Current state of Windows services on a host

Many critical IT applications and services running on Windows operating systems run as a Windows Service. If an expected Windows Service is not currently in a running state, it may result in stability issues for a critical application. You want to be able to see the current state one or more services running on a host.

Data required

Windows update logs

Procedure

For an example inputs.conf file that can be deployed to the universal forwarder on the Windows host to collect service state information, click here.

1. Verify that you deployed the Splunk Add-on for Microsoft Windows add-on to your search heads, indexer, and Splunk Universal Forwarders on the monitored systems. For more information, see About installing Splunk add-ons.

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

```
host="<name of host to check>" DisplayName="<name of service to check>" sourcetype=WinHostMon source=service
| rename DisplayName AS "Service"
| stats latest(State) AS State BY host Service Path
```

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>host=&quot;&lt;name of host to check&gt;&quot; DisplayName=&quot;&lt;name of service to check&gt;&quot;</td>
<td>Search index(es) where Windows service status data is being collected and filter down to the desired host(s) and service(s) to check.</td>
</tr>
<tr>
<td>sourcetype=WinHostMon source=service</td>
<td>Search only Windows host monitoring data.</td>
</tr>
<tr>
<td></td>
<td>rename DisplayName AS &quot;Service&quot;</td>
</tr>
<tr>
<td></td>
<td>stats latest(State) AS State BY host Service Path</td>
</tr>
</tbody>
</table>
Splunk Search | Explanation
---|---
| the service in the results for additional context.

**Next steps**

Use these results to monitor services and proactively manage potential stability issues.

You might be interested in other processes associated with the [Maintaining Microsoft Windows systems](#) use case.