Disabled AWS CloudTrail logging

You might want to view and alert when AWS CloudTrail logging becomes disabled 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 CloudTrail data
- Splunk Add-on for Amazon Web Services

Example

CloudTrail logs provide critical ground truth auditing of all AWS activity. Whether malicious or otherwise, timely detection of CloudTrail logging becoming disabled is important. Use this procedure to detect and alert when CloudTrail logs have been disabled.

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:cloudtrail" eventName=StopLogging
| rename requestParameters.name AS trail_name userIdentity.arn AS who_done_it
| table _time aws_account_id region eventName trail_name who_done_it
```

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>Expression</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>index=&quot;&lt;AWS index name&gt;&quot;&lt;br&gt;sourcetype=&quot;aws:cloudtrail&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS CloudTrail data.</td>
</tr>
<tr>
<td>eventName=StopLogging</td>
<td>Filter the results down to the StopLogging event which is emitted when Cloudtrail logging is disabled.</td>
</tr>
<tr>
<td></td>
<td>rename requestParameters.name AS trail_name&lt;br&gt;userIdentity.arn AS who_done_it&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>table _time aws_account_id region eventName&lt;br&gt;trail_name who_done_it&lt;br&gt;</td>
</tr>
</tbody>
</table>

### Result

Use the results of this search to re-enable CloudTrail logging and to take the appropriate measures to address the account that disabled it.