Windows CPU utilization nearing capacity

Excessive CPU utilization on a host, particularly abnormal or prolonged, is a sign of potential issues with the critical applications running on the host. You want to detect when an application is starved for CPU resources so you can prevent performance degradations or application instability.

Data required

Technologies:

- Splunk Enterprise or Splunk Cloud Platform and [Splunk Add-on for Microsoft Windows](https://www.splunk.com/software/add-ons/windows-monitoring) OR
- Splunk Infrastructure Monitoring and the [Splunk OpenTelemetry Connector](https://www.splunk.com/software/open-telemetry)

Data:

- [Windows event logs](https://docs.microsoft.com/en-us/Windows/winlog)

Procedure

Option 1

1. In Splunk Enterprise or Splunk Cloud Platform, verify that you deployed the [Add-on for Microsoft Windows](https://www.splunk.com/software/add-ons/windows-monitoring) add-on to your search heads, indexer, and Splunk Universal Forwarders on the monitored systems. For more information, see [About installing Splunk add-ons](https://www.splunk.com/help/add-ons/about-installing-splunk