📌Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

❎Components
📌EC2 Instance - An Amazon EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure.
📌- Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time.

❎In the below hands-on steps, we are going to create an ec2 instance, one cloudwatch alarm and one SNS topic . So here we want to show when the cpu utilization of the server goes beyond 40%, the ec2 instance should be stopped and we should receive an email in the registered email ID.

❎Create an EC2 instance with all default settings except on Network settings.
Follow below to setup network settings:

## Network settings Info

VPC - *required* Info

vpc-0119ae136d2e37942 (Default VPC) (default)
172.31.0.0/16

Subnet Info

No preference — Create new subnet

Auto-assign public IP Info

Enable

**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.

- (selected) Create security group
- Select existing security group

Security group name - *required*

sns-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

sns-sg

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0) — Remove

| Type Info | Protocol Info | Port range Info |
|---|---|---|
| ssh | TCP | 22 |

| Source type Info | Source Info | Description - *optional* Info |
|---|---|---|
| Anywhere | Add CIDR, prefix list or security<br>0.0.0.0/0 × | e.g. SSH for admin desktop |

Security group rule 2 (TCP, 80, 0.0.0.0/0) — Remove

| Type Info | Protocol Info | Port range Info |
|---|---|---|
| HTTP | TCP | 80 |

| Source type Info | Source Info | Description - *optional* Info |
|---|---|---|
| Anywhere | Add CIDR, prefix list or security<br>0.0.0.0/0 × | e.g. SSH for admin desktop |

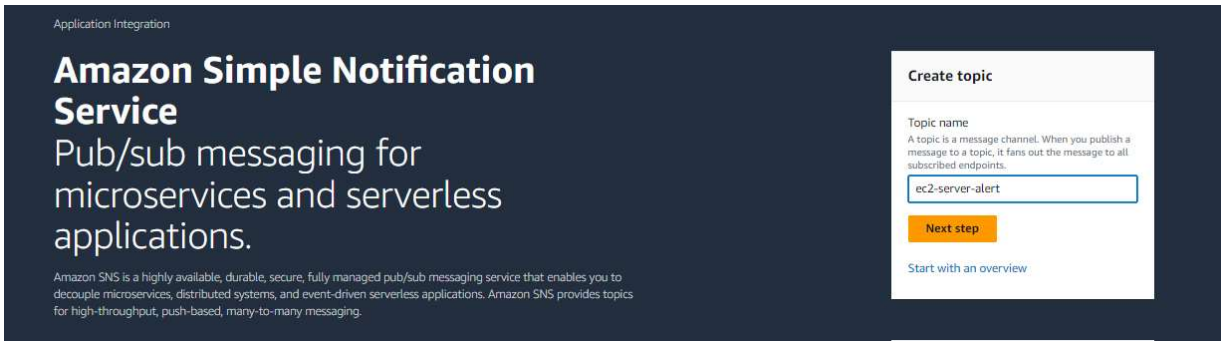
Security group rule 3 (ICMP, All) — Remove

Security group rule 4 (ICMP, All, 0.0.0.0/0) — Remove

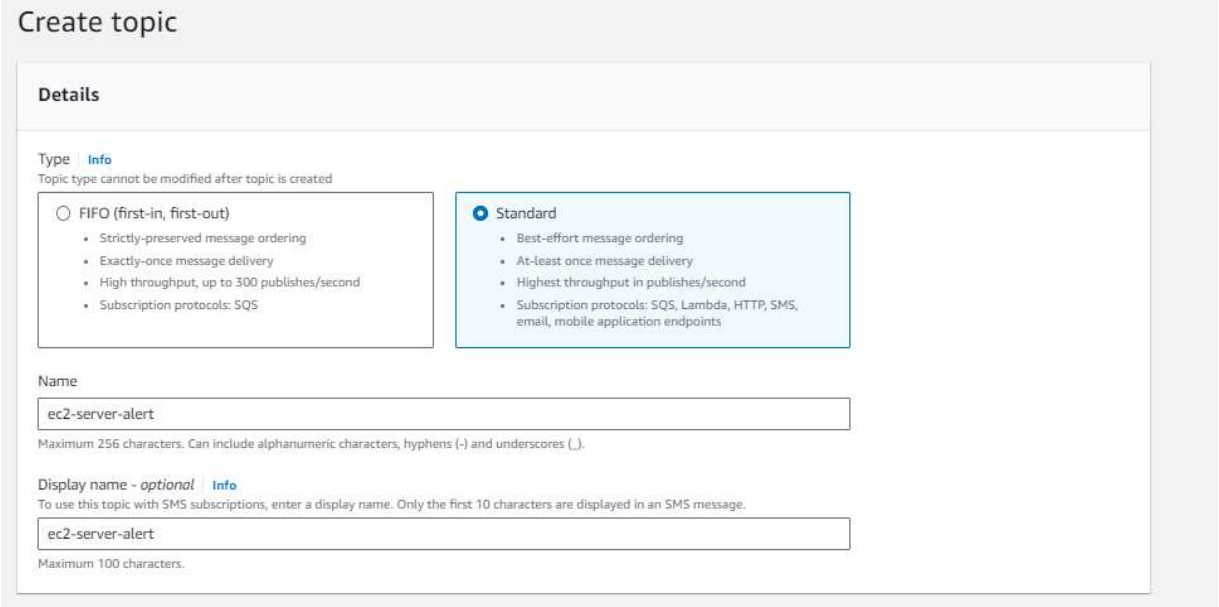
| Type Info | Protocol Info | Port range Info |
|---|---|---|
| All ICMP - IPv4 | ICMP | All |

| Source type Info | Source Info | Description - *optional* Info |
|---|---|---|
| Anywhere | Add CIDR, prefix list or security<br>0.0.0.0/0 × | e.g. SSH for admin desktop |

