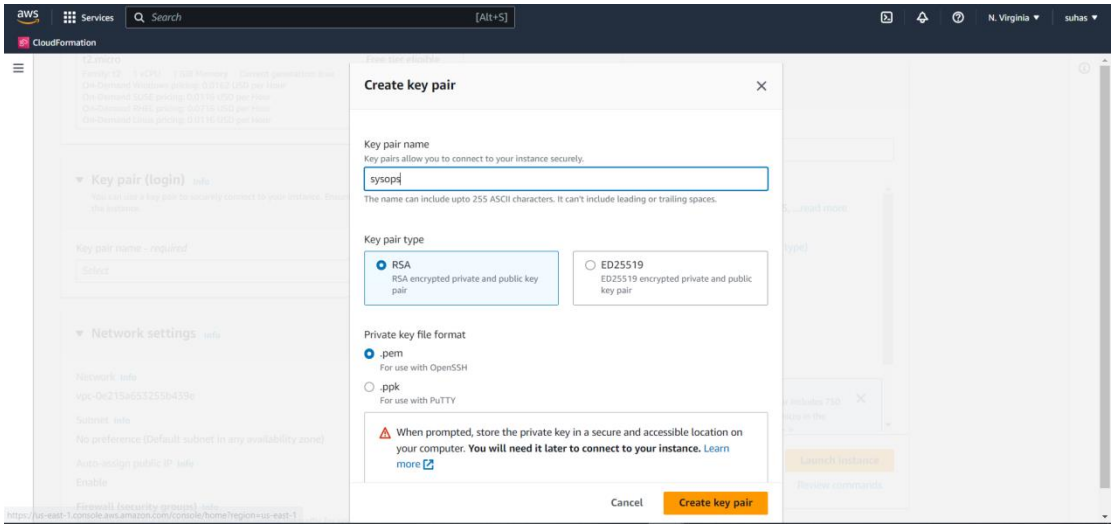
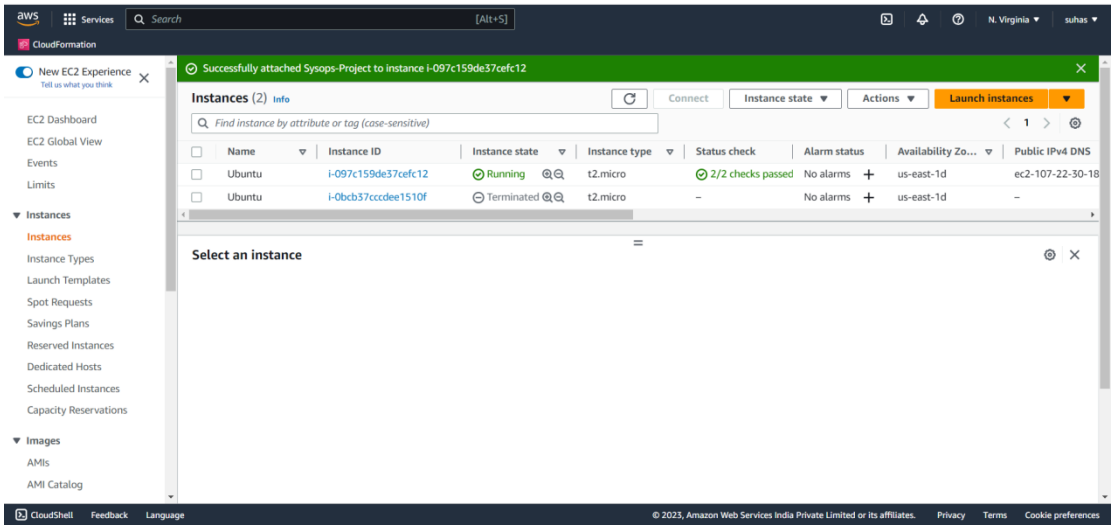
Q)Implement CloudWatch to monitor EC2 instance logs for failed SSH attempts with Alarm notification.

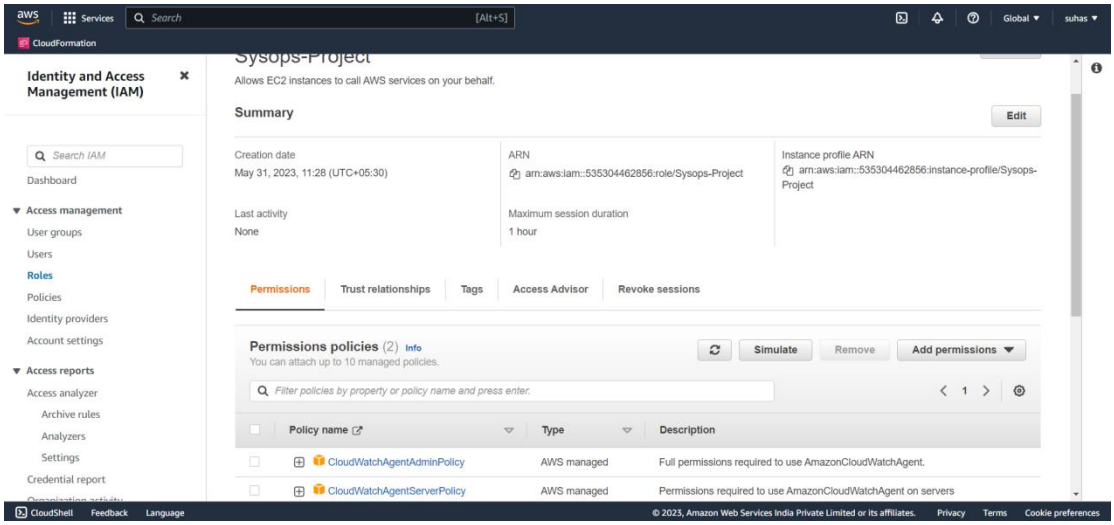
A)

Create an EC2 instance with UBUNTU AMI and launch it. (Keep .pem file for key pair)

