Logging output from AWS Cloudwatch

You might want to collect, search, and analyze logging output from AWS Cloudwatch logs when doing the following:

- Managing an Amazon Web Services environment

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Cloudwatch logs
- Splunk Add-on for Amazon Web Services

Example

Like Cloudwatch metrics, Cloudwatch logs can be collected for a wide range of AWS infrastructure. After Cloudwatch logs are collected in Splunk, the full power of Splunk’s search processing language can be applied to help accelerate incident investigations involving cloud infrastructure.

To optimize the search shown below, you should specify a time range.

1. Ensure that your deployment is ingesting AWS data through one of the following methods:
   - Pulling the data from Splunk via AWS APIs. At small scale, pull via the AWS APIs will work fine.
   - Pushing the data from AWS into Splunk via Lambda/Firehose to Splunk HTTP event collector. As the size and scale of either your AWS accounts or the amount of data to be collected grows, pushing data from AWS into Splunk is the easier and more scalable method.

2. Run the following search:

```bash
index="<AWS index name>" sourcetype="aws:cloudwatchlogs" source="**"
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>index=&quot;&lt;AWS index name&gt;&quot; sourcetype=&quot;aws:cloudwatchlogs&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS Cloudwatch Logs sourcetype.</td>
</tr>
<tr>
<td>source=&quot;*&quot;</td>
<td>Search all sources.</td>
</tr>
</tbody>
</table>

### Result

You can tailor this search to your investigation or troubleshooting needs in two ways:

- Update the source filter to return logs from a specific log group, such as the log group associated with a certain Lambda function.
- Add keywords to the search. For example, adding (error OR fail*) to the search might help uncover AWS resources that have experienced errors recently.