Karthik Pradeep Hegadi

2KE20CS032

Assignment 51

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

AWS

==========

Assignment: 1 : AWS Monitoring using Cloud watch

==========

Overview

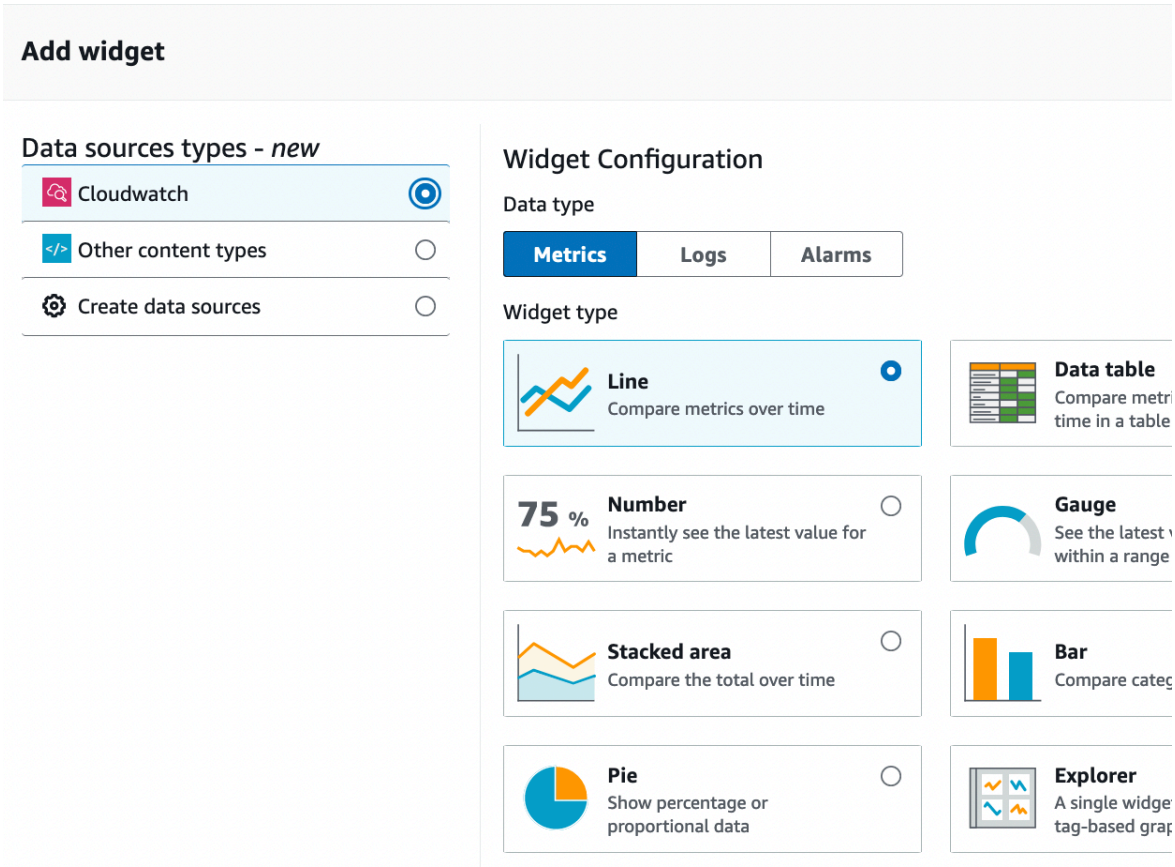
1.Creating custom dashboard

2. Setting up cloud Alarm

3.Configure cloudwatch log

Create a Custom Dashboard

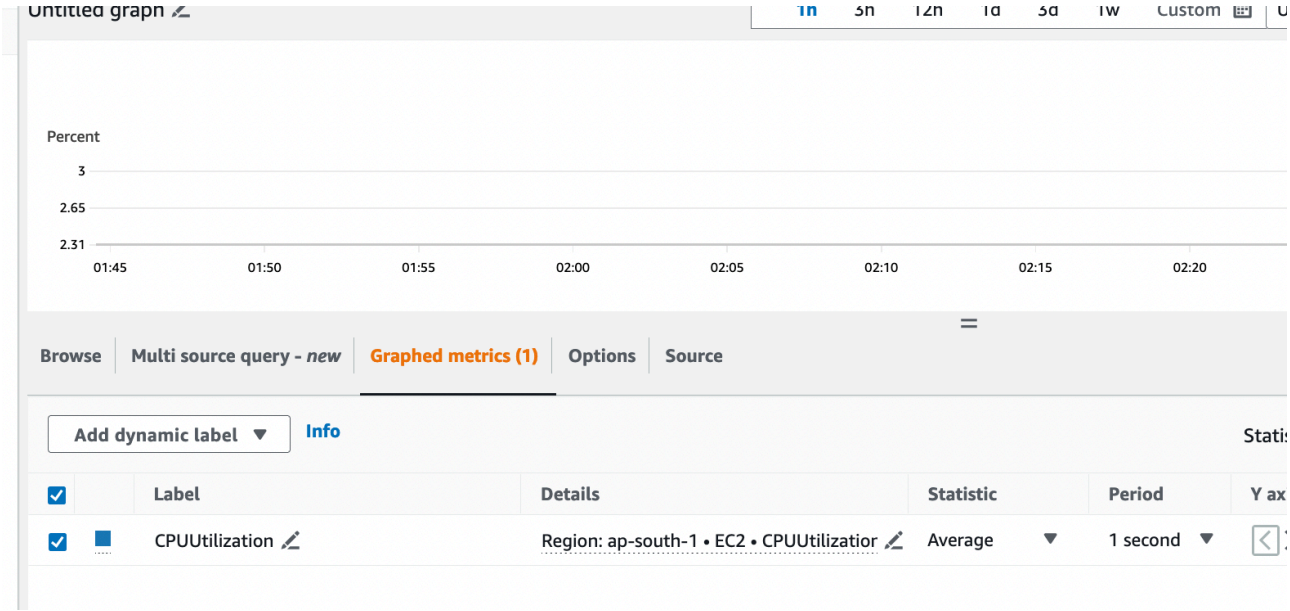
1. Navigate to cloudwatch service



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
5. Now select Per-Instance metrics