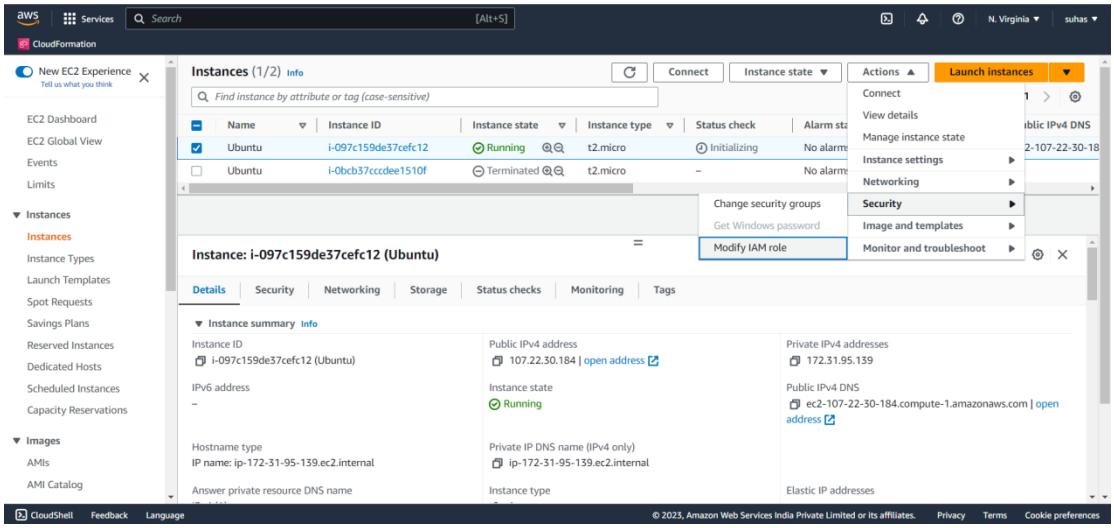


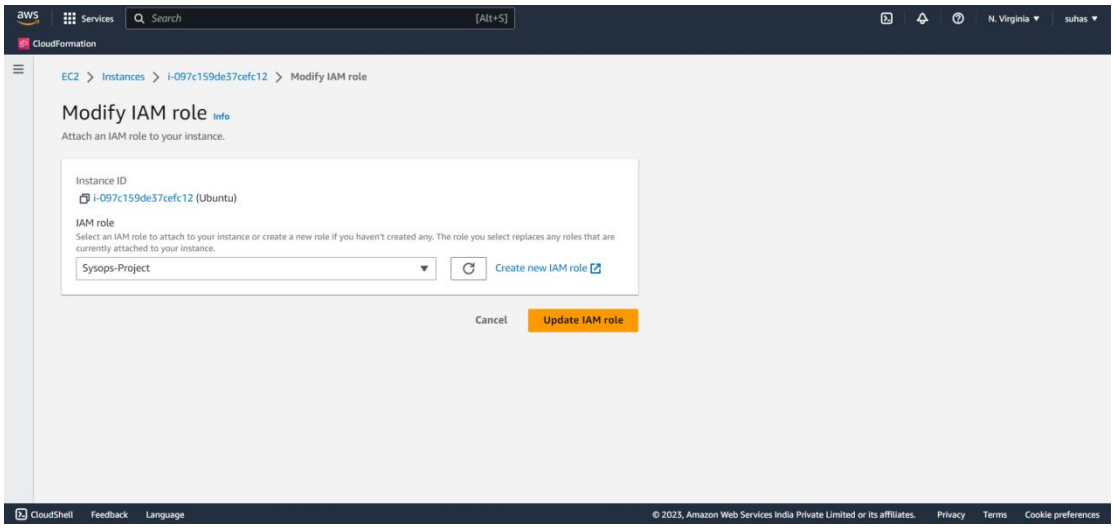


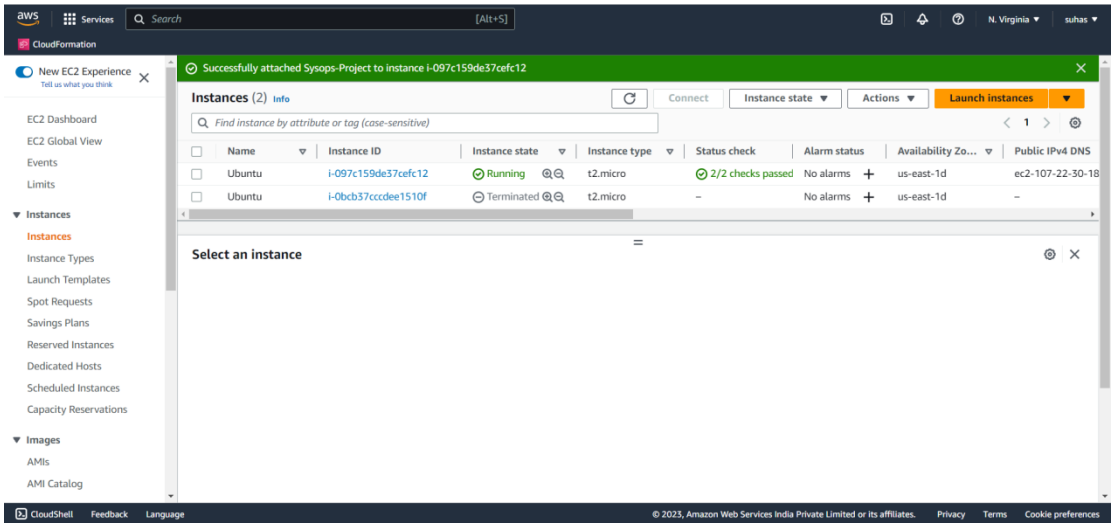
Create an IAM Role with (EC2) Use Case and add CloudWatchAgentAdminPolicy and CloudWatchAgentServerPolicy policies to the role.



Attach this role to the EC2 instance you have created.







Connect to the EC2 instance using EC2 Instance Connect and execute following commands to install and configure wizard for Cloudwatch Agent into the ec2 instance -

1) sudo apt update

2) sudo apt install -y unzip

3) wget https://s3.amazonaws.com/amazoncloudwatch-agent/ubuntu/amd64/latest/amazon-cloudwatch-agent.deb

4) sudo dpkg -i amazon-cloudwatch-agent.deb

5) sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard

Enter the log file path in wizard -

/var/log/auth.log

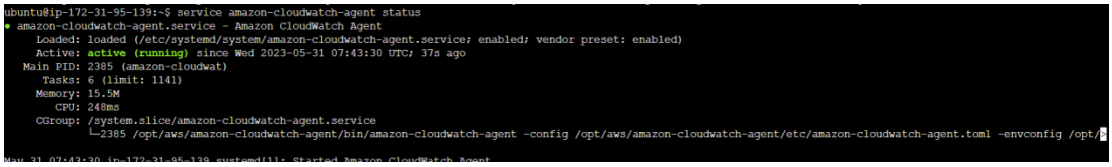
Once Cloudwatch Agent configuration is over -

Enter the Fetch command :

