AWS Monitoring using Cloud watch

Overview

1.Creating custom dashboard

2.Setting up cloud Alarm

3.Configure cloudwatch log

Create a Custom Dashboard

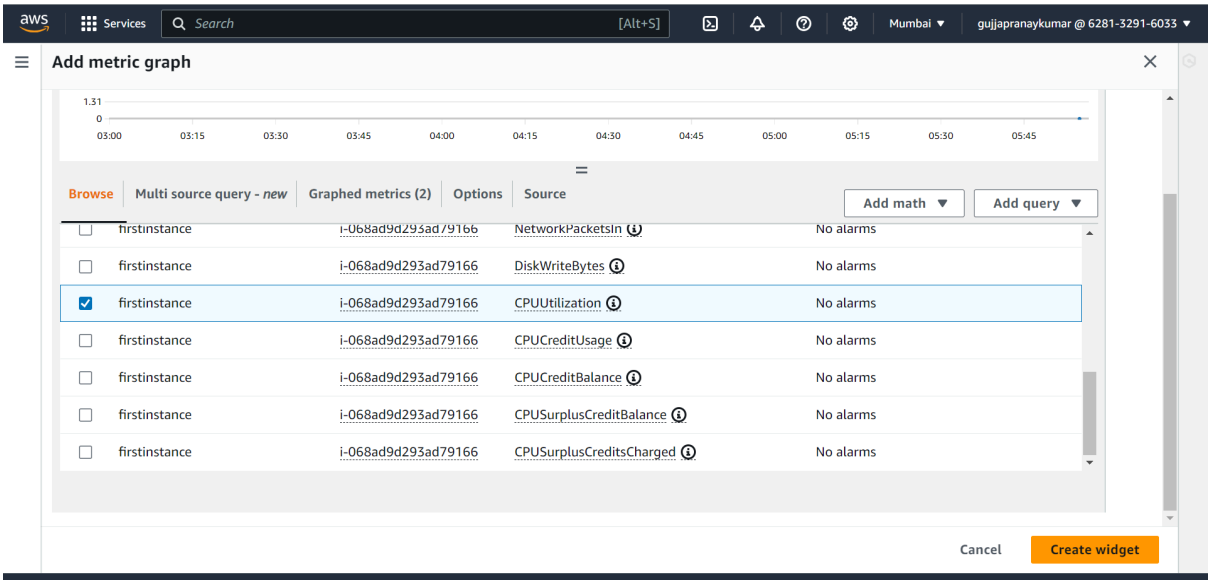
1.Navigate to cloudwatch service

2.Click Dashboard -> Create Dashboard

3.Provide the name and proceed next and select any type of widget ex:Line

4.Select the data source as Metrics and then select EC2 in the Metrics
A:
5.Now select Per-Instance metrics

6.Select any one of your nginx server and metric name as CPUUtilization
A:

