

ICT & Infra S3 S/NO week 16: Capturing and analysing logs with different AWS native tools

Date: Sep 2020
Version 1.0

Class: CB01

Student numbers: 4961854

Student names: Heiko Morales

Introduction

S/NO: Following these exercises you will learn how to:

- Capture events with CloudTrail and store them in CloudWatch
- Viewing logs in CloudWatch
- Creating alerts with CloudWatch Alarms
- Searching Logs with Athena

How to deliver your assignments?

Fill in this document with required information. Answer questions and upload the document to Canvas at most one week after the assignment is given.

Assignment: Demonstrate security controls in your case-study project

- Brainstorm together with your case-study fellow students about what kind of CloudTrail events in AWS you are going to capture. Think about the management or data events, relevant for your case-study security controls, security incident and/or problem managements analysis?
- Provide the analysis of these events either using CloudWatch or Athena tools.
- Think about alarms, notifications you can set up based on certain conditions, CloudWatch metrics.
- Think about if you can deploy Lambda functions from these alarms/notifications generated (e.g. automatic processing of the events).
- Bonus: How can you generate alarms/notifications from the results returned by Athena?

Provide screenshots and descriptions of the steps above

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

The screenshot shows the 'Choose trail attributes' form in the AWS CloudTrail console. The form is titled 'Choose trail attributes' and has a 'General details' section. In the 'Trail name' field, 'SampleTrail' is entered. Below this, there is a checkbox for 'Enable for all accounts in my organization'. The 'Storage location' section has two options: 'Create new S3 bucket' (selected) and 'Use existing S3 bucket'. The 'Trail log bucket and folder' field contains the text 'aws-cloudtrail-logs-231606114051-3fc89a15'. At the bottom, a note states: 'Logs will be stored in aws-cloudtrail-logs-231606114051-3fc89a15/AWSLogs/231606114051'.

Choose trail attributes

General details

Trail name
Enter a display name for your trail.
SampleTrail
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-231606114051-3fc89a15

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

MyKMSKey|

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.

☒ 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.

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.

Event history (50+) [Info](#)
Download events Create Athena table

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

Lookup attributes
Read-only × 30m 1h 3h 12h Custom < 1 2 ... > ⊞

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

CloudWatch > CloudWatch Logs > Logs Insights Switch to the original interface.

Select log group(s) 5m 30m **1h** 3h 12h custom

Type to search

- ☒ aws-cloudtrail-logs-231606114051-5472f207
- ☐ RDSOSMetrics

All log groups loaded.

Run query Save History

Logs Visualization Export results Add to dashboard

No results
Run a query to see related events

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

CloudWatch > CloudWatch Logs > Logs Insights Switch to the original interface.

Select log group(s) 5m 30m **1h** 3h 12h custom

Clear aws-cloudtrail-logs-231606114051-5472f207 **X**

```
fields eventName, requestParameters.origin as keyMaterial, responseElements.keyMetadata.keyUsage as keyUsage, awsRegion as region,
userIdentity.arn as arn, responseElements.keyMetadata.keyId as keyID
| filter eventName="CreateKey" and keyMaterial!="AWS_*
```

Run query Save History

Logs Visualization Export results Add to dashboard

Showing 3 of 3 records matched ⓘ
1,144 records (1.3 MB) scanned in 3.3s @ 346 records/s (419.0 kB/s) Hide histogram

#	eventName	keyMaterial	keyUsage	region	arn	keyID
1	CreateKey	AWS_KMS	ENCRYPT_DECRYPT	us-east-1	arn:aws:iam:...	8459e1c2-1562-4202-b5fe-c320668464da
2	CreateKey	AWS_KMS	ENCRYPT_DECRYPT	us-east-1	arn:aws:iam:...	5800707e-2f1e-48a9-bcaa-ac07a706edc1

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.

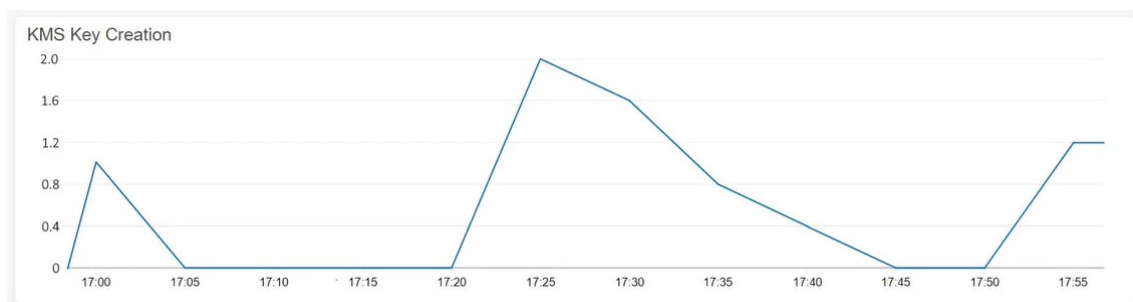
Log group: aws-cloudtrail-logs-23160611405

