Current AWS elastic load balancer instances

You might want to retrieve basic information about your elastic load balancer (ELB) instances 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

Your organization has a large number of ELB instances currently deployed to AWS. You want to be able to quickly take an inventory of all of them, as well as their configured fully qualified domain names (FQDN), to better manage your cloud infrastructure.

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="*_load_balancers" sourcetype="aws:description"
|eval name=if(isnull(name),LoadBalancerName,name), vpc_id=if(isnull(vpc_id),VpcId,vpc_id), dns_name=if(isnull(dns_name),DNSName,dns_name), id=((((name . "." . account_id) . "." . region) ."" . region
|dedup id sortby - created_time
|table account_id created_time region name dns_name vpc_id
```

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

```
source="*_load_balancers"
sourcetype="aws:description"
```

**Explanation**

Search only your load balancers and filter by description data.

```
|eval name=if(isnull(name),LoadBalancerName,name),
vpc_id=if(isnull(vpc_id),VpcId,vpc_id),
dns_name=if(isnull(dns_name),DNSName,dns_name),
id=((((name . "#") . account_id) . "#") . region)
```

If the name field is null, set it to the value in LoadBalancer, otherwise set name to name. Repeat for the vpc_id and dns_name fields.

```
|dedup id sortby - created_time
```

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

```
|table account_id created_time region name dns_name vpc_id
```

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

---

**Result**

Sample results for this search are shown in the table below. Created_time is an interesting field to sort on because you could determine how long the ELB has been in service. The table also shows information on network dns, virtual private cloud id, location, and account owner. Other fields that are available but not shown below include subnets, ports, protocols, listener, and instance state and ssl_certificate_id. Depending on the information you are trying to track, these might be of interest to add to the table or track separately.

<table>
<thead>
<tr>
<th>account_id</th>
<th>created_time</th>
<th>region</th>
<th>name</th>
<th>dns_name</th>
<th>vpc_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>2015-11-11T06:00:57.730Z</td>
<td>ap-southeast-1</td>
<td>TestELB3</td>
<td>TestELB2-1018 970143.ap-southeast-1.elb.amazonaws.com</td>
<td>vpc-d2d110ba</td>
</tr>
<tr>
<td>63605715280</td>
<td>2015-11-11T06:00:57.730Z</td>
<td>ap-southeast-1</td>
<td>TATestELB6</td>
<td>TestELB2-1018 970143.ap-southeast-1.elb.</td>
<td>vpc-d2d110ba</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>created_time</th>
<th>region</th>
<th>name</th>
<th>dns_name</th>
<th>vpc_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>2015-12-09T09:01:33.070Z</td>
<td>ap-southeast-1</td>
<td>SaaSQATestELB3</td>
<td>SaaSQATestELB3-792083005.ap-southeast-1.elb.amazonaws.com</td>
<td>vpc-d2d110ba</td>
</tr>
<tr>
<td>63605715280</td>
<td>2015-12-11T05:10:170Z</td>
<td>ap-southeast-1</td>
<td>TAtestelb3</td>
<td>saastestelb-1720685174.ap-southeast-1.elb.amazonaws.com</td>
<td>vpc-d2d110ba</td>
</tr>
<tr>
<td>63605715280</td>
<td>2015-11-12T05:21:170Z</td>
<td>ap-southeast-1</td>
<td>TATestELB5</td>
<td>TestELB1-2109315026.ap-southeast-1.elb.amazonaws.com</td>
<td>vpc-d2d110ba</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.