 08:11:07 UTC):

The system will power off now!
```

When the CPU Utilization is completed, that time alarm changes its state to **in alarm** and Terminate the EC2 Instance.

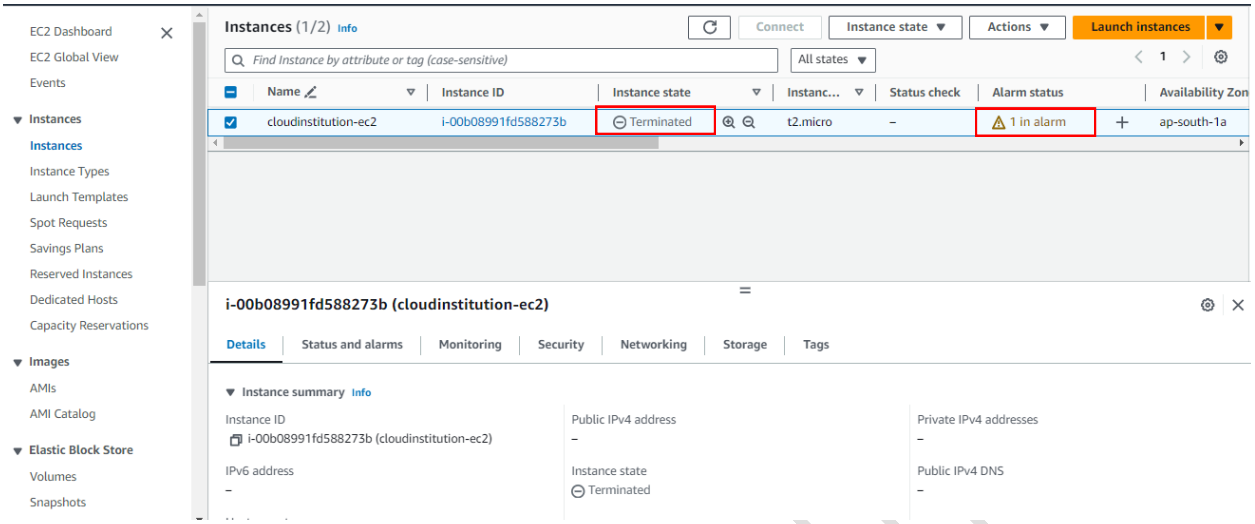


Alarms (1)

Alarm state: In alarm | Alarm type: Any | Actions status: Any

□	Name	State	Last state update (UTC)	Conditions	Actions
□	terminate-ec2	⚠ In alarm	2024-06-11 07:35:16	CPUUtilization >= 40 for 1 datapoints within 5 minutes	✓ Actions enabled

Instance terminated



☑	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability Zon
☑	cloudinstitution-ec2	i-00b08991fd588273b	⊖ Terminated	t2.micro	–	⚠ 1 in alarm	ap-south-1a

i-00b08991fd588273b (cloudinstitution-ec2)

Instance ID
i-00b08991fd588273b (cloudinstitution-ec2)

Public IPv4 address
–

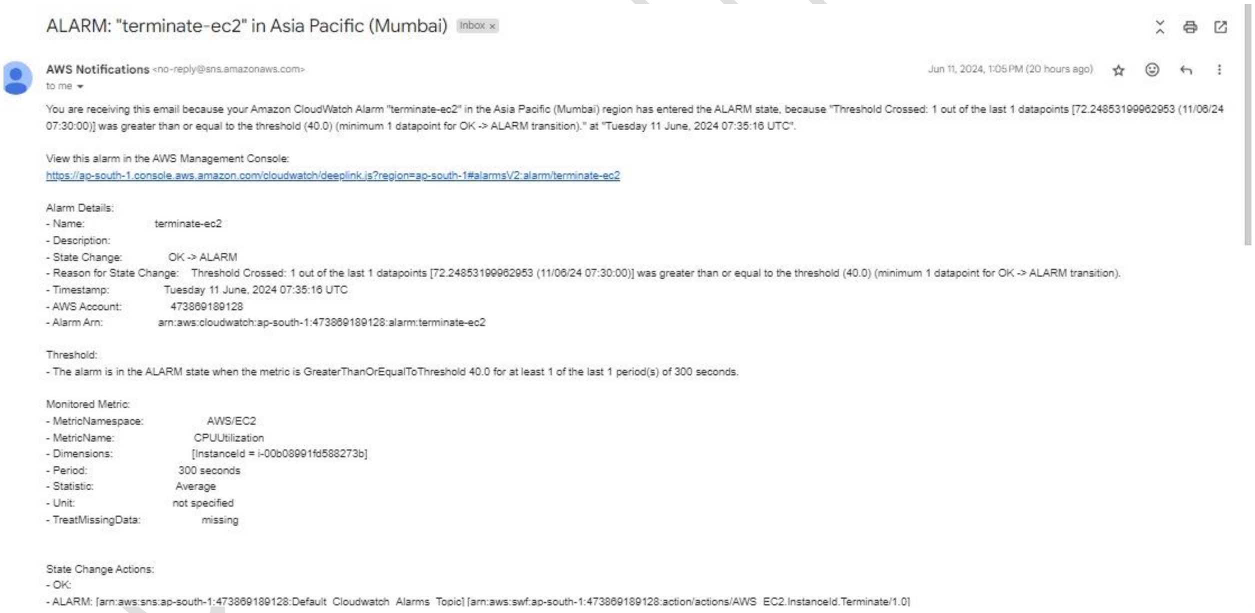
Private IPv4 addresses
–

IPv6 address
–

Instance state
⊖ Terminated

Public IPv4 DNS
–

You will also receive an email confirming that the EC2 is terminated.



ALARM: "terminate-ec2" in Asia Pacific (Mumbai)

AWS Notifications <no-reply@sns.amazonaws.com>
to me

Jun 11, 2024, 1:05 PM (20 hours ago)

You are receiving this email because your Amazon CloudWatch Alarm "terminate-ec2" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [72.24853199962953 (11/06/24 07:30:00)] was greater than or equal to the threshold (40.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 11 June, 2024 07:35:16 UTC".

View this alarm in the AWS Management Console:
https://ap-south-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/terminate-ec2

```
Alarm Details:
- Name:                      terminate-ec2
- Description:
- State Change:              OK -> ALARM
- Reason for State Change:   Threshold Crossed: 1 out of the last 1 datapoints [72.24853199962953 (11/06/24 07:30:00)] was greater than or equal to the threshold (40.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp:                 Tuesday 11 June, 2024 07:35:16 UTC
- AWS Account:               473869189128
- Alarm Arn:                 arn:aws:cloudwatch:ap-south-1:473869189128:alarm:terminate-ec2

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 40.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace:           AWS/EC2
- MetricName:                CPUUtilization
- Dimensions:                [InstanceId = i-00b08991fd588273b]
- Period:                    300 seconds
- Statistic:                 Average
- Unit:                      not specified
- TreatMissingData:          missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:ap-south-1:473869189128:Default_Cloudwatch_Alarms_Topic] [arn:aws:swf:ap-south-1:473869189128:action/actions/AWS_EC2.InstanceId.Terminate/1.0]
```