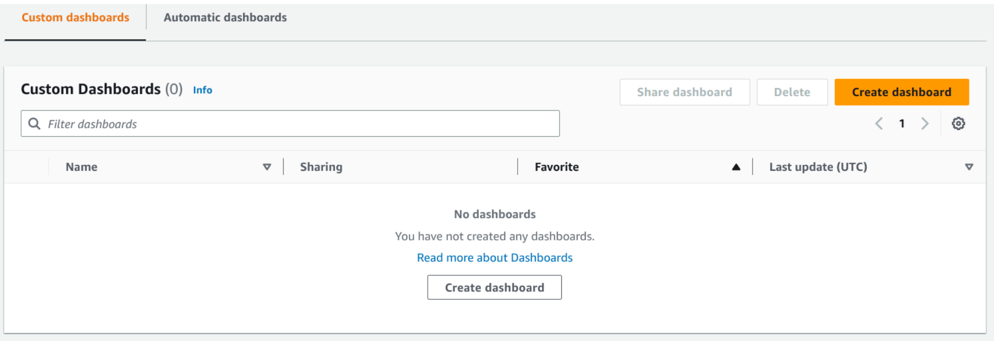
AWS Monitoring

Day 2 - Assignment — 26th July 2023

Assignment 1 - Creating custom CloudWatch dashboard.

Step 1 - Navigate to the CloudWatch console.



Custom Dashboards (0) Info

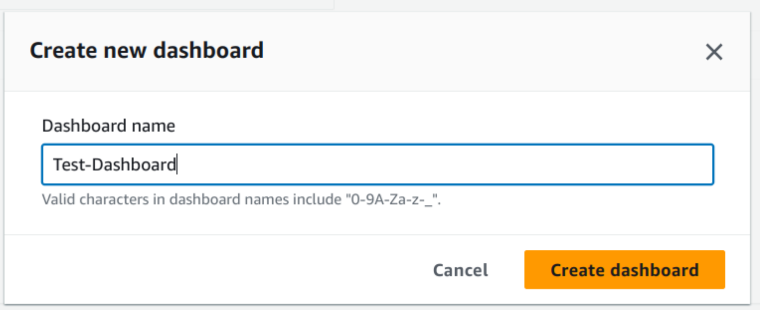
Name	Sharing	Favorite	Last update (UTC)

No dashboards

You have not created any dashboards.

Read more about Dashboards

Step 2 - Click on the “Create dashboard” button and give a name to the custom dashboard.

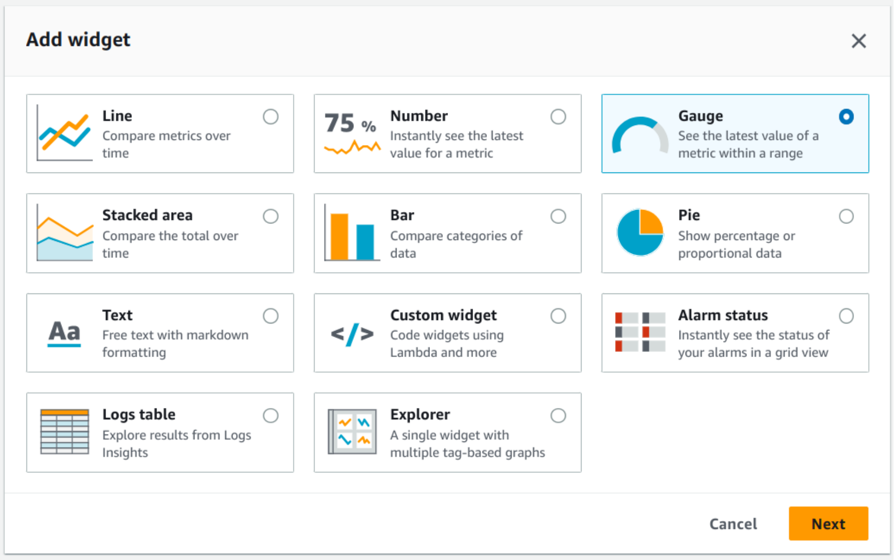


Create new dashboard

Dashboard name: Test-Dashboard

Valid characters in dashboard names include "0-9A-Za-z-_".

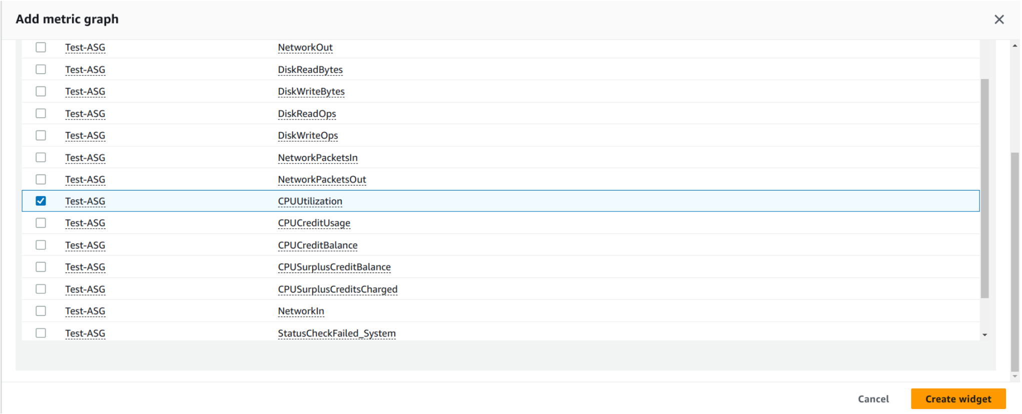
Step 3 - Select a widget for the dashboard.



Add widget

- ○ Line — Compare metrics over time
- ○ Number — Instantly see the latest value for a metric
- ● Gauge — See the latest value of a metric within a range
- ○ Stacked area — Compare the total over time
- ○ Bar — Compare categories of data
- ○ Pie — Show percentage or proportional data
- ○ Text — Free text with markdown formatting
- ○ Custom widget — Code widgets using Lambda and more
- ○ Alarm status — Instantly see the status of your alarms in a grid view
- ○ Logs table — Explore results from Logs Insights
- ○ Explorer — A single widget with multiple tag-based graphs

Step 4 - Select a metric for the widget. Here we select “CPU utilization” of the Auto scaling group.

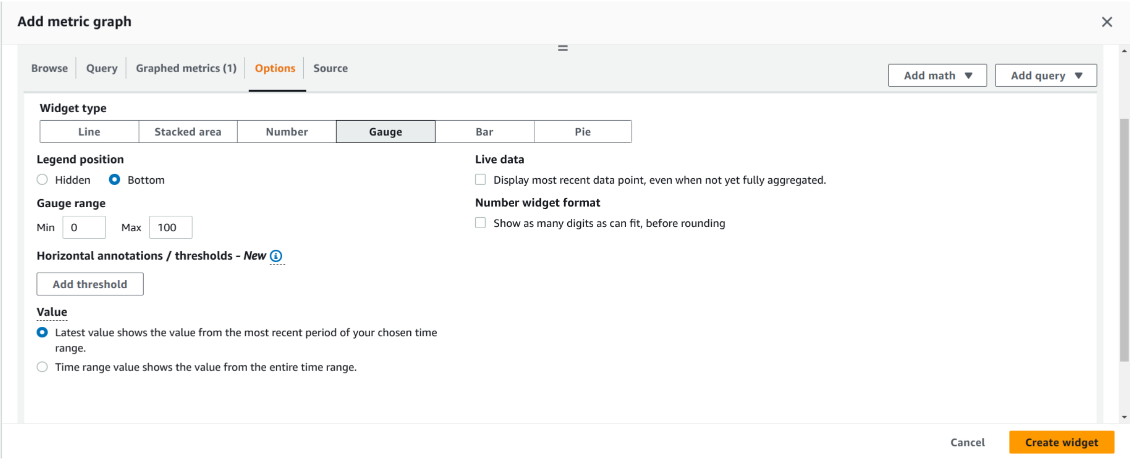


Add metric graph ✕

□	Test-ASG	NetworkOut
□	Test-ASG	DiskReadBytes
□	Test-ASG	DiskWriteBytes
□	Test-ASG	DiskReadOps
□	Test-ASG	DiskWriteOps
□	Test-ASG	NetworkPacketsIn
□	Test-ASG	NetworkPacketsOut
☑	Test-ASG	CPUUtilization
□	Test-ASG	CPUCreditUsage
□	Test-ASG	CPUCreditBalance
□	Test-ASG	CPUSurplusCreditBalance
□	Test-ASG	CPUSurplusCreditsCharged
□	Test-ASG	NetworkIn
□	Test-ASG	StatusCheckFailed_System

Cancel | Create widget

Step 5 - Set the minimum and maximum range for the “gauge” widget.



Add metric graph ✕

Browse | Query | Graphed metrics (1) | Options | Source | Add math ▼ | Add query ▼

Widget type

Line | Stacked area | Number | Gauge | Bar | Pie

Legend position

○ Hidden ● Bottom

Live data

□ Display most recent data point, even when not yet fully aggregated.

Gauge range

Min 0 Max 100

Number widget format

□ Show as many digits as can fit, before rounding

Horizontal annotations / thresholds - *New* ⓘ

Add threshold

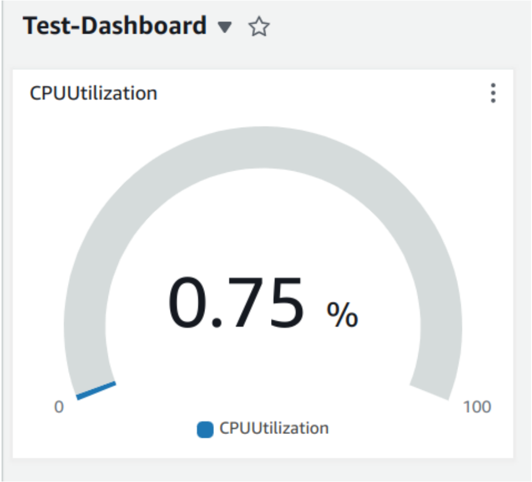
Value

● Latest value shows the value from the most recent period of your chosen time range.

○ Time range value shows the value from the entire time range.

Cancel | Create widget

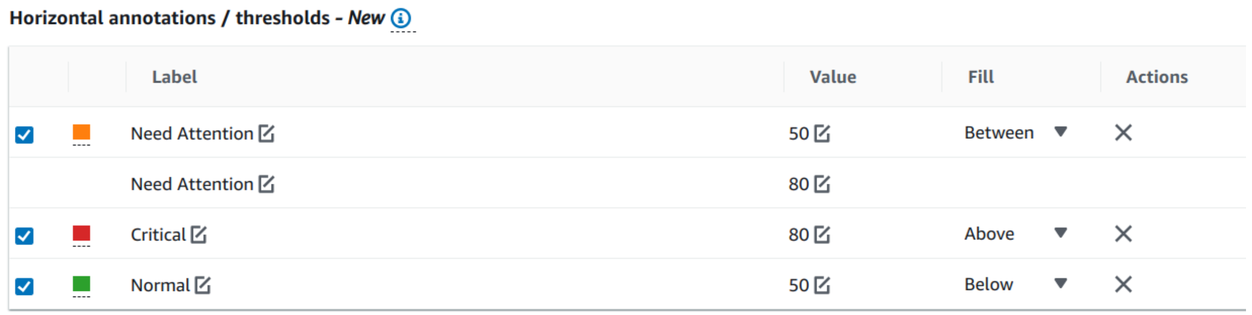
Step 6 - Click on “Create widget”. The widget is created in the dashboard.



