Unattached AWS elastic block store volumes

You might want to know which of your AWS elastic block store (EBS) volumes are unattached 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

Unattached EBS volumes represent storage that's allocated but not in use or accessible to any system. You want to see which of your EBS volumes are unattached so you can decide if they should be deleted to save on cloud costs.

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:

   ```splunk
   sourcetype="aws:description" region="*" source="*:ec2_volumes" status!="in-use" |dedup id sortby -_time |rename "attach_data.instance_id" AS instanceId |table account_id id region instanceId size status type
   ```

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:description" region="*" source="*:ec2_volumes"
```

**Explanation**

Search only your EC2 volumes and filter by description data for all regions.

```
status!="in-use"
```

**Explanation**

Return only volumes where the status is not "in use."

```
|dedup id sortby -_time
```

**Explanation**

Remove duplicate instances by ID and sort the remaining results with the most recent instances first.

```
|rename "attach_data.instance_id" AS instanceld
```

**Explanation**

Rename the field as shown for better readability.

```
|table account_id id region instanceld size status type
```

**Explanation**

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 volumes listed are not in use and could be eligible for deletion or archiving to less expensive storage.

<table>
<thead>
<tr>
<th>account_id</th>
<th>id</th>
<th>region</th>
<th>instanceld</th>
<th>size</th>
<th>status</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>vol-c884c715</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>80</td>
<td>available</td>
<td>standard</td>
</tr>
<tr>
<td>63605715280</td>
<td>vol-c880c7c1</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>80</td>
<td>available</td>
<td>standard</td>
</tr>
<tr>
<td>63605715280</td>
<td>vol-c990c709</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>80</td>
<td>available</td>
<td>standard</td>
</tr>
<tr>
<td>63605715280</td>
<td>vol-s9821717</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>100</td>
<td>available</td>
<td>gp2</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>account_id</th>
<th>id</th>
<th>region</th>
<th>instanceId</th>
<th>size</th>
<th>status</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>vol-c898c701</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>80</td>
<td>available</td>
<td>standard</td>
</tr>
<tr>
<td>63605715280</td>
<td>vol-c891c7c1</td>
<td>ap-southeast-1</td>
<td>null</td>
<td>80</td>
<td>available</td>
<td>standard</td>
</tr>
</tbody>
</table>

The AWS app does a similar search and provides additional insight for EBS volumes, including Non-Optimized EBS, no recent snapshot, and large and small IOPS. These can be found by navigating to EBS Insights > Insights Filter.

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.