

AWS Security

Day 2 - Assignment

11th July 2023

Assignment 1

Enable CloudTrail and use CloudWatch to generate alert through SNS

Step 1 - Create a new CloudTrail Trail. Select a new S3 bucket in which the logs will be stored, allow cloudwatch logs to store the logs in log groups.

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.

RootUserAccess

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-237042273450-e4573353

Logs will be stored in aws-cloudtrail-logs-237042273450-e4573353/AWSLogs/237042273450

Log file SSE-KMS encryption [Info](#)

☐ Enabled

▼ **Additional settings**

Log file validation [Info](#)

☒ Enabled

SNS notification delivery [Info](#)

☐ Enabled

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

aws-cloudtrail-logs-237042273450-754d4402

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

► Policy document

▼ Policy document

JSON view

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream20141110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:ap-south-1:237042273450:log-group:aws-cloudtrail-logs-237042273450-754d4402:log-stream:237042273450_CloudTrail_ap-south-1*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:ap-south-1:237042273450:log-group:aws-cloudtrail-logs-237042273450-754d4402:log-stream:237042273450_CloudTrail_ap-south-1*"
      ]
    }
  ]
}
```

 Copy

Step 2 - Choose a log event. To log events for root user sign-in, select insight events.

Choose log events

Events [Info](#)
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

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.

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
Choose the activities you want to log.

☒ **Read**

☒ **Write**

☐ **Exclude AWS KMS events**

☐ **Exclude Amazon RDS Data API events**

Insights events [Info](#)
Identify unusual activity, errors, or user behavior in your account. [Additional charges apply](#)

Choose Insights types
Insights measure unusual activity against a seven-day baseline.

☒ **API call rate**
A measurement of write-only management API calls that occur per minute against a baseline API call volume.

☐ **API error rate**
A measurement of management API calls that result in error codes. The error is shown if the API call is unsuccessful.

Step 3 - We can see the S3 bucket is created for storing cloudtrail logs.

Amazon S3 > Buckets

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Total storage
Pending

Object count
Pending

Average object size
Pending

You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (3) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

Copy content

Empty

Delete

Create bucket

Name	AWS Region	Access	Creation date
<input type="radio"/> aws-cloudtrail-logs-237042273450-e4573353	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	July 11, 2023, 16:56:54 (UTC+05:30)
<input type="radio"/> accesstestbucket1	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	July 11, 2023, 11:59:33 (UTC+05:30)
<input type="radio"/> test-bucket-sk	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	July 11, 2023, 08:59:46 (UTC+05:30)

Step 4 - Create a metric filter in the cloudwatch log group for root user signin event.

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.

{ \$.userIdentity.type = "Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.e X

Test pattern

Select log data to test

Custom log data ▼

Log event messages

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

[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Running Start Crawl
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Classification complete
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Crawler configured with Scheduler
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Created table gluetest in database
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Finished writing to CloudTrail
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Crawler has finished

Test pattern

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

RootAccountUsage

Filter pattern

{ \$.userIdentity.type = "Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.event

Metric details

Metric namespace

Namespaces let you group similar metrics. [Learn more](#)

CloudTrailMetrics

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](#)

RootAccountUsageCount

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

Metric value

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

Review and create

Step 1: Pattern

Edit

Create filter pattern

Filter pattern