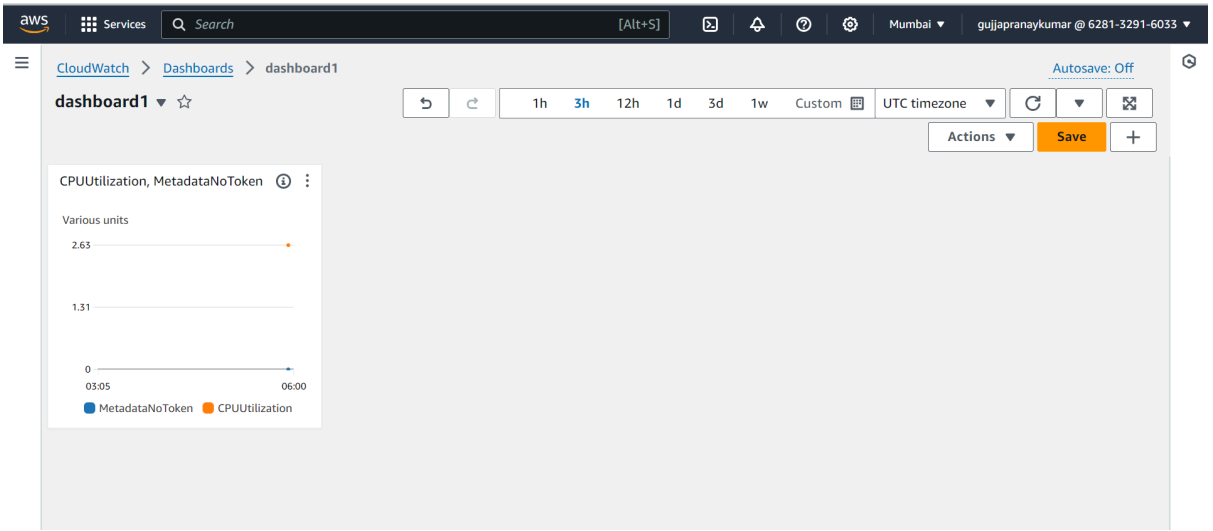


7.Click on create widget

8.Your dashboard should now be created

9.You can analyze your instance CPUUtilization using the graph

A:



Set a Cloud Alarm for CPUUtilization

1.Navigate to Alarm dashboard -> create alarm

2.Select Metric

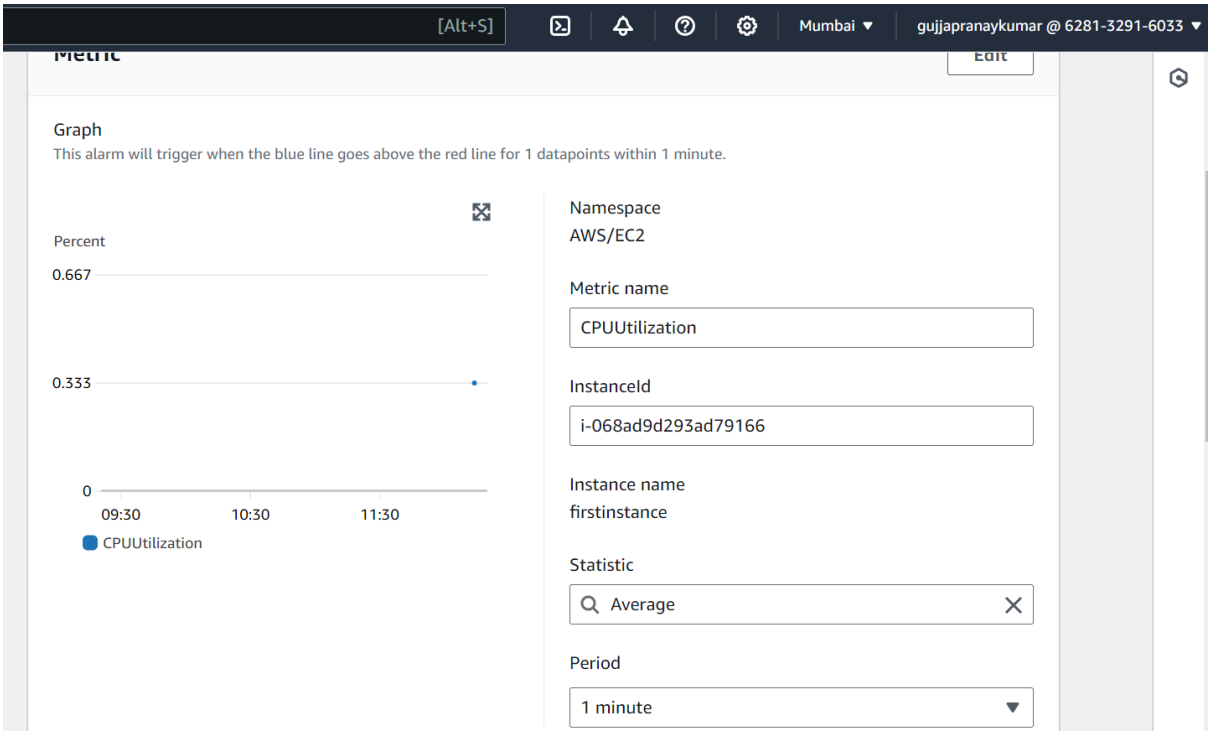
3.Select the data source as Metrics and then select EC2 in the Metrics