Step 7 - Configuring the gauge widget. Edit the threshold for the gauge widget.

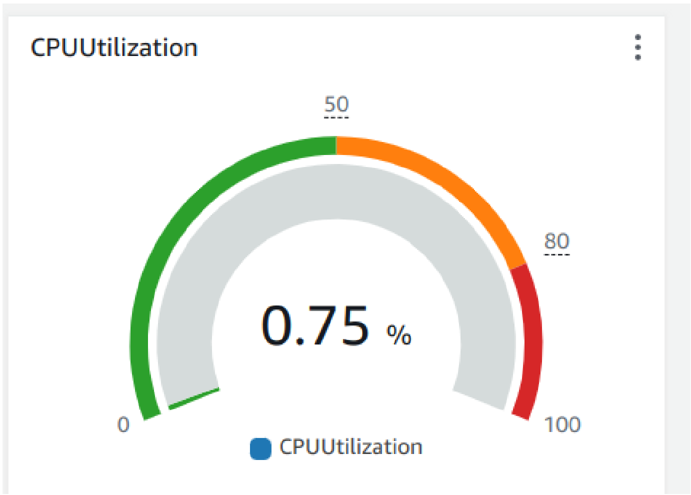
The gauge will be divided in three parts -

- **Normal -** It will be shown in green, representing normal or expected CPU utilization.
- **Need Attention -** It is shown in orange, representing high CPU utilization which can be handled but needs some attention.
- **Critical -** It is shown in red, representing critical CPU utilization and some action needs to be taken to reduce it or remediate it.

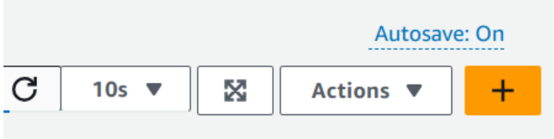


Horizontal annotations / thresholds - *New*

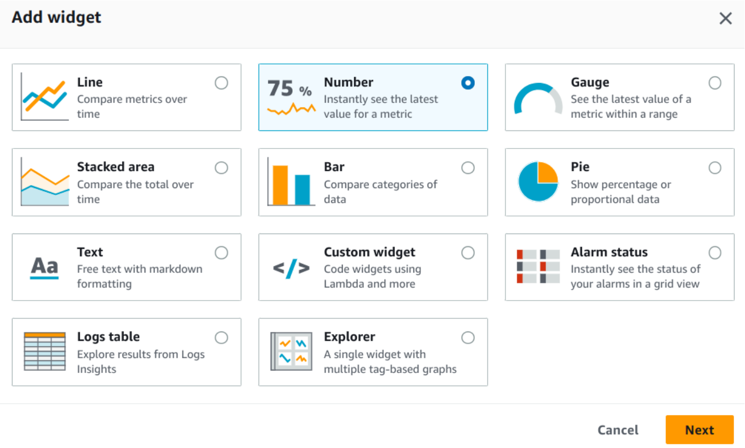
		Label	Value	Fill	Actions
☑	🟧	Need Attention	50	Between ▼	✕
		Need Attention	80		
☑	🟥	Critical	80	Above ▼	✕
☑	🟩	Normal	50	Below ▼	✕



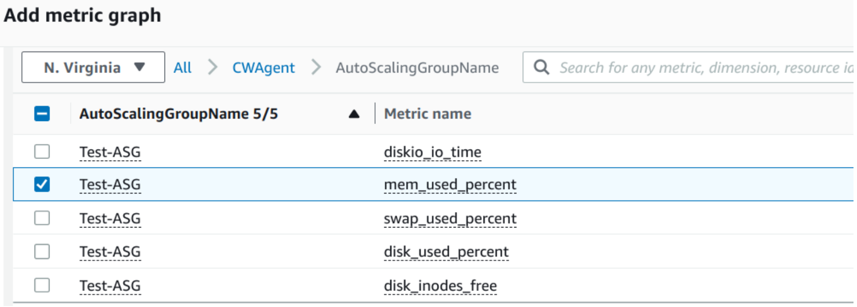
Step 8 - Create more widgets in the dashboard. Click on the plus button.



1. Number widget for displaying memory utilization based on ASG.

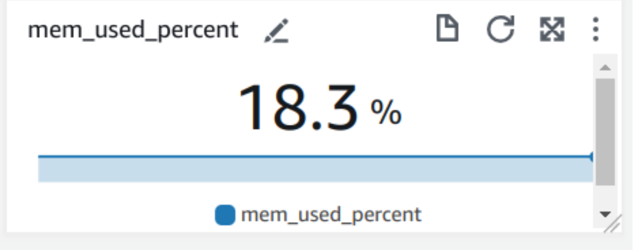

Add widget

- ○ **Line** Compare metrics over time
- ● **Number** Instantly see the latest value for a metric
- ○ **Gauge** See the latest value of a metric within a range
- ○ **Stacked area** Compare the total over time
- ○ **Bar** Compare categories of data
- ○ **Pie** Show percentage or proportional data
- ○ **Text** Free text with markdown formatting
- ○ **Custom widget** Code widgets using Lambda and more
- ○ **Alarm status** Instantly see the status of your alarms in a grid view
- ○ **Logs table** Explore results from Logs Insights
- ○ **Explorer** A single widget with multiple tag-based graphs


Add metric graph

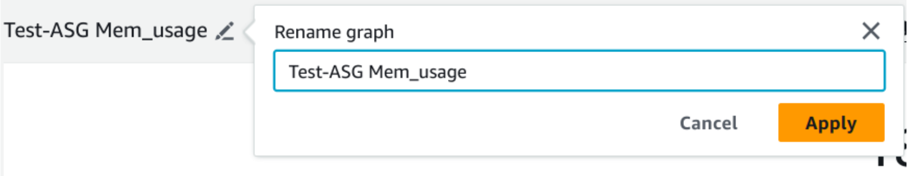
N. Virginia ▼ | All > CWAgent > AutoScalingGroupName | Search for any metric, dimension, resource id

▬	AutoScalingGroupName 5/5 ▲	Metric name
□	Test-ASG	diskio_io_time
☑	Test-ASG	mem_used_percent
□	Test-ASG	swap_used_percent
□	Test-ASG	disk_used_percent
□	Test-ASG	disk_inodes_free


mem_used_percent

18.3 %

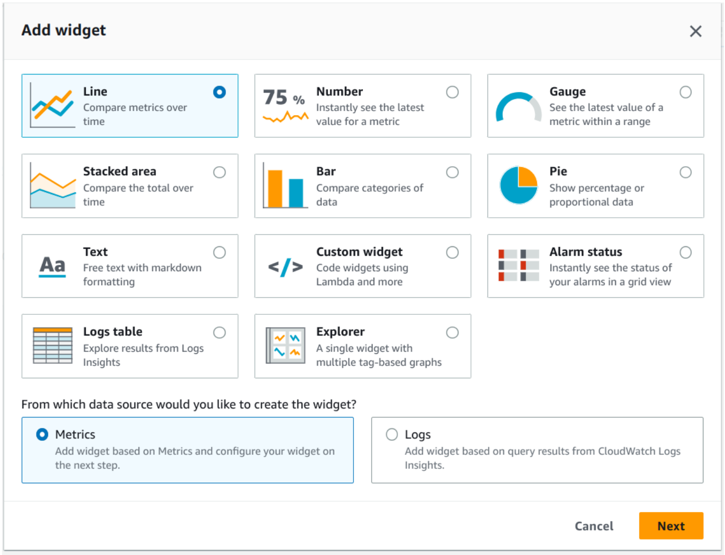
Updating the name of the graph.


Test-ASG Mem_usage

Rename graph

Test-ASG Mem_usage

2. Line widget for disk usage.

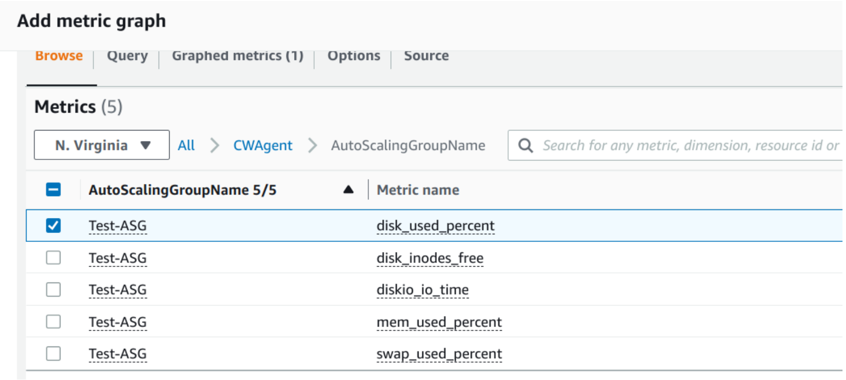


Add widget

- ● **Line** Compare metrics over time
- ○ **Number** Instantly see the latest value for a metric
- ○ **Gauge** See the latest value of a metric within a range
- ○ **Stacked area** Compare the total over time
- ○ **Bar** Compare categories of data
- ○ **Pie** Show percentage or proportional data
- ○ **Text** Free text with markdown formatting
- ○ **Custom widget** Code widgets using Lambda and more
- ○ **Alarm status** Instantly see the status of your alarms in a grid view
- ○ **Logs table** Explore results from Logs Insights
- ○ **Explorer** A single widget with multiple tag-based graphs

From which data source would you like to create the widget?

- ● Metrics Add widget based on Metrics and configure your widget on the next step.
- ○ Logs Add widget based on query results from CloudWatch Logs Insights.

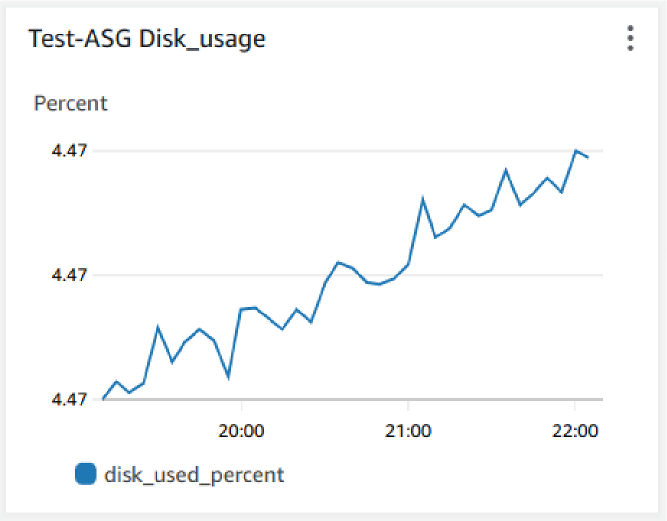


Add metric graph

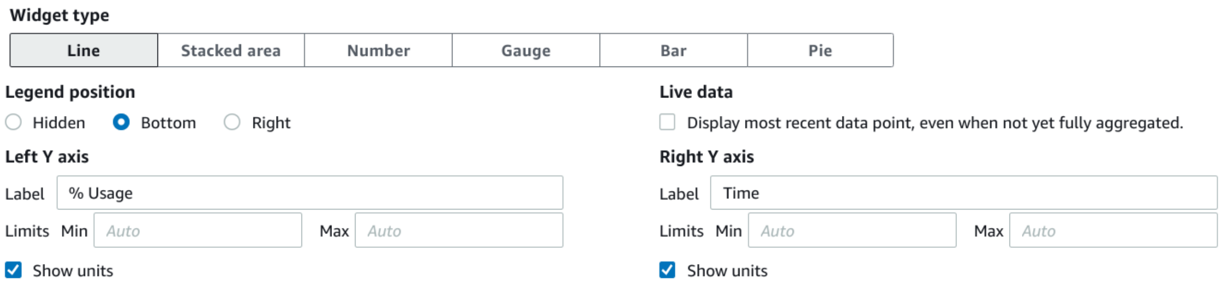
Metrics (5)

N. Virginia ▼ All > CWAgent > AutoScalingGroupName

☐	AutoScalingGroupName 5/5 ▲	Metric name
☑	Test-ASG	disk_used_percent
☐	Test-ASG	disk_inodes_free
☐	Test-ASG	diskio_io_time
☐	Test-ASG	mem_used_percent
☐	Test-ASG	swap_used_percent



The line widget can be configured to show labels for X and Y axis as required. The values on both the axes can be configured.



