\*\*\*CLOUDWATCH\*\*\*

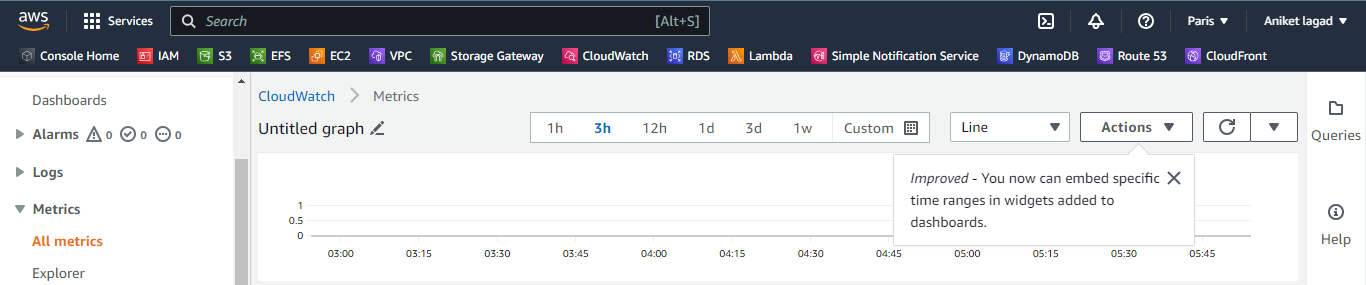
1.EC2 Instance Monitoring:

Enable detailed monitoring for all EC2 instances in your environment to capture metrics at a 1-minute frequency.

🡺

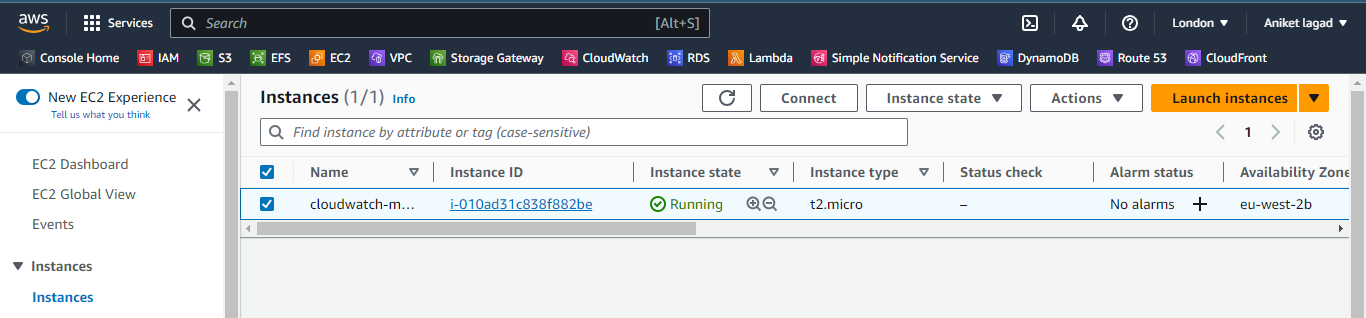
Step 1:-

We have to create cloudWatch metrics so first login to aws account and then go clouWatch service and click on metrics section.



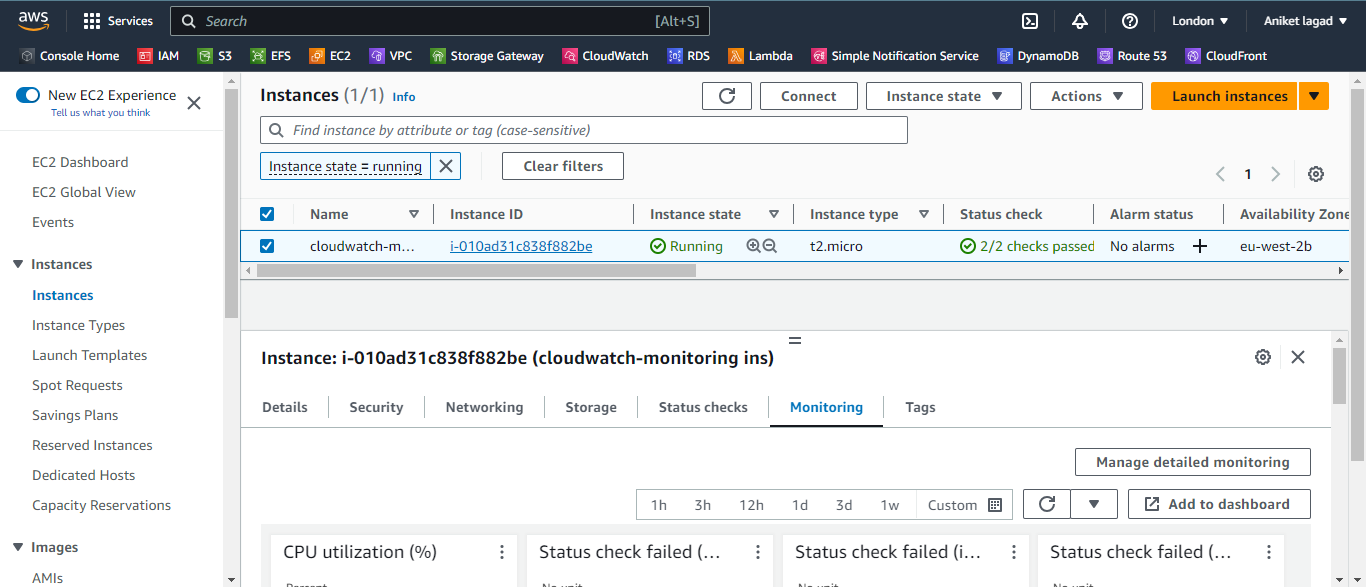
Step 2:-

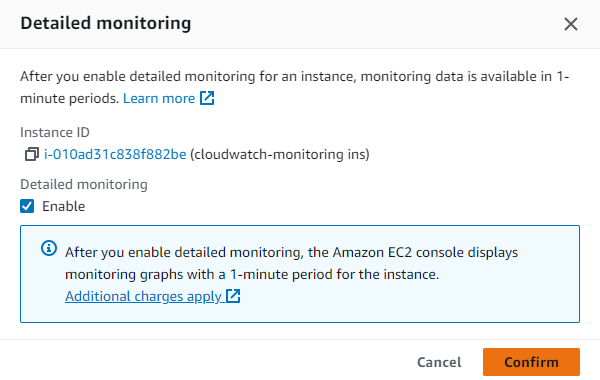
Open new tab on browser and go ec2 service and After that create instance which you have to monitor.



Step 3:-

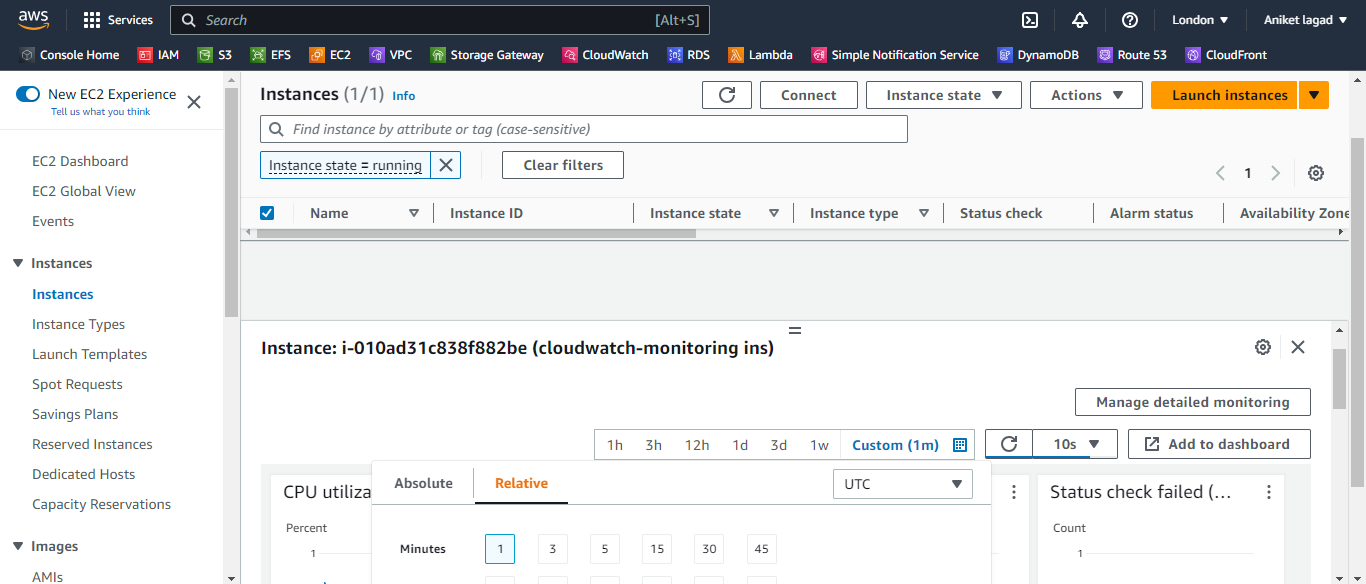
Now you have to select and enable it monitoring so click on monitoring option and then click on manage detailed monitoring and then you see option of enable it select it and then click on conform and your instance monitoring is on.





Step 3:-

After that you have see then option of custom option so click on it and then select 1 mini option so your instance send 1 minit matric.



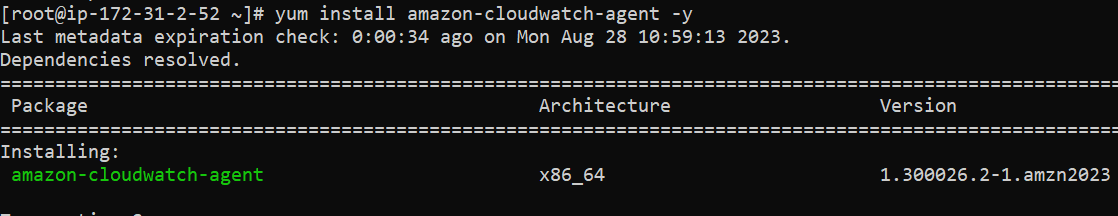
2.Custom Metrics:

Create a custom CloudWatch metric named "ResponseTime" to monitor the response time of an API endpoint on your application. Simulate sending data for this metric to CloudWatch.

🡺

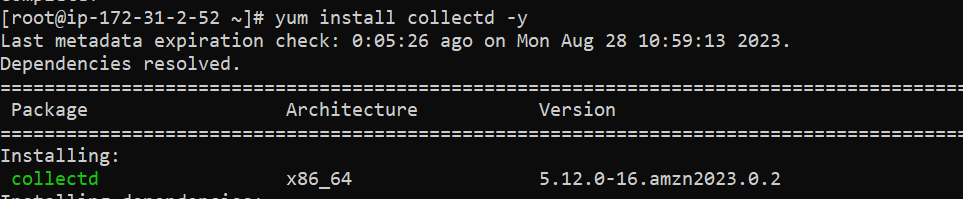
Step 1:-

We have to create a custom metric so there was one service in aws as name cloudagent so get remotely access of your instance you can send metrics to aws clouwdwatch. And after that download package of cloudwatch agent.



