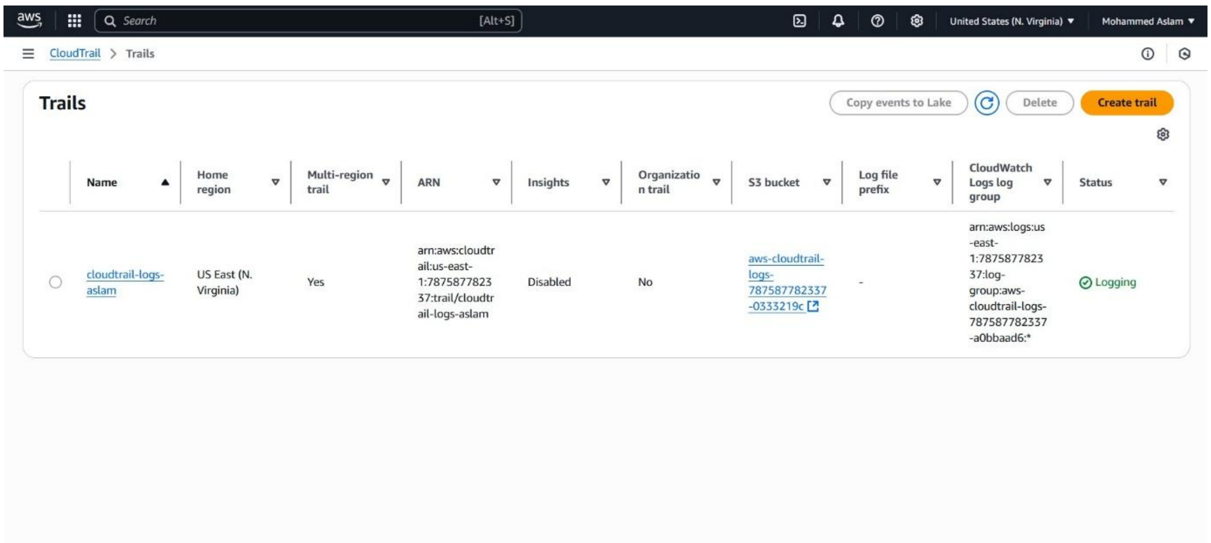
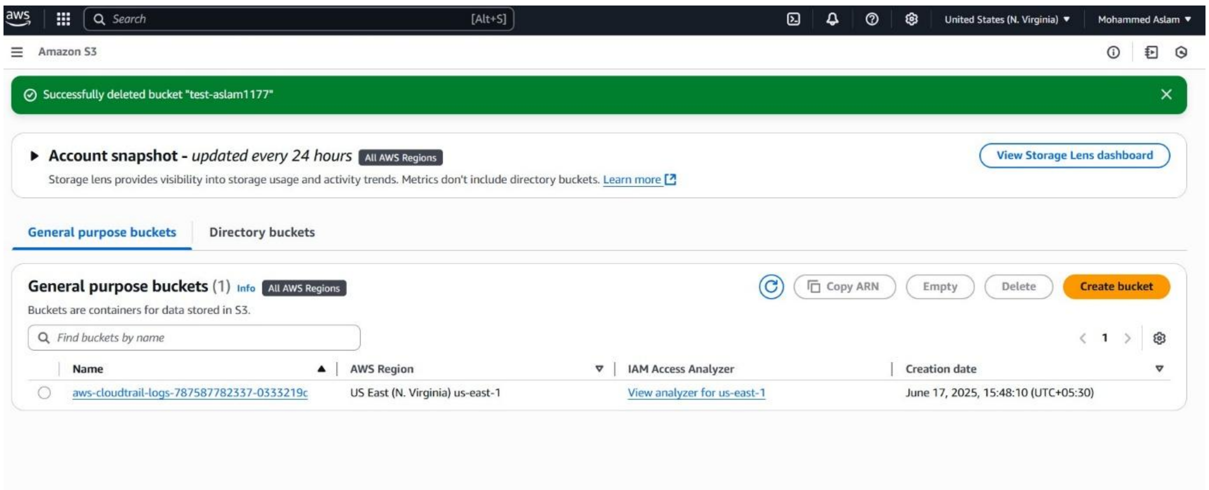
1) Enable cloudtrail monitoring and store the events in s3 and cloudwatch log events.



Trails

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	cloudtrail-logs-aslam	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:787587782337:trail/cloudtrail-logs-aslam	Disabled	No	aws-cloudtrail-logs-787587782337-0333219c	-	arn:aws:logs:us-east-1:787587782337:log-group:aws-cloudtrail-logs-787587782337-a0bbaad6:*	✓ Logging

S3 bucket created after cloudtrail enabling



✓ Successfully deleted bucket "test-aslam1177"

