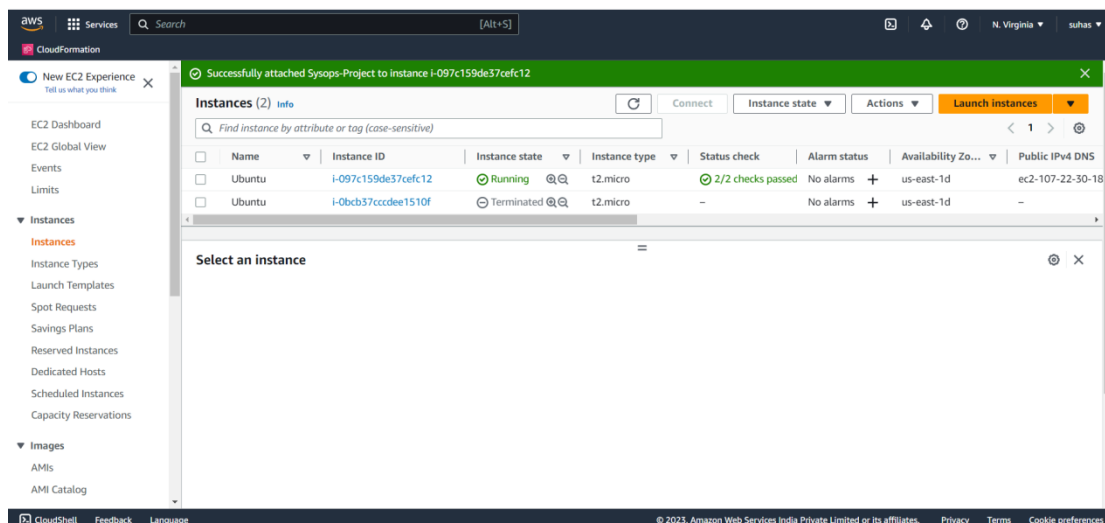
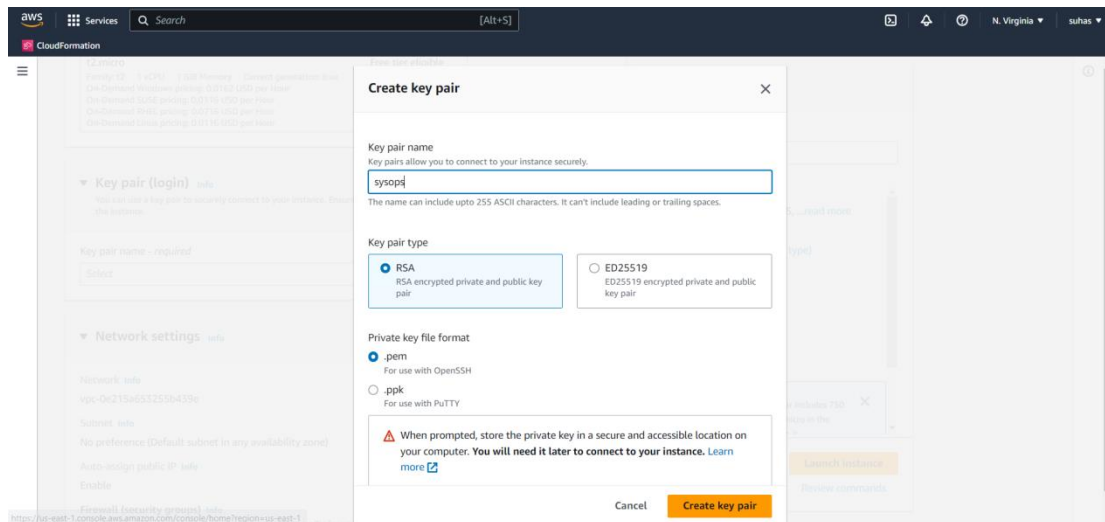


Q)Implement CloudWatch to monitor EC2 instance logs for failed SSH attempts with Alarm notification.