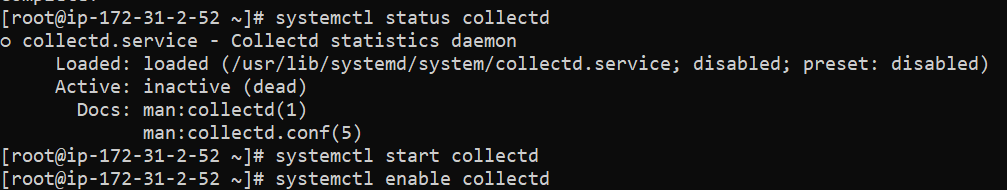
Step 2:-

Then now install collectd package it is necessary package for aws cloudwatch agent.



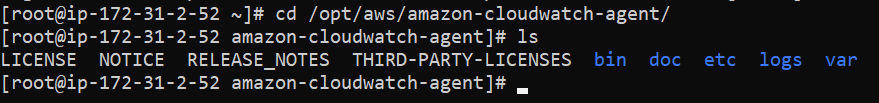
Step 3:-

And after that get configure collectd service.

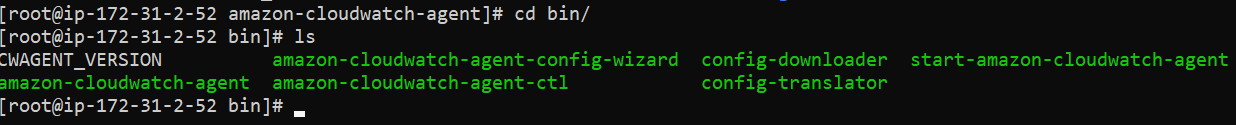


Step 4:-

Now you have to change directory to clowdwatch so run command cd /opt/aws/amazon-clowdwatch-agent. Clouwdwatch agent is by default stored in /opt directory.



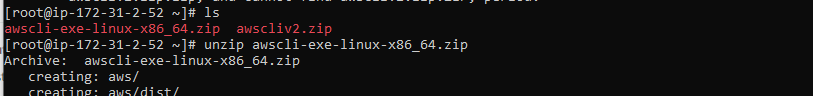
Step 5:-

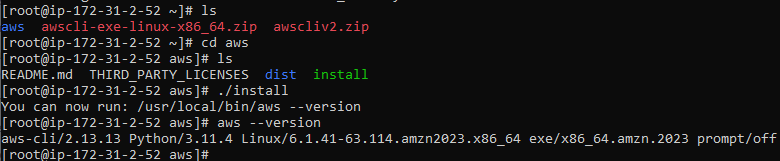
Now you have to send your systems matrics to cloudwatch so go to bin . there was amazon-cloudwatch-agent-config-wizard. 

Step 6:-

Now install the aws cli. It is for the installation of aws cli in your account so you can configure user.

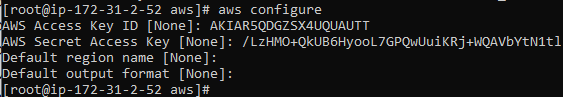
Step 7:-

Now unzip that package and then go to thata directory name aws. #cd aws and then there was install name .sh file so run that script file force full as ./install. And then your aws cli is ready.

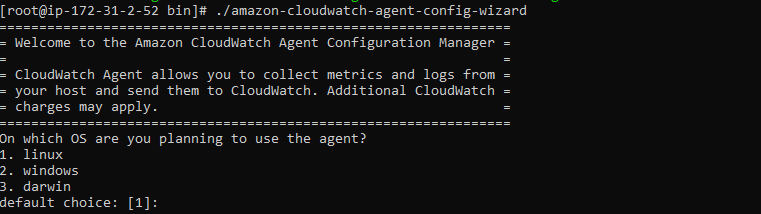


Step 8:-

Now configure aws by any users keys. Run command #aws configure and gave the user’s access key and then secret key and enter enter 2 time for by default all region and output format.



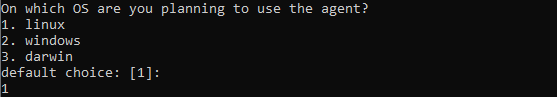
Step 8:-

After that download package of python. And then go to bin directory of a cloudwatch-agent . and then run .sh file amazon-cloudwatch-agent-config-wizard and then you have see the Amazon CloudWatch Agent Configuration Manager. So one by one gave default numbers means answers. 

Step 10:-

So first question is On which OS are you planning to use the agent?

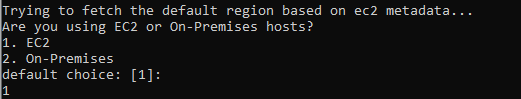
So we have to select OS linux so enter 1 and hit enter.



Step 11:-

Are you using EC2 or On-Premises hosts?

So gave it 1 because we will send matricx and logs of ec2.



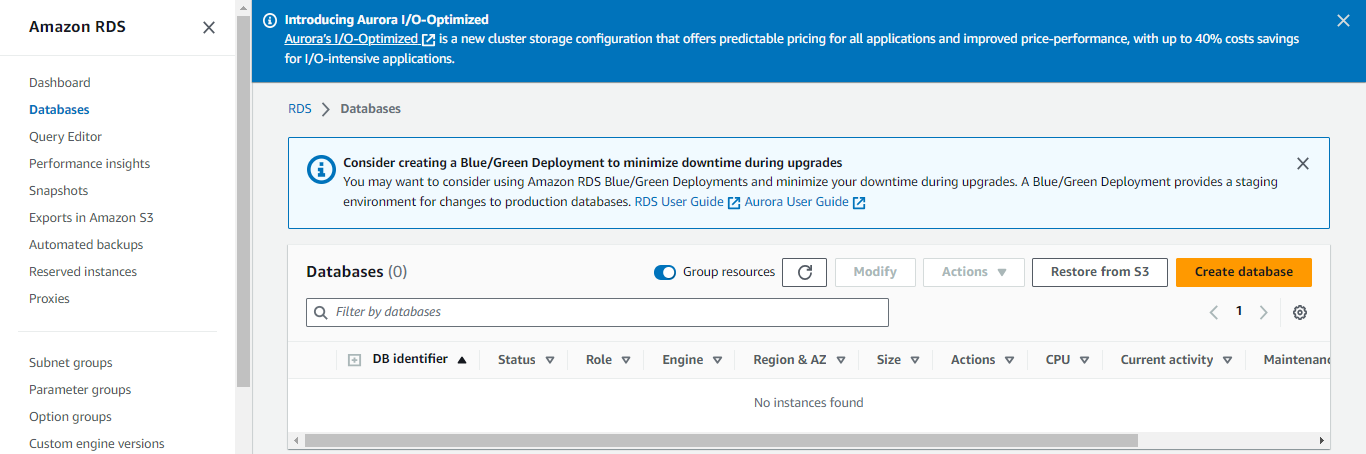
Step 12:-

3.RDS Instance Monitoring:

Set up a CloudWatch alarm that triggers whenever the RDS instance's CPU utilization exceeds 70% for at least two consecutive 5-minute periods.

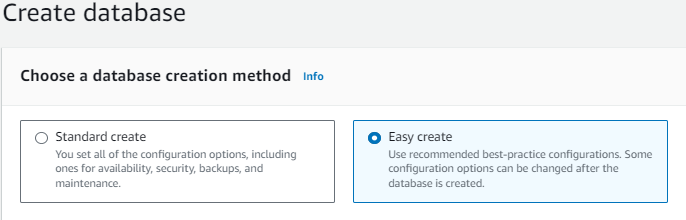
🡺

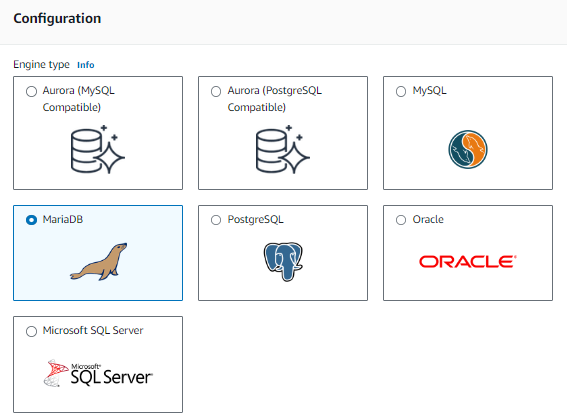
Step 1:-

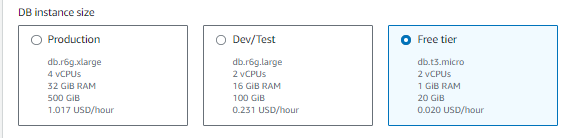
First of all go to RDS service to create data base . click on create database. 

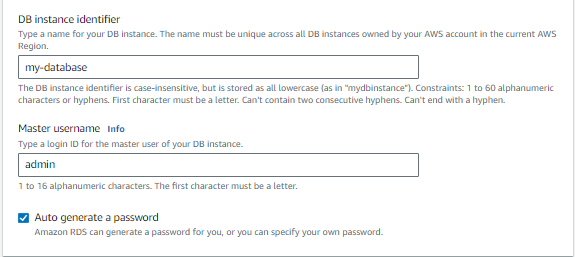
Step 2 :-

Now you will see the create database setting so select easy create option fisrt. Then select engine as mariadb and then select free tier so not applicable extra charges and then gave database name and then gave user name of who access your database and after that gave password that user or leave auto assign password and then click on create database.



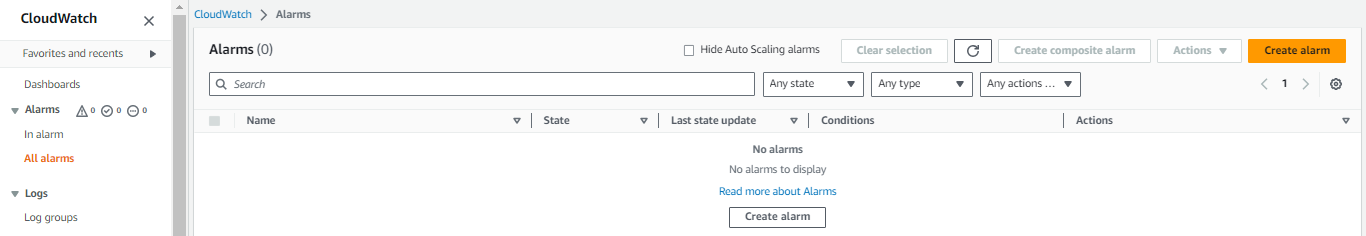






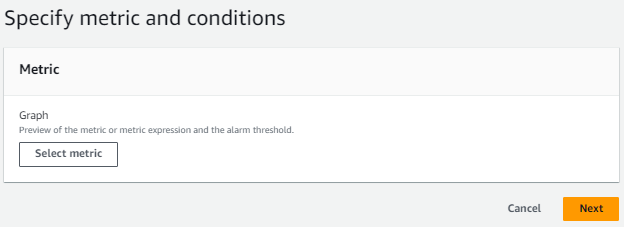
Step 3:-

Now go to cloudwatch service to create alarm. Click on create alarm.