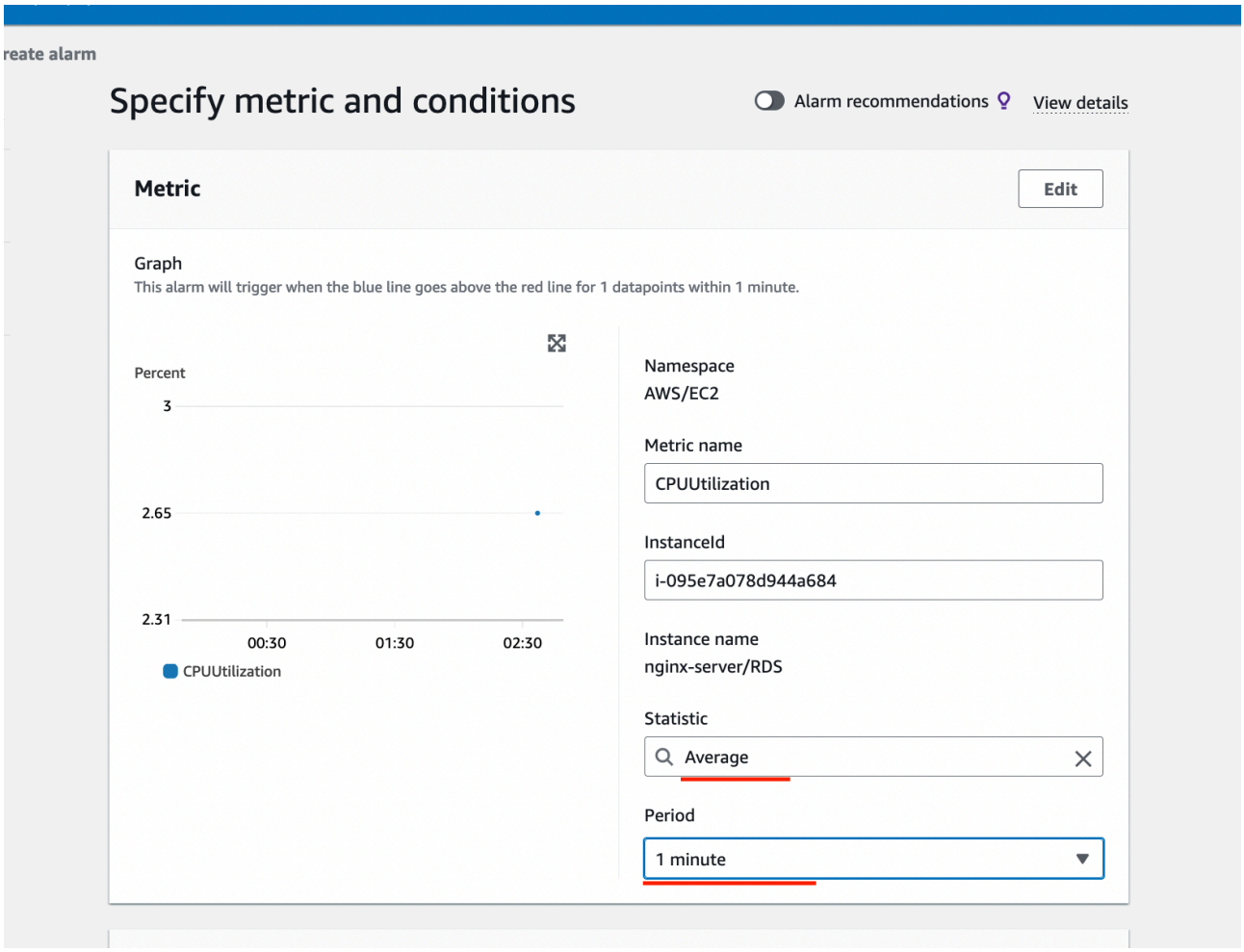
6.Select any one of your nginx server and metric name as CPUUtilization

7. Click on create widget
8. Your dashboard should now be created
9. You can analyze your instance CPUUtilization using the graph



