



# Logging & Monitoring for Security

## Key Takeaways

# All rights reserved to nnSoftware GmbH

No part of this publication may be reproduced, copied, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of nnSoftware GmbH

# About TechWorld with Nana

TechWorld with Nana is an established name in the DevOps and Cloud industry, and it stands for the quality trainings helping 1,000s of engineers acquire the most in-demand skills in this field.



Our mission is enable individual engineers as well as companies to take advantage of the recent developments in Cloud and DevOps fields, to use technologies and concepts in order to create efficient, automated, streamlined DevSecOps processes in organisations.

# Why Logging & Monitoring?

- Despite all security measurements, there is **always a chance** that someone hacks into our systems

## Before Attack

- **Prevent by getting alerts** when seeing suspicious behavior in systems



We need to be **ready**, when there is an attempt to hack into

## After Attack

- **Analyze logs:** Understand what happened, and how the attack occurred to secure weak links in systems and complete proper incident analysis



**Incident Response:** We need to identify, contain, mitigate and recover from security incidents in a timely and efficient manner

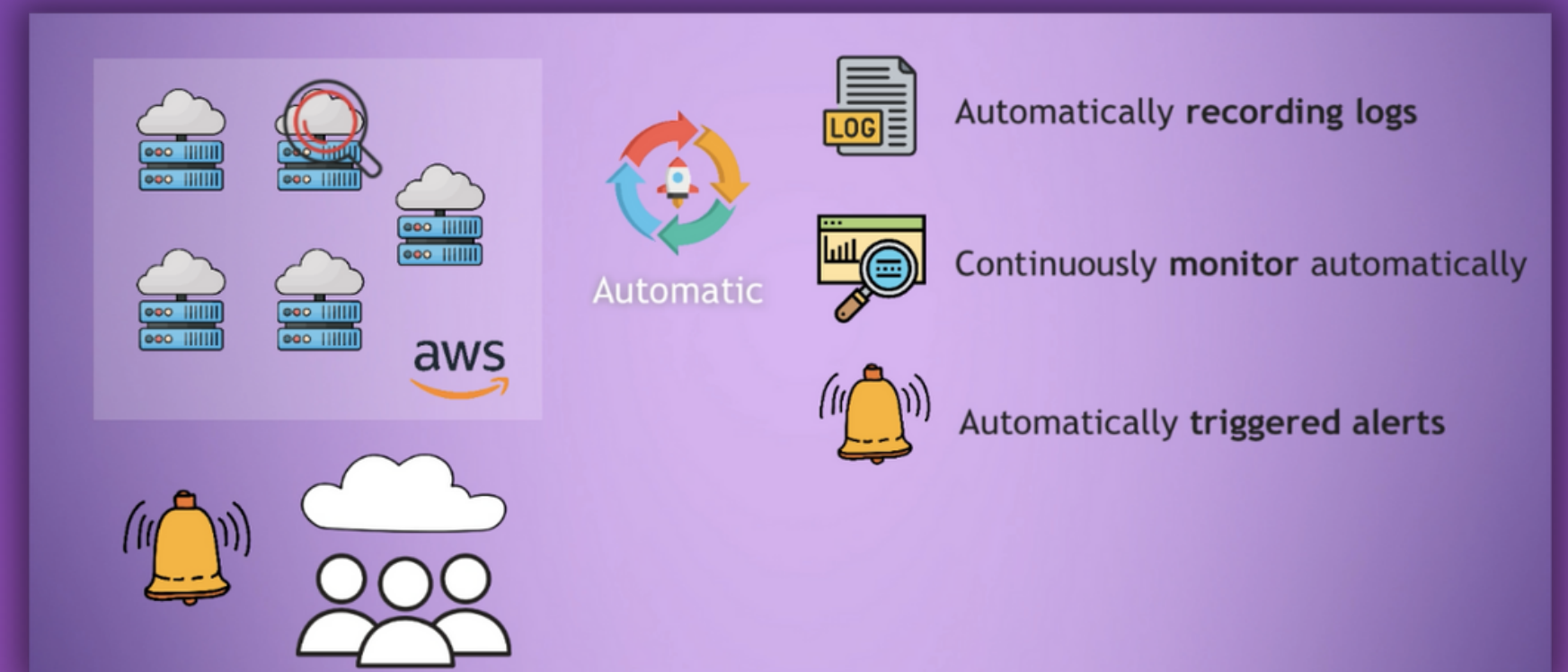


# Automated Logging & Monitoring

- 3 aspects of Logging and Monitoring



- Again, with DevOps we want to have this automated



# AWS CloudWatch and CloudTrail

# AWS CloudTrail & CloudWatch

- AWS has 2 services that help us to configure logging, monitoring and alerting in AWS cloud



Comprehensive monitoring and observability service that collects and tracks metrics, collects and monitors log files and sets alarms

AWS CloudWatch



Records API calls made on your AWS account, providing audit and security information

AWS CloudTrail

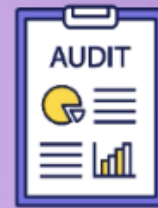
# What is AWS CloudTrail?