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

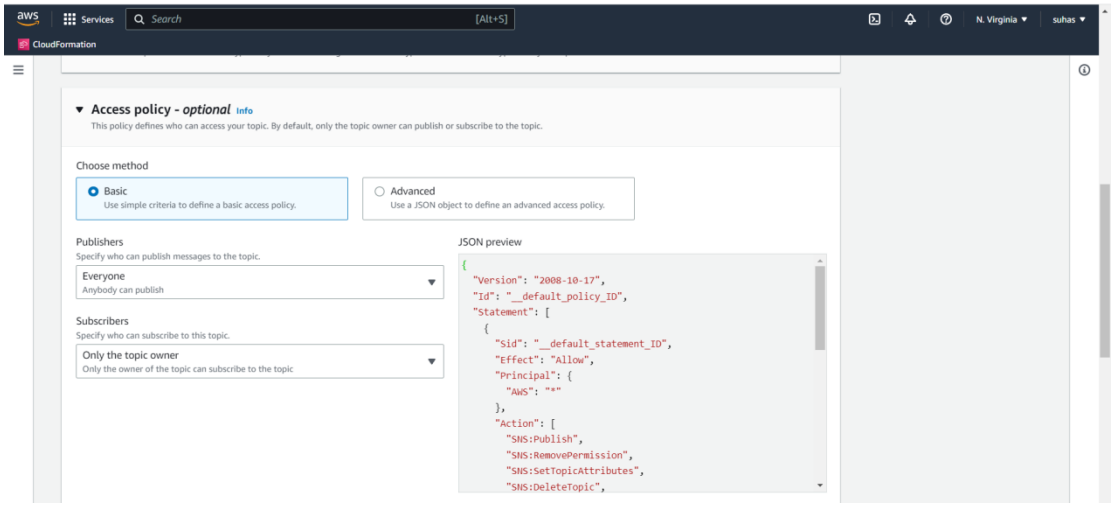
Enter the command to check Status -

service amazon-cloudwatch-agent status

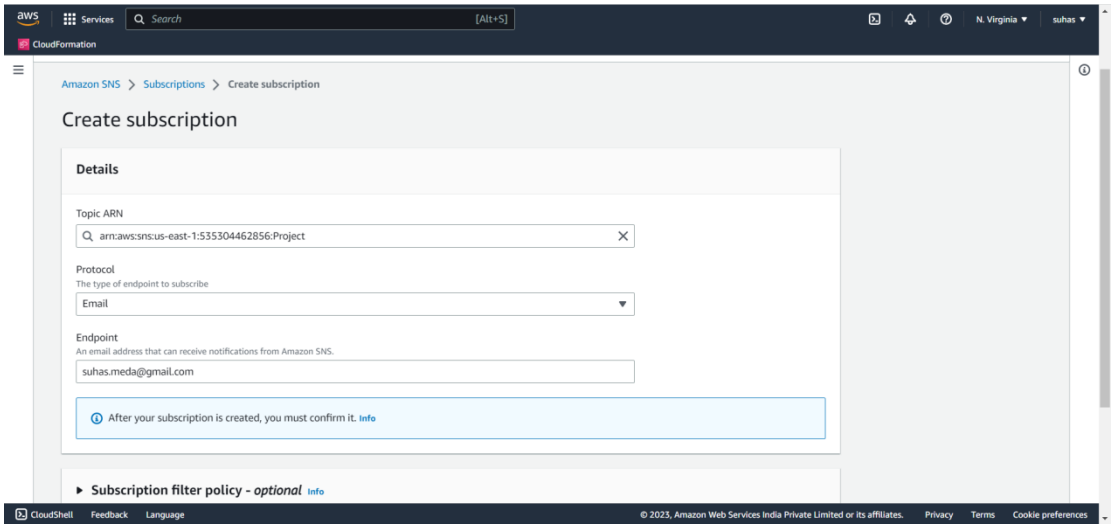


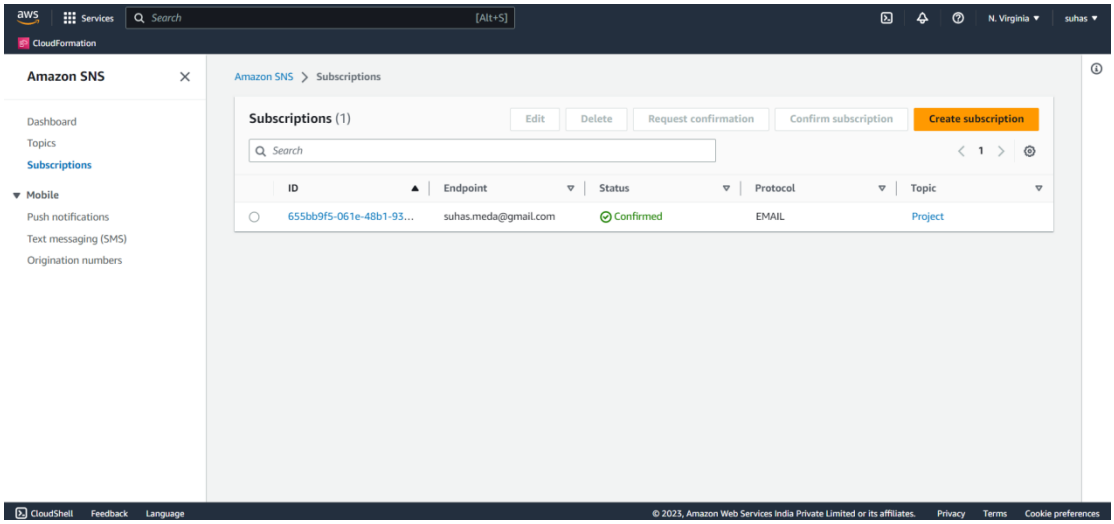
Should display “active (running) ”

