Problems with a specific network device

If you suspect a particular device is having issues, there will often be evidence of a problem resident in the syslog messages. You want to use Splunk to isolate syslog messages coming from that device and look for messages with elevated severity.

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 (*)
   host=<Hostname/IP of Device> (severity_name IN (emergency, alert, critical, error, warning) OR sc4s_syslog_severity IN (emergency, alert, critical, error, warning))
   ```

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>)</td>
<td>Search the syslog data in the Splunk Connect for Syslog app.</td>
</tr>
<tr>
<td>host=&lt;Hostname/IP of Device&gt;</td>
<td>Search the host or IP of the device you want to investigate.</td>
</tr>
<tr>
<td>(severity_name IN (emergency, alert, critical, error, warning))</td>
<td>Search for specific warning messages.</td>
</tr>
</tbody>
</table>
### Splunk Search

| warning) OR sc4s_syslog_severity IN (emergency, alert, critical, error, warning) |

### Explanation

### 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.