- Service that allows you to monitor and log activity in your AWS account

## Key features



Tracks user activity and **API usage** on AWS and in hybrid and multicloud environments



Immutably **store audit-worthy events** and easily generate audit reports



Monitors and **records account activity** across your AWS infrastructure



**Detect unusual API activity** with CloudTrail Insights



Trail signifies the **recorded history** or path of actions taken - CloudTrail creates a chronological record (or trail)



CloudTrail delivers events to Amazon S3 and CloudWatch Logs



# What is AWS CloudWatch?

- Monitoring and observability service that helps you collect and analyze data from various resources within your AWS infrastructure

## Key features



**Collects metrics and logs** from your resources, applications and services that run on AWS or on-premises servers



**Visualize** applications and infrastructure with dashboards, troubleshoot with correlated logs and metrics and **set alerts**



## Automated Alerts



Based on metrics, you can configure **automated actions**



Get alert, whenever EC2 instance crashes



Get alert, whenever 5 failed login attempts happen



# Event History

- CloudTrail provides an Event History for the **most recent events** in an AWS region

CloudTrail is enabled by default for your AWS account

The Event history provides a viewable, searchable, downloadable and immutable record of the past 90 days of management events in an AWS region

- Filter events

- See detailed log entry

Event history (50+) Info

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

Lookup attributes

User name: gitlab

Filter by date and time

Event name	Event time	User name	Event source
GetCommandInvocation	August 03, 2023, 13:14:50 (UTC...)	gitlab	ssm.amazonaws.com
BatchGetImage	August 03, 2023, 13:14:36 (UTC...)	gitlab	ecr.amazonaws.com
GetAuthorizationToken	August 03, 2023, 13:14:35 (UTC...)	gitlab	ecr.amazonaws.com
SendCommand	August 03, 2023, 13:14:34 (UTC...)	gitlab	ssm.amazonaws.com
BatchGetImage	August 03, 2023, 13:12:50 (UTC...)	gitlab	ecr.amazonaws.com

```
}  
,  
"eventTime": "2023-08-04T12:37:32Z",  
"eventSource": "ssm.amazonaws.com",  
"eventName": "UpdateInstanceInformation",  
"awsRegion": "eu-west-3",  
"sourceIPAddress": "15.237.26.72",  
"userAgent": "aws-sdk-go/1.44.78 (go1.18.3; linux; amd64) amazon-ssm-agent/",  
"requestParameters": {  
  "instanceId": "i-0910b120c81a9eead",  
  "agentVersion": "3.1.1927.0",  
  "agentStatus": "Active",  
  "platformType": "Linux",  
  "platformName": "Ubuntu",  
  "platformVersion": "22.04",  
  "ipAddress": "10.0.101.177",  
  "computerName": "ip-10-0-101-177.eu-west-3.compute.internal",  
  "agentName": "amazon-ssm-agent",  
  "availabilityZone": "eu-west-3a",  
}
```

