Changes made to AWS cloud infrastructure

You might want to know what changes were made in your AWS cloud infrastructure 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 logs
- Splunk Add-on for Amazon Web Services

Example

Knowing what modifications have been made to cloud infrastructure resources, when they were made, and who made them can help you identify or isolate the origin of a problem or incident. You need a search that shows what changes have been made to AWS resources.

To optimize the search shown below, you should specify an index and 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:

```
sourcetype="aws:cloudtrail" readOnly=False |eval requestParameters=mvindex(split(mvindex(split(_raw, ""requestParameters":""),1),""responseElements\":""),0) |table _time src requestParameters
```

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

dsourcetype="aws:cloudtrail"

|eval
|requestParameters=mvindex(mvindex(split(_raw, "\"requestParameters\":"),1),"\"responseElements\":"),0)

Explanation

Search only AWS CloudTrail data.

Filter to non-readOnly events.

Depending on the type of changes being reported in CloudTrail logs, you may want to add additional filters. For instance adding (NOT "userIdentity.invokedBy"="cloudtrail.amazonaws.com") would filter out CloudTrail logging activity which could be noisy.

|table _time src requestParameters

Divide the full text into two parts using "requestParameters:" as the delimiter. Split the results of the first split using "responseElements:" as the delimiter. Take the first part of the split and save the extracted text into the requestParameters field.

The text of the event is a JSON document and the entire text is in the field _raw.

Display the results in a table with columns in the order shown.

Result

Sample results for this search are shown in the table below. The table shows the time of the event, the src or host the changes were made on, and all the request parameters extracted by the search. This is a way of gaining understanding of the activity taking place on your AWS cloud. For example, you can see that ipAddressPermissions were changed for tcp port 22 on the 204.107.141.244 src (host).

<table>
<thead>
<tr>
<th>_time</th>
<th>src</th>
<th>requestParameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-10-14T13:19:20.000+0000</td>
<td>204.107.141.244</td>
<td>{&quot;ipPermissions&quot;: {&quot;items&quot;: [{&quot;ipProtocol&quot;: &quot;tcp&quot;, &quot;toPort&quot;: 22, &quot;fromPort&quot;: 22, &quot;prefixListIds&quot;: {}, &quot;groups&quot;: {}, &quot;ipRanges&quot;: {&quot;items&quot;:}}}...}</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>_time</th>
<th>src</th>
<th>requestParameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-10-14T13:11:41.000+0000</td>
<td>54.175.25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.140</td>
<td></td>
</tr>
<tr>
<td>2020-10-14T13:11:21.000+0000</td>
<td>54.171.211.111</td>
<td></td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>_time</th>
<th>src</th>
<th>requestParameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-10-14T13:10:09.000+0000</td>
<td>54.171.211.111</td>
<td>&quot;arn&quot;: &quot;arn:aws:iam::063605715280:user/kieffer&quot; }, &quot;eventName&quot;: &quot;DeleteAccessKey&quot;, &quot;eventVersion&quot;: &quot;1.01&quot;, &quot;userAgent&quot;: &quot;AWSConsole&quot;,</td>
</tr>
<tr>
<td>2020-10-14T13:08:15.000+0000</td>
<td>204.107.141.244</td>
<td>{&quot;userName&quot;: &quot;bitcoin_miner&quot;, &quot;accessKeyId&quot;: &quot;AKIAIVVLOMXHGFQUCTVA&quot;}, &quot;awsRegion&quot;: &quot;us-east-1&quot;, &quot;userIdentity&quot;: {&quot;accountId&quot;: &quot;063605715280&quot;, &quot;userName&quot;: &quot;khungus&quot;, &quot;sessionContext&quot;: {&quot;attributes&quot;: {&quot;creationDate&quot;: &quot;2014-05-02T23:09:55Z&quot;, &quot;mfaAuthenticated&quot;: &quot;false&quot;}}, &quot;accessKeyId&quot;: &quot;PU3RC0M4LN00DL3T1M3Z&quot;, &quot;type&quot;: &quot;IAMUser&quot;, &quot;principalId&quot;: &quot;AIR0NM4NU5R6GQ5T4RKLW&quot;, &quot;arn&quot;: &quot;arn:aws:iam::063605715280:user/khungus&quot; }, &quot;eventName&quot;: &quot;DeleteAccessKey&quot;, &quot;eventVersion&quot;: &quot;1.01&quot;, &quot;userAgent&quot;: &quot;AWSConsole&quot;,</td>
</tr>
<tr>
<td>2020-10-14T13:03:40.000+0000</td>
<td>204.107.141.244</td>
<td>{&quot;vpclId&quot;: &quot;vpc-d2d110ba&quot;, &quot;groupName&quot;: &quot;launch-wizard-5&quot;, &quot;groupDescription&quot;: &quot;launch-wizard-5 created 2016-01-27T11:12:38.947+08:00&quot;}, &quot;requestID&quot;: &quot;af4a15b7-2c71-4eab-b09f-f8d9783cd21b&quot;}</td>
</tr>
<tr>
<td>_time</td>
<td>src</td>
<td>requestParameters</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;groupName&quot;: &quot;launch-wizard-5&quot;, &quot;groupDescription&quot;: &quot;launch-wizard-5 created 2016-01-27T11:12:38.947+08:00&quot;}, &quot;requestID&quot;: &quot;af4a15b7-2c71-4eab-b09f-f8d9783cd21b&quot;</td>
</tr>
</tbody>
</table>

You can update the table to show additional fields, such as the following:

```
| _time | eventName | userIdentity.arn | userIdentity.userName | src | requestParameters |
```

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.