▶ **Account snapshot -** *updated every 24 hours* All AWS Regions

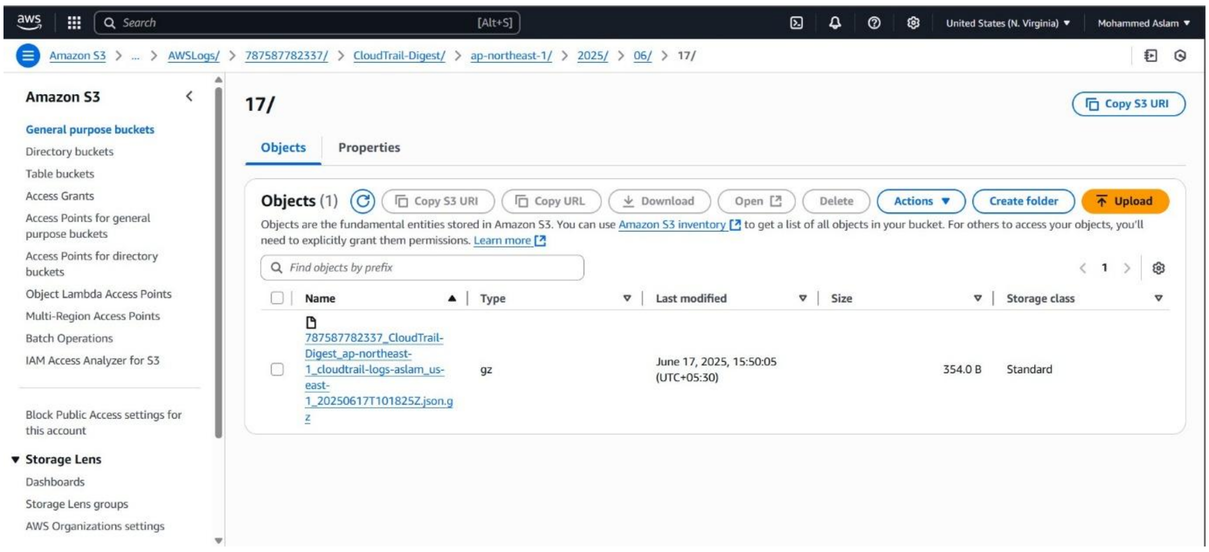
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	aws-cloudtrail-logs-787587782337-0333219c	US East (N. Virginia) us-east-1	View analyzer for us-east-1	June 17, 2025, 15:48:10 (UTC+05:30)

Logs in s3



aws
Search
[Alt+S]
United States (N. Virginia) ▼
Mohammed Aslam ▼
Amazon S3 > ... > AWSLogs/ > 787587782337/ > CloudTrail-Digest/ > ap-northeast-1/ > 2025/ > 06/ > 17/
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points for general purpose buckets
Access Points for directory buckets
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
Storage Lens groups
AWS Organizations settings
17/
Copy S3 URI
Objects
Properties

Objects (1)

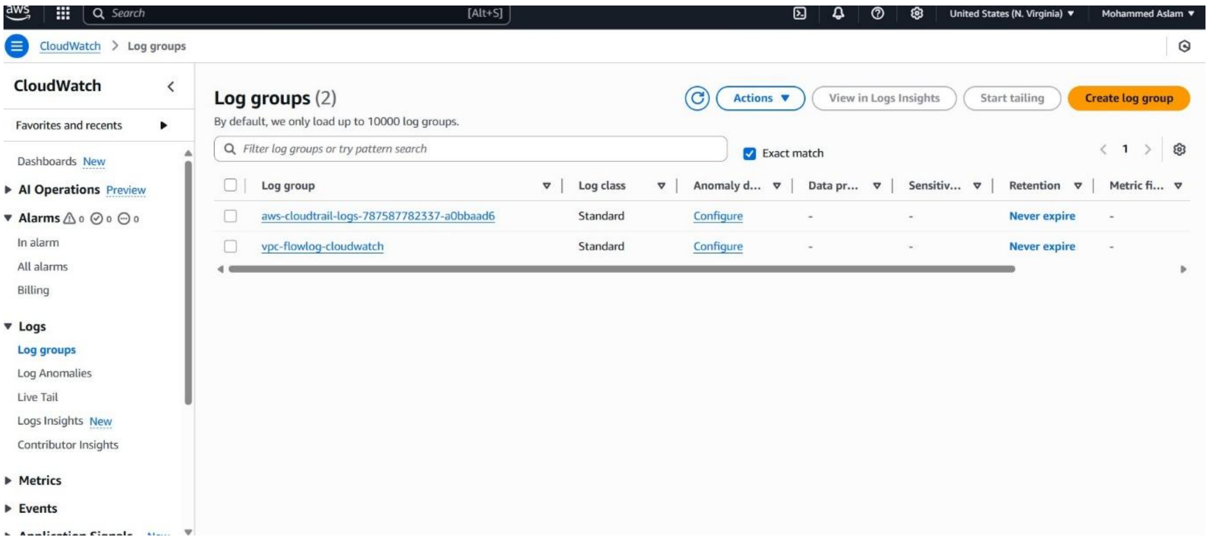
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix
< 1 >

□	Name	Type	Last modified	Size	Storage class
□	787587782337_CloudTrail-Digest_ap-northeast-1_cloudtrail-logs-aslam_us-east-1_20250617T101825Z.json.gz	gz	June 17, 2025, 15:50:05 (UTC+05:30)	354.0 B	Standard

