Common AWS resource tags and tag values

You might want to visualize and analyze common resource tags and tag values 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 description data
- Splunk Add-on for Amazon Web Services

Example

Resource tags are a critical part of the cloud asset management strategy for most organizations. However, with such a flexible design, tag management and analysis can be challenging to review and manage.

You can use this search to identify the most frequent tags and tag values in use across your 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:

   ```splunk
   index=<AWS-INDEX> sourcetype=aws:description
   | dedup _raw
   | rex field=source "(?<resource_type>.*)"
   | table tags.* resource_type
   | untable resource_type tag tag_value
   | top limit=0 tag BY resource_type
   | table resource_type tag percent
   ```
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.

<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:description&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS description data.</td>
</tr>
<tr>
<td></td>
<td>Remove duplicate _raw values to get the latest results for each resource type.</td>
</tr>
<tr>
<td></td>
<td>Extract the type of AWS resource out of the source field.</td>
</tr>
<tr>
<td></td>
<td>Create a table of rows for each resource type tag and tag value.</td>
</tr>
<tr>
<td></td>
<td>Find the most frequent tag for each resource type.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

Result

This search is one of many ways you can analyze tag data. You should modify the search to analyze the data in a way that is more relevant to how your organization uses tagging. For instance, you may wish to visualize all resources using the same tag name which may help analyze how much infrastructure is supporting a particular application, or how much infrastructure is supporting non-production workloads.