List of Azure resource network interface cards

A network interface card (NIC) is a component that holds the public and private IP address of a virtual machine. You might want a comprehensive list of NICs 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 Cloud Services network data
- Splunk Add-on for Microsoft Cloud Services

Example

As an administrator, you want to have a high-level view of the number of NICs in your Azure infrastructure, along with their source network and source virtual machine.

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

1. Run the following search:

   ```bash
   sourcetype="mscs:resource:networkInterfaceCard"
   |rex field=virtual_network_id "virtualNetworks\(<\?<Network>\>\)"
   |rex field=vm_id "virtualMachines\(<\?<vm>\>\)"
   |stats count BY location, name, properties.ipConfigurations{}.properties.privateIPAddress, properties.ipConfigurations{}.properties.privateIPAllocationMethod, Network, vm
   |fields - count
   |rename location AS Location name AS NIC properties.ipConfigurations{}.properties.privateIPAddress AS "Private IP" properties.ipConfigurations{}.properties.privateIPAllocationMethod AS "Allocation Method" Network AS "Source Network" vm AS "Source VM"
   ```

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 | Explanation
---|---
sourcetype="mscs:resource:networkInterfaceCard" | Search only Azure resource network interface card usage data.
| rex field=virtual_network_id "virtualNetworks\/(?<Network>.+)" | Extract the network ID from the full path name.
| rex field=vm_id "virtualMachines\/(?<vm>.+)" | Extract the virtual machine name from the full path name.
| stats count BY location, name, properties.ipConfigurations{}.properties.privateIPAddress, properties.ipConfigurations{}.properties.privateIPAllocationMethod, Network, vm | Count the number of instances for a combination of location, name, IP address, allocation method, and source network, and VM. Return one row for each distinct combination of values.
| fields - count | Remove the count field from the results.
| rename location AS Location name AS NIC properties.ipConfigurations{}.properties.privateIPAddress AS "Private IP" properties.ipConfigurations{}.properties.privateIPAllocationMethod AS "Allocation Method" Network AS "Source Network" vm AS "Source VM" | Rename the fields as shown for better readability.

Result

Sample results for this search are shown in the table below. The results show all network interface cards provisioned in the environment, including the name of the virtual machine (VM) that the NIC is contained within. 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.
<table>
<thead>
<tr>
<th>Location</th>
<th>NIC</th>
<th>Private IP</th>
<th>Allocation Method</th>
<th>Source Network</th>
<th>Source VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>australiaeast</td>
<td>ry-win10746</td>
<td>10.0.0.4</td>
<td>Dynamic</td>
<td>bots-vnet</td>
<td>Ry-Win10</td>
</tr>
<tr>
<td>australiaeast</td>
<td>splunk64</td>
<td>10.0.0.4</td>
<td>Dynamic</td>
<td>bots-vnet</td>
<td>Splunk</td>
</tr>
<tr>
<td>australiaeast</td>
<td>splunkhf01402</td>
<td>10.1.0.4</td>
<td>Dynamic</td>
<td>splunk</td>
<td>SPLUNKHF01</td>
</tr>
<tr>
<td>centralus</td>
<td>ryan726</td>
<td>10.0.6.4</td>
<td>Dynamic</td>
<td>ryan</td>
<td>Ryan</td>
</tr>
<tr>
<td>southcentralus</td>
<td>WVD-Win10-0-nic</td>
<td>10.0.1.5</td>
<td>Dynamic</td>
<td>frothly-vnet</td>
<td>WVD-Win10-0</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.