```
{ $.userIdentity.type = "Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent" }
```

Step 2: Metric

Edit

Assign metric

Filter name

RootAccountUsage

Metric name

RootAccountUsageCount

Metric namespace

CloudTrailMetrics

Metric value

1

Default value

-

Unit

-

Cancel

Previous

Create metric filter

Step 5 - Create a new alarm for the above metric filter.

Click on “Create alarm”.

Metric filters (1)

EditDeleteCreate alarmCreate metric filter

Find metric filters

<1>

RootAccountUsage

Filter pattern

{ \$.userIdentity.type = "Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent" }

Metric

CloudTrailMetrics / RootAccountUsageCount

Metric value

1

Default value

-

Define condition and threshold for the alarm.

Conditions

Threshold type

☒ **Static**
Use a value as a threshold

☐ **Anomaly detection**
Use a band as a threshold

Whenever `RootAccountUsageCount` is...
Define the alarm condition.

☐ **Greater**
> threshold

☒ **Greater/Equal**
≥ threshold

☐ **Lower/Equal**
≤ threshold

☐ **Lower**
< threshold

than...
Define the threshold value.

Must be a number

► **Additional configuration**

Cancel Next

Select “In Alarm” for state, and create a new SNS topic.

Configure actions

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.

Remove

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.

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.

user1@example.com, user2@example.com

Create topic

Add name and description

Name and description

Alarm name

RootUserUsage_SignIn

Alarm description - optional [View formatting guidelines](#)

EditPreview

This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

ⓘ 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

Next

Step 6 - Confirm the SNS subscription.

Amazon SNS > Subscriptions

Subscriptions (1)

EditDeleteRequest confirmationConfirm subscriptionCreate subscription

Q Search

< 1 > ⚙

ID	Endpoint	Status	Protocol	Topic
3466b6f5-be35-4042-8c...	skayarkar89@gmail.com	Confirmed	EMAIL	RootUser-signIn

< 1 >

Step 7 - Login to the root user.

Reset to default layout

Account ID: 2370-4227-3450

Account

Organization

Service Quotas

Billing Dashboard

Security credentials

Settings

Sign out

⋮

Welcome to AWS

🚀

Getting started with AWS

Learn the fundamentals and get the most out of your AWS account.

📄

Training and certification

Learn from AWS experts and gain new skills and knowledge.

💡

What's new with AWS?

Discover new AWS services, features, and Regions.

Step 8 - SNS will send notification alert to the specified email address.

ALARM: "RootUserUsage_SignIn" in Asia Pacific (Mumbai) Inbox x

AWS Notifications <no-reply@sns.amazonaws.com> 5:53 PM (6 minutes ago) ☆ ↶ ⋮
to me ▼

You are receiving this email because your Amazon CloudWatch Alarm "RootUserUsage_SignIn" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [6.0 (11/07/23 12:18:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 11 July, 2023 12:23:15 UTC".

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

Alarm Details:

- Name: RootUserUsage_SignIn
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [6.0 (11/07/23 12:18:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).

ALARM transition).

- Timestamp: Tuesday 11 July, 2023 12:23:15 UTC
- AWS Account: 237042273450
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:237042273450:alarm:RootUserUsage_SignIn

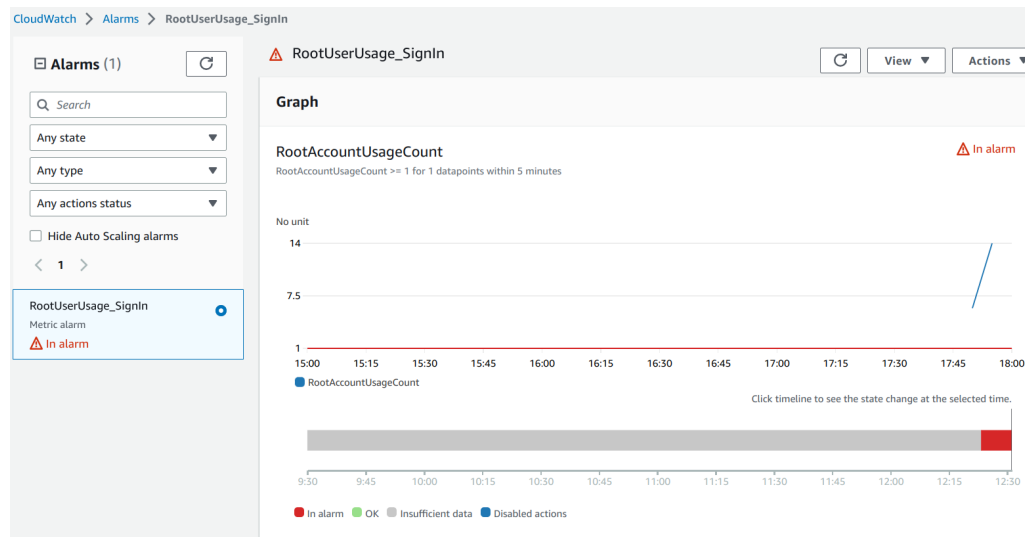
Threshold:

- 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: CloudTrailMetrics
- MetricName: RootAccountUsageCount
- Dimensions:
- Period: 300 seconds
- Statistic: Sum

CloudWatch shows the "In Alarm" state for the metric.



Assignment 2

Launch EC2 instance and configure CloudWatch agent on it to send metrics to cloudwatch.

Step 1 - Create an EC2 instance and attach an IAM role to it with “CloudWatchAgentServerPolicy” permission, which allows the instance to send metrics to cloudwatch.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

CW-instance-01

[Add additional tags](#)

▼ Instance type [Info](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0124 USD per Hour
On-Demand Windows pricing: 0.017 USD per Hour
On-Demand RHEL pricing: 0.0724 USD per Hour
On-Demand SUSE pricing: 0.0124 USD per Hour

☒ All generations

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

instancePEM

[Create new key pair](#)

▼

Advanced details

Info

Purchasing option

Info

☐ Request Spot Instances

Domain join directory

Info

Select

▼

↻

Create new directory

🔗

IAM instance profile

Info

CloudWatchAgentServerRole

▼

arn:aws:iam::237042273450:instance-profile/CloudWatchAgentServerRole

↻

Create new IAM profile

🔗

Hostname type

Info

IP name

▼

DNS Hostname

Info

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

Step 2 - Installing Cloudwatch agent in the EC2 instance.