Create SNS Topic -

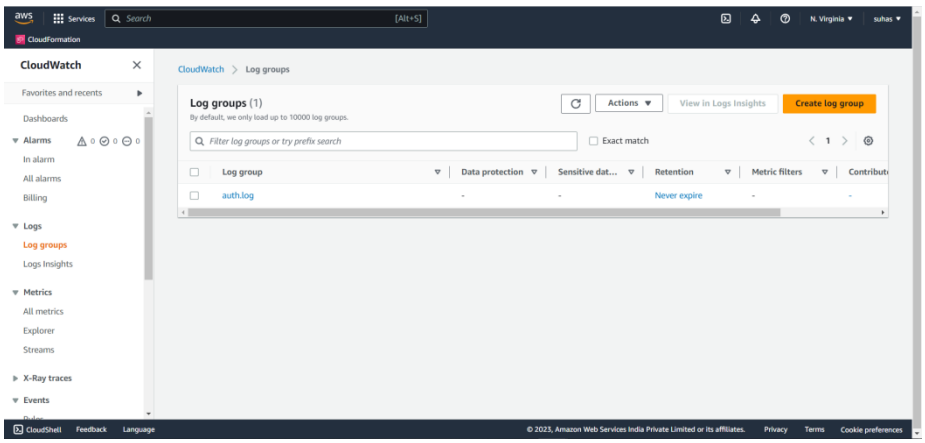


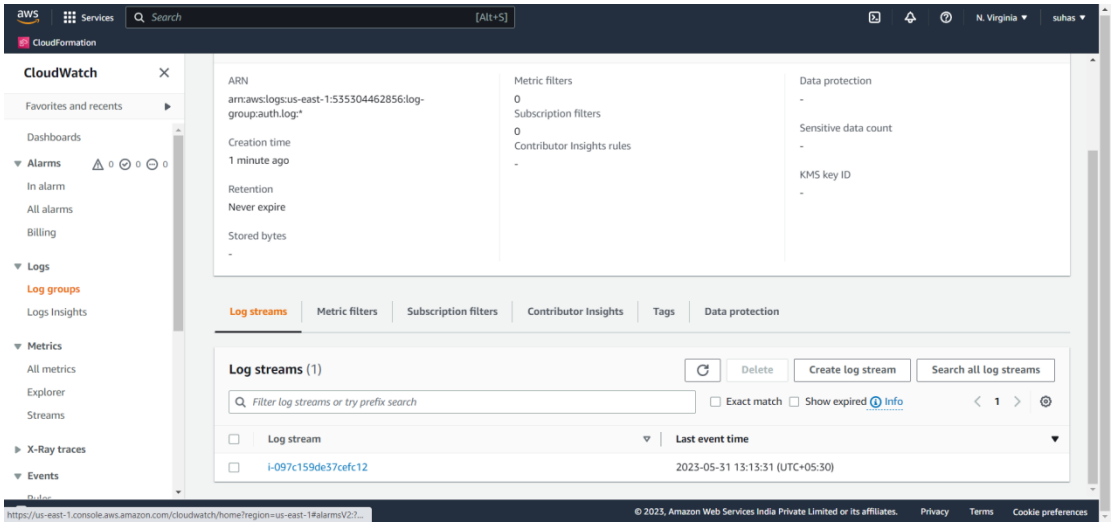
Once SNS Topic has been created, create a Subscription for the topic -

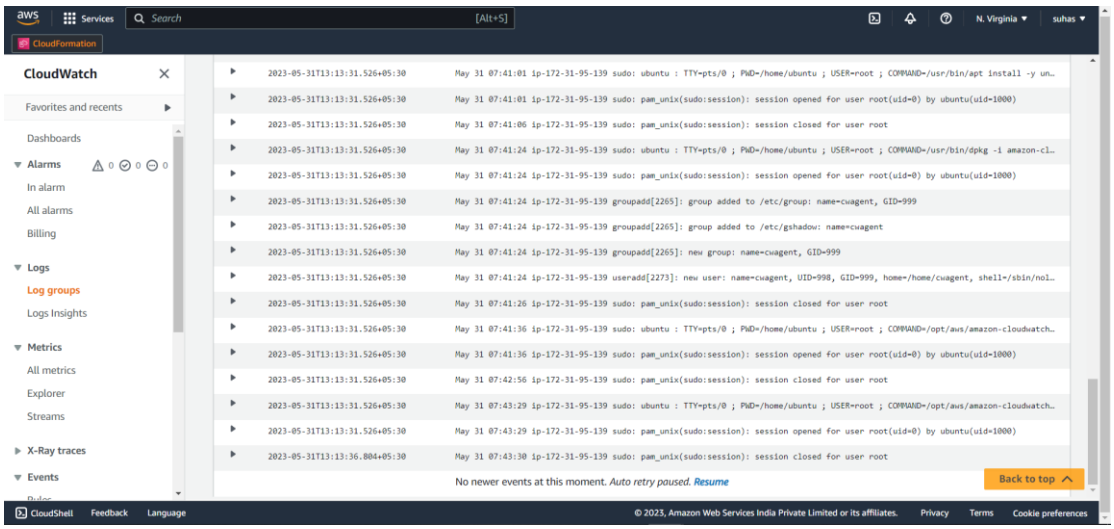




Go to Cloudwatch - Log Groups ->We can see a log group called "auth.log" has been created.Click on the log group - we can see a Log stream has been created as well by default according to configuration given in the Wizard.







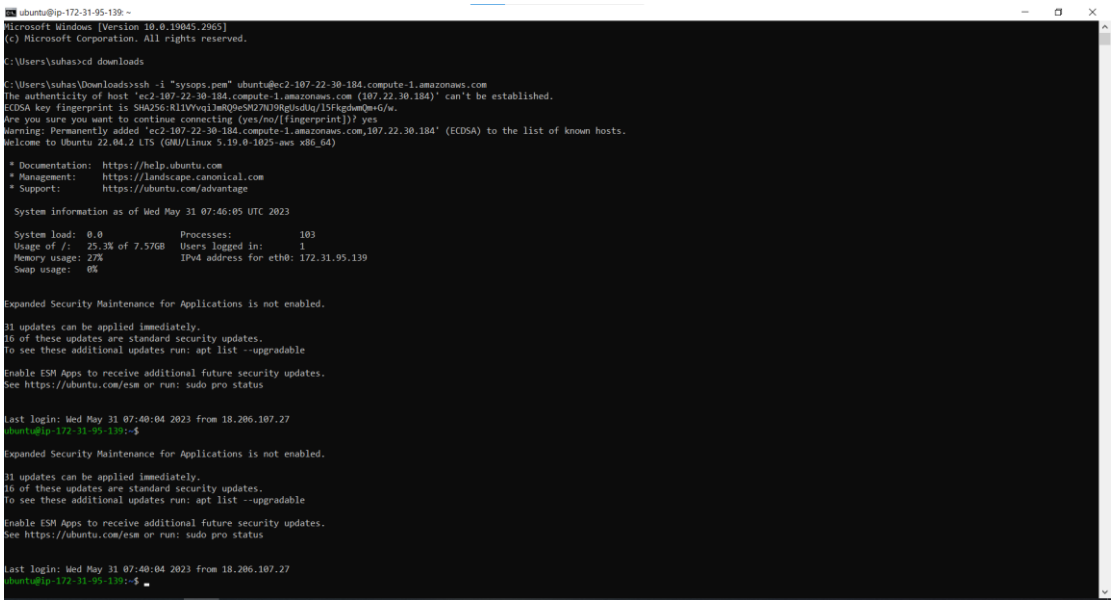
Go to ec2 instance and right click to connect.Then go to SSH Client tab and copy Example command.

ssh -i "sysops.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com

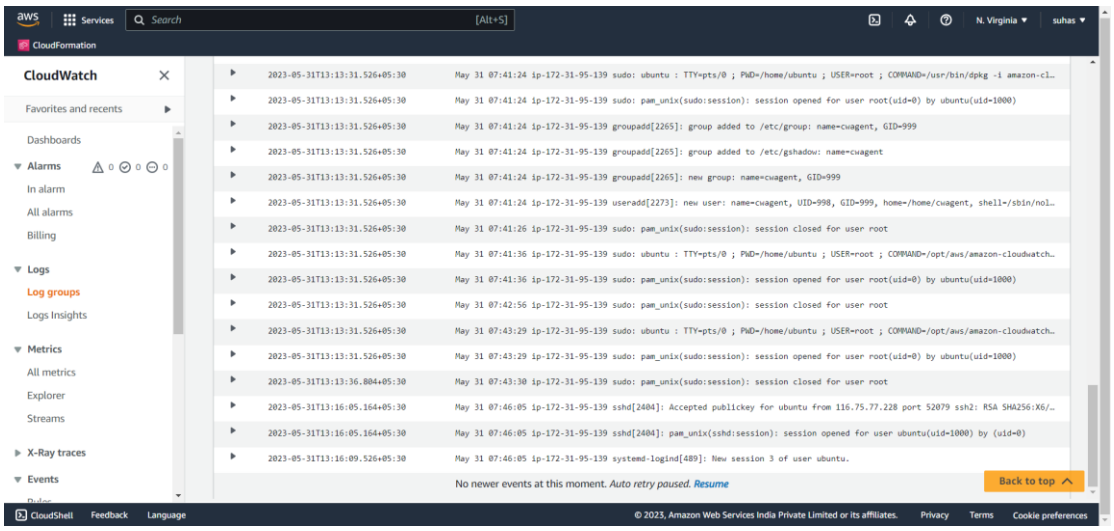
Open Command prompt-

Type command - cd downloads (location where your .pem file is located)

Paste Example command you had copied from SSH Client Tab in Ec2.