A)

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



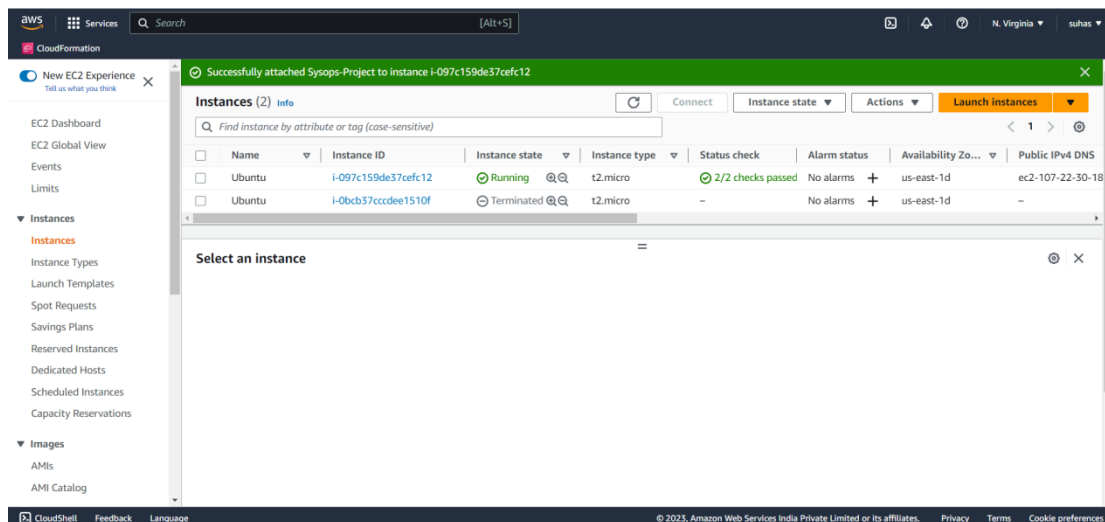
Create an IAM Role with (EC2) Use Case and add CloudWatchAgentAdminPolicy and CloudWatchAgentServerPolicy policies to the role.

The screenshot shows the AWS IAM console for the 'Sysops-Project' role. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, and Credential report. The main content area displays the 'Summary' tab for the 'Sysops-Project' role, which allows EC2 instances to call AWS services on their behalf. The summary includes creation date (May 31, 2023, 11:28 UTC+05:30), ARN (arn:aws:iam::535304462856:role/Sysops-Project), and instance profile ARN (arn:aws:iam::535304462856:instance-profile/Sysops-Project). Below the summary, the 'Permissions' tab shows two attached policies: 'CloudWatchAgentAdminPolicy' and 'CloudWatchAgentServerPolicy', both AWS managed. The bottom of the console shows the footer with '© 2023, Amazon Web Services India Private Limited or its affiliates' and links for Privacy, Terms, and Cookie preferences.

Attach this role to the EC2 instance you have created.

The screenshot shows the AWS EC2 console. The left sidebar contains the 'Instances' menu with options like EC2 Dashboard, EC2 Global View, Events, Limits, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, AMIs, and AMI Catalog. The main content area displays the 'Instances (1/2)' list. The first instance, 'Ubuntu' with ID 'i-097c159de37cfc12', is in the 'Running' state. The 'Actions' menu is open, showing options like Connect, View details, Manage instance state, Instance settings, Networking, Security, Image and templates, and Monitor and troubleshoot. The 'Modify IAM role' option is highlighted. Below the instance list, the 'Instance summary' for 'i-097c159de37cfc12 (Ubuntu)' is shown, including details like Instance ID, Public IPv4 address (107.22.30.184), Private IPv4 address (172.31.95.139), Instance state (Running), Hostname type, IP name, and Elastic IP addresses.

The screenshot shows the 'Modify IAM role' dialog for the EC2 instance 'i-097c159de37cfc12 (Ubuntu)'. The dialog prompts the user to 'Attach an IAM role to your instance.' and shows a dropdown menu with 'Sysops-Project' selected. There is a 'Create new IAM role' link next to the dropdown. At the bottom of the dialog, there are 'Cancel' and 'Update IAM role' buttons. The footer of the console shows '© 2023, Amazon Web Services India Private Limited or its affiliates' and links for Privacy, Terms, and Cookie preferences.



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

```
do you want to monitor any log files?
1. yes
2. no
default choice: [1]:
log file path:
/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
```