4.Now select Per-Instance metrics

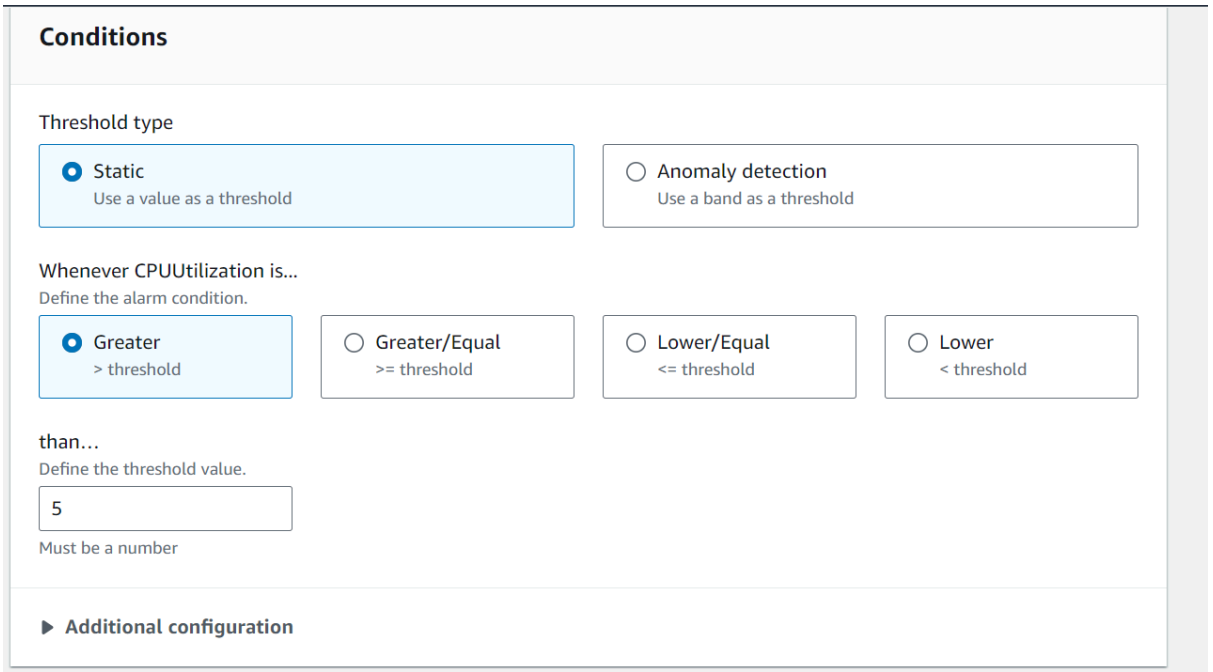
5.Select any one of your nginx server and metric name as CPUUtilization

6.In the period you can provide the minutes , say if 1 minute

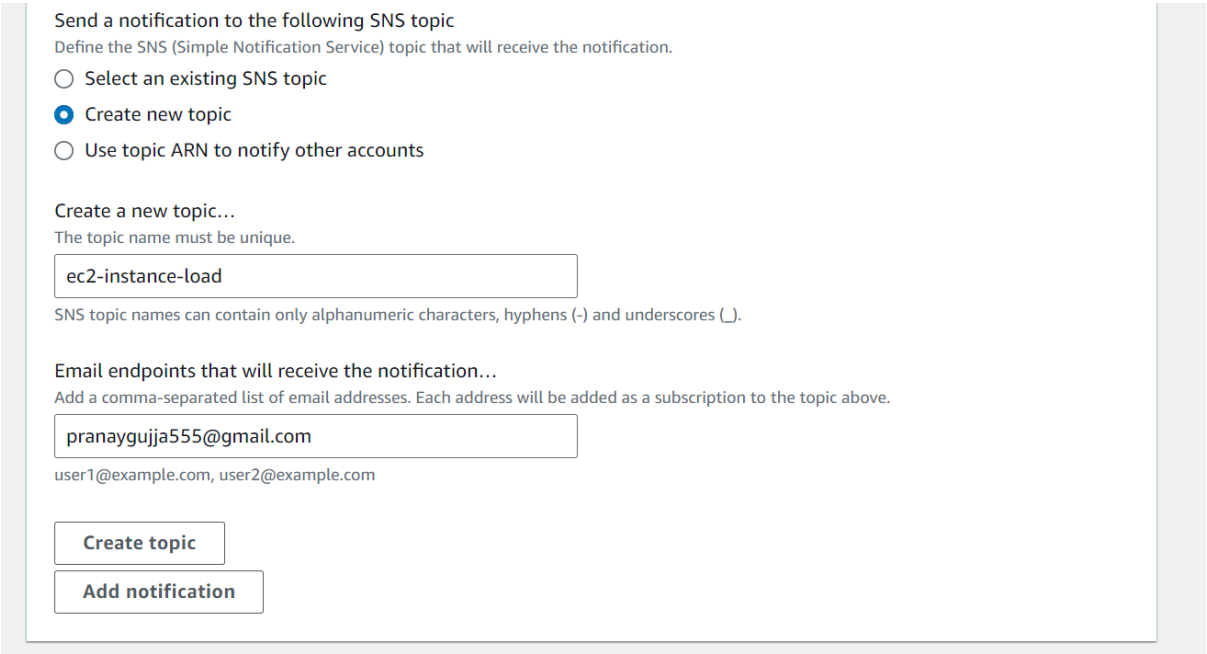
A:



7.Provide CPU utilization condition say if it is 5%, Click ‘Next’
A:

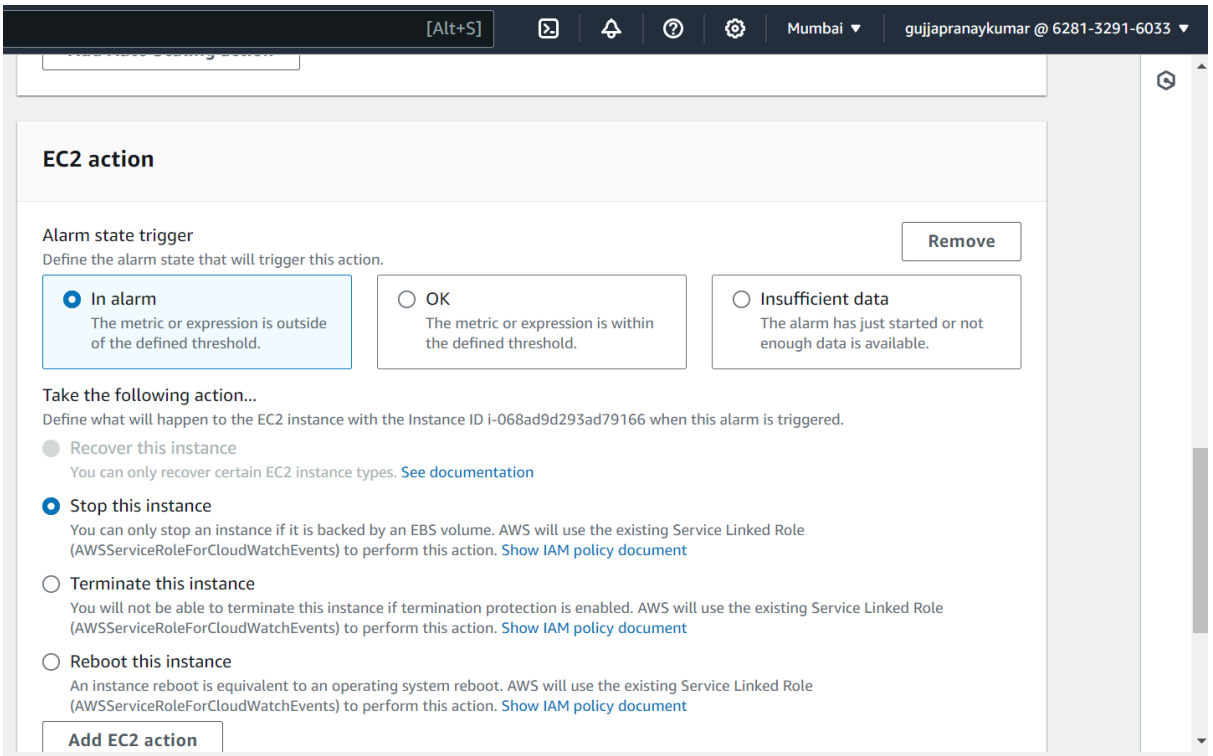


8.For sending email notification you can click create new topic by providing your email address
A:



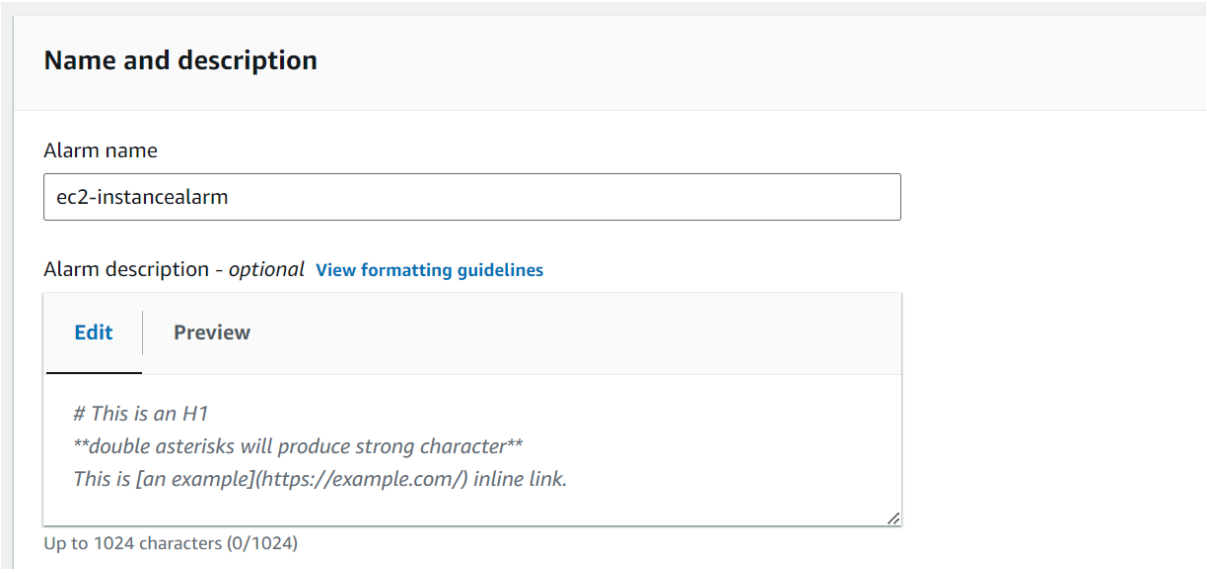
9.You can choose any EC2 action if your CPU utilization goes beyond 5 % you can select Stop this instance and click “Next”

A:



10. Provide the Alarm name / description click ‘Next’ , preview the settings and click click ‘create alarm’

A:



11. Now you can see the alarm created

12. You can run the load test using jmeter to cross the Threshold your Instance will be stopped automatically and a mail will be triggered as below

A:

ALARM: "ec2-instancealarm" in Asia Pacific (Mumbai) Inbox ×

AWS Notifications 10:43 PM (1 minute ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "ec2-instancealarm" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [6.380445185391014 (16/02/24 17:07:00)] was greater than the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 16 February, 2024 17:13:37 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/ec2-instancealarm

Alarm Details:
- Name: ec2-instancealarm
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [6.380445185391014 (16/02/24 17:07:00)] was greater than the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 16 February, 2024 17:13:37 UTC
- AWS Account: 628132916033
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:628132916033:alarm:ec2-instancealarm

Create IAM roles and policies for cloud watch logs

1.Navigate to IAM dashboard

2.Click on policies -> create policy
A:

Policy details

Policy name
Enter a meaningful name to identify this policy.
cloudwatchiampolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
a policy for cloud watch
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

3.Navigate to JSON tab

4.Modify the json as below

```
{

"Version": "2012-10-17",

"Statement": [

{
```

"Effect": "Allow",

"Action": [

"logs:CreateLogGroup",

"logs:CreateLogStream",

"logs:PutLogEvents",

"logs:DescribeLogStreams"

],

"Resource": [

"*"

]