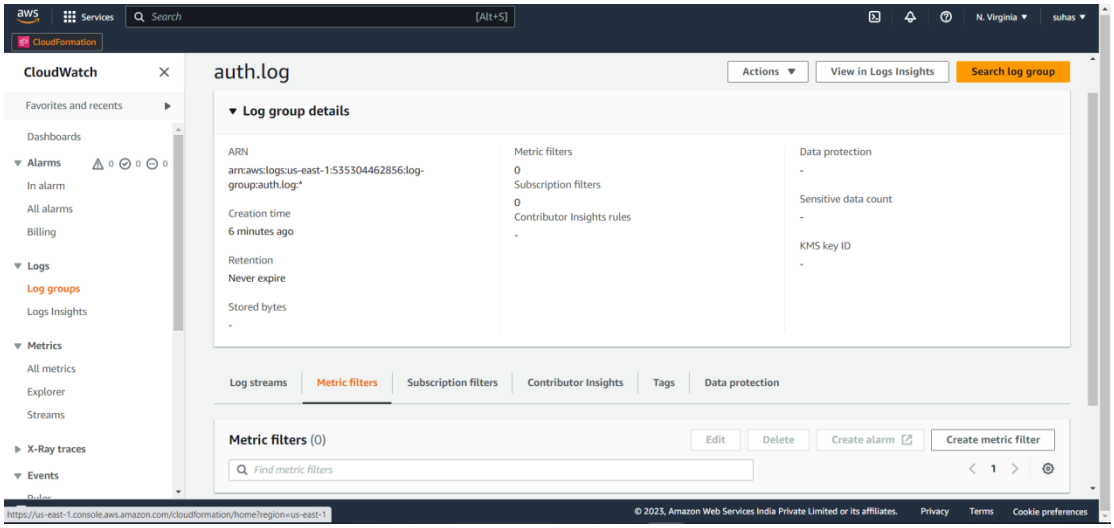


Then go to the Cloudwatch log streams in log groups again and we can see new logs have been generated.

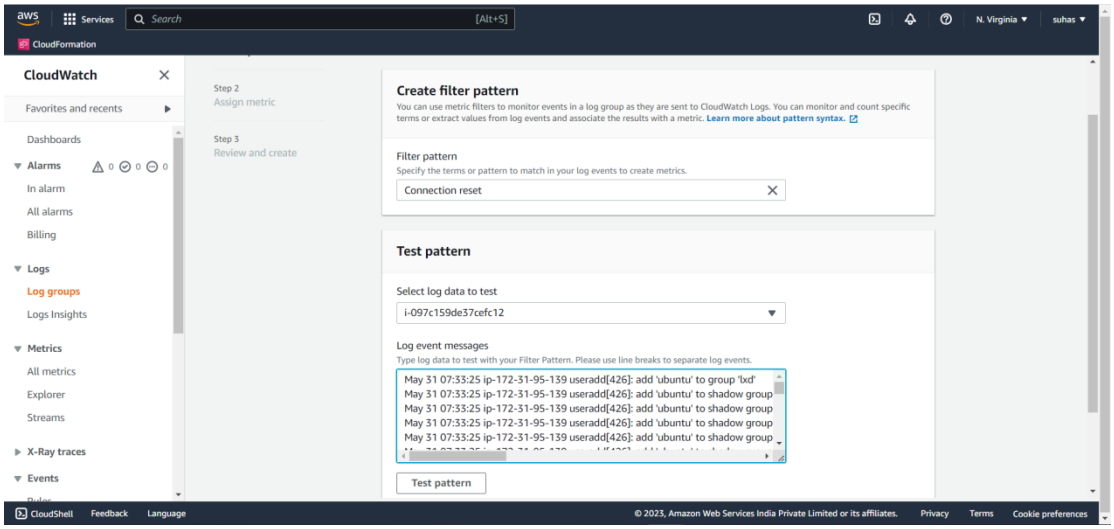


In the Cloudwatch log groups ,

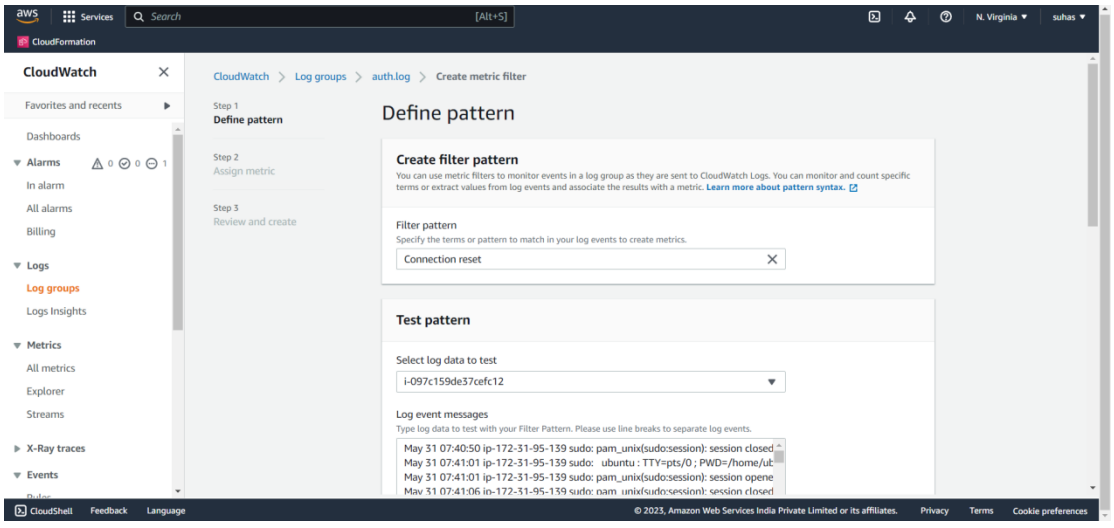
Select the Log group we have generated (auth.log) and create a Metric filter for it.