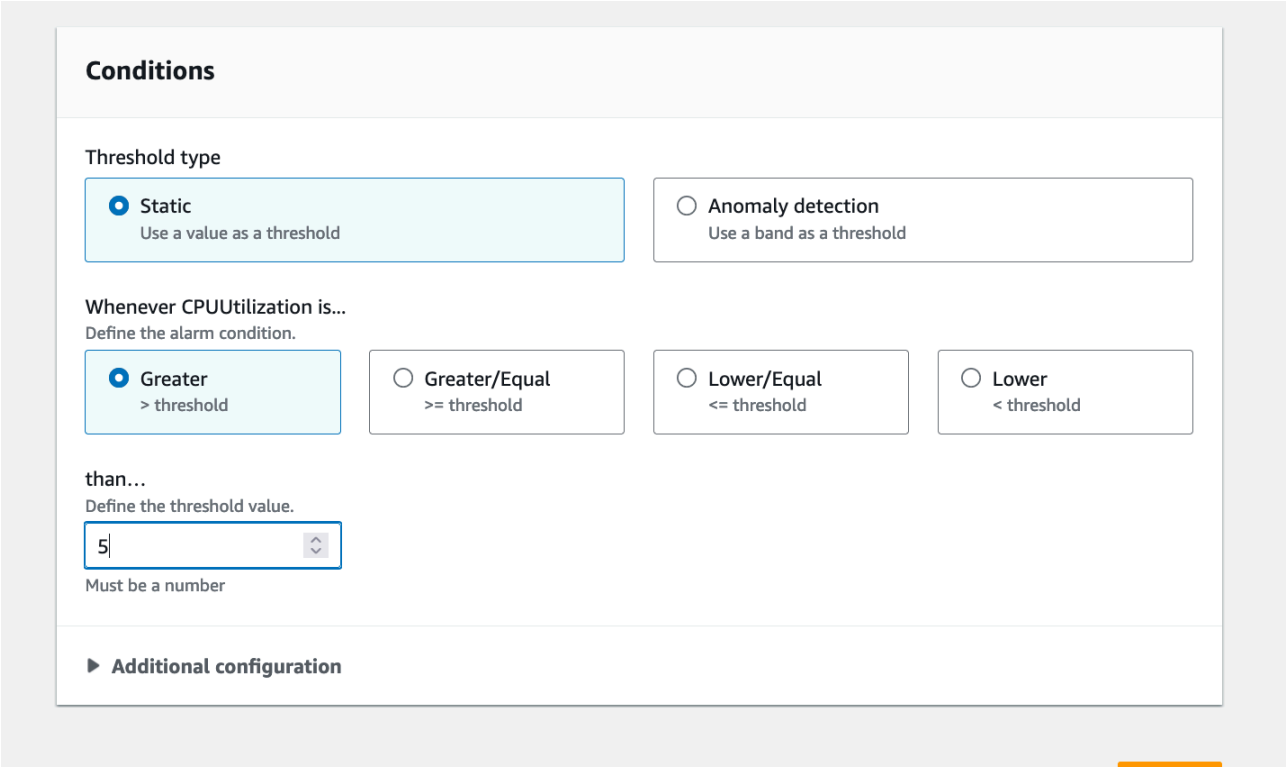
Set a Cloud Alarm for CPUUtilization

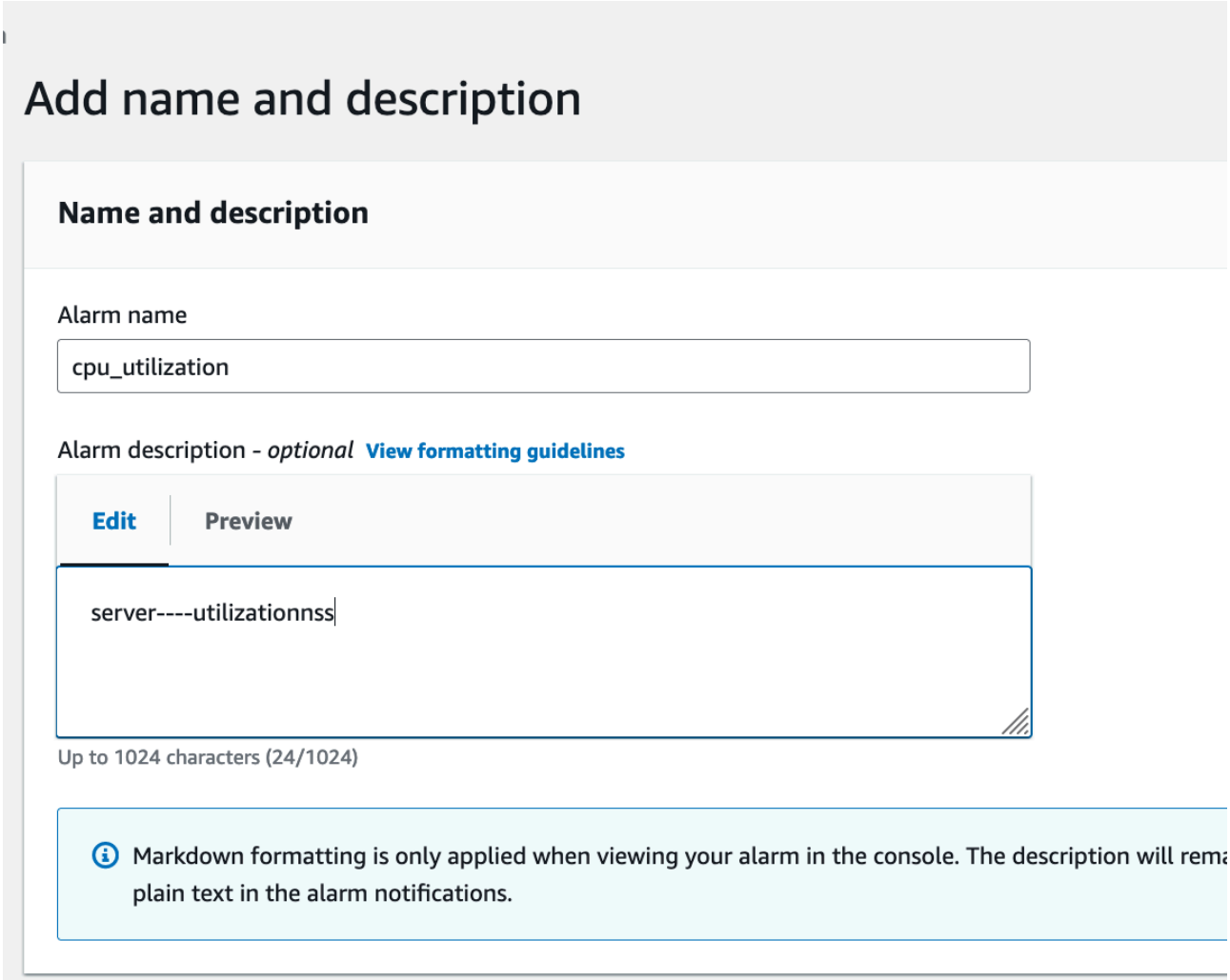
1. Navigate to Alarm dashboard -> create alarm
2. Select Metric
3. Select the data source as Metrics and then select EC2 in the Metrics
4. Now select Per-Instance metrics
5. Select any one of your nginx server and metric name as CPUUtilization