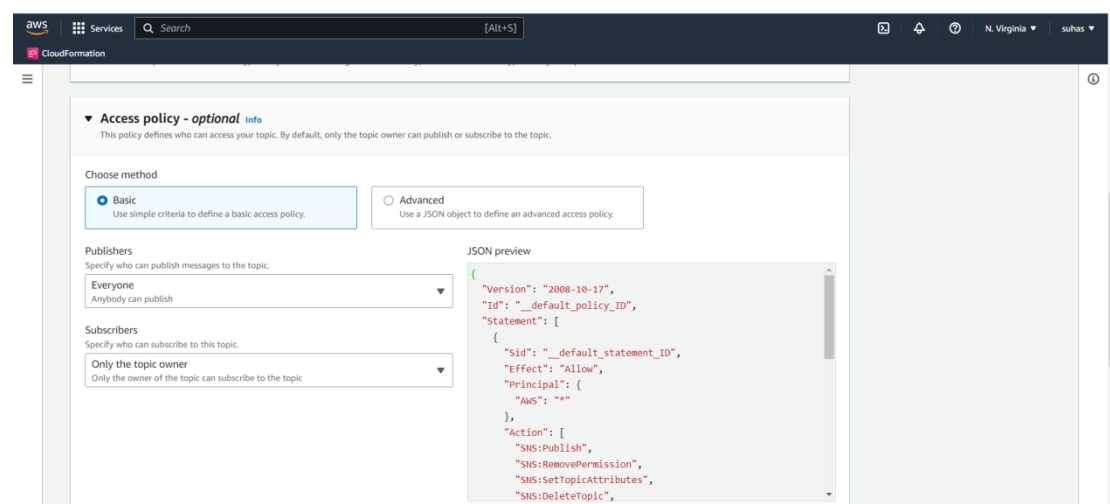
Enter the command to check Status -

service amazon-cloudwatch-agent status

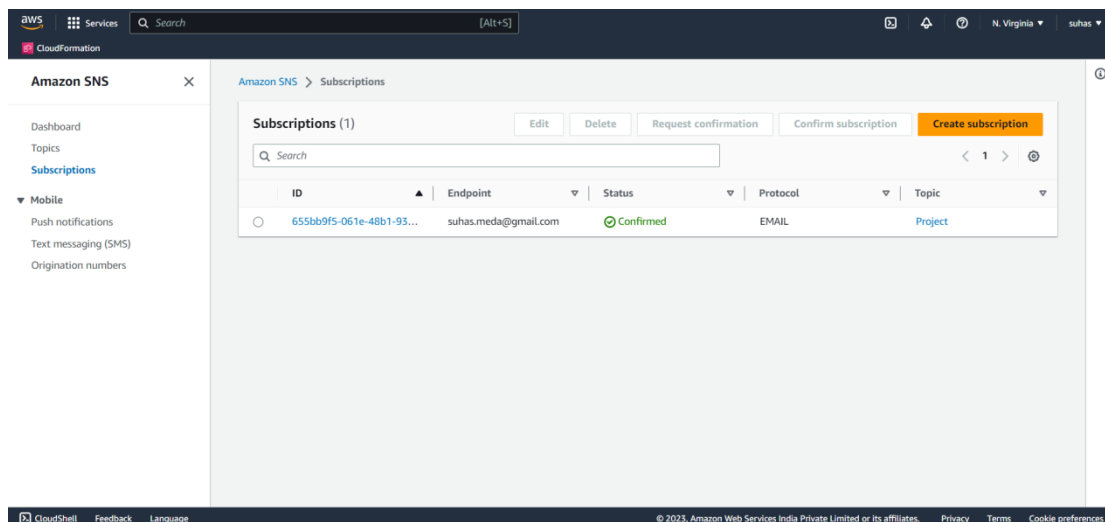
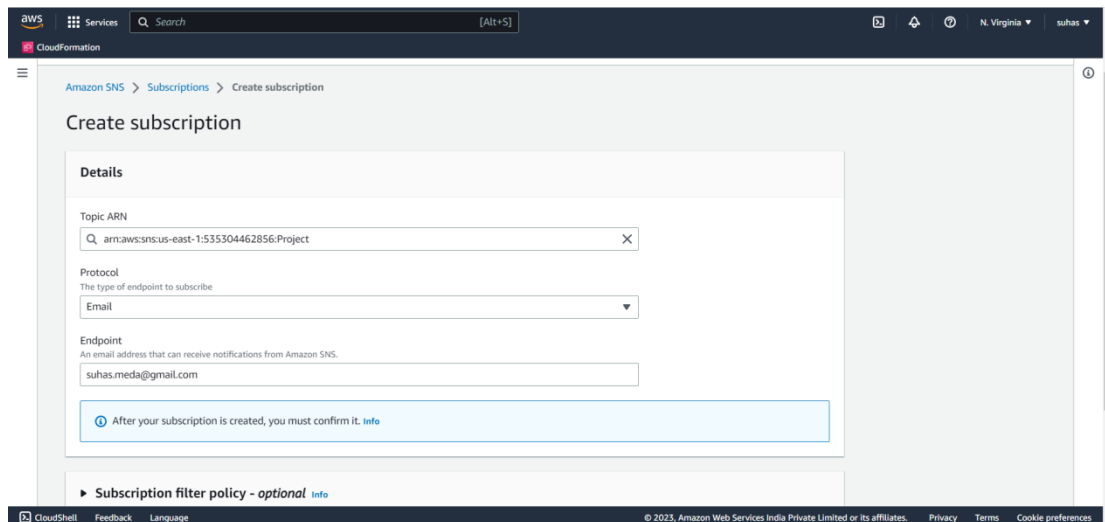
```
abunt@ip-172-31-95-139:~$ service amazon-cloudwatch-agent status
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
   Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-05-31 07:43:30 UTC; 37s ago
     Main PID: 2385 (amazon-cloudwat)
       Tasks: 6 (limit: 1141)
      Memory: 15.5M
         CPU: 240ms
    OGroup: /system.slice/amazon-cloudwatch-agent.service
            └─2385 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /opt/...
```