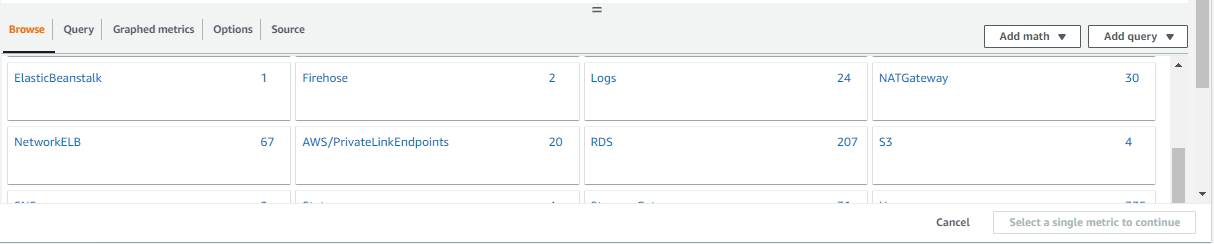
Step 5:-

Then select a matric type.



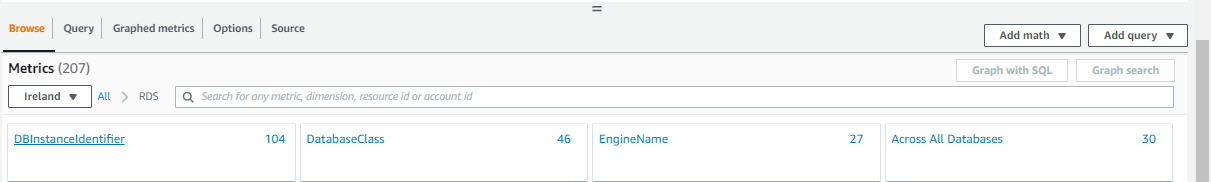
Step 6:-

After that you will see the types of resources so select RDS to create alarm to on RDS instance Utilization .



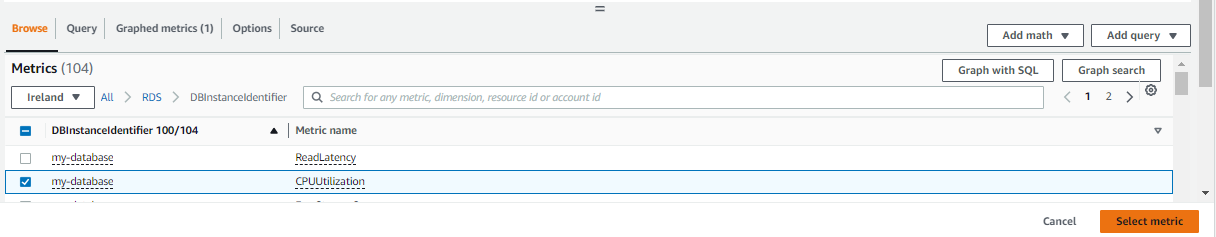
Step 7:-

Now select matrics type as DBInstanceIdentifierand.

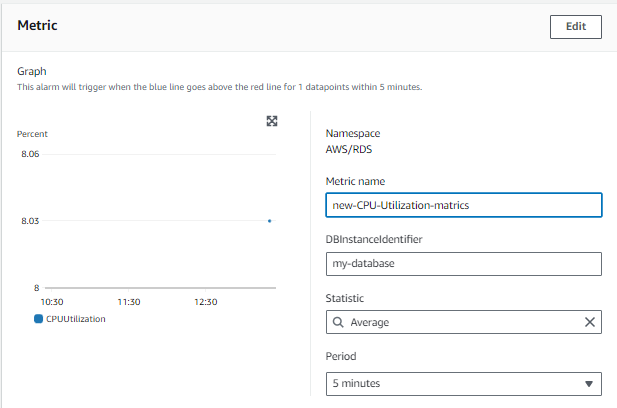


Step 8:-

After select your database instance and then click on select metrics.

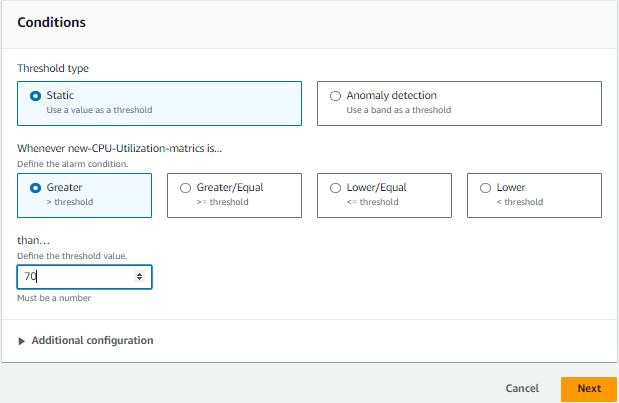


Step 9:-

After that you have to specify the setting of metrics CPU Utilization so gave it name and then click period of time and in that column select 5 minutes.

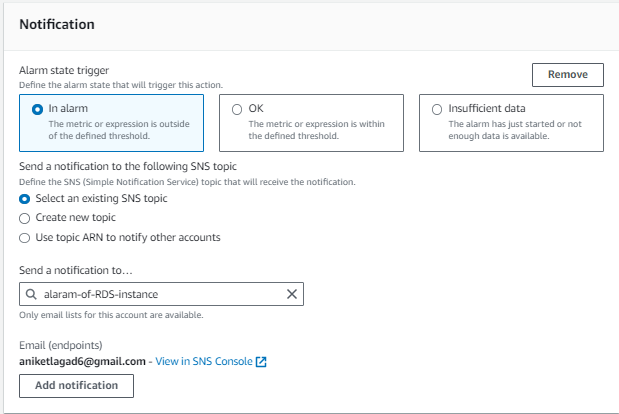
Step 10:-

Now gave condition to that metrics. So select threshold type and then define the threshold condition as greater than threshold and in than column write exact value 70 and clickc on next.



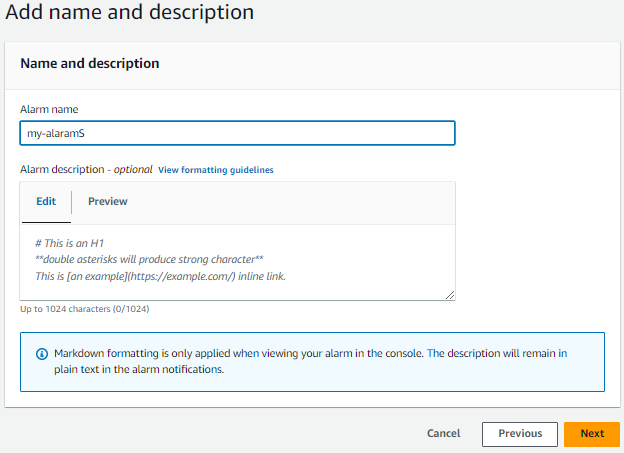
Step 11:-

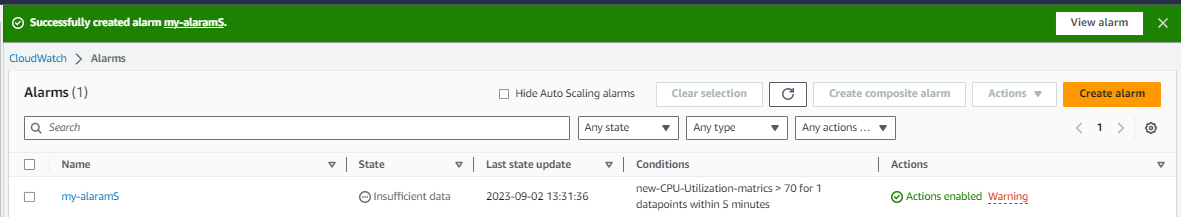
Now you have to specify the notification setting so select alarm state trigger is In Alarm and then select create new topic and gave it name and then write your gmail in which you have to get notification.



Step 12:-

After that at last gave alarm name and then click on next and on next yyou will see the all your specified information so look all oky or not and then click on create alarm and your alarm was set to check CPU utilization.





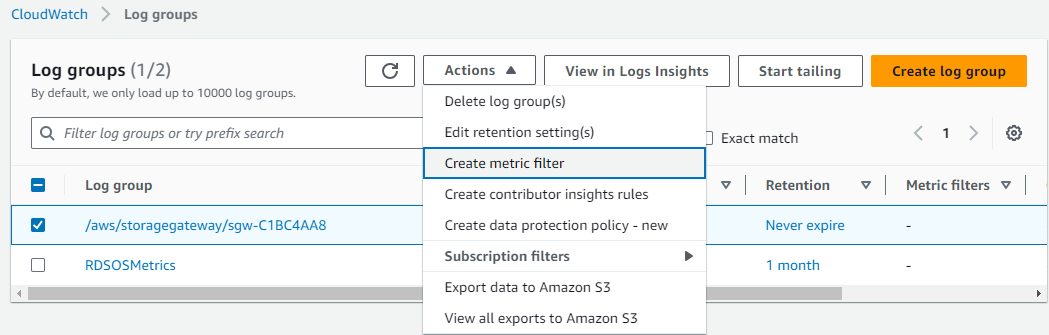
4.CloudWatch Logs:

Create a metric filter for CloudWatch Logs to extract and count occurrences of a specific keyword ("ERROR") in your application logs. Configure an alarm that activates when the error count exceeds 10.

🡺

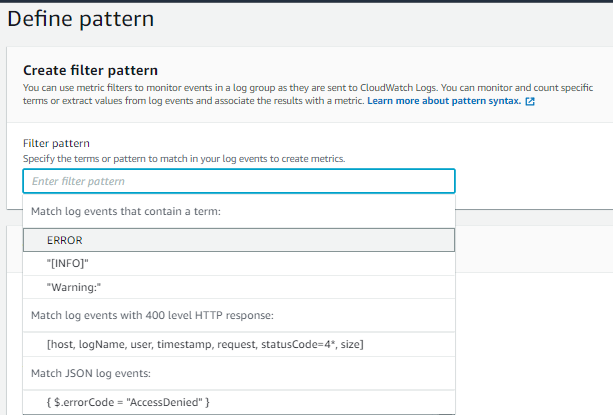
Step 1:-

We have to create a metric filter for ERROR logs. So first go to cloudwatch service and then click on logs and after that click on groups. And then select your already created log group and click on actins and then click on create metric filter.



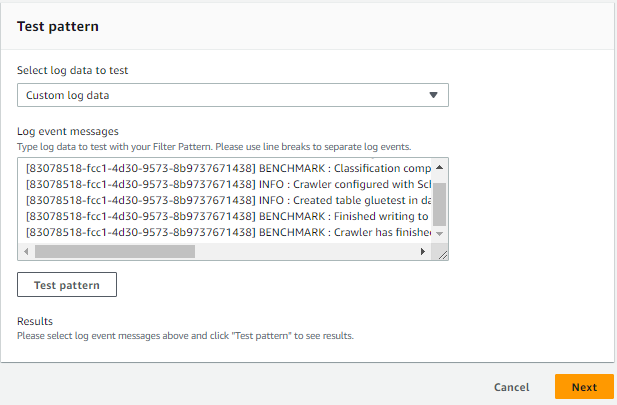
Step 2:-

Now you have see the create filter setting so first select filter pattern as ERROR.