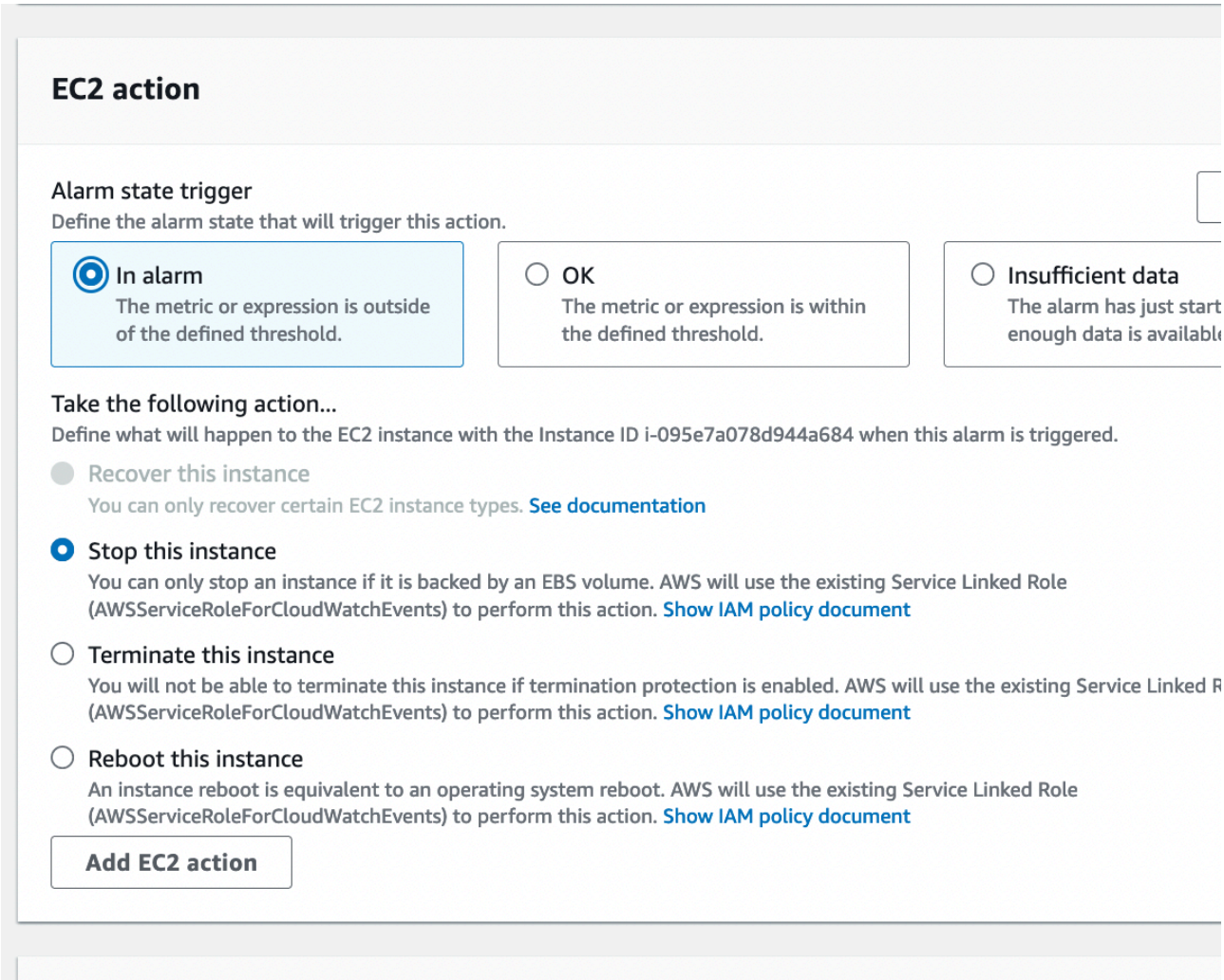


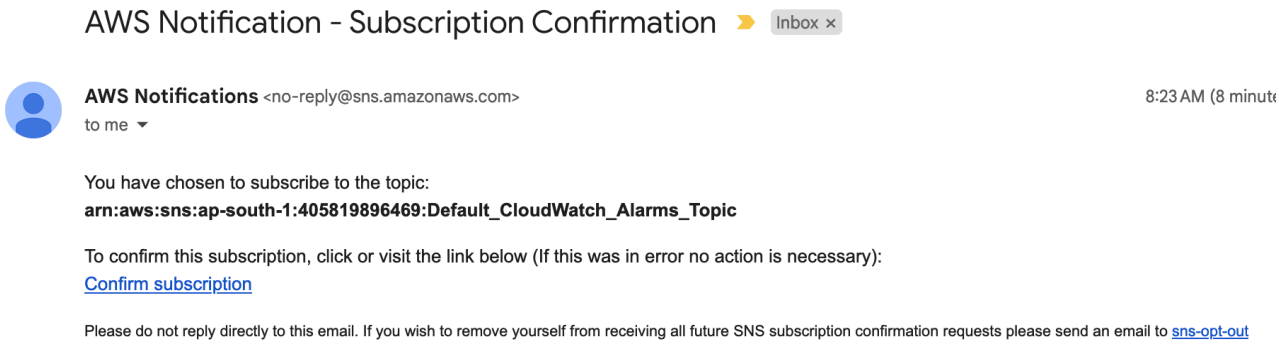
6. In the period you can provide the minutes , say if 1 minute
7. Provide CPU utilization condition say if it is 5%, Click ‘Next’

8. For sending email notification you can click create new topic by providing your email address
9. You can choose any EC2 action if your CPU utilization goes beyond 5 % you can select Stop this instance and click "Next"
10. Provide the Alarm name / description click 'Next', preview the settings and click click 'create alarm'
11. Now you can see the alarm created


Conditions
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.
5
Must be a number
Additional configuration


Add name and description
Name and description
Alarm name
cpu_utilization
Alarm description - optional
View formatting guidelines
Edit
Preview
server----utilizationnss
Up to 1024 characters (24/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will rema
plain text in the alarm notifications.



