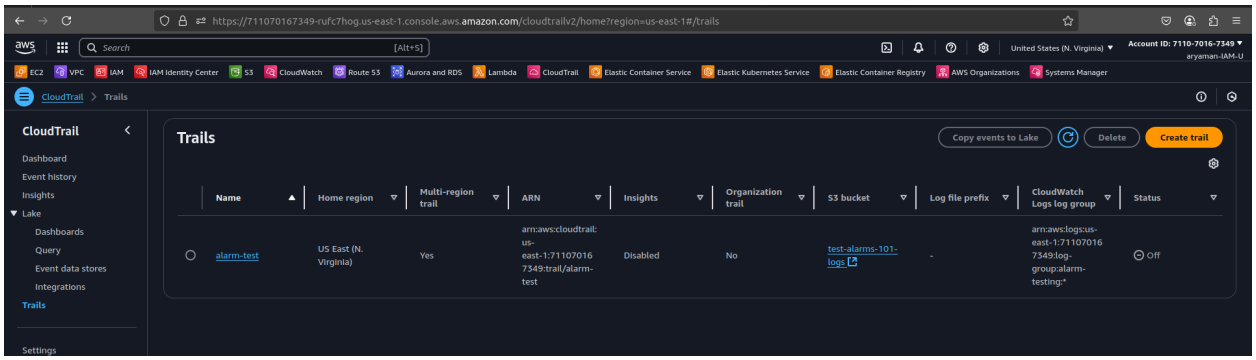
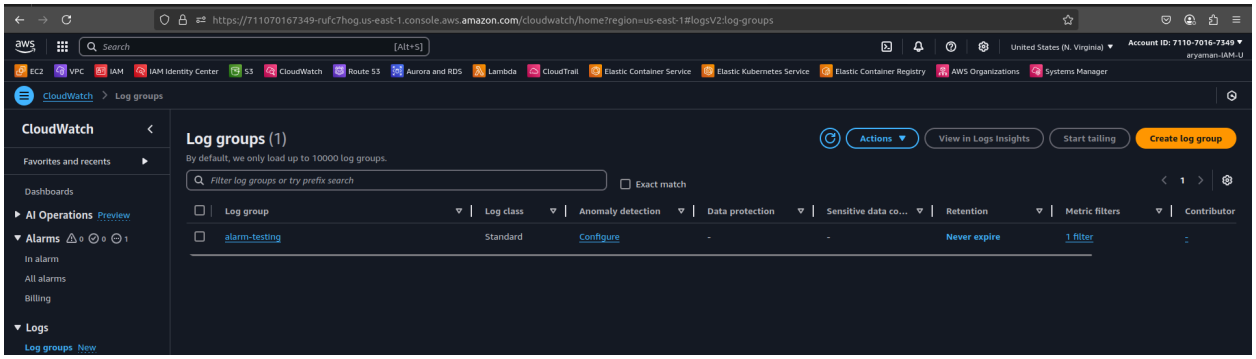
1. SG config change. **Done**
2. AWS console login failure multiple times. **Done**
3. Root account login. **Done**
4. Change in any resource policy.
5. Source IP is outside India or US **For this i have to use AWS WAF or cloudfront because by default cloudwatch does not support geographical origin of a request**
6. Deletion of any PEM key from EC2 console. **Done**
7. Any account is given an admin access policy.
8. Notify when a new IAM user is made from any other account instead of root account.
9. Any new route is created in a VPC.
10. If someone creates a custom policy.
11. Someone tried to SSH into an EC2 but his IP was not allowed. **Done**
12. No MFA console login. **Done**
13. Cloudtrail config changes.
14. Unothorised API calls.
15. Changes in KMS keys. **Done**
16. Applying any role to any service.

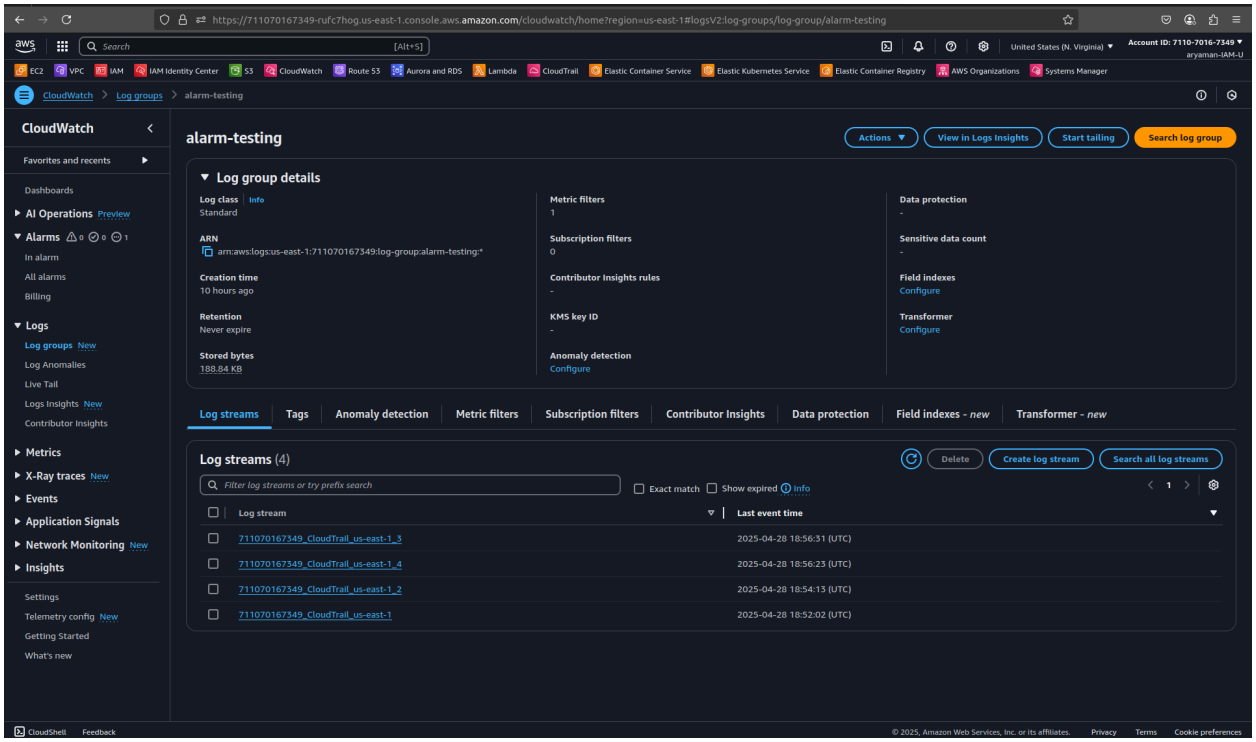
17. Unused resources.

