

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

#### Add widget

**Data sources types - new**

- Cloudwatch
- Other content types
- Create data sources

**Widget Configuration**

Data type

- Metrics
- Logs
- Alarms

Widget type

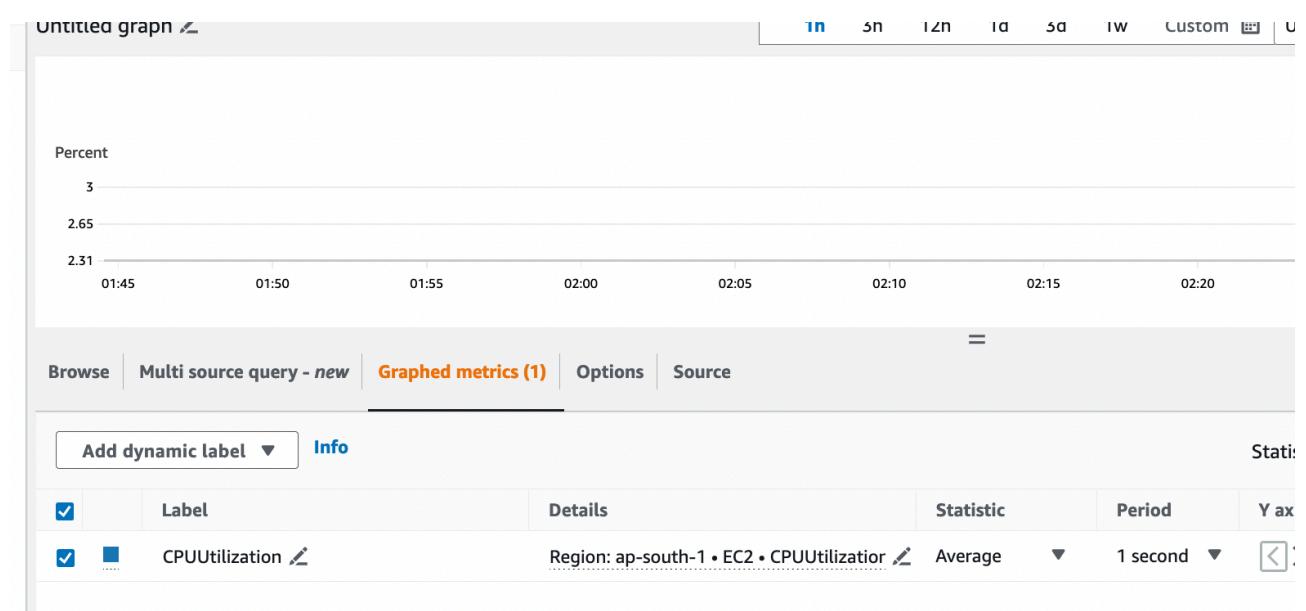
- Line**  
Compare metrics over time
- Data table**  
Compare metrics over time in a table
- Number**  
Instantly see the latest value for a metric
- Gauge**  
See the latest value within a range
- Stacked area**  
Compare the total over time
- Bar**  
Compare categories
- Pie**  
Show percentage or proportional data
- Explorer**  
A single widget for tag-based graphs

