

## ICT & Infra S3 Monitoring & Supporting Services week 5.2

Class:	CB01
Student number:	4961854
Student name:	Heiko Morales

### Introduction

in this practice I am going to learn how to monitor CloudTrail logs in amazon CloudWatch. because, with CloudWatch, you can visualize and explore your CloudTrail logs, analyse time-series log data, and create metric filters for the data.

### Assignment. Create a step function

first, we will go to CloudTrail and fill in the form.

#### Choose trail attributes

**General details**

**Trail name**  
Enter a display name for your trail.  
  
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.  
  
Logs will be stored in aws-cloudtrail-logs-231606114051-3fc89a15/AWSLogs/231606114051

#### CloudWatch Logs - optional

You can enable SNS notifications in CloudWatch Logs for specific API actions. Standard CloudWatch and CloudWatch Logs charges apply.

##### CloudWatch Logs Info

☒ Enabled

##### Log group Info

☒ New  
☐ Existing

##### Log file SSE-KMS encryption Info

☒ Enabled

##### AWS KMS Key

☒ New  
☐ Existing

##### AWS KMS alias

KMS key and S3 bucket must be in the same region.

► Additional settings

Log group [Info](#)

☒ New  
☐ Existing

Log group name

aws-cloudtrail-logs-231606114051-5472f207

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

IAM Role [Info](#)

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

☒ New  
☐ Existing

Role name

CloudTrailRoleForCloudWatchLogs\_SampleTrail

*in the next section we will choose what we want to monitor.*

## 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.

<input checked="" type="checkbox"/> Management events	<input checked="" type="checkbox"/> Data events	<input checked="" type="checkbox"/> Insights events
Capture management operations performed on your AWS resources.	Log the resource operations performed on or within a resource.	Identify unusual activity, errors, or user behavior in your account.

Data events [Info](#)

[Additional charges apply](#) Data events show information about the resource operations performed on or within a resource.

Data event: S3 [Info](#) Remove

Data event source

Select source of data events to log

S3

S3 bucket

You can choose to log read and/or write events for all buckets. You can also choose individual buckets.

All current and future S3 buckets ☒ Read ☒ Write

Individual bucket selection

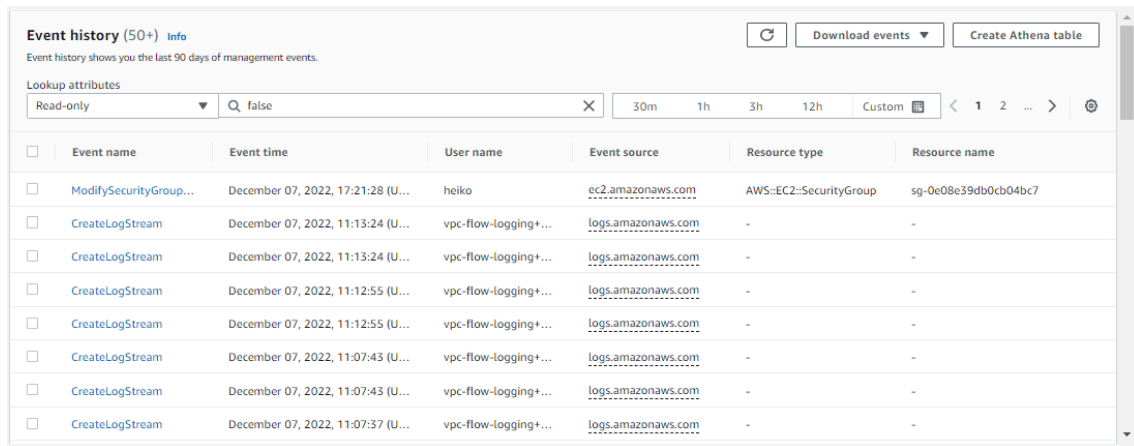
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

Browse ☒ Read ☒ Write ×

Add bucket

Add data event type

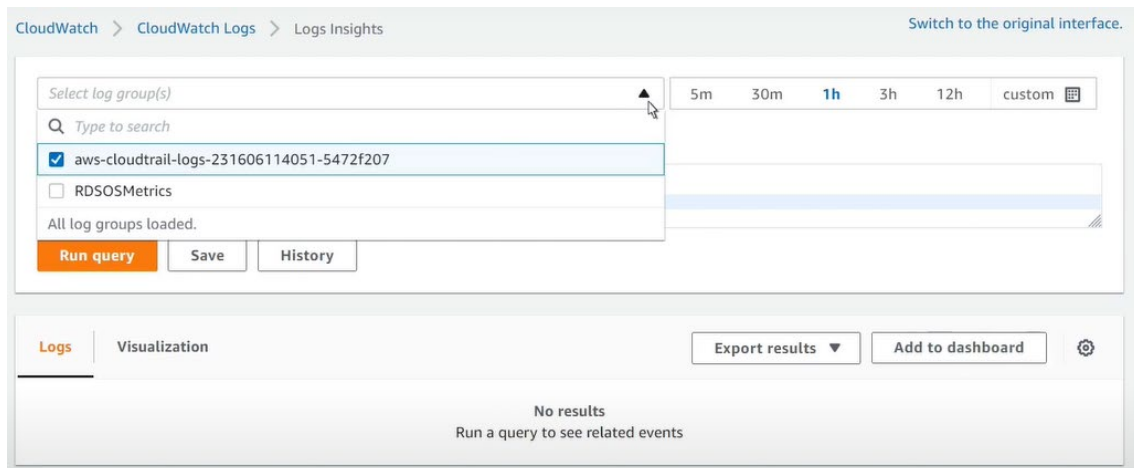
once created we can see after a while that we start to receive logs.



