Netsurion | EventTracker®

How to - Configure AWS GuardDuty to forward logs to EventTracker

EventTracker v9.2 and later

Publication Date: October 22, 2020

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.

Table of Content

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 Guarduty 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.**

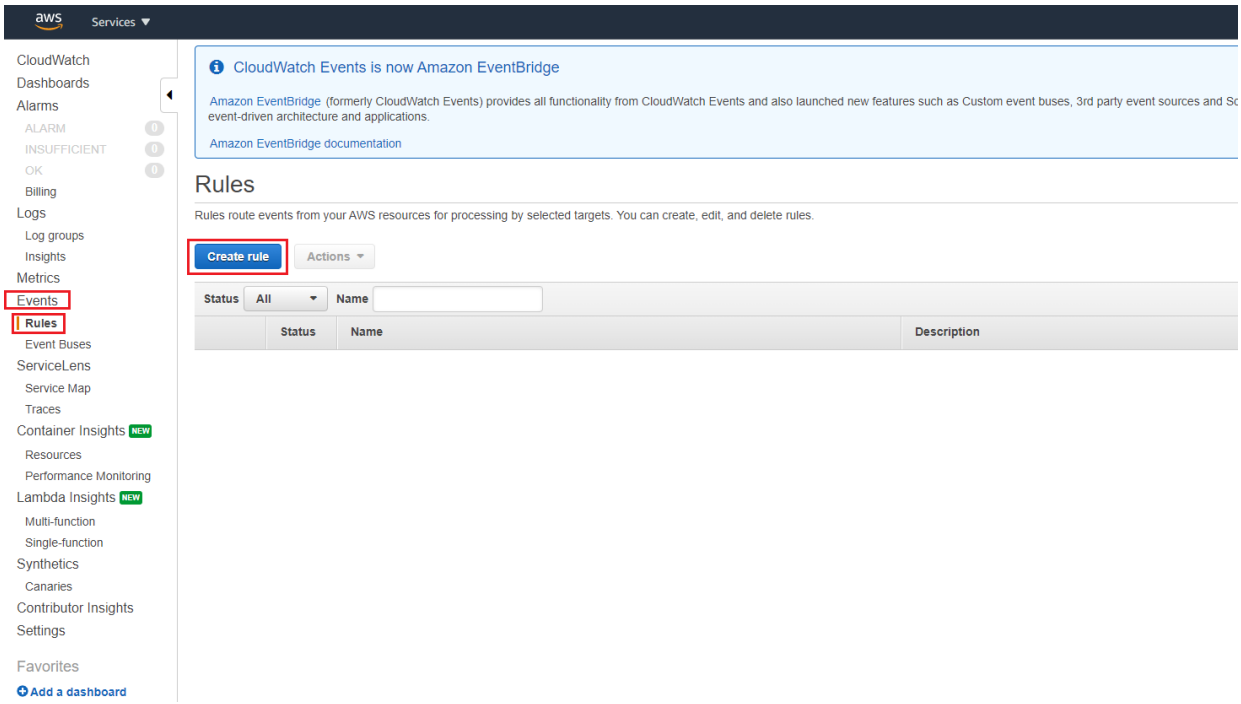

Figure 1

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

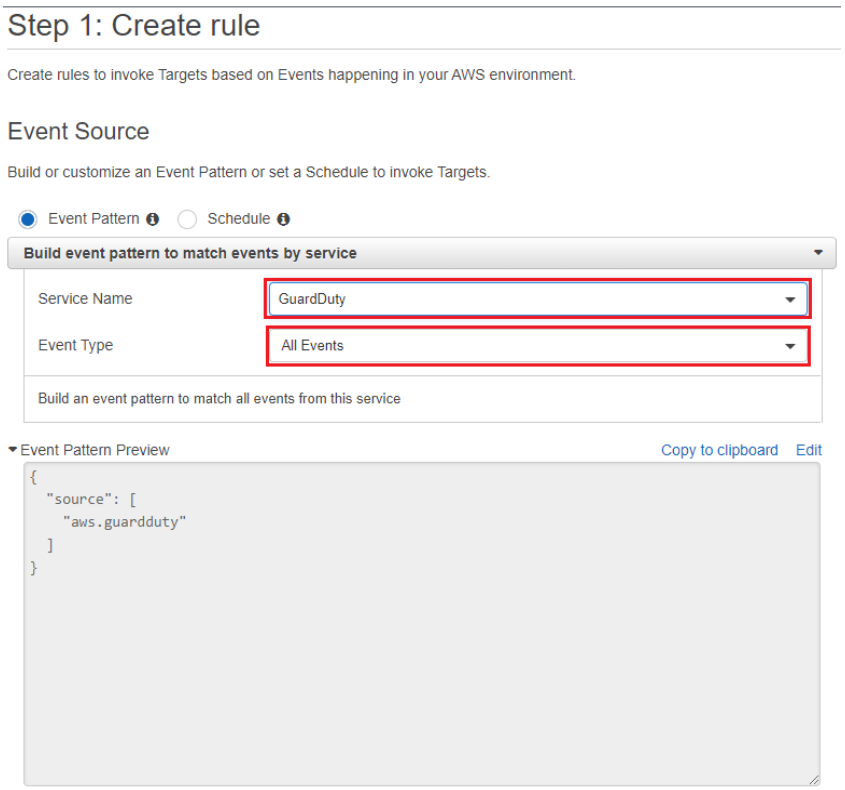

Figure 2

4. 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.

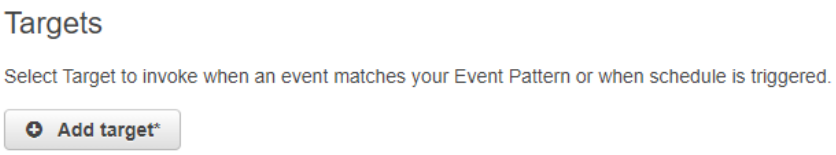

Figure 3

Keep the remaining section as default.

