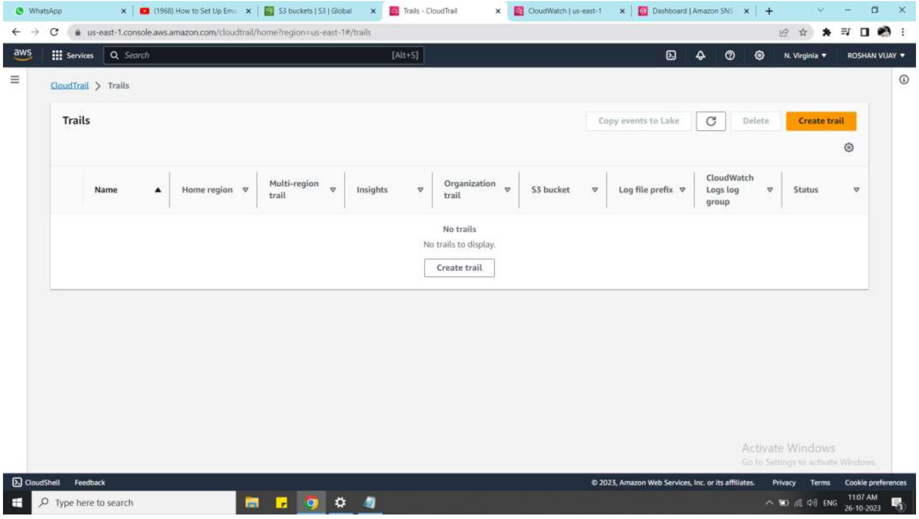
Set Up Email Notifications for CloudWatch Alarms using CloudWatch Log Groups and CloudTrail

Step1:

Go to Cloud trial and create a trial



Trails

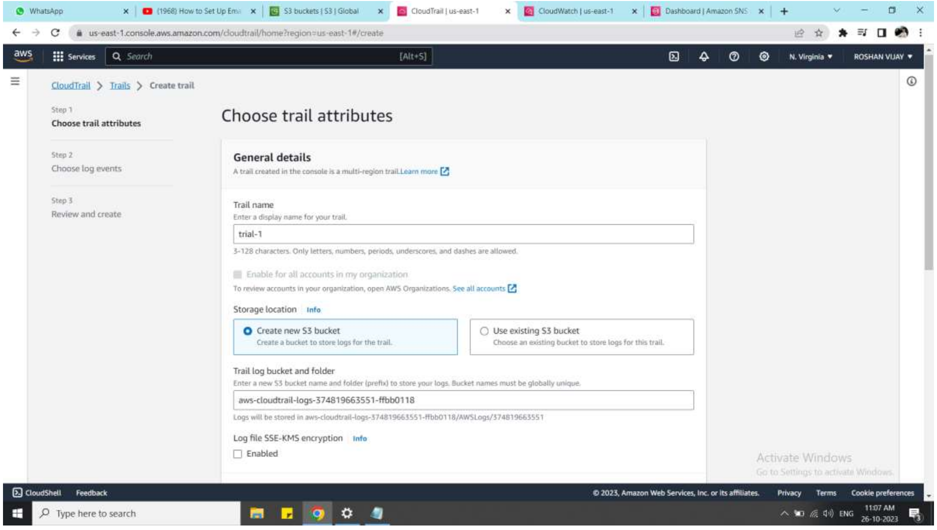
Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status

No trails

No trails to display.

Step 2:

In storage location select create a new s3 bucket and disable the log file SSE-KMS encryption and enable the log file validation



Choose trail attributes

General details

A trail created in the console is a multi-region trail.Learn more

Trail name

Enter a display name for your trail.

trial-1

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info

● Create new S3 bucket
Create a bucket to store logs for the trail.

○ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-374819663551-ffbb0118

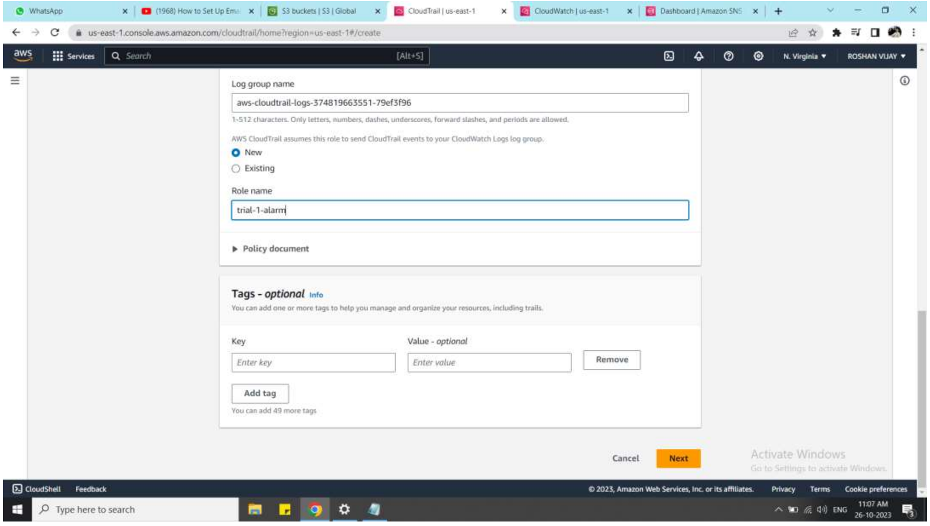
Logs will be stored in aws-cloudtrail-logs-374819663551-ffbb0118/AWSLogs/374819663551

Log file SSE-KMS encryption Info

□ Enabled

Step 3:

In IAM role ,create a new role and give the name to the role and click next



Log group name

aws-cloudtrail-logs-374819663551-79ef3f96

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

● New

○ Existing

Role name

trial-1-alarm

Tags - *optional* Info

You can add one or more tags to help you manage and organize your resources, including trails.

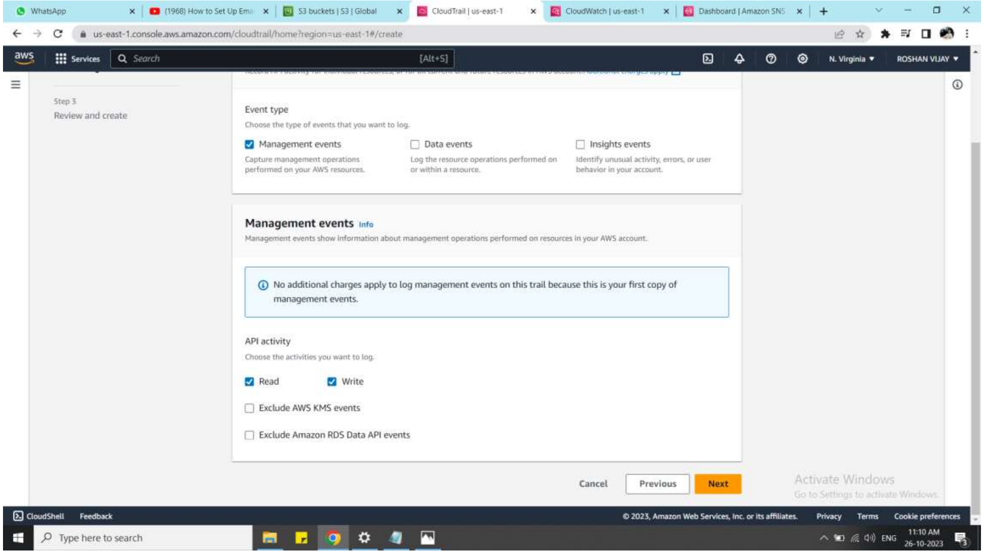
Key: Enter key

Value - *optional*: Enter value

You can add 49 more tags

Step 4:

In the choose Log events tab, select the event type as Event and click next



Event type

Choose the type of events that you want to log.

☑ Management events
Capture management operations performed on your AWS resources.

□ Data events
Log the resource operations performed on or within a resource.

□ Insights events
Identify unusual activity, errors, or user behavior in your account.

Management events Info

Management events show information about management operations performed on resources in your AWS account.

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

API activity

Choose the activities you want to log.