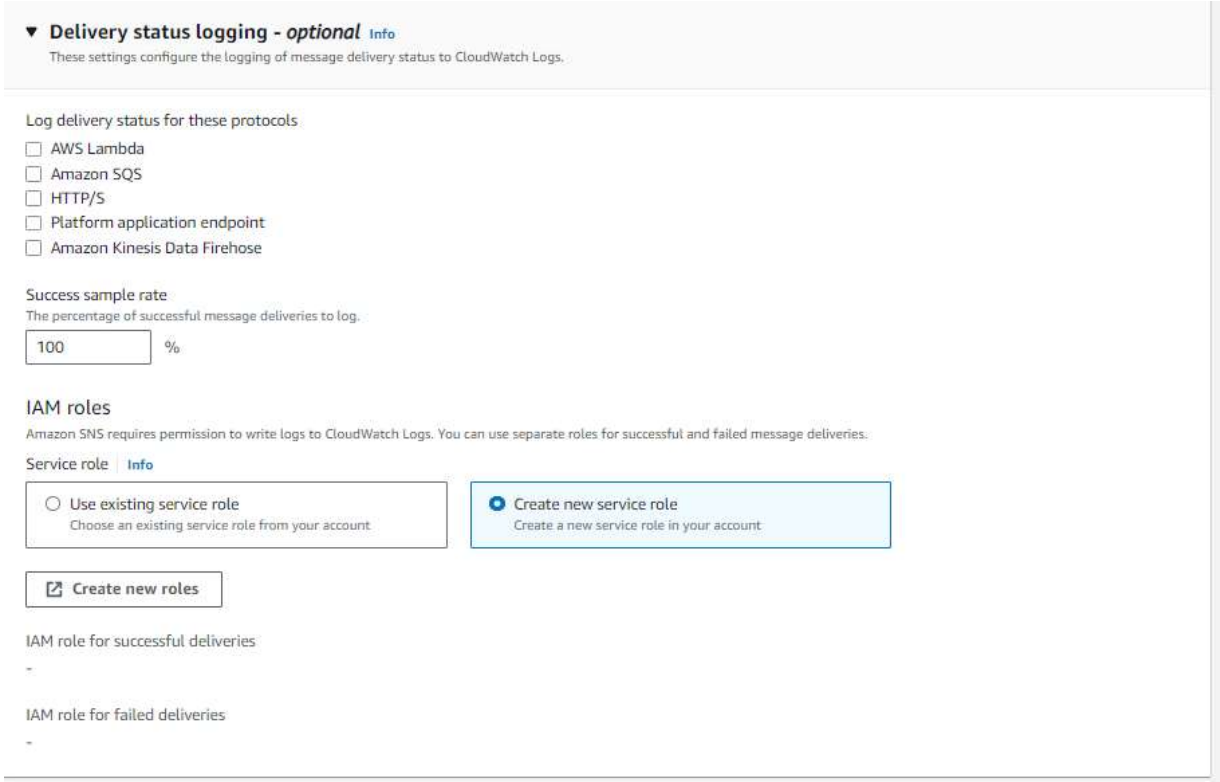
❎ Now we are going to create SNS.Search for Amazon Simple Notification Service  and give a topic to the text area as below:



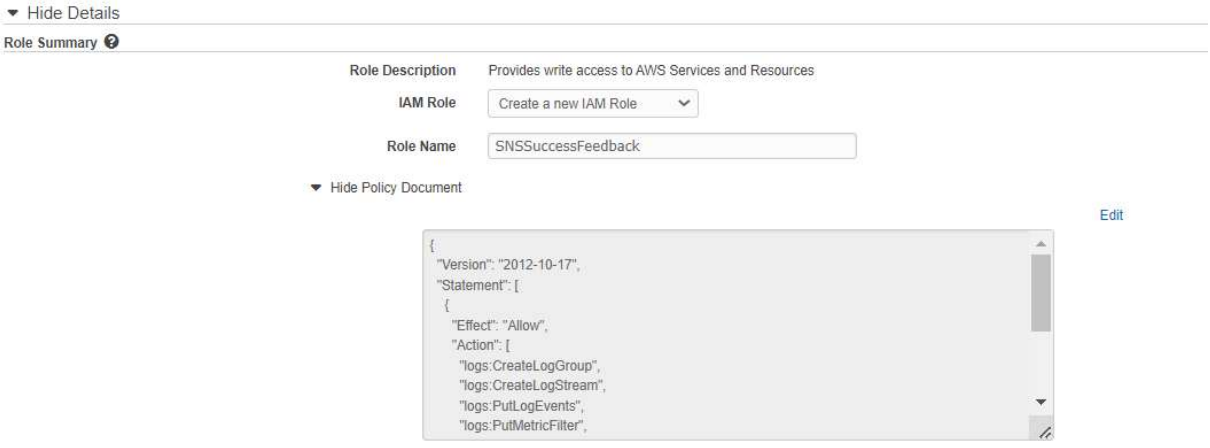

❎ Under Details , we're selecting standard type as FIFO is strictly for message delivering.

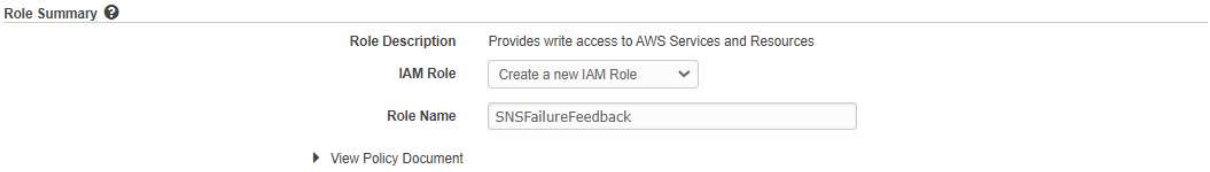



❎ Delivery status logging - click on Create new service role and create new role. We will get a new tab for the IAM console.