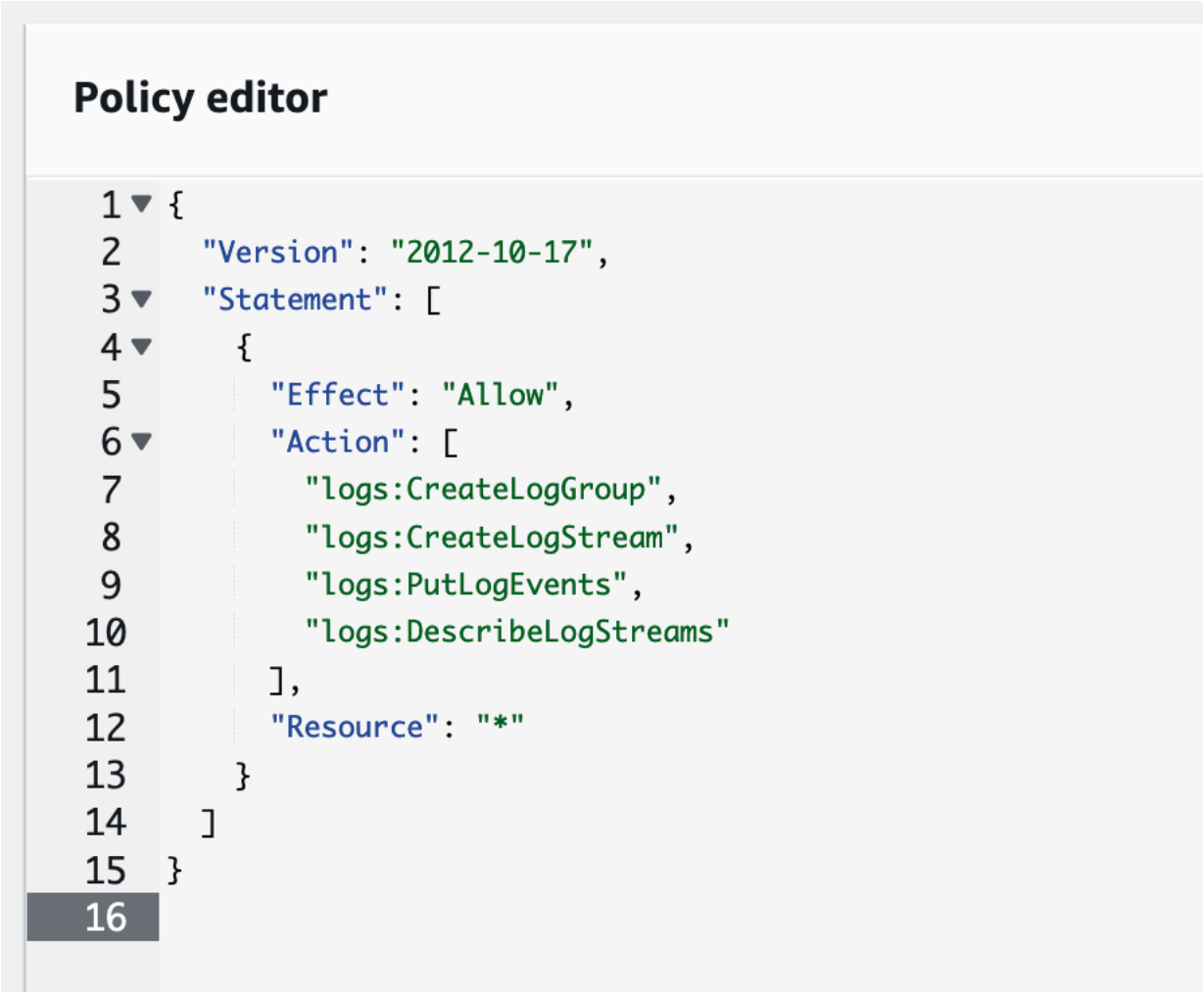


12. You can run the load test using meter to cross the Threshold your Instance will be stopped automatically and a mail will be triggered as below

Create IAM roles and policies for cloud watch logs

1. Navigate to AM dashboard
2. Click on policies -> create policy
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"
1.
"Resource": [1]



AmazonGrafanaCloudWa...	AWS managed
AWSAppSyncPushToClou...	AWS managed
AWSCloudWatchAlarms_...	AWS managed
AWSOpsWorksCloudWatc...	AWS managed
AWSrePostPrivateCloudW...	AWS managed
AWSServiceRoleForCloud...	AWS managed
AWSServiceRoleForCloud...	AWS managed
cloudwatch_iam_role	Customer managed
CloudWatch-CrossAccoun...	AWS managed
CloudWatchActionsEC2Ac...	AWS managed
CloudWatchAgentAdmin...	AWS managed