Should display “active (running) ”

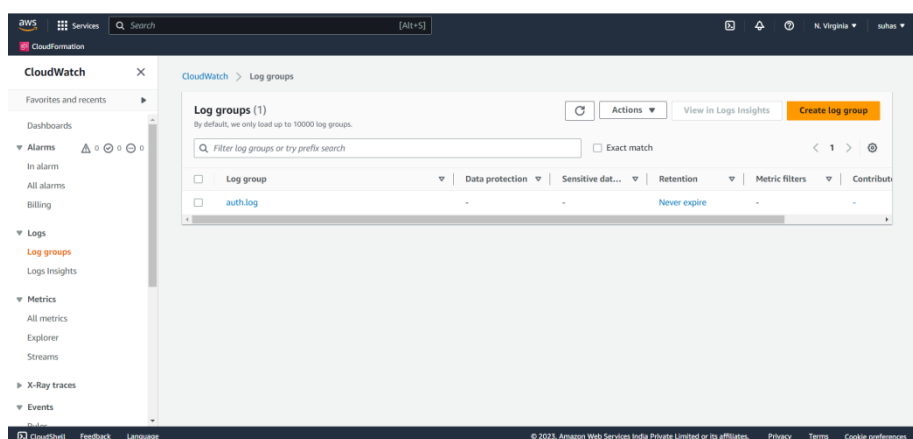
Create SNS Topic -

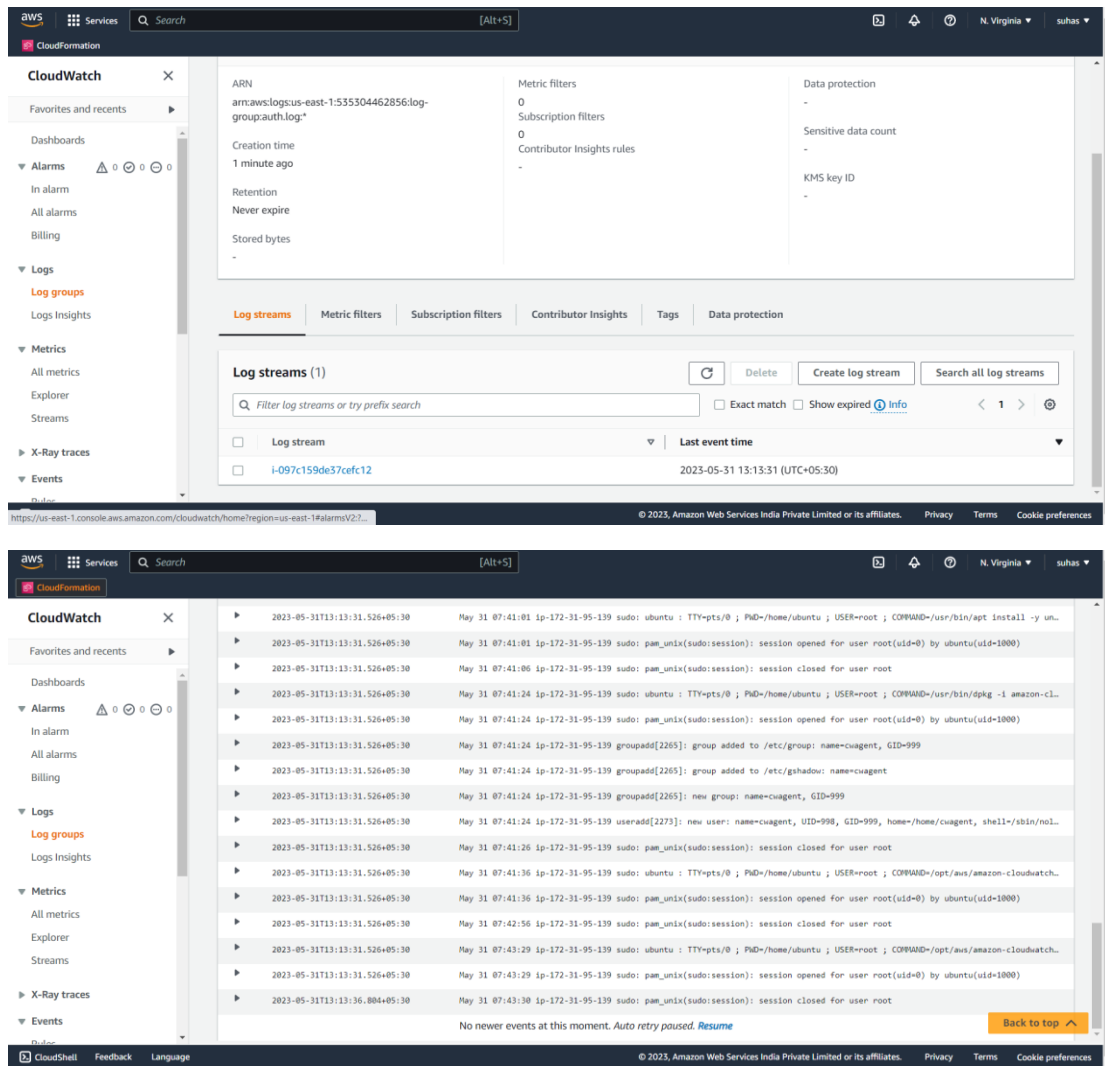


Once SNS Topic has been created, create a Subscription for the topic -



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.

```
ubuntu@ip-172-31-95-139:~$ ssh -i "sysops.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\suhasc> cd downloads
C:\Users\suhasc\Downloads> ssh -i "sysops.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
The authenticity of host 'ec2-107-22-30-184.compute-1.amazonaws.com (107.22.30.184)' can't be established.
ECDSA key fingerprint is