# AWS GuardDuty Integrations

## Introduction

The Amazon GuardDuty integration collects and parses data from Amazon GuardDuty Findings REST APIs.

The Amazon GuardDuty integration can be used in three different modes to collect data:

- HTTP REST API - Amazon GuardDuty pushes logs directly to an HTTP REST API.
- AWS S3 polling - Amazon GuardDuty writes data to S3 and Elastic Agent polls the S3 bucket by listing its contents and reading new files.
- AWS S3 SQS - Amazon GuardDuty writes data to S3, S3 pushes a new object notification to SQS, Elastic Agent receives the notification from SQS, and then reads the S3 object. Multiple Agents can be used in this mode.

### Assumptions

The procedures described in Section 3 assume that a Log Collector has already been setup.

## Requirements

You need Elasticsearch for storing and searching your data and Kibana for visualizing and managing it. You can use our hosted Elasticsearch Service on Elastic Cloud, which is recommended, or self-manage the Elastic Stack on your own hardware.

Note: It is recommended to use AWS SQS for Amazon GuardDuty.

## Aws GuardDuty integration Procedures

To collect data from AWS S3 Bucket, follow the steps below:

- Configure the Data Forwarder to ingest data into an AWS S3 bucket. However, the user can set the parameter "Bucket List Prefix" according to the requirement.

To collect data from AWS SQS, follow the steps below:

1. If data forwarding to an AWS S3 bucket hasn't been configured, then first setup an AWS S3 bucket as mentioned in the documentation above.

2. To setup an SQS queue, follow "Step 1: Create an Amazon SQS queue" mentioned in the Documentation.

   - While creating an SQS queue, please provide the same bucket ARN that has been generated after creating the AWS S3 bucket.

3. Setup event notification for an S3 bucket. Follow this guide.

   - The user has to perform Step 3 for the guardduty data-stream, and the prefix parameter should be set the same as the S3 Bucket List Prefix as created earlier. For example, logs/ for guardduty data stream.

   - For all the event notifications that have been created, select the event type as s 3:ObjectCreated:*, select the destination type SQS Queue, and select the queue that has been created in Step 2.

Note:

- Credentials for the above AWS S3 and SQS input types should be configured according to the input configuration guide.

- Data collection via AWS S3 Bucket and AWS SQS are mutually exclusive in this case.

To collect data from Amazon GuardDuty API, users must have an Access Key and a Secret Key. To create an API token follow the steps below:

1. Login to https://console.aws.amazon.com/.

2. Go to https://console.aws.amazon.com/iam/ to access the IAM console.

3. On the navigation menu, choose Users.

4. Choose your IAM user name.

5. Select Create access key from the Security Credentials tab.

6. To see the new access key, choose Show.

Note

- The Secret Access Key and Access Key ID are required for the current integration package.

---

Revision #2
Created 23 April 2024 10:41:43
Updated 19 June 2024 06:54:01