Widget type

[✓ Line]	Stacked area	Number	Gauge	Bar	Pie

Legend position

○ Hidden ● Bottom ○ Right

Left Y axis

Label: % Usage

Limits Min: Auto Max: Auto

☑ Show units

Live data

□ Display most recent data point, even when not yet fully aggregated.

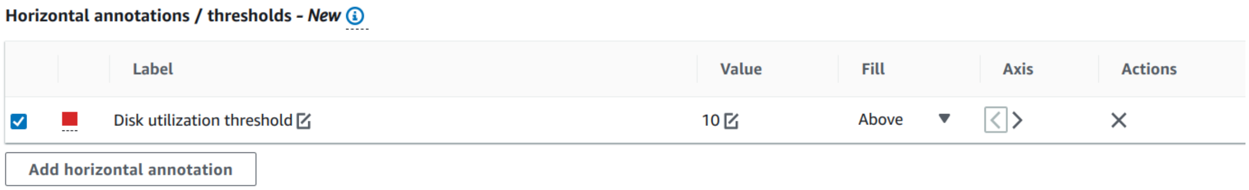
Right Y axis

Label: Time

Limits Min: Auto Max: Auto

☑ Show units

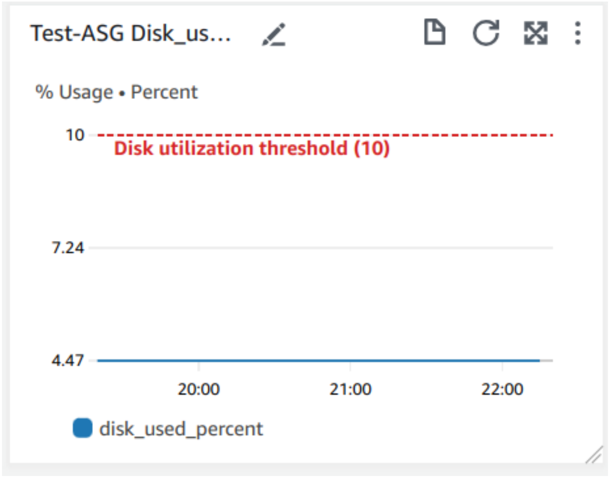
Adding horizontal annotation can help to display certain limits and values.



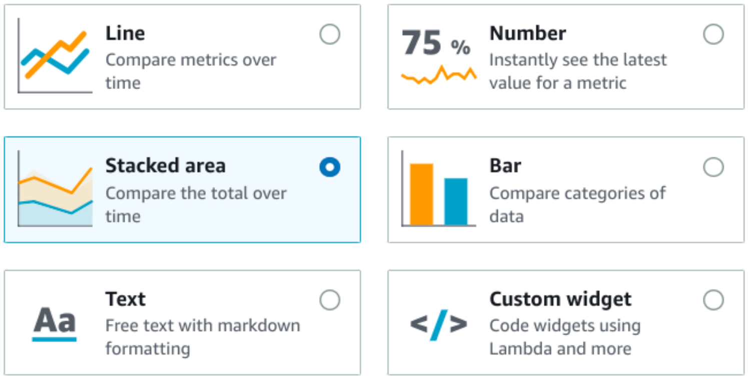
Horizontal annotations / thresholds - *New*

		Label	Value	Fill	Axis	Actions
☑	🟥	Disk utilization threshold	10	Above ▼	< >	×

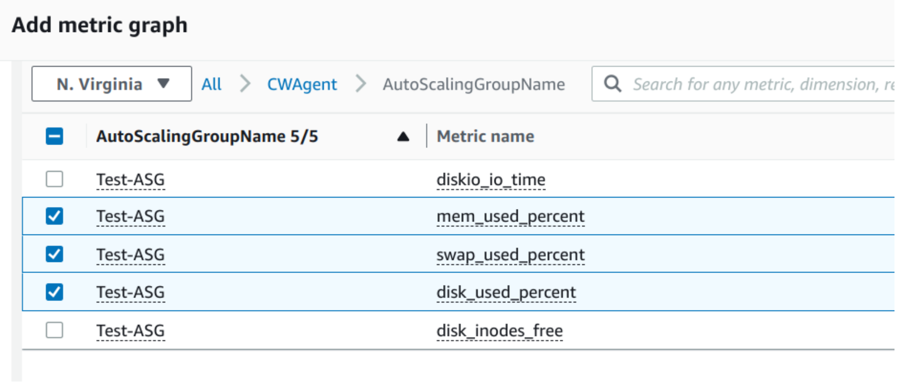
Add horizontal annotation



3. Stacked area widget to display and compare trends for related metrics.



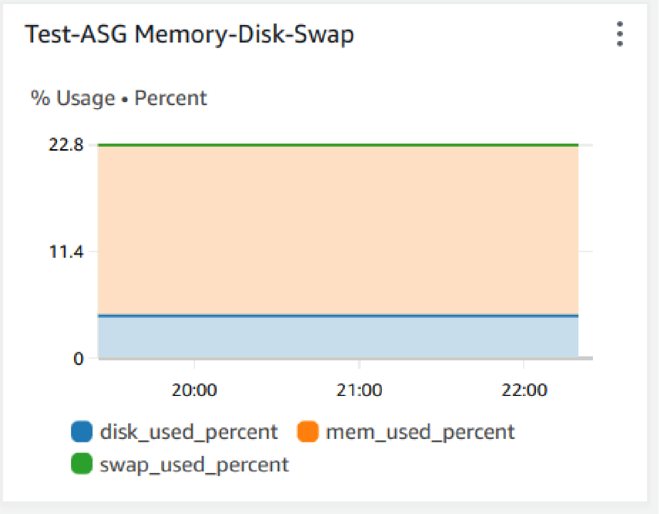
- **Line** ○ Compare metrics over time
- **Number** ○ Instantly see the latest value for a metric
- **Stacked area** ● Compare the total over time
- **Bar** ○ Compare categories of data
- **Text** ○ Free text with markdown formatting
- **Custom widget** ○ Code widgets using Lambda and more



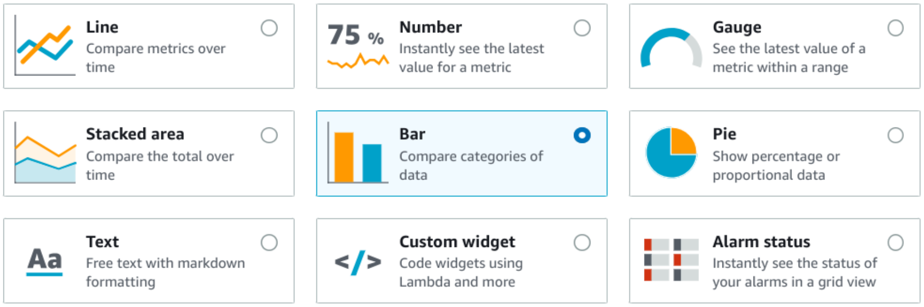
Add metric graph

N. Virginia ▼ | All > CWAgent > AutoScalingGroupName | Search for any metric, dimension, re

⊟	AutoScalingGroupName 5/5 ▲	Metric name
☐	Test-ASG	diskio_io_time
☑	Test-ASG	mem_used_percent
☑	Test-ASG	swap_used_percent
☑	Test-ASG	disk_used_percent
☐	Test-ASG	disk_inodes_free

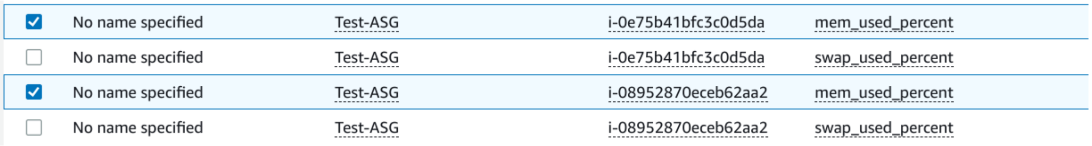


4. Bar graph to compare different metrics.

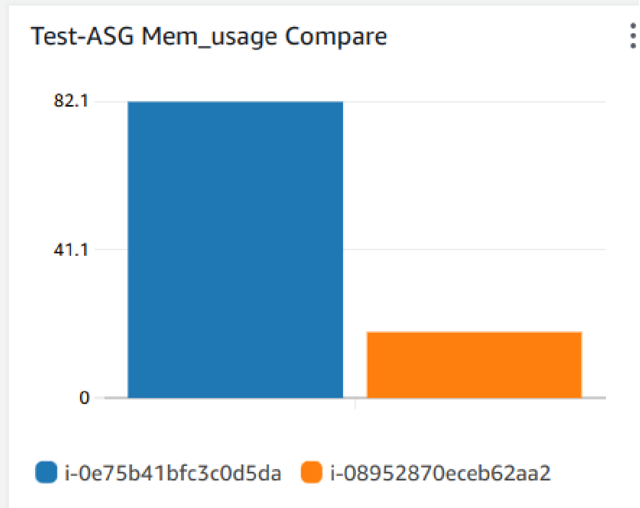


- **Line** Compare metrics over time ○
- **Number** Instantly see the latest value for a metric ○
- **Gauge** See the latest value of a metric within a range ○
- **Stacked area** Compare the total over time ○
- **Bar** Compare categories of data ●
- **Pie** Show percentage or proportional data ○
- **Text** Free text with markdown formatting ○
- **Custom widget** Code widgets using Lambda and more ○
- **Alarm status** Instantly see the status of your alarms in a grid view ○

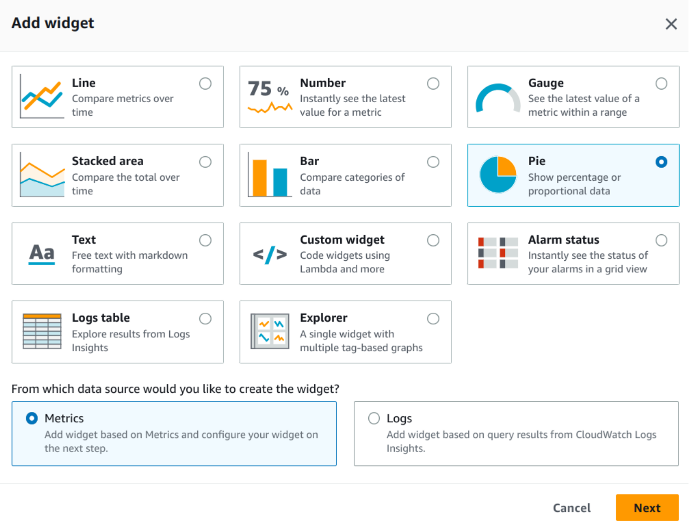
Taking memory usage metrics of the two instances running in the ASG.