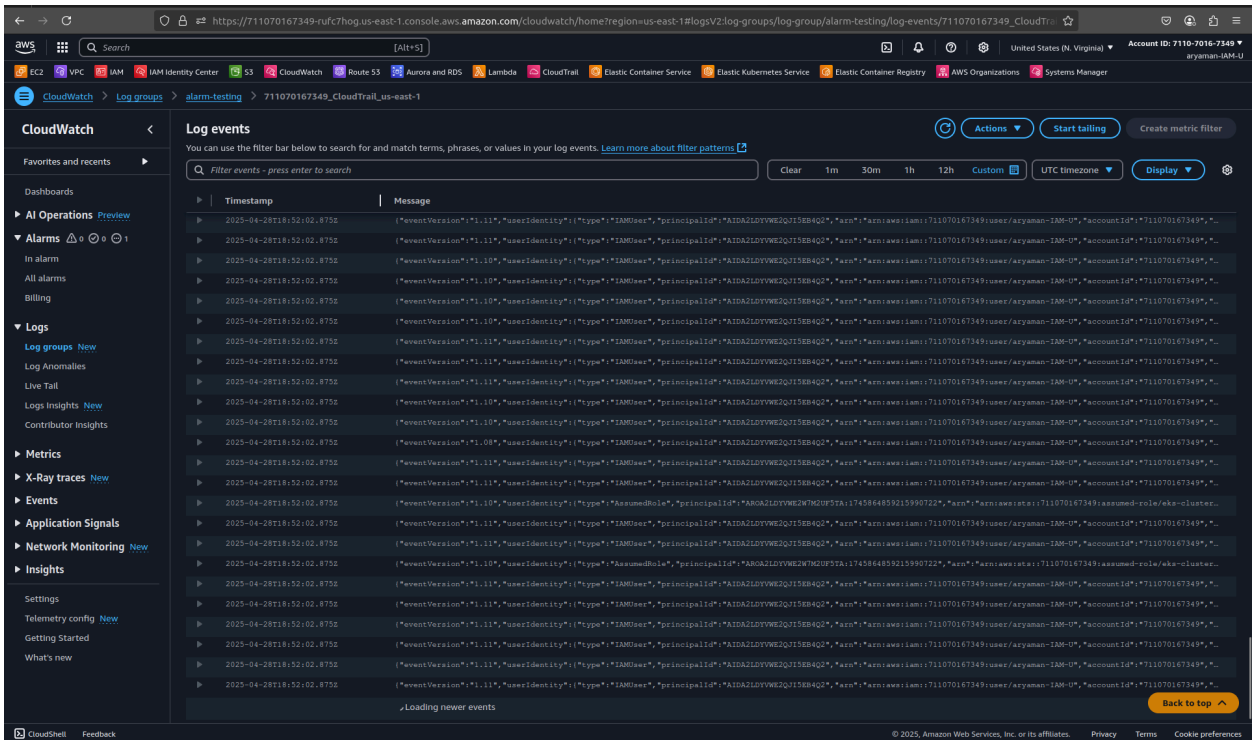
Steps to set up an alarm:

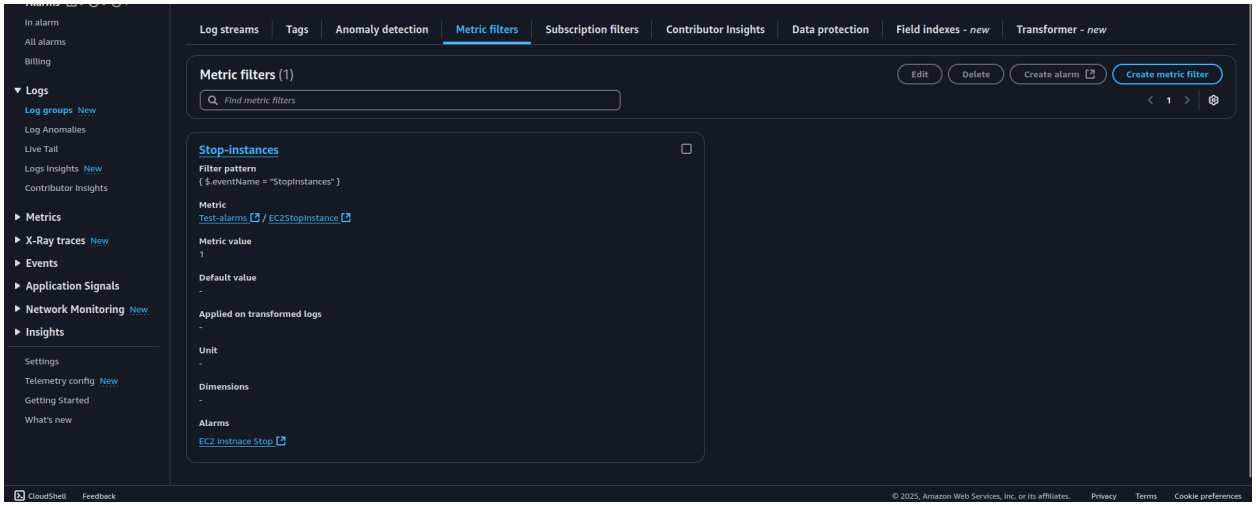
1. Go to cloudtrail make a trail choose an option to send trail logs to cloudwatch to create a log group.
2. Then go to cloudwatch and then select the log group that you want to set up an alarm for.
3. There would be multiple data streams that select your desired data stream.
4. And then click on to create a metric filter.
5. After creating the alarm test the pattern from the sample data.
6. And then connect that metric filter to an alarm.