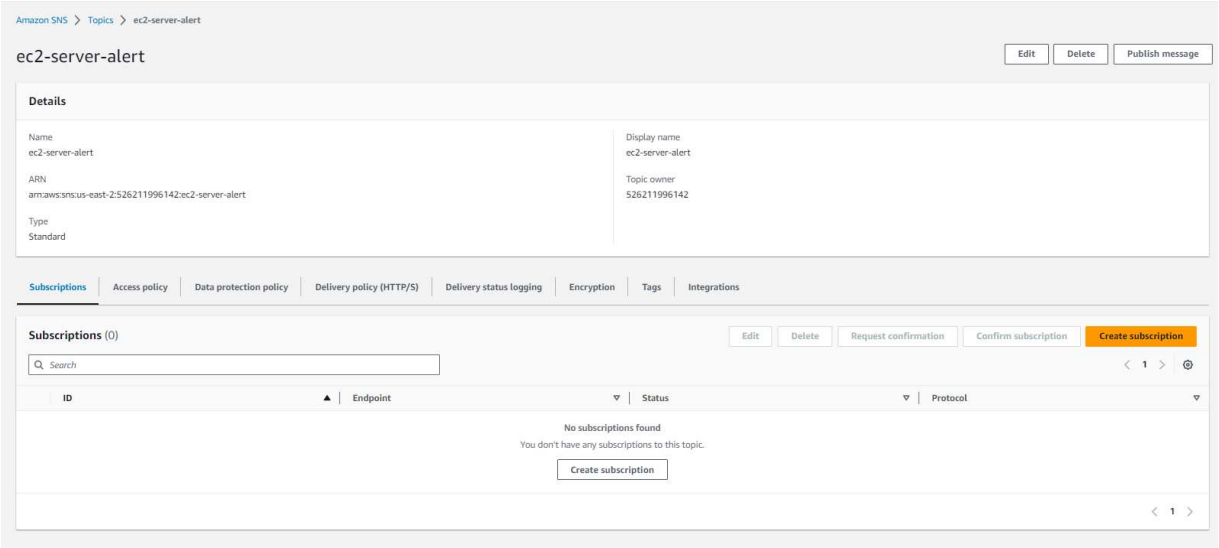



❎ IAM Management Console - we're going with the default settings and click on allow.

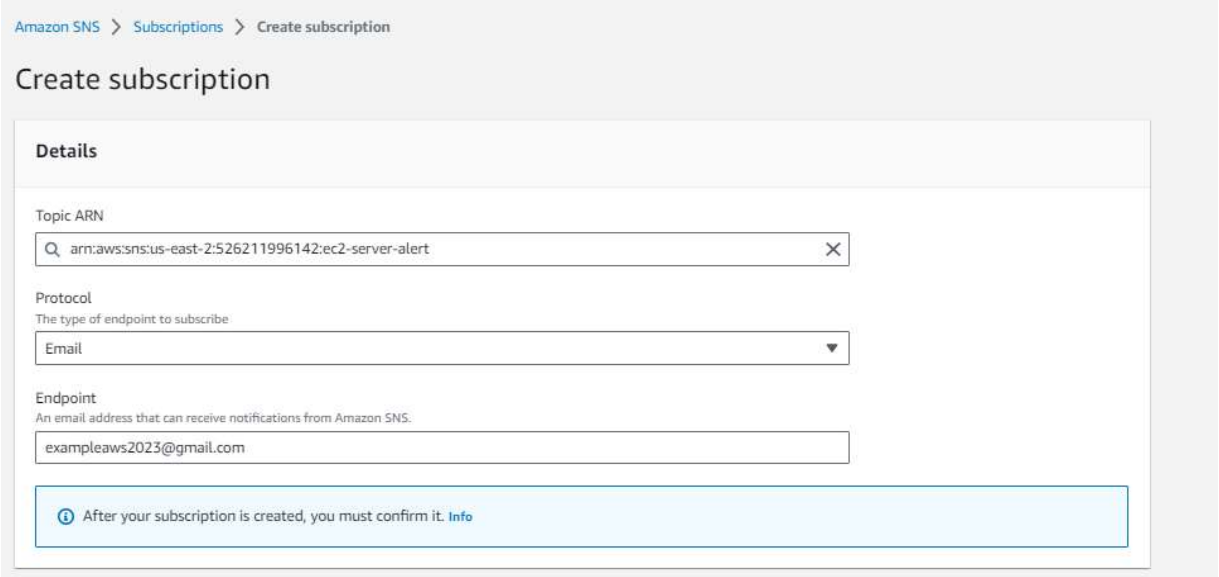



❎ All the other settings are set be default in SNS.Click on create subscription

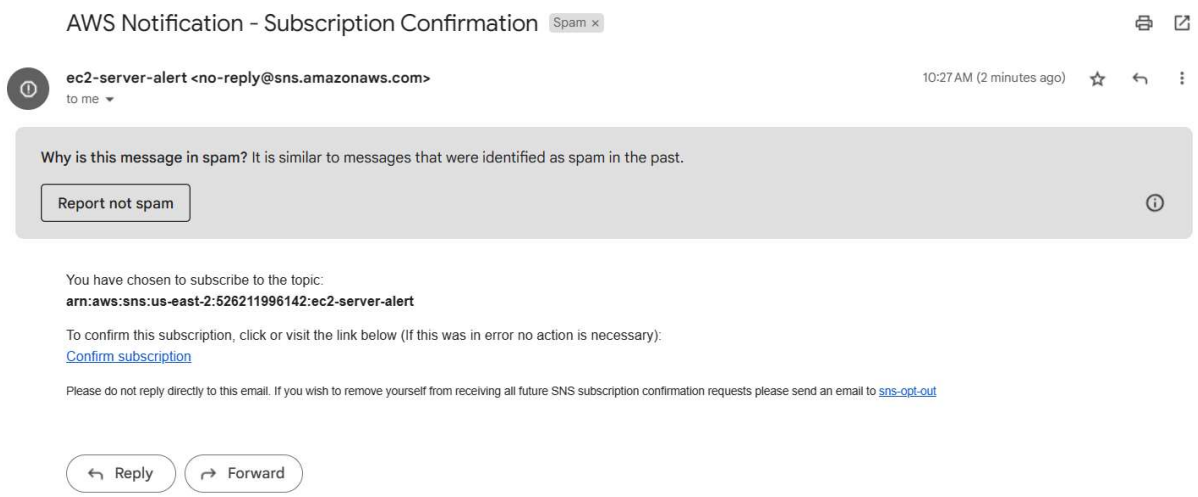



✅ Now we need to enter the email ID which we need to receive notifications.

