Current AWS elastic block store volumes

You might want to retrieve basic information about your elastic block store (EBS) volumes 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

Insights into how many, what size, what types, current snapshot size, and usage of EBS volumes are all valuable information for cost and potential performance ramifications. In addition, unused EBS volumes are very common and eliminating them provides an easy way to reduce cost in your AWS environment. As an IT administrator, you want to start monitoring this information.

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:

```
source="*:ec2_volumes" sourcetype="aws:description"
| dedup id sortby -_time
| table account_id zone_id snapshot_id type size attach_data.instance_id status
| sort -status
```

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

source="*:ec2_volumes" sourcetype="aws:description"

|dedup id sortby -_time

|table account_id zone id snapshot_id type size attach_data.instance_id status

|sort -status

Explanation

Search only your EC2 volumes and filter by description data.

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

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

Sort the results by status in descending order.

Result

Sample results for this search are shown in the table below. They serve as a good baseline for understanding the EBS inventory, scale, location, type, and usage.

<table>
<thead>
<tr>
<th>account_id</th>
<th>zone</th>
<th>id</th>
<th>snapshot_id</th>
<th>type</th>
<th>size</th>
<th>attach_data.instance_id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>ap-southeast-1a</td>
<td>vol-1823a616</td>
<td>snap-b71cfa5b</td>
<td>standard</td>
<td>500</td>
<td>i-18472f4e</td>
<td>in-use</td>
</tr>
<tr>
<td>63605715280</td>
<td>ap-southeast-1b</td>
<td>vol-f01626f8</td>
<td>snap-742b7598</td>
<td>standard</td>
<td>300</td>
<td>i-33b05718</td>
<td>in-use</td>
</tr>
<tr>
<td>63605715280</td>
<td>ap-southeast-1b</td>
<td>vol-f05c08f8</td>
<td>snap-bdf1b850</td>
<td>standard</td>
<td>250</td>
<td>i-6e6a4e46</td>
<td>in-use</td>
</tr>
<tr>
<td>636057152</td>
<td>ap-</td>
<td>vol-</td>
<td>snap-</td>
<td>gp2</td>
<td>100</td>
<td>null</td>
<td>available</td>
</tr>
</tbody>
</table>
The sample shown can be augmented by many other fields in this source and sourcetype data. Another useful field is attach_data, which includes the attach time and the deleteOnTermination flag. Knowing these would help you understand the age of volumes and could inform a cost reducing policy that requires justification for volumes that are past a certain age. Delete on termination is the default behavior for root volumes. You may want to expand that behavior to other volumes with data that is considered ephemeral. If the data needs to be retained, then having the age of the volume is used for archiving decisions.

Inventory data such as usage, age and location can be used to find efficiencies, which are important in a cloud environment due to usage fees. This type of information can help you maintain infrastructure in the most cost effective way.