Windows host stops reporting data

Host availability is a critical aspect of IT operations monitoring. You want to monitor and alert on hosts that have become unavailable either because it has gone down, or has otherwise lost its ability to send data to your Splunk deployment.

In Splunk Enterprise or Splunk Cloud Platform, this procedure can operate on any event data which is consistently received from the host including data from the Splunk Add-on for Microsoft Windows add-on.

Data required

Technologies:
- Splunk Enterprise or Splunk Cloud Platform and Splunk Add-on for Microsoft Windows OR
- Splunk Infrastructure Monitoring and the Splunk OpenTelemetry Connector

Data:
- Windows event logs
- Windows update logs

Procedure

Option 1

Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
|tstats dc(host) AS val max(_time) AS _time WHERE index="<index to check>" host="<hosts to check>" BY host |append [[metadata type=hosts index="<index to check>" | table host lastTime | rename lastTime AS _time | where _time>now()-(60*60*12) | eval val=0] |stats max(val) AS val max(_time) AS _time by host | where val=0 | rename val AS "Has Data" | eval Missing Duration= tostring(now()-_time, "duration") | table host "Has Data" "Missing Duration"
```

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>`</td>
<td>tstats dc(host) AS val max(_time) AS _time WHERE index=&quot;&lt;index to check&gt;&quot; host=&quot;&lt;hosts to check&gt;&quot; BY host`</td>
</tr>
<tr>
<td>`</td>
<td>append [</td>
</tr>
<tr>
<td>`</td>
<td>stats max(val) AS val max(_time) AS _time by host`</td>
</tr>
<tr>
<td>`</td>
<td>where val=0`</td>
</tr>
<tr>
<td>`</td>
<td>rename val AS &quot;Has Data&quot;`</td>
</tr>
<tr>
<td>`</td>
<td>eval Missing Duration= tostring(now()-_time, &quot;duration&quot;)`</td>
</tr>
<tr>
<td>`</td>
<td>table host &quot;Has Data&quot; &quot;Missing Duration&quot;`</td>
</tr>
</tbody>
</table>

### Next steps

The metric cpu.utilization is fundamental and should be present on all hosts. Create an alert based on this search so you can proactively manage potential stability issues. To alert when a host is no longer sending data, you can configure one of the following two recommendations:

- Use the SPL from this procedure to configure a Core Splunk alert.
- Build a new Vital Metric in IT Essentials Work for the desired entity type and configure vital metric alerting.

Finally, you might be interested in other processes associated with the Maintaining Microsoft Windows systems use case.

### Option 2

1. Ensure that you have the Splunk OTEL Collector installed on the host you want to monitor.
2. In Splunk Infrastructure Monitoring, use the following SignalFlow to search for hosts not reporting metrics after a fixed period of time.

   ```plaintext
   A = data('cpu.utilization', filter=filter('host.name', '<HOSTS-TO-CHECK>')).publish(label='A')
   ```

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.
Next steps

To alert when a host stops reporting data, use the SignalFlow from this procedure to configure a detector with an alert condition of "Heartbeat Check" and Alert Settings of "Hasn't reported For: 5m".

Finally, you might be interested in other processes associated with the Maintaining Microsoft Windows systems use case.