}

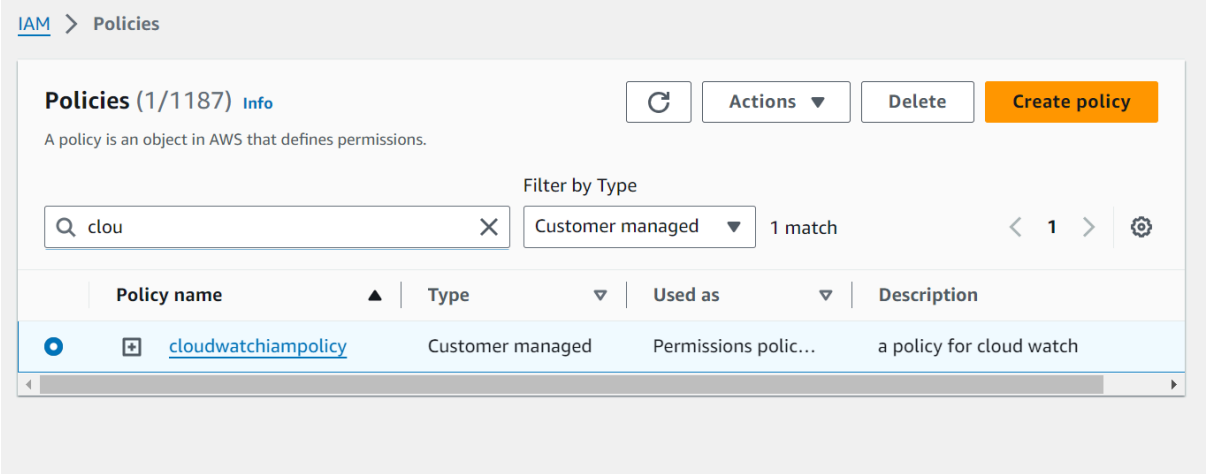
]

}

5.Click on Add tags, you can provide the tags and click on review

6.Provide the name and the description

7Review once and click on create policy, your policy will be created
A:

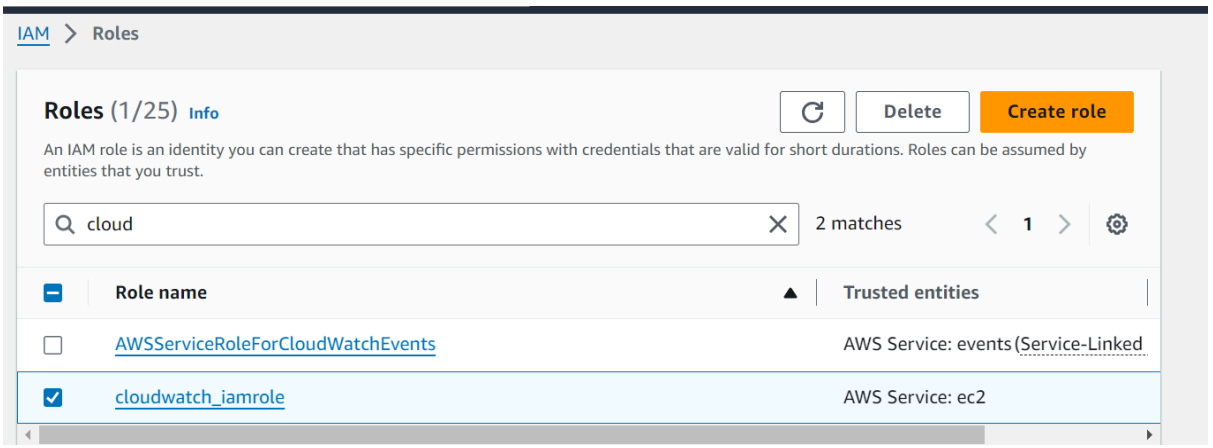


8.Navigate to IAM roles tab -> click create role

9.Select service as ec2 and click on Next

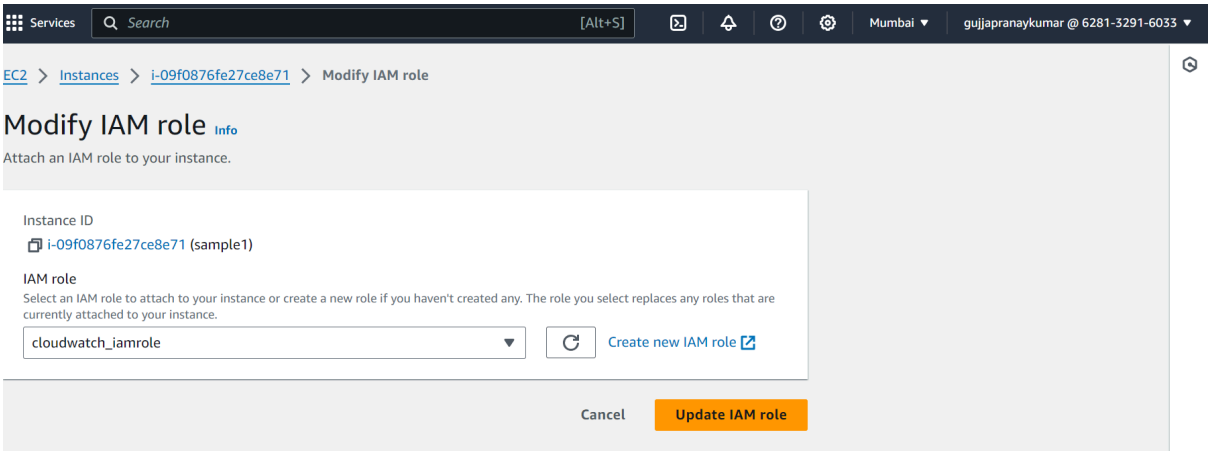
10. Select the policy that you have created and then click Next

11. Provide the role name, review once and then create role your role should be created
A:



12. You need to attach this Role to the ec2 instance (nginx server which you configured in cloudwatch)

13. Select the instance -> Actions -> security -> Modify IAM rule, you need to select the IAM role and update the IAM role
A:



Configure the cloudwatch logs

1.Navigate to your ec2 instance (nginx server which you configured in cloudwatch)

2.Run sudo yum install awslogs -y

3.Now open the awscli.conf using sudo vi /etc/awslogs/awscli.conf and add modify your region

4.Open awslogs.conf file using sudo vi /etc/awslogs/awslogs.conf

A:

```
[plugins]
cwlogs = cwlogs
[default]
region = ap-south-1
```

5.Modify the lines as below

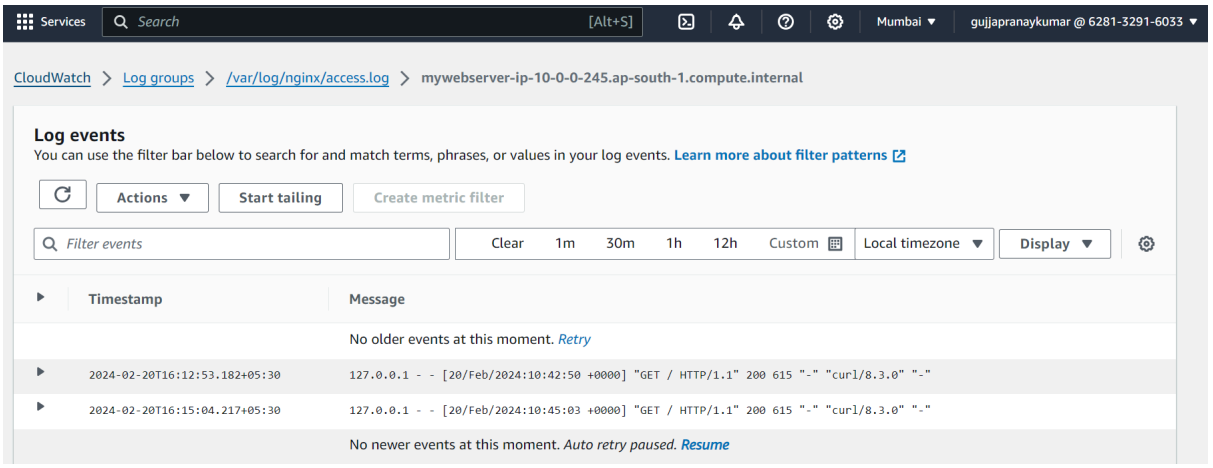
6.Now start your aws logs service using the following command sudo systemctl start awslogsd

A:

```
[/var/log/nginx/error.log]
datetime_format = %b %d %H:%M:%S
file = /var/log/nginx/error.log
buffer_duration = 5000
log_stream_name = mywebserver-{instance_id}
initial_position = start_of_file
log_group_name = /var/log/nginx/error.log
```

7.Now navigate to your cloudwatch console and navigate to the log group and you will see the logs attached as below

A:



_____END_____