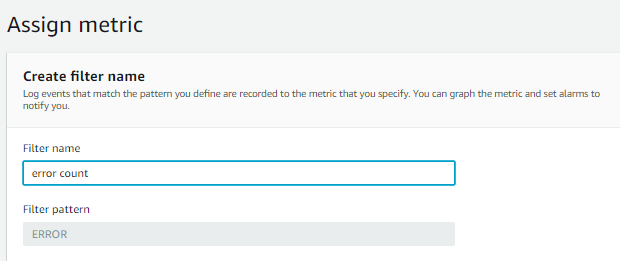
Step 3:-

After that click on test pattern and choose test pattern. And then click on next.



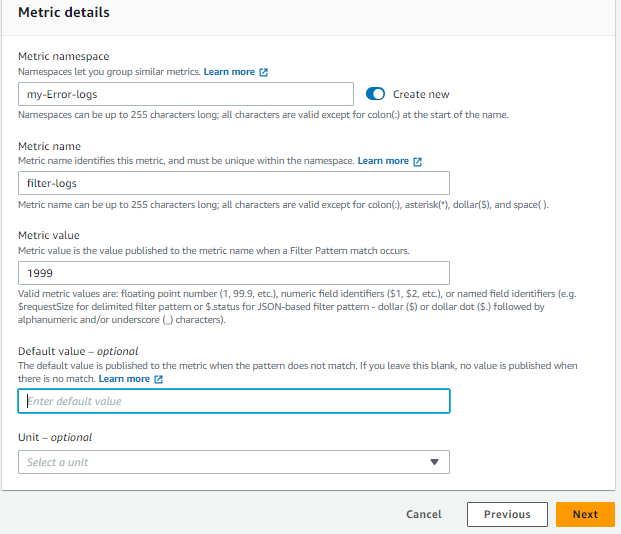
Step 4:-

Now gave filter name as your choice.



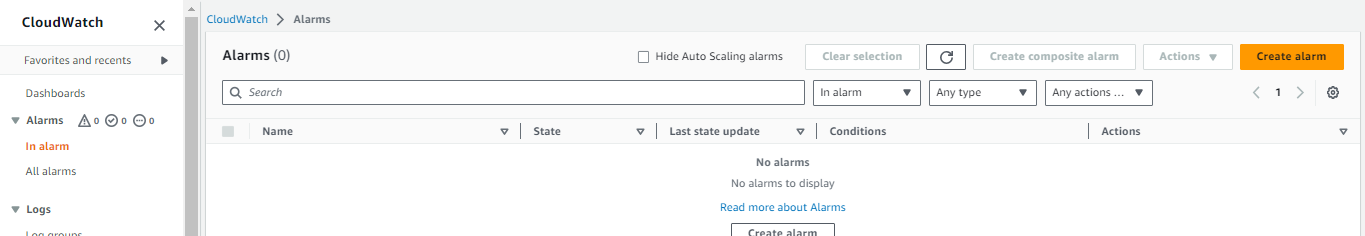
Step 5:

Now you have specify metric details so gave metric namespace and then gave different name to metric and then gave metric as you want after that click on next. Now you have see the all you configured information check is it oky and then click on create filter



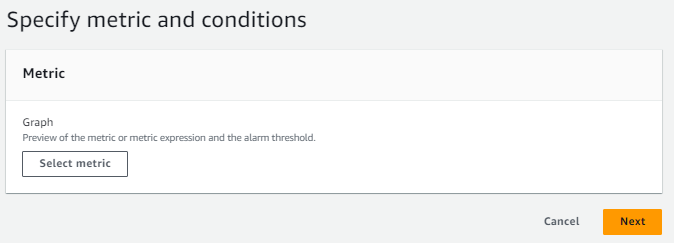
Step 6:-

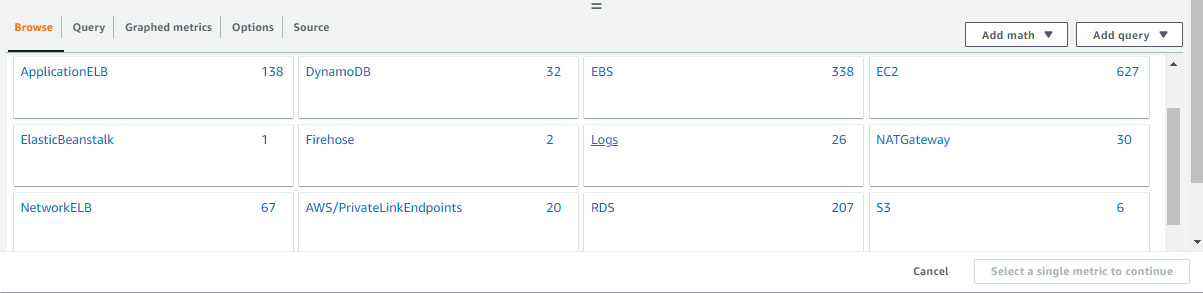
Now you have to create alarm to trigger whenever error log generate 10+ then alarm triggered and you got notify. So go to alarm session and then click on create alarm.



Step 7:-

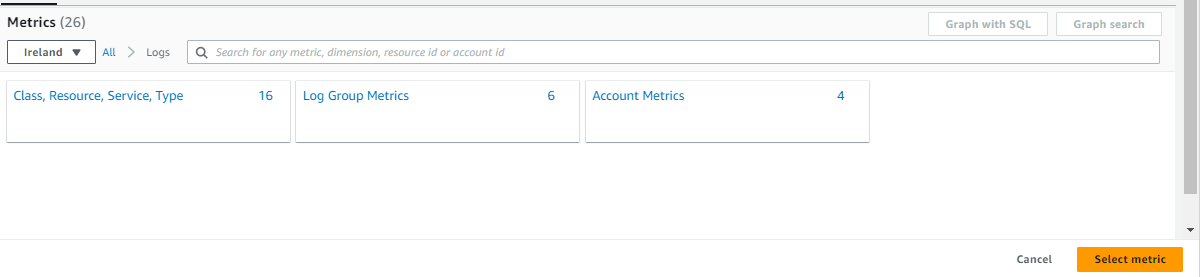
After that click on select metrics. And after that select logs.

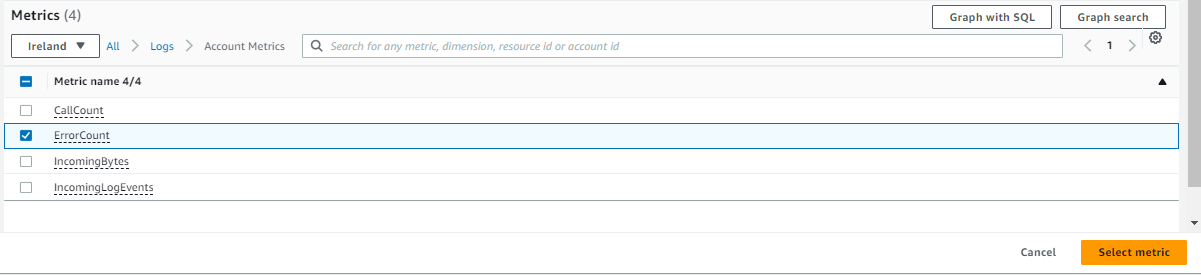




Step 8:-

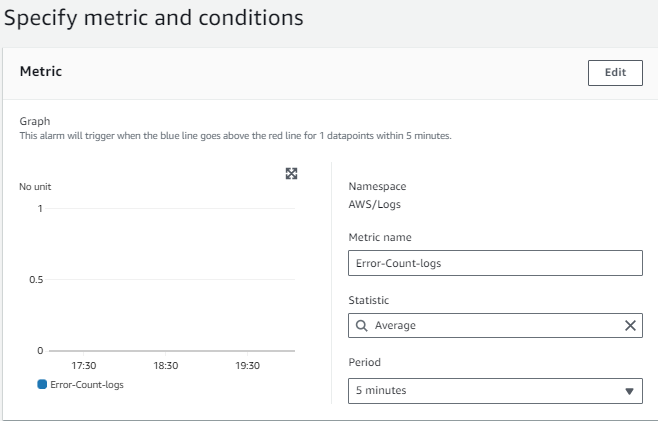
Now select account metrics and then select ErrorCount and then click on select metrics.





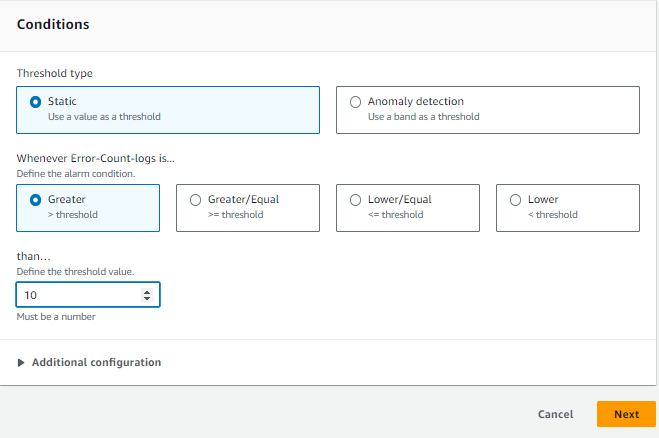
Step 9:-

Now specify the setting of metrics so first gave it name and then select time period.



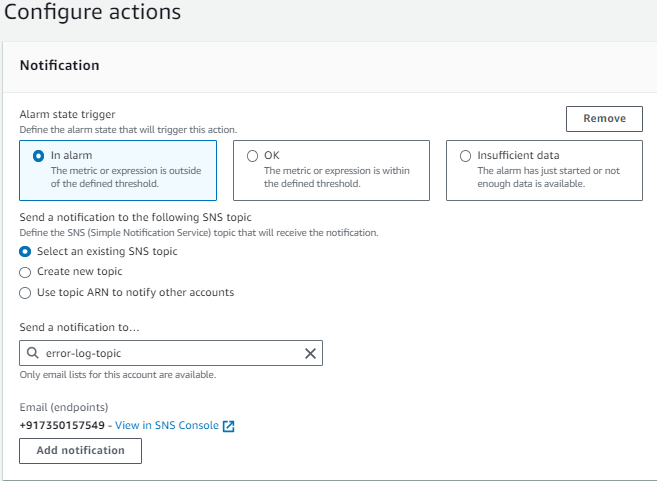
Step 10:-

Now you have to specify conditions so first select threshold type as static and then select when alarm triggered and then in than column write 10 value. And then click on next.