```
[ec2-user@ip-172-31-8-217 ~]$ wget https://s3.amazonaws.com/amazoncloudwatch-agent/linux/amd64/latest/AmazonCloudWatchAgent.zip
--2023-07-11 15:42:42-- https://s3.amazonaws.com/amazoncloudwatch-agent/linux/amd64/latest/AmazonCloudWatchAgent.zip
Resolving s3.amazonaws.com (s3.amazonaws.com)... 52.216.208.104, 54.231.231.56, 52.217.133.176, ...
Connecting to s3.amazonaws.com (s3.amazonaws.com)[52.216.208.104]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 70431160 (67M) [application/zip]
Saving to: 'AmazonCloudWatchAgent.zip'

AmazonCloudWatchAgent.zip      100%[=====] 67.17M  8.28MB/s  in 9.6s
2023-07-11 15:42:53 (6.98 MB/s) - 'AmazonCloudWatchAgent.zip' saved [70431160/70431160]
```

```
[ec2-user@ip-172-31-8-217 ~]$ unzip AmazonCloudWatchAgent.zip
sudo ./install.sh
Archive: AmazonCloudWatchAgent.zip
  inflating: amazon-cloudwatch-agent.rpm
  inflating: amazon-cloudwatch-agent.deb
  inflating: manifest.json
  inflating: install.sh
  inflating: uninstall.sh
  inflating: detect-system.sh
create group cwagent, result: 0
create user cwagent, result: 0
```

Step 3 - It is required to create a cloudwatch agent configuration file, it is a JSON file that specifies the metrics and logs that the agent is to collect, including custom metrics.

Enter the following values in the cloudwatch agent configuration file wizard.

On which OS are you planning to use the agent?	Linux
Are you using EC2 or On-Premises hosts?	EC2
Which user are you planning to run the agent?	Others - ec2-user
Do you want to turn on the StatsD daemon?	No

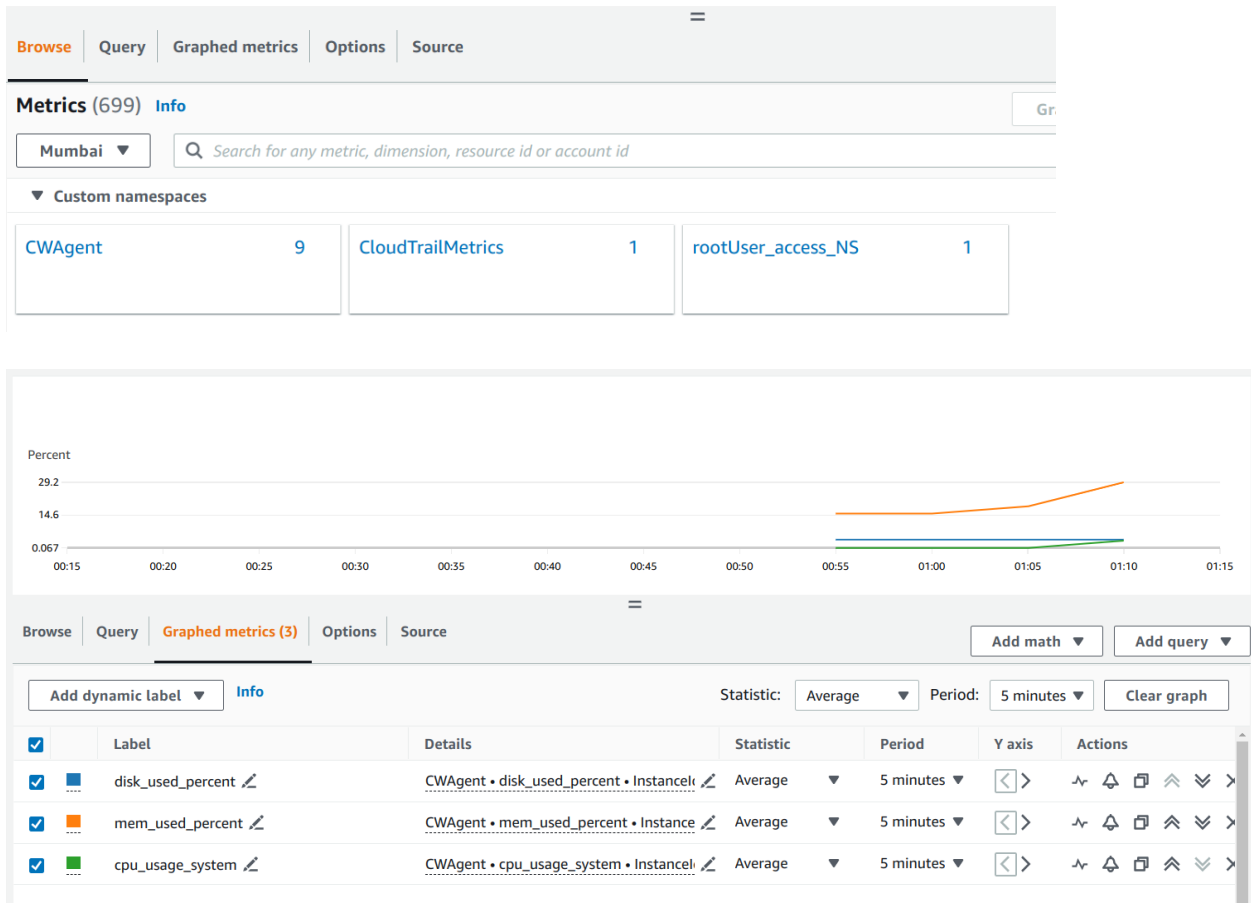
Do you want to monitor metrics from CollectD?	No
Do you want to monitor any host metrics?	Yes
Do you want to monitor cpu metrics per core?	Yes
Do you want to add ec2 dimensions?	Yes
Would you like to collect your metrics at high resolution?	60s
Which default metrics config do you want?	Standard
Are you satisfied with the above config?	Yes
Do you have any existing CloudWatch Log Agent?	No
Do you want to monitor any log files?	No
Do you want to store the config in the SSM parameter store?	No

```
[ec2-user@ip-172-31-8-217 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
=
= CloudWatch Agent allows you to collect metrics and logs from =
= your host and send them to CloudWatch. Additional CloudWatch =
= charges may apply.
=====
```

Step 4 - Start the cloudwatch agent after creating the configuration file.