Add permissions Info

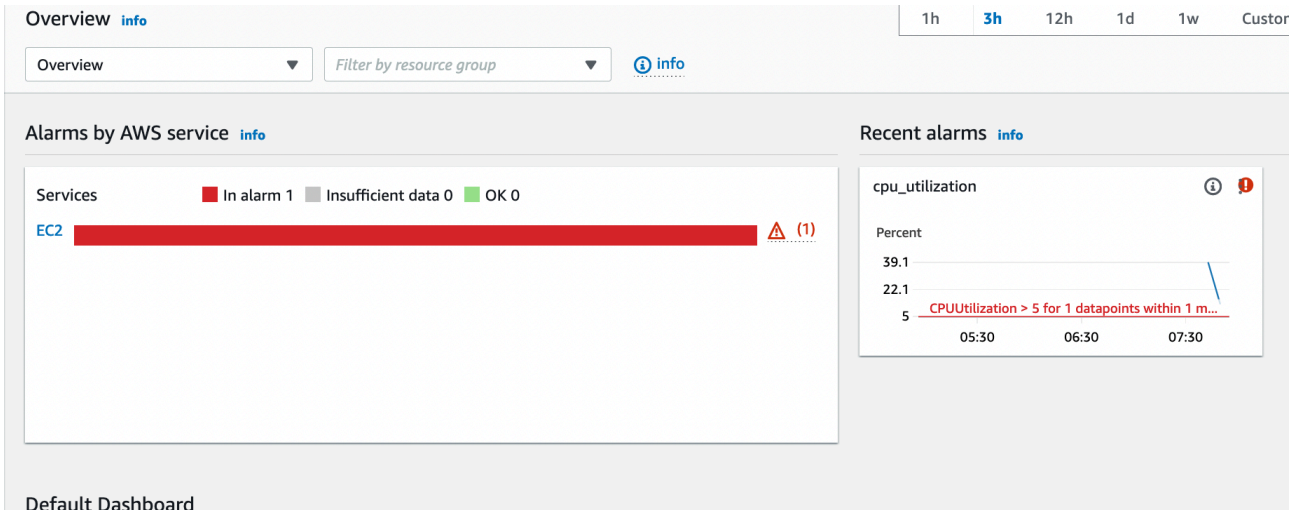
Permissions policies (1/930) Info

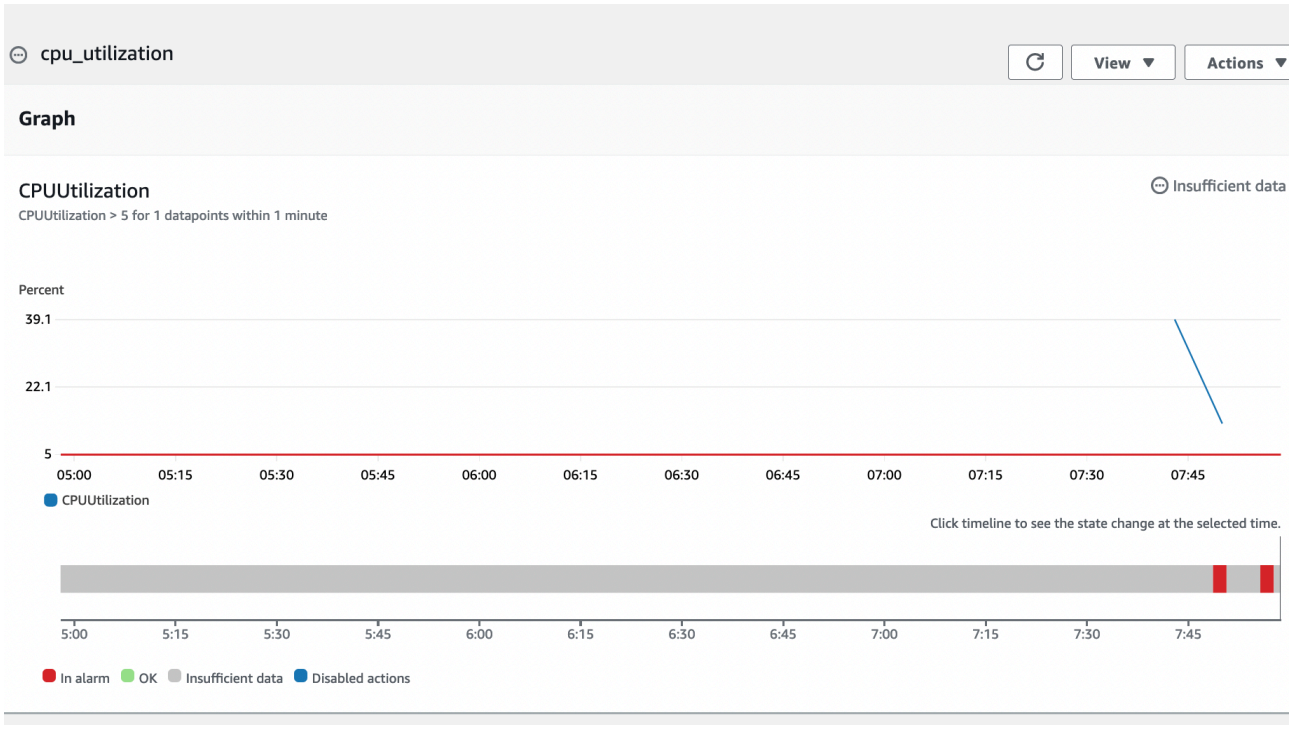
Choose one or more policies to attach to your new role.

