Logging output from AWS Lambda functions

You might want to search, analyze, and troubleshoot logging output from AWS Lambda functions 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
- AWS CloudWatch data
- Splunk Add-on for Amazon Web Services

Example

Like most other application logs, Lambda function logging from CloudWatch logs provides valuable information that can be used during an investigation to facilitate answering questions about the functions behavior and health. Use this procedure to search all CloudWatch logs collected for a specific Lambda function.

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:

   ```
   index="<AWS index name>" sourcetype="aws:cloudwatchlogs" source="*/aws/lambda/*" source="*<Lambda function name>*"
   ```

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.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>index=&quot;&lt;AWS index name&gt;&quot; sourcetype=&quot;aws:cloudwatchlogs&quot;</code></td>
<td>Search the index(s) where AWS data is stored, filtered to just the AWS Cloudwatch logs.</td>
</tr>
<tr>
<td><code>source=&quot;/aws/lambda/*&quot; source=&quot;&quot;&lt;Lambda function name&gt;&quot;&quot;</code></td>
<td>Filter results to those associated to a given Lambda function.</td>
</tr>
</tbody>
</table>

### Result

In the search, add additional keywords relevant to the investigation. For instance, adding (error OR fail*) to the search might help uncover problems occurring with the Lambda function.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.