# Event History Limitations



Limited to recent activity



Captures only management events

## Different Events

### Management Events

- Information about management operations that are performed on resources

### Data Events

- Information about the resource operations performed on or in a resource

### Insight Events

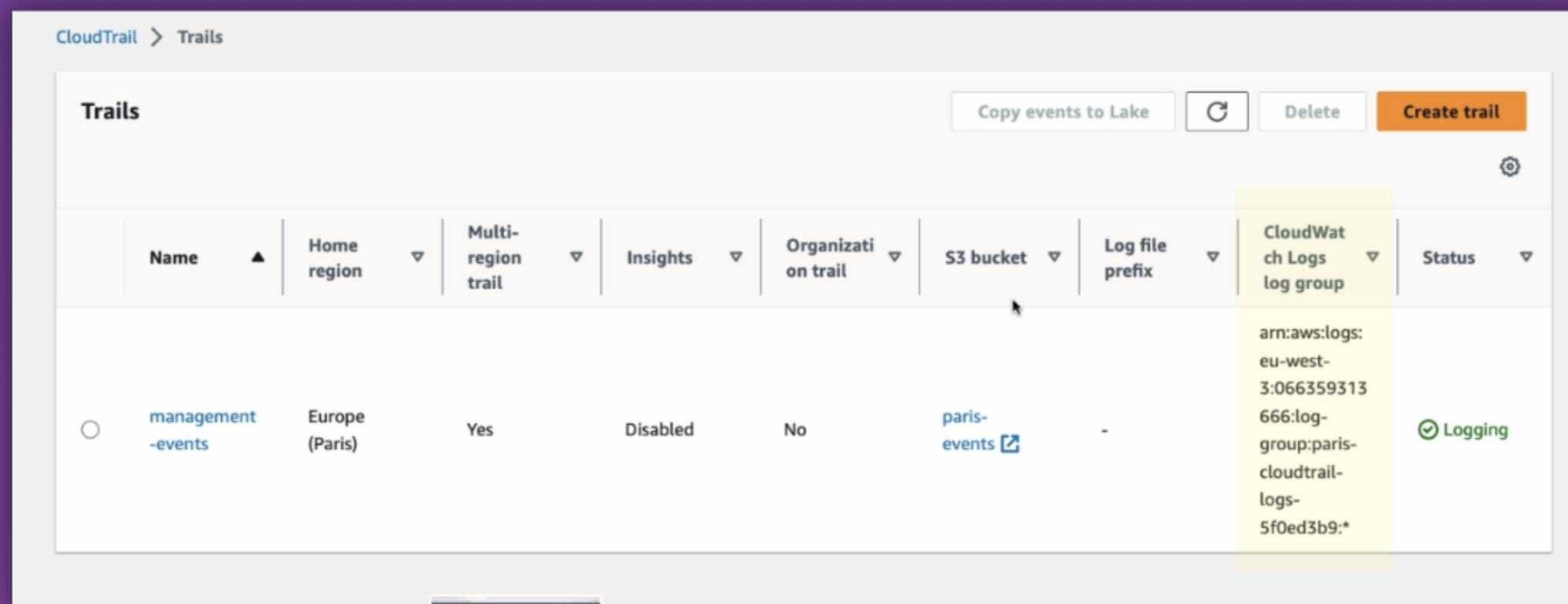
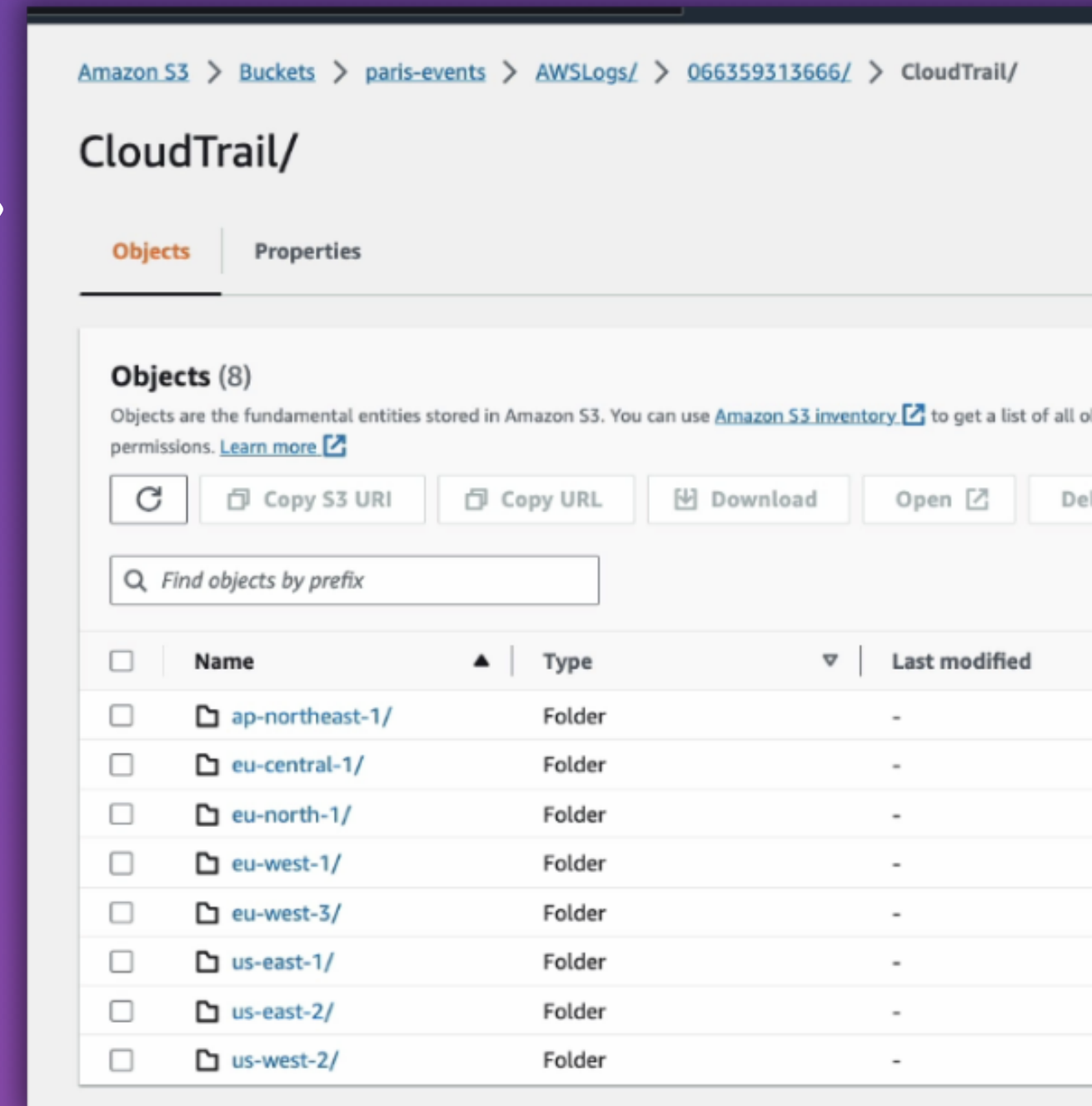
- Capture unusual API call rate or error rate activity analyzing CloudTrail management activity



# Multi-region CloudTrail

- Multi-Region enabled by default - saves event logs from all regions
- **Home region of trail**, where the trail can be configured viewed and deleted
- Forward logs to S3 bucket storage for persistence
- Forward logs to CloudWatch for automated alarm configuration

S3 bucket with event logs of different regions



# CloudWatch Log Group

- **Log Stream** = Sequence of log events that share the same source. Each separate source of logs in CloudWatch logs makes up a separate log stream
- **Log Group** = A group of log streams that share the same retention, monitoring and access control settings