SHA256:R11VYvq1m0Q9eSH27N39RglSdUq/15FkgdwmGm+G/w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-107-22-30-184.compute-1.amazonaws.com,107.22.30.184' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed May 31 07:46:05 UTC 2023

System load: 0.0          Processes:           103
Usage of /: 25.3k of 7.57GB   Users logged in:       1
Memory usage: 27%          IPv4 address for eth0: 172.31.95.139
Swap usage: 0%

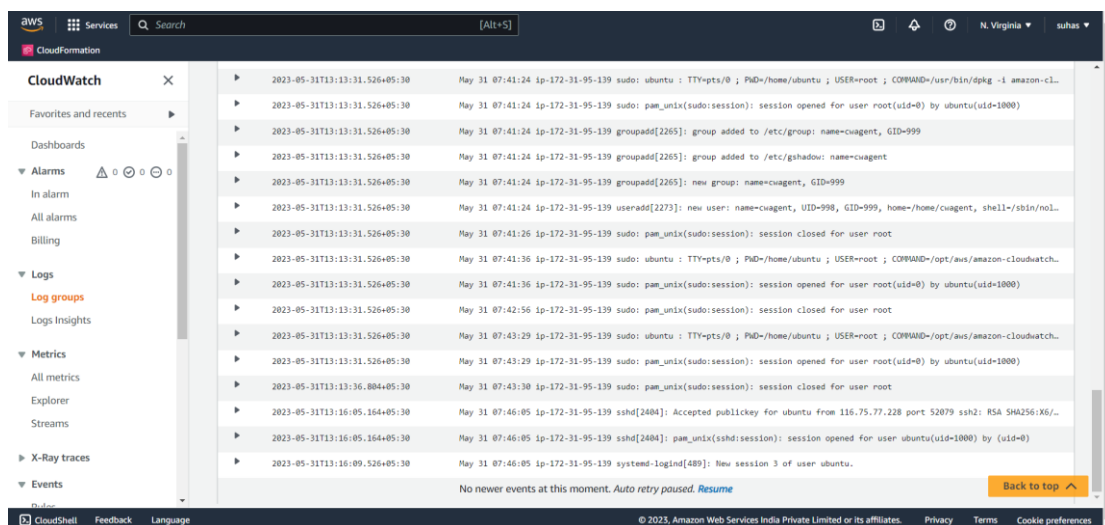
Expanded Security Maintenance for Applications is not enabled.

11 updates can be applied immediately.
10 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

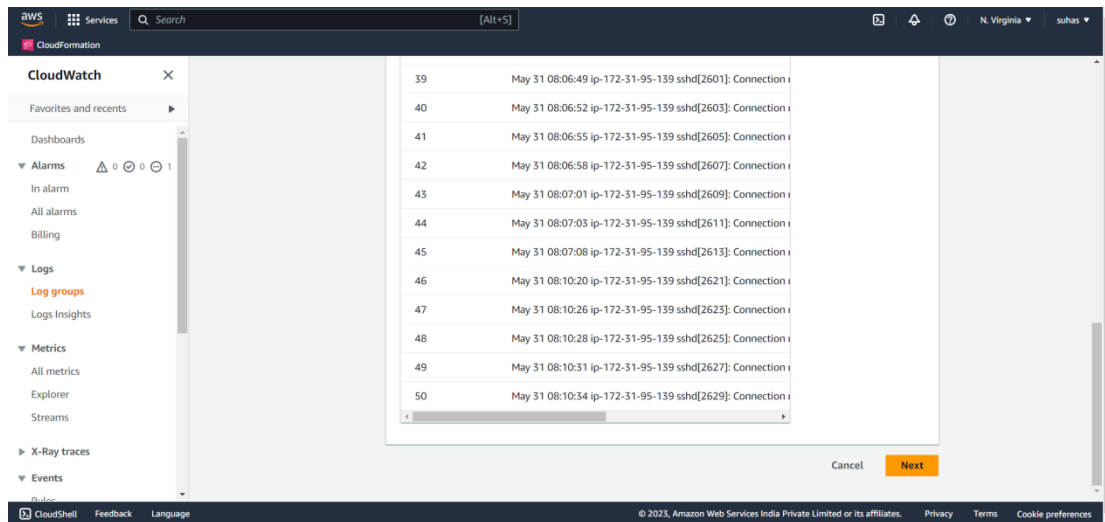
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed May 31 07:40:04 2023 from 18.206.107.27
ubuntu@ip-172-31-95-139:~$
```

