Current AWS virtual private cloud infrastructure

You might want to retrieve basic information about your organization’s virtual private cloud (VPC) infrastructure 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

As an administrator, you’d like to have a high level view of every Virtual Private Cloud (VPC) currently configured in AWS, as well as its current availability and Classless Inter-Domain Routing (CIDR) range.

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="*:vpcs" sourcetype="aws:description"
   |dedup id sortby -_time
   |table account_id region id cidr_block state
   |sort +state
   ```

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.

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

<table>
<thead>
<tr>
<th>Source Code</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| `source=":vpcs"`  
  `sourcetype="aws:description"` | Search only your VPC instances and filter by description data. |
| `|dedup id sortby -_time` | Remove duplicate instances by ID and sort the remaining results with the most recent instances first. |
| `|table account_id region id cidr_block state` | Display the results in a table with columns in the order shown. |
| `|sort +state` | Sort the results by state in ascending order. |

### Result

Sample results for this search are shown in the table below. It shows the number of unique VPCs associated with the account id, as well as the state, cidr_block, and the id of the eVPC itself. These are all fundamental attributes of a VPC.

<table>
<thead>
<tr>
<th>account_id</th>
<th>region</th>
<th>id</th>
<th>cidr_block</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>ap-southeast-1</td>
<td>vpc-40c55125</td>
<td>10.95.0.0/16</td>
<td>available</td>
</tr>
<tr>
<td>63605715280</td>
<td>ap-southeast-1</td>
<td>vpc-311b8f54</td>
<td>10.0.0.0/16</td>
<td>available</td>
</tr>
<tr>
<td>63605715280</td>
<td>ap-southeast-1</td>
<td>vpc-d2d110ba</td>
<td>172.31.0.0/16</td>
<td>available</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.