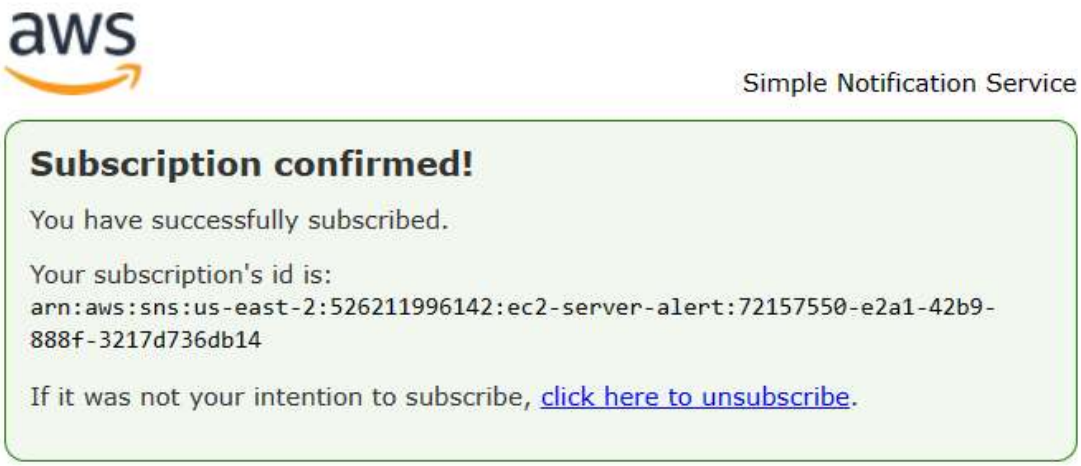



✅ other settings are default and click on create subscription.

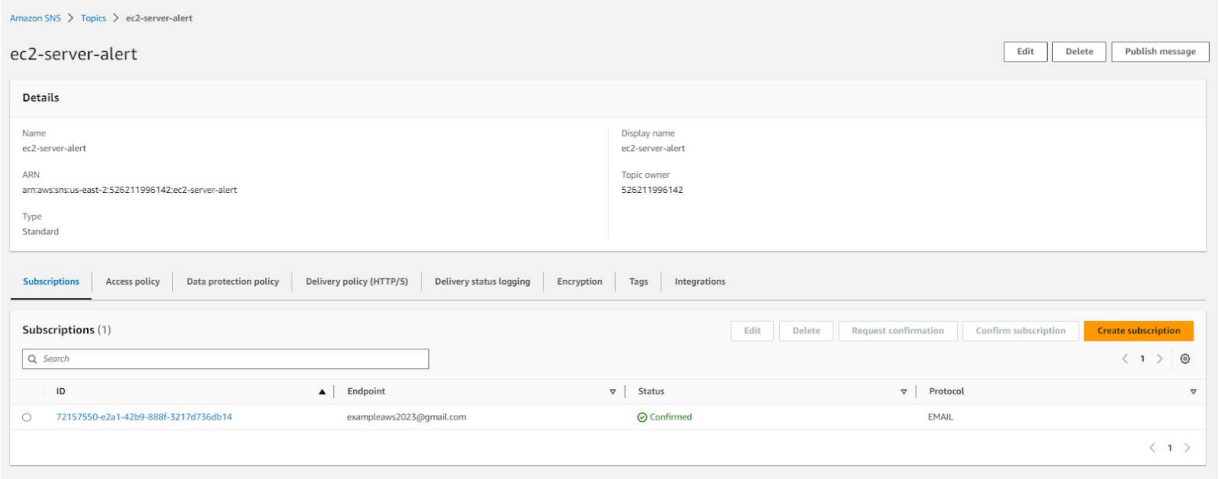
✅ We will receive an email to the above specified ID for the confirmation on subscription. (Please check spam folder also if did not received in Inbox)