☑	No name specified	Test-ASG	i-0e75b41bfc3c0d5da	mem_used_percent
☐	No name specified	Test-ASG	i-0e75b41bfc3c0d5da	swap_used_percent
☑	No name specified	Test-ASG	i-08952870eceb62aa2	mem_used_percent
☐	No name specified	Test-ASG	i-08952870eceb62aa2	swap_used_percent



5. Pie chart to display proportional data.



Add widget

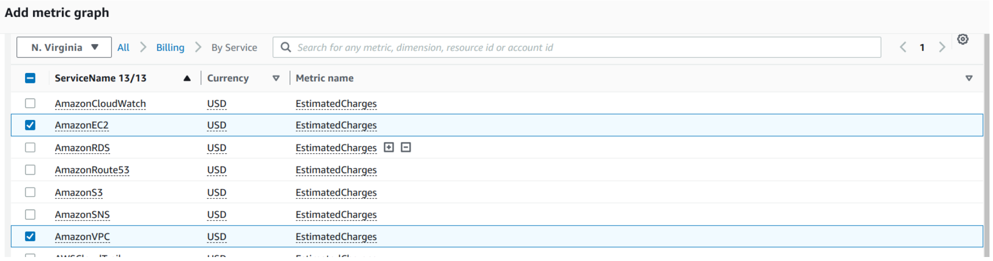
Line ○ Compare metrics over time	Number ○ Instantly see the latest value for a metric	Gauge ○ See the latest value of a metric within a range
Stacked area ○ Compare the total over time	Bar ○ Compare categories of data	Pie ● Show percentage or proportional data
Text ○ Free text with markdown formatting	Custom widget ○ Code widgets using Lambda and more	Alarm status ○ Instantly see the status of your alarms in a grid view
Logs table ○ Explore results from Logs Insights	Explorer ○ A single widget with multiple tag-based graphs	

From which data source would you like to create the widget?

● Metrics
Add widget based on Metrics and configure your widget on the next step.

○ Logs
Add widget based on query results from CloudWatch Logs Insights.

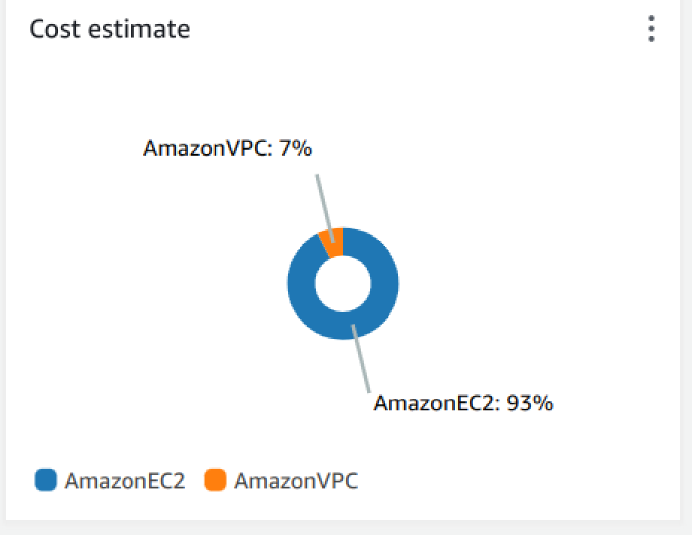
×
75 %
Aa
</>
Cancel
Next



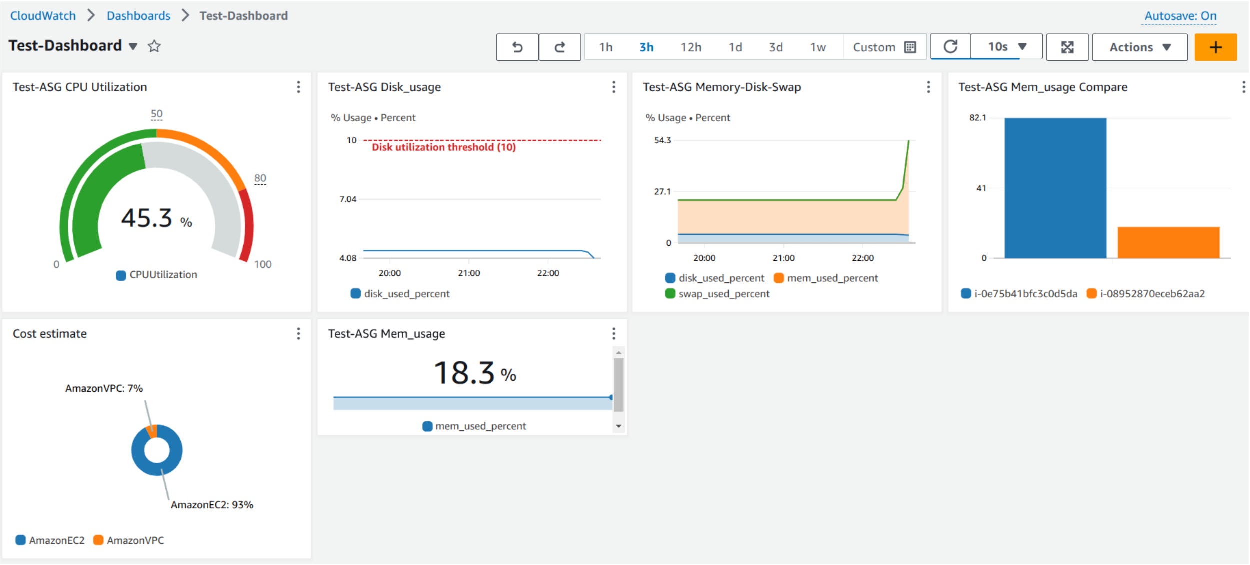
Add metric graph

N. Virginia ▼
All > Billing > By Service
Search for any metric, dimension, resource id or account id
< 1 >

☐	ServiceName 13/13 ▲	Currency ▽	Metric name ▽
☐	AmazonCloudWatch	USD	EstimatedCharges
☑	AmazonEC2	USD	EstimatedCharges
☐	AmazonRDS	USD	EstimatedCharges ⊞ ⊟
☐	AmazonRoute53	USD	EstimatedCharges
☐	AmazonS3	USD	EstimatedCharges
☐	AmazonSNS	USD	EstimatedCharges
☑	AmazonVPC	USD	EstimatedCharges

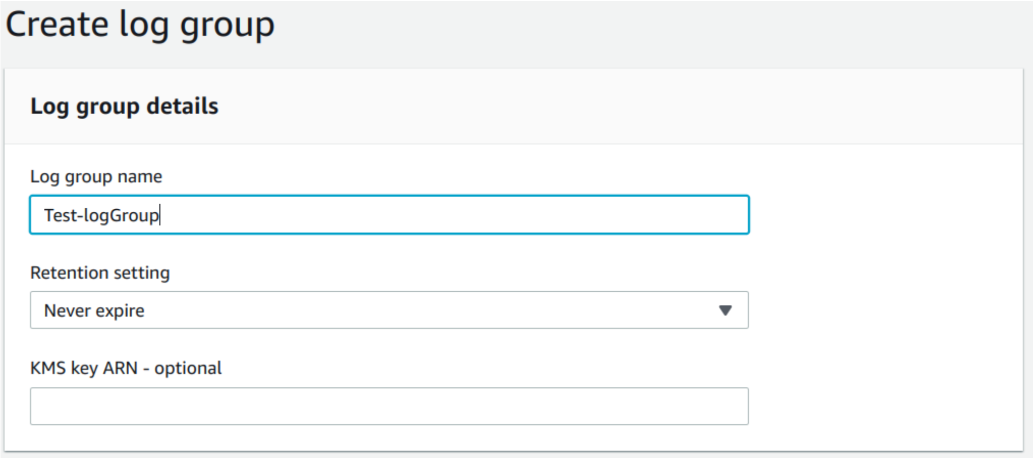


Step 9 - The complete dashboard.



Assignment 2 - Create metric filter in cloudwatch for security group and user authorization.

Step 1 - Navigate to the CloudWatch console and create a log group.



Create log group

Log group details

Log group name

Test-logGroup

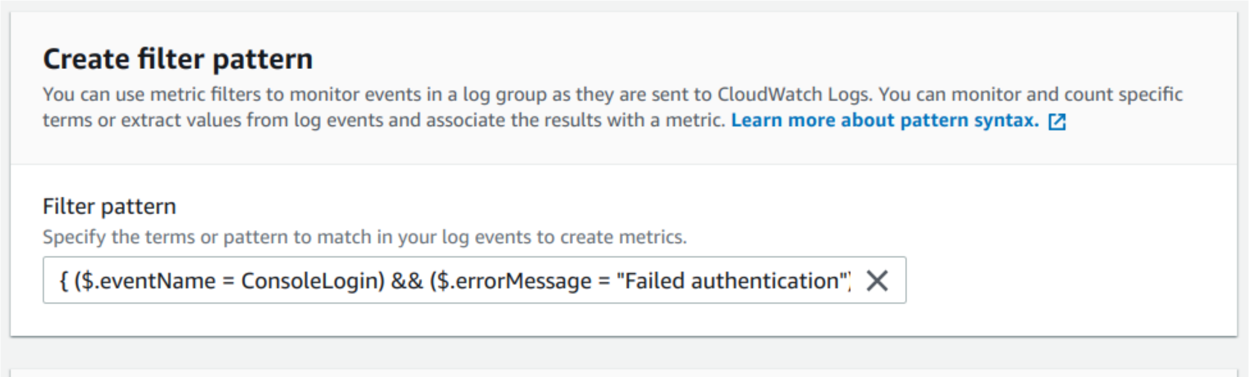
Retention setting

Never expire ▼

KMS key ARN - optional

Step 2 - Create a metric filter in the log group.

"{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }" - The filter pattern will filter out the specified events of console login requests with an error message of failed authentication.



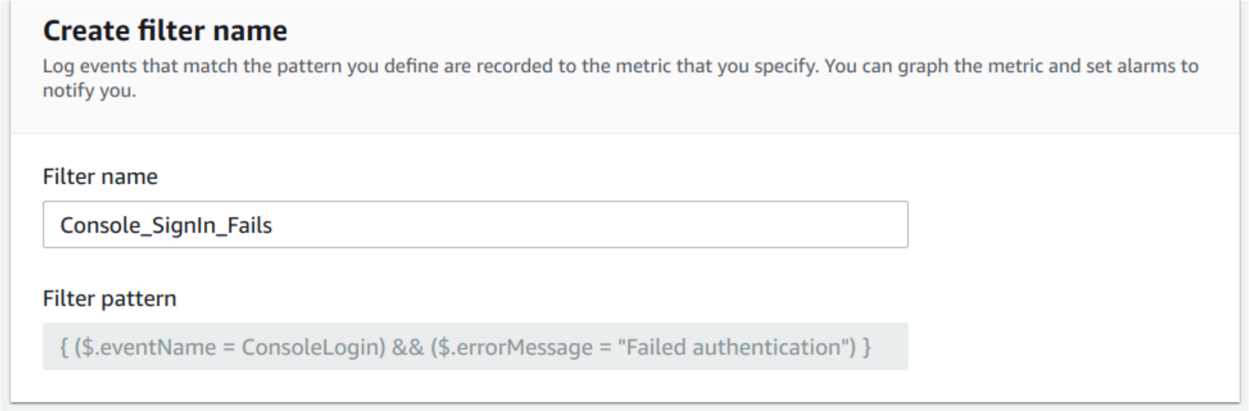
Create filter pattern

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. Learn more about pattern syntax.

Filter pattern

Specify the terms or pattern to match in your log events to create metrics.

{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") ✕



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.