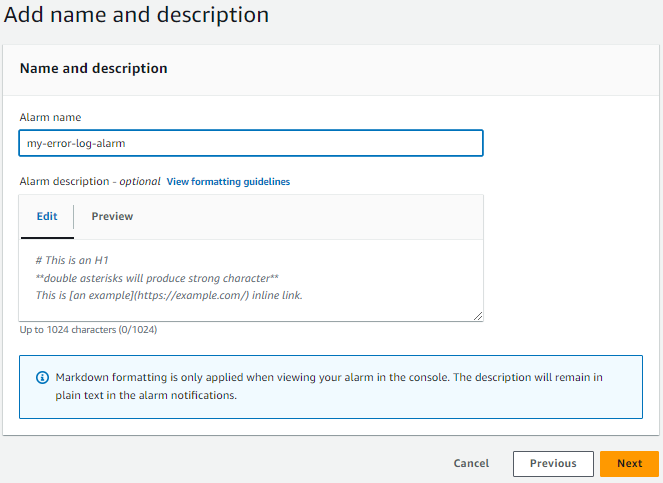
Step 11:-

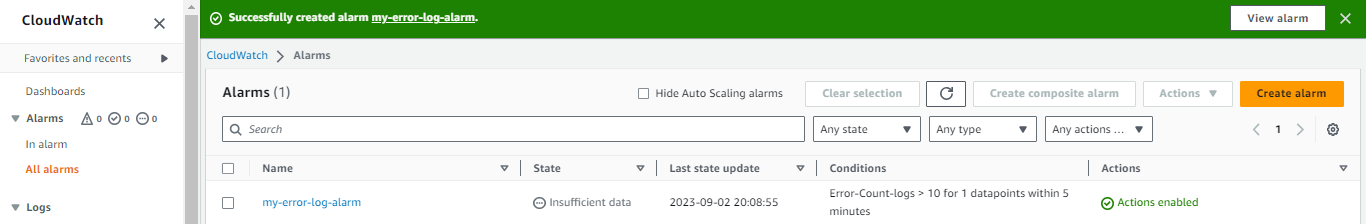
Now you have to specify alarm notification setting so select in alarm and then select sns service topic and the click on next .



Step 12:-

Now gave your alarm name and then click on next and you have see the you configured all setting and then click on create alarm. And your alarm was set.



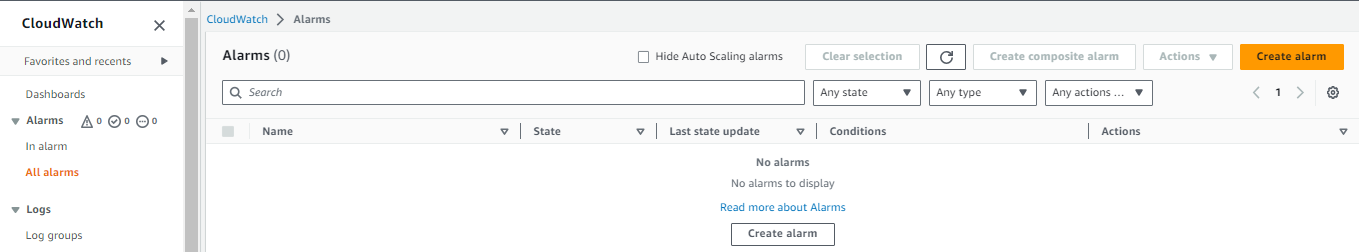


5.S3 Bucket Monitoring:

Configure CloudWatch to monitor the size of objects in an S3 bucket. Create an alarm that triggers when the bucket's total size surpasses 1 GB.

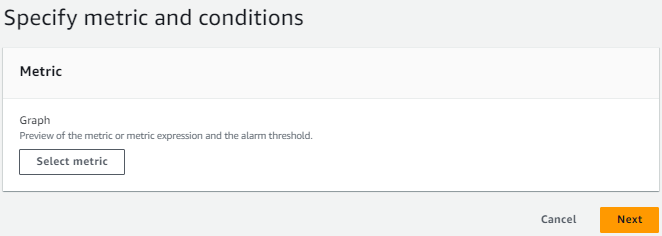
🡺

Step 1:-

Go to CloudWatch service and click on all alarm and then click of create alarm.

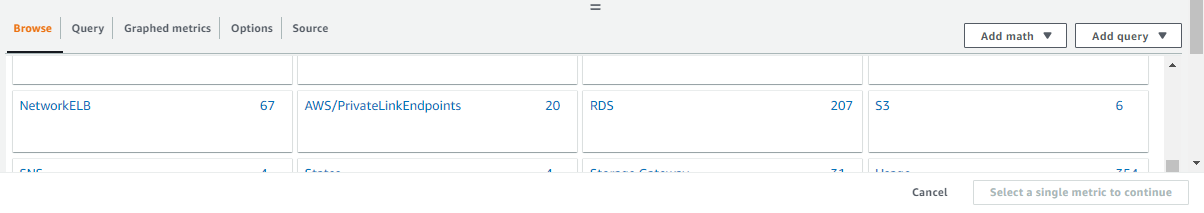
Step 2:-

Now Select metrics and then click on next.



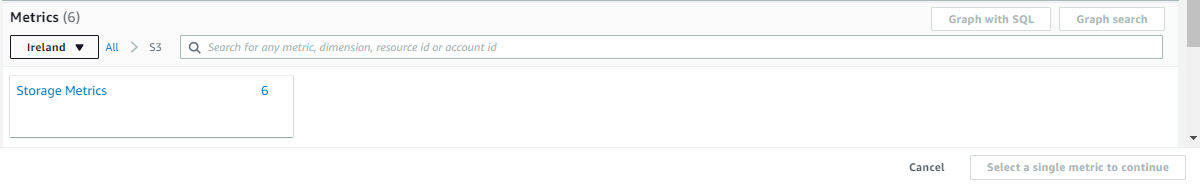
Step 3:-

After that click on s3 service in option.



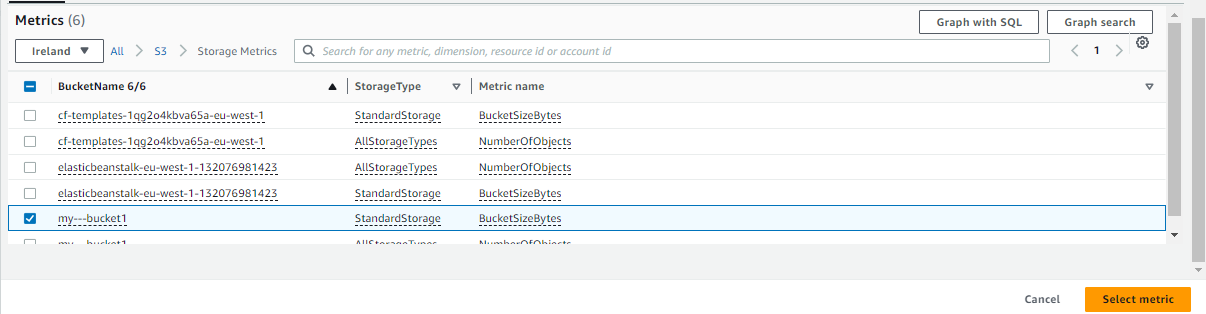
Step 4:-

Now click on storage metrics option.



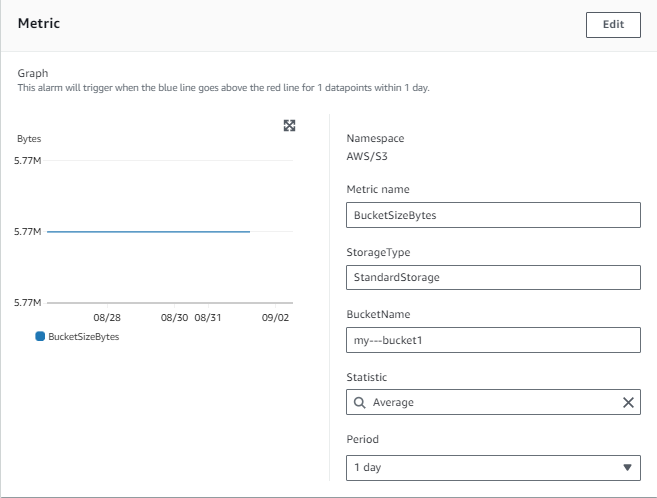
Step 5:-

After thata you have to search your which you have to on metrics of storage in that you have to select as metrics of BucketSizedBytes and then click on select metrics.



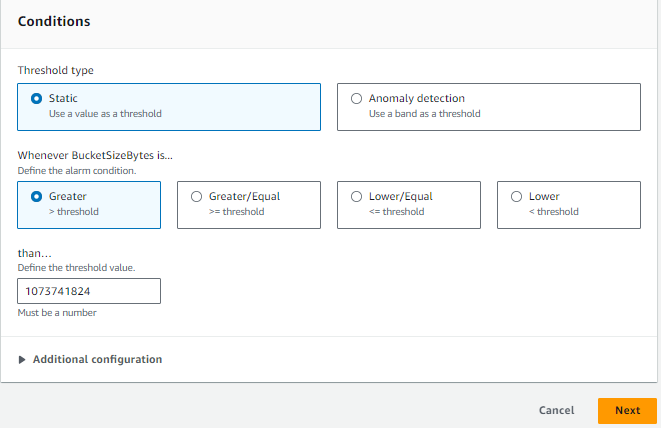
Step 6:-

Now select metrics setting gave it name or leave as it is and then select period of time as 5 minute.



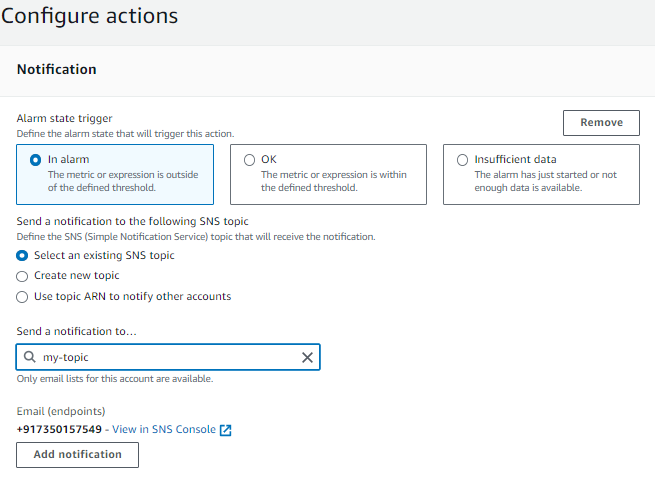
Step 7:-

Now select condition of threshold type as static and then select the alarm was trigger as 1 GB+ space was fill so choose greater than threshold and in than column write value of 1 GB in the unit gigabyte as 1073741824. And then click on next.



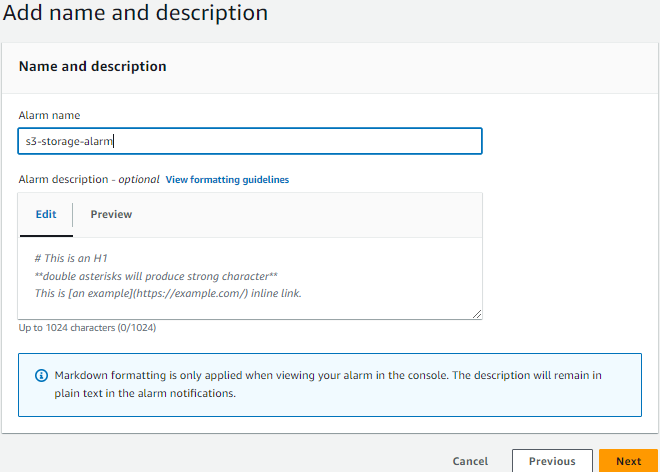
Step 8:-

Now you have specify the notification setting so first select in alarm and after that select sns topic and then click at the end option next.



Step 9:-

Now gave alarm name and then click on next and then see the all configured information and then click on create alarm. And your alarm is set.