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

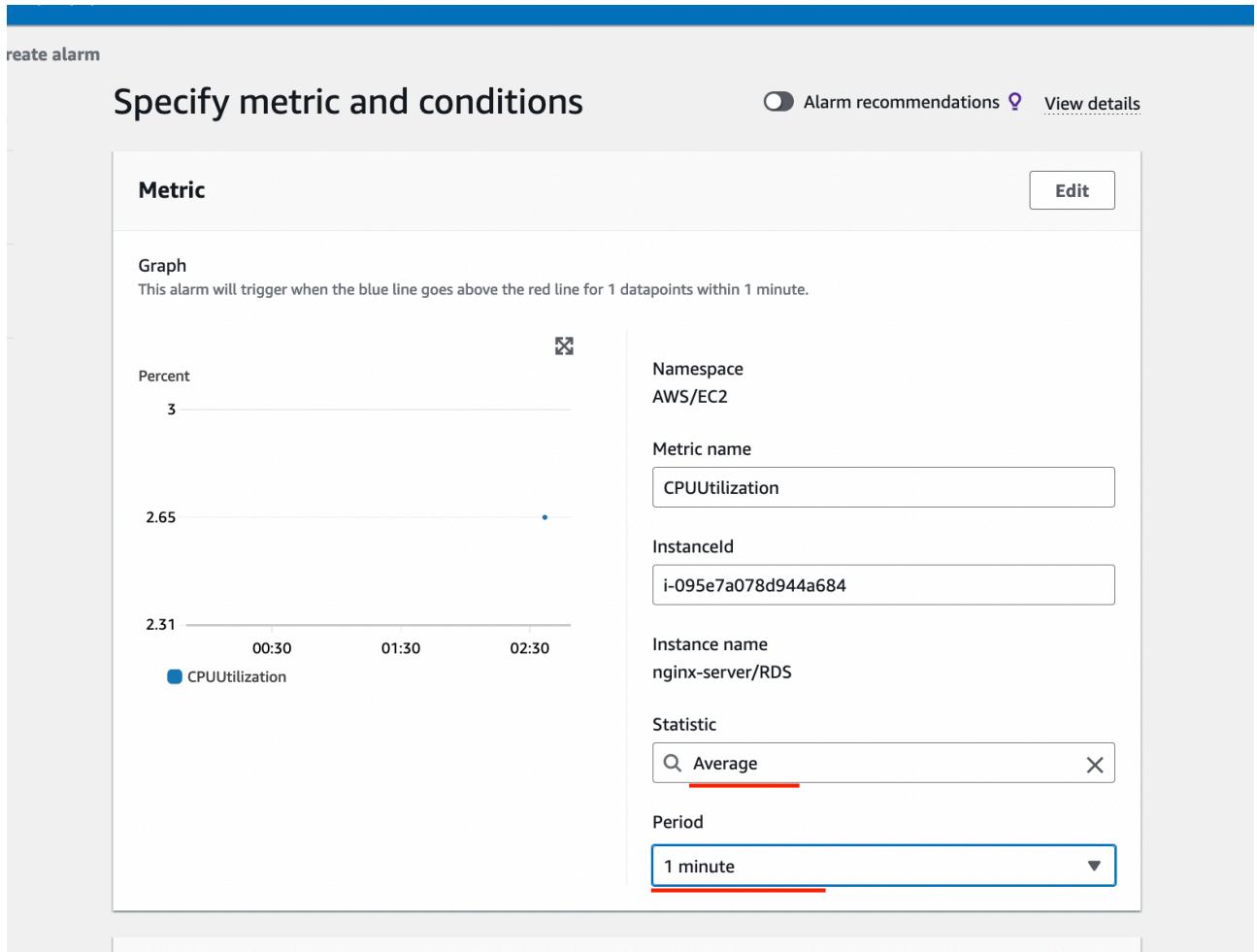
<input type="checkbox"/>	nginx-server/RDS	i-095e7a078d944a684	DiskReadOps ⓘ
<input type="checkbox"/>	nginx-server/RDS	i-095e7a078d944a684	DiskWriteBytes ⓘ
<input type="checkbox"/>	nginx-server/RDS	i-095e7a078d944a684	DiskWriteOps ⓘ
<input checked="" type="checkbox"/>	nginx-server/RDS	i-095e7a078d944a684	CPUUtilization ⓘ
<input type="checkbox"/>	nginx-server/RDS	i-095e7a078d944a684	NetworkPacketsOut ⓘ

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  
 $\geq$  threshold

Lower/Equal  
 $\leq$  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 remain plain text in the alarm notifications.

## EC2 action

### 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 and enough data is available.

### Take the following action...

Define what will happen to the EC2 instance with the Instance ID i-095e7a078d944a684 when this alarm is triggered.