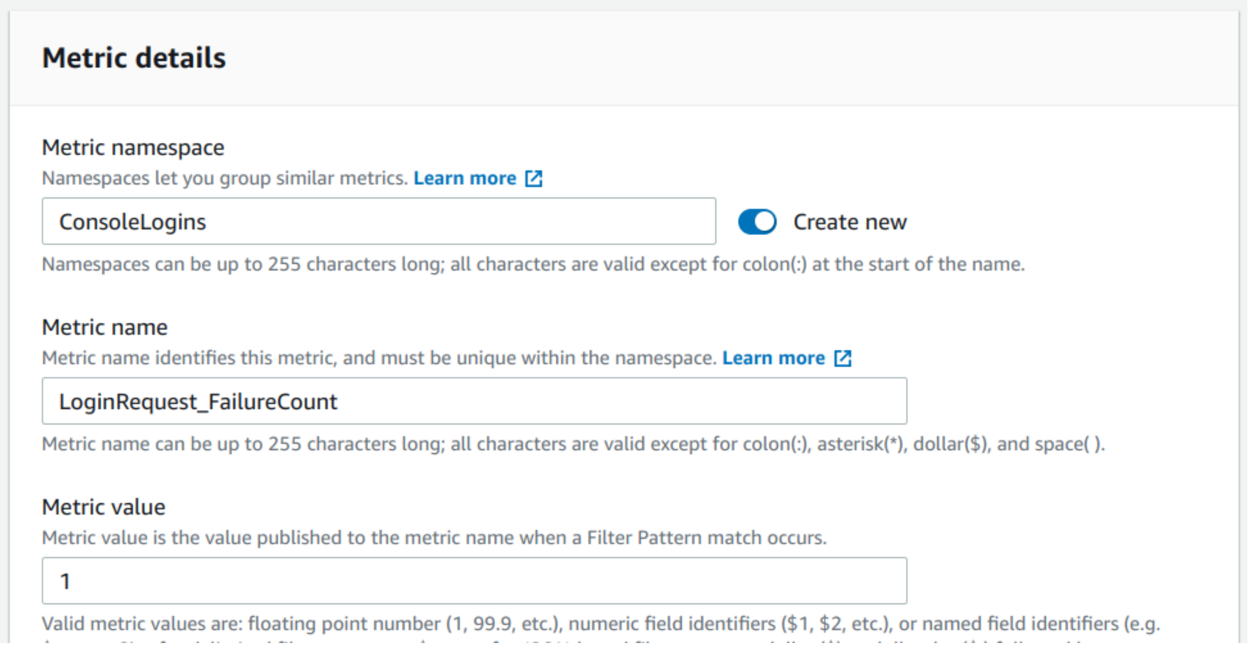
Filter name

Console_SignIn_Fails

Filter pattern

{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }

The metric will have the name “LoginRequest_FailureCount” and will be stored in the “ConsoleLogins” namespace.



Metric details

Metric namespace

Namespaces let you group similar metrics. Learn more

ConsoleLogins

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

LoginRequest_FailureCount

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

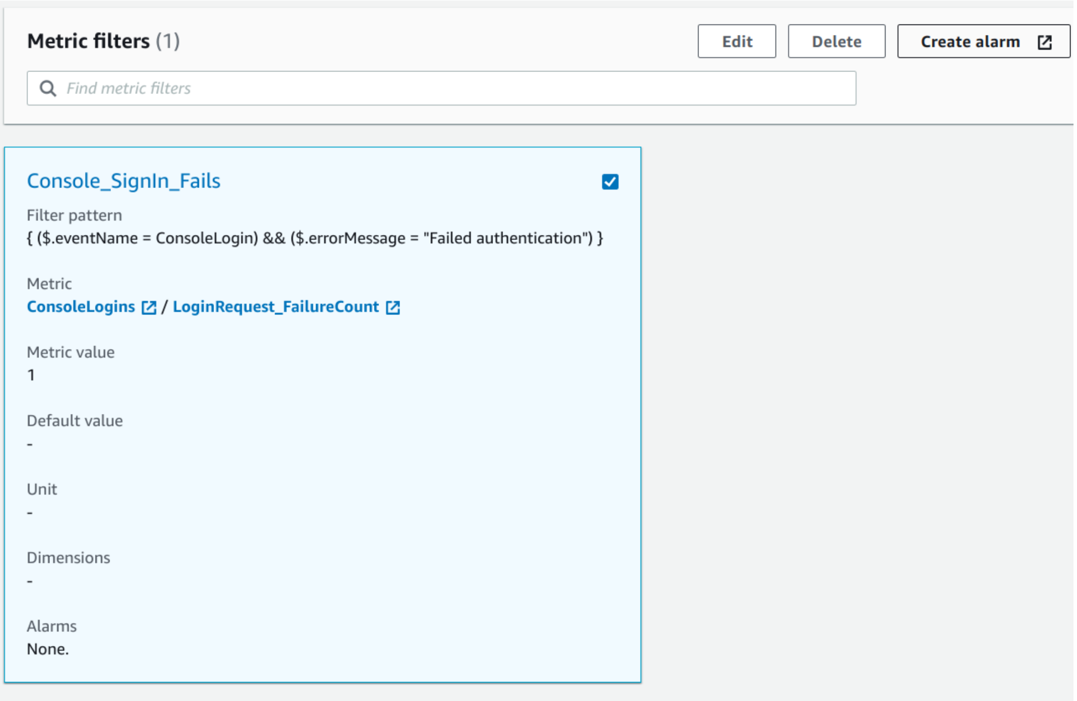
Metric value

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.

Step 3 - Select the metric filter and create an alarm.



Console_SignIn_Fails ☑

Filter pattern

{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }

Metric

ConsoleLogins / LoginRequest_FailureCount

Metric value

1

Default value

-

Unit

-

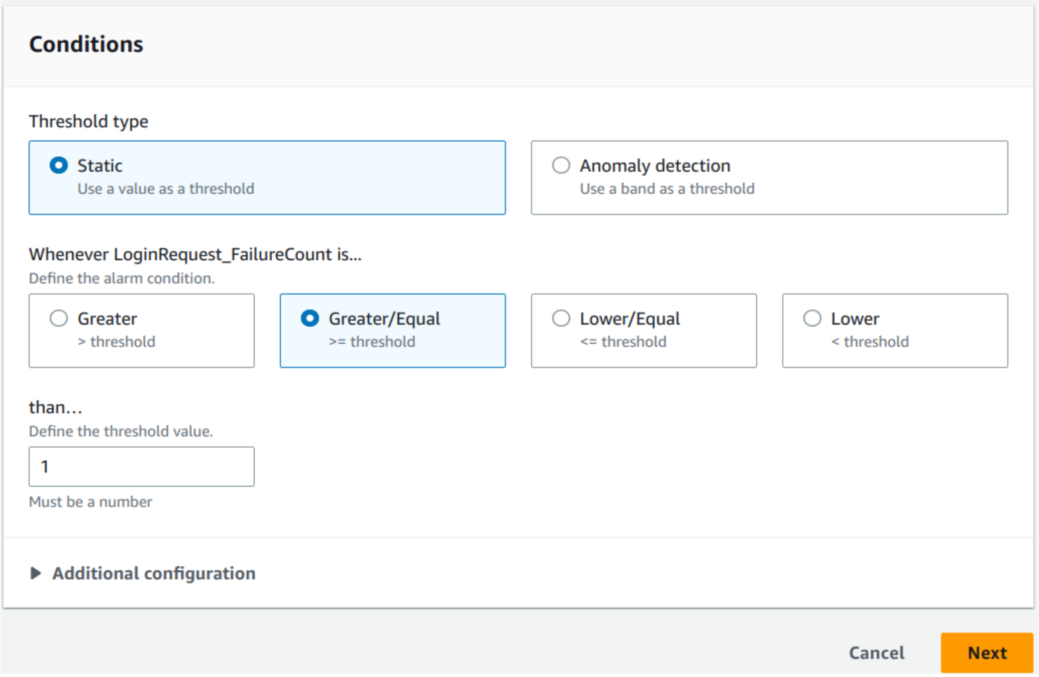
Dimensions

-

Alarms

None.

The alarm will be triggered whenever the condition meets. Here the condition is whenever the metric value is greater than or equal to one, the action to send an alert through the SNS topic will be triggered.



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever LoginRequest_FailureCount is...
Define the alarm condition.

○ Greater
> threshold

● Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

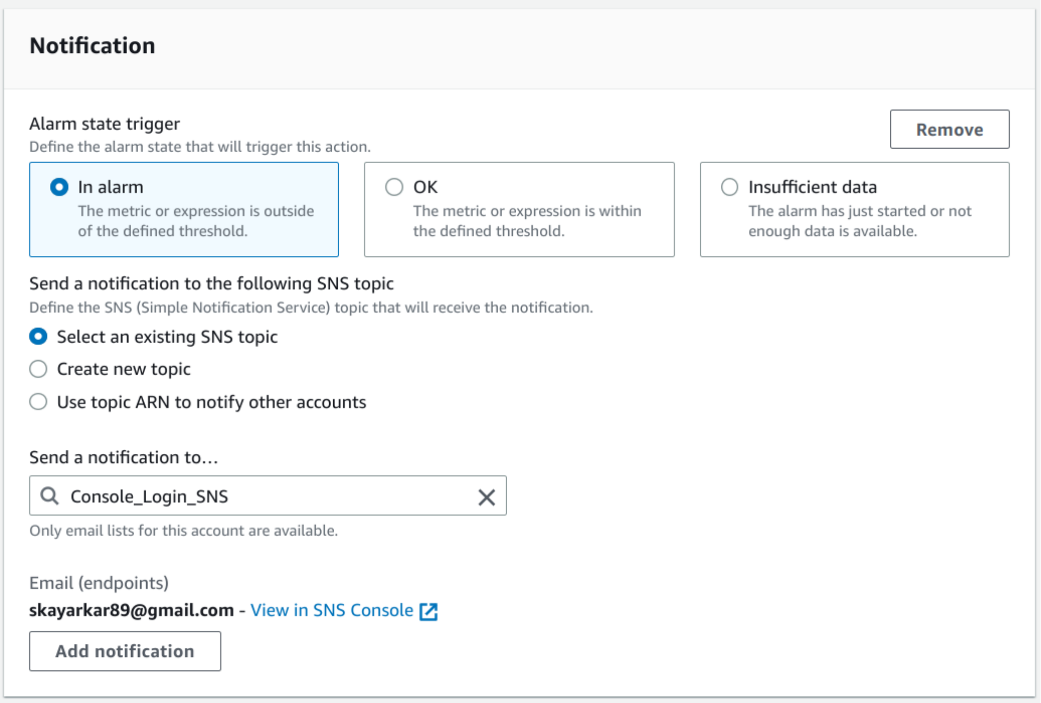
○ Lower
< threshold

than...
Define the threshold value.

1

Must be a number

▶ Additional configuration



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.

