Fluent Bit: Output Plugin for AWS CloudTrail Data Service

Date:	2024-11-12
modified:	2024-11-12
tags:	FluentBit, Go, Coding, Plugin, AWS, CloudTrail, OpenSource
description:	Open Source AWS CloudTrail Data Service output plugin written in Go for Fluent Bit
category:	Code
slug:	fluent-bit-output-plugin-for-aws-cloudtrail-data-service
Author:	Dominik Wombacher
lang:	en
transid:	fluent-bit-output-plugin-for-aws-cloudtrail-data-service
Status:	published

I recently wrote a AWS CloudTrail Data Service output plugin (Mirror: [1], [2], [3]) in Golang for Fluent Bit. It's Open Source under the Apache-2.0 license. The plugin ingest events into AWS CloudTrail Lake through the CloudTrail Data Service by making a PutAuditEvents API call.

I wrote a guest Article in the SUSE Blog: Send SUSE Security (NeuVector) events to AWS CloudTrail Lake (Archive: [1], [2]). It covers the Architecture and usage, in the context of SUSE Security (NeuVector) and Syslog as Fluent Bit input. But given the modular nature of Fluent Bit, your Input can be one of the other over 40 sources. Which makes the Blog a blueprint for other use-cases too.

The Heart and Soul of the plugin is out_aws-cloudtrail-data.go, which is based on the boilerplate example out_gstdout.go. It's my first Fluent Bit plugin and I enjoyed the nice coding exercise to hack a first working version together and release it. There is, as always in life, room for improvement but it does the job and is more than enough to get started.

Looking forward for feedback to improve the plugin and to the next opportunity to write another one.

Helpful resources to understand the Fluent Bit concepts and to write a plugin in Go:

- Fluent Bit - Key Concepts
- Fluent Bit - Golang Output Plugins
- fluent-bit-go / examples

Recommended resources to learn more about the AWS CloudTrail Data Service and the API to ingest events into AWS CloudTrail Lake:

- AWS CloudTrail – API Reference – PutAuditEvents
- AWS CloudTrail – User Guide – Create a custom integration with the console
- CloudTrail Lake integrations event schema