The screenshot displays the AWS CloudWatch console interface. On the left is a navigation sidebar with sections like 'Favorites and recents', 'Dashboards', 'Alarms', 'Logs', 'Metrics', 'X-Ray traces', 'Events', and 'Application monitoring'. The 'Logs' section is expanded, showing 'Log groups' as the selected option. The main content area shows the details for a specific log group: 'paris-cloudtrail-logs-5f0ed3b9'. At the top of this section are buttons for 'Actions', 'View in Logs Insights', and 'Start tailing'. Below this is a 'Log group details' section. Further down, there are tabs for 'Log streams', 'Tags', 'Metric filters', and 'Subscription filters'. The 'Log streams' tab is active, showing a list of four log streams, each with a checkbox and a link to its details. The first stream is '066359313666\_CloudTrail\_eu-west-3\_3'. An overlay window titled 'Log events' is positioned in front of the main console. This window shows a search bar with the filter '\$.awsRegion = "ca-central-1"', a 'Start tailing' button, and a 'Create metric filter' button. Below these is a table of log events with columns for 'Timestamp', 'Message', and 'Log stream name'. The table contains several rows of log data, all from the '066359313666\_CloudTrail\_eu-west-3\_3' stream.

CloudWatch > Log groups > paris-cloudtrail-logs-5f0ed3b9

paris-cloudtrail-logs-5f0ed3b9

Actions View in Logs Insights Start tailing

Log group details

Log streams (4)

Filter log streams or try prefix search

Log stream
<input type="checkbox"/> 066359313666_CloudTrail_eu-west-3_3
<input type="checkbox"/> 066359313666_CloudTrail_eu-west-3
<input type="checkbox"/> 066359313666_CloudTrail_eu-west-3_4
<input type="checkbox"/> 066359313666_CloudTrail_eu-west-3_2

CloudWatch > Log groups > paris-cloudtrail-logs-5f0ed3b9 > All events

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

Q {\$.awsRegion = "ca-central-1"} Clear 1m 30m 1h 12h Custom Local Display

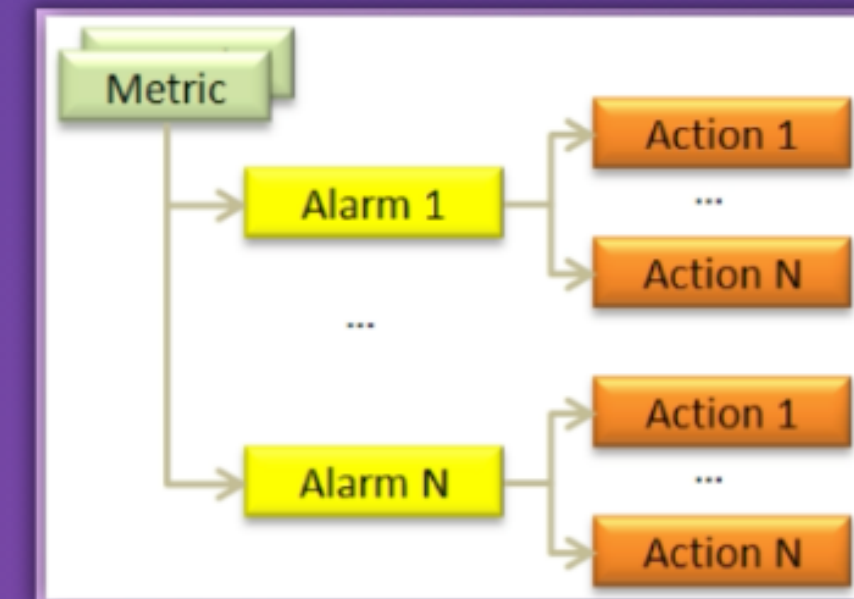
Timestamp	Message	Log stream name
2023-09-19T18:28:00.582+02:00	{"eventVersion":"1.08","userIdentity":{"accountId":"066359313666","invokedBy":"ec...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.582+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.582+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...
2023-09-19T18:28:00.645+02:00	{"eventVersion":"1.08","userIdentity":{"type":"Root","principalId":"066359313666"...	066359313666_CloudTrail_eu...



# Configure Alarms

# CloudWatch Alarms

- Used to **monitor and respond to specific conditions or thresholds** in your AWS resources or applications
- When the conditions specified in the alarm are met, CloudWatch can automatically take actions or send notifications to alert you about the situation



## Metrics

- Metrics are data about the performance of your systems
- There are resource and application metrics
- It's a time-ordered set of data points that represent the values of a resource over time
- For example, you can create a metric to track CPU utilization of an EC2 instance



## Alarms

- Alarms allow you to watch CloudWatch metrics and to receive notifications when the metrics fall outside of the configured thresholds

# Configure CloudWatch Alarms

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

### Specify metric and conditions

**Metric**

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

Select metric

Cancel Next


CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create



**Metrics** = Sequence of log events that share the same source. Each separate source of logs in CloudWatch logs makes up a separate log stream