cloudwatch_

Policy name	
cloudwatch_iam_role	

▶ **Set permissions boundary - *optional***



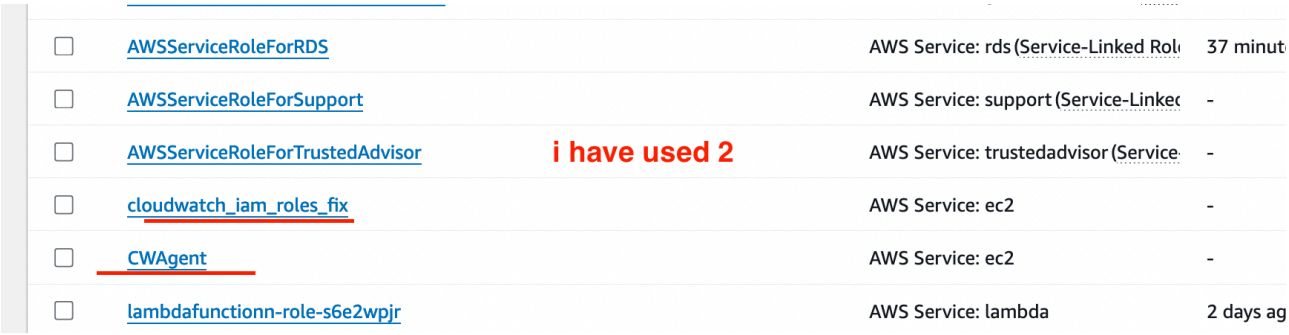


5. Click on Add tags, you can provide the tags and click on review
6. Provide the name and the description
7. Review once and click on create policy, your policy will be created
8. Navigate to IAM roles tab -> click create role
9. Select service as ec2 and click on Next
10. Select the policy that you have created and then click Next
11. Provide the role name, review once and then create role your role should be

created
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

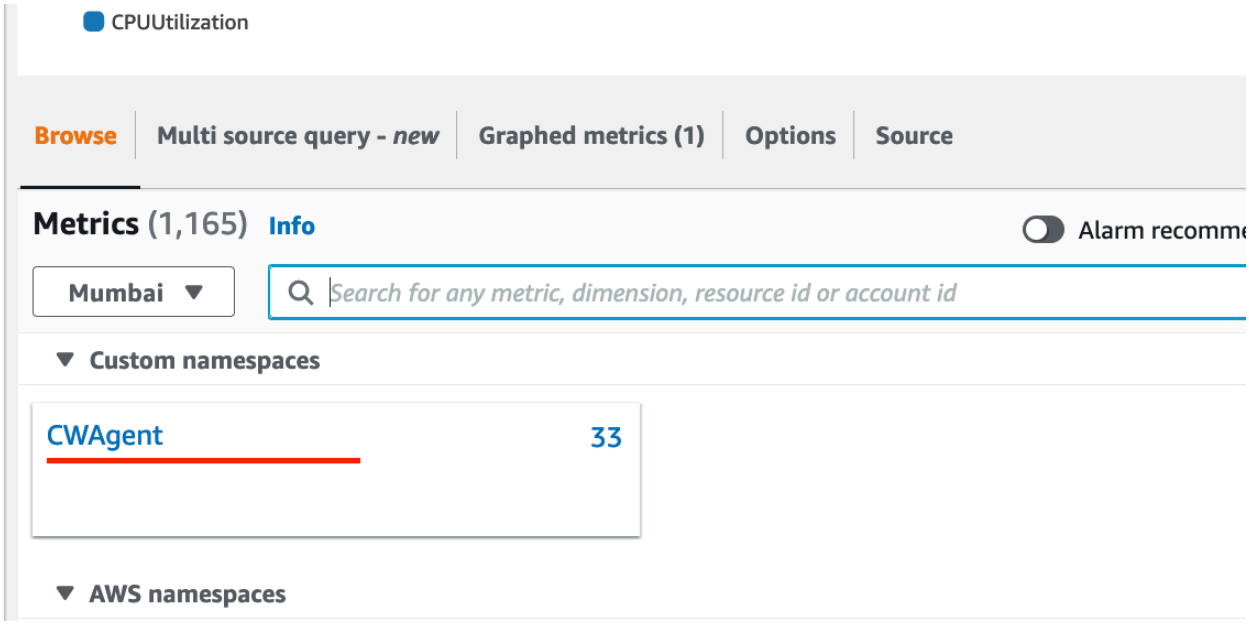
Configure the cloudwatch logs((Method-2))

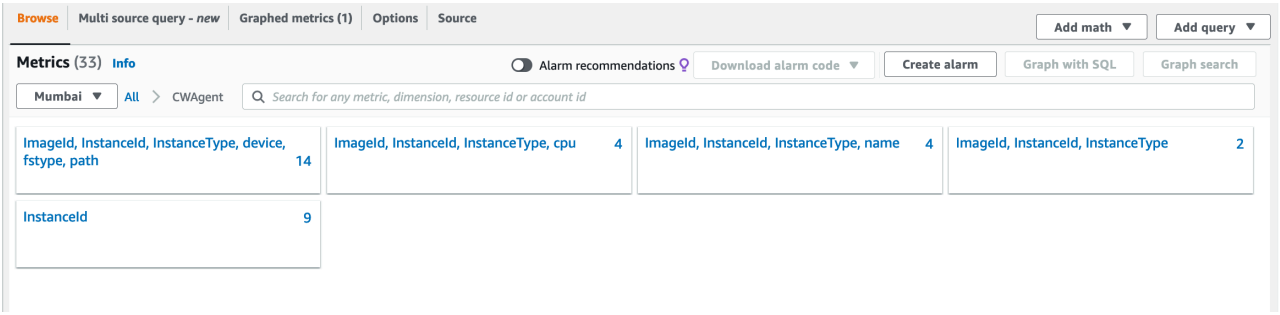
1.Navigate to your ec2 instance (nginx server which you configured in cloudwatch)
2. Run sudo yum install awslogs -y
3. Now open the awscli.conf using sudo vi /etc/awslogs/awscli.conf and add modify your region
4.
Open awslogs.conf file using sudo vi /etc/awslogs/awslogs.conf
5. Modify the lines as below
6.Now start your aws logs service using the following command sudo systemctl start awslogsd
7. Now navigate to your cloudwatch console and navigate to the log group and you will see the logs attached as below