```
[ec2-user@ip-172-31-8-217 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp -s
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2023/07/11 15:54:51 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2023/07/11 15:54:51 I! Valid Json input schema.
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
No csm configuration found.
No log configuration found.
Configuration validation first phase succeeded
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service → /etc/systemd/system/amazon-cloudwatch-agent.service.
```

Step 5 - Open custom namespace “CWAgent”



Assignment 3

Create an SNS topic and send email notification if metrics of EC2 crosses the 50% threshold.

Step 1 - Browse to the SNS console and create a new topic.

Create topic

Details

Type [Info](#)
Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

EC2_threshold

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional [Info](#)
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

My Topic

Maximum 100 characters.

Step 2 - Create a new subscription for the above topic.

[Subscriptions](#) | [Access policy](#) | [Data protection policy](#) | [Delivery policy \(HTTP/S\)](#) | [Delivery status logging](#) | [Encryption](#) | [Tags](#) | [>](#)

Subscriptions (0)

[Edit](#) | [Delete](#) | [Request confirmation](#) | [Confirm subscription](#) | [Create subscription](#)

ID | Endpoint | Status | Protocol

No subscriptions found
You don't have any subscriptions to this topic.
[Create subscription](#)

Details

Topic ARN

Protocol
The type of endpoint to subscribe



Email

Endpoint
An email address that can receive notifications from Amazon SNS.

skayarkar89@gmail.com

[After your subscription is created, you must confirm it. Info](#)

Step 3 - After creating a subscription, click on request confirmation for the subscription and confirm the email received or by copying the URL received in the confirm subscription field.

Subscriptions (1)			
<div><div>Search</div><div>< 1 > ⚙</div></div>			
ID	Endpoint	Status	Protocol
 Pending confirmation	skayarkar89@gmail.com	 Pending confirmation	EMAIL

Confirm subscription

Enter the subscription confirmation url.

898217d7bff336d7d6101d320a0cf7bf7ff1a7ef7&Endpoint=skayarkar89@gmail.com

Cancel

Confirm subscription

Step 4 - Launch an EC2 instance.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

CW_instance_01

Add additional tags

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.017 USD per Hour

On-Demand RHEL pricing: 0.0724 USD per Hour

On-Demand SUSE pricing: 0.0124 USD per Hour

Free tier eligible

▼

☐ All generations

[Compare instance types](#)

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

instancePEM ▼

Create new key pair

Instance summary for i-097a82b056571dfb0 (CW_instance_01) Info

Connect Instance state ▼ Actions ▼

Instance ID
i-097a82b056571dfb0 (CW_instance_01)

IPv6 address
-

Hostname type
IP name: ip-172-31-4-104.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Public IPv4 address
3.111.35.169 | [open address](#)

Instance state
⌚ Pending

Private IP DNS name (IPv4 only)
ip-172-31-4-104.ap-south-1.compute.internal

Instance type
t2.micro

Private IPv4 addresses
172.31.4.104

Public IPv4 DNS
ec2-3-111-35-169.ap-south-1.compute.amazonaws.com | [open address](#)

Elastic IP addresses
-

Step 5 - Create an alarm in Cloudwatch for the threshold required for the EC2 instance.

Specify metric and conditions