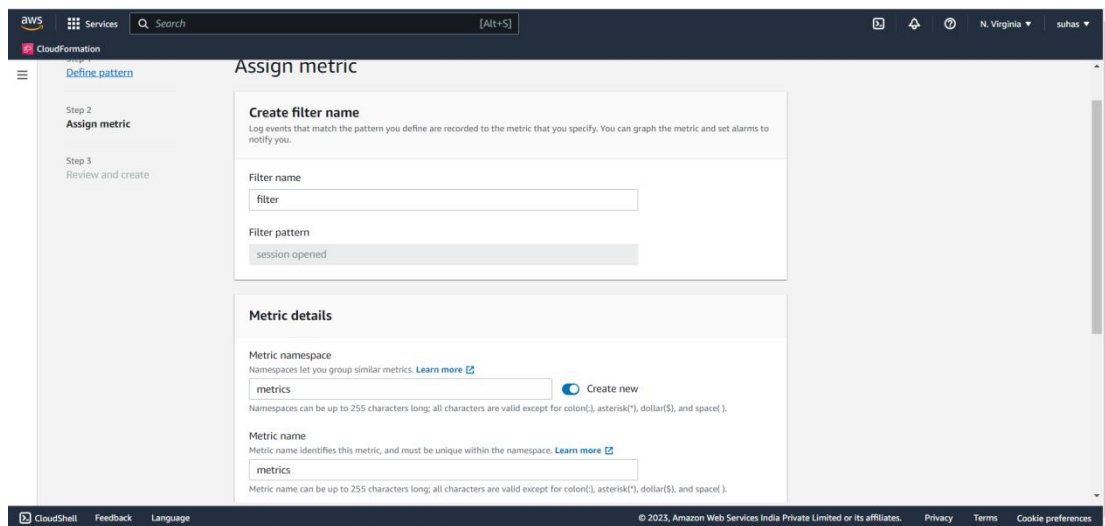
Then go to the Cloudwatch log streams in log groups again and we can see new logs have been generated.