#### Recover this instance

You can only recover certain EC2 instance types. [See documentation](#)

#### 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 (AWSLambdaRoleForCloudWatchEvents) 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 (AWSLambdaRoleForCloudWatchEvents) 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 (AWSLambdaRoleForCloudWatchEvents) to perform this action. [Show IAM policy document](#)

[Add EC2 action](#)

### AWS Notification - Subscription Confirmation ➔ Inbox x



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

8:23 AM (8 minutes ago)

You have chosen to subscribe to the topic:

[arn:aws:sns:ap-south-1:405819896469: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](#)

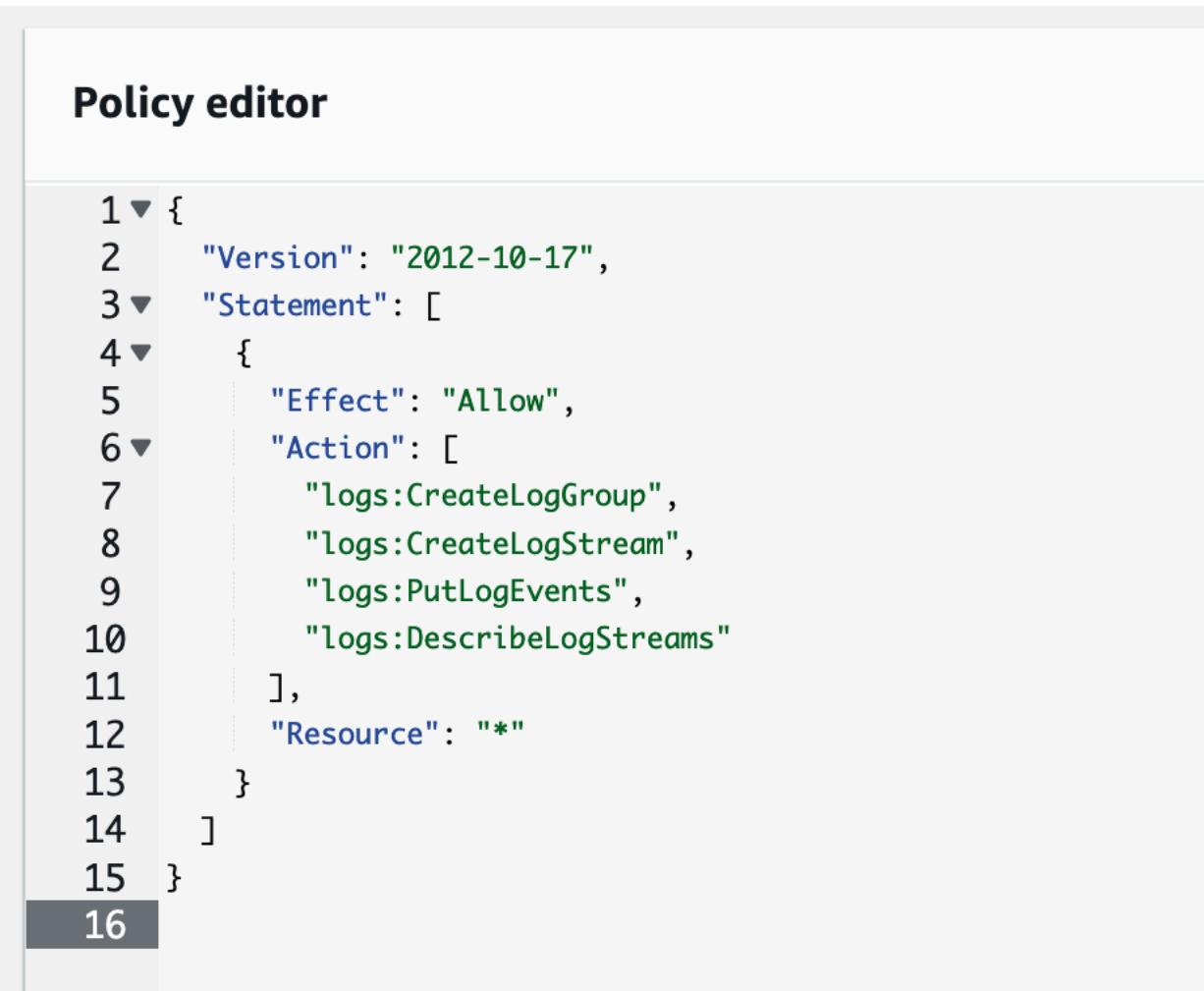
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

