Inventory of devices reporting network data

You need broad network visibility to set the stage for availability monitoring and alerting should devices stop sending data. You know that the best place to start is obtaining an inventory of every device on the network.

Data required

System log data

To collect SNMP traps in Splunk, you will need to run an snmptrapd server on a Linux or Windows machine to collect traps and write them to a file. After they are written to disk, you can configure the Universal Forwarder to read those files and forward them to Splunk; this configuration is outlined in our documentation.

Procedure

1. Ensure you have configured Splunk Connect for Syslog.
2. If you are switching to Splunk software from another vendor, front SC4S with the same IP address that your previous software used to collect syslog traffic. Doing so helps prevent the need to reconfigure all network devices and firewall rules that would be necessary to allow syslog traffic to flow to a new syslog receiver.
3. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```splunk
index IN (*) sourcetype IN (*) sc4s_vendor_product=* | stats count BY host, sourcetype, sc4s_vendor_product
```

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>index IN (<em>) sourcetype IN (</em>) sc4s_vendor_product=*</td>
<td>Search all data coming into the Splunk Connect for Syslog app.</td>
</tr>
<tr>
<td></td>
<td>Display a count of the source types and related products for each host on your network.</td>
</tr>
</tbody>
</table>
Next steps

To further restrict your search, limit the search to include only the source types associated with your networking devices. Use the results to determine what needs to be investigated further.

You might be interested in other processes associated with the Recovering lost visibility of IT infrastructure use case.