6.CloudWatch Dashboard:

Create a CloudWatch dashboard named "ApplicationDashboard" to visualize the following widgets:

Line graph showing the "ResponseTime" custom metric over the last hour.

CPU utilization metric for the RDS instance and EC2 instances.

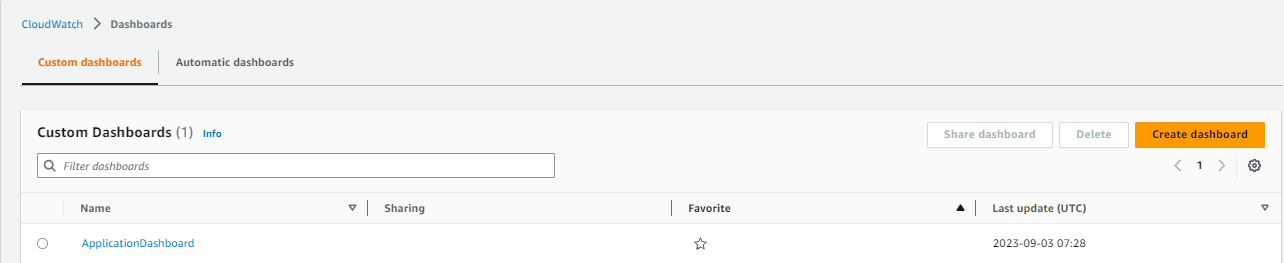
Log-based metric showing the count of "ERROR" messages over the past hour.

An S3 bucket storage usage metric.

🡺

Step 1:-

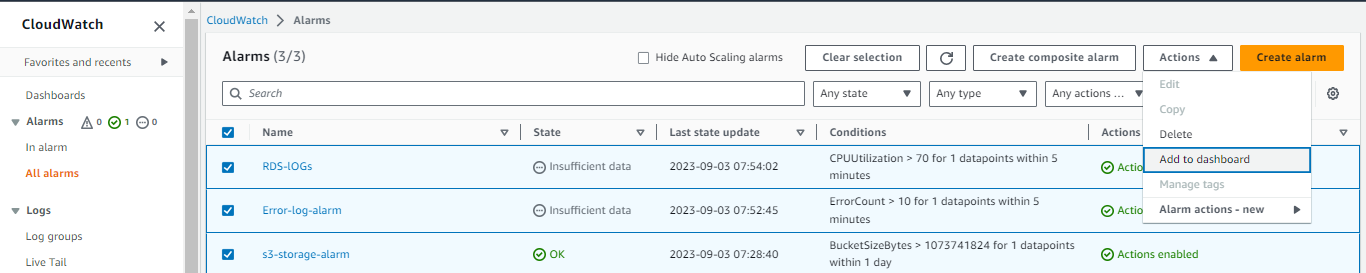
Now we have to create one dashboard name application in which we have to add all widgets we created in the all last task. So first go to cloudwatch service in that click on dashboard session in that click on create dashboard and then gave it dashboard name as “’ApplicationDashboard” and save.





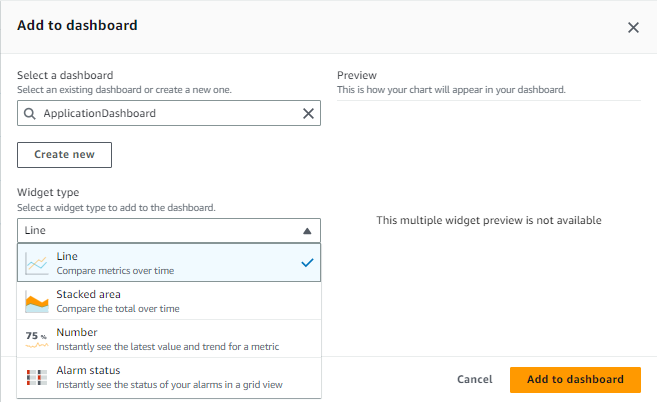
Step 2:-

Now go to all alarm session and select all we created alarm and then click on actions and then select option s add to dashboard.



Step 3:-

And select a dashboard as name ApplictaionDashboard and then select widget type as line click on add to dashboard. Your dashboard has created.



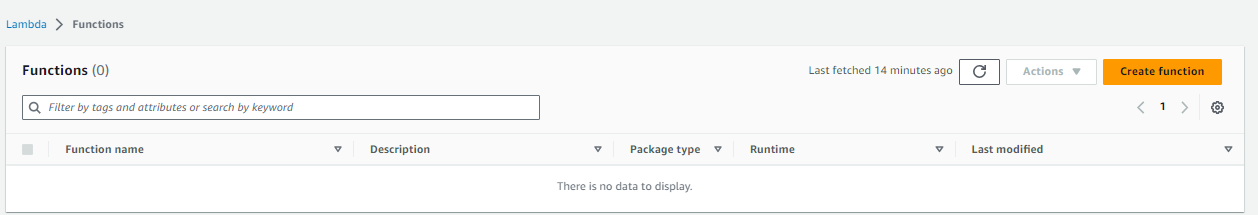
7.Scheduled Event:

Set up a scheduled CloudWatch Events rule that triggers a Lambda function every day at 8 AM UTC. The Lambda function should automatically start a specific EC2 instance.

🡺

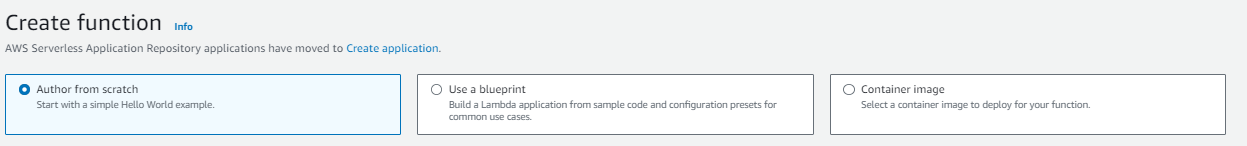
Step 1:-

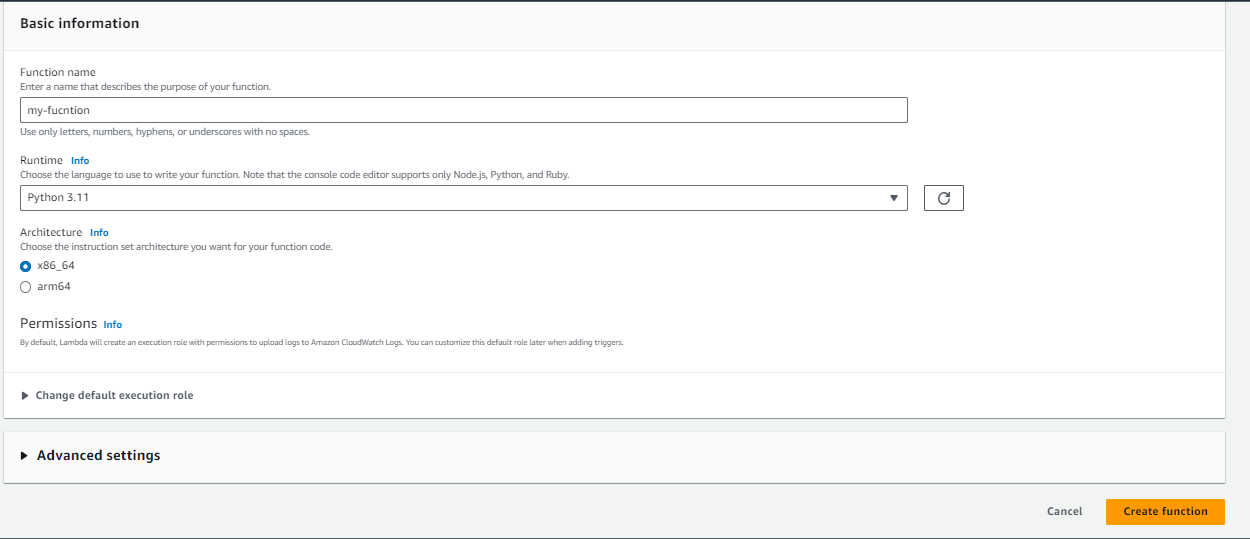
First of all go to lambda service to create lambda function. Click on create function.



Step 2:-

Now you have see the creation setting of lambda function. So first select author from scratch and then gave lambda function name and then select runtime as python and the select architecture as x86\_64 and then click on create.





Step 3:-

Now click on your lambda function and paste a code of python which run instance on event occur. In this code change only instance id. And then click on deploy.

import boto3

ec2 = boto3.client('ec2')

def lambda\_handler(event, context):

# Replace 'your-instance-id' with the ID of your EC2 instance

instance\_id = 'your-instance-id'

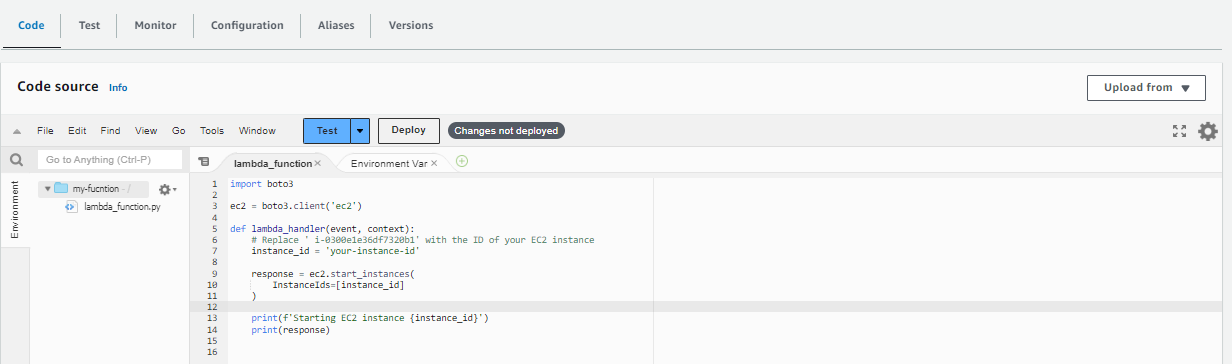
response = ec2.start\_instances(

InstanceIds=[instance\_id]

)

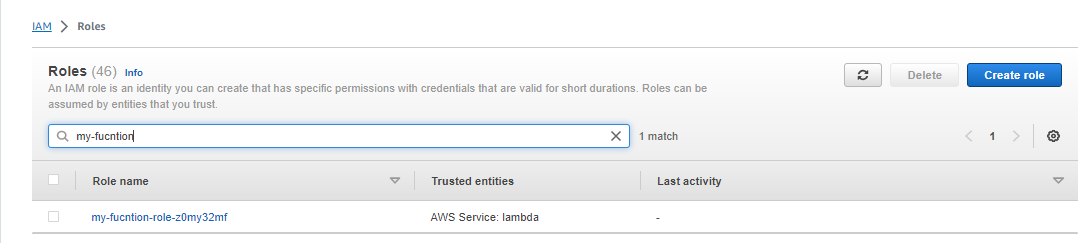
print(f'Starting EC2 instance {instance\_id}')

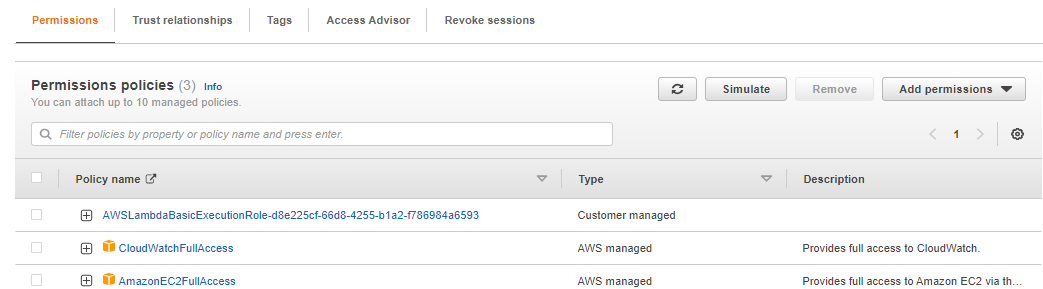
print(response)



Step 4:-

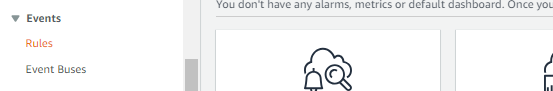
Now you have to gave permission to your lambda function to trigger ec2 instance start. So go iam service and search your role which is attached to your lambda function and gave it permission of ec2 full access and clouwd access.