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"  
    ],  
    "Resource": [1]
```



The screenshot shows the 'Policy editor' interface in the AWS IAM console. The title 'Policy editor' is at the top. Below it is a code editor window containing the JSON policy code. The code is numbered from 1 to 16 on the left. Lines 1 through 15 are part of the JSON object, while line 16 is a dark grey footer bar.

```
1 ▼ {  
2     "Version": "2012-10-17",  
3 ▼     "Statement": [  
4 ▼         {  
5             "Effect": "Allow",  
6 ▼             "Action": [  
7                 "logs:CreateLogGroup",  
8                 "logs:CreateLogStream",  
9                 "logs:PutLogEvents",  
10                "logs:DescribeLogStreams"  
11            ],  
12            "Resource": "*"  
13        }  
14    ]  
15}  
16
```

○	<input type="checkbox"/>  <a href="#">AmazonGrafanaCloudWa...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSAppSyncPushToClou...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSCloudWatchAlarms_...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSOpsWorksCloudWatc...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSrePostPrivateCloudW...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSServiceRoleForCloud...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">AWSServiceRoleForCloud...</a>	AWS managed
○	<input type="checkbox"/> <a href="#">cloudwatch_iam_role</a>	Customer managed
○	<input type="checkbox"/>  <a href="#">CloudWatch-CrossAccoun...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">CloudWatchActionsEC2Ac...</a>	AWS managed
○	<input type="checkbox"/>  <a href="#">CloudWatchAgentAdmin...</a>	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*

Overview [info](#)

1h | **3h** | 12h | 1d | 1w | Custom

Overview Filter by resource group [info](#)

Alarms by AWS service [info](#)

Services ■ In alarm 1 ■ Insufficient data 0 ■ OK 0

**EC2** In alarm 1 ⚠ (1)

Recent alarms [info](#)

cpu\_utilization ■ In alarm 1 ■ Insufficient data 0 ■ OK 0

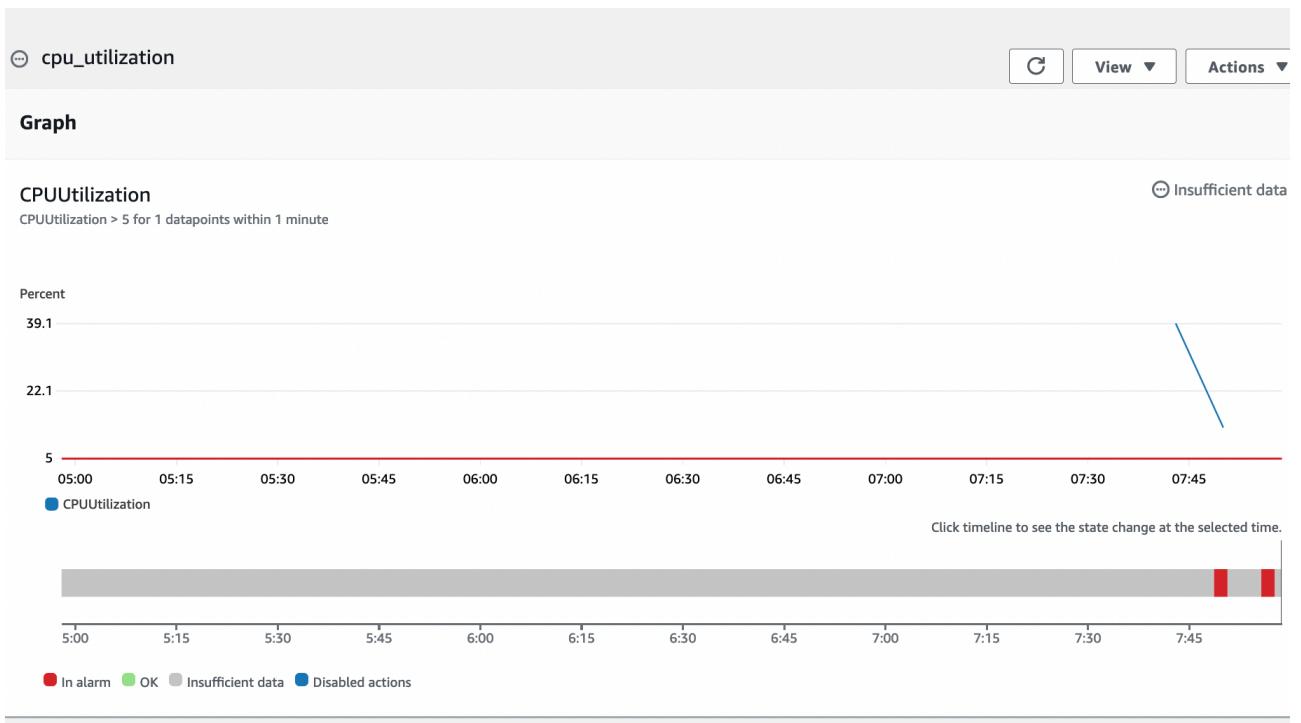
Percent

39.1  
22.1  
5

CPUUtilization > 5 for 1 datapoints within 1 minute

05:30 06:30 07:30

Default Dashboard



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

<input type="checkbox"/> <a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds (Service-Linked Role)	37 minut
<input type="checkbox"/> <a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/> <a href="#">AWSServiceRoleForTrustedAdvisor</a>	<b>i have used 2</b>	AWS Service: trustedadvisor (Service-Linked Role)
<input type="checkbox"/> <a href="#">cloudwatch_iam_roles_fix</a>	AWS Service: ec2	-
<input type="checkbox"/> <a href="#">CWAgent</a>	AWS Service: ec2	-
<input type="checkbox"/> <a href="#">lambdafunctionn-role-s6e2wpjr</a>	AWS Service: lambda	2 days ag

