Justin Slade

G00409678

CS 435

Fall 2024

Big Data & Cloud Security

AWS Lab Report 6.1

Date: 10/04/2024

Grambling State University

Big Data and Cloud Security

**Purpose or Objective:** Learn how to monitor resources and users for anomalous events with the use of various services.

**Procedure/s:**

* Analyze event details in the CloudTrail event history.
* Create a CloudTrail trail with CloudWatch logging enabled.
* Create an SNS topic and an email subscription to it.
* Configure an Event Bridge rule to monitor changes to resources in an AWS account.
* Create CloudWatch metric filters and CloudWatch alarms.
* Query CloudTrail logs by using CloudWatch Logs Insights.

**Task 1.**

A screenshot of a computer

Description automatically generatedI need to create a CloudTrail with CloudWatch logs enabled. I can already see a bit of information. Seeing that there is a log showing I created this event

A screenshot of a computer

Description automatically generatedI go over to trail and Set up a trail while enabling CloudWatch as told with the set parameters required. Unfortunately they wont allow me to create a trail due to the limitations of my access since im doing it through a lab

**Task 2.**

Now I need to Create and Simple Notification Service (SNS) and allow it to notify me.

A screenshot of a computer screen

Description automatically generatedI also need to allow everyone to access to this so I can use it for later with minimum interference.

A screenshot of a subscription box

Description automatically generatedI set up the service to send me an email to my email so I can be subscribed to the notifications that happen during this lab.

**Task 3.**

Now I need to create an EventBridge rule so I can see other groups activity

A screenshot of a computer screen

Description automatically generatedSo I create a new rule to do exactly that.

A screenshot of a computer

Description automatically generated

Then I used a Json file to set events that would occur if certain thresholds were to happen Such as notifying me.

A screenshot of a computer

Description automatically generatedThen after I needed to set another parameters with more Json files to state what information I wanted to extract should the aforementioned event was to occur.

A screenshot of a computer

Description automatically generatedI did get stuck here for a bit, but I just needed to click the link to get me access to another tab that would allow me to edit the Inbound rules.

A screenshot of a computer

Description automatically generatedFinally I can see everything I did and when I did it in the Cloud Trail Console.

Note: I should have received an email here but im not sure what went wrong.

**Task 4.**

A screenshot of a computer

Description automatically generatedI now need to setup my Cloud watch alarm and we start with a login metric that will send my a notification should someone fail logging in 3 times.

A screenshot of a login form

Description automatically generatedThis is me testing the 3 attempts of logging in.

Once again im not sure why but I received no such notification despite setting everything up to their description (might be my connection im using)

**Conclusions:**

Unfortunately, I wasn’t able to complete the lab with the expected results but if I did this lab in a different environment, I should be able to get the results I needed. The concept was fun and it’s a shame the lab didn’t work out entirely for me despite my best efforts. I documented all the steps I did before so maybe you could see what I missed out on. Once again, the lab was great, and I was able to see some metrics but they wasn’t relevant to the lab or its objectives.

**Knowledge Check (6) Screenshot:**

A screenshot of a computer test results

Description automatically generated