✅ Click on confirm subscription

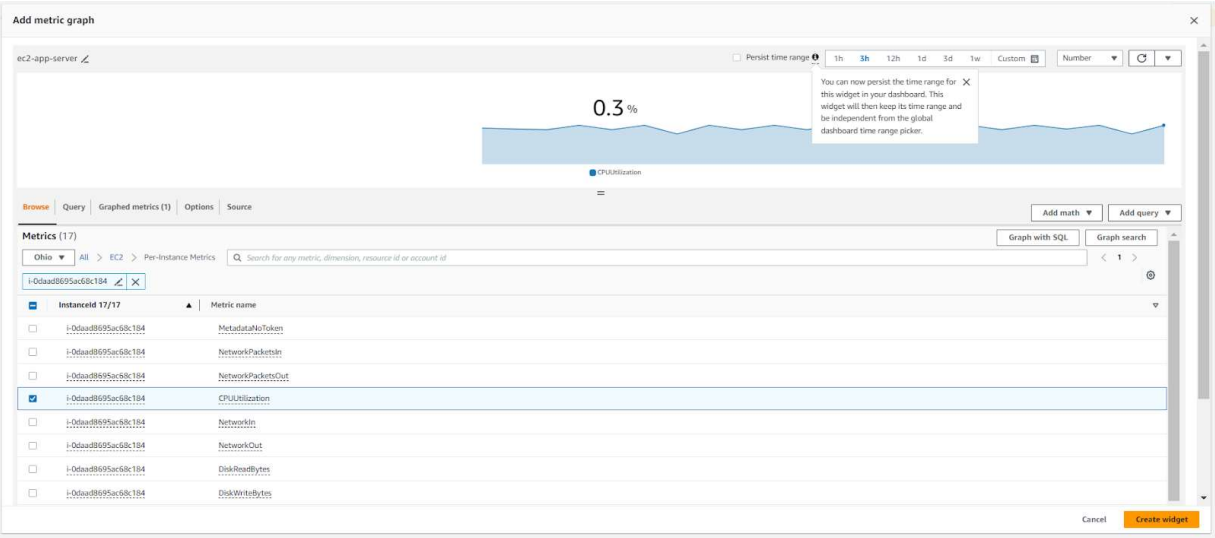



✅ We could see the email ID is confirmed from SNS page

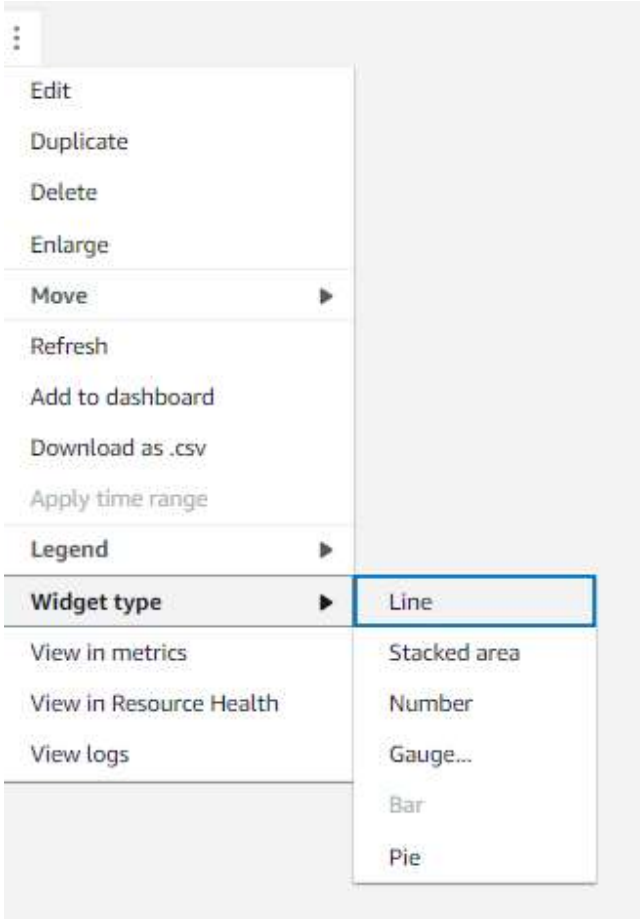


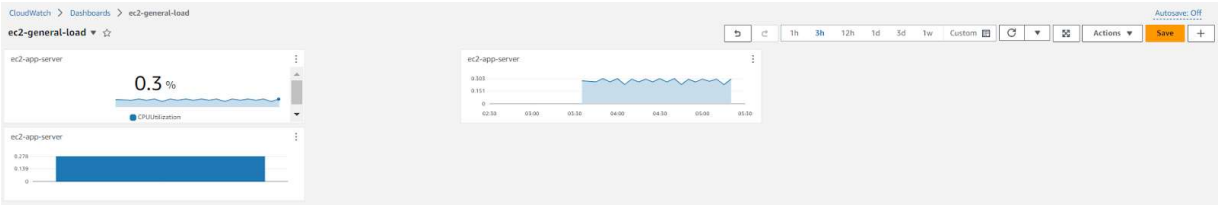
❎ we are going to create CloudWatch

❎ Goto Dashboards → Create Dashboard → give a name → Add Widget → select Number → Click on Next. Then give a graph name ( here : ec2-app-server) then select EC2 → Click on Per-Instance metrics .
❎ Now give instance ID from the ec2 instance we have created and select the metric name as per your wish. Here we're selecting CPU Utilization.

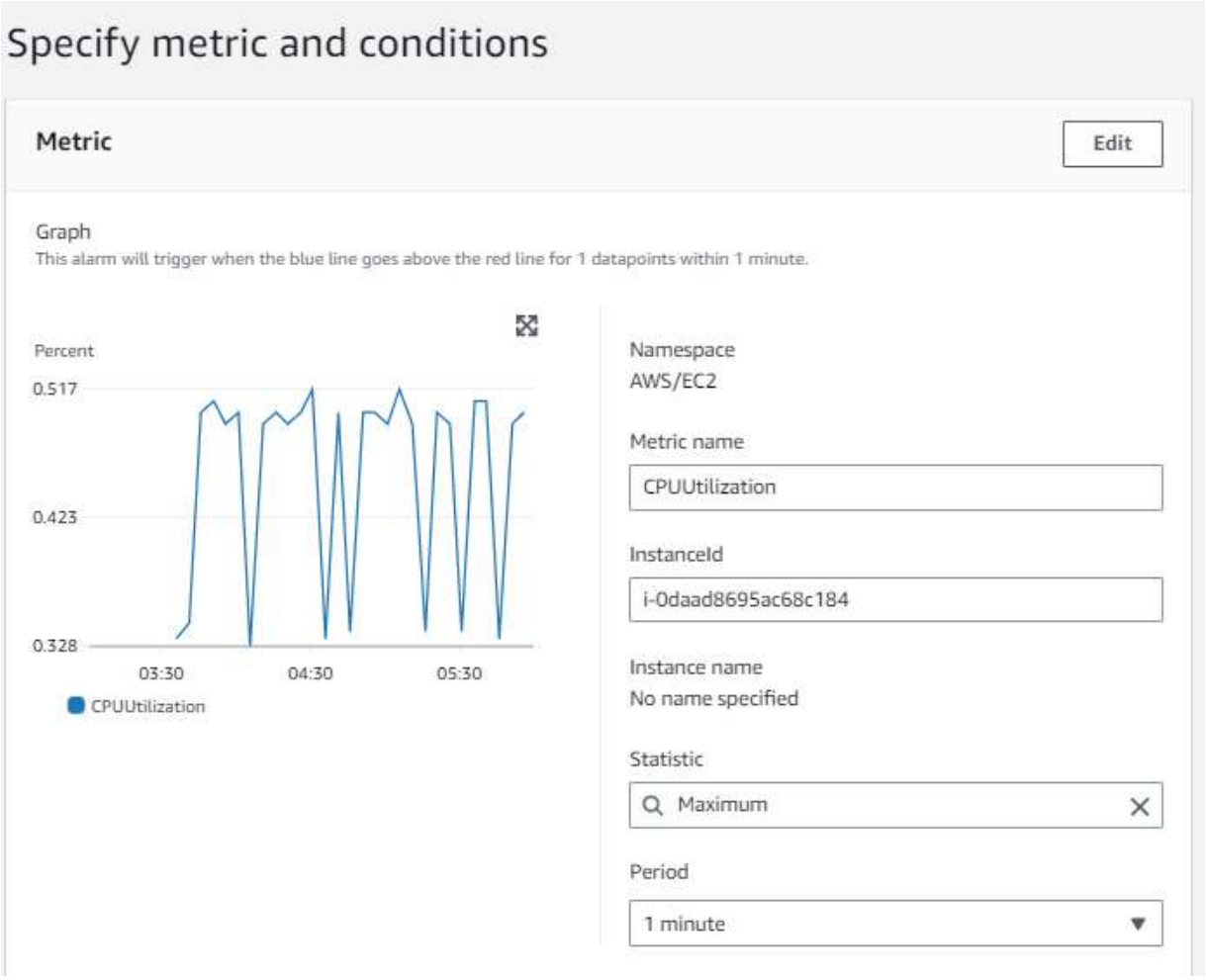



❎ Click on Create Widget.We can also create multiple widgets by clicking Duplicate and change widget type to desired type.