Browse Query | Graphed metrics | Options | Source

Add math ▼ Add query ▼

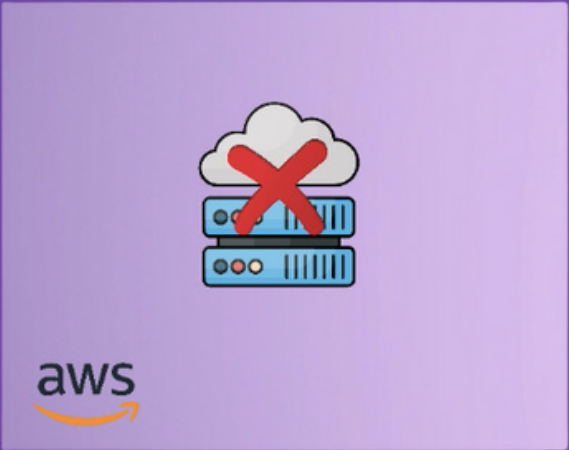
Metrics (422)

Graph with SQL Graph search

Search for any metric, dimension, resource id or account id

EBS	50	EC2	110	ECR	1	Events	5
Logs	14	NATGateway	84	S3	2	SSM Run Command	3
Usage	153						

# EC2 Alarm Example



Alarm when EC2 Instance is down

CloudWatch > Alarms

Alarms (1) ☐ Hide Auto Scaling alarms

Any state Any type Any actions ... < 1 >

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	EC2 Instance Down	OK	2023-08-09 08:07:40	StatusCheckFailed_Instance > 0 for 1 datapoints within 5 minutes	Actions enabled

- No alarm - within threshold

- Alarm triggered by bringing down EC2 instance

Instances (1/1) [Info](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input checked="" type="checkbox"/>	app-server	i-041c76ab746aa81ca	Running	t2.micro	1/2 checks passed	1/1 in al +	eu-west-3c

Alarms (1) ☐ Hide Auto Scaling alarms

Any state Any type Any actions ... < 1 >

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	EC2 Instance Down	In alarm	2023-08-09 08:22:40	StatusCheckFailed_Instance > 0 for 1 datapoints within 5 minutes	Actions enabled

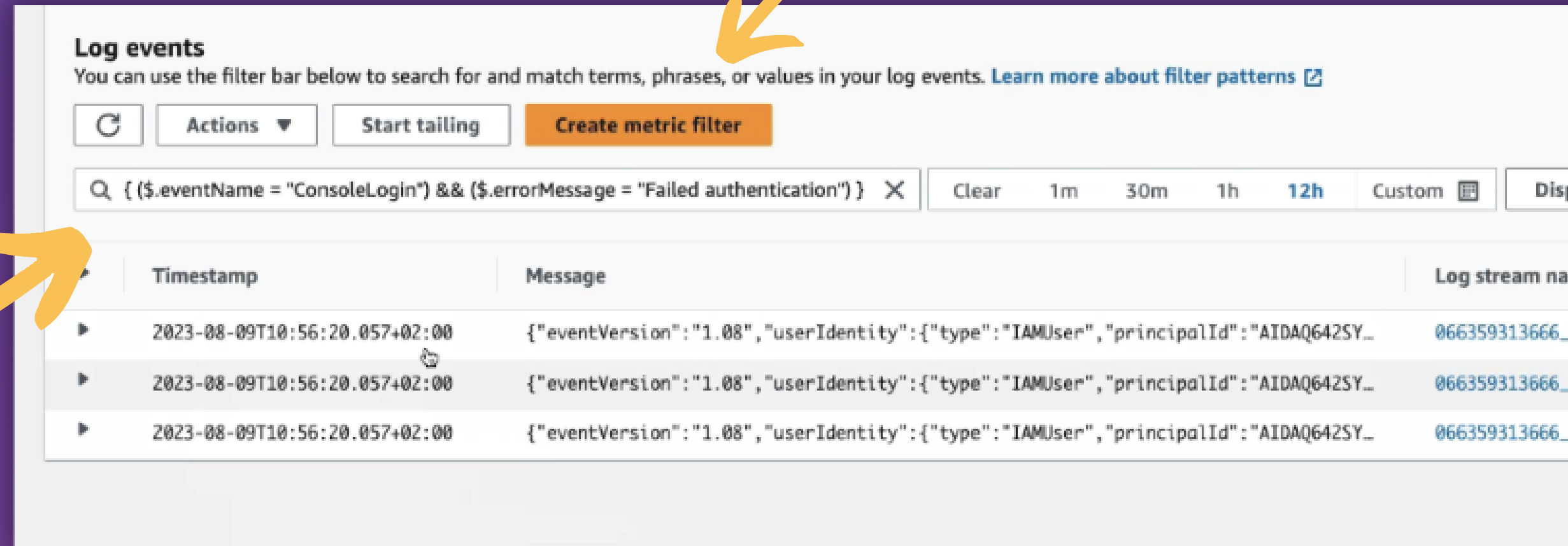
- In alarm state



# Custom Metrics Filter

- Instead of using existing metrics, we can create own custom metrics

- Filter pattern to filter specific logs and create metric filter from it



**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**

🔍 { (\$.eventName = "ConsoleLogin") && (\$.errorMessage = "Failed authentication") } ✕ Clear 1m 30m 1h **12h** Custom ⌵ Dis