```
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/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 timesSuccessful
ully 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

```

● CPUUtilization

**Browse** | **Multi source query - new** | **Graphed metrics (1)** | **Options** | **Source**

### Metrics (1,165) Info

Mumbai ▾ Search for any metric, dimension, resource id or account id

▼ Custom namespaces

**CWAgent** 33

▼ AWS namespaces

**Browse** | **Multi source query - new** | **Graphed metrics (1)** | **Options** | **Source**

Metrics (33) Info

Mumbai ▾ All > CWAgent Search for any metric, dimension, resource id or account id

Create alarm Graph with SQL Graph search

<span style="color: blue;">ImageId, InstanceId, InstanceType, device, fstype, path</span> 14	<span style="color: blue;">ImageId, InstanceId, InstanceType, cpu</span> 4	<span style="color: blue;">ImageId, InstanceId, InstanceType, name</span> 4	<span style="color: blue;">ImageId, InstanceId, InstanceType</span> 2
<span style="color: blue;">InstanceId</span> 9			

CloudWatch > Metrics

Untitled graph Actions Line G ▼

Percent

1h 3h 12h 1d 3d 1w Custom UTC timezone Actions Line G ▼

Legend:

- AWS/EC2 CPUUtilization
- CWAgent cpu0 ami-0a0f1259dd1c90938 t2.micro cpu\_usage\_system
- CWAgent cpu0 ami-0a0f1259dd1c90938 t2.micro cpu\_usage\_user
- CWAgent cpu0 ami-0a0f1259dd1c90938 t2.micro cpu\_usage\_idle
- CWAgent cpu0 ami-0a0f1259dd1c90938 t2.micro cpu\_usage\_iowait

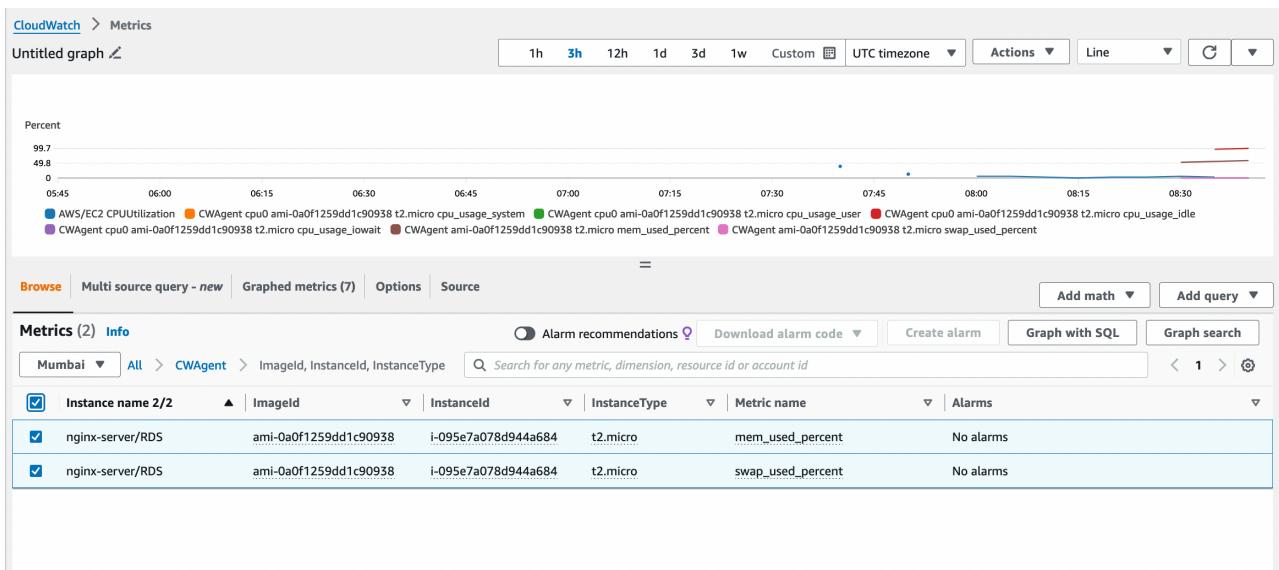
**Browse** | **Multi source query - new** | **Graphed metrics (5)** | **Options** | **Source**

Metrics (4) Info

Mumbai ▾ All > CWAgent > ImageId, InstanceId, InstanceType Search for any metric, dimension, resource id or account id

Create alarm Graph with SQL Graph search

Instance name	InstanceId	InstanceType	cpu	Metric name	Alarms
nginx-server/RDS	ami-0a0f1259dd1c90938	i-095e7a078d944a684	t2.micro	cpu_usage_system	No alarms
nginx-server/RDS	ami-0a0f1259dd1c90938	i-095e7a078d944a684	t2.micro	cpu_usage_user	No alarms
nginx-server/RDS	ami-0a0f1259dd1c90938	i-095e7a078d944a684	t2.micro	cpu_usage_idle	No alarms
nginx-server/RDS	ami-0a0f1259dd1c90938	i-095e7a078d944a684	t2.micro	cpu_usage_iowait	No alarms



```

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

```

### CloudWatch > Log groups > CWAgent

## CWAgent

**Log group details**

Log class - new   <a href="#">Info</a>	Metric filters 0
Standard	Subscription filters 0
ARN <a href="#">arn:aws:logs:ap-south-1:405819896469:log-group:CWAgent:*</a>	Contributor Insights rules -
Creation time 6 minutes ago	KMS key ID -
Retention Never expire	
Stored bytes	