Missing AWS resource tags

You might want to identify resources missing a specific tag 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 a resource that is missing a tag that is expected by your organization.

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 name>* sourcetype=aws:description
| dedup id
| rex field=source ".(<resource_type>.*)*"
| search resource_type IN (ec2_instances)
| search (NOT tags.<tag name>=*)
| table account_id region, id, tags.*
```

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.
## 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><code>index=&lt;AWS index name&gt;</code>, 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>dedup id`</td>
</tr>
<tr>
<td>`</td>
<td>rex field=source &quot;:(?&lt;resource_type&gt;.*)&quot;`</td>
</tr>
<tr>
<td>`</td>
<td>search resource_type IN (ec2_instances)`</td>
</tr>
<tr>
<td>`</td>
<td>search (NOT tags.&lt;tag name&gt;=*)`</td>
</tr>
<tr>
<td>`</td>
<td>table account_id region, id, tags.*`</td>
</tr>
</tbody>
</table>

## Result

The resulting table shows any AWS resource that doesn't have a value for the tag name you chose to search for.