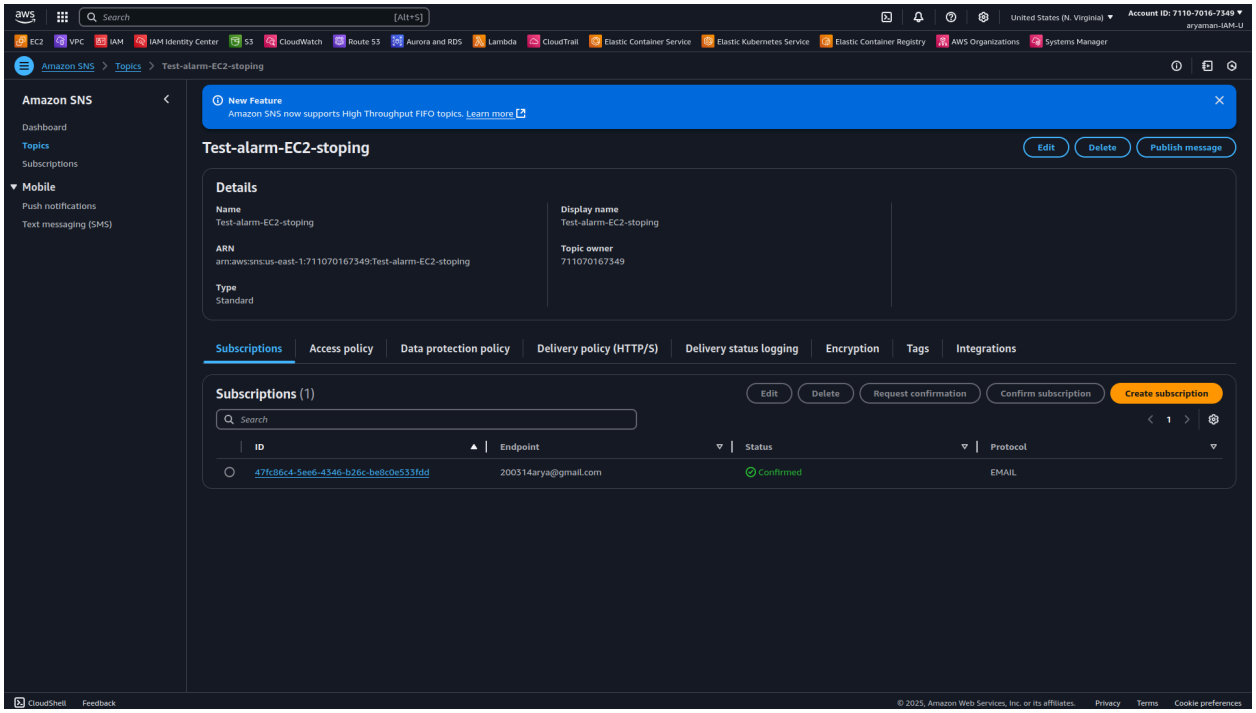




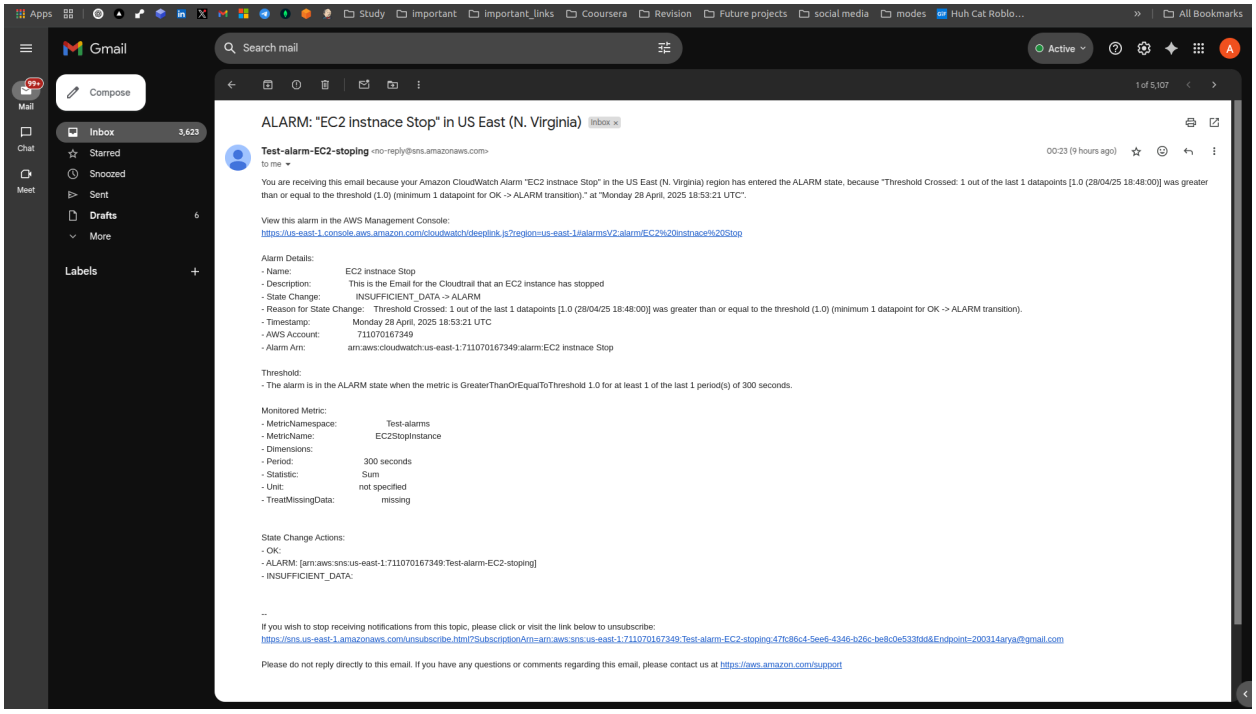

https://711070167349-rufc7hog.us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/alarm-testing
CloudWatch > Log groups > alarm-testing
alarm-testing
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
Log class Info
Standard
ARN
arn:aws:logs:us-east-1:711070167349:log-group:alarm-testing:*
Creation time
10 hours ago
Retention
Never expire
Stored bytes
188.84 KB
Metric filters
1
Subscription filters
0
Contributor Insights rules
-
KMS key ID
-
Anomaly detection
Configure
Data protection
-
Sensitive data count
-
Field indexes
Configure
Transformer
Configure
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data protection
Field indexes - new
Transformer - new
Log streams (4)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired Info
Log stream
Last event time
711070167349_CloudTrail_us-east-1_3
2025-04-28 18:56:31 (UTC)
711070167349_CloudTrail_us-east-1_4
2025-04-28 18:56:23 (UTC)
711070167349_CloudTrail_us-east-1_2
2025-04-28 18:54:13 (UTC)
711070167349_CloudTrail_us-east-1
2025-04-28 18:52:02 (UTC)


https://711070167349-rufc7hog.us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/alarm-testing/log-events/711070167349_CloudTrail_us-east-1
CloudWatch > Log groups > alarm-testing > 711070167349_CloudTrail_us-east-1
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
Actions
Start tailing
Create metric filter
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display
Timestamp
Message
Loading newer events
Back to top

