List of Azure resource public IP addresses

You might want a comprehensive list of IP addresses in your environment when doing the following:

- Managing Azure cloud infrastructure

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Microsoft Azure resource data
- Splunk Add-on for Microsoft Cloud Services

Example

As an administrator, you want to have a high-level view of the number of IP addresses in your Azure infrastructure, as well as their location and allocation method.

To optimize the search shown below, you should specify an index and a time range.

1. Run the following search:

   ```sh
   sourcetype=mscs:resource:publicIPAddress
   |stats count BY location, name, properties.publicIPAddressVersion, properties.publicIPAllocationMethod
   |fields - count
   |rename location AS Location name AS Name properties.publicIPAddressVersion AS Version properties.publicIPAllocationMethod AS "Allocation Method"
   ```

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>sourcetype=mscs:resource:publicIPAddress&quot;</td>
<td>Search only Azure resource public IP address data.</td>
</tr>
</tbody>
</table>
## Splunk Search

```splunk
|stats count BY location, name, properties.publicIPAddressVersion, properties.publicIPAllocationMethod|
```

### Explanation

Count the number of instances for a combination of location, IP address, version, and allocation method. Return one row for each distinct combination of values.

```splunk
|fields - count|
```

### Explanation

Remove the count field from the results.

```splunk
|rename location AS Location name AS Name properties.publicIPAddressVersion AS Version properties.publicIPAllocationMethod AS "Allocation Method"|
```

### Explanation

Rename the fields as shown for better readability.

## Result

Sample results for this search are shown in the table below. The results show all the public IP addresses provisioned in the environment. This data could be the foundation for asset management data collection. Inventory and asset management tracking is considered a best practice in the ITIL framework. A search like this can be used to gather information on provisioned assets, in this case virtual networks. Asset management is critical in the cloud because it affects operation expenses, as well as security, and informs lifecycle management. Public IP addresses are not free.

<table>
<thead>
<tr>
<th>Location</th>
<th>Name</th>
<th>Version</th>
<th>Allocation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>australiaeast</td>
<td>CentOS-ip</td>
<td>IPv4</td>
<td>Dynamic</td>
</tr>
<tr>
<td>australiaeast</td>
<td>ChiefConverseOfficer-ip</td>
<td>IPv4</td>
<td>Static</td>
</tr>
<tr>
<td>australiaeast</td>
<td>Forum2019-ip</td>
<td>IPv4</td>
<td>Dynamic</td>
</tr>
<tr>
<td>australiaeast</td>
<td>RHEL-ip</td>
<td>IPv4</td>
<td>Dynamic</td>
</tr>
<tr>
<td>australiaeast</td>
<td>Test-ip</td>
<td>IPv4</td>
<td>Dynamic</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.