	Timestamp	Message	Log stream na
▶	2023-08-09T10:56:20.057+02:00	{"eventVersion":"1.08","userIdentity":{"type":"IAMUser","principalId":"AIDAQ642SY...	066359313666_
▶	2023-08-09T10:56:20.057+02:00	{"eventVersion":"1.08","userIdentity":{"type":"IAMUser","principalId":"AIDAQ642SY...	066359313666_
▶	2023-08-09T10:56:20.057+02:00	{"eventVersion":"1.08","userIdentity":{"type":"IAMUser","principalId":"AIDAQ642SY...	066359313666_



Define the terms and patterns to look for in log data as it is sent to CloudWatch Logs

CloudWatch Logs uses these metric filters to turn log data into numerical CloudWatch metrics that you can set an alarm on



# Custom Metrics Filter for Failed Login Attempts

Create a metrics filter for failed logins

Metrics filter created

### Create metric filter

Filter name

Filter pattern

Metric namespace

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

Namespaces can be up to 255 characters long; all characters are lowercase and no spaces.

Metric name

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

Metric name can be up to 255 characters long; all characters are lowercase and no spaces.

Metric value

Metric value is the value published to the metric name when a log event matches the filter pattern.

Valid metric values are: floating point number (1, 99.9, etc.), named field identifiers (e.g. \$requestSize for delimited filter pattern - dollar (\$) or dollar dot (\$) followed by alphanumeric characters).

CloudWatch

Favorites and recents

Dashboards

Alarms 0 0 0 0

In alarm

All alarms

Billing

Logs

Log groups

Logs Insights New

Live Tail New

Metrics

All metrics

Explorer

Streams

X-Ray traces

Log streams

Tags

Metric filters

Subscription filters

Metric filters (1)

Find metric filters

FailedLogin

Filter pattern

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

Metric

Login / FailedLogin

Metric value

1

Default value

-

Unit

Count

Dimensions

-

CloudWatch

Favorites and recents

Dashboards

Alarms 0 0 0 0

In alarm

All alarms

Logs

Log groups

Live Tail

Logs Insights

Metrics

All metrics

Explorer

Streams

X-Ray traces

Events

CloudWatch > Metrics

Untitled graph

1

0.5

0

05:15 05:30 05:45

Browse Query Graphed metrics Options

Metrics (95) Info

Paris

Search for any metric, dimension, or namespace

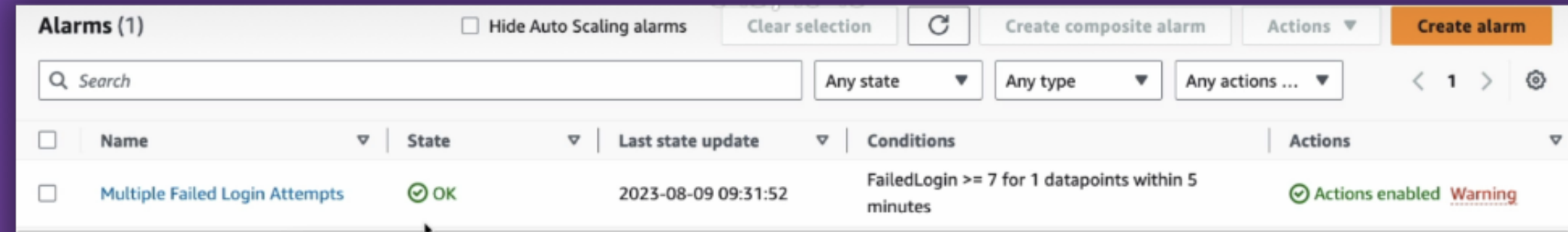
Custom namespaces

Login 1

AWS namespaces

# Alarm for Failed Login Attempts

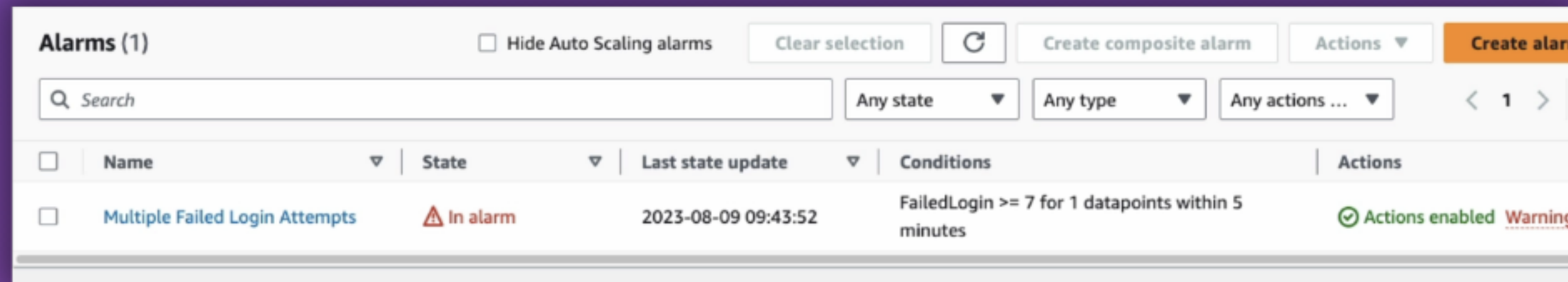
- No alarm - within threshold



This screenshot shows the AWS Alarms console with one alarm, 'Multiple Failed Login Attempts', in the 'OK' state. The alarm is configured with the condition 'FailedLogin >= 7 for 1 datapoints within 5 minutes' and has actions enabled. The last state update was on 2023-08-09 at 09:31:52.