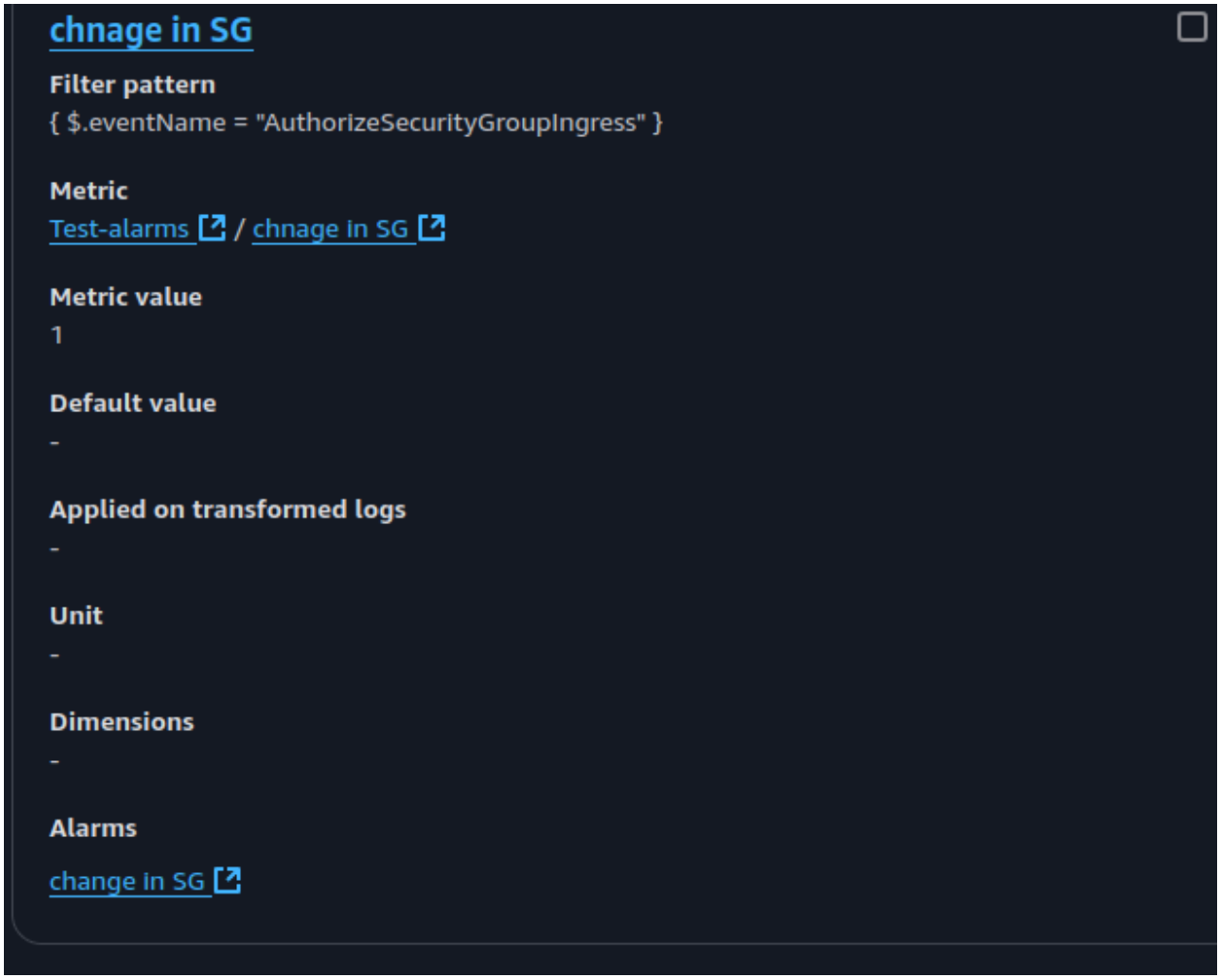

In alarm
All alarms
Billing
Logs
Log groups New
Log Anomalies
Live Tail
Logs Insights New
Contributor Insights
Metrics
X-Ray traces New
Events
Application Signals
Network Monitoring New
Insights
Settings
Telemetry config New
Getting Started
What's new
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data protection
Field indexes - new
Transformer - new
Metric filters (1)
Find metric filters
Edit
Delete
Create alarm
Create metric filter
Stop-instances
Filter pattern
{ $.eventName = "StopInstances" }
Metric
Test-alarms / EC2StopInstance
Metric value
1
Default value
-
Applied on transformed logs
-
Unit
-
Dimensions
-
Alarms
EC2 instnace Stop
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