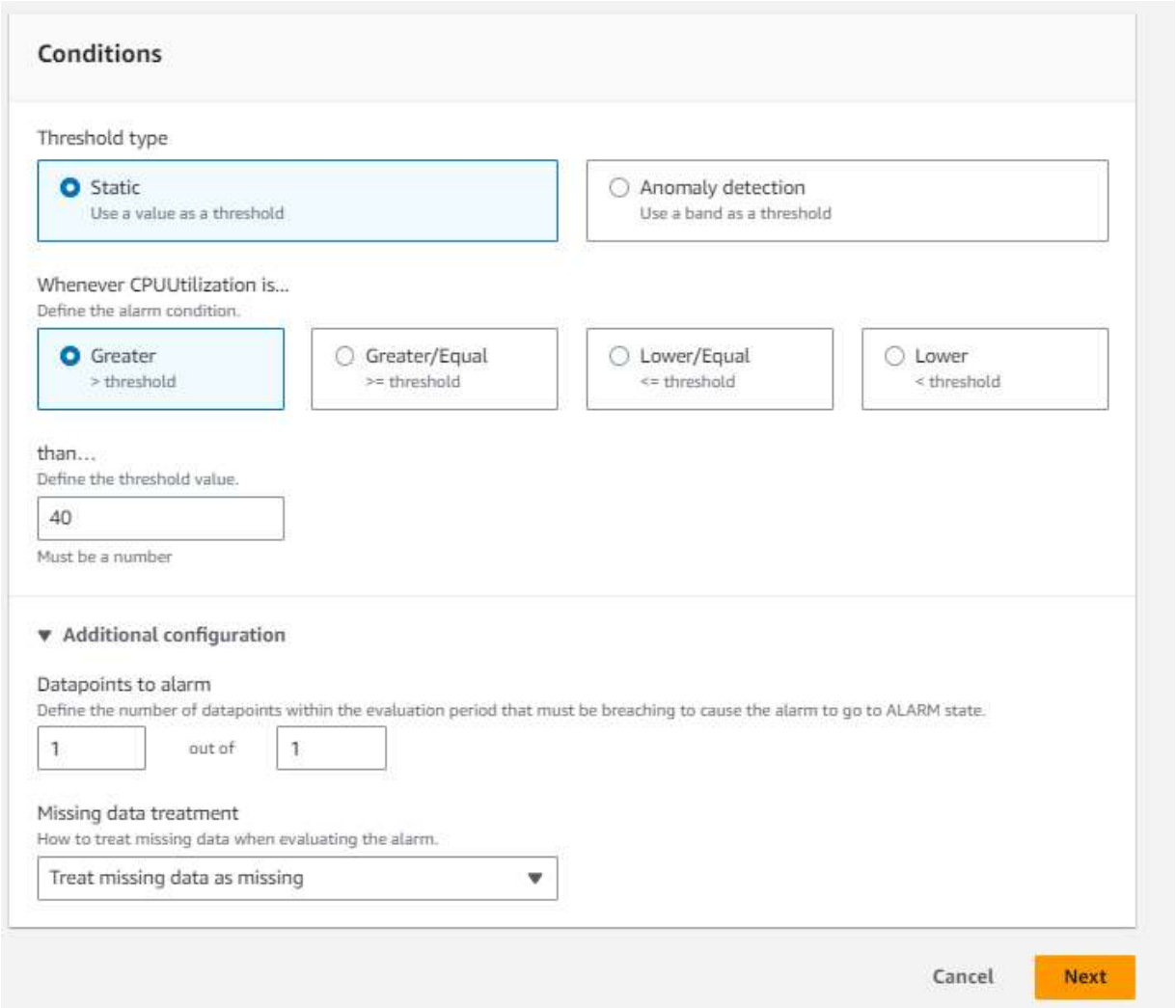


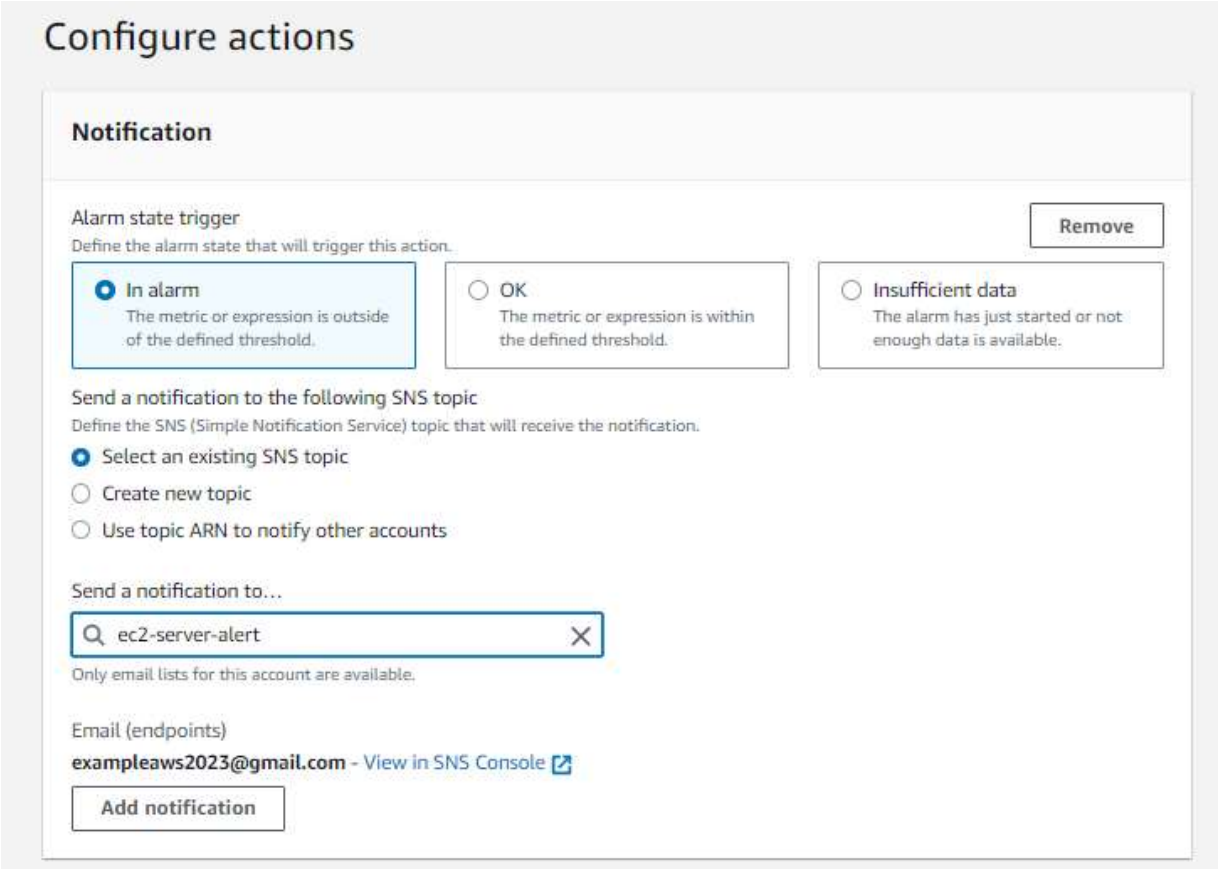

❎ Go to Alarms → In alarm → Create Alarm → Select Metric → click on EC2 → Per-Instance Metrics → select CPU Utilization → click on Select Metric



