# AWS Cloudtrails Integrations

## Introduction

The AWS CloudTrail integration allows you to monitor AWS CloudTrail

Reference: https://aws.amazon.com/cloudtrail/

Use the AWS CloudTrail integration to collect and parse logs related to account activity across your AWS infrastructure. Then visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference logs when troubleshooting an issue.

For example, you could use the data from this integration to spot unusual activity in your AWS accounts—like excessive failed AWS console sign in attempts.

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

## Data streams

The AWS CloudTrail integration collects one type of data: logs.

Logs help you keep a record of every event that CloudTrail receives. These logs are useful for many scenarios, including security and access audits. See more details in the Logs reference.

Reference : https://aquila-elk.kb.us-east-1.aws.found.io:9243/app/integrations/detail/aws-1.28.3/overview?integration=cloudtrail - logs-reference

## Assumptions

The procedures described in Section 3 assumes 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.

Before using any AWS integration you will need:

- AWS Credentials to connect with your AWS account.
- AWS Permissions to make sure the user you're using to connect has permission to share the relevant data.

For more details about these requirements, see the AWS integration documentation.

## Setup

Use this integration if you only need to collect data from the AWS CloudTrail service.

If you want to collect data from two or more AWS services, consider using the AWS integration. When you configure the AWS integration, you can collect data from as many AWS services as you'd like.

For step-by-step instructions on how to set up an integration, see the Getting started guide.

## Logs reference

The cloudtrail data stream collects AWS CloudTrail logs. CloudTrail monitors events like user activity and API usage in AWS services. If a user creates a trail, it delivers those events as log files to a specific Amazon S3 bucket.

## AWS CloudTrail integration Procedures

The following will need to be provided in the Configure integration when adding the AWS Audit CloudTrail integration.

Procedures:

Please provide the following information to CyTech:

Configure Integration

1. Collect CloudTrail logs from S3 (Enable)

- Queue URL is required (URL of the AWS SQS queue that messages will be received from.)

2. Collect CloudTrail logs from CloudWatch(Optional)

- Log Group ARN (ARN of the log group to collect logs from.)

3. Collect CloudTrail logs from third-party REST API (Optional)

- URL of Splunk Enterprise Server (i.e. scheme://host:port, path is automatic)
- Splunk REST API Username
- Splunk REST API Password
- Splunk Authorization Token (Bearer Token or Session Key, e.g. "Bearer eyJFd3e46..." or "Splunk 192fd3e...". Cannot be used with username and password.)

---

Revision #2
Created 23 April 2024 10:37:16
Updated 19 June 2024 06:54:01