Automatically group got creating post enabling cloud trail



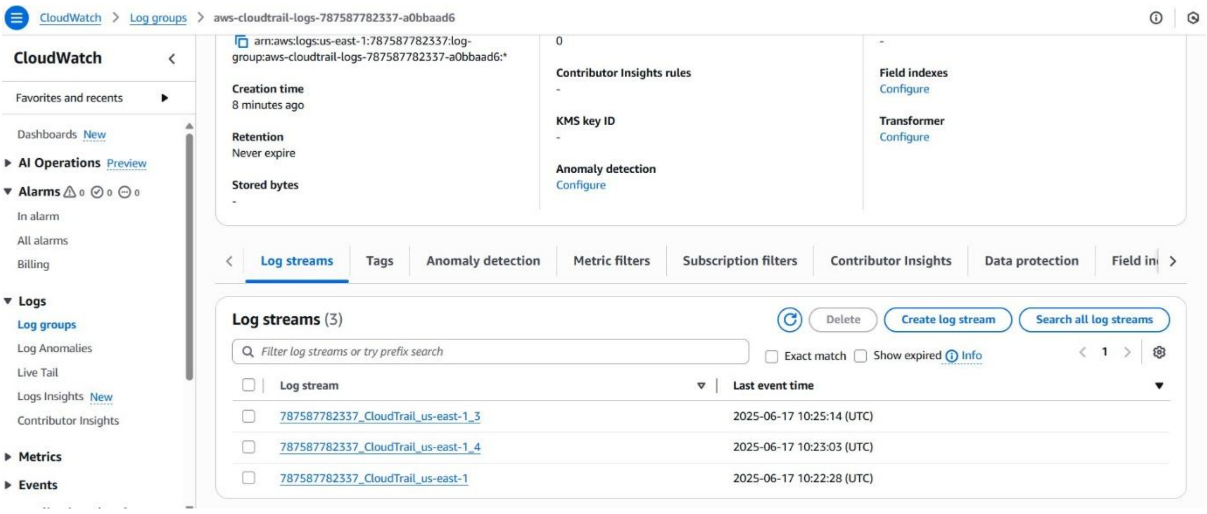
Log groups (2)

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

Filter log groups or try pattern search ☑ Exact match

□	Log group	Log class	Anomaly d...	Data pr...	Sensitiv...	Retention	Metric fi...
□	aws-cloudtrail-logs-787587782337-a0bbaad6	Standard	Configure	-	-	Never expire	-
□	vpc-flowlog-cloudwatch	Standard	Configure	-	-	Never expire	-

Logs in cloudwatch



arn:aws:logs:us-east-1:787587782337:log-group:aws-cloudtrail-logs-787587782337-a0bbaad6:*

Creation time
8 minutes ago

Retention
Never expire

Stored bytes
-

0

Contributor Insights rules
-

KMS key ID
-

Anomaly detection
Configure

-

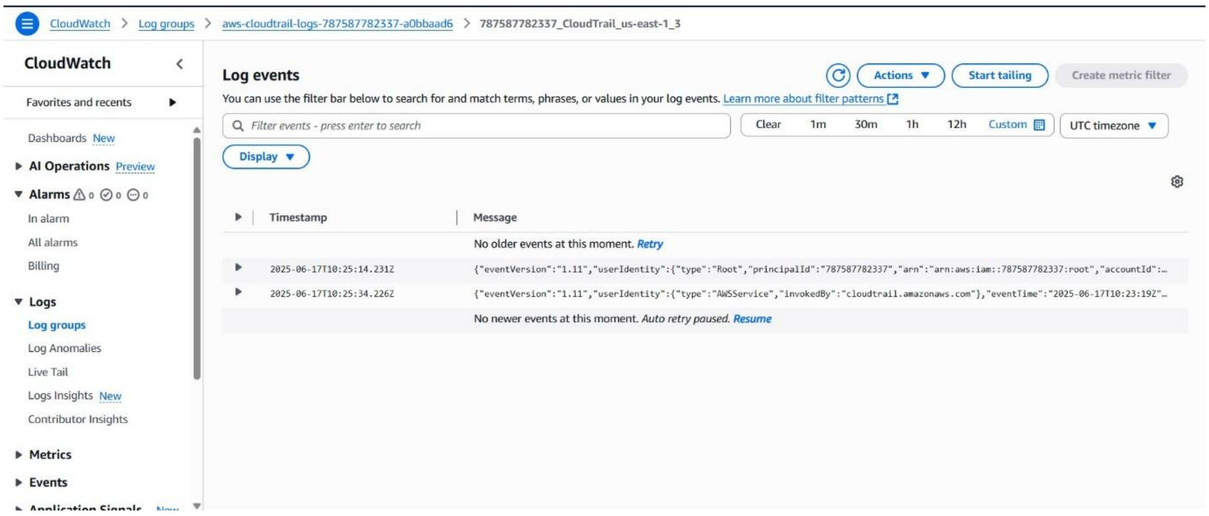
Field indexes
Configure

Transformer
Configure

Log streams (3)

Filter log streams or try prefix search □ Exact match □ Show expired Info

□	Log stream	Last event time
□	787587782337_CloudTrail_us-east-1_3	2025-06-17 10:25:14 (UTC)
□	787587782337_CloudTrail_us-east-1_4	2025-06-17 10:23:03 (UTC)
□	787587782337_CloudTrail_us-east-1	2025-06-17 10:22:28 (UTC)