Preview

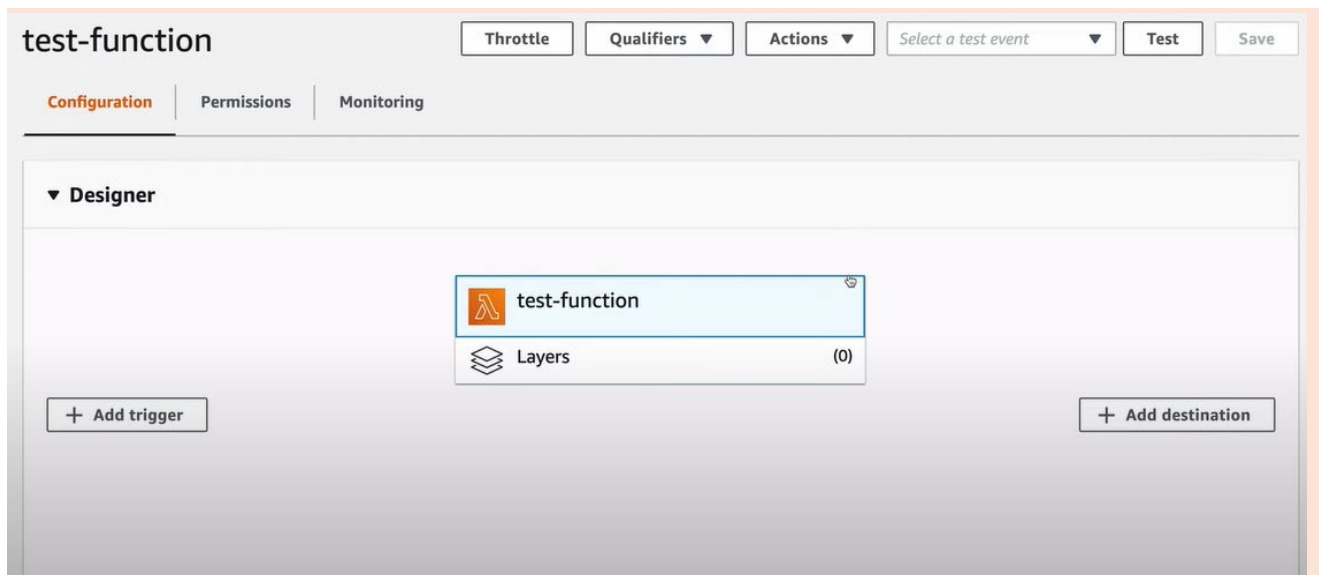
This is how your chart will appear in your dashboard.

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



for lambda and notifications first we will go to lambda



Here we will create a function that detects errors and gives an exception.

```
import json

def lambda_handler(event, context):

    if "error" in event:
        raise Exception(event["error"])

    # TODO implement
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Then we will create an alarm notification and we will write the email to where the alert has to be sent.

Notification

Whenever this alarm state is...
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

Select an 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

Send a notification to...

Only email lists for this account are available

Add notification

We create the notification with the specified conditions.

Preview and create

Step 1: Specify conditions

Edit

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute

Count

1

0.8

0.6

0.4

0.2

0

15:00 16:00 17:00

Errors

Namespace

AWS/Lambda

Metric name

Errors

FunctionName

test-function

Statistic

Sum

Period

Add a description and create the alarm

Add a description

Name and description

Define a unique name

Alarm name

Alarm description - optional

Define a description for this alarm.

Alarm description

Up to 1024 characters (0/1024)

Cancel Previous Next

As we can see, the alarm is created and I receive a notification by email

CloudWatch > Alarms Switch to your original interface

Alarms (1) ☐ Hide Auto Scaling alarms Refresh Add to dashboard Action ▼ Create alarm

Any state ▼ < 1 > Settings

<input type="checkbox"/>	Name	State	Conditions	Action
<input type="checkbox"/>	TestFunctionLambdaError	Insufficient data	Errors > 0 for 1 datapoints within 1 minute	Pen conf

AWS Notification - Subscription Confirmation Inbox x

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

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:598217419300:Default_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

Reply Forward

Later we execute the function lamda and we can see in the graph how it is registered.



Finally we see that in the mail comes a notification about the error and we already have the alerts configured with a lamda function.