Name	State	Last state update	Conditions	Actions
Multiple Failed Login Attempts	OK	2023-08-09 09:31:52	FailedLogin >= 7 for 1 datapoints within 5 minutes	Actions enabled Warning

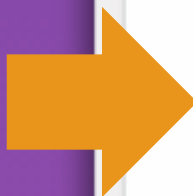
- Trigger alarm by simulating failed login attempts



This screenshot shows the same AWS Alarms console, but the 'Multiple Failed Login Attempts' alarm is now in the 'In alarm' state. The last state update was on 2023-08-09 at 09:43:52.

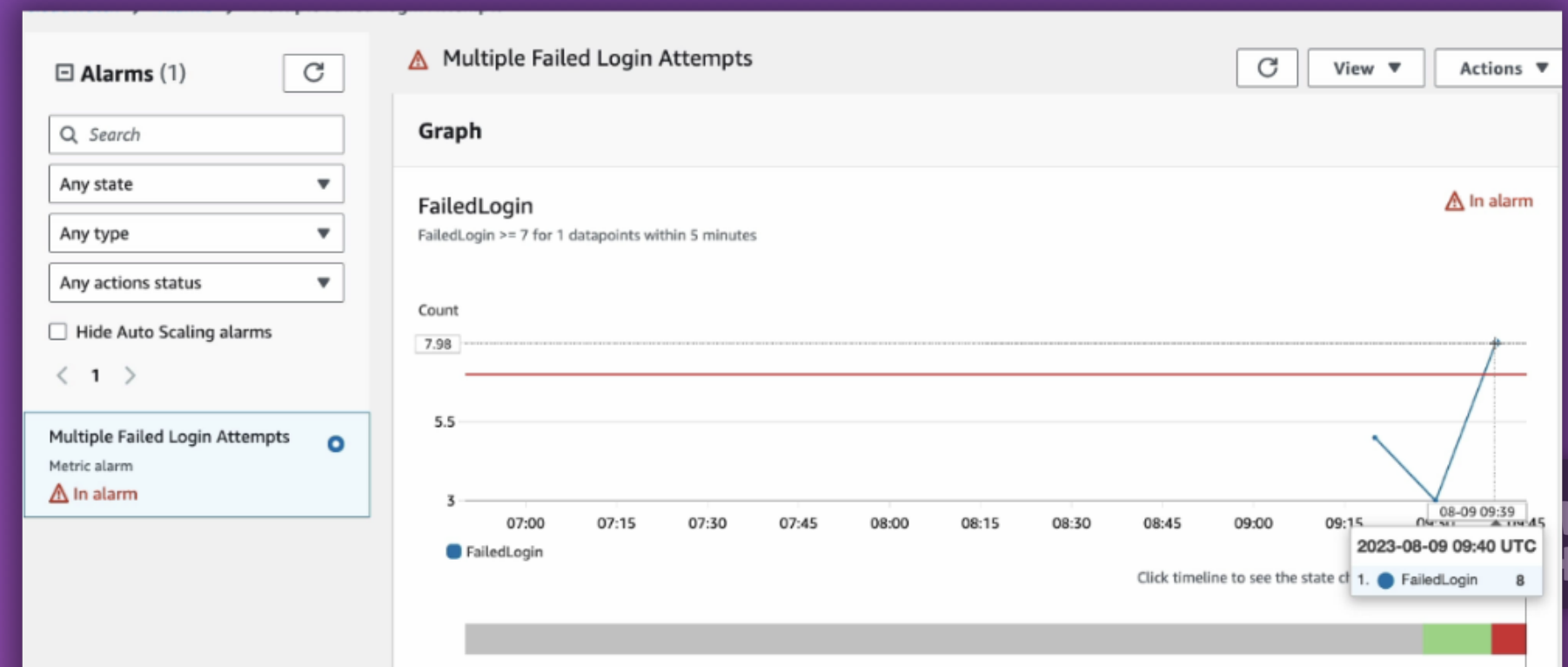
Name	State	Last state update	Conditions	Actions
Multiple Failed Login Attempts	In alarm	2023-08-09 09:43:52	FailedLogin >= 7 for 1 datapoints within 5 minutes	Actions enabled Warning

- Failed login event log

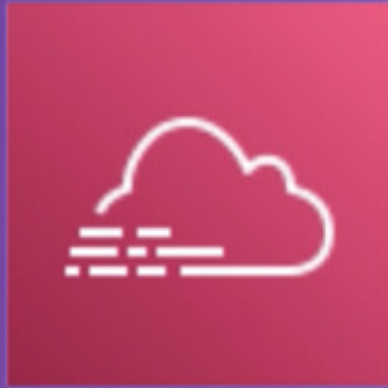


```
{
  "eventTime": "2023-08-04T14:07:20Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "eu-north-1",
  "sourceIPAddress": "213.143.108.155",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
Chrome/115.0.0.0 Safari/537.36",
  "errorMessage": "Failed authentication",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
```

