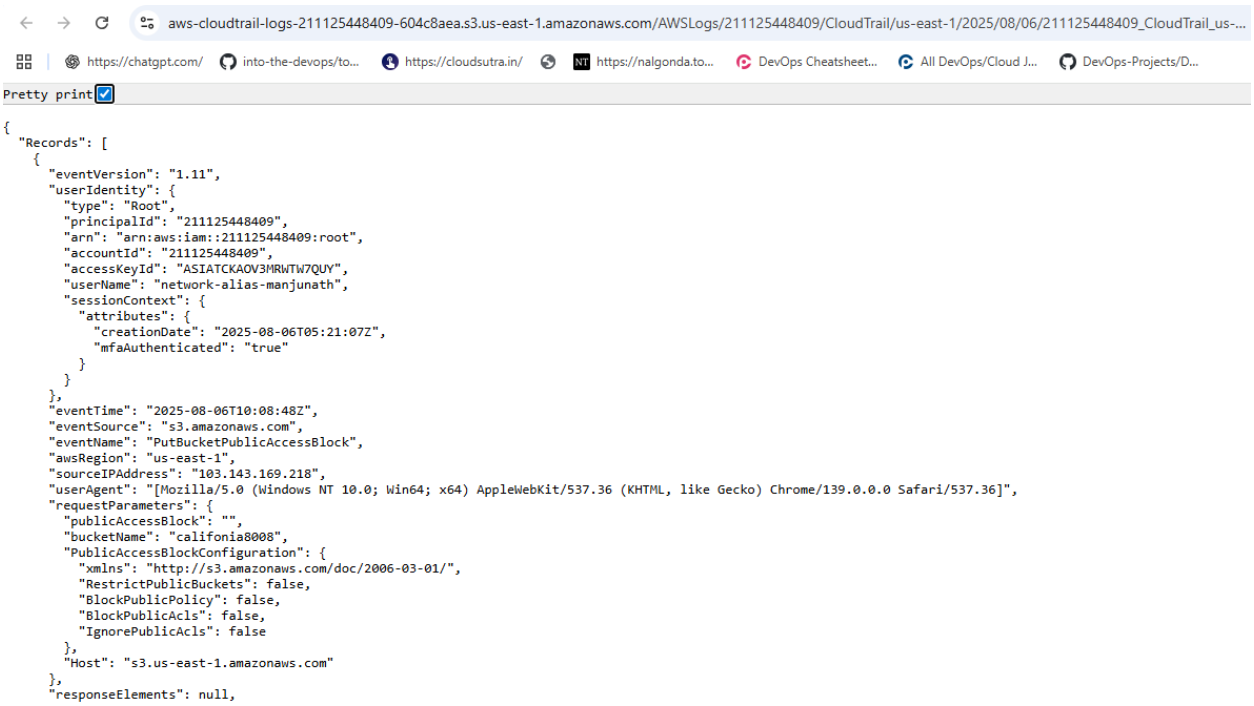
1) Enable cloudtrail monitoring and store the events in s3 and cloudwatch log events.

S3



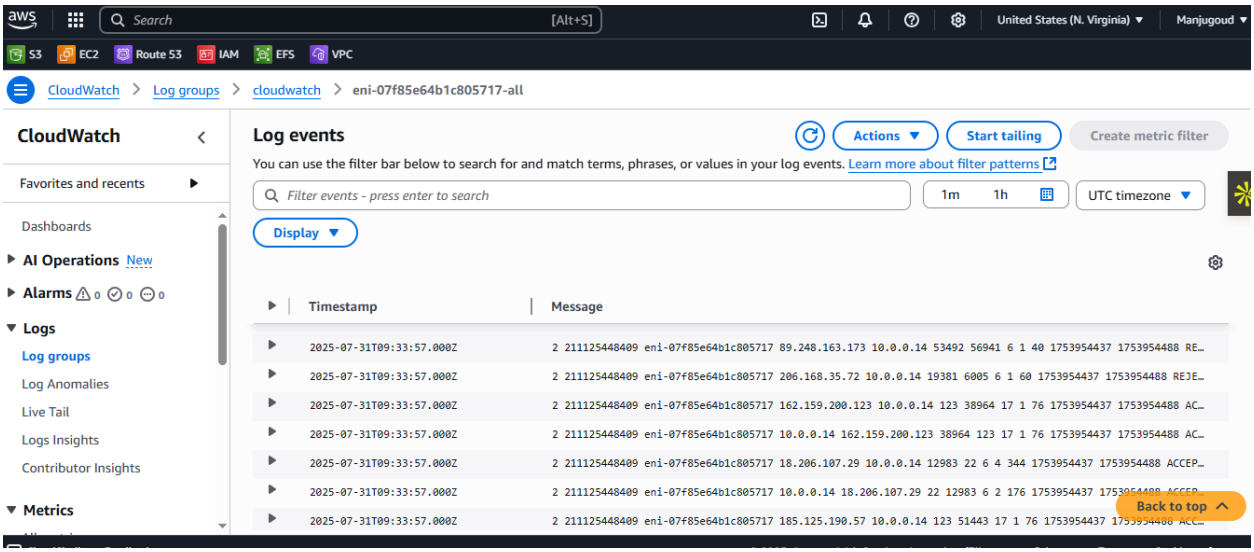
aws-cloudtrail-logs-211125448409-604c8aea.s3.us-east-1.amazonaws.com/AWSLogs/211125448409/CloudTrail/us-east-1/2025/08/06/211125448409_CloudTrail_us-...

