

How to - Configure AWS GuardDuty to forward logs to EventTracker

EventTracker v9.2 and later

Abstract

This guide provides instructions to integrate AWS with EventTracker manager using AWS GuardDuty.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Amazon AWS**.

Audience

Administrators who are assigned the task to monitor **Amazon AWS** using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Content

- 1. Prerequisites..... 3
- 2. Overview..... 3
- 3. Integrate AWS Guardduty using Lambda Function..... 4

1. Prerequisites

- EventTracker v9.2 and above/EventTracker agent should be installed.
- Administrative access for AWS Account.
- EventTracker syslog VCP port / EventTracker syslog relay port (e.g. 514) should be allowed on public IP.
- GuardDuty should be enabled on your AWS account.
- CloudWatch Should be enabled on your AWS account.

2. Overview

Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.

Amazon GuardDuty can be integrated with EventTracker using EventTracker Lambda function. After receiving the logs from GuardDuty, EventTracker alerts you of the following findings:

- Backdoor
- Crypto Currency
- Discovery
- Impact
- Pentest
- Persistence
- Policy
- Privilege Escalation
- Recon
- Resource Consumption
- Stealth
- Trojan
- Unauthorized Access

EventTracker dashboard will display the summarized view of GuardDuty findings based on Threat type, Source IP and Map view of suspicious activities source location.

EventTracker reports will provide activities summary on scheduled basis. These reports will also furnish details about all activities, resources affected, about the threat actor, etc.

3. Integrate AWS GuardDuty using Lambda Function

Before integrating AWS GuardDuty with EventTracker manager, we need to integrate AWS with EventTracker using Lambda function. Follow [this](#) guide before proceeding with the below instructions:

1. Login into [AWS CloudWatch portal](#).
2. Click on **Rules** tab under **Events** and create rule by **Create rule**.

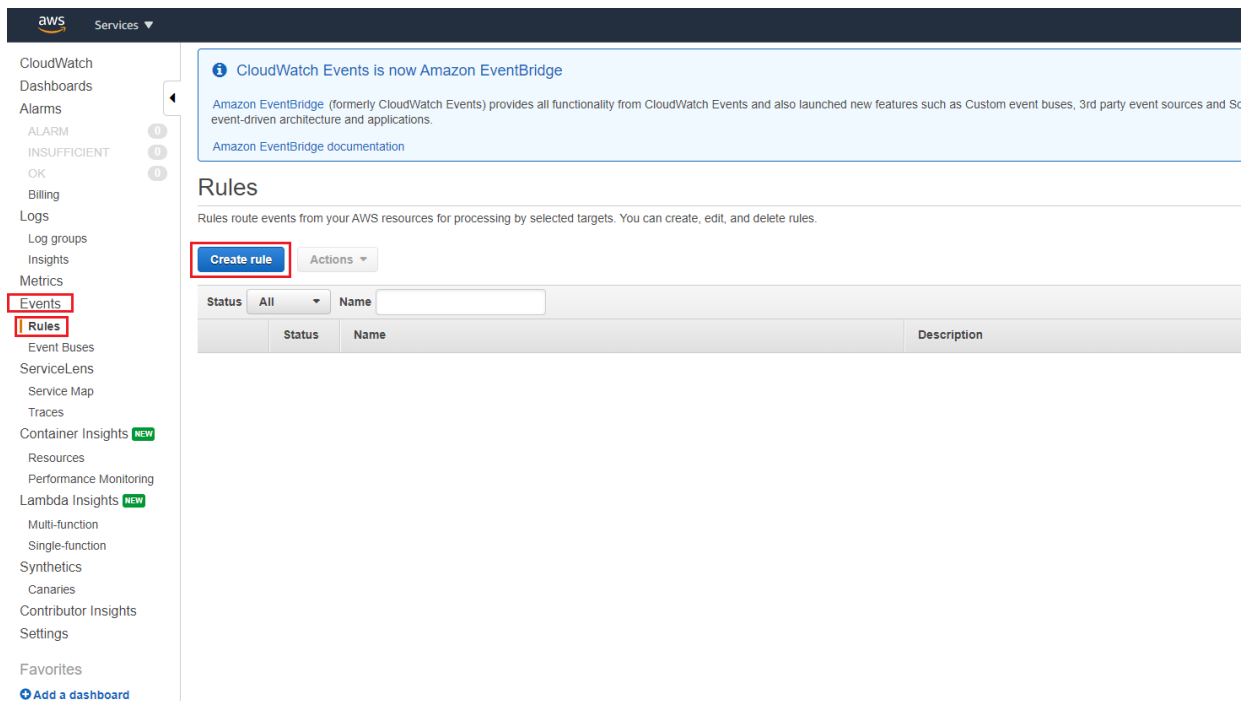


Figure 1

3. Under rule creation screen, select **GuardDuty** in **Service Name** and **All Events** in **Event Types** as **Event Source**

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern ⓘ Schedule ⓘ

Build event pattern to match events by service

Service Name:

Event Type:

Build an event pattern to match all events from this service

Event Pattern Preview Copy to clipboard Edit

```

{
  "source": [
    "aws.guardduty"
  ]
}

```

Figure 2

- In **Targets** section, click **Add Target** and select **Lambda** function created for EventTracker. If Lambda function for EventTracker is still not create. Follow [this](#) Instructions.

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

[+](#) Add target*

Figure 3

Keep the remaining section as default.

Lambda function

Function*

▼ Configure version/alias

Default

Version

Alias

▼ Configure input

Matched event ⓘ

Part of the matched event ⓘ

Constant (JSON text) ⓘ

Input Transformer ⓘ

Figure 4

5. After filling the section, click **Configure details**.

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern ⓘ Schedule ⓘ

Build event pattern to match events by service

Service Name

Event Type

Build an event pattern to match all events from this service

Event Pattern Preview Copy to clipboard Edit

```
{
  "source": [
    "aws.guardduty"
  ]
}
```

▶ Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

Lambda function

Function*

▼ Configure version/alias

Default

Version

Alias

▼ Configure input

Matched event ⓘ

Part of the matched event ⓘ

Constant (JSON text) ⓘ

Input Transformer ⓘ

Cancel

Figure 5

6. Provide **Rule name** (e.g. Guardduy_ET_Integration) and click **Create rule** for the completion of GuardDuty integration with EventTracker.

Step 2: Configure rule details

Rule definition

Name*

Description

State Enabled

CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.

* Required Cancel Back **Create rule**

Figure 6

Rules

Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.

Create rule Actions ↻ ⓘ

Status **All** Name « < Viewing 1 to 2 of 2 Rules > »

Status	Name	Description
<input checked="" type="radio"/>	Guardduty_ET_Integration	

Figure 7