Resources with non-compliant AWS configuration rules

You might want to know what resources in your AWS infrastructure are violating configuration rules 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 configuration logs
- Splunk Add-on for Amazon Web Services

Example

AWS configuration rules let you define configuration policies and monitor resources created in violation of those policies. You want to evaluate all resources currently in violation of one or more config rules.

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:
   ```plaintext
   sourcetype="aws:config:rule" ComplianceType=NON_COMPLIANT
   |rename EvaluationResultIdentifier.EvaluationResultQualifier.* AS *
   |stats max(_time) AS _time BY ConfigRuleName ResourceType ResourceId account_id region
   |table _time *
   ```

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**

```
sourcetype="aws:config:rule"
```

- **Explanation**: Search only AWS configuration rules.

```
ComplianceType=NON_COMPLIANT
```

- **Explanation**: Return only results with a status of non-compliant.

```
|rename EvaluationResultIdentifier.EvaluationResultQualifier.* AS *
```

- **Explanation**: Rename the field as shown for better readability.

```
|stats max(_time) AS _time BY ConfigRuleName
```

- **Explanation**: Set the _time field to the latest time available for each resource.

```
ResourceType ResourceId account_id region
```

- **Explanation**: Display the results in a table with columns in the order shown. Use the wildcard to match the fields in the stats command.

## Result

Sample results for this search are shown in the table below. After identifying items that are not in compliance with the desired configuration, a logical next step is to send this information to the contact for the account_id and request that the required configuration rule be remediated to a compliant setting. If your organization isn’t using configuration rules to validate the integrity of cloud resources, it might be a good time to revisit that decision.

<table>
<thead>
<tr>
<th>_time</th>
<th>ConfigRuleName</th>
<th>ResourceId</th>
<th>ResourceType</th>
<th>account_id</th>
<th>region</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-10-16T00:01:30.000+0000</td>
<td>cloudtrail-enabled</td>
<td>i-3c89ef98</td>
<td>AWS::EC2::Instance</td>
<td>63605715280</td>
<td>us-west-2</td>
</tr>
<tr>
<td>2020-10-15T13:24:59.000+0000</td>
<td>cloudtrail-enabled</td>
<td>i-91b5c935</td>
<td>AWS::EC2::Instance</td>
<td>63605715280</td>
<td>us-west-2</td>
</tr>
<tr>
<td>2020-10-16T01:00:00.000+0000</td>
<td>cloudtrail-enabled</td>
<td>i-d655b2fd</td>
<td>AWS::EC2::Instance</td>
<td>63605715280</td>
<td>us-west-2</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>ConfigRuleName</th>
<th>ResourceId</th>
<th>ResourceType</th>
<th>account_id</th>
<th>region</th>
</tr>
</thead>
<tbody>
<tr>
<td>29:24.000+0000</td>
<td>enabled</td>
<td></td>
<td>instance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020-10-15T20:53:47.000+0000</td>
<td>cloudtrail-enabled</td>
<td>i-f775b8dc</td>
<td>AWS::EC2::Instance</td>
<td>63605715280</td>
<td>us-west-2</td>
</tr>
<tr>
<td>2020-10-15T14:31:46.000+0000</td>
<td>eip-attached</td>
<td>i-33780497</td>
<td>AWS::EC2::Instance</td>
<td>63605715280</td>
<td>us-west-2</td>
</tr>
</tbody>
</table>

The AWS app does a similar search and provides additional insight for configuration rules. The configuration dashboard is found by navigating to Insights -> Config Rules.