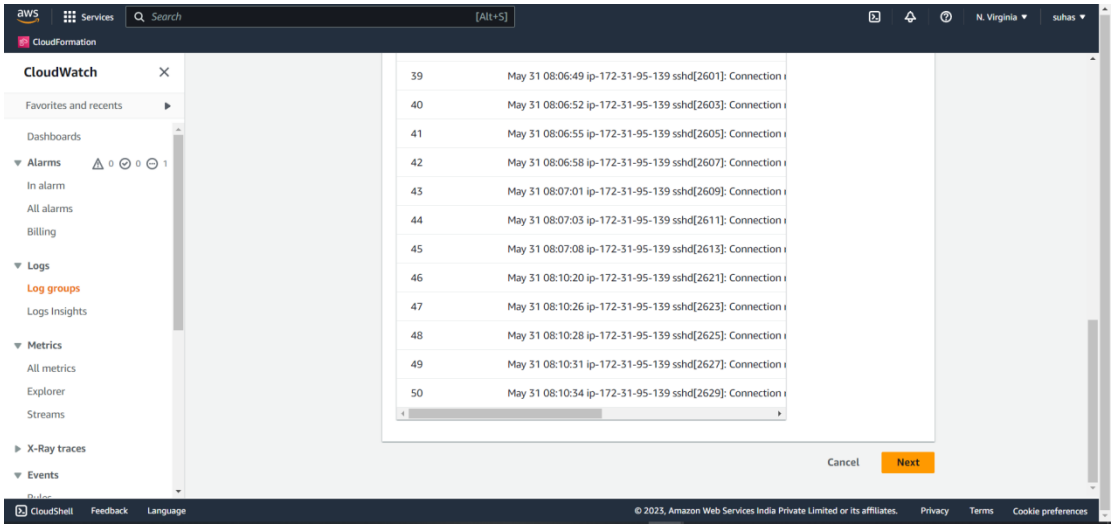


Enter “Connection reset” for the filter pattern and for test pattern , select the Ec2 instance id and click test pattern.

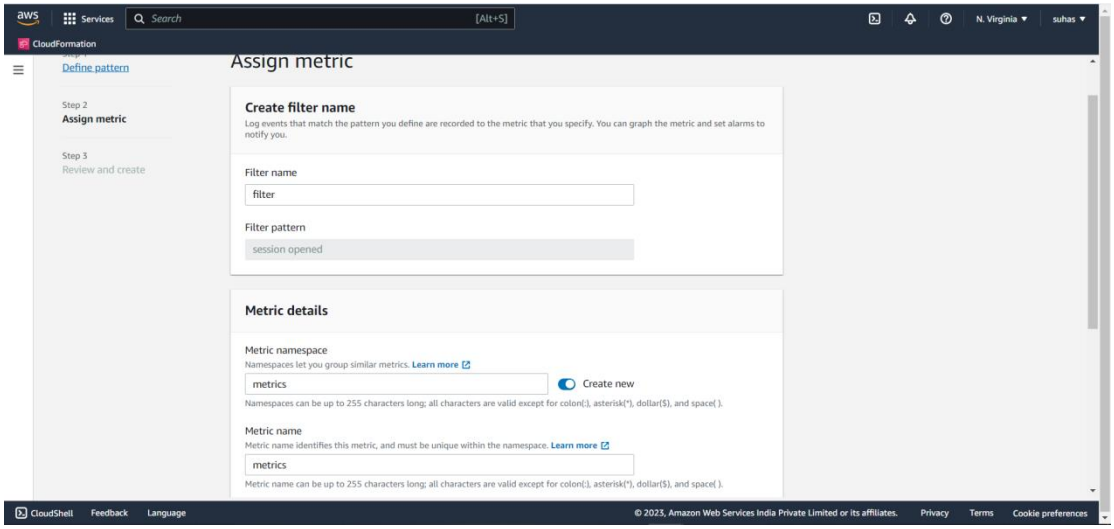


Some log event messages of EC2 related to “connection reset” get displayed.