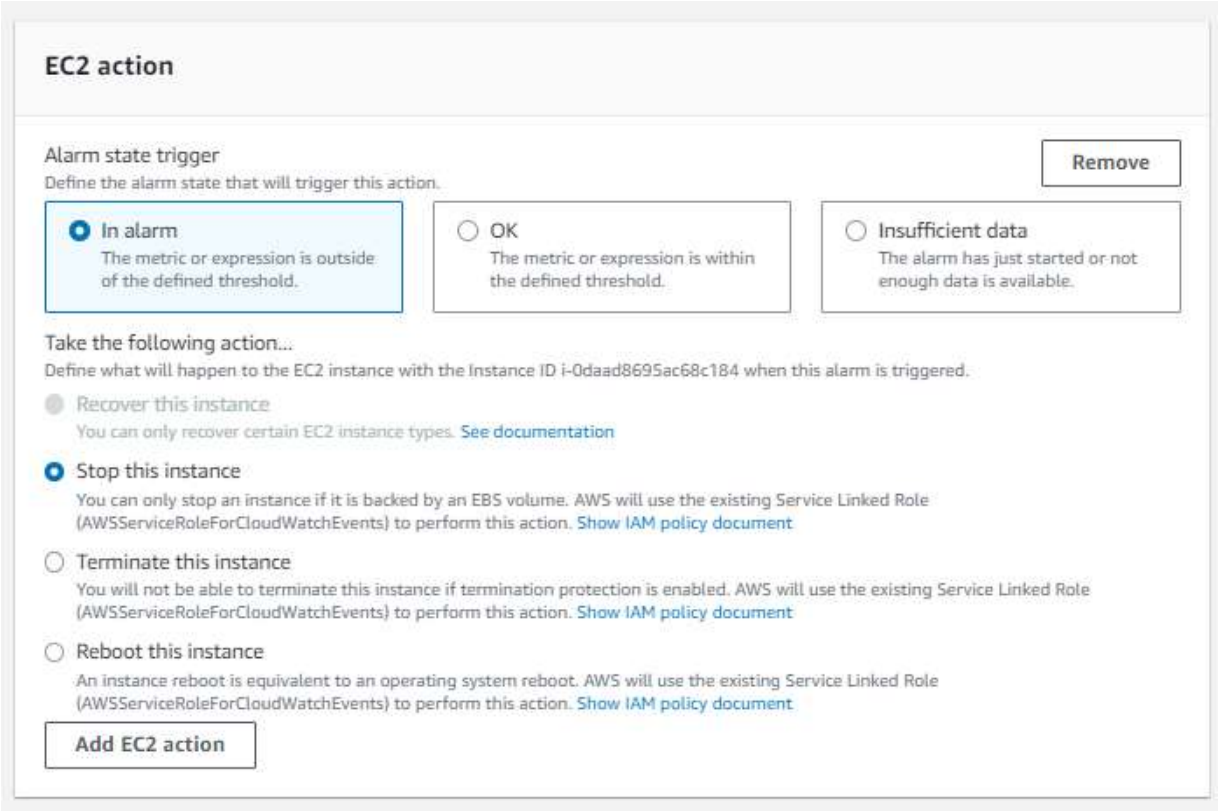

❎Now we're going to give the condition that if utilization goes greater than 40% then we need to get notified.



