

To alert the subscriber about the instances termination by other users using CloudTrail and CloudWatch.

1. Log in to [AWS Management Console](#)

--Go to the [AWS Management Console](#). --Sign in with your credentials.

Navigate to EC2

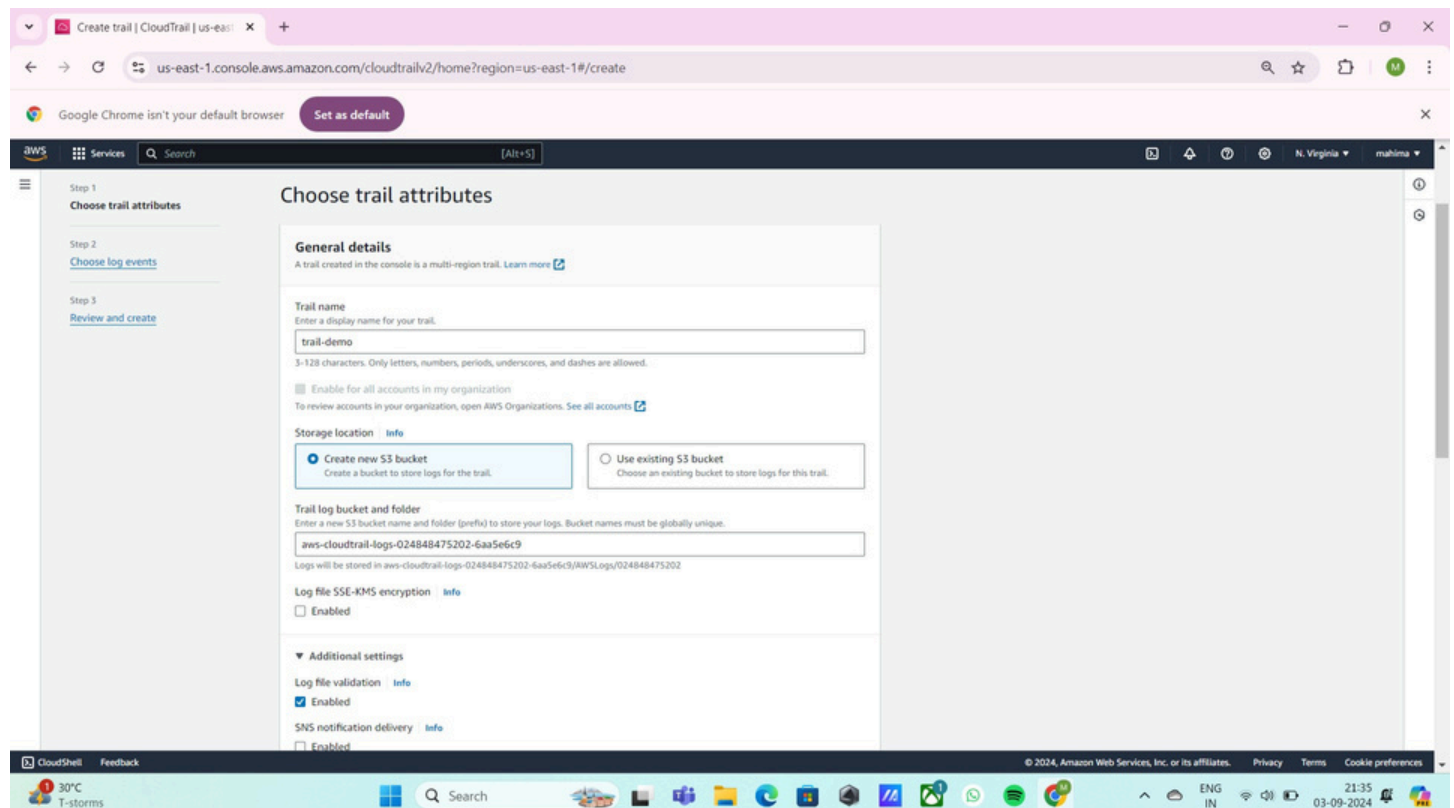
--In the AWS Management Console, type EC2 in the search bar and select it from the list of services.

Launch an Instance

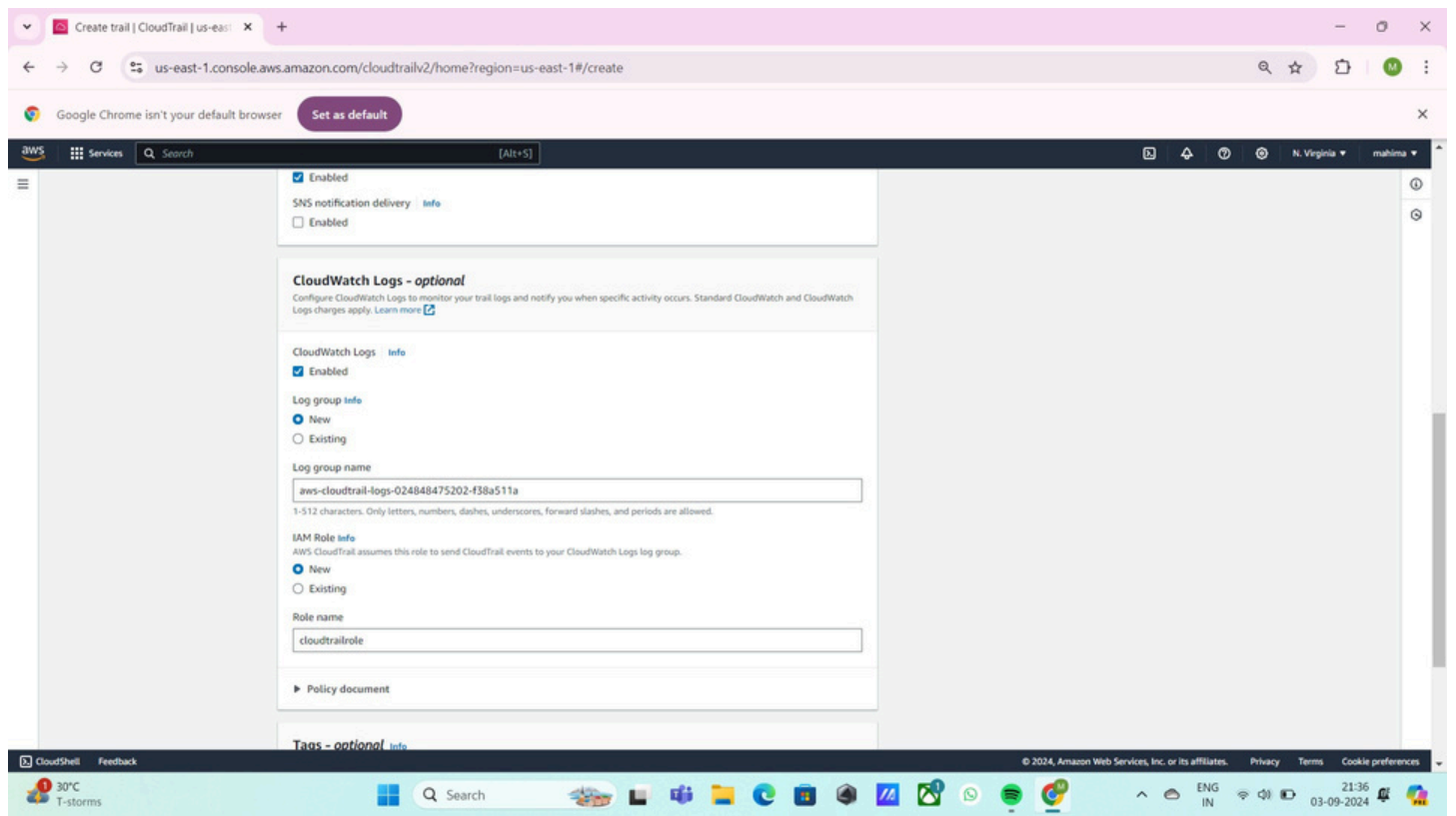
--In the EC2 Dashboard, click on the Launch Instance button.

2.Search for CloudTrail and open CloudTrail Console.

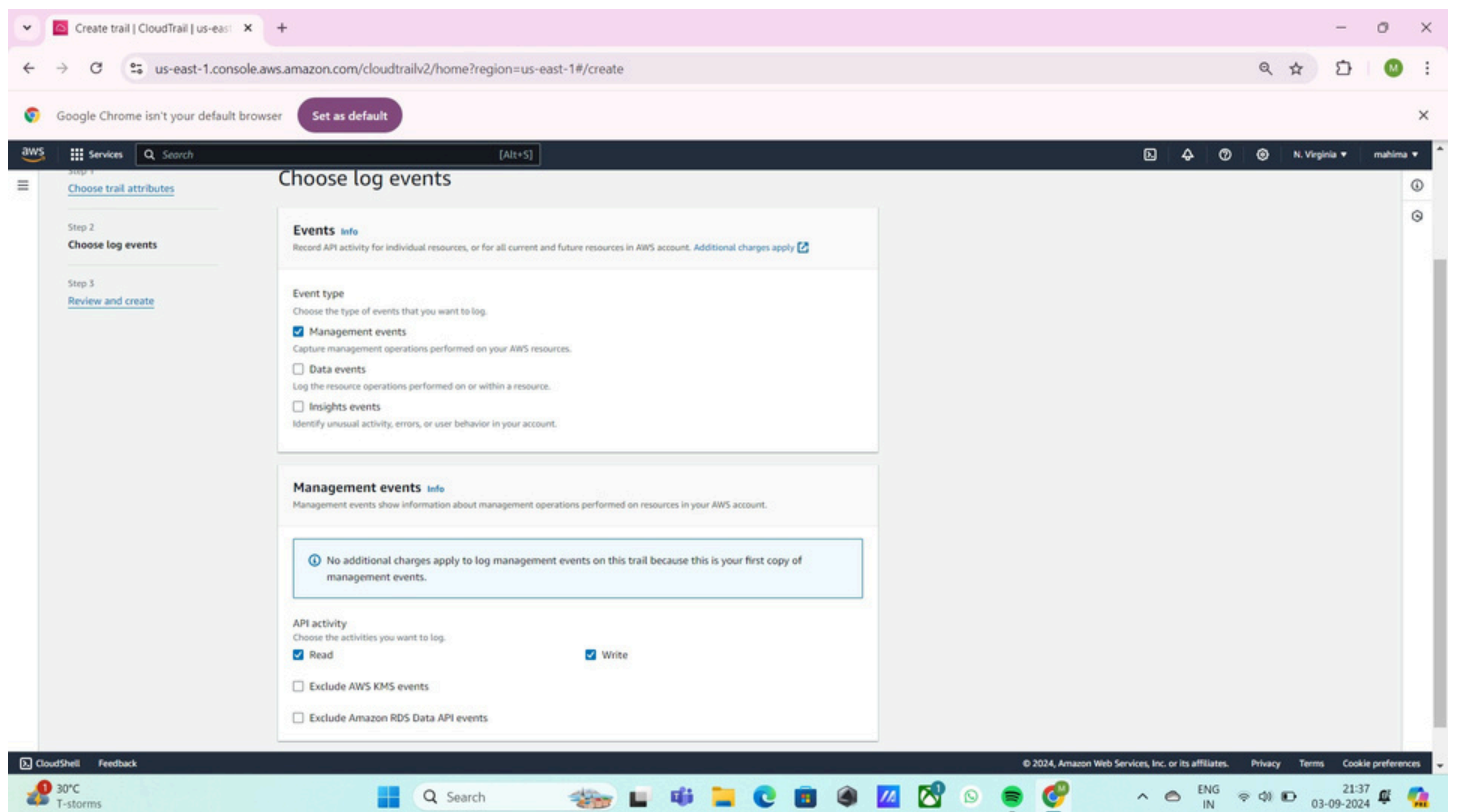
--Click on "Trails" in the navigation pane, then click on "Create trail". --create s3 buckets to store the logs.



--keep the other options as default.



3. Choose event Type as Management events and review and create the Trail.



us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/create

Google Chrome isn't your default browser [Set as default](#)

Step 1: Choose trail attributes

General details

Trail name	Trail log location	Log file validation
trail-demo	aws-cloudtrail-logs-024848475202-6aa5e6c9/AWSLogs/024848475202	Enabled
Multi-region trail		SNS notification delivery
Yes	2	Disabled
Apply trail to my organization	Log file SSE-KMS encryption	
Not enabled	Not enabled	

CloudWatch Logs

Log group	IAM Role
aws-cloudtrail-logs-024848475202-f38a511a	cloudtrailrole

Tags

Key	Value
No tags	
No tags associated with this trail	

Step 2: Choose log events

Management events

No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity	Exclude AWS KMS events
All	No
	Exclude Amazon RDS Data API events
	No

Data events

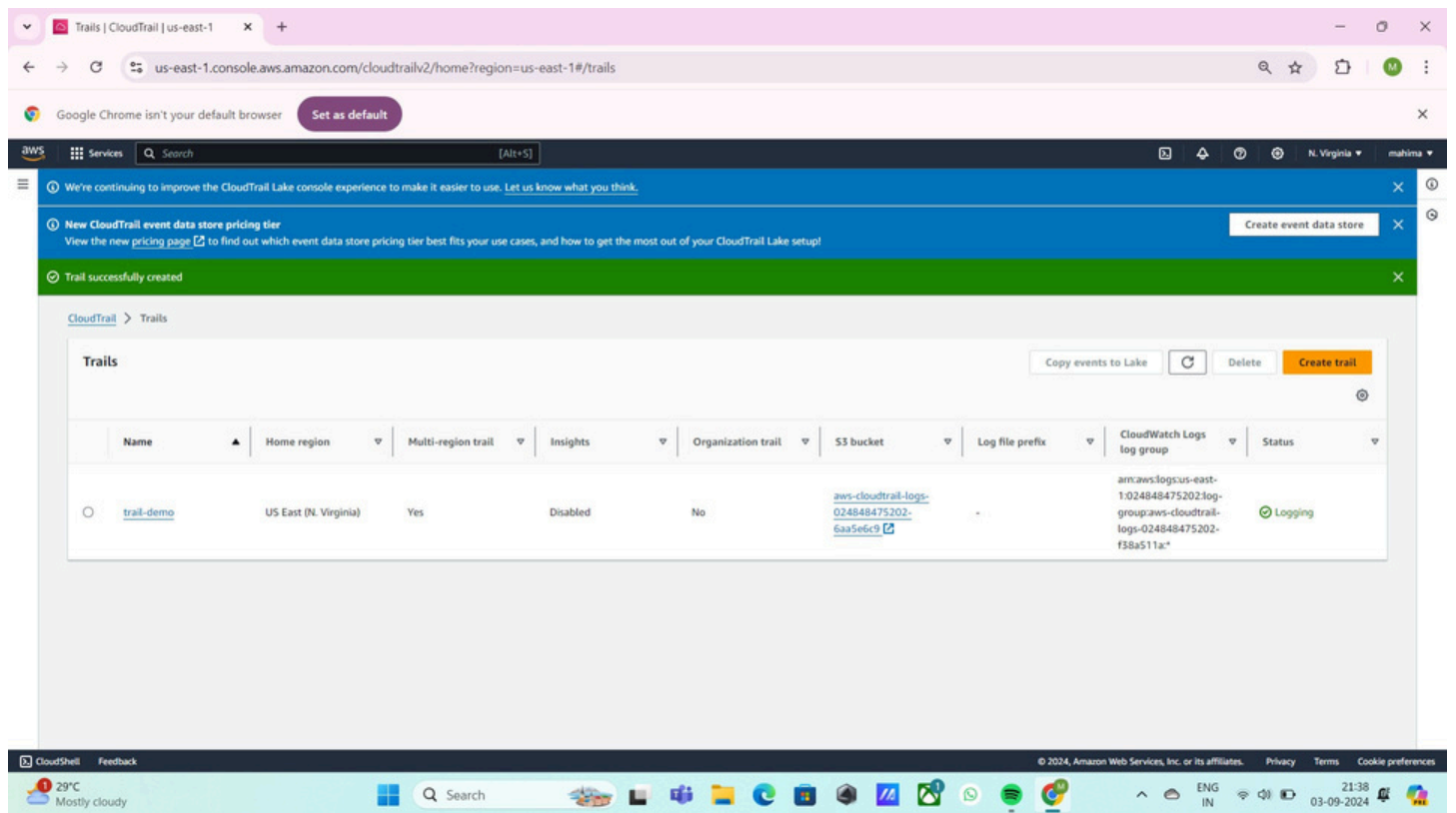
Data event collection is not configured for this trail

Insights events

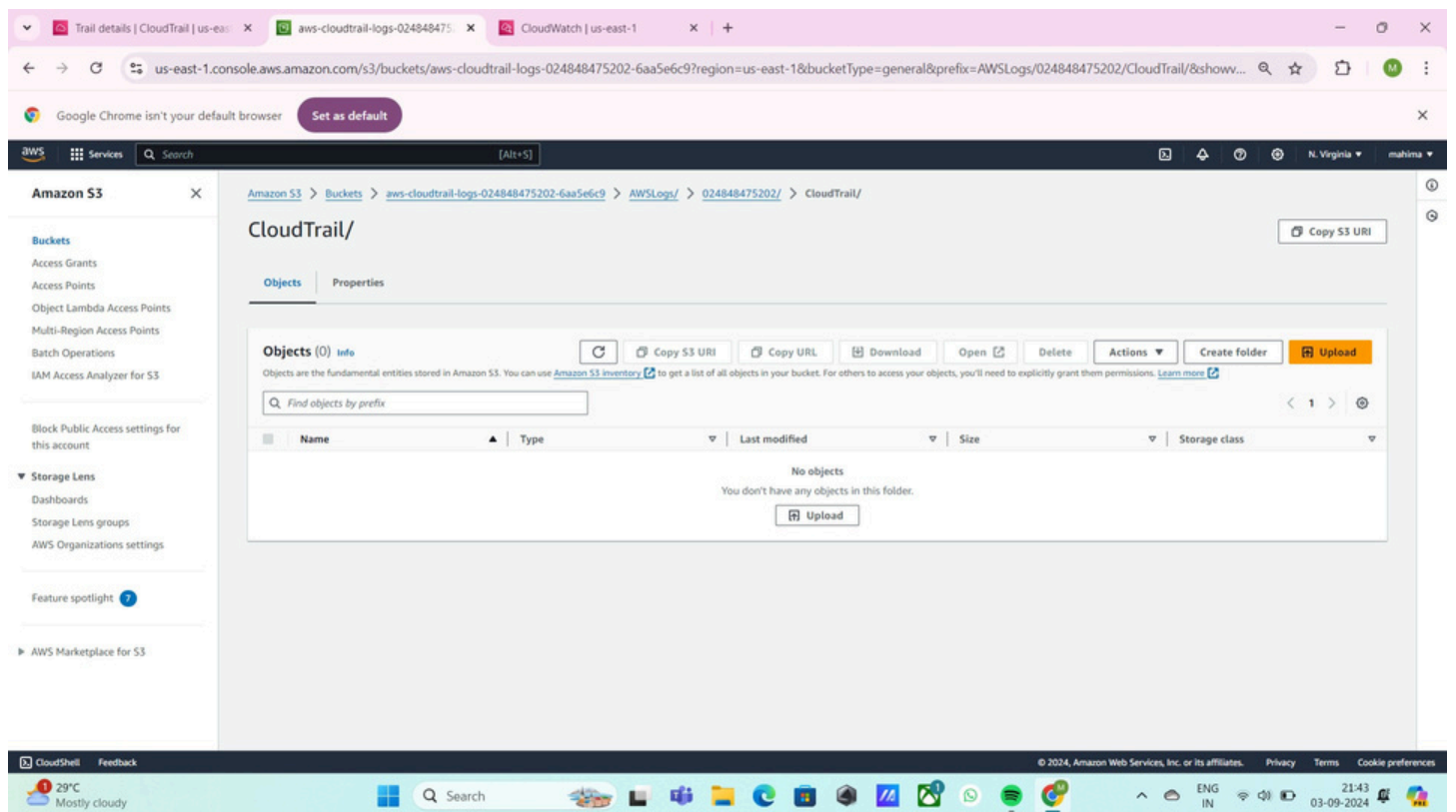
You can only enable CloudTrail Insights on trails that log management events. [Learn more](#)

Cancel Previous Create trail

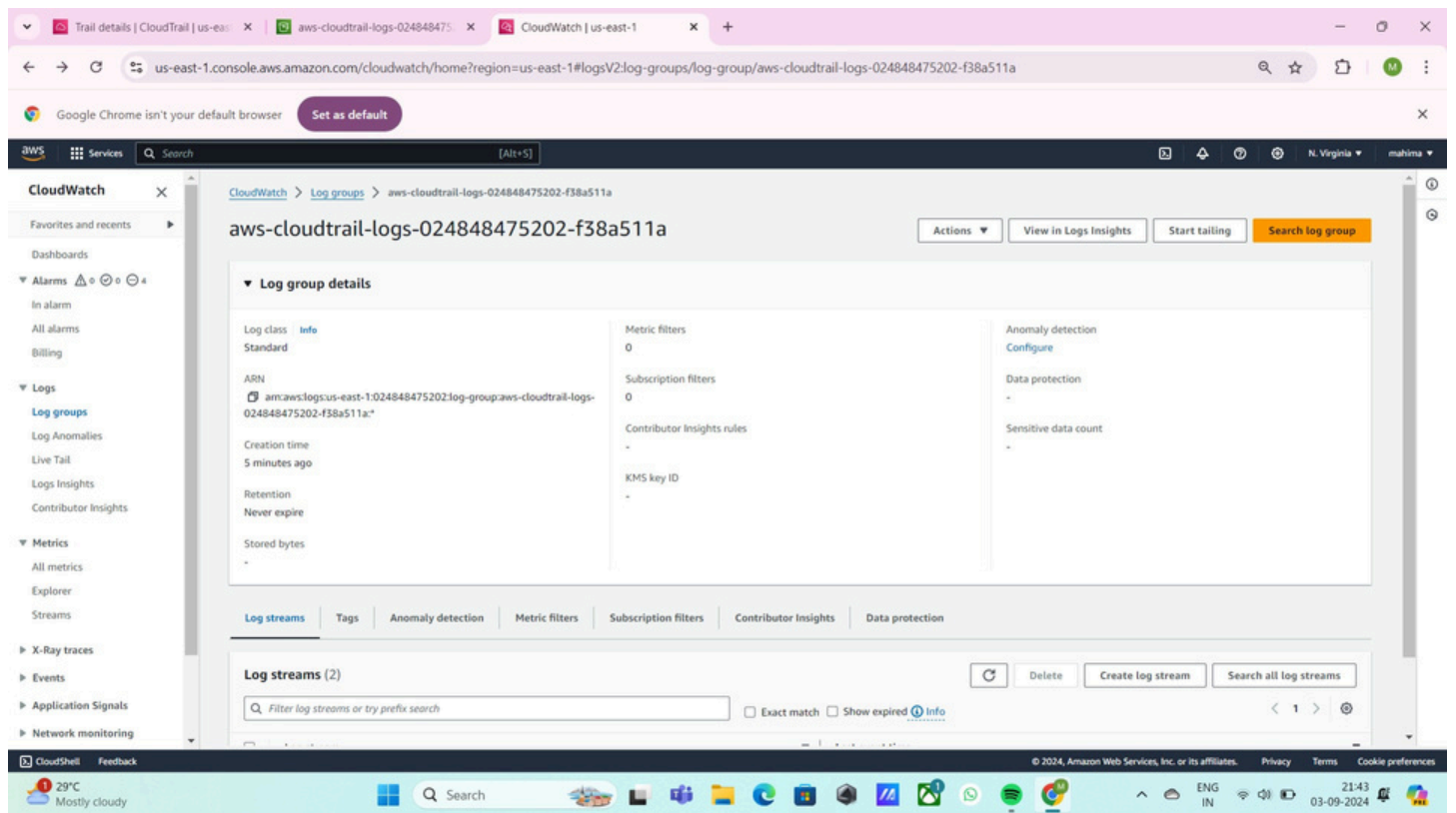
4. Trail created Successfully



5.Go for Buckets in the left navigation pane and then check whether the bucket is created or not.



--The log streams are in log grops where every logs are recorded.



Log streams	Tags	Anomaly detection	Metric filters	Subscription filters	Contributor Insights	Data protection
<div>Log streams (4)</div> <div> <input type="text" value="Filter log streams or try prefix search"/> <input type="checkbox"/> Exact match <input type="checkbox"/> Show expired Info </div> <div> <div>1</div> </div>						
<input type="checkbox"/>	Log stream					
<input type="checkbox"/>	024848475202_CloudTrail_us-east-1_3	2024-09-03 16:15:23 (UTC)				
<input type="checkbox"/>	024848475202_CloudTrail_us-east-1_2	2024-09-03 16:13:12 (UTC)				
<input type="checkbox"/>	024848475202_CloudTrail_us-east-1_4	2024-09-03 16:11:02 (UTC)				
<input type="checkbox"/>	024848475202_CloudTrail_us-east-1	-				

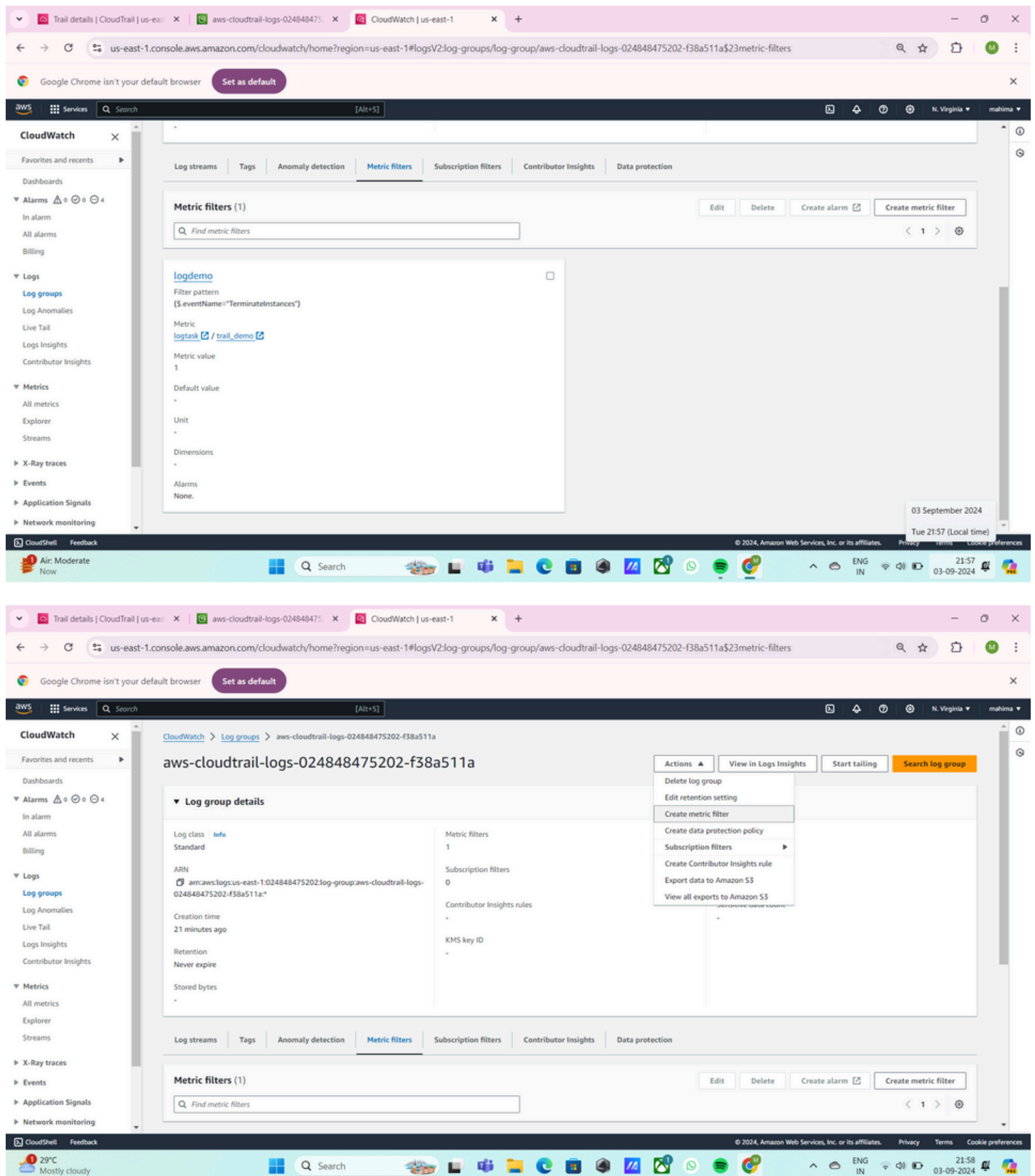
--The format of logs are shown down.

```

2024-09-03T16:13:12.796Z {"eventVersion":"1.10","userIdentity":{"type":"Root","principalId":"024848475202","arn":"arn:aws:iam::024848475202:root","accountId":"024848475202","accessKeyId":"ASIAQLSIVUR8OPL7M46","sessionContext":{"attributes":{"creationDate":"2024-09-03T15:54:50Z","mfaAuthenticated":"false"}}}},
{"eventVersion":"1.10",
"userIdentity": {
  "type": "Root",
  "principalId": "024848475202",
  "arn": "arn:aws:iam::024848475202:root",
  "accountId": "024848475202",
  "accessKeyId": "ASIAQLSIVUR8OPL7M46",
  "sessionContext": {
    "attributes": {
      "creationDate": "2024-09-03T15:54:50Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2024-09-03T16:10:42Z",
"eventSource": "s3.amazonaws.com",
"eventName": "GetBucketVersioning",
"awsRegion": "us-east-1",
"sourceIPAddress": "49.204.137.126",
"userAgent": "[S3Console/0.4, aws-internal/3 aws-sdk-java/1.12.750 Linux/5.10.223-190.872.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.412-b09 java/1.8.0_412 vendor/Oracle_Corporation cfg/retry-mode/standard]",
"requestParameters": {
  "bucketName": "aws-cloudtrail-logs-024848475202-6aa5ec9",
  "Host": "s3.amazonaws.com",
  "versioning": ""
},
"responseElements": null,
"additionalEventData": {
  "SignatureVersion": "SigV4",
  "CipherSuite": "TLS_AES_128_GCM_SHA256",
  "bytesTransferredIn": 0,
  "AuthenticationMethod": "AuthHeader",
  "x-amz-id-2": "9QwPaW8KQALE1TS/Deo5NMcIxH3eZu1jo2FwH2BQXT+VW8Cu6PVPWNe53H4MEHgHvd3LsPC/VYSABtv8jP8RpzVW0pz9Kd",

```

6.create the Filter Pattern for metric.Here I created {\$.eventName="TerminateInstances"}.it indicates that an event with the name TerminateInstances has occurred or is being tracked.



7. Open cloudwatch console to create alarm for creating alarm we need to specify metrics and conditions and configure the actions.

Configure Actions

- Choose the actions to take when the alarm state is triggered:
- Send a notification to an SNS topic: Select or create an SNS topic and add the necessary recipients (e.g., email, SMS).

EC2 action: Stop, terminate, reboot, or recover an EC2 instance.

Trail details | CloudTrail | us-east-1

aws-cloudtrail-logs-024848475

CloudWatch | us-east-1

Create alarm | Alarms | CloudWatch

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~MetricSelection~AlarmType~MetricAlarm~AlarmData~(Namespace~logtask~MetricName~trail_demo~Statistic~Sum~Period~1 minute))

Google Chrome isn't your default browser Set as default

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

No unit

2

1

1

0

14:30

15:30

16:30

trail_demo

Namespace

logtask

Metric name

trail_demo

Statistic

Sum

Period

1 minute

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

1

1

0

14:30

15:30

16:30

trail_demo

Statistic

Sum

Period

1 minute

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

Whenever trail_demo is...

Define the alarm condition.

Greater

> threshold

Greater/Equal

>= threshold

Lower/Equal

<= threshold

Lower

< threshold

than...

Define the threshold value.

1

Must be a number

Additional configuration

Cancel

Next

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Light rain

Search

ENG IN

22:17 03-09-2024

Trail details | CloudTrail | us-east-1

aws-cloudtrail-logs-024848475

CloudWatch | us-east-1

Create alarm | Alarms | CloudWatch

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~MetricSelection~AlarmType~MetricAlarm~AlarmData~(Namespace~logtask~MetricName~trail_demo~Statistic~Sum~Period~1 minute))

Google Chrome isn't your default browser Set as default

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

No unit

2

1

1

0

14:30

15:30

16:30

trail_demo

Namespace

logtask

Metric name

trail_demo

Statistic

Sum

Period

1 minute

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

1

1

0

14:30

15:30

16:30

trail_demo

Statistic

Sum

Period

1 minute

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

Whenever trail_demo is...

Define the alarm condition.

Greater

> threshold

Greater/Equal

>= threshold

Lower/Equal

<= threshold

Lower

< threshold

than...

Define the threshold value.

1

Must be a number

Additional configuration

Cancel

Next

CloudShell Feedback

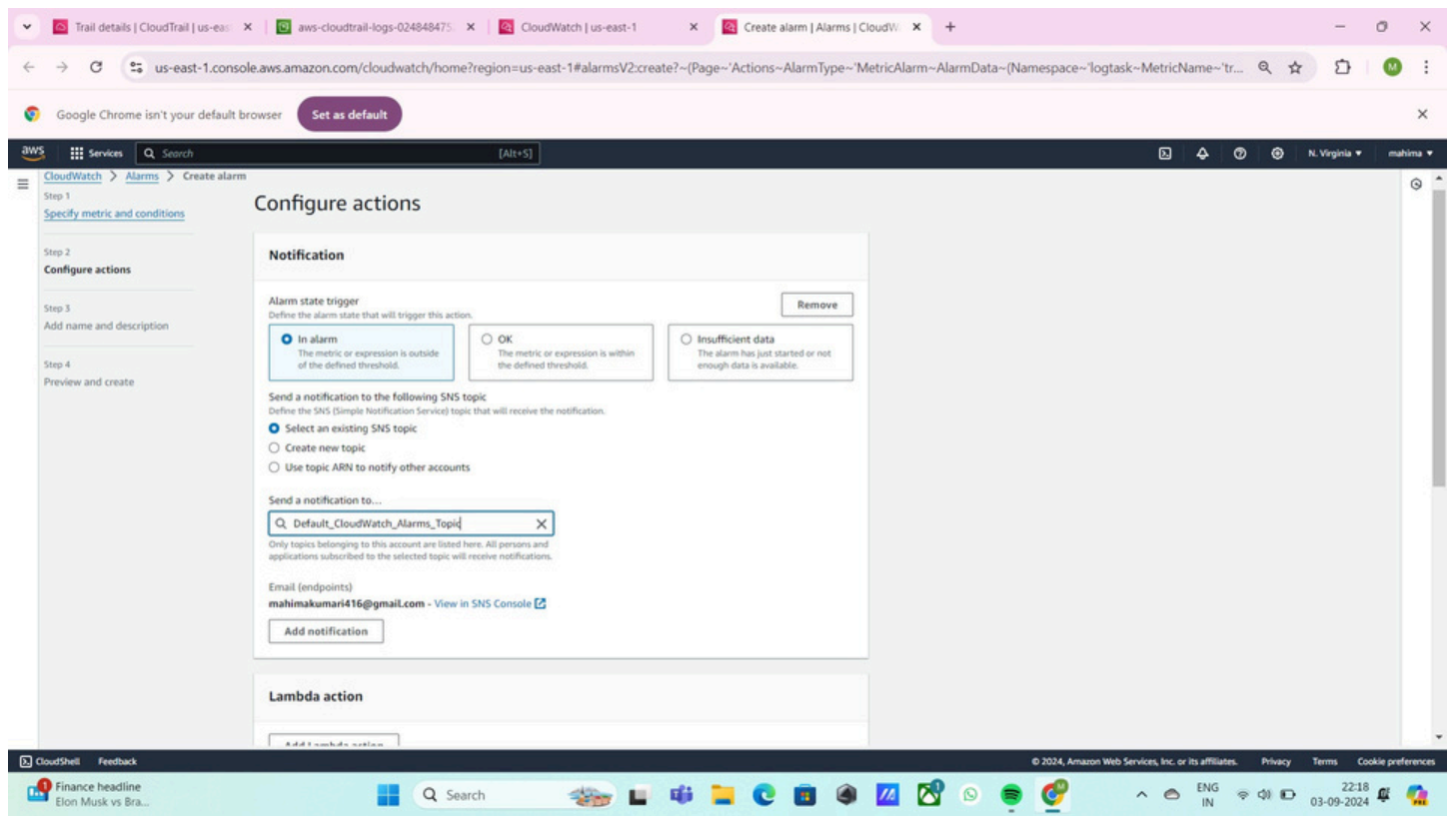
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Light rain

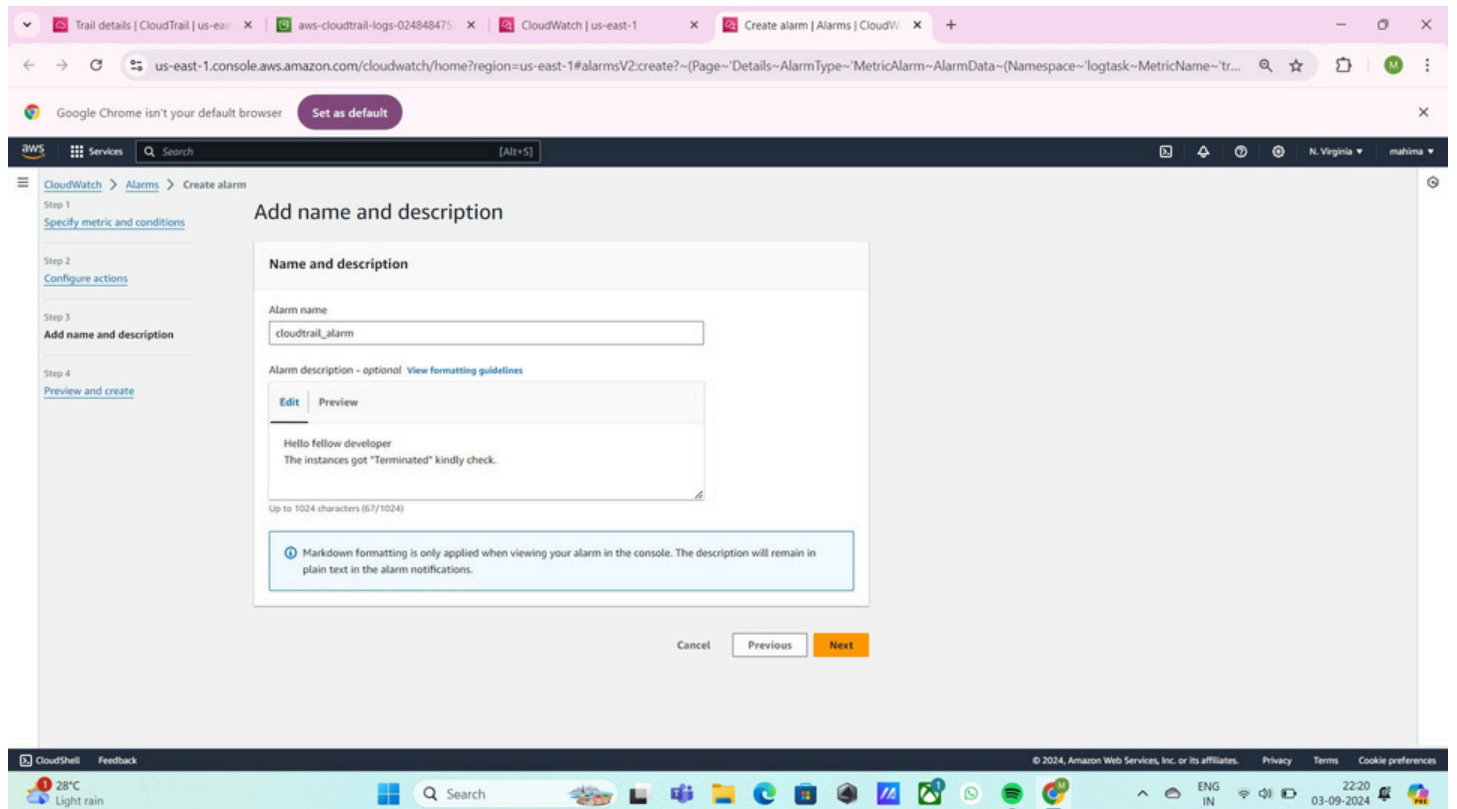
Search

ENG IN

22:18 03-09-2024



8. Add name and description for Alarm and after that preview and create.



Trail details | CloudTrail | us-east-1

aws-cloudtrail-logs-024848475

CloudWatch | us-east-1

Create alarm | Alarms | CloudWatch

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Preview~AlarmType~'MetricAlarm~AlarmData~(Namespace~'logtask~MetricName~'tr...

Google Chrome isn't your default browserSet as default

Services

Search

[Alt+S]

N. Virginia

mahima

Step 1

Specify metric and conditions

Step 2

Configure actions

Step 3

Add name and description

Step 4

Preview and create

Preview and create

Step 1: Specify metric and conditions

Edit

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

No unit

2

1

0

14:30

15:30

16:30

trail_demo

Namespace

logtask

Metric name

trail_demo

Statistic

Sum

Period

1 minute

Conditions

Threshold type

Static

Whenever trail_demo is

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

28°C

Light rain

Search

ENG

IN

22:20

03-09-2024

Trail details | CloudTrail | us-east-1

aws-cloudtrail-logs-024848475

CloudWatch | us-east-1

Create alarm | Alarms | CloudWatch

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Preview~AlarmType~'MetricAlarm~AlarmData~(Namespace~'logtask~MetricName~'tr...

Google Chrome isn't your default browserSet as default

Services

Search

[Alt+S]

N. Virginia

mahima

Step 1

Specify metric and conditions

Step 2

Configure actions

Step 3

Add name and description

Step 4

Preview and create

Conditions

Threshold type

Static

Whenever trail_demo is

Greater/Equal (>=)

than...

1

Additional configuration

Step 2: Configure actions

Edit

Actions

Notification

When in alarm, send a notification to "Default_CloudWatch_Alarms_Topic"

Step 3: Add name and description

Edit

Name and description

Name

cloudtrail_alarm

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

28°C

Light rain

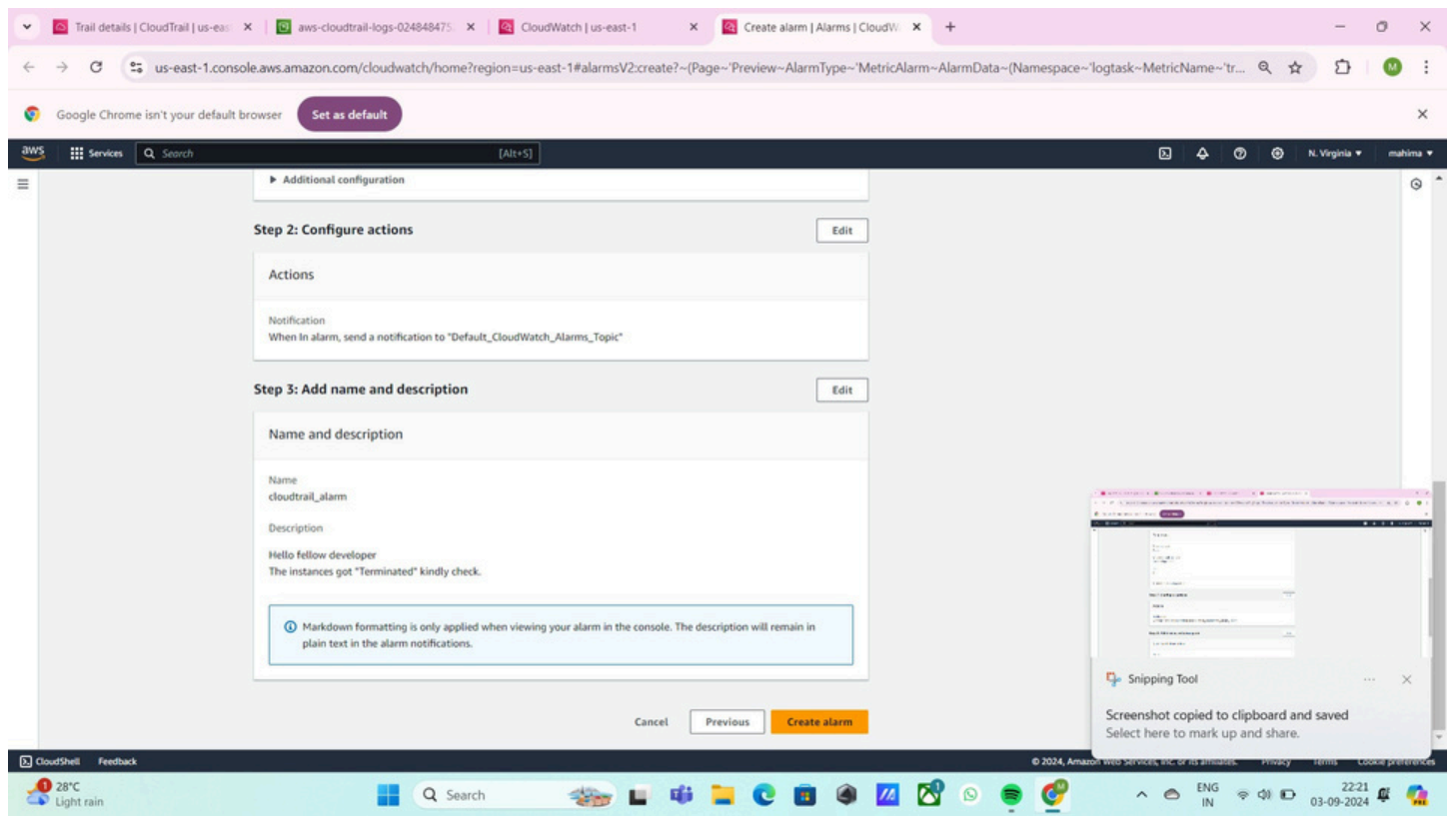
Search

ENG

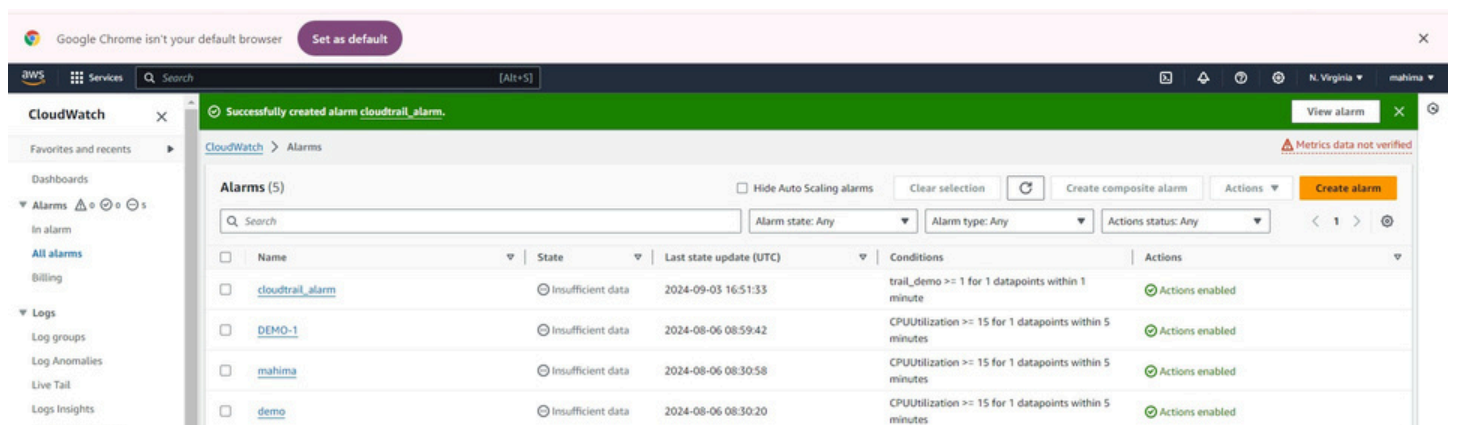
IN

22:21

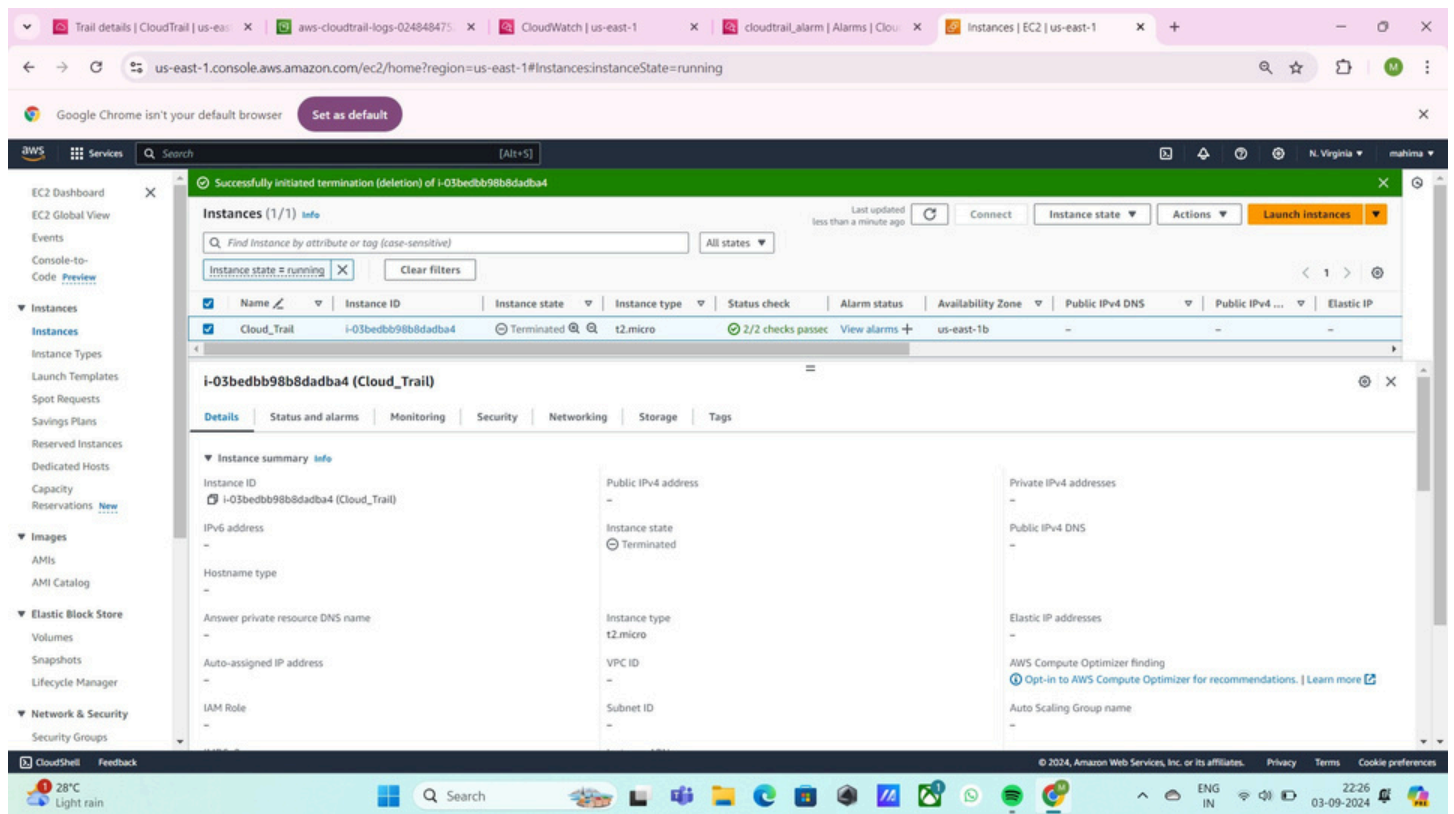
03-09-2024



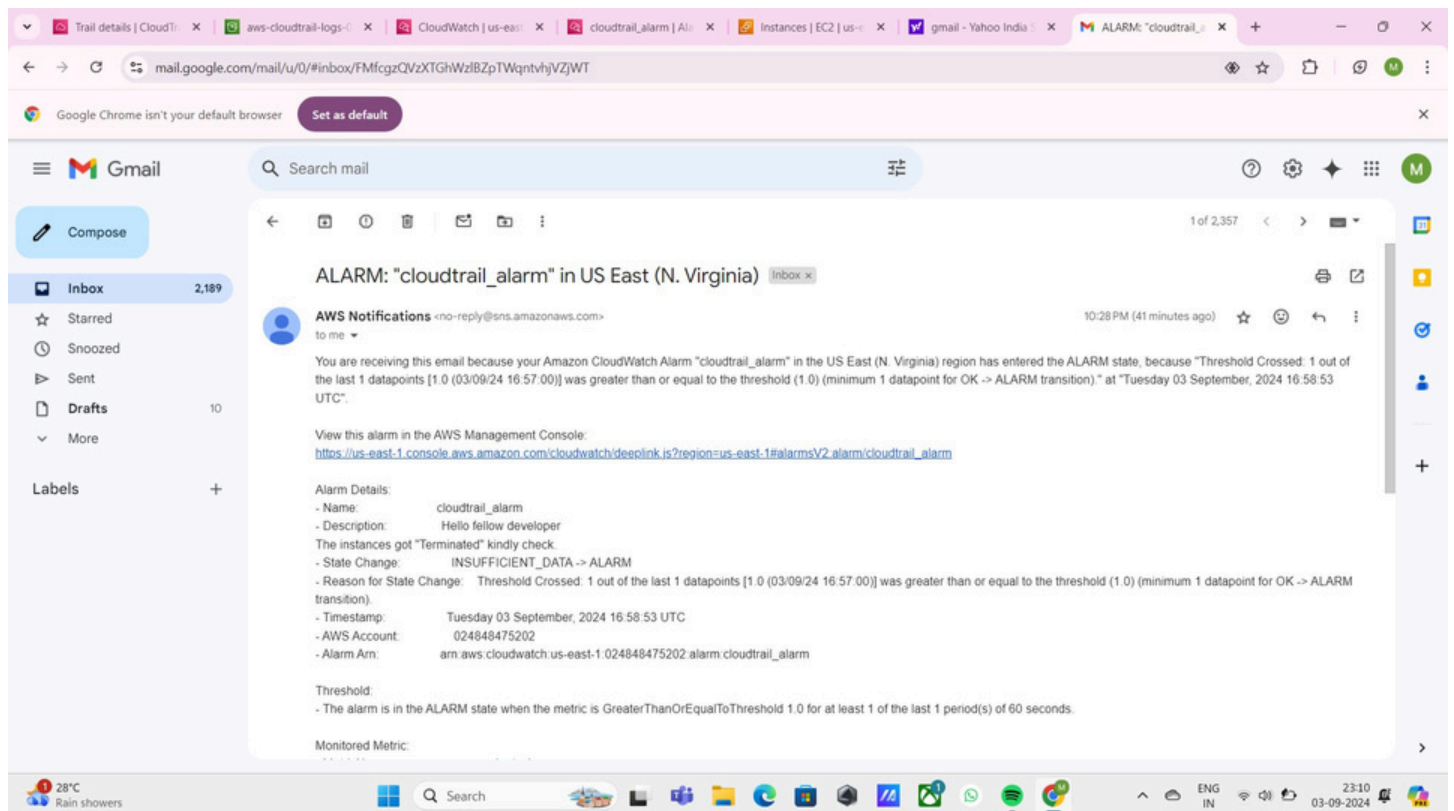
--Successfully created alarm.



9.The termination state will be initiated for the created EC2 instance.



10.If you already have subscription then you can use the same endpoint.
 --Here the alarm is triggered when the instance got terminated.



Trail details | CloudTr...aws-cloudtrail-logs...CloudWatch | us-east...cloudtrail_alarm | Al...Instances | EC2 | us-e...gmail - Yahoo India...ALARM: "cloudtrail...

mail.google.com/mail/u/0/#inbox/FMfcgzQVzXTGhWzIBZpTWqntvhjVZJWT

Google Chrome isn't your default browserSet as default

Gmail

Compose

Inbox2,189

Starred

Snoozed

Sent

Drafts10

More

Labels+

Search mail

1 of 2,357

Threshold:

The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:

MetricNamespace:logtask

MetricName:trail_demo

Dimensions:

Period:60 seconds

Statistic:Sum

Unit:not specified

TreatMissingData:missing

State Change Actions:

OK:

ALARM: [arn:aws:sns:us-east-1:024848475202:Default_CloudWatch_Alarms_Topic]

INSUFFICIENT_DATA:

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:024848475202:Default_CloudWatch_Alarms_Topic:1ac450e0-71b0-4d04-93d9-f5a59148344d&Endpoint=mahimakumar416@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

SIN - MASGame score

Search

ENG IN23:1003-09-2024