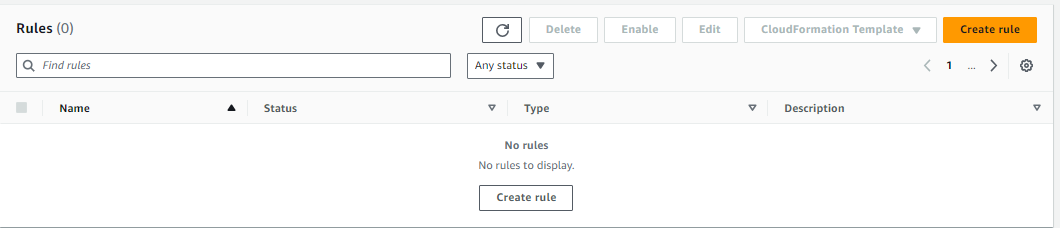
Step 5:-

Now you have to create event to trigger your lambda function on time. So go to cloudwatch service and click on events and then click on rules to create rule.



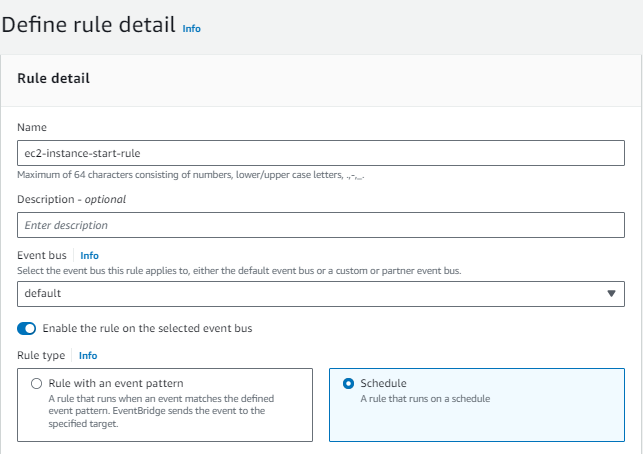
Step 6:-

Now click on create rule .



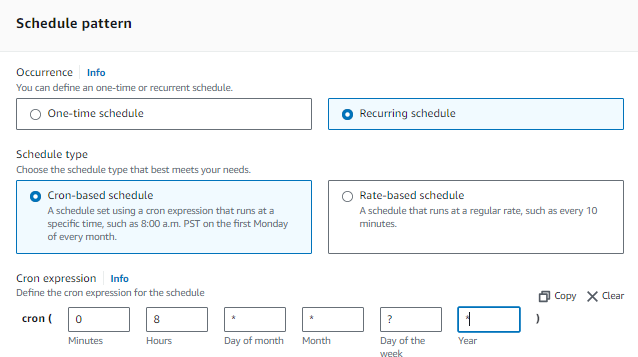
Step 7:-

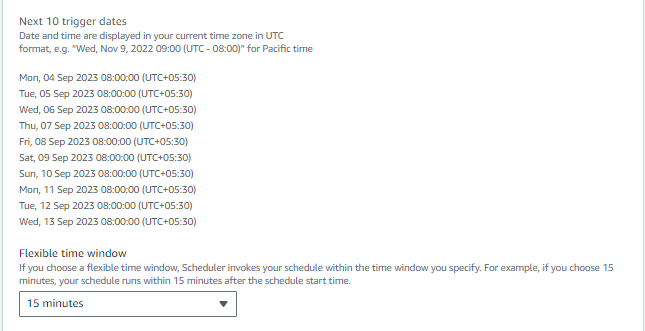
Now you specify the setting of creating event rule so first gave it name and then select rule type as schedule. And then click on next.



Step 8:-

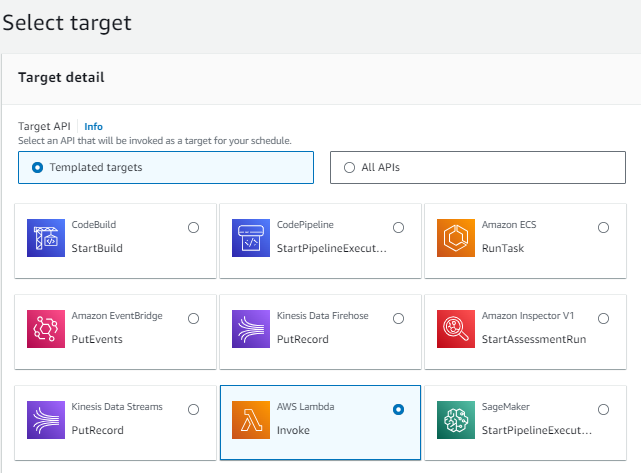
After that you have to select schedule pattern as recurring schedule and in that select cron based schedule and then gave the cron tab fields as 0 8 \* \* ? \*. And then you will see the your next 10 trigger dates and next to that you will see the flexible time window means from trigger event run within that time so choose as 15 minute. After that click on next.

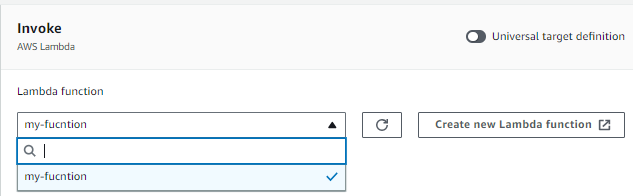




Step 9:

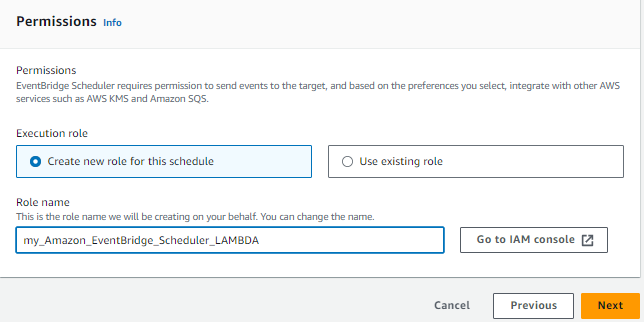
Now you have to select target so select target as lambda service anad then select your lambda function which you have too trigger.





Step 10:-

After that last step is choose role to it or create new role for gave it permission so I have create new. And then click on next and then you will all configure info see all oky and then click on create event. And your event is created.



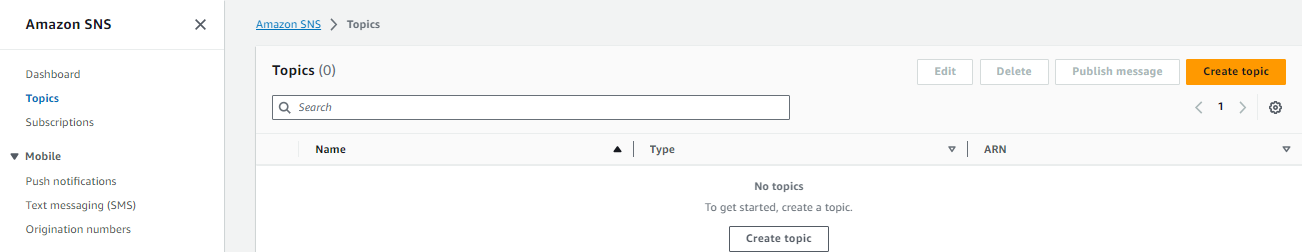
8.Notifications:

Configure CloudWatch Alarms to send notifications to an SNS topic whenever any alarm state is triggered.

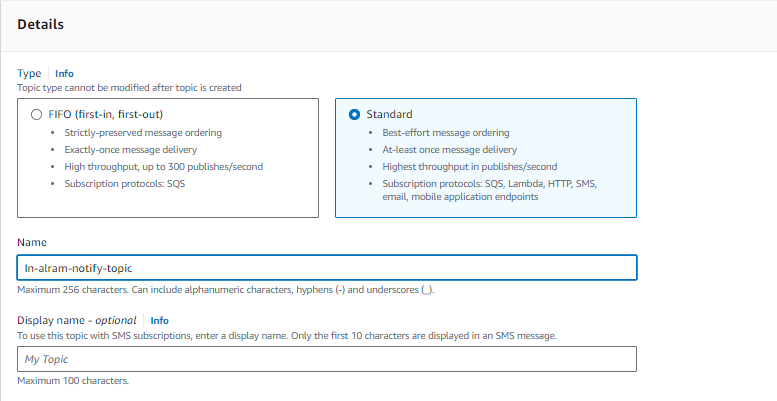
🡺

Step 1:-

First of all go to SNS service and then click on create topic.

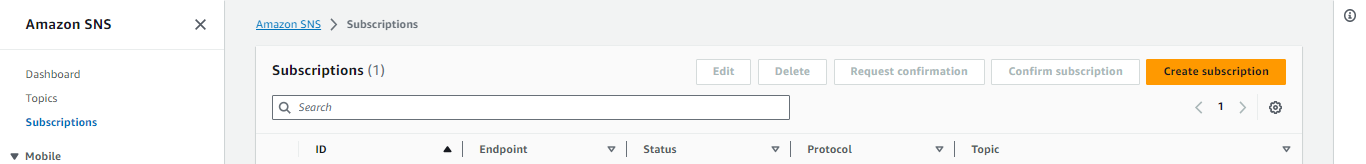


Step 2:-

Now select type of topic as standard and then give it name and click on create.