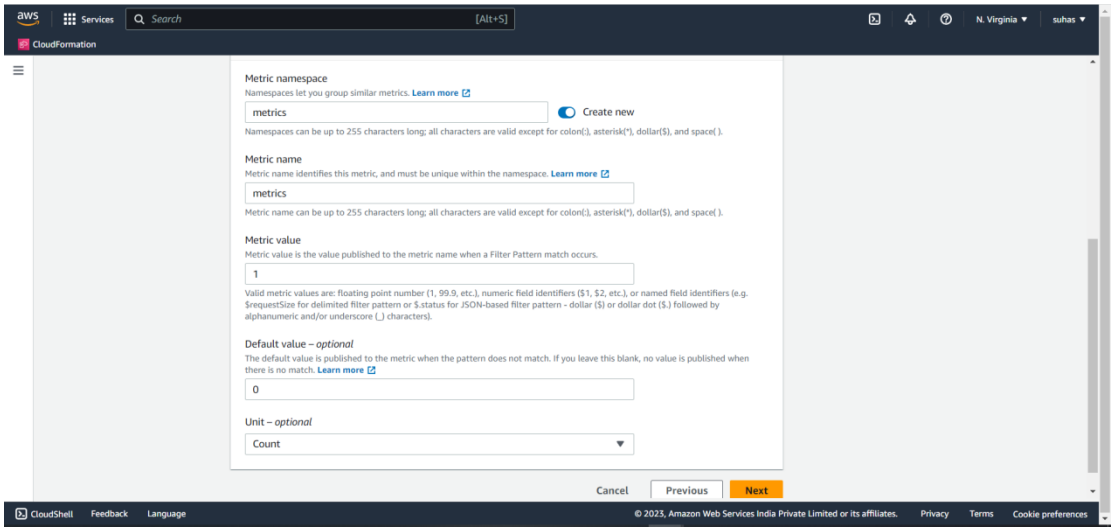


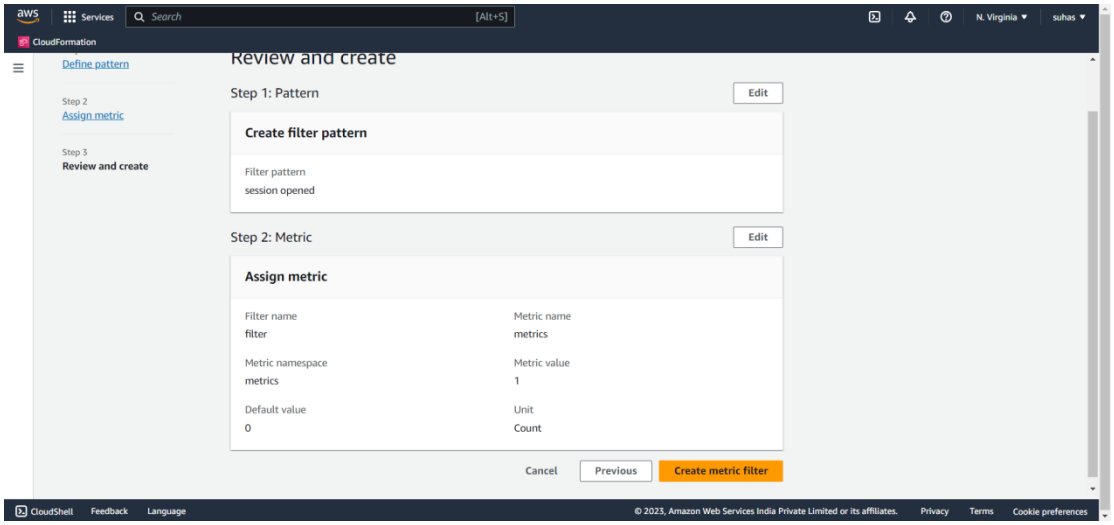


Click Next to assign Metric

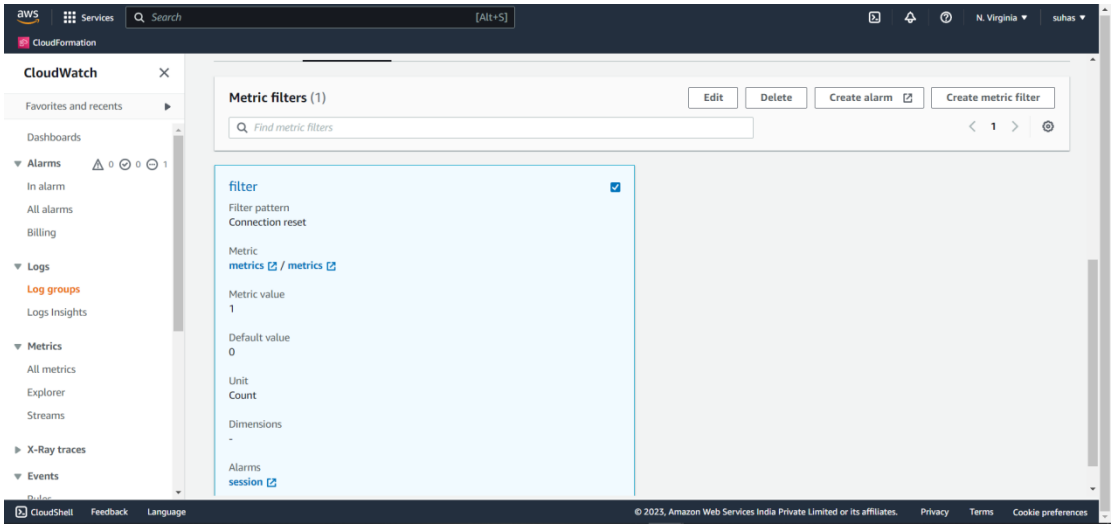


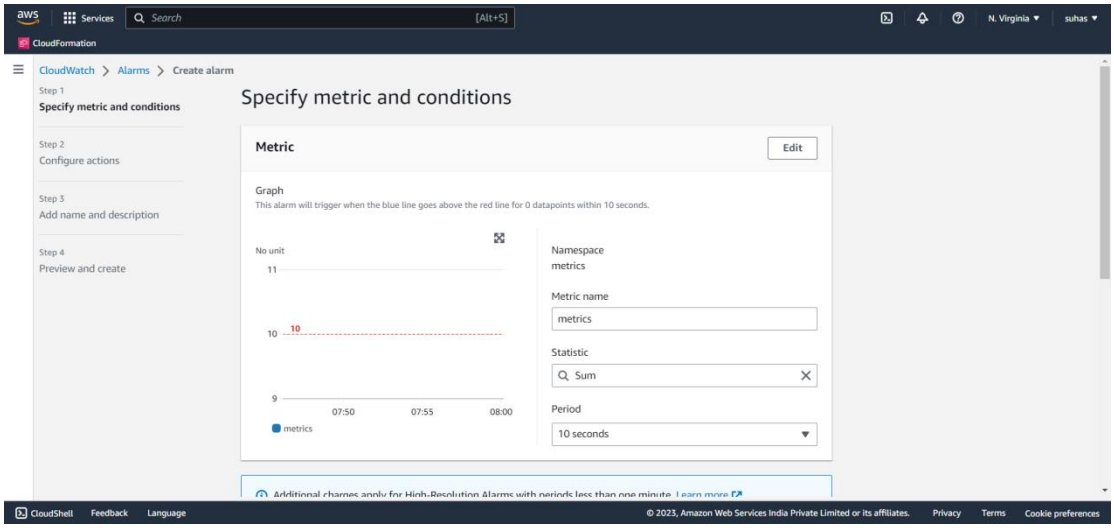
Keep metric value - 1 , Default value- 0 , Unit - count



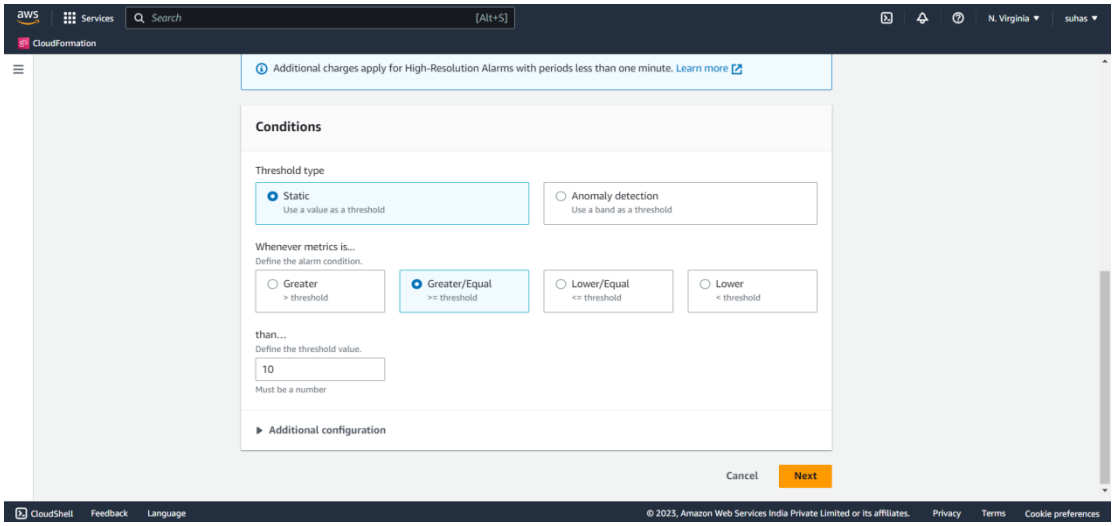


Once Metric filter has been created, select it and click on “create alarm”.