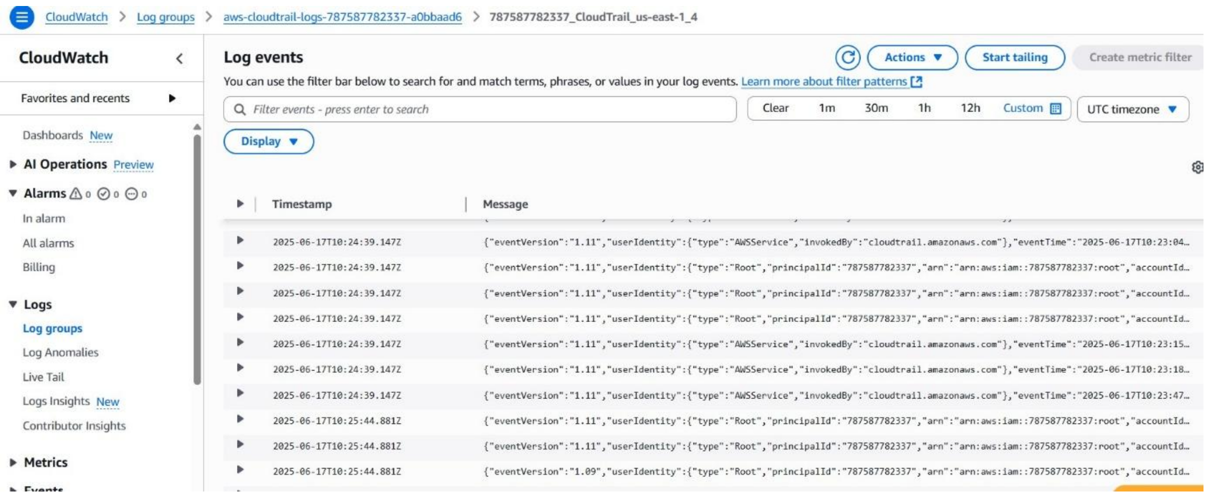


Log events

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

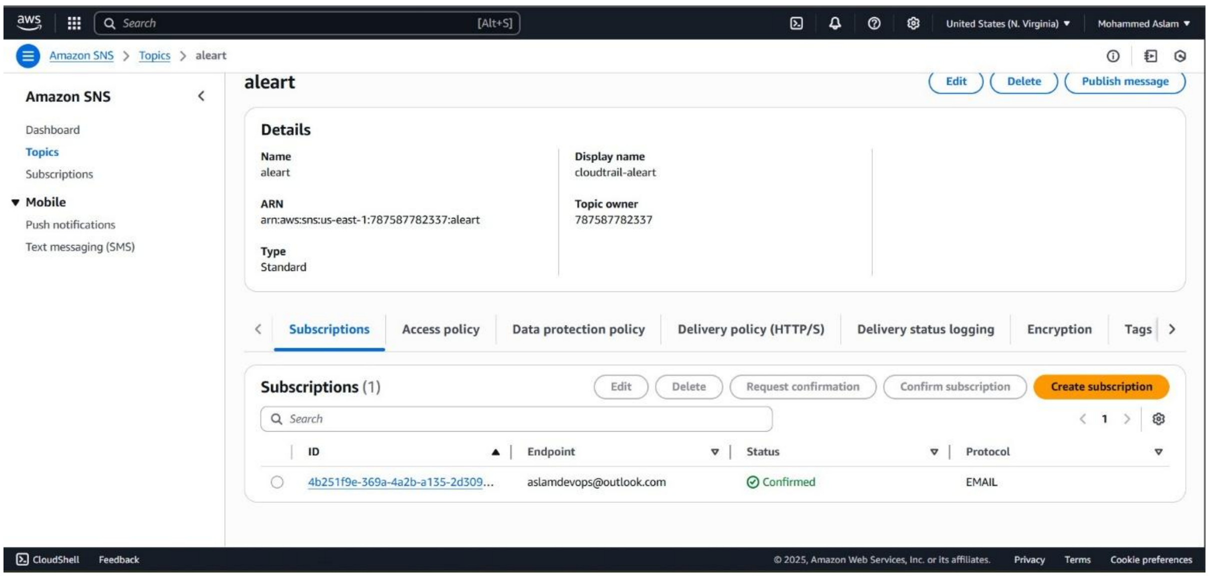
```
Timestamp                  Message
                           No older events at this moment. Retry
2025-06-17T10:25:14.231Z   {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId":…
2025-06-17T10:25:34.226Z   {"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-06-17T10:23:19Z"…
                           No newer events at this moment. Auto retry paused. Resume
```



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

```
Timestamp                 Message
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-06-17T10:23:04…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-06-17T10:23:15…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-06-17T10:23:18…
2025-06-17T10:24:39.147Z  {"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-06-17T10:23:47…
2025-06-17T10:25:44.881Z  {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
2025-06-17T10:25:44.881Z  {"eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
2025-06-17T10:25:44.881Z  {"eventVersion":"1.09","userIdentity":{"type":"Root","principalId":"787587782337","arn":"arn:aws:iam::787587782337:root","accountId…
```

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



aleart

Details

Name: aleart

Display name: cloudtrail-aleart

ARN: arn:aws:sns:us-east-1:787587782337:aleart

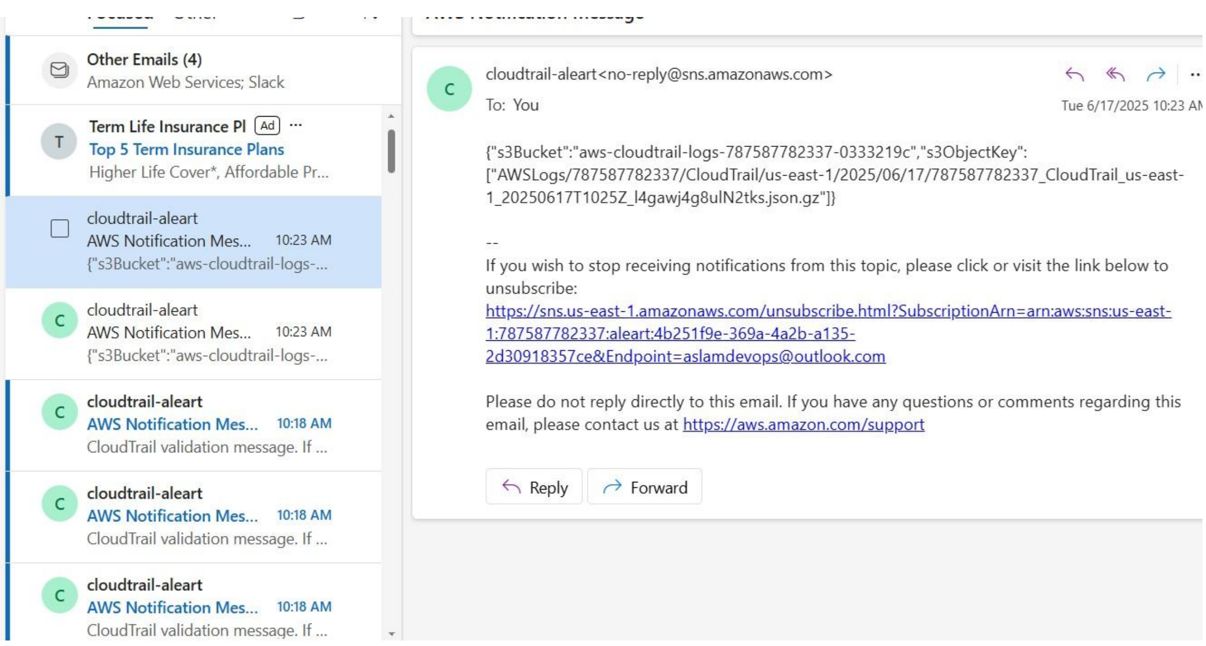
Topic owner: 787587782337

Type: Standard

Subscriptions (1)

ID	Endpoint	Status	Protocol
4b251f9e-369a-4a2b-a135-2d309…	aslamdevops@outlook.com	Confirmed	EMAIL

SNS notification are coming in emails.



Other Emails (4)
Amazon Web Services; Slack

Term Life Insurance Pl Ad
Top 5 Term Insurance Plans
Higher Life Cover*, Affordable Pr…

cloudtrail-aleart
AWS Notification Mes… 10:23 AM
{"s3Bucket":"aws-cloudtrail-logs-…

cloudtrail-aleart
AWS Notification Mes… 10:23 AM
{"s3Bucket":"aws-cloudtrail-logs-…

cloudtrail-aleart
AWS Notification Mes… 10:18 AM
CloudTrail validation message. If …

cloudtrail-aleart
AWS Notification Mes… 10:18 AM
CloudTrail validation message. If …

cloudtrail-aleart
AWS Notification Mes… 10:18 AM
CloudTrail validation message. If …

cloudtrail-aleart<no-reply@sns.amazonaws.com>
To: You
Tue 6/17/2025 10:23 AM

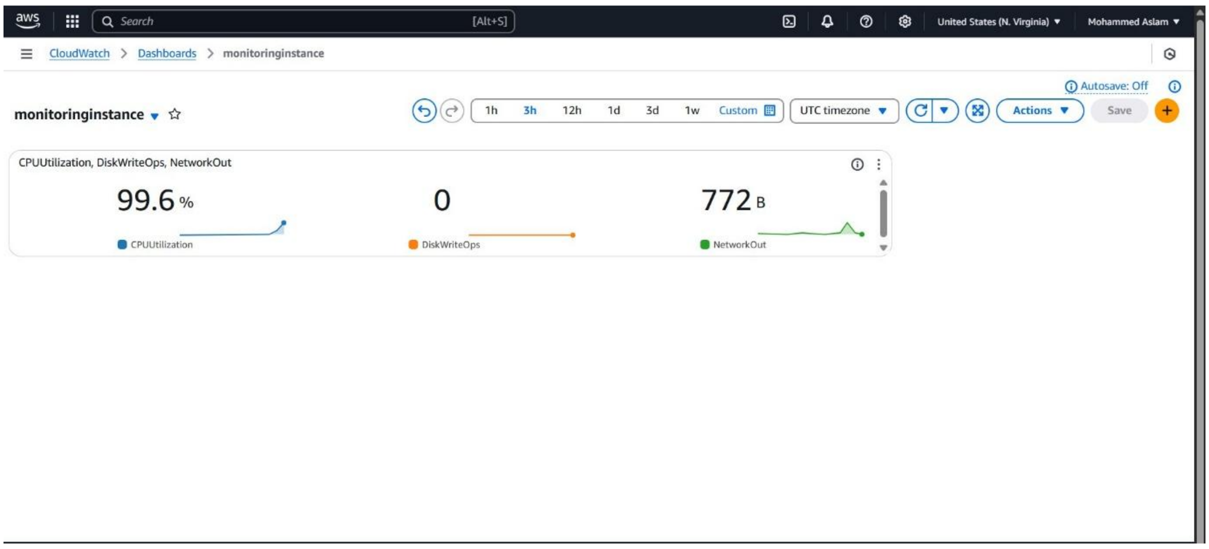
{"s3Bucket":"aws-cloudtrail-logs-787587782337-0333219c","s3ObjectKey":["AWSLogs/787587782337/CloudTrail/us-east-1/2025/06/17/787587782337_CloudTrail_us-east-1_20250617T1025Z_l4gawj4g8ulN2tks.json.gz"]}

--

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-1:787587782337:aleart:4b251f9e-369a-4a2b-a135-2d30918357ce&Endpoint=aslamdevops@outlook.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

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

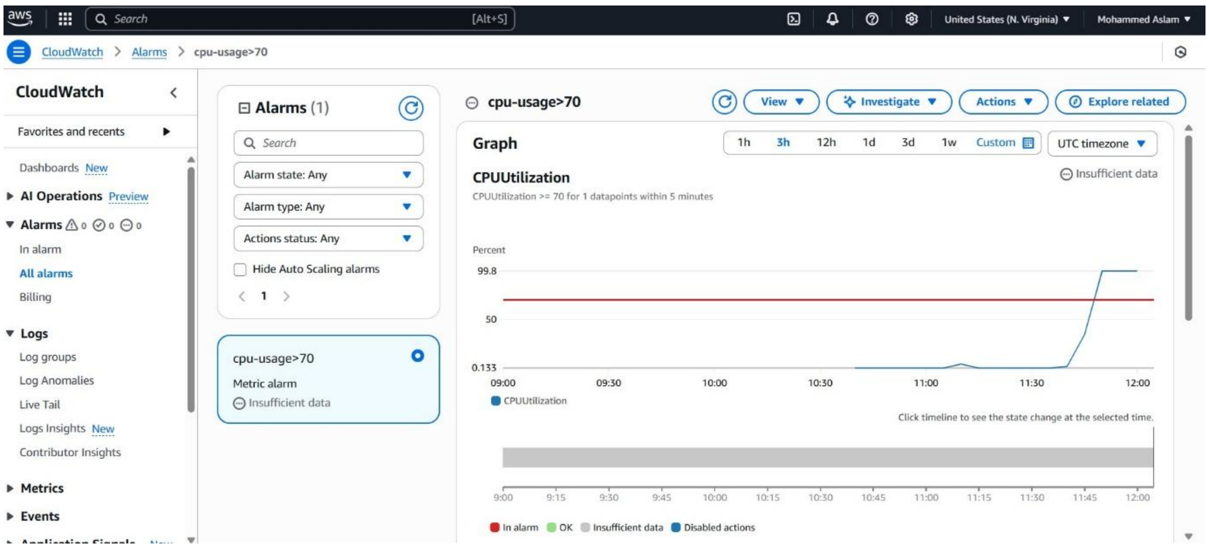

aws
Search
[Alt+S]
United States (N. Virginia)
Mohammed Aslam
CloudWatch > Dashboards > monitoringinstance
Autosave: Off
monitoringinstance
1h 3h 12h 1d 3d 1w Custom
UTC timezone
Actions
Save

CPUUtilization, DiskWriteOps, NetworkOut

CPUUtilization	DiskWriteOps	NetworkOut
99.6 %	0	772 B

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

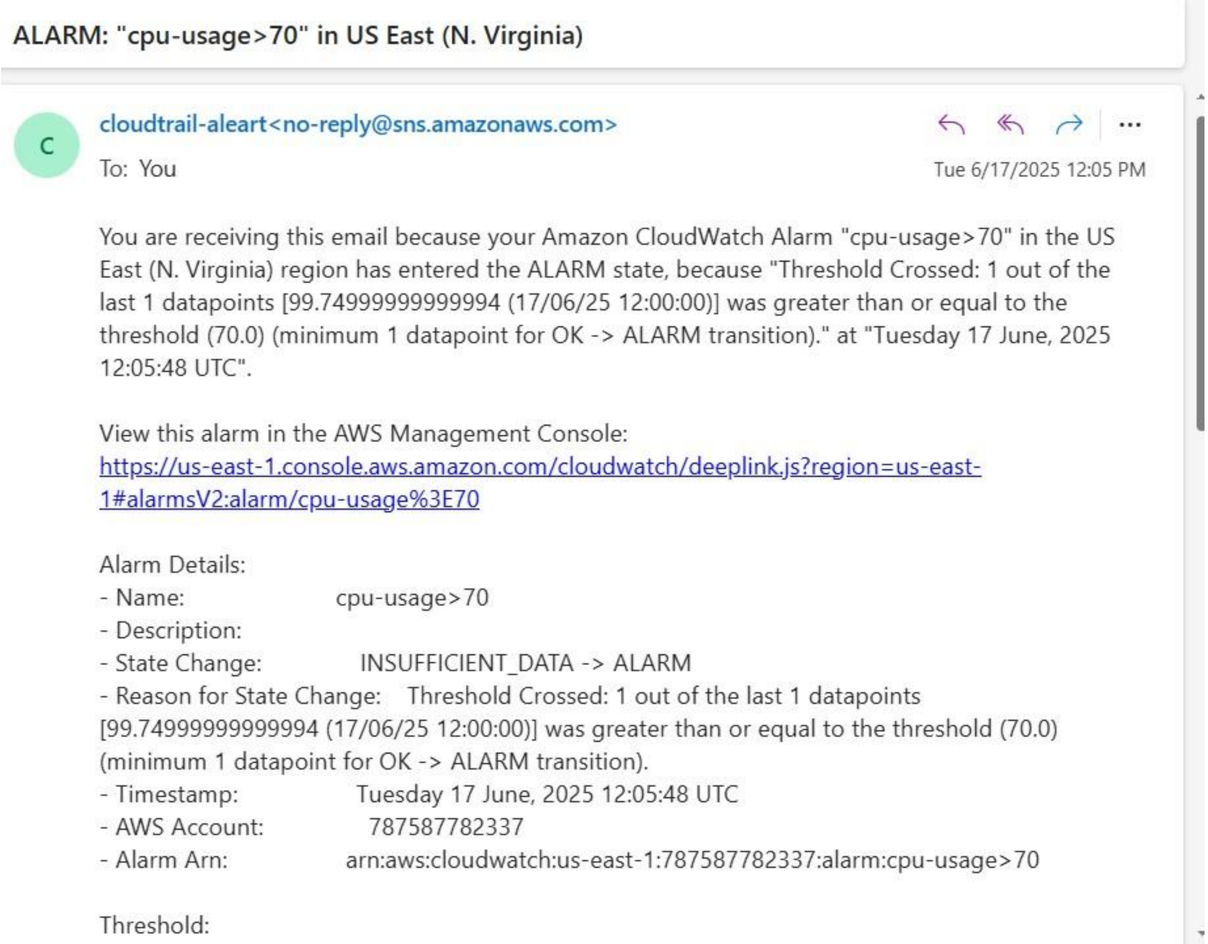
Created an alarm for cpu usage



cpu-usage>70
Metric alarm
Insufficient data

CPUUtilization
CPUUtilization >= 70 for 1 datapoints within 5 minutes
Insufficient data

Email received



ALARM: "cpu-usage>70" in US East (N. Virginia)

cloudtrail-aleart<no-reply@sns.amazonaws.com>

To: You

Tue 6/17/2025 12:05 PM

You are receiving this email because your Amazon CloudWatch Alarm "cpu-usage>70" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [99.74999999999994 (17/06/25 12:00:00)] was greater than or equal to the threshold (70.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 17 June, 2025 12:05:48 UTC".

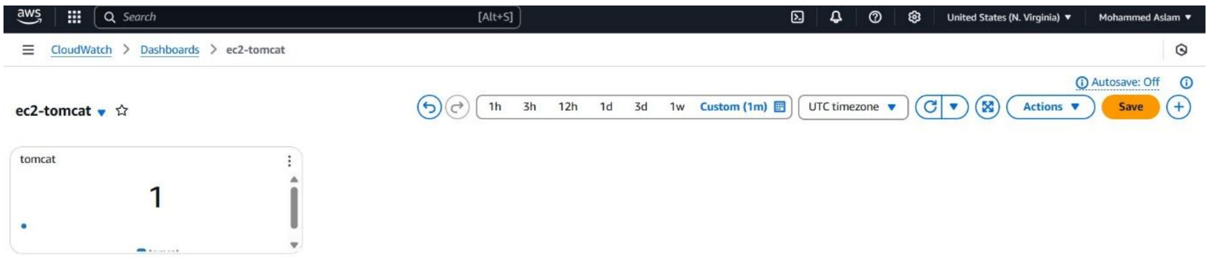
View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/cpu-usage%3E70

Alarm Details:
- Name: cpu-usage>70
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [99.74999999999994 (17/06/25 12:00:00)] was greater than or equal to the threshold (70.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 17 June, 2025 12:05:48 UTC
- AWS Account: 787587782337
- Alarm Arn: arn:aws:cloudwatch:us-east-1:787587782337:alarm:cpu-usage>70

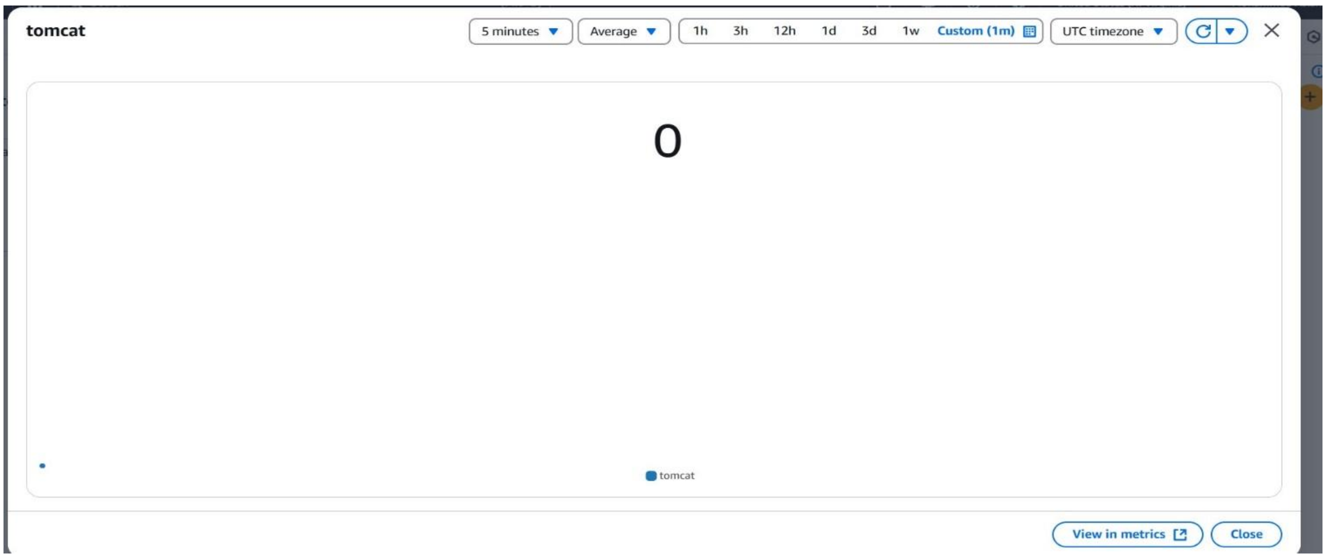
Threshold:

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

output of graph when tomcat is running

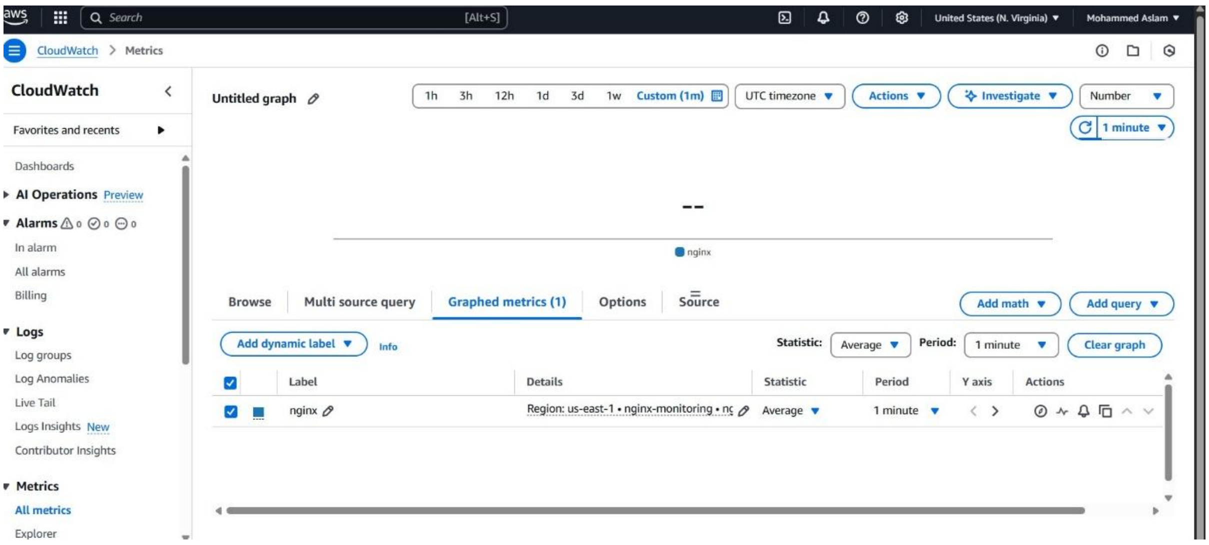


Output of graph when tomcat is stopped



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

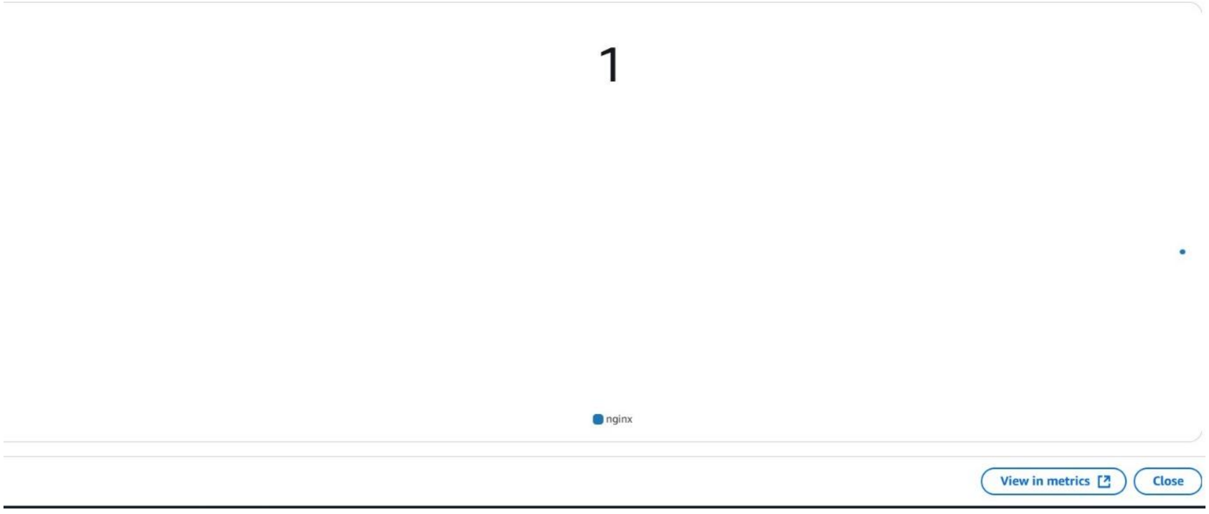
When nginx is not Working no update



Statistic: Average Period: 1 minute

☑	Label	Details	Statistic	Period	Y axis	Actions
☑	nginx	Region: us-east-1 • nginx-monitoring • nç	Average	1 minute	< >	

Nginx is working


1
nginx
View in metrics
Close