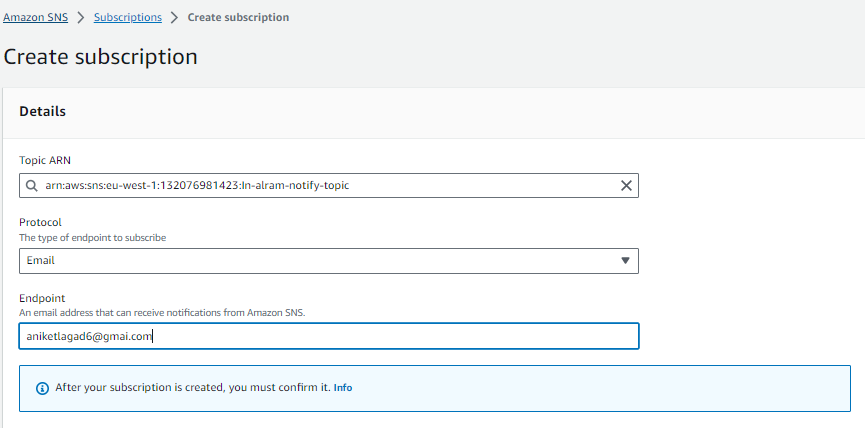
Step 3:-

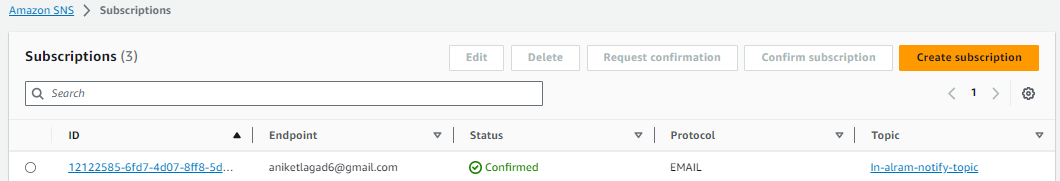
Now you have subscribe your topic to send notification on email or other.



Step 4:-

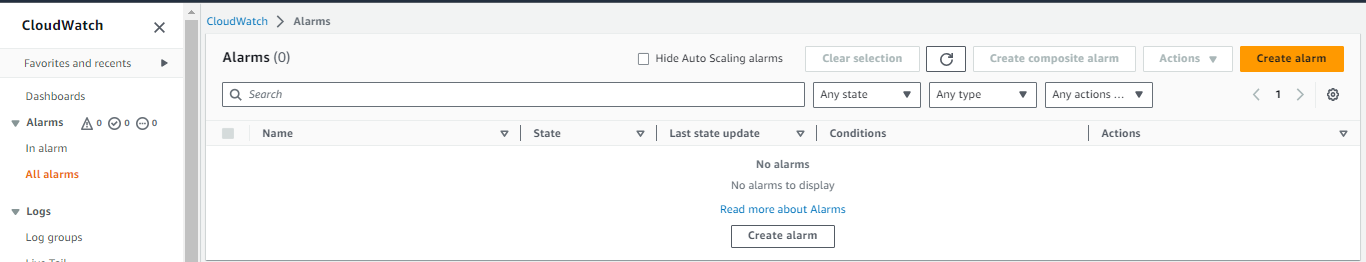
And then you have see the create subscription setting so first select topic ARN and then choose protocol as email and then gave endpoint as your gmail. And then go to your email and conform subscription.





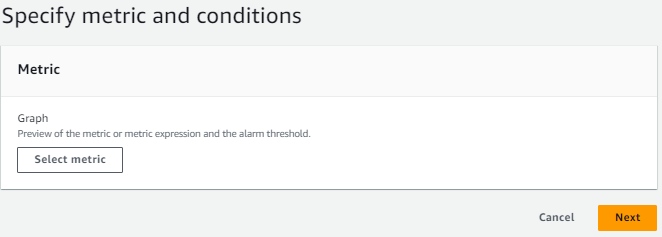
Step 5:-

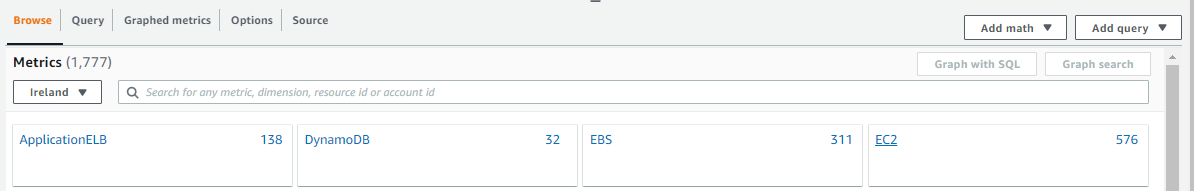
Now go to cloudwatch service and then click on create alarm.



Step 6:-

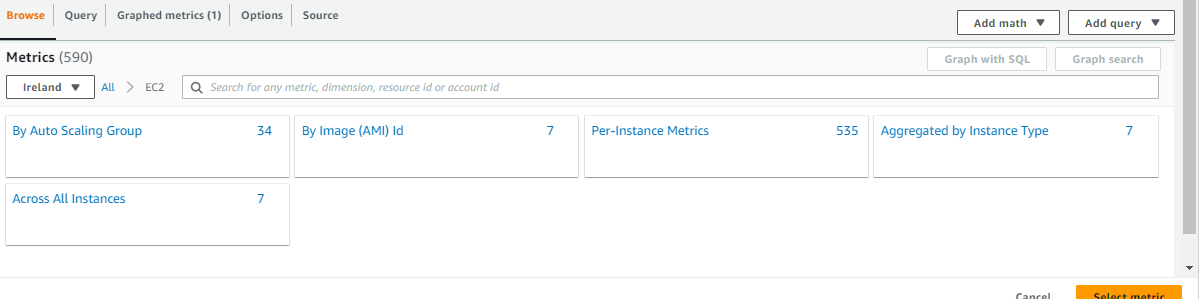
Then click on select metrics. And then click on ec2 service option.





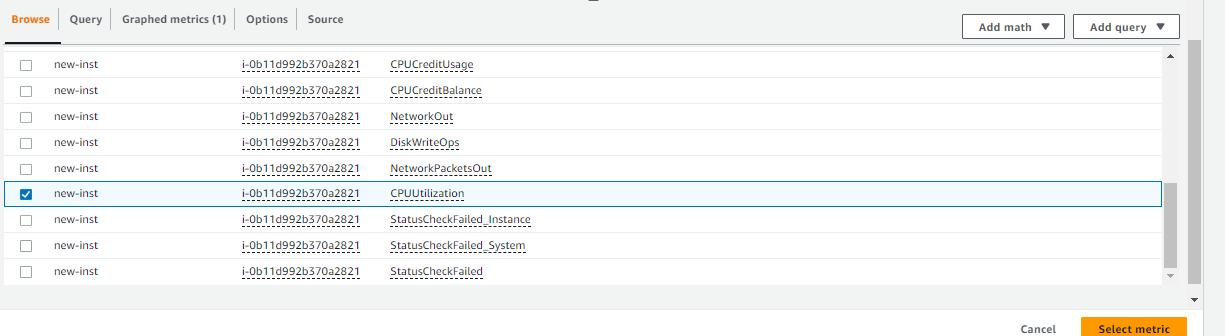
Step 7:-

And after that click on per-instance metrics.



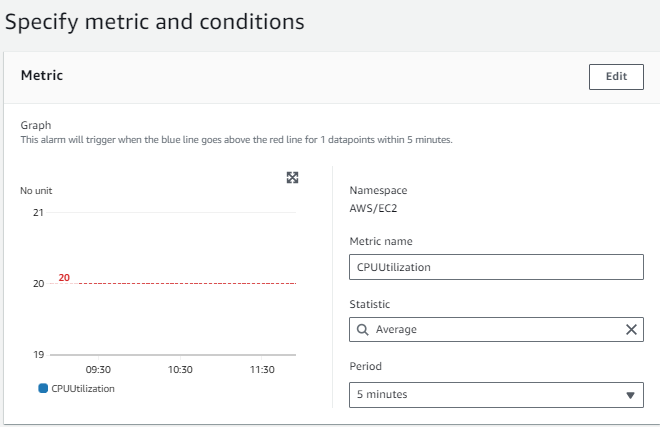
Step 8:-

And then in search bar passe your instance and id and ten select CPUUtillization of that instance.



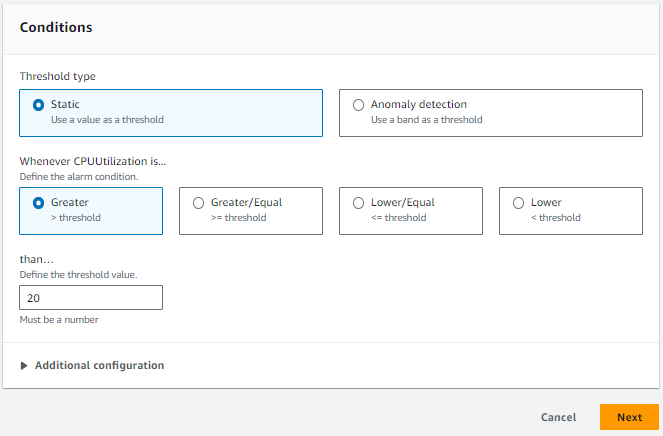
Step 9:-

After that specify metric and condition or leave as it is default.



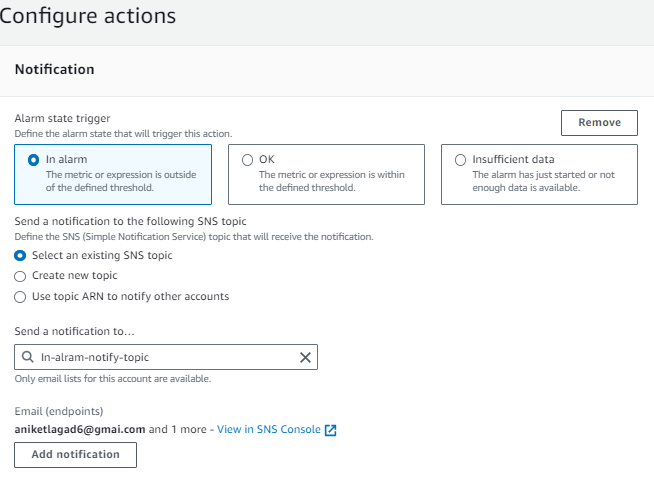
Step 10:-

After that specify condition so select threshold type and then select greater threshold and after that in than column select 20 value.



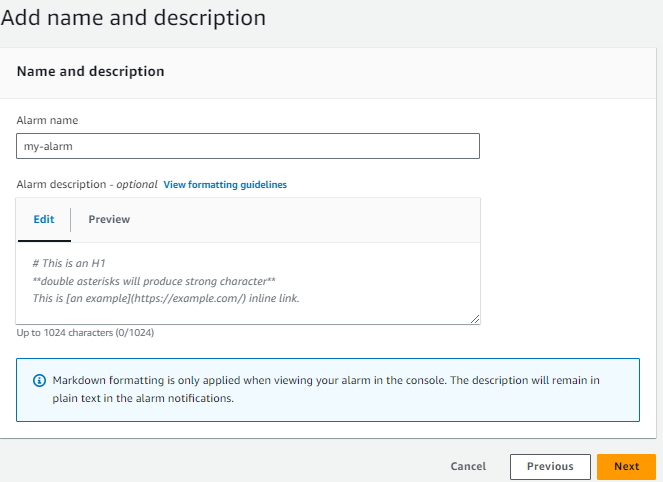
Step 11:-

Now configure alarm notification trigger setting so select alarm state trigger as in alarm and the select we have created sns topic and then click on next.



Step 12:-

Then gave alarm name and then click on next and then click on next check all configured info and then click create alarm. and your alarm



\*\*\*THE END\*\*\*