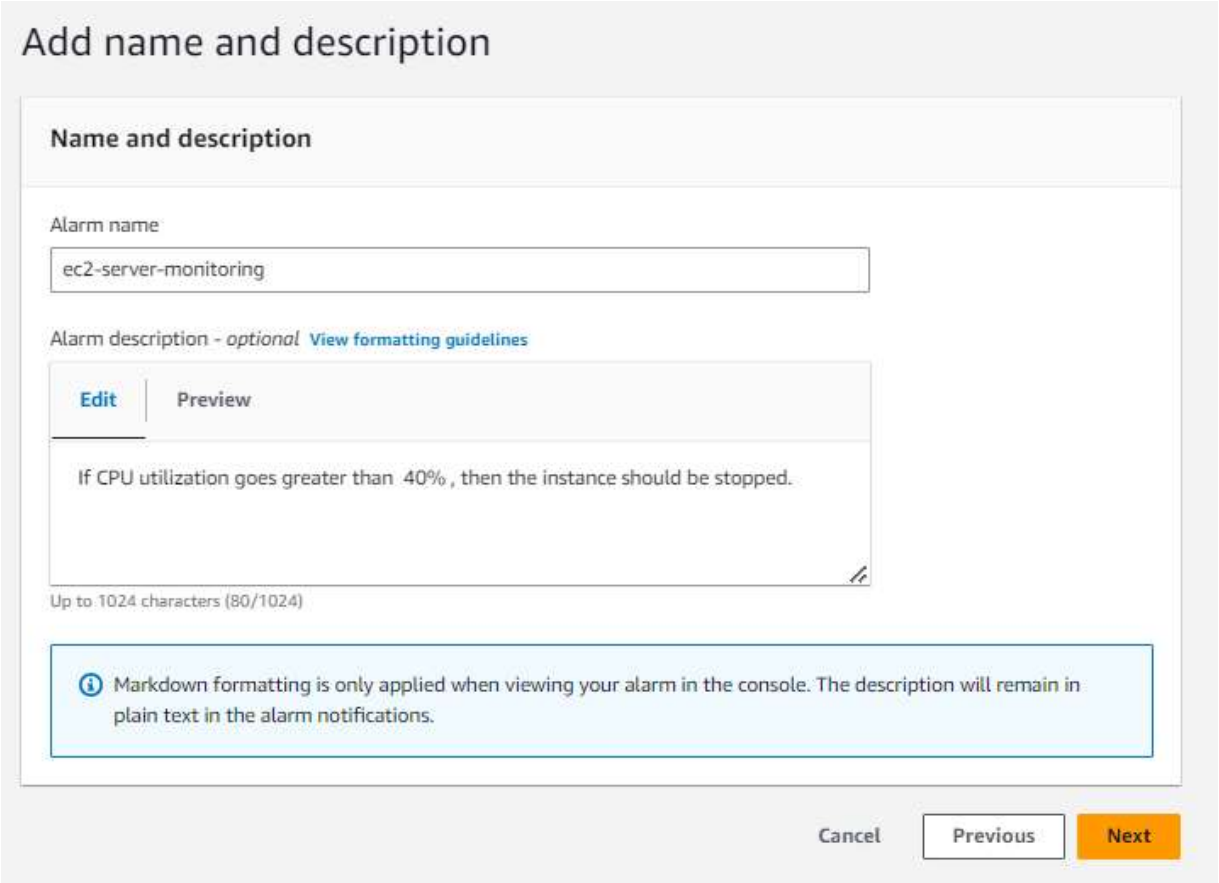

❎ Then click on Next.Select the Dashboard name which we have created




❎ specify what action needs to be taken if utilization goes beyond 40%. Here we're selecting to stop instances.




❎ Give an alarm name and description and click next → Create Alarm

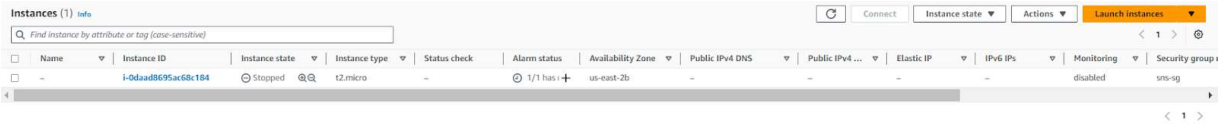



☒ to the server ssh connection (here I'm using MobaXterm) using public IP of the instance
Give the below commands to make the cpu utilization is high.

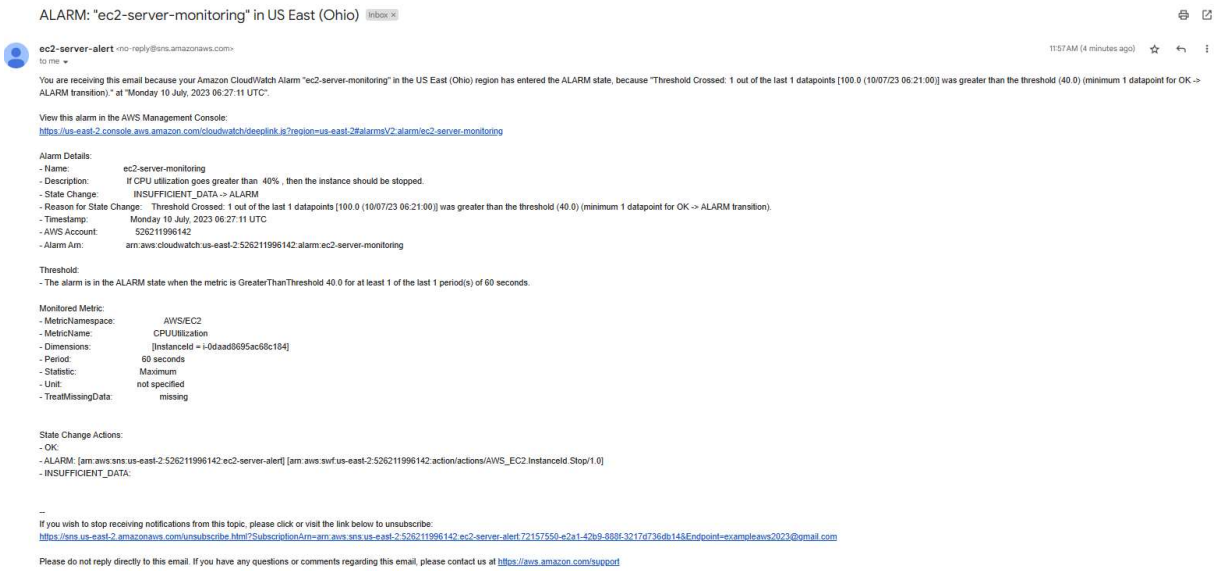
- ☐ yum install https://dl.fedoraproject.org/pub/epel/7Server/x86_64/Packages/e/epel-release-7-14.noarch.rpm -y --skip-broken
- ☐ yum install stress -y
- ☐ stress --cpu 80 ——-----> we are giving cpu load 80

☒ Give the 'top' command in the duplicate session and see the cpu load is getting high.


✅ the instance got automatically stopped as it reach beyond 40%.




✅ Also we will receive an email that cpu utilization threshold crossed.



ALARM: "ec2-server-monitoring" in US East (Ohio) Inbox ×

**ec2-server-alert** <no-reply@sns.amazonaws.com> 11:57 AM (4 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "ec2-server-monitoring" in the US East (Ohio) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [100.0 (10/07/23 06:21:00)] was greater than the threshold (40.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Monday 10 July, 2023 06:27:11 UTC".

View this alarm in the AWS Management Console:
https://us-east-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-2#alarmsV2:alarm/ec2-server-monitoring

Alarm Details:
- Name: ec2-server-monitoring
- Description: If CPU utilization goes greater than 40% , then the instance should be stopped.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [100.0 (10/07/23 06:21:00)] was greater than the threshold (40.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Monday 10 July, 2023 06:27:11 UTC
- AWS Account: 526211996142
- Alarm Arn: arn:aws:cloudwatch:us-east-2:526211996142:alarm:ec2-server-monitoring

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 40.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-0daad8695ac68c184]
- Period: 60 seconds
- Statistic: Maximum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-2:526211996142:ec2-server-alert] [arn:aws:swf:us-east-2:526211996142:action/actions/AWS_EC2.InstanceId.Stop/1.0]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-2:526211996142:ec2-server-alert:72157550-e2a1-42b9-888f-3217d736db14&Endpoint=exampleaws2023@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support