Metric

Graph
Preview of the metric or metric expression and the alarm threshold.

Select metric

Cancel

Next

Click on “EC2”.

▼ AWS namespaces			
ApiGateway11	CodeBuild28	DynamoDB17	EBS81
EC2153	Lambda36	Logs25	RDS96
S310	SNS6	Usage316	

Select the metric for CPU usage.

<input type="checkbox"/>	i-005b7ec2c5930dad3	NetworkPacketsOut
<input checked="" type="checkbox"/>	i-005b7ec2c5930dad3	CPUUtilization
<input type="checkbox"/>	i-005b7ec2c5930dad3	NetworkIn
<input type="checkbox"/>	i-005b7ec2c5930dad3	NetworkOut
<input type="checkbox"/>	i-005b7ec2c5930dad3	NetworkIn

Select threshold value and condition.

Metric Edit

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

50

25.3

0.598

08:00 09:00 10:00

CPUUtilization

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-005b7ec2c5930dad3

Instance name
task_instance_01

Statistic
Average

Period
5 minutes

Conditions

Threshold type

☒ **Static**
Use a value as a threshold

☐ **Anomaly detection**
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

☐ **Greater**
> threshold

☒ **Greater/Equal**
≥ threshold

☐ **Lower/Equal**
≤ threshold

☐ **Lower**
< threshold

than...
Define the threshold value.

50

Must be a number

Additional configuration

Cancel Next

Configure actions for the threshold. Select the SNS topic created in earlier steps.

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

Remove

☒ **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...

EC2_threshold

Only email lists for this account are available.

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

Add notification

Enter the name for the alarm and the message to be sent on Email.

Add name and description

Name and description

Alarm name

EC2_CPUUsage_50

Alarm description - optional [View formatting guidelines](#)

EditPreview

CPU utilization exceeded the threshold.
The CPU utilization of the EC2 instance exceeded the threshold of 50%.
Perform actions to to reduce the load on the EC2 instance.

Up to 1024 characters (169/1024)

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

CancelPreviousNext

Step 6 - Create an alarm for disk usage in the same way.

Preview and create

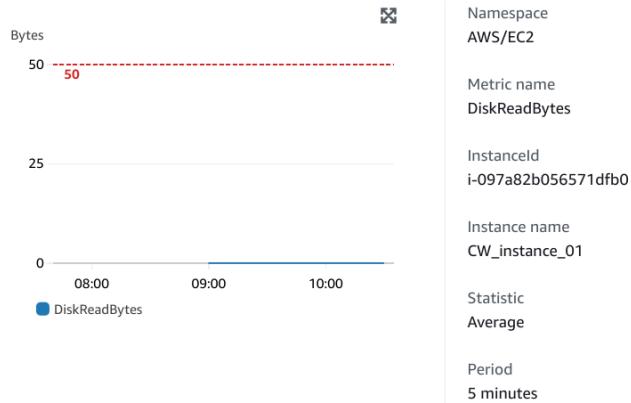
Step 1: Specify metric and conditions

[Edit](#)

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.



Conditions

Threshold type

Static

Whenever **DiskReadBytes** is
Greater/Equal (\geq)

than...
50

► Additional configuration

Step 2: Configure actions

[Edit](#)

Actions

Notification

When In alarm, send a notification to "EC2_threshold"

Step 3: Add name and description
Edit

Name and description

Name
EC2_DiskUsage_50

Description
Disk usage exceeded the threshold.
The disk usage of the EC2 instance exceeded the threshold of 50%.

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 7 - Alarms are in “OK” state initially.

Alarms (2)

☐ Hide Auto Scaling alarms
Clear selection
Refresh
Create composite alarm
Actions
Create alarm

Search
Any state
Any type
Any actions ...
1

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	EC2_DiskUsage_50	OK	2023-07-12 05:12:22	DiskReadBytes >= 50 for 1 datapoints within 5 minutes	Actions enabled
<input type="checkbox"/>	EC2_CPUUsage_50	OK	2023-07-12 05:08:13	CPUUtilization >= 50 for 1 datapoints within 5 minutes	Actions enabled

Step 5 - Run a stress workload on the EC2 instance to increase the CPU utilization and disk usage more than 50%.