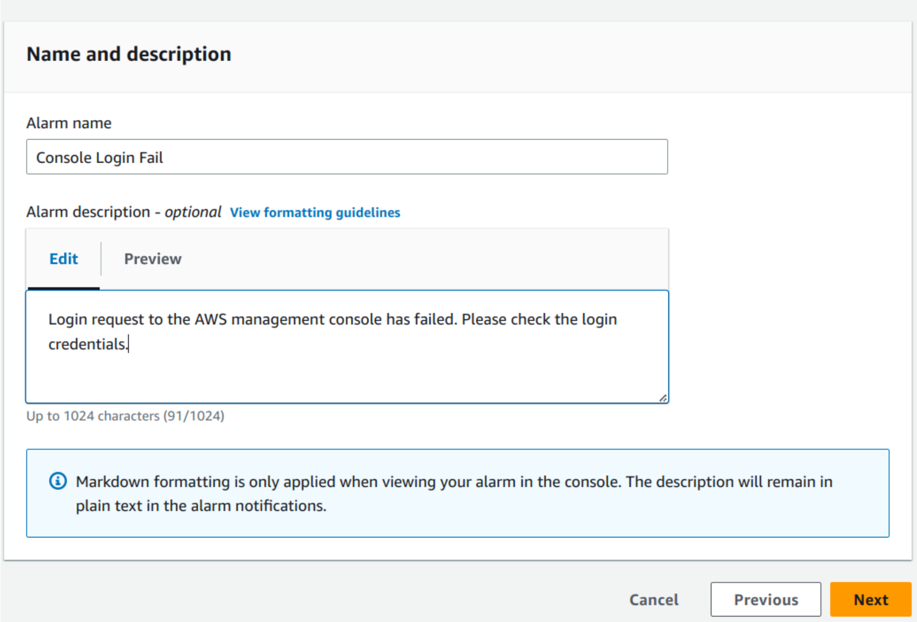
● Select an existing SNS topic
○ Create new topic
○ Use topic ARN to notify other accounts

Send a notification to...

Console_Login_SNS

Only email lists for this account are available.

Email (endpoints)
skayarkar89@gmail.com - View in SNS Console



Name and description

Alarm name

Console Login Fail

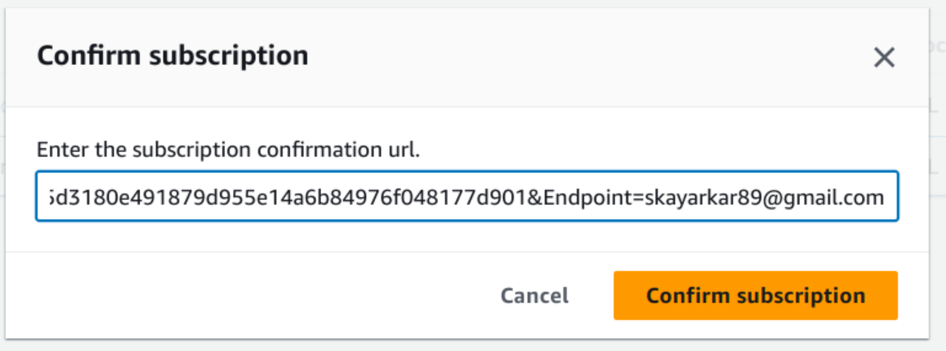
Alarm description - *optional* View formatting guidelines

Login request to the AWS management console has failed. Please check the login credentials.

Up to 1024 characters (91/1024)

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

Confirm the subscription request of SNS topic.



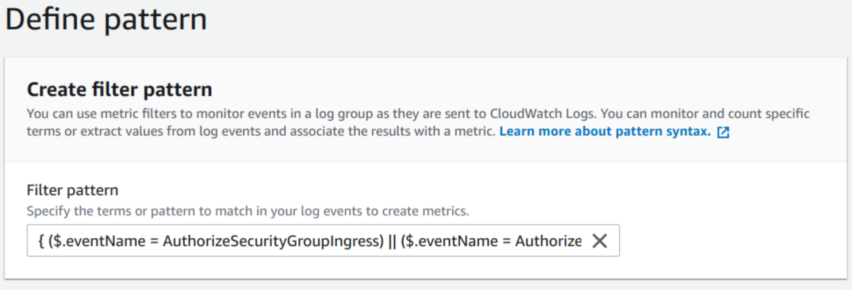
Confirm subscription

Enter the subscription confirmation url.

;d3180e491879d955e14a6b84976f048177d901&Endpoint=skayarkar89@gmail.com

Step 4 - Create a second metric filter for security group configuration changes.

"{($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }" - This filter pattern will filter out the logs of any security group configuration changes based on the event names specified in the pattern.



Define pattern

Create filter pattern

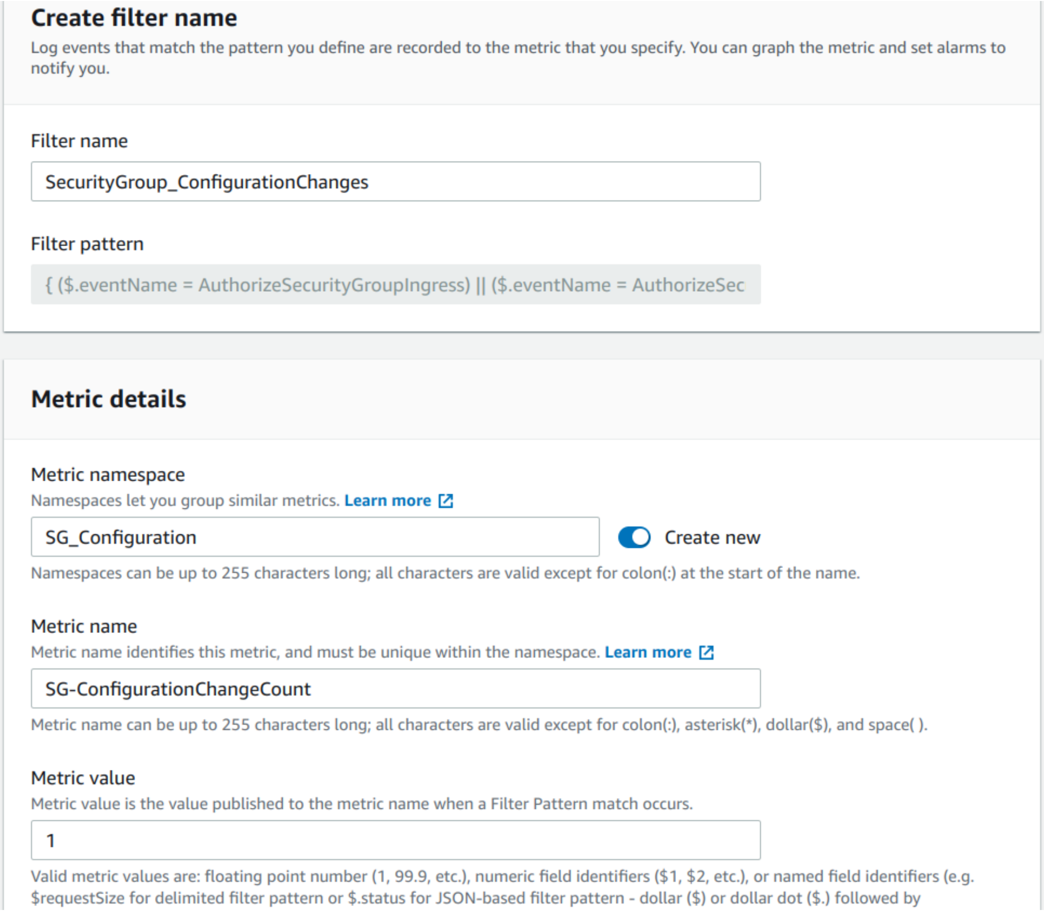
You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. Learn more about pattern syntax.

Filter pattern

Specify the terms or pattern to match in your log events to create metrics.

{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = Authorize

The filter name is “SecurityGroup_ConfigurationChanges”, with the metric “SG-ConfigurationChangeCount” stored in the “SG_Configuration” metric namespace.



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

SecurityGroup_ConfigurationChanges

Filter pattern

{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSec

Metric details

Metric namespace

Namespaces let you group similar metrics. **Learn more**

SG_Configuration ● 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**

SG-ConfigurationChangeCount

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

Metric value

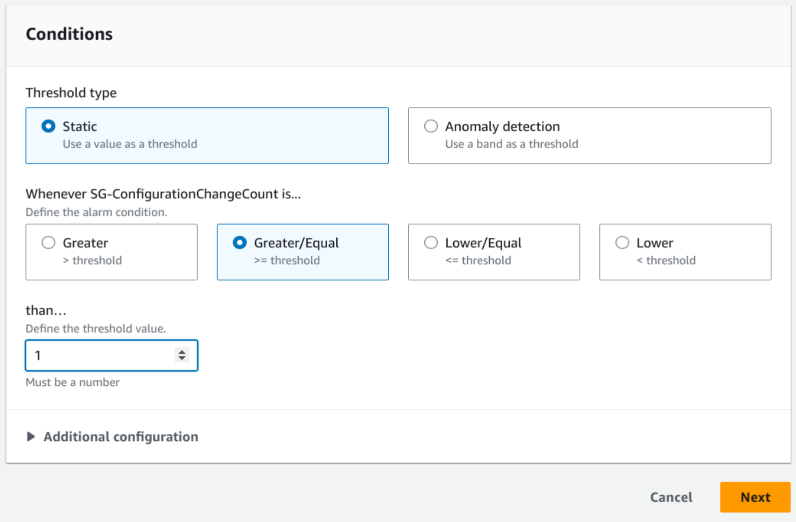
Metric value is the value published to the metric name when a Filter Pattern match occurs.

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

Step 5 - Create an alarm for the above metric filter.

The alarm will be triggered whenever the metric value is equal to or greater than 1.



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever SG-ConfigurationChangeCount is...
Define the alarm condition.

○ Greater
> threshold

● Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

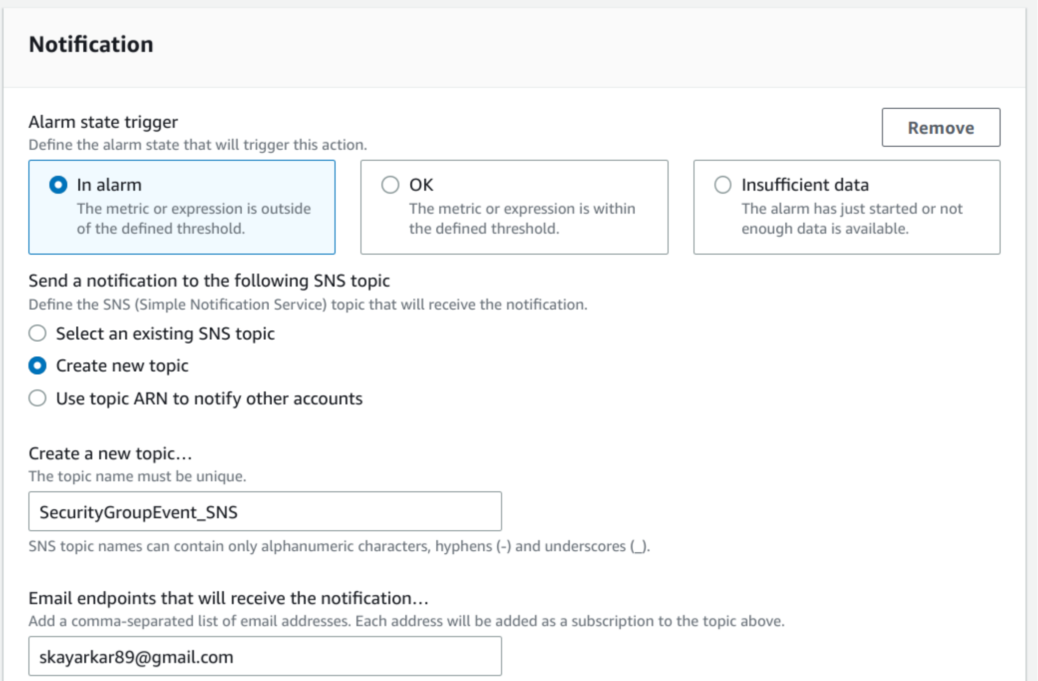
○ Lower
< threshold

than...
Define the threshold value.