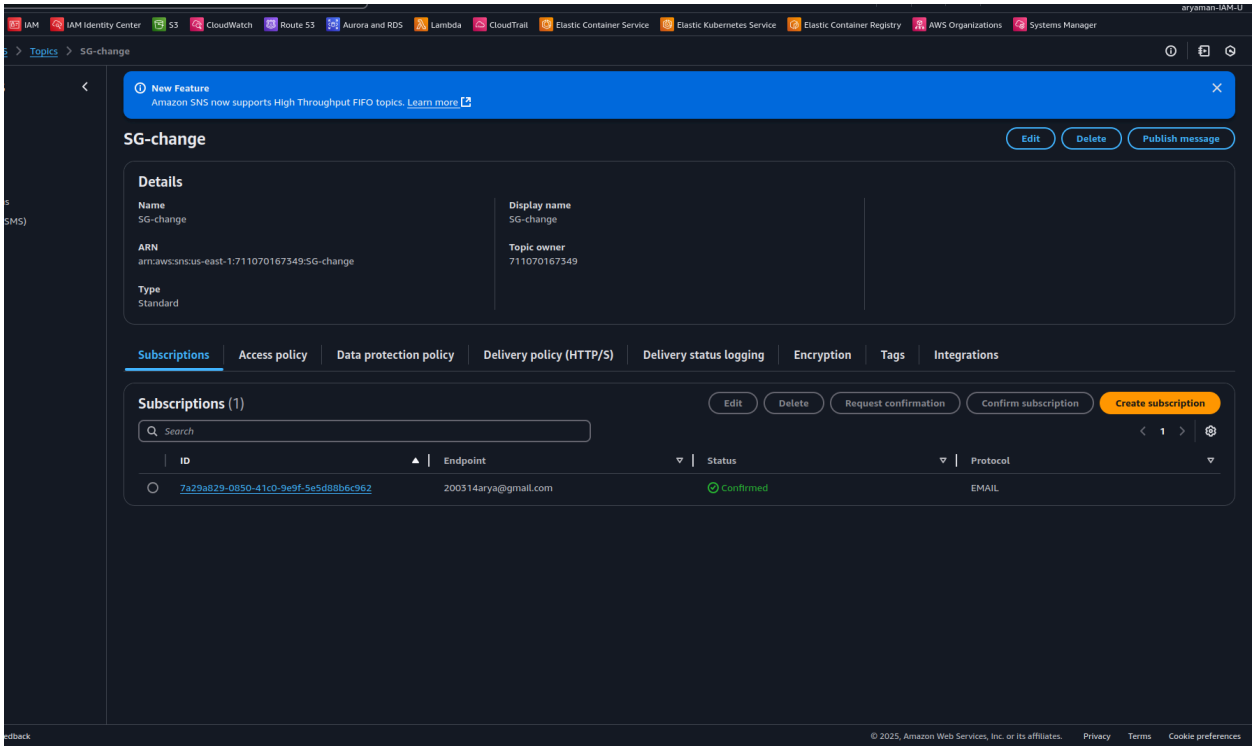

Search
[Alt+S]
United States (N. Virginia)
Account ID: 7110-7016-7349
aryaman-IAM-U
EC2
VPC
IAM
IAM Identity Center
S3
CloudWatch
Route 53
Aurora and RDS
Lambda
CloudTrail
Elastic Container Service
Elastic Kubernetes Service
Elastic Container Registry
AWS Organizations
Systems Manager
Amazon SNS
Topics
Test-alarm-EC2-stoping
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Test-alarm-EC2-stoping
Edit
Delete
Publish message
Details
Name
Test-alarm-EC2-stoping
ARN
arn:aws:sns:us-east-1:711070167349:Test-alarm-EC2-stoping
Type
Standard
Display name
Test-alarm-EC2-stoping
Topic owner
711070167349
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Integrations
Subscriptions (1)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
47fc86c4-5ee6-4346-b26c-be8c0e533fdd
200314arya@gmail.com
Confirmed
EMAIL
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Test Email:

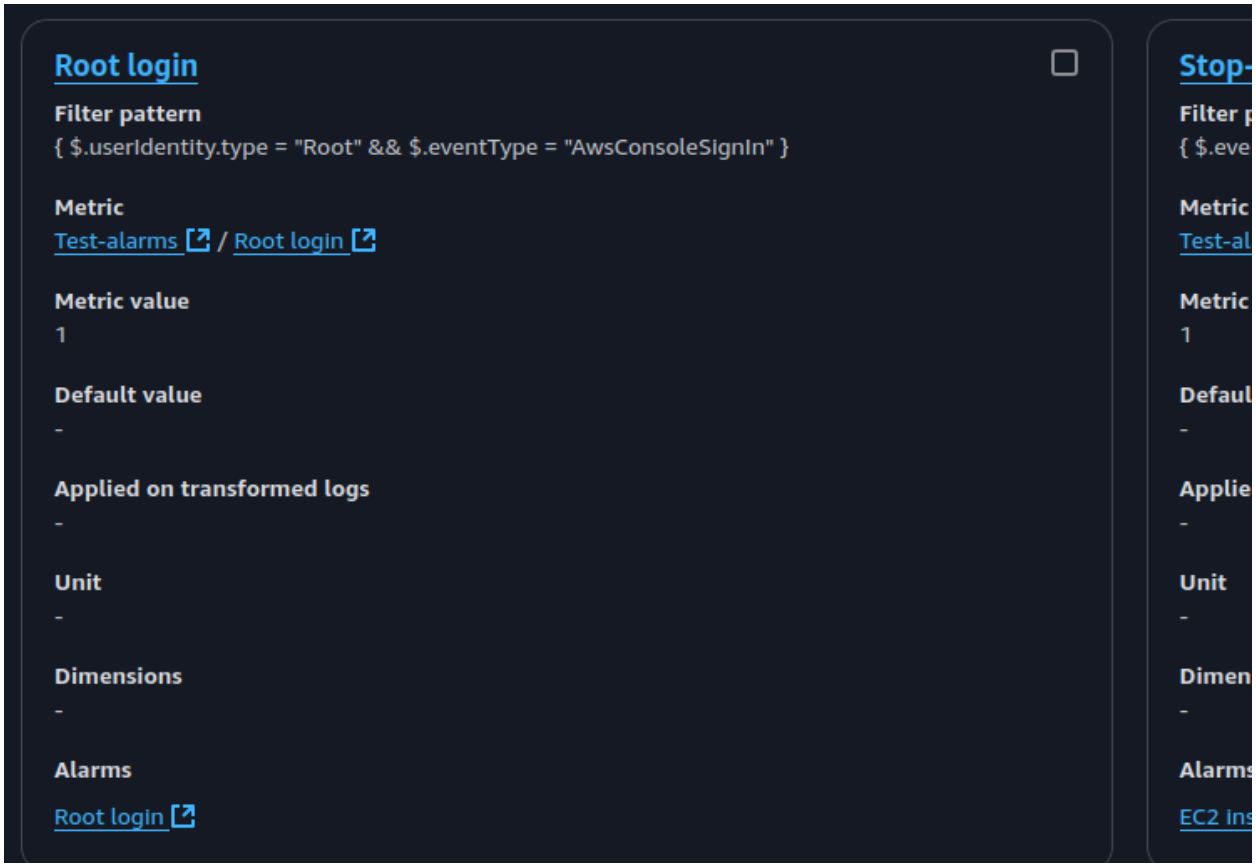

Gmail
Search mail
Compose
Inbox 3,623
Starred
Snoozed
Sent
Drafts 6
More
Labels
ALARM: "EC2 instnace Stop" in US East (N. Virginia)
Test-alarm-EC2-stoping <no-reply@sns.amazonaws.com>
to me
You are receiving this email because your Amazon CloudWatch Alarm "EC2 instnace Stop" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (28/04/25 18:48:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Monday 28 April, 2025 18:53:21 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/EC2%20instnace%20Stop
Alarm Details:
- Name: EC2 instnace Stop
- Description: This is the Email for the Cloudtrail that an EC2 instance has stopped
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (28/04/25 18:48:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Monday 28 April, 2025 18:53:21 UTC
- AWS Account: 711070167349
- Alarm Arn: arn:aws:cloudwatch:us-east-1:711070167349:alarm:EC2 instnace Stop
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 300 seconds.
Monitored Metric:
- MetricNamespace: Test-alarms
- MetricName: EC2StopInstance
- Dimensions:
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing
State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:711070167349:Test-alarm-EC2-stoping]
- 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-1:711070167349:Test-alarm-EC2-stoping:47fc86c4-5ee6-4346-b26c-be8c0e533fdd&Endpoint=200314arya@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

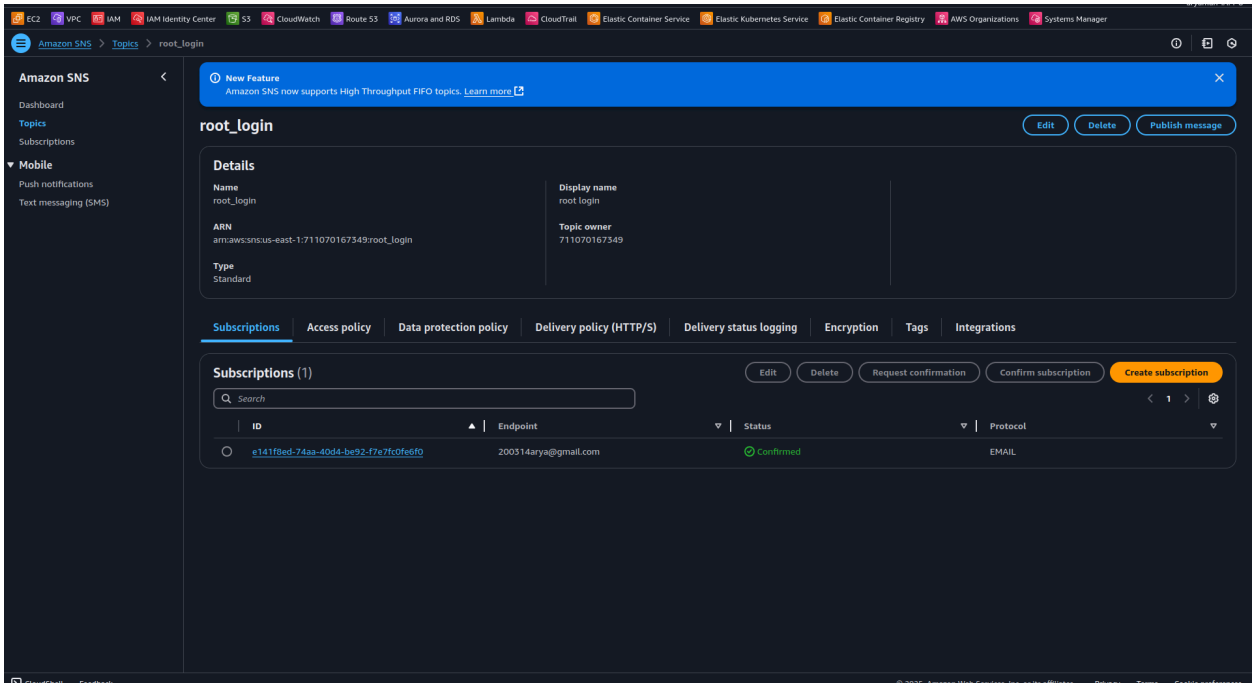
Setting up alarms:



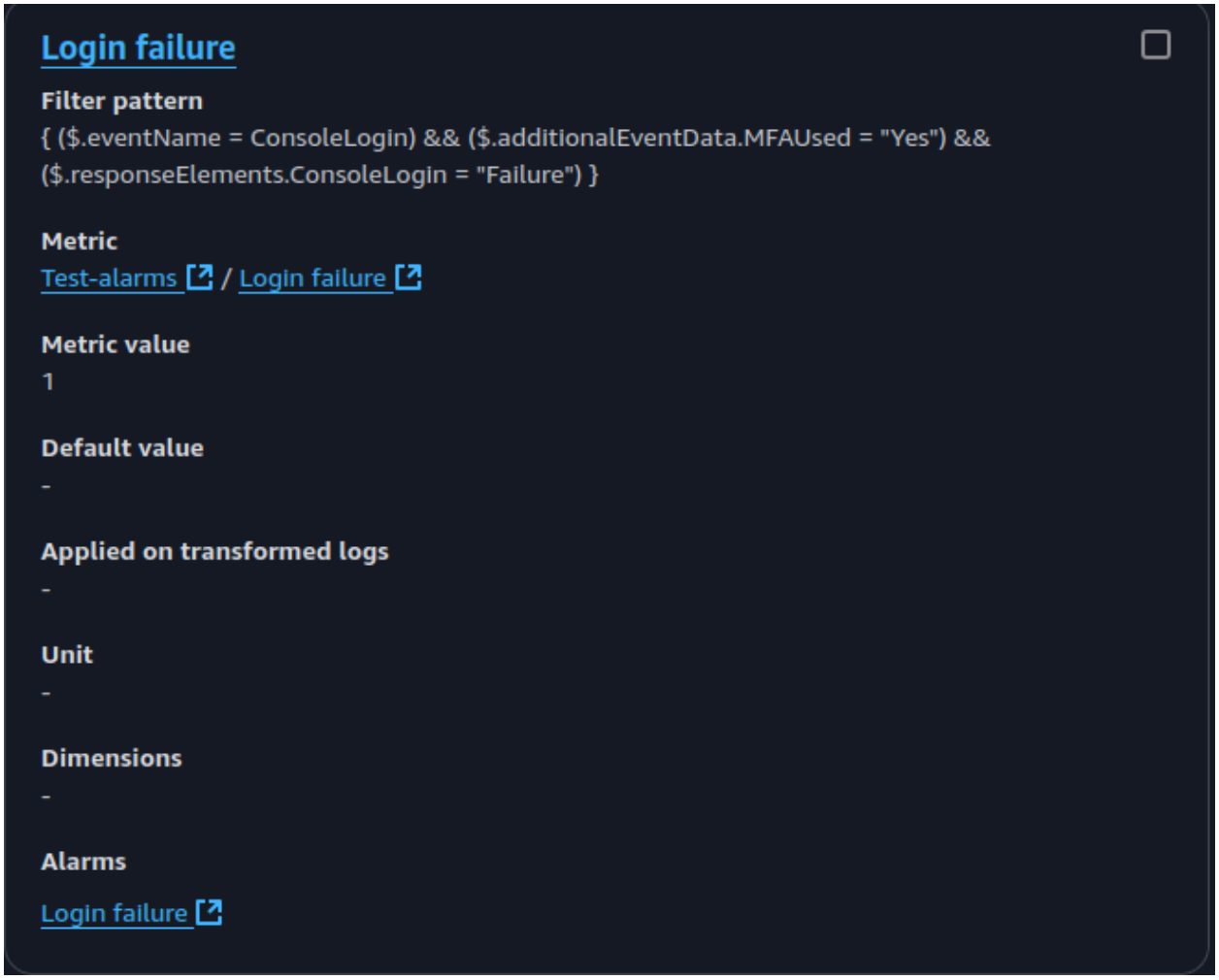

aryaman-IAM-U
IAM
IAM Identity Center
S3
CloudWatch
Route 53
Aurora and RDS
Lambda
CloudTrail
Elastic Container Service
Elastic Kubernetes Service
Elastic Container Registry
AWS Organizations
Systems Manager
Topics
SG-change
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
SG-change
Edit
Delete
Publish message
Details
Name
SG-change
Display name
SG-change
ARN
arn:aws:sns:us-east-1:711070167349:SG-change
Topic owner
711070167349
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Integrations
Subscriptions (1)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
7a29a829-0850-41c0-9e9f-5e5d88b6c962
200314arya@gmail.com
Confirmed
EMAIL
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

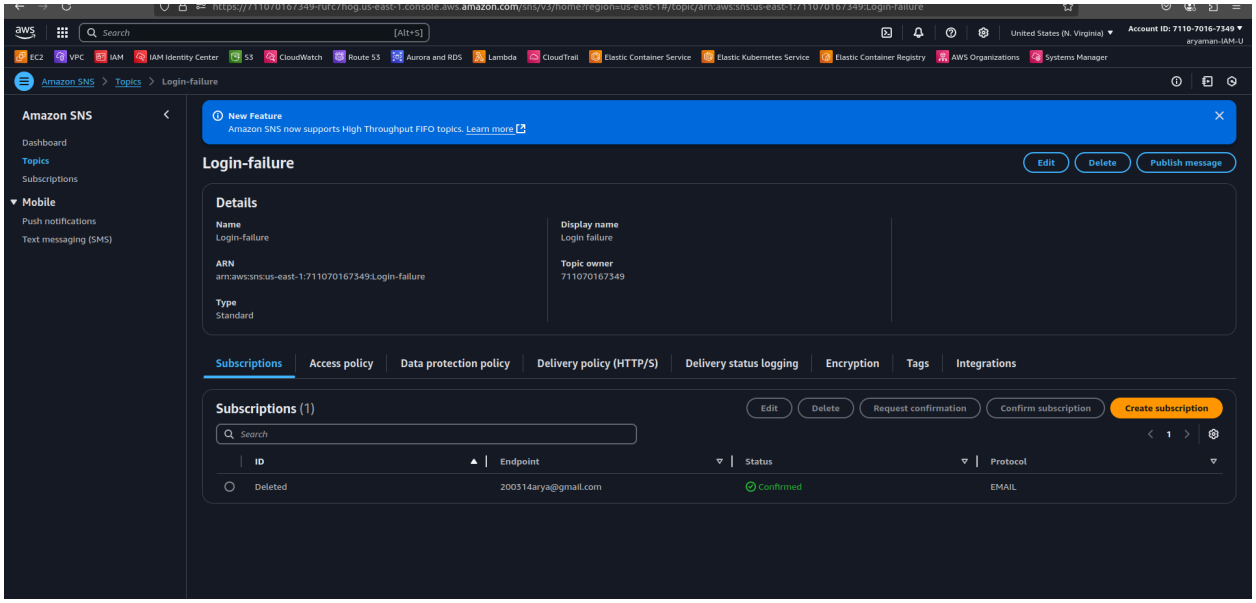
2:


Root login
Filter pattern
{ $.userIdentity.type = "Root" && $.eventType = "AwsConsoleSignIn" }
Metric
Test-alarms / Root login
Metric value
1
Default value
-
Applied on transformed logs
-
Unit
-
Dimensions
-
Alarms
Root login

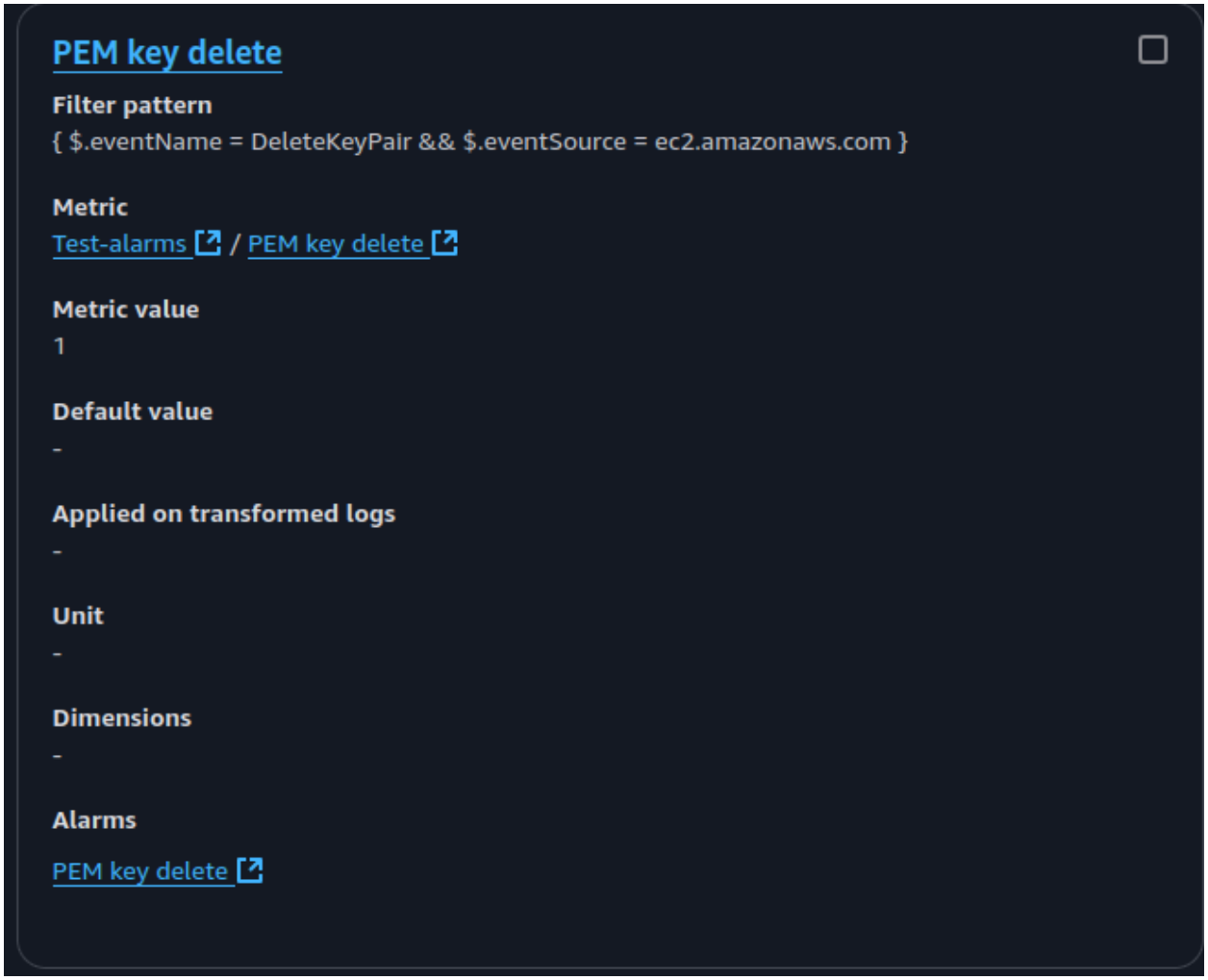

Amazon SNS
Topics
root_login
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
root_login
Edit
Delete
Publish message
Details
Name
root_login
Display name
root login
ARN
arn:aws:sns:us-east-1:711070167349:root_login
Topic owner
711070167349
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Integrations
Subscriptions (1)
Request confirmation
Confirm subscription
Create subscription
ID
Endpoint
Status
Protocol
e141f8ed-74aa-40d4-be92-f7e7fc0fe6f0
200314arya@gmail.com
Confirmed
EMAIL

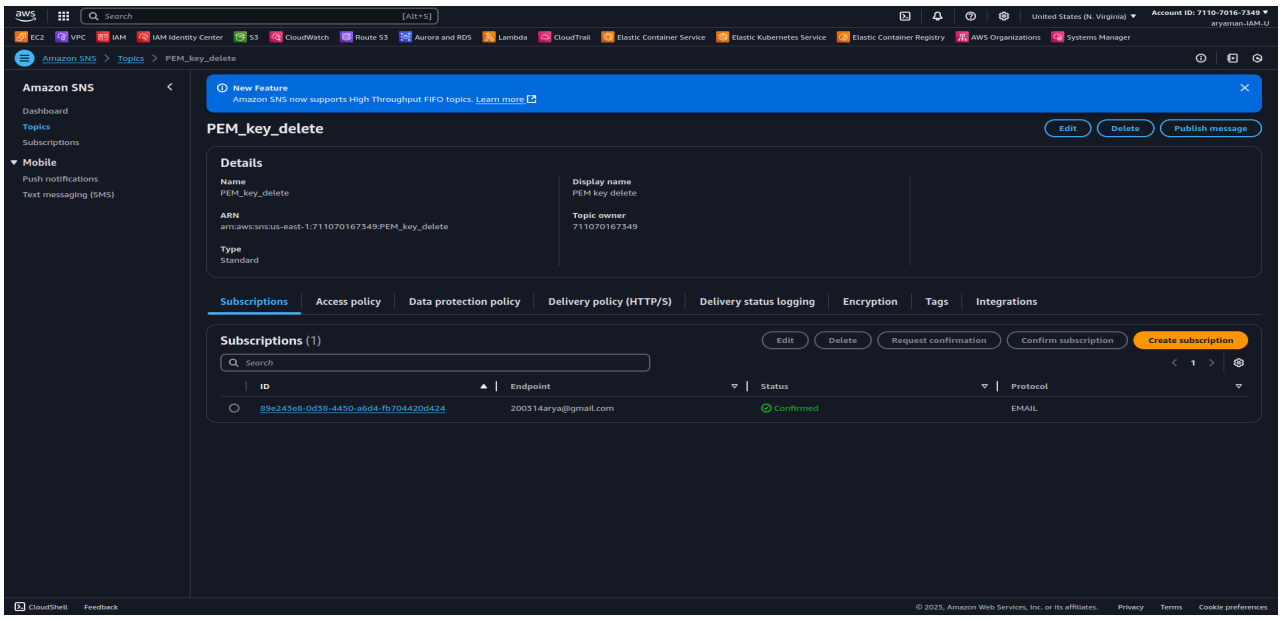
3:


Login failure
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.additionalEventData.MFAUsed = "Yes") &&
($.responseElements.ConsoleLogin = "Failure") }
Metric
Test-alarms / Login failure
Metric value
1
Default value
-
Applied on transformed logs
-
Unit
-
Dimensions
-
Alarms
Login failure


Amazon SNS
Topics
Login-failure
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Login-failure
Edit
Delete
Publish message
Details
Name
Login-failure
Display name
Login failure
ARN
arn:aws:sns:us-east-1:711070167349:Login-failure
Topic owner
711070167349
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Integrations
Subscriptions (1)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
Deleted
200314arya@gmail.com
Confirmed
EMAIL

4:


PEM key delete
Filter pattern
{ $.eventName = DeleteKeyPair && $.eventSource = ec2.amazonaws.com }
Metric
Test-alarms / PEM key delete
Metric value
1
Default value
-
Applied on transformed logs
-
Unit
-
Dimensions
-
Alarms
PEM key delete


Amazon SNS
Topics
PEM_key_delete
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
PEM_key_delete
Edit
Delete
Publish message
Details
Name
PEM_key_delete
Display name
PEM key delete
ARN
arn:aws:sns:us-east-1:711070167349:PEM_key_delete
Topic owner
711070167349
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Integrations
Subscriptions (1)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
ID
Endpoint
Status
Protocol
89e243e8-0d58-4450-a6d4-fb704420d424
200314arya@gmail.com
Confirmed
EMAIL