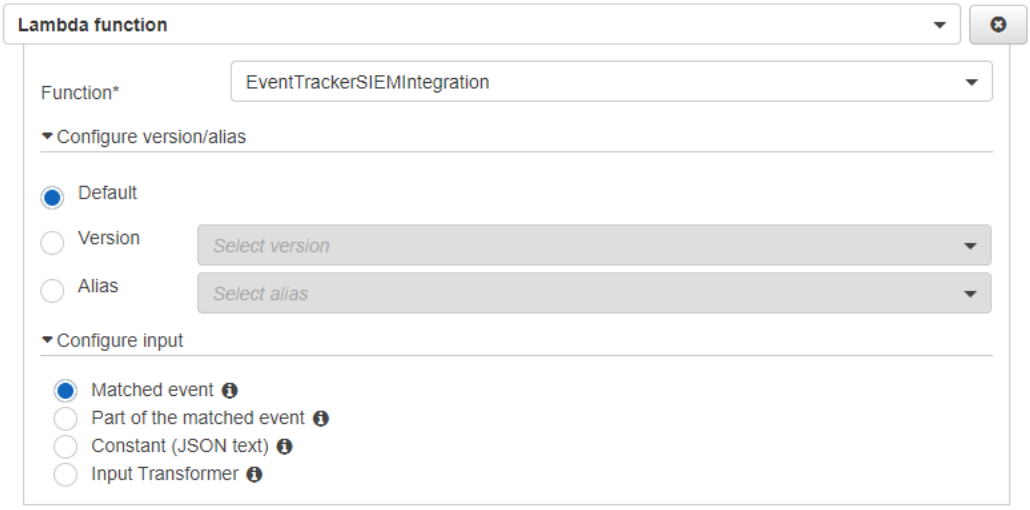

Figure 4

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

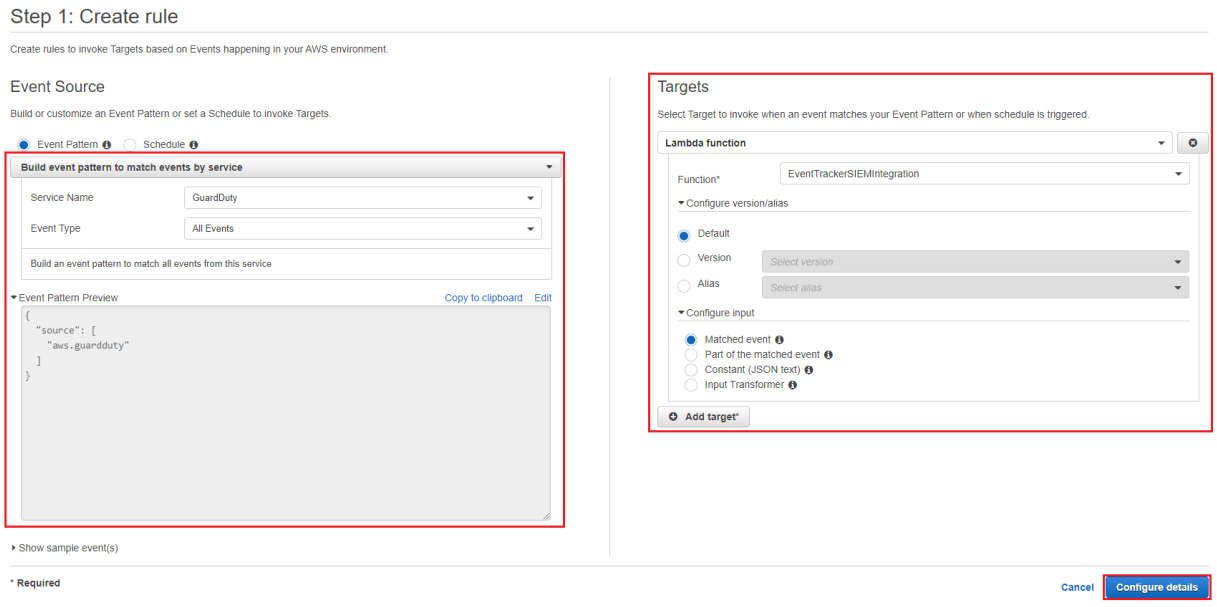

Figure 5

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

Figure 6

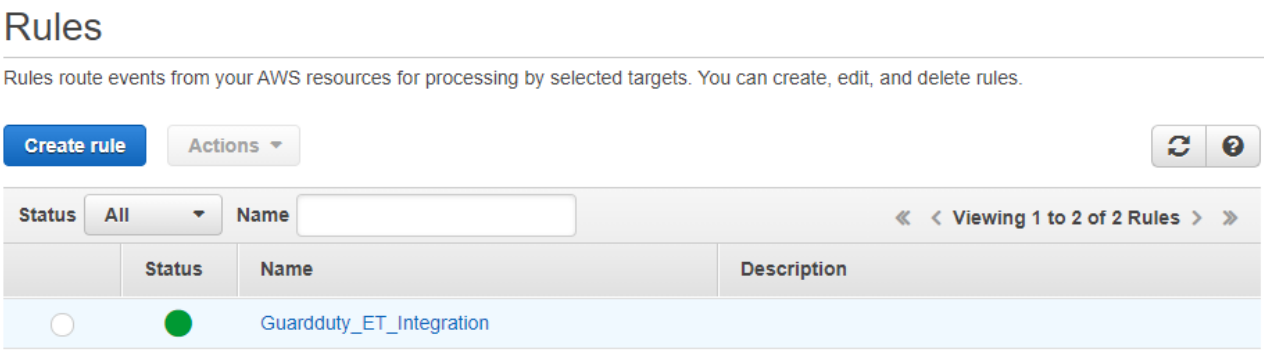

Figure 7