1

Must be a number

Add the action to notify through the SNS topic and confirm the subscription request in SNS console.



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.

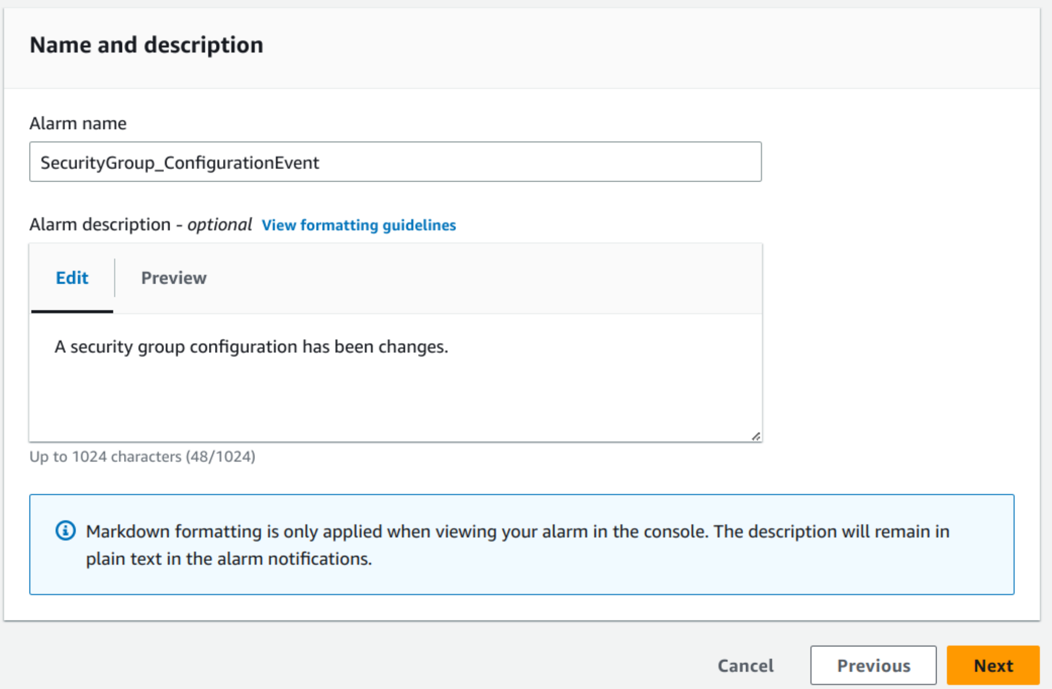
SecurityGroupEvent_SNS

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.

skayarkar89@gmail.com



Name and description

Alarm name

SecurityGroup_ConfigurationEvent

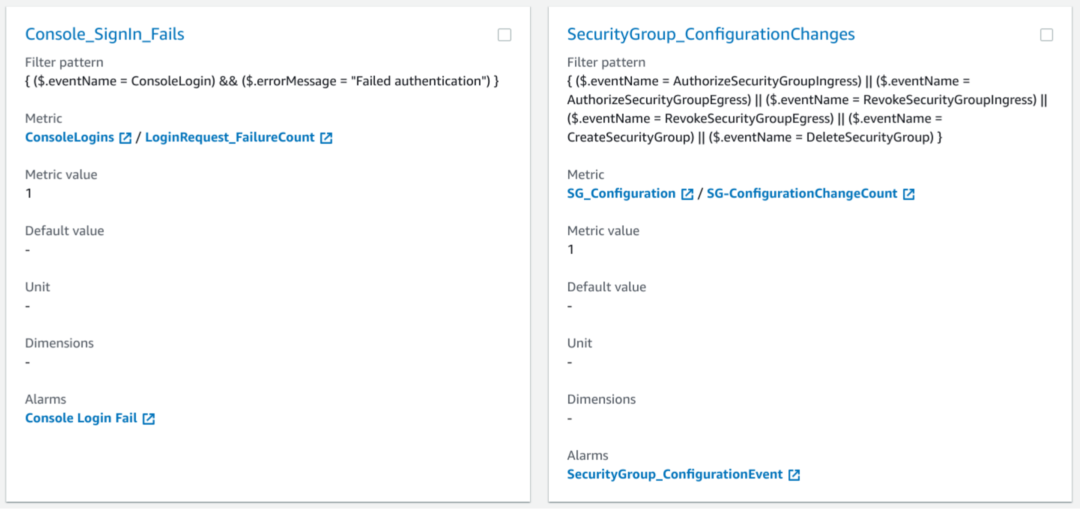
Alarm description - *optional* View formatting guidelines

A security group configuration has been changes.

Up to 1024 characters (48/1024)

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

Both the metric filters are created.



Console_SignIn_Fails ☐

Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }

Metric
ConsoleLogins / LoginRequest_FailureCount

Metric value
1

Default value
-

Unit
-

Dimensions
-

Alarms
Console Login Fail

SecurityGroup_ConfigurationChanges ☐

Filter pattern
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }

Metric
SG_Configuration / SG-ConfigurationChangeCount

Metric value
1

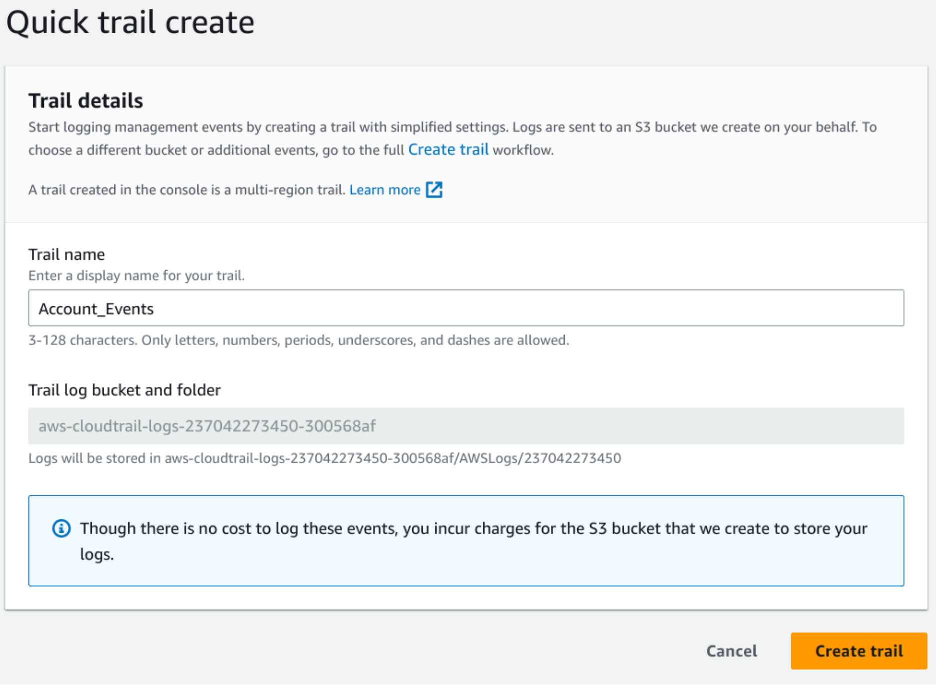
Default value
-

Unit
-

Dimensions
-

Alarms
SecurityGroup_ConfigurationEvent

Step 6 - Create a CloudTrail trail. To log API calls in the cloudwatch log group that was created in the previous step.



Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full Create trail workflow.

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

Trail name
Enter a display name for your trail.

Account_Events

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

Trail log bucket and folder

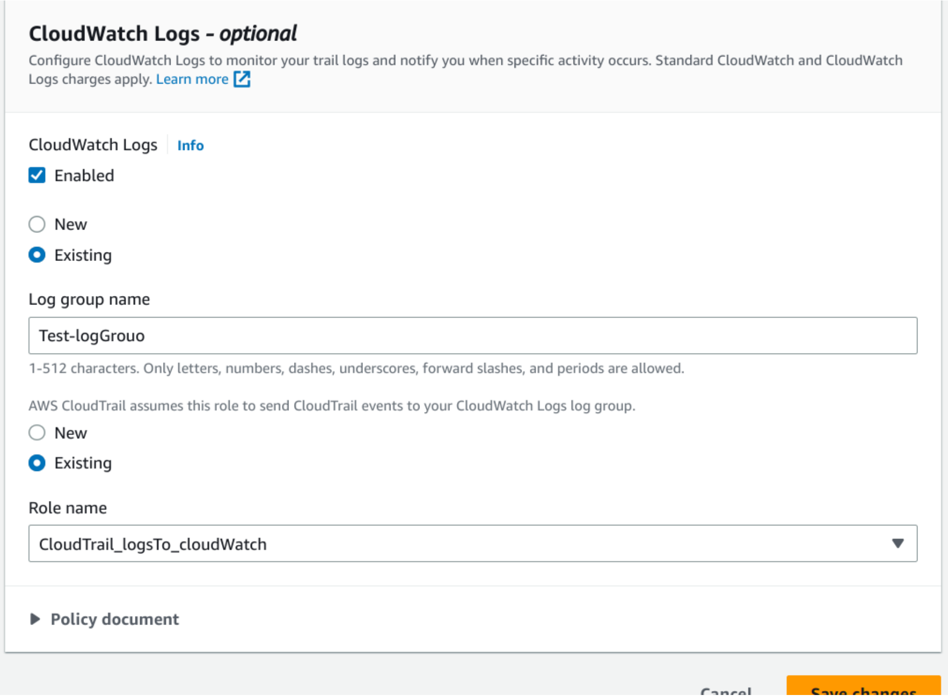
aws-cloudtrail-logs-237042273450-300568af

Logs will be stored in aws-cloudtrail-logs-237042273450-300568af/AWSLogs/237042273450

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

Step 7 - Edit the trail and enable CloudWatch logs.

The role attached will allow CloudTrail to push logs to CloudWatch log group “Test-logGroup”.



CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more

CloudWatch Logs Info

☑ Enabled

○ New

● Existing

Log group name

Test-logGrouo

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

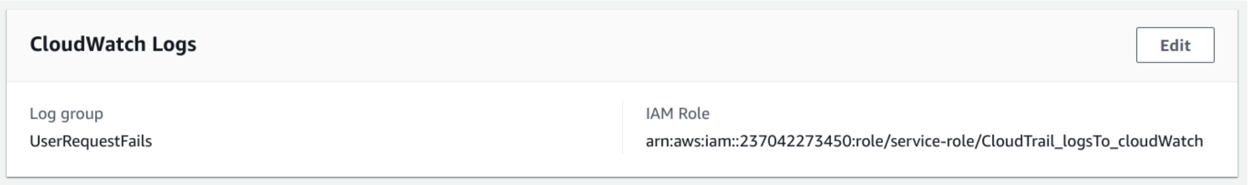
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

○ New

● Existing

Role name

CloudTrail_logsTo_cloudWatch



CloudWatch Logs

Log group

UserRequestFails

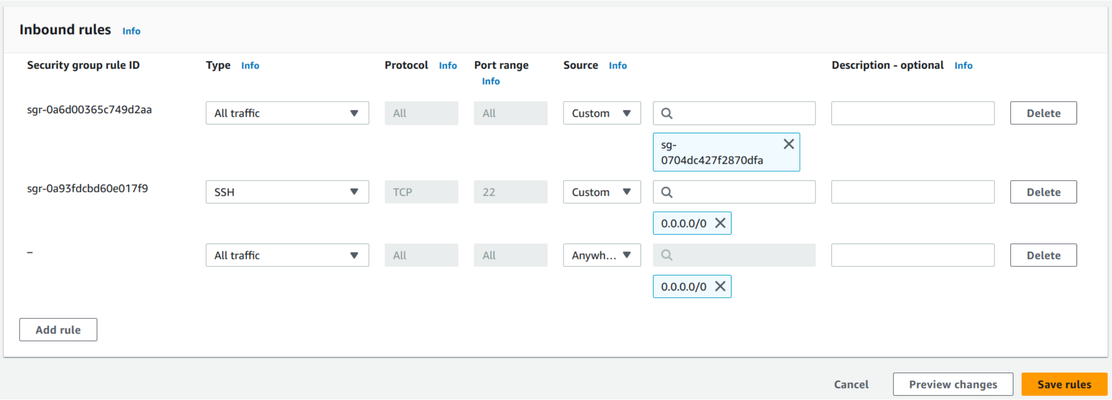
IAM Role

arn:aws:iam::237042273450:role/service-role/CloudTrail_logsTo_cloudWatch

Step 8 - Check if the alarms and metric filters are working correctly.