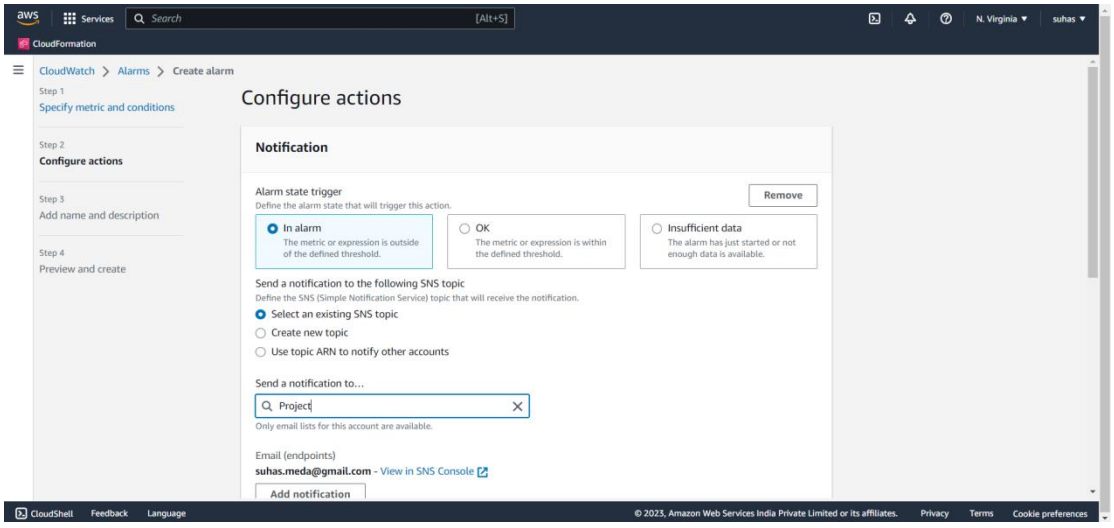




Mention threshold value as 10 (has to be the number of failed SSH attempts we perform atleast)



Keep "In alarm" state trigger and select your created SNS Topic to receive the alarms.



Once alarm has been created, got to command prompt-

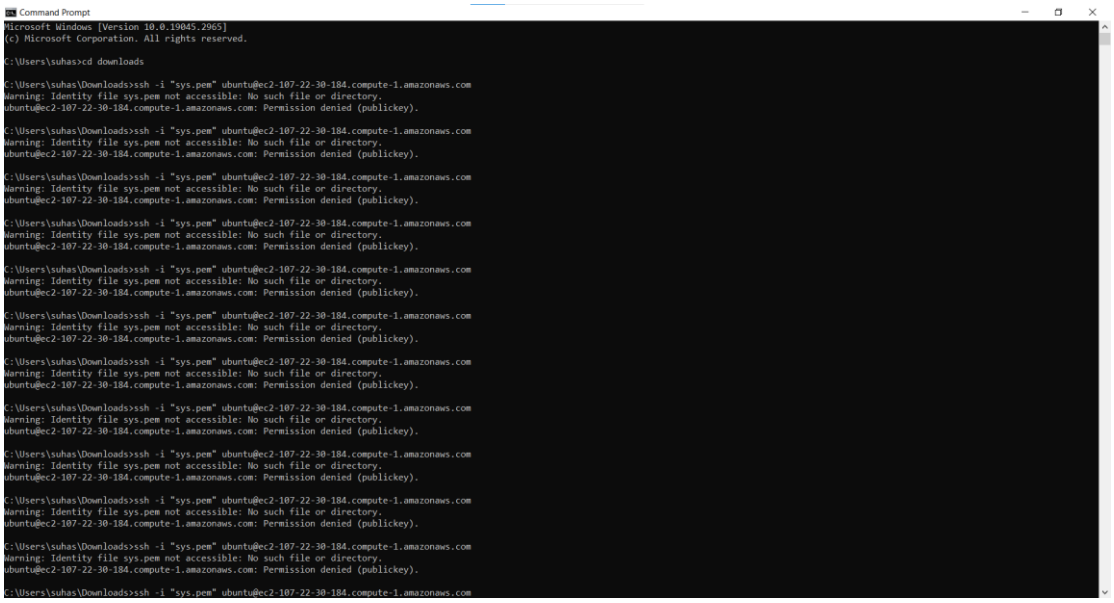
type commands:

cd downloads(or wherever your .pem file is present)

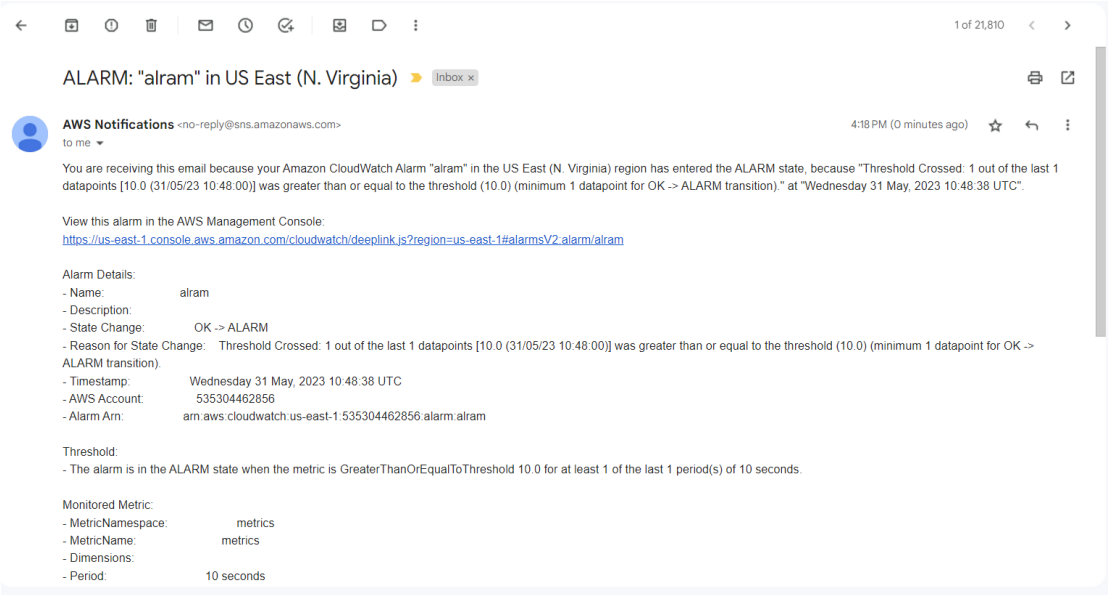
Copy paste the SSH Client Example command of your Ec2 instance. (In this command rename the .pem file in quotes with some other name so as to get failed ssh message in the logs to trigger an alarm)

ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com

Execute this same command multiple times (atleast 10 times - depending on the threshold value you have mentioned in Metrics filter) so as to trigger the alarm.



Now you should get an alarm email sent to you regarding failed SSH attempts.



1 of 21,810

ALARM: "alram" in US East (N. Virginia) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com> 4:18 PM (0 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "alram" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [10.0 (31/05/23 10:48:00)] was greater than or equal to the threshold (10.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 31 May, 2023 10:48:38 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/alram

Alarm Details:
- Name: alram
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [10.0 (31/05/23 10:48:00)] was greater than or equal to the threshold (10.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 31 May, 2023 10:48:38 UTC
- AWS Account: 535304462856
- Alarm Arn: arn:aws:cloudwatch:us-east-1:535304462856:alarm:alram

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 10.0 for at least 1 of the last 1 period(s) of 10 seconds.

Monitored Metric:
- MetricNamespace: metrics
- MetricName: metrics
- Dimensions:
- Period: 10 seconds