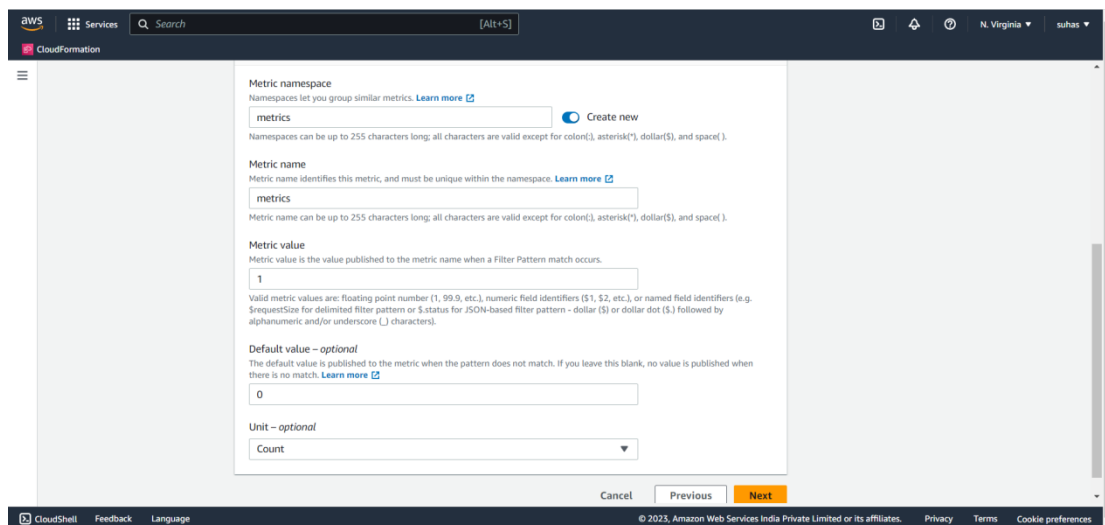
In the Cloudwatch log groups ,
Select the Log group we have generated (auth.log) and create a Metric filter for it.