- **Configure one of the security groups.**

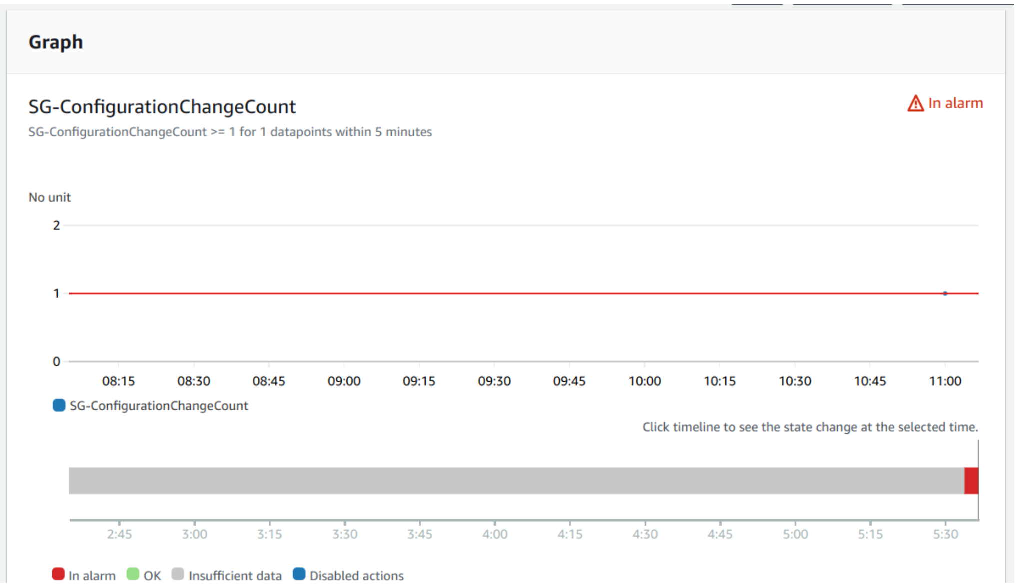
  Adding an inbound rule to allow all traffic from anywhere.



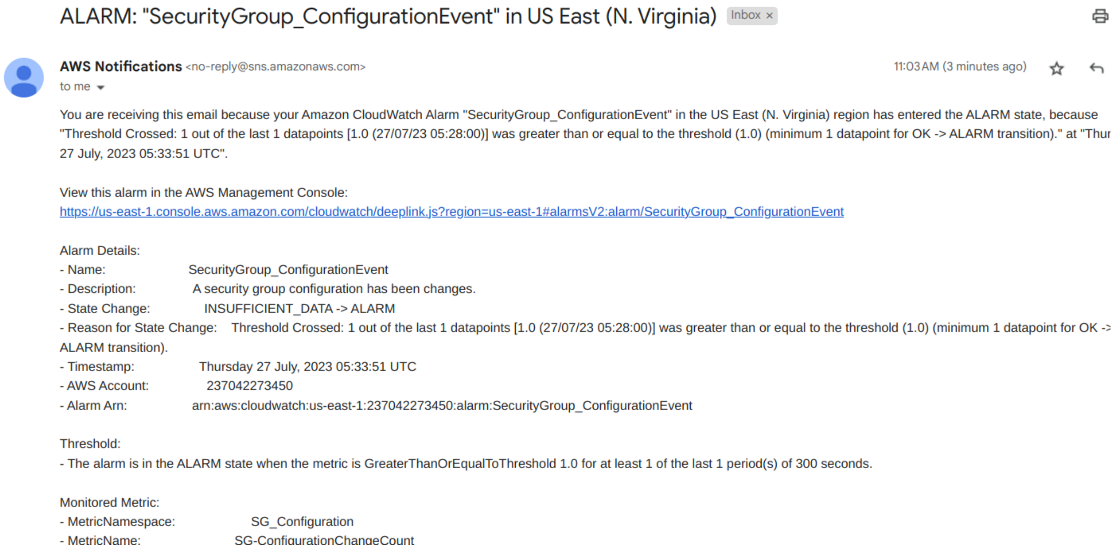
Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0a6d00365c749d2aa	All traffic	All	All	Custom	sg-0704dc427f2870dfa		Delete
sgr-0a93fdcbd60e017f9	SSH	TCP	22	Custom	0.0.0.0/0		Delete
–	All traffic	All	All	Anywh...	0.0.0.0/0		Delete

The alarm state turns to an “in-alarm” state.



Email alert sent through SNS topic.


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

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

11:03 AM (3 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "SecurityGroup_ConfigurationEvent" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (27/07/23 05:28:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thur 27 July, 2023 05:33:51 UTC".

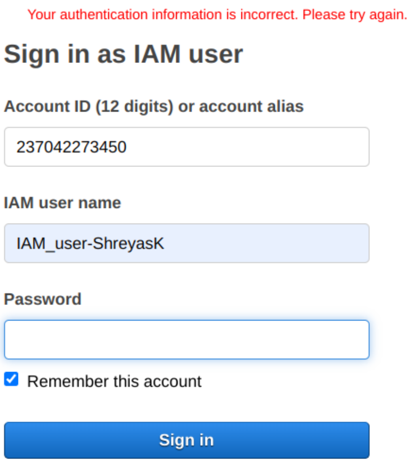
View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/SecurityGroup_ConfigurationEvent

Alarm Details:
- Name: SecurityGroup_ConfigurationEvent
- Description: A security group configuration has been changes.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (27/07/23 05:28:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 27 July, 2023 05:33:51 UTC
- AWS Account: 237042273450
- Alarm Arn: arn:aws:cloudwatch:us-east-1:237042273450:alarm:SecurityGroup_ConfigurationEvent

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: SG_Configuration
- MetricName: SG-ConfigurationChangeCount

- **Make a console login fail attempt.**



Your authentication information is incorrect. Please try again.

Sign in as IAM user

Account ID (12 digits) or account alias

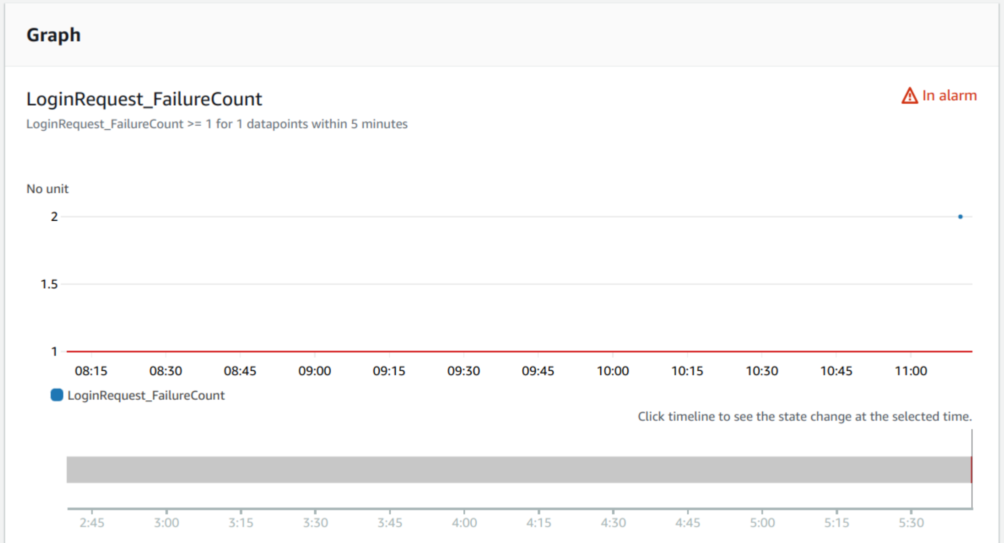
237042273450

IAM user name

IAM_user-ShreyasK

Password

☑ Remember this account

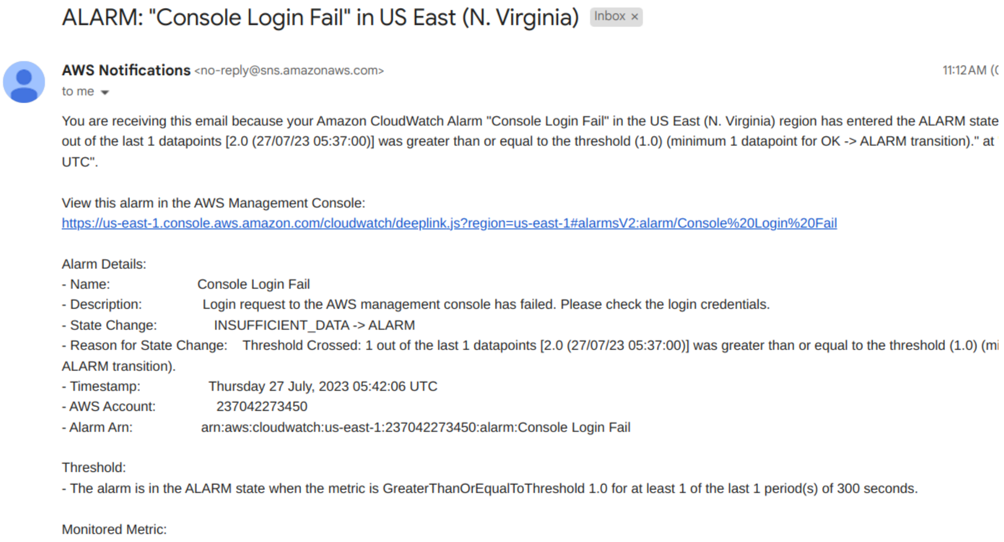


Graph

LoginRequest_FailureCount

LoginRequest_FailureCount >= 1 for 1 datapoints within 5 minutes

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



ALARM: "Console Login Fail" in US East (N. Virginia)

AWS Notifications <no-reply@sns.amazonaws.com> 11:12 AM ((

to me

You are receiving this email because your Amazon CloudWatch Alarm "Console Login Fail" in the US East (N. Virginia) region has entered the ALARM state out of the last 1 datapoints [2.0 (27/07/23 05:37:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at 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/Console%20Login%20Fail

Alarm Details:
- Name: Console Login Fail
- Description: Login request to the AWS management console has failed. Please check the login credentials.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [2.0 (27/07/23 05:37:00)] was greater than or equal to the threshold (1.0) (mi ALARM transition).
- Timestamp: Thursday 27 July, 2023 05:42:06 UTC
- AWS Account: 237042273450
- Alarm Arn: arn:aws:cloudwatch:us-east-1:237042273450:alarm:Console Login Fail

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: