

Introduction

The requirements for this exercise are to use the Web Server Log Group and the Invalid SSH Login metric filter to trigger a CloudWatch alarm set for 2 data points within 1 minute. This alarm should publish to an alarm notification SNS topic and send you an email as well as trigger a Lambda function to stop the instance.

Make sure you are in us-east-1.

Use the Web Server Log Group and the Invalid SSH Login metric filter to trigger a CloudWatch alarm set for 2 data points within 1 minute.

This alarm should publish to an alarm notification SNS topic and send you an email as well as trigger a Lambda function to stop the instance.

Steps to complete

1. **Verify Alarm Settings on the Metric Filter**

Complete the following:

1. Navigate to CloudWatch.
2. Select **Alarms**.
3. Select **InvalidSSHLoginAlarm**.
4. Set the Actions drop-down to **Modify**.
5. Change the threshold from **222** to **2**.
6. **An Alarm Should Trigger an Email Notification**

Complete the following:

1. Navigate to SNS.
2. Choose the **AlarmNotificationTopic**.
3. Subscribe via email.
4. **An Alarm Should Trigger the Lambda Function**

Two methods:

1. SNS

* Navigate to SNS.
* Select **AlarmNotificationTopic**.
* Subscribe to the Lambda function.

1. Lambda

* Navigate to Lambda.
* Select the **SNS** trigger.
* Configure it to use the **AlarmNotificationTopic**.

1. **Verify the EC2 Instance is Stopped**

* Attempting 2 failed logins within 1 minute, navigate to EC2.
* Observe that the instance is in the stopped state.