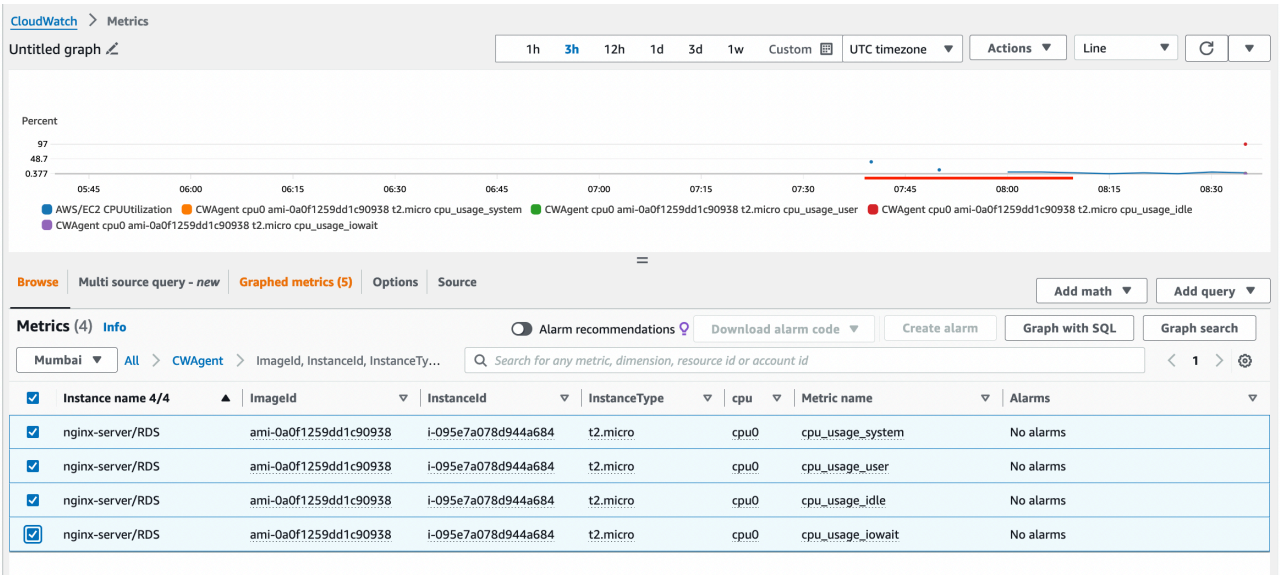


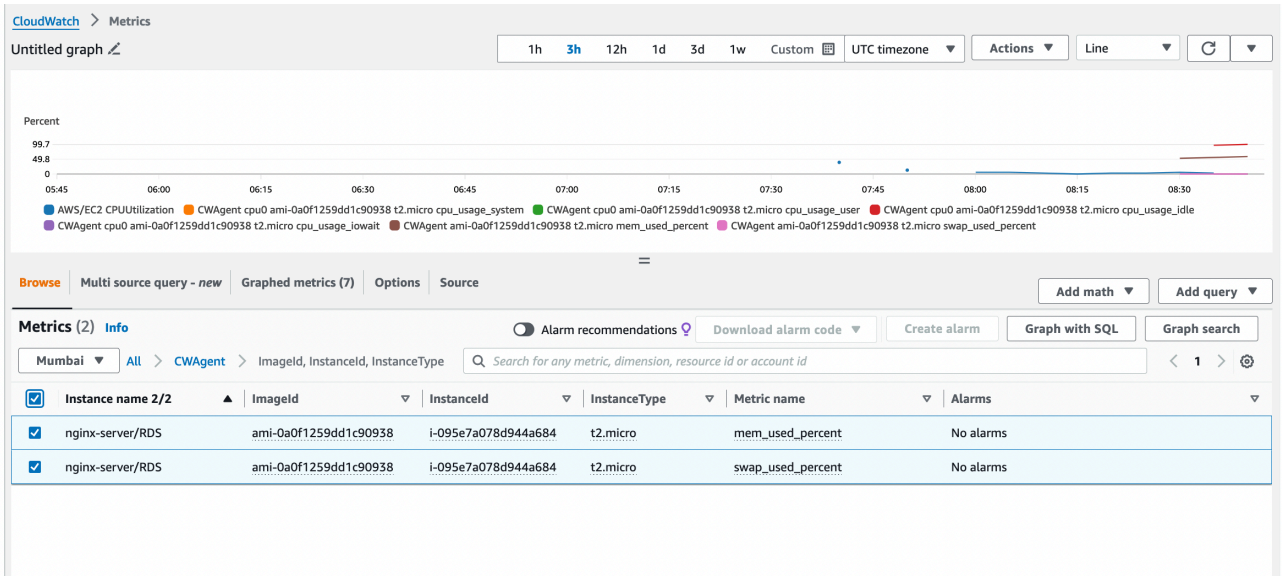
```
ec2-user@ip-10-0-1-197.ap-south-1.compute.internal /opt/aws/amazon-cloudwatch-agent/bin (2.581s)
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json

****** processing amazon-cloudwatch-agent ******
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/01/03 08:34:11 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/01/03 08:34:11 I! Valid Json input schema.
2024/01/03 08:34:11 D! ec2tagger processor required because append_dimensions is set
```










```
ec2-user@ip-10-0-1-197.ap-south-1.compute.internal /opt/aws/amazon-cloudwatch-agent/logs (0.092s)
ls
amazon-cloudwatch-agent.log  configuration-validation.log  state

ec2-user@ip-10-0-1-197.ap-south-1.compute.internal /opt/aws/amazon-cloudwatch-agent/logs
```