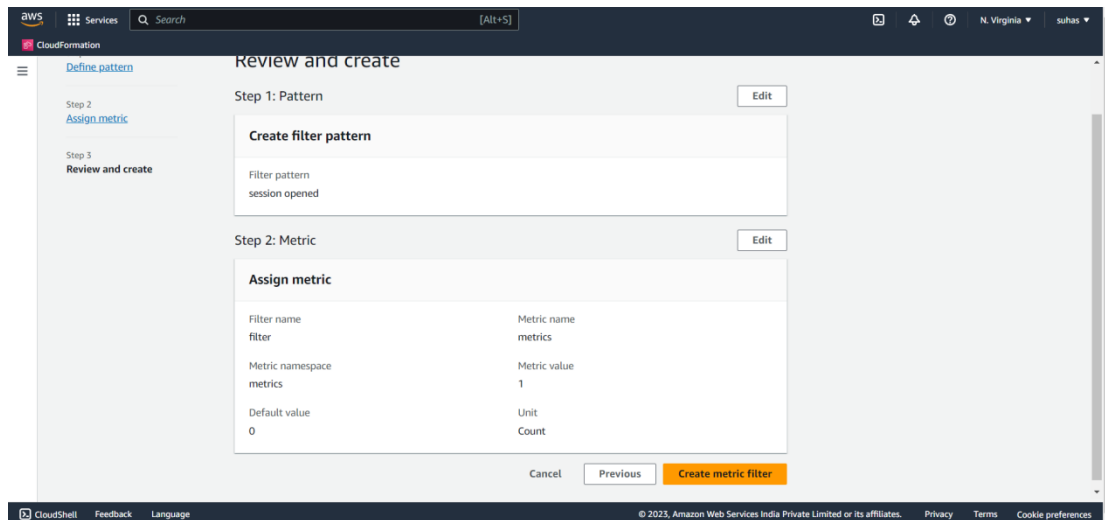


Click Next to assign Metric

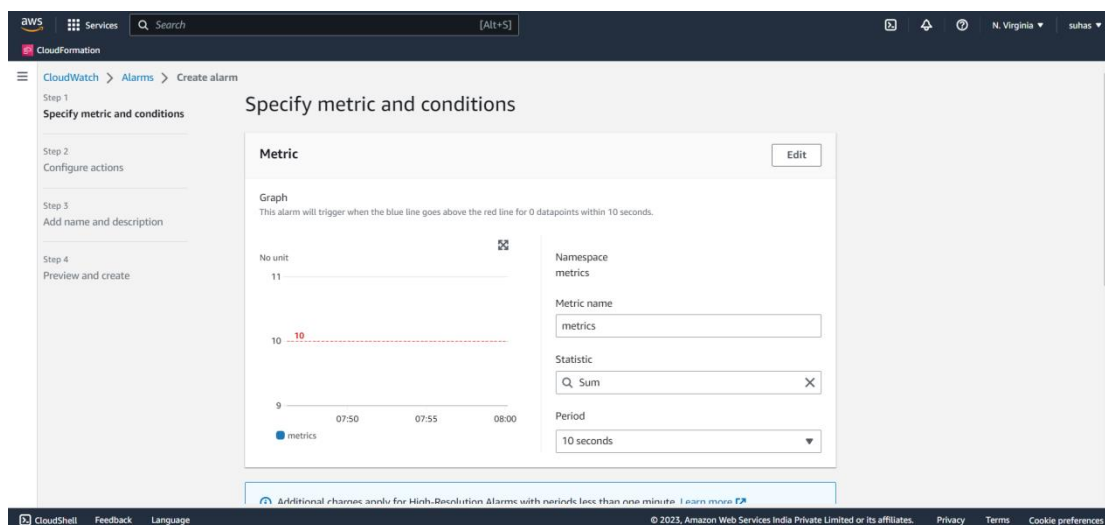
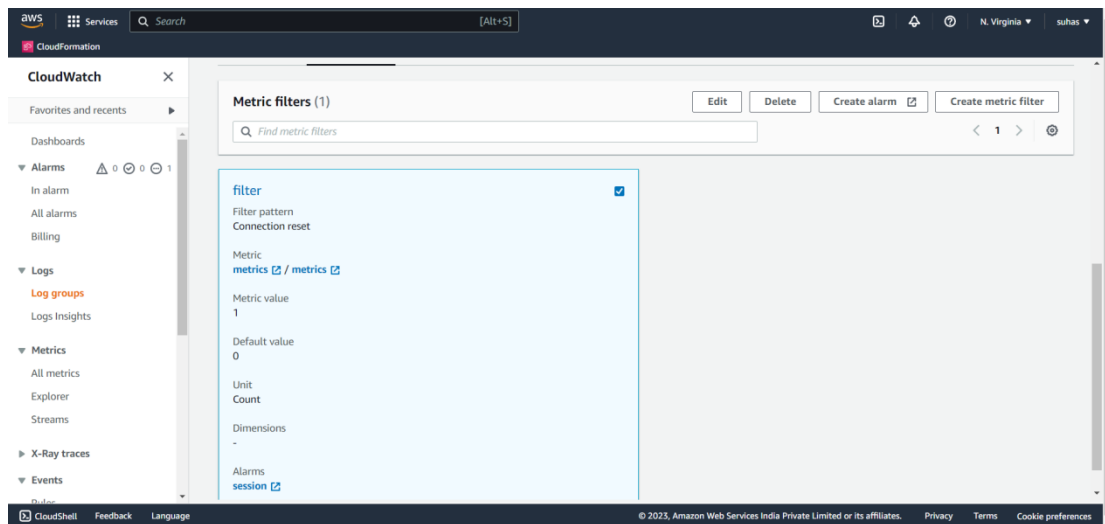


Keep metric value - 1 , Default value- 0 , Unit - count





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)

The screenshot shows the 'Conditions' configuration step in the AWS CloudFormation console. At the top, a note states: 'Additional charges apply for High-Resolution Alarms with periods less than one minute. [Learn more](#)'. The 'Threshold type' section has two options: 'Static' (selected) with the subtext 'Use a value as a threshold', and 'Anomaly detection' with the subtext 'Use a band as a threshold'. The 'Whenever metrics is...' section has four options: 'Greater' (radio button), 'Greater/Equal' (selected, radio button), 'Lower/Equal' (radio button), and 'Lower' (radio button). Below these, the 'than...' section has a text input field containing '10' and a note 'Must be a number'. At the bottom right of the configuration area are 'Cancel' and 'Next' buttons.

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

The screenshot shows the 'Configure actions' step in the AWS CloudFormation console. The left sidebar indicates the current step is 'Step 2: Configure actions'. The main section is titled 'Notification'. Under 'Alarm state trigger', there are three options: 'In alarm' (selected), 'OK', and 'Insufficient data'. Below this, the 'Send a notification to the following SNS topic' section has three options: 'Select an existing SNS topic' (selected), 'Create new topic', and 'Use topic ARN to notify other accounts'. A search bar shows 'Project' with a dropdown arrow. Below the search bar, it says 'Only email lists for this account are available.' and lists an email endpoint 'suhas.meda@gmail.com' with a link to 'View in SNS Console'. At the bottom is an 'Add notification' button.

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.

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\suhass>cd downloads
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
C:\Users\suhass\Downloads>ssh -i "sys.pem" ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com
Warning: Identity file sys.pem not accessible: No such file or directory.
ubuntu@ec2-107-22-30-184.compute-1.amazonaws.com: Permission denied (publickey).
```

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