https://chatgpt.com/ into-the-devops/to... https://cloudsutra.in/ https://nalgonda.to... DevOps Cheatsheet... All DevOps/Cloud J... DevOps-Projects/D...

Pretty print


```
{
  "Records": [
    {
      "eventVersion": "1.11",
      "userIdentity": {
        "type": "Root",
        "principalId": "211125448409",
        "arn": "arn:aws:iam::211125448409:root",
        "accountId": "211125448409",
        "accessKeyId": "ASIATCKAOV3MRWTW7QUY",
        "userName": "network-alias-manjunath",
        "sessionContext": {
          "attributes": {
            "creationDate": "2025-08-06T05:21:07Z",
            "mfaAuthenticated": "true"
          }
        }
      },
      "eventTime": "2025-08-06T10:08:48Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucketPublicAccessBlock",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "103.143.169.218",
      "userAgent": "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36]",
      "requestParameters": {
        "publicAccessBlock": "",
        "bucketName": "califonia8008",
        "PublicAccessBlockConfiguration": {
          "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
          "RestrictPublicBuckets": false,
          "BlockPublicPolicy": false,
          "BlockPublicAcls": false,
          "IgnorePublicAcls": false
        },
        "Host": "s3.us-east-1.amazonaws.com"
      },
      "responseElements": null,
```


Cloudwatch



aws Search [Alt+S] United States (N. Virginia) Manjugoud

S3 EC2 Route 53 IAM EFS VPC

CloudWatch > Log groups > cloudwatch > eni-07f85e64b1c805717-all

CloudWatch

Favorites and recents

Dashboards

AI Operations New

Alarms 0 0 0

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

Log events

Actions Start tailing Create metric filter

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

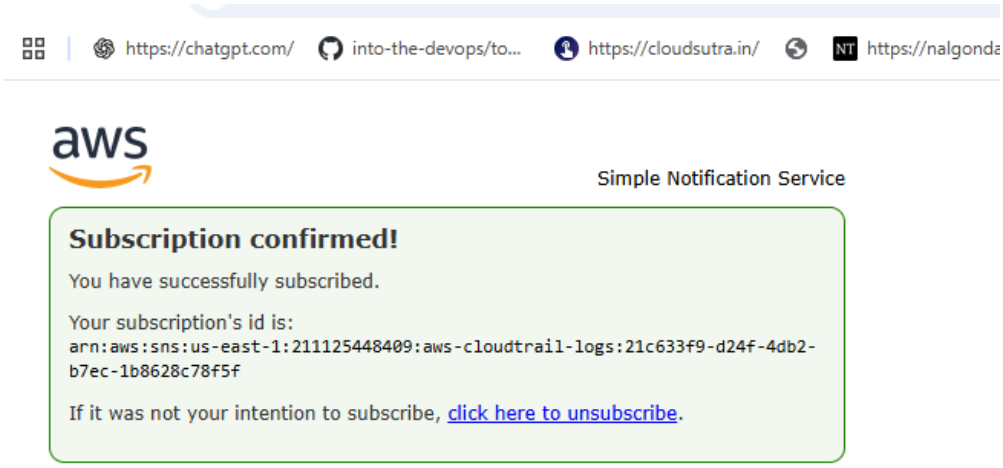
Filter events - press enter to search 1m 1h UTC timezone

Display

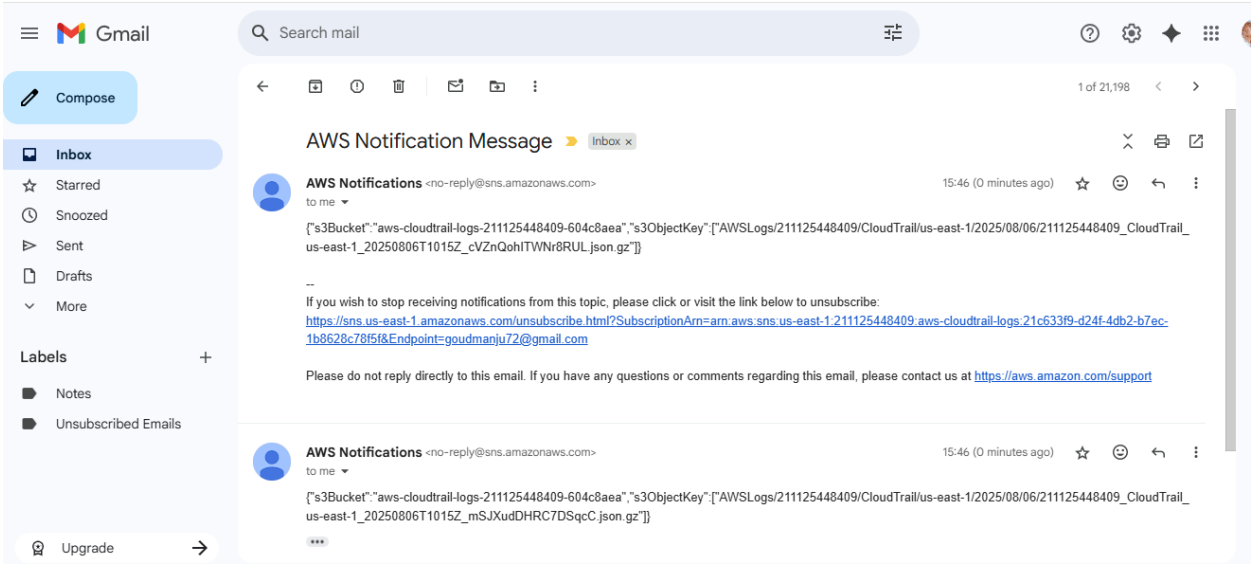
Timestamp	Message
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 89.248.163.173 10.0.0.14 53492 56941 6 1 40 1753954437 1753954488 RE…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 206.168.35.72 10.0.0.14 19381 6005 6 1 60 1753954437 1753954488 REJE…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 162.159.200.123 10.0.0.14 123 38964 17 1 76 1753954437 1753954488 AC…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 10.0.0.14 162.159.200.123 38964 123 17 1 76 1753954437 1753954488 AC…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 18.206.107.29 10.0.0.14 12983 22 6 4 344 1753954437 1753954488 ACCEP…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 10.0.0.14 18.206.107.29 22 12983 6 2 176 1753954437 1753954488 ACCEP…
2025-07-31T09:33:57.000Z	2 211125448409 eni-07f85e64b1c805717 185.125.190.57 10.0.0.14 123 51443 17 1 76 1753954437 1753954488 ACC…

Back to top

2) Enable SNS for cloudtrial to send alert on email.

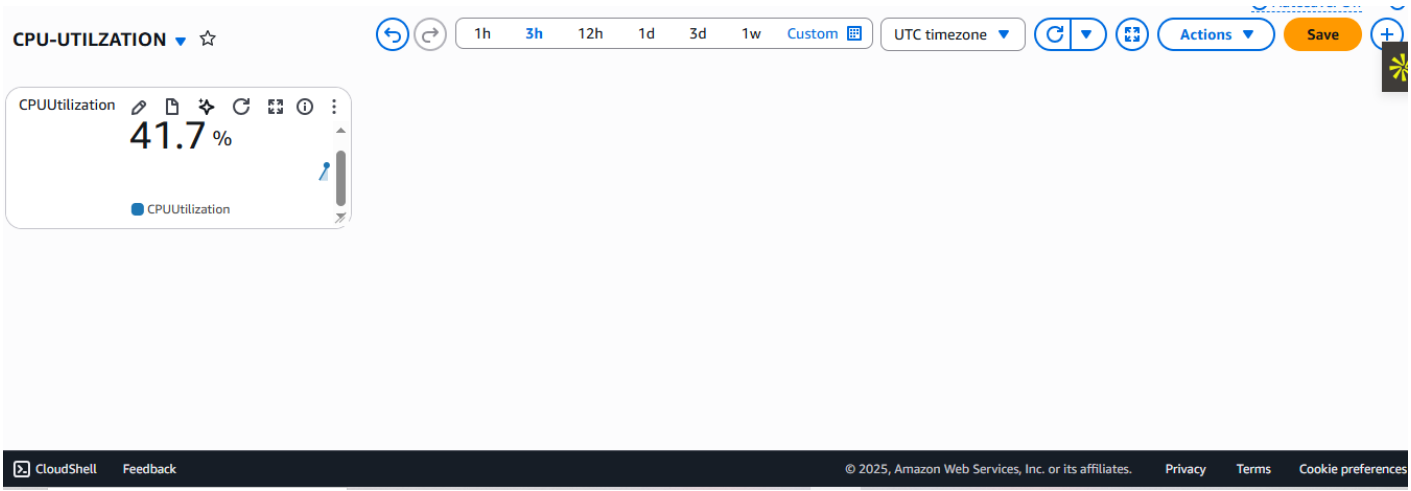


0



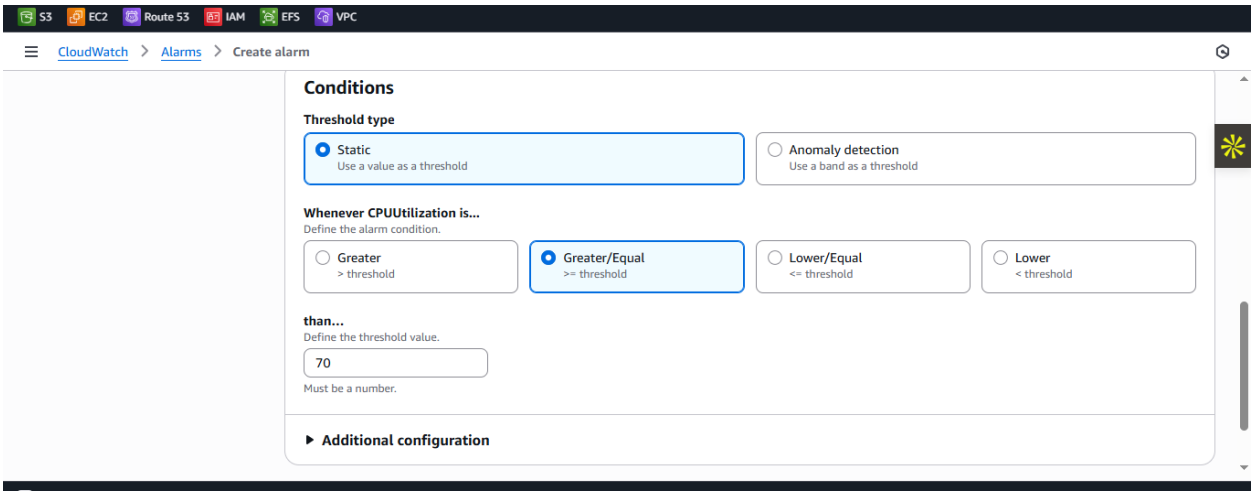
3) Configure cloud watch monitoring and record the cpu utilization and other metrics of ec2.