```
[ec2-user@ip-172-31-4-104 ~]$ sudo stress --cpu 8 --vm-bytes $(awk '/MemAvailable/{printf "%d\n", $2 * 0.9;}'  
< /proc/meminfo)k --vm-keep -m 1  
stress: info: [28452] dispatching hogs: 8 cpu, 0 io, 1 vm, 0 hdd
```

Step 6 - Email notification received for CPU usage exceeding 50% of threshold.

ALARM: "EC2_CPUUsage_50" in Asia Pacific (Mumbai)
Inbox x

AWS Notifications
<no-reply@sns.amazonaws.com>
10:52AM (2 minutes ago)

to me

You are receiving this email because your Amazon CloudWatch Alarm "EC2_CPUUsage_50" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [65.40591831064185 (12/07/23 05:17:00)] was greater than or equal to the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 12 July, 2023 05:22:13 UTC".

View this alarm in the AWS Management Console:
https://ap-south-1-console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/EC2_CPUUsage_50

Alarm Details:

- Name: EC2_CPUUsage_50
- Description: CPU utilization exceeded the threshold.
The CPU utilization of the EC2 instance exceeded the threshold of 50%.
Perform actions to reduce the load on the EC2 instance.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [65.40591831064185 (12/07/23 05:17:00)] was greater than or equal to the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 12 July, 2023 05:22:13 UTC
- AWS Account: 237042273450
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:237042273450:alarm:EC2_CPUUsage_50

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	EC2_CPUUsage_50	In alarm	2023-07-12 05:22:13	CPUUtilization >= 50 for 1 datapoints within 5 minutes	Actions enabled