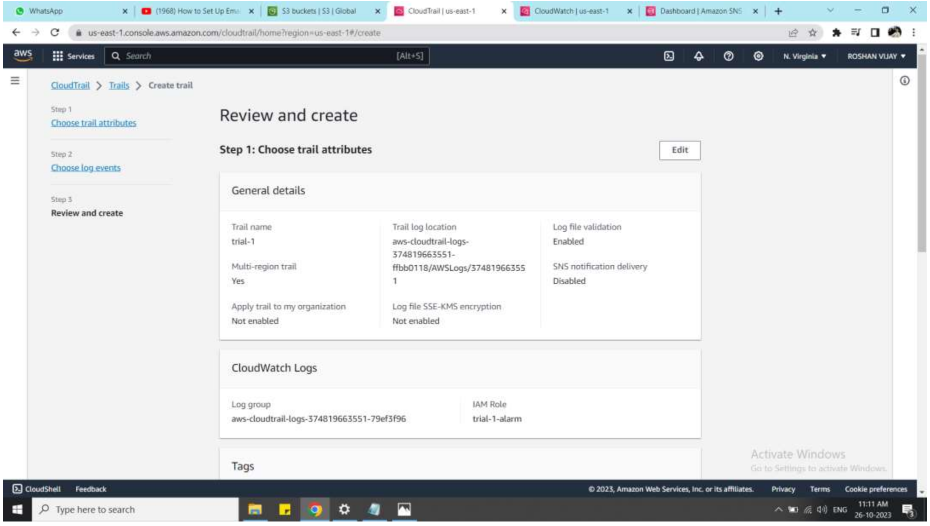
☑ Read ☑ Write

□ Exclude AWS KMS events

□ Exclude Amazon RDS Data API events

Step 5:

Review and create the Cloudtrial log



Review and create

Step 1: Choose trail attributes

General details

Trail name: trial-1

Multi-region trail: Yes

Apply trail to my organization: Not enabled

Trail log location: aws-cloudtrail-logs-374819663551-ffbb0118/AWSLogs/374819663551

Log file SSE-KMS encryption: Not enabled

Log file validation: Enabled

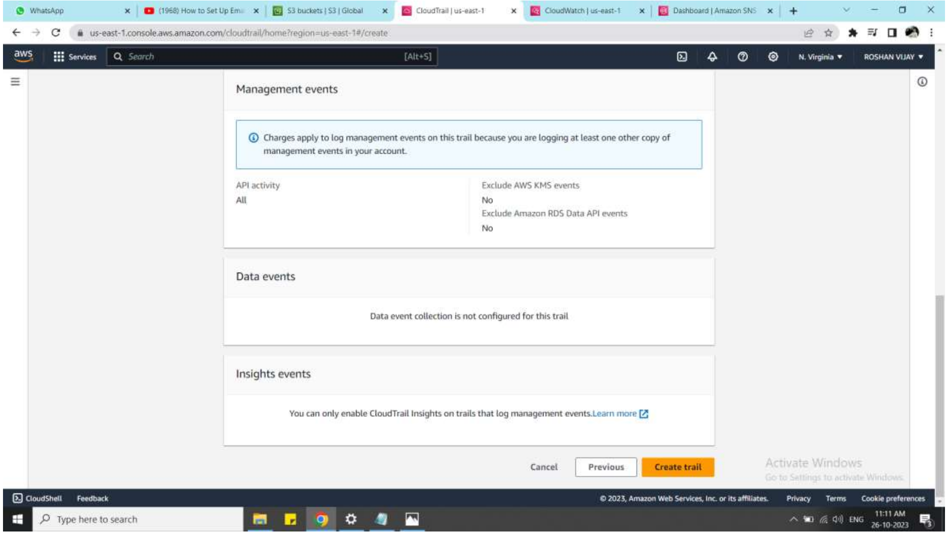
SNS notification delivery: Disabled

CloudWatch Logs

Log group: aws-cloudtrail-logs-374819663551-79ef3f96

IAM Role: trial-1-alarm

Tags



Management events

Charges apply to log management events on this trail because you are logging at least one other copy of management events in your account.

API activity: All

Exclude AWS KMS events: No

Exclude Amazon RDS Data API events: No

Data events

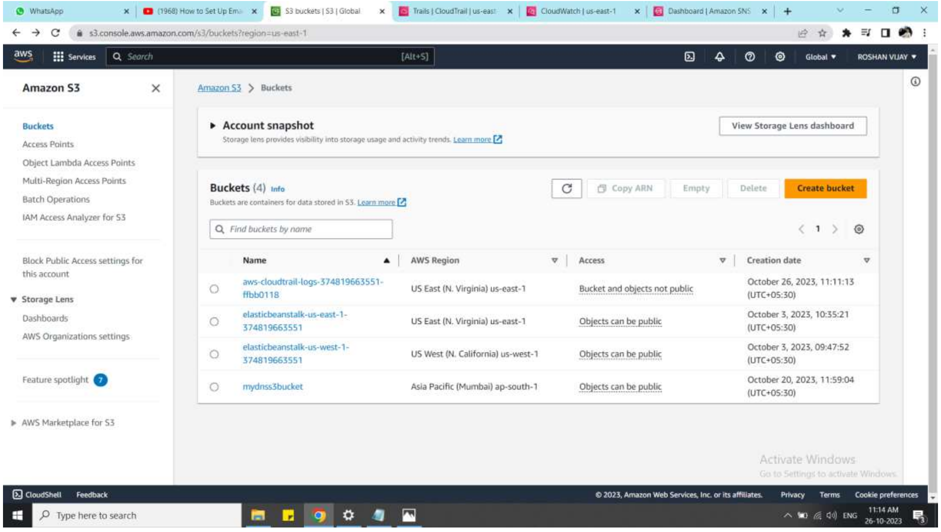
Data event collection is not configured for this trail

Insights events

You can only enable CloudTrail Insights on trails that log management events.Learn more

Step 6:

Now a new s3 bucket is created automatically



Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (4) Info

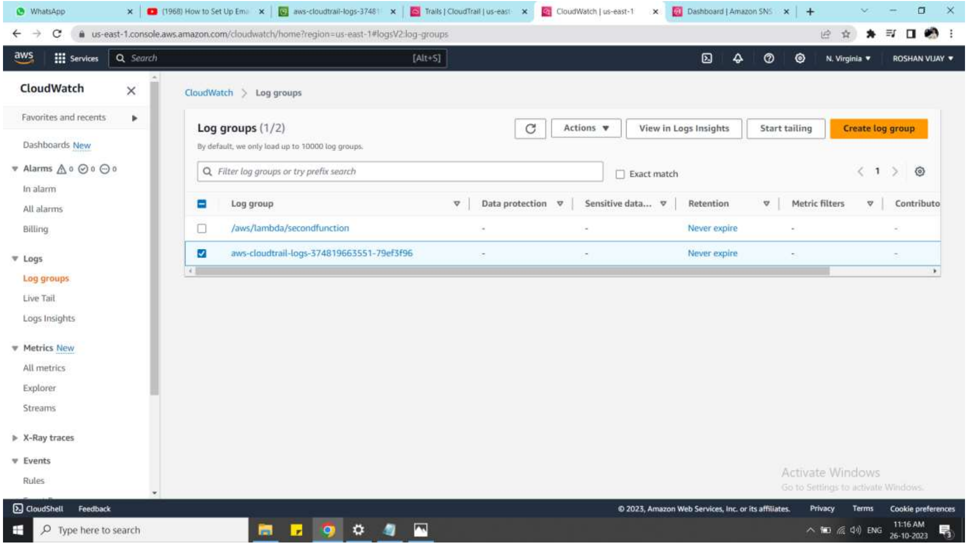
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	aws-cloudtrail-logs-374819663551-ffbb0118	US East (N. Virginia) us-east-1	Bucket and objects not public	October 26, 2023, 11:11:13 (UTC+05:30)
○	elasticbeanstalk-us-east-1-374819663551	US East (N. Virginia) us-east-1	Objects can be public	October 3, 2023, 10:35:21 (UTC+05:30)
○	elasticbeanstalk-us-west-1-374819663551	US West (N. California) us-west-1	Objects can be public	October 3, 2023, 09:47:52 (UTC+05:30)
○	mydnss3bucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	October 20, 2023, 11:59:04 (UTC+05:30)

s3.console.aws.amazon.com/s3/buckets?region=us-east-1
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
View Storage Lens dashboard
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
ROSHAN VIJAY
11:14 AM
26-10-2023

Step 7:

In the cloudwatch log groups, a new cloud trial log is created,it collects some log streams

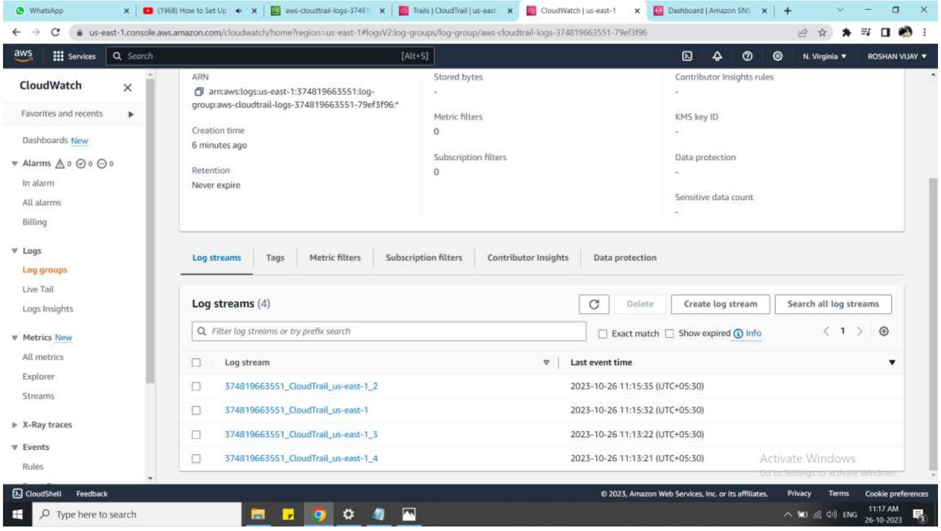


CloudWatch > Log groups

Log groups (1/2)

By default, we only load up to 10000 log groups.

	Log group	Data protection	Sensitive data...	Retention	Metric filters	Contributo
□	/aws/lambda/secondfunction	-	-	Never expire	-	-
☑	aws-cloudtrail-logs-374819663551-79ef3f96	-	-	Never expire	-	-



ARN
arn:aws:logs:us-east-1:374819663551:log-group:aws-cloudtrail-logs-374819663551-79ef3f96:*

Creation time
6 minutes ago

Retention
Never expire

Stored bytes
-

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

KMS key ID
-

Data protection
-

Sensitive data count
-

Log streams (4)

Log stream	Last event time
374819663551_CloudTrail_us-east-1_2	2023-10-26 11:15:35 (UTC+05:30)
374819663551_CloudTrail_us-east-1	2023-10-26 11:15:32 (UTC+05:30)
374819663551_CloudTrail_us-east-1_3	2023-10-26 11:13:22 (UTC+05:30)
374819663551_CloudTrail_us-east-1_4	2023-10-26 11:13:21 (UTC+05:30)

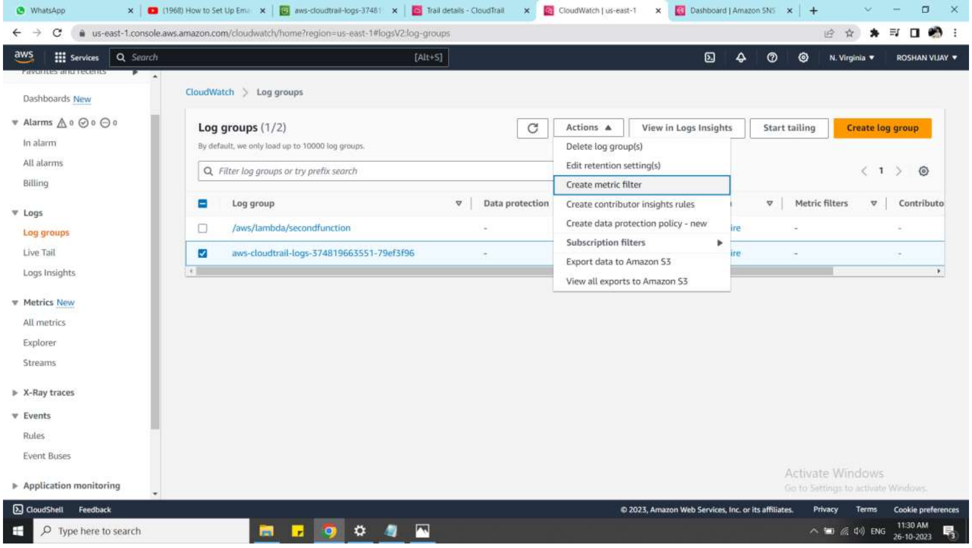
Step 8:

Go to cloud watch metric

cloudwatch log --> Actions --> create a metric filter -->metric filter condition -->next

with this metric filter condition,filter the log which matches the condition

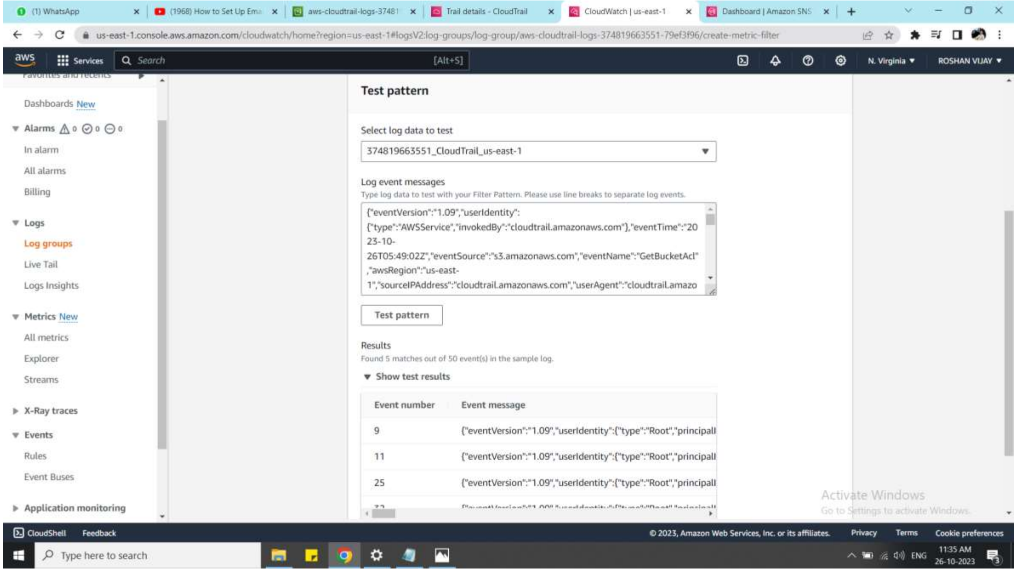
{ ($.eventName = DescribeLogStreams) && ($.recipientAccountId= "374819663551") }



Log groups (1/2)

By default, we only load up to 10000 log groups.

Log group	Data protection	Metric filters
/aws/lambda/secondfunction	-	-
aws-cloudtrail-logs-374819663551-79ef3f96	-	-



Test pattern

Select log data to test

374819663551_CloudTrail_us-east-1

Log event messages

Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

```
{"eventVersion":"1.09","userIdentity":
{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"20
23-10-
26T05:49:02Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketAcl"
,"awsRegion":"us-east-
1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazo
```

Test pattern

Results

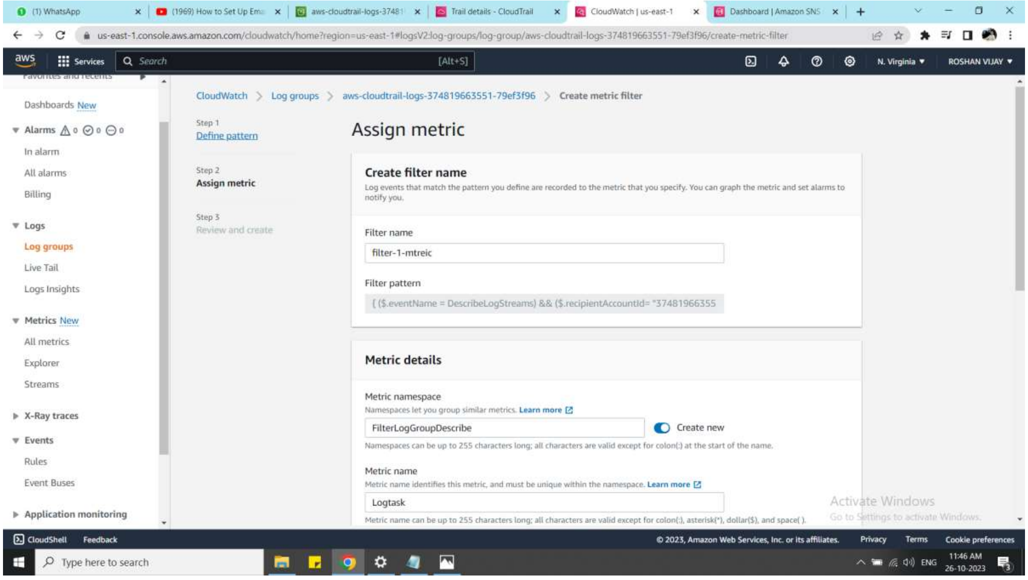
Found 5 matches out of 50 event(s) in the sample log.

▼ Show test results

Event number	Event message
9	{"eventVersion":"1.09","userIdentity":{"type":"Root","principalI
11	{"eventVersion":"1.09","userIdentity":{"type":"Root","principalI
25	{"eventVersion":"1.09","userIdentity":{"type":"Root","principalI

Step 9:

metric filter name --> metric name space --> metric name --> metric value-->next-->review and create



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/aws-cloudtrail-logs-374819663551-79ef3f96/create-metric-filter
Services
Search
[Alt+S]
N. Virginia
ROSHAN VIJAY
CloudWatch > Log groups > aws-cloudtrail-logs-374819663551-79ef3f96 > Create metric filter
Step 1
Define pattern
Step 2
Assign metric
Step 3
Review and create
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Assign metric

Create filter name

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter name: filter-1-mtreic

Filter pattern: { ($.eventName = DescribeLogStreams) && ($.recipientAccountId= "37481966355

Metric details

Metric namespace

Namespaces let you group similar metrics. Learn more

FilterLogGroupDescribe ● Create new

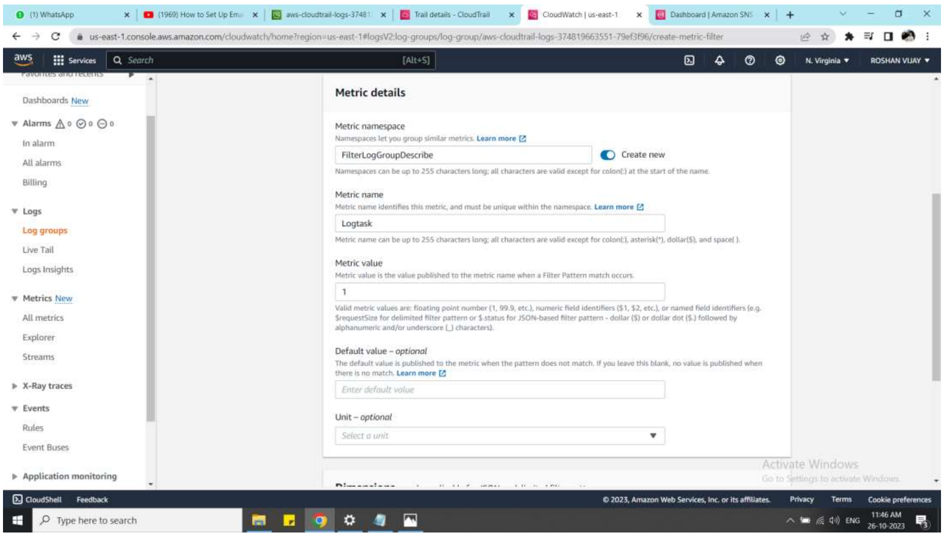
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

Metric name

Metric name identifies this metric, and must be unique within the namespace. Learn more

Logtask

Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).



Metric details

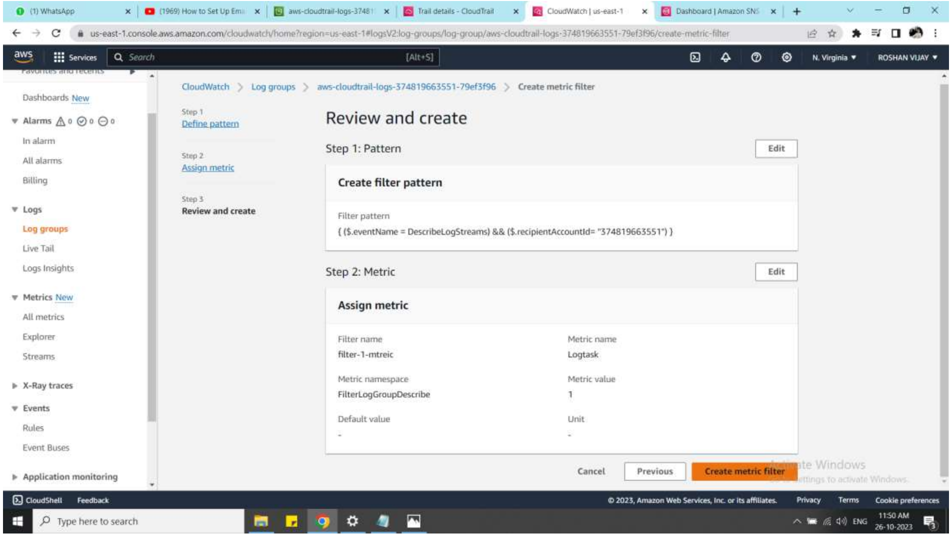
Metric namespace
Namespaces let you group similar metrics. Learn more
FilterLogGroupDescribe ● Create new
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

Metric name
Metric name identifies this metric, and must be unique within the namespace. Learn more
Logtask
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).

Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.
1
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers ($1, $2, etc.), or named field identifiers (e.g. $requestSize for delimited filter pattern or $.status for JSON-based filter pattern - dollar ($) or dollar dot ($.) followed by alphanumeric and/or underscore (_) characters).

Default value – *optional*
The default value is published to the metric when the pattern does not match. If you leave this blank, no value is published when there is no match. Learn more
Enter default value

Unit – *optional*
Select a unit ▼


CloudWatch | us-east-1
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/aws-cloudtrail-logs-374819663551-79ef3f96/create-metric-filter
CloudWatch > Log groups > aws-cloudtrail-logs-374819663551-79ef3f96 > Create metric filter
Step 1
Define pattern
Step 2
Assign metric
Step 3
Review and create

Review and create

Step 1: Pattern — Edit

Create filter pattern

Filter pattern
{ ($.eventName = DescribeLogStreams) && ($.recipientAccountId= "374819663551") }

Step 2: Metric — Edit

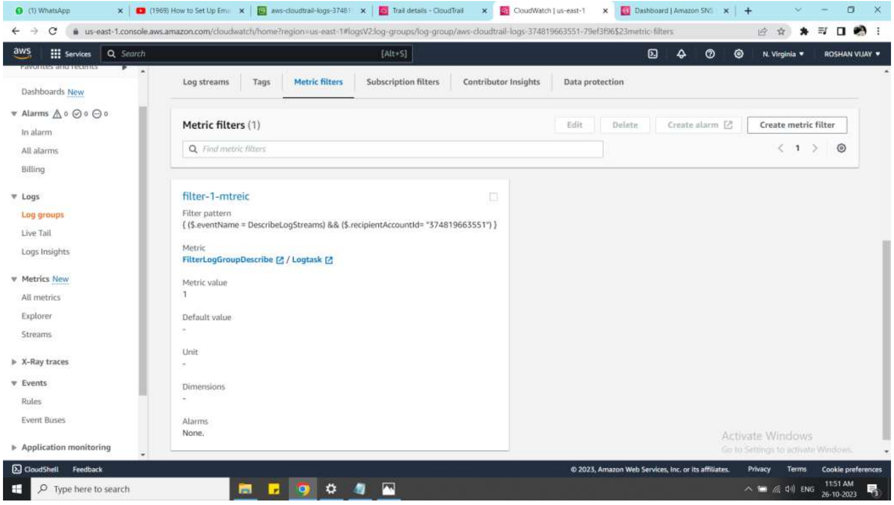
Assign metric

Filter name	Metric name
filter-1-mtreic	Logtask
Metric namespace	Metric value
FilterLogGroupDescribe	1
Default value	Unit
-	-

Cancel
Previous
Create metric filter

Step 10:

We have configured the metric filter.



Metric filters (1)

filter-1-mtreic

Filter pattern
{ ($.eventName = DescribeLogStreams) && ($.recipientAccountId= "374819663551") }

Metric
FilterLogGroupDescribe / Logtask

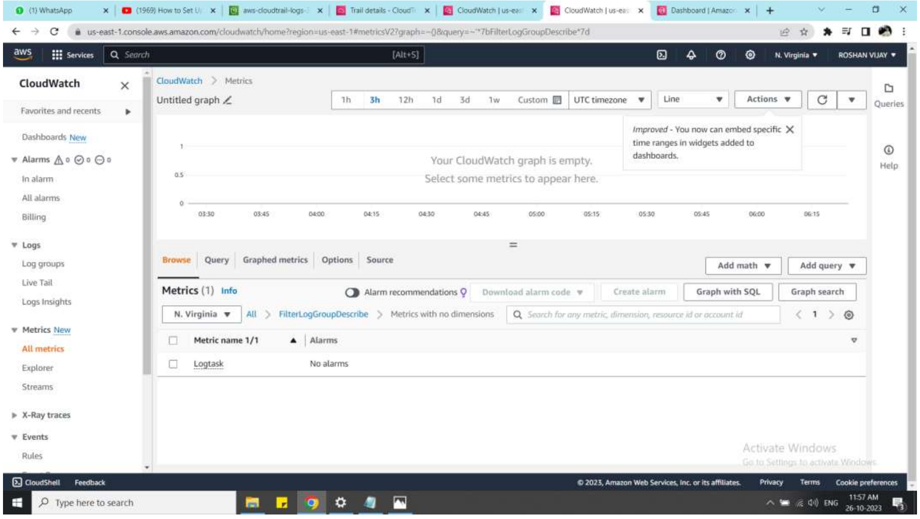
Metric value
1

Default value
-

Unit
-

Dimensions
-

Alarms
None.



CloudWatch > Metrics

Untitled graph

Improved - You now can embed specific time ranges in widgets added to dashboards.

Your CloudWatch graph is empty.
Select some metrics to appear here.

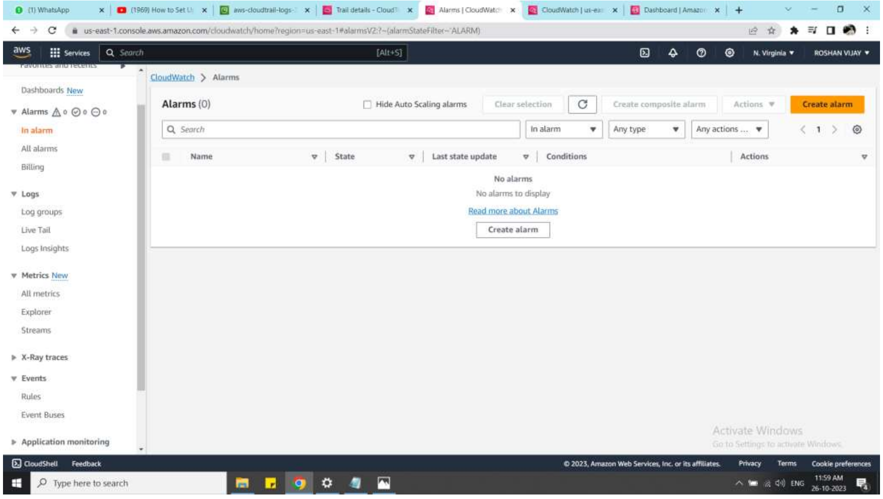
Metrics (1)

N. Virginia > All > FilterLogGroupDescribe > Metrics with no dimensions

Metric name 1/1	Alarms
Logtask	No alarms

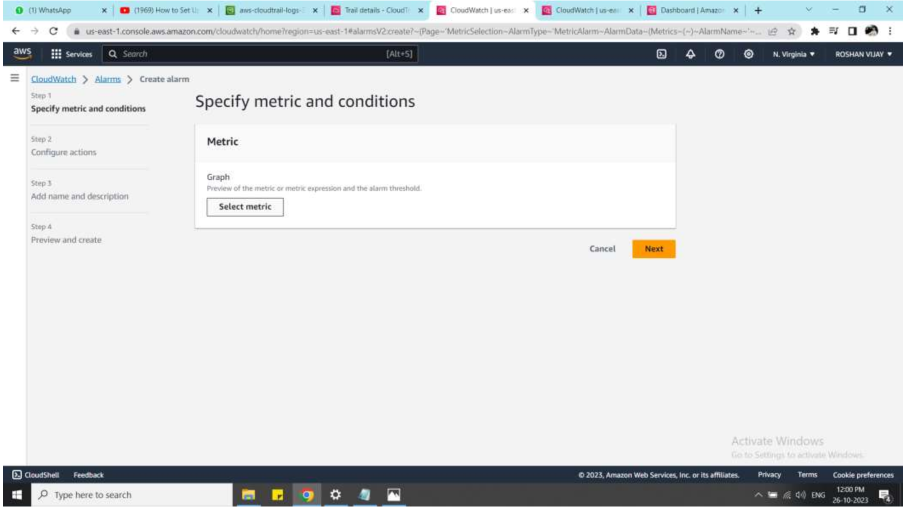
Step 11:

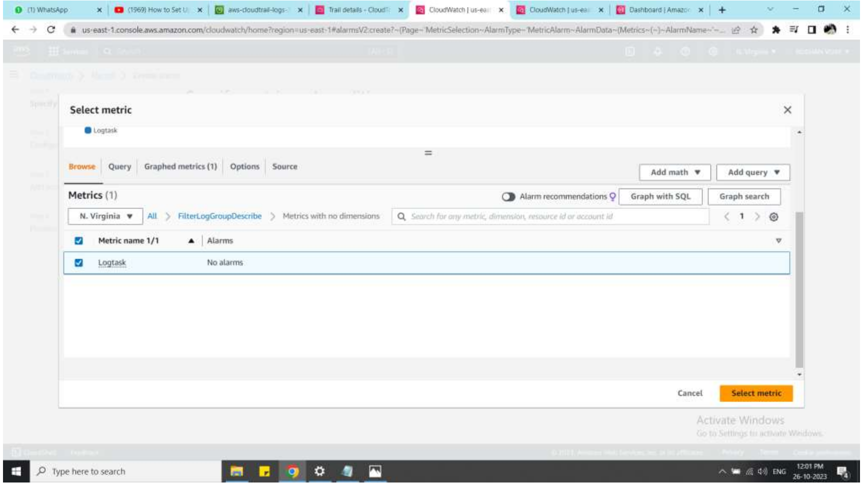
Next goto the cloudwatch alarm and create the new alarm



Step 12:

select metric --> in the metric section,select the time period to 10s


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
Specify metric and conditions
Metric
Graph
Preview of the metric or metric expression and the alarm threshold.
Select metric
Cancel
Next



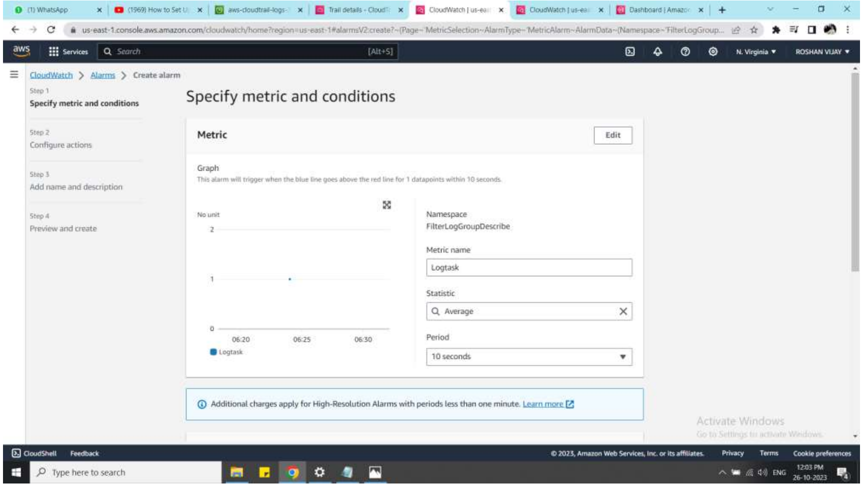
Select metric

Browse | Query | Graphed metrics (1) | Options | Source

Metrics (1)

N. Virginia ▾ | All > FilterLogGroupDescribe > Metrics with no dimensions

☑ Metric name 1/1	Alarms
☑ Logtask	No alarms



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

Specify metric and conditions

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 10 seconds.

Namespace
FilterLogGroupDescribe

Metric name
Logtask

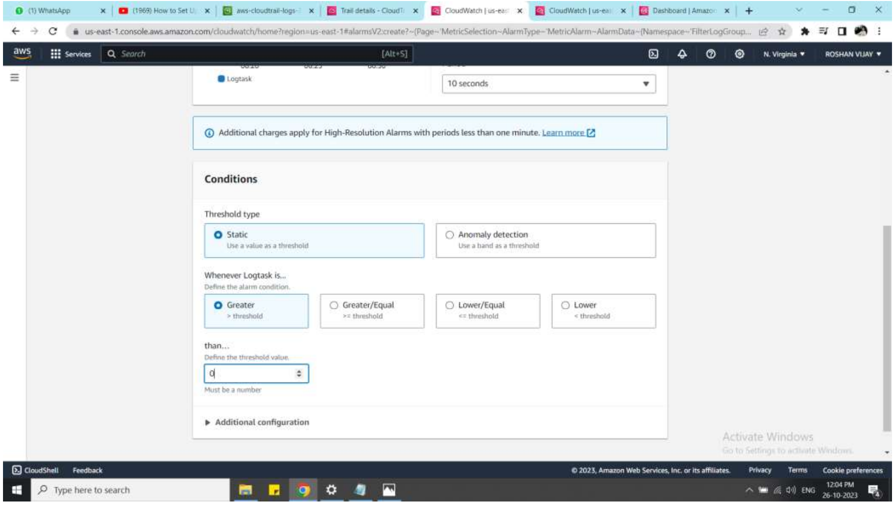
Statistic
Average

Period
10 seconds

Additional charges apply for High-Resolution Alarms with periods less than one minute. Learn more

Step 13:

in conditions select the threshhold type as static and greater than 0 --> next



Period
10 seconds

Additional charges apply for High-Resolution Alarms with periods less than one minute. Learn more

Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever Logtask is...
Define the alarm condition.

● Greater
> threshold

○ Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

○ Lower
< threshold

than...
Define the threshold value.

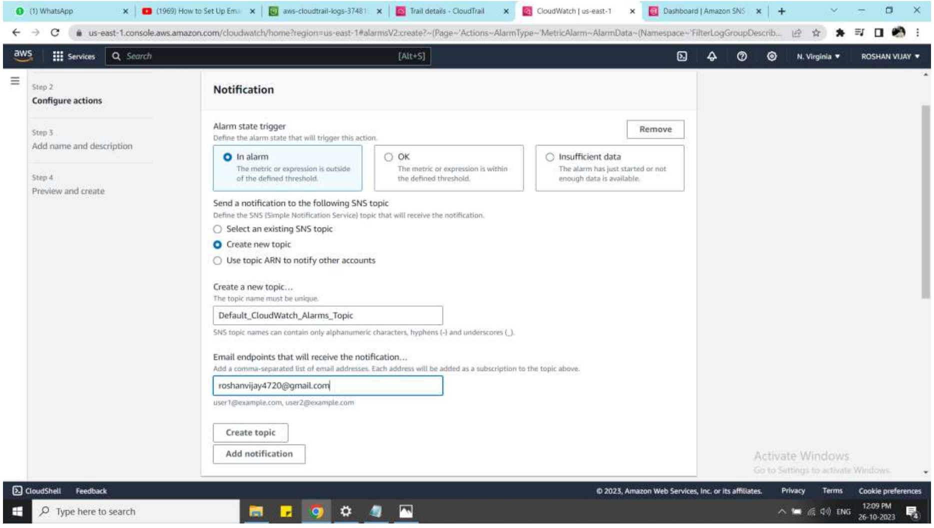
0

Must be a number

▸ Additional configuration

Step 14:

In the configure notification tab, alarm state trigger --> In alarm -->SNS topic --> create a new topic --> add the user email-id --> create topic



Notification

Alarm state trigger

Define the alarm state that will trigger this action.

● In alarm — The metric or expression is outside of the defined threshold.

○ OK — The metric or expression is within the defined threshold.

○ Insufficient data — The alarm has just started or not enough data is available.

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

○ Select an existing SNS topic

● Create new topic

○ Use topic ARN to notify other accounts

Create a new topic...

The topic name must be unique.

Default_CloudWatch_Alarms_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

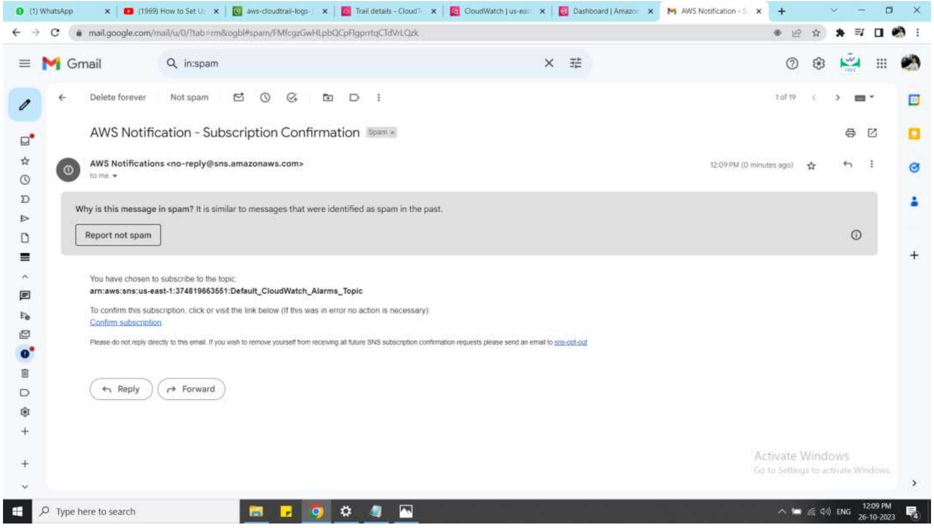
roshanvijay4720@gmail.com

user1@example.com, user2@example.com

Step 15:

now check the email inbox and confirm the subscription

now new SNS topic has been created



AWS Notification - Subscription Confirmation

AWS Notifications <no-reply@sns.amazonaws.com>

to me

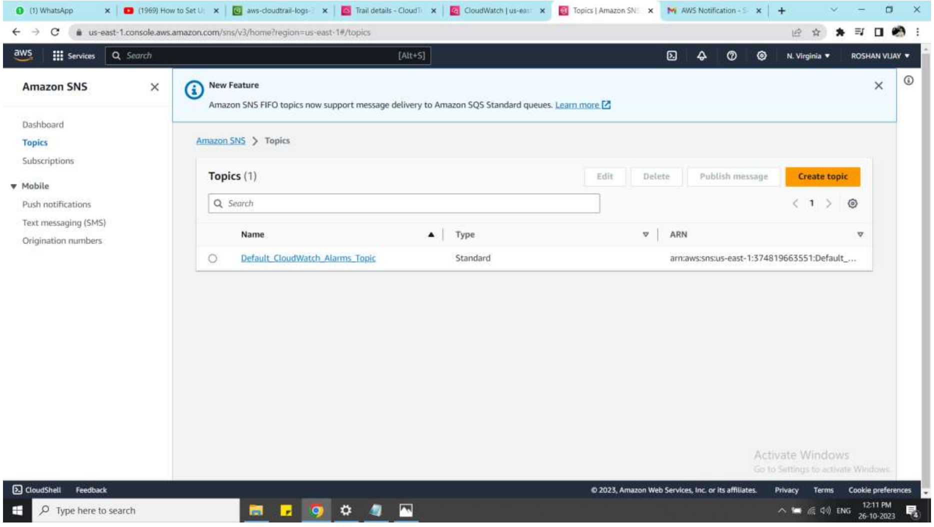
12:09 PM (0 minutes ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:374819663551:Default_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out



New Feature

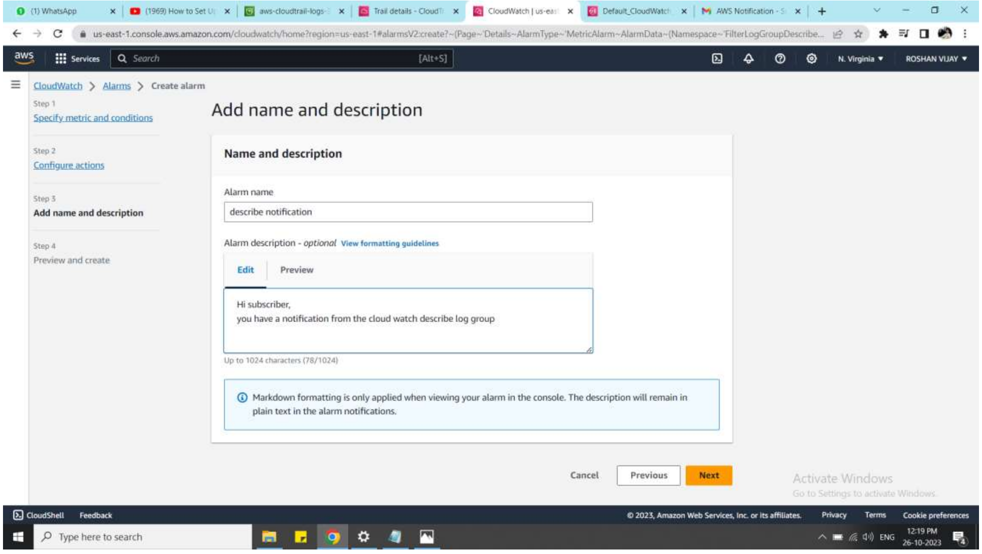
Amazon SNS FIFO topics now support message delivery to Amazon SQS Standard queues. Learn more

Topics (1)

Name	Type	ARN
○ Default_CloudWatch_Alarms_Topic	Standard	arn:aws:sns:us-east-1:374819663551:Default_...

Step 16:

Add the alarm name and customize the notification message and review the alarm configuration and create alarm


us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Details~AlarmType~'MetricAlarm~AlarmData~(Namespace~'FilterLogGroupDescribe...
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
Edit
Preview
View formatting guidelines
Cancel
Previous
Next
N. Virginia
ROSHAN VIJAY
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Activate Windows
Go to Settings to activate Windows.
Type here to search
12:19 PM
26-10-2023

Add name and description

Name and description

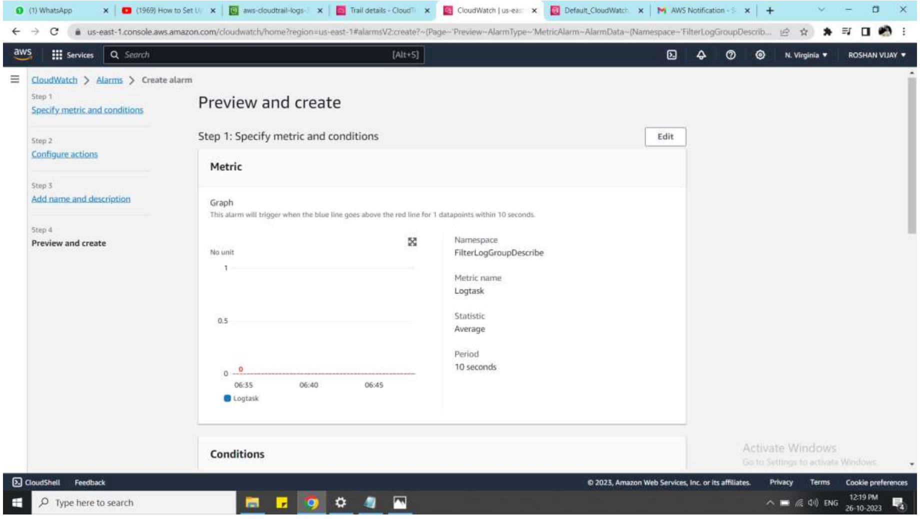
Alarm name: describe notification

Alarm description - *optional*

Hi subscriber,
you have a notification from the cloud watch describe log group

Up to 1024 characters (78/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.



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 10 seconds.

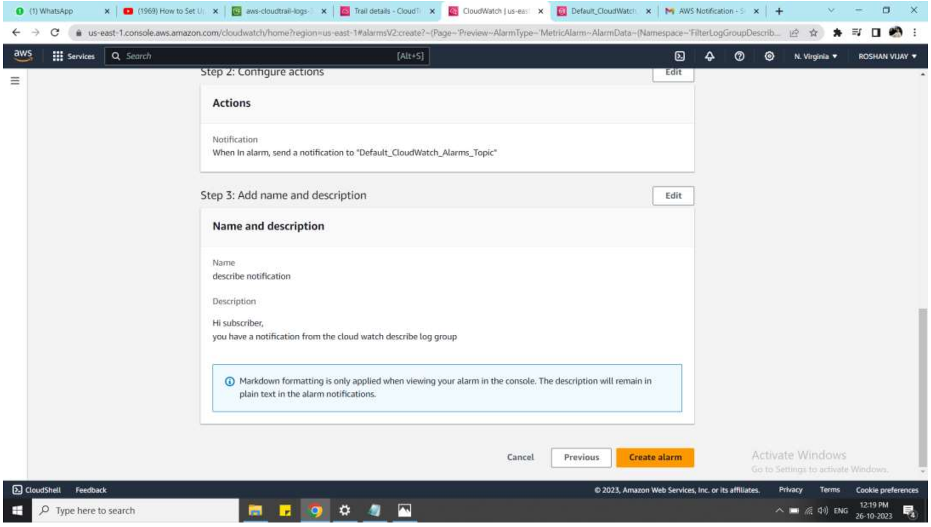
Namespace
FilterLogGroupDescribe

Metric name
Logtask

Statistic
Average

Period
10 seconds

Conditions



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
describe notification

Description

Hi subscriber,
you have a notification from the cloud watch describe log group

ⓘ Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

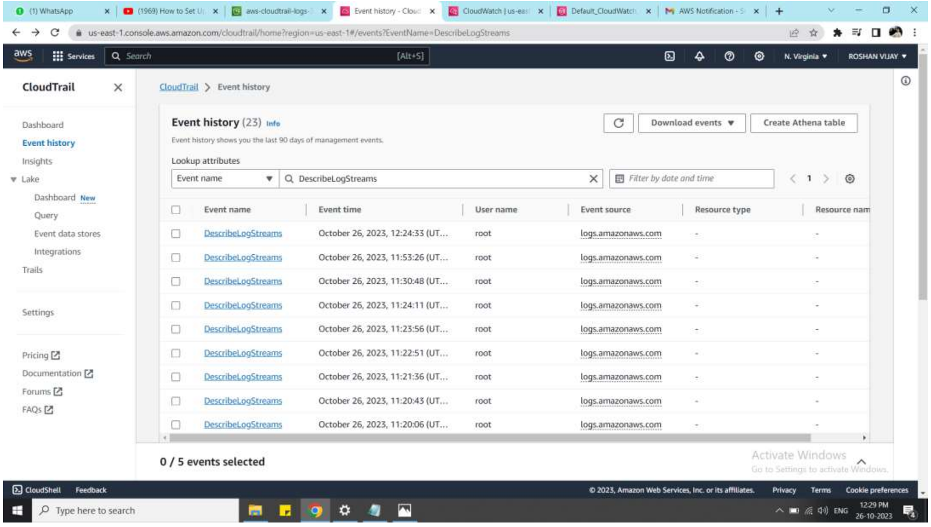
Cancel

Previous

Create alarm

Step 17:

Now go to the cloud Trial Event history and check whether the log configured is started creating the logs



us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/events?EventName=DescribeLogStreams

CloudTrail > Event history

Event history (23)

Event history shows you the last 90 days of management events.

Lookup attributes

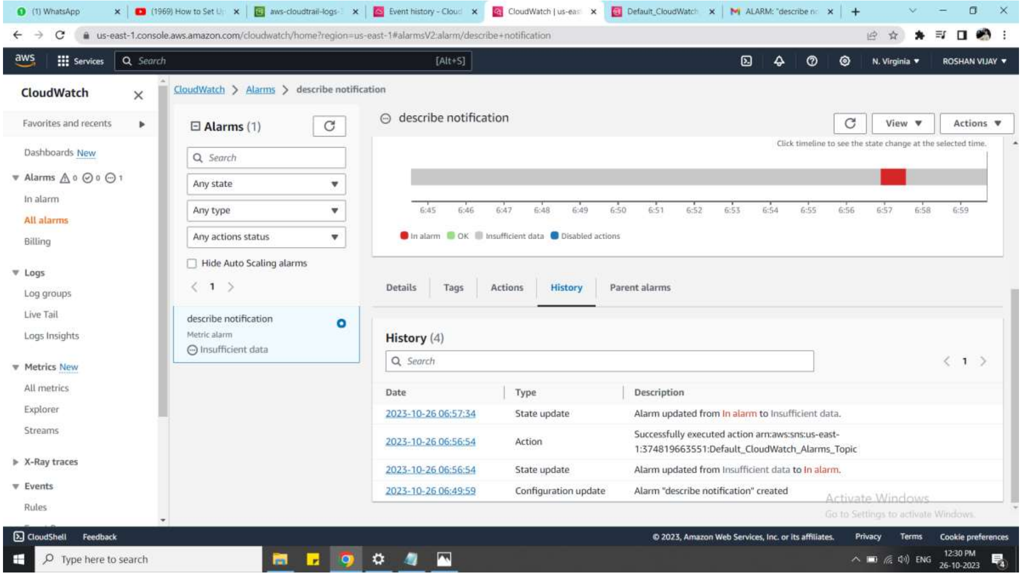
Event name: DescribeLogStreams

Event name	Event time	User name	Event source	Resource type	Resource nam
DescribeLogStreams	October 26, 2023, 12:24:33 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:53:26 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:30:48 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:24:11 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:23:56 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:22:51 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:21:36 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:20:43 (UT...	root	logs.amazonaws.com	-	-
DescribeLogStreams	October 26, 2023, 11:20:06 (UT...	root	logs.amazonaws.com	-	-

0 / 5 events selected

Step 18:

In the cloud watch alarm, check the alarm history changes, and now the notification email will be dropped in the inbox



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/describe+notification

CloudWatch > Alarms > describe notification

describe notification — Metric alarm — Insufficient data

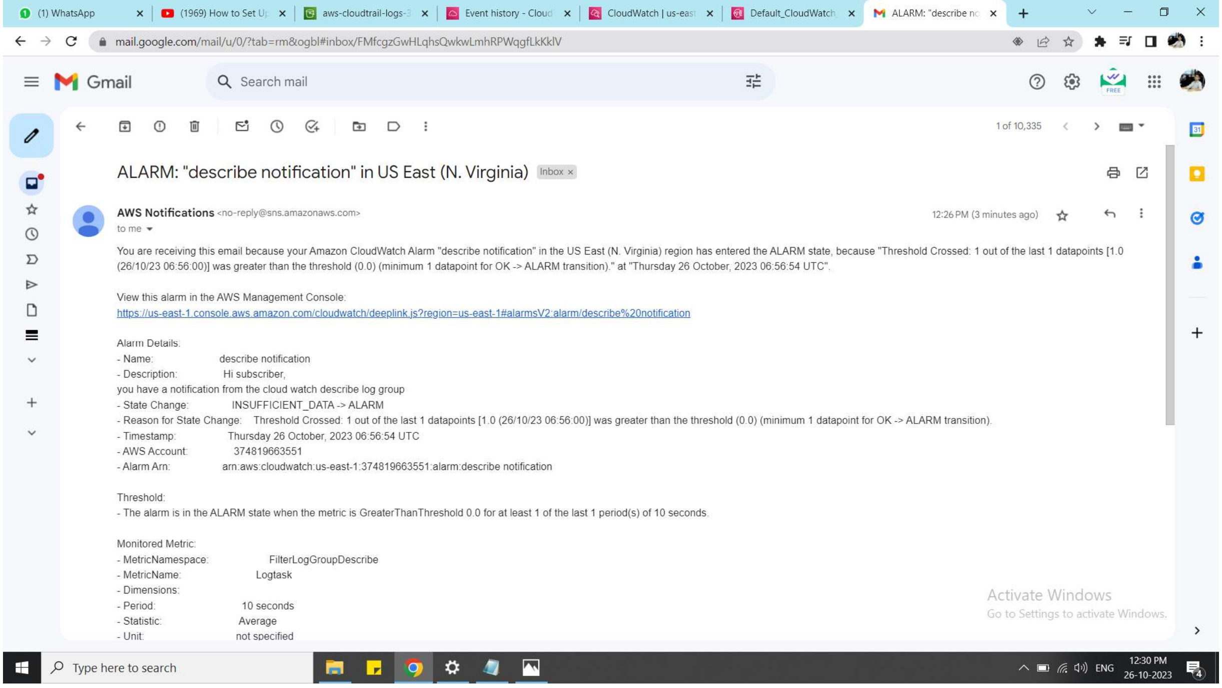
Click timeline to see the state change at the selected time.

● In alarm ● OK ● Insufficient data ● Disabled actions

Details | Tags | Actions | History | Parent alarms

History (4)

Date	Type	Description
2023-10-26 06:57:34	State update	Alarm updated from In alarm to Insufficient data.
2023-10-26 06:56:54	Action	Successfully executed action arn:aws:sns:us-east-1:374819663551:Default_CloudWatch_Alarms_Topic
2023-10-26 06:56:54	State update	Alarm updated from Insufficient data to In alarm.
2023-10-26 06:49:59	Configuration update	Alarm "describe notification" created



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

AWS Notifications <no-reply@sns.amazonaws.com>
to me

12:26 PM (3 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "describe notification" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (26/10/23 06:56:00)] was greater than the threshold (0.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thursday 26 October, 2023 06:56:54 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/describe%20notification

Alarm Details:
- Name: describe notification
- Description: Hi subscriber,
you have a notification from the cloud watch describe log group
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (26/10/23 06:56:00)] was greater than the threshold (0.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 26 October, 2023 06:56:54 UTC
- AWS Account: 374819663551
- Alarm Arn: arn:aws:cloudwatch:us-east-1:374819663551:alarm:describe notification

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 0.0 for at least 1 of the last 1 period(s) of 10 seconds.

Monitored Metric:
- MetricNamespace: FilterLogGroupDescribe
- MetricName: Logtask
- Dimensions:
- Period: 10 seconds
- Statistic: Average
- Unit: not specified