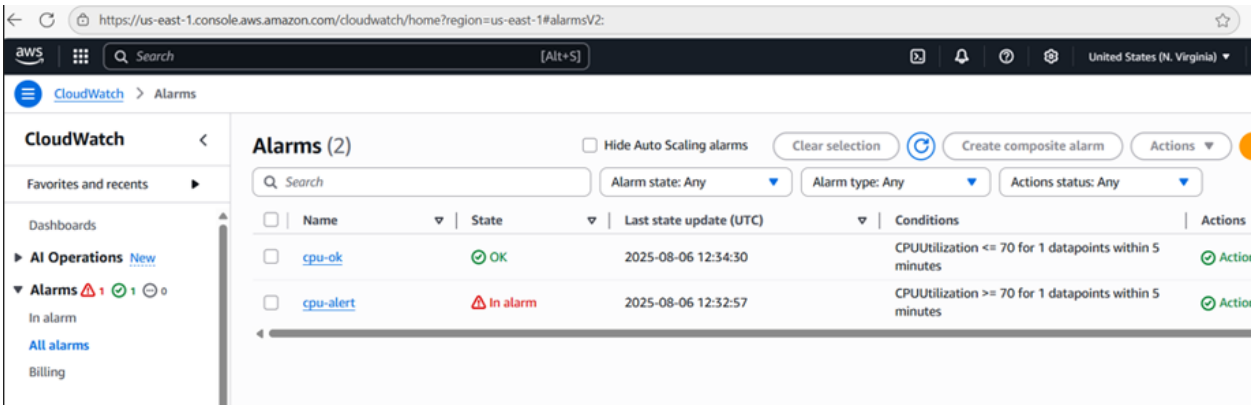
```
[ec2-user@ip-172-31-19-32 ~]$
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null & -d
[9] 26313
-bash: -d: command not found
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null & -d
[10] 26315
-bash: -d: command not found
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null & -d
[11] 26317
-bash: -d: command not found
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null & -d
[12] 26319
-bash: -d: command not found
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null &
[13] 26321
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null &
[14] 26322
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null &
[15] 26323
[ec2-user@ip-172-31-19-32 ~]$ yes > /dev/null &
[16] 26324
[ec2-user@ip-172-31-19-32 ~]$
```



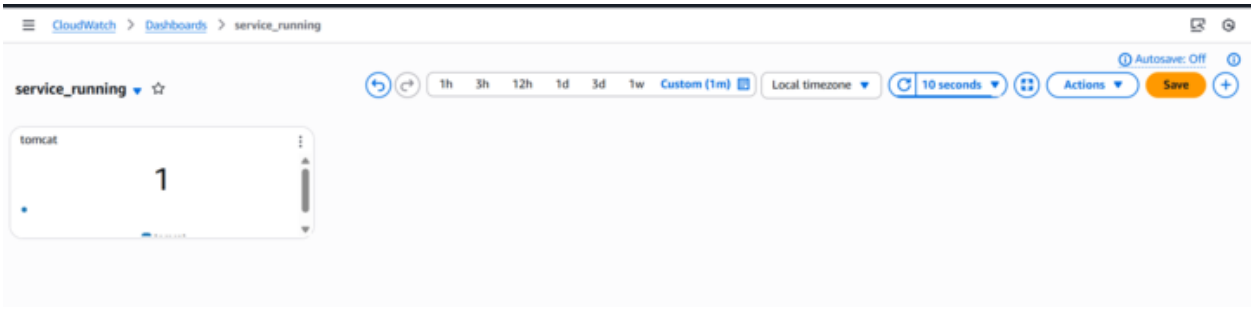
To create a CPU utilization Dashboard we need to go to cloudwatch Dashboard--->create Dashboard.

4) Create one alarm to send alert to email if the cpu utilization is more than 70 percent.

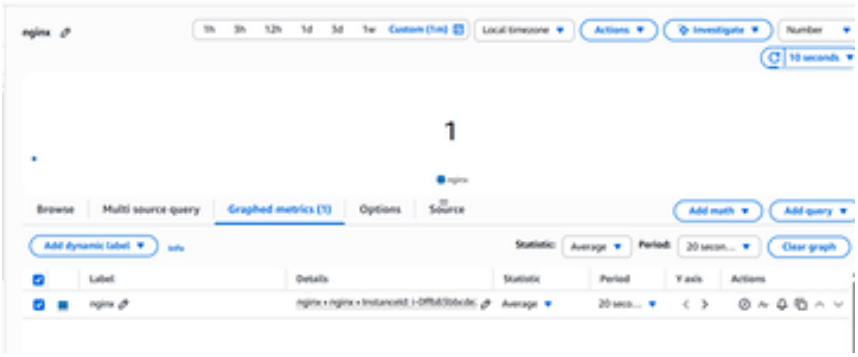




5) Create Dashboard and monitor tomcat service whether it is running or not and send the alert.



6) Create Dashboard and monitor nginx service to send the alert if nginx is not running.


nginx
1h
3h
12h
1d
3d
1w
Custom (1m)
Local timezone
Actions
Investigate
Number
10 seconds
1
nginx
Browse
Multi source query
Graphed metrics (1)
Options
Source
Add math
Add query
Add dynamic label
Info
Statistic:
Average
Period:
20 secon...
Clear graph
Label
Details
Statistic
Period
Y axis
Actions
nginx
Average
20 seco...