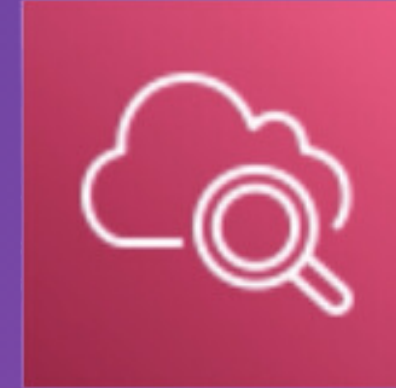
- Alarm detail view



# Wrap Up



CloudTrail



CloudWatch



✓ Visibility

✓ Forensics and Troubleshooting

✓ Powerful log management & analysis capabilities

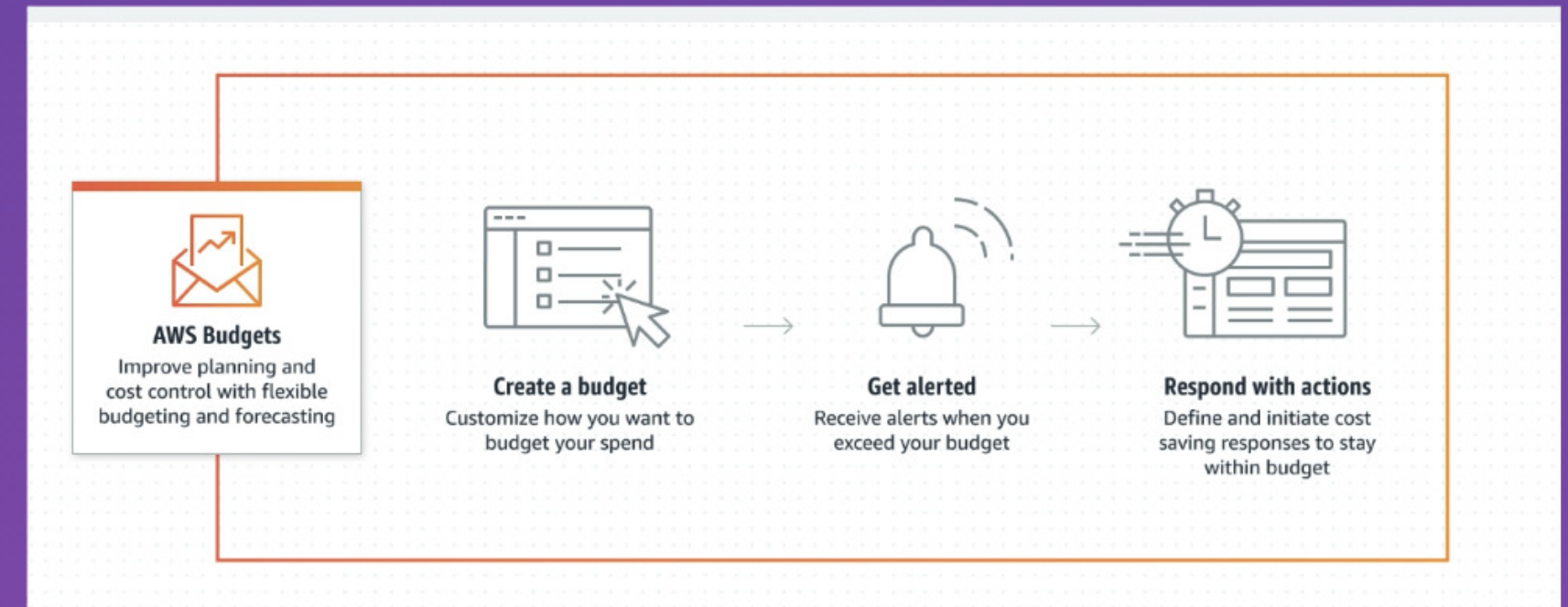
✓ Proactive Issue Detection



# AWS Budgets

## What is AWS Budgets?

- With AWS Budgets service you can set custom budgets to track your cost and usage
- Get alerted if budget exceeds certain threshold



## Why it's useful

- AWS cloud is a paid platform
- We might forget to delete resources or don't know about a service that was created in the background
- So it's useful to set a limit to be aware of the costs and be able to take actions



# AWS Budgets

You can set up a monthly cost budget

AWS Billing > Budgets > Budget details 11.08 - 2023.09.23 - aws budgets.mp4 (speed 1.5x)

## My Monthly Cost Budget [Info](#)

[Delete](#) [Edit](#)

### Budget health [Info](#)

Current vs. budgeted	Forecasted vs budgeted (MTD)
<div><div></div></div> 26.11%	<div><div></div></div> 0.00%
Amount spent: \$10.45 of \$40.00	Amount spent: - of \$40.00

### Alerts [Info](#)

Thresholds

✓ OK

Actions

-

AWS Billing > Budgets > Overview

## Overview [Info](#)

[Download CSV](#) [Actions](#) [Create budget](#)

[Show all budgets](#) < 1 > ⚙

<input type="checkbox"/>	Name	Thresholds	Budget	Amount used	Forecasted ...	Current vs. budgeted
<input type="checkbox"/>	My Monthly Cost Budget	✓ OK	\$40.00	\$10.45	-	<div><div></div></div> 26.11%