The screenshot shows the AWS Event History console. At the top, it says "Event history (50+) Info" and "Event history shows you the last 90 days of management events." Below this is a "Lookup attributes" section with a dropdown set to "Read-only" and a search bar containing "false". To the right of the search bar are filters for "30m", "1h", "3h", "12h", and "Custom". Below the filters is a table with the following columns: "Event name", "Event time", "User name", "Event source", "Resource type", and "Resource name". The table contains several rows of events, including "ModifySecurityGroup...", "CreateLogStream", and "CreateLogStream".

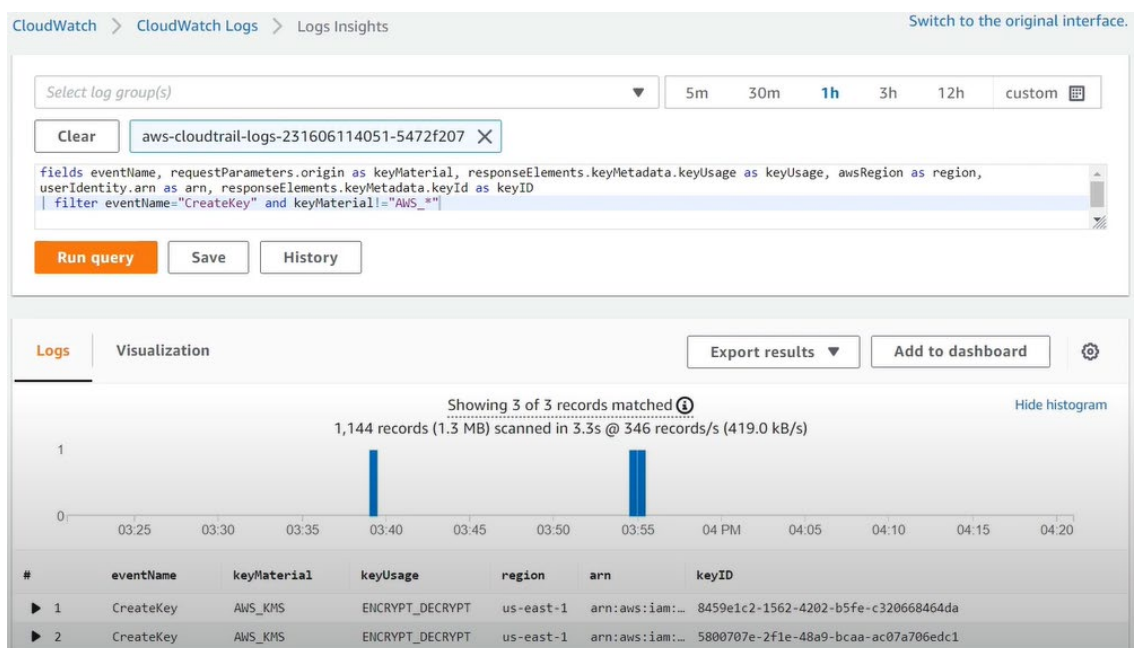
Event name	Event time	User name	Event source	Resource type	Resource name
ModifySecurityGroup...	December 07, 2022, 17:21:28 (U...	heiko	ec2.amazonaws.com	AWS::EC2::SecurityGroup	sg-0e08e39db0cb04bc7
CreateLogStream	December 07, 2022, 11:13:24 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:13:24 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:12:55 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:12:55 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:07:43 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:07:43 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-
CreateLogStream	December 07, 2022, 11:07:37 (U...	vpc-flow-logging+...	logs.amazonaws.com	-	-

Next, we go to cloudwatch logs and in insights we select our already created cloudtrail.



The screenshot shows the AWS CloudWatch Logs Insights console. At the top, it says "CloudWatch > CloudWatch Logs > Logs Insights" and "Switch to the original interface." Below this is a "Select log group(s)" dropdown menu with a search bar. The dropdown menu is open, showing a list of log groups. The first log group, "aws-cloudtrail-logs-231606114051-5472f207", is selected. Below the dropdown menu are buttons for "Run query", "Save", and "History". To the right of the dropdown menu are filters for "5m", "30m", "1h", "3h", "12h", and "custom". Below the filters is a table with the following columns: "Log group", "Log stream", and "Log event". The table is empty, and the message "No results" is displayed. Below the table are buttons for "Export results" and "Add to dashboard".

at this point we can now filter the logs we are receiving



We can also add this new log filtering to a dashboard for better visualisation.

Add to dashboard

1. Select a dashboard

Select an existing dashboard or create a new one.

Select dashboard

Create new

2. Select a widget type

Use line charts for trends, stacked areas to compare parts of a whole, and numbers to monitor the latest value and the alarm status to display instantly the status of the alarm in the dashboard.

Line

Stacked area

Bar

Logs table

3. Customize the widget title

Widgets get an automatic title. You can optionally customize the title here.

Log group: aws-cloudtrail-logs-23160611405

Preview

This is how your chart will appear in your dashboard.

Log group: aws-cloudtrail-logs-231606114051-5...

#	eventName	keyMaterial	keyUsage	r
1	CreateKey	AWS_KMS	ENCRYPT_DECRYPT	us
2	CreateKey	AWS_KMS	ENCRYPT_DECRYPT	us
3	CreateKey	AWS_KMS	ENCRYPT_DECRYPT	us

KMS Key Creation

Time	Count
17:00	1.0
17:05	0.0
17:10	0.0
17:15	0.0
17:20	0.0
17:25	2.0
17:30	1.6
17:35	0.8
17:40	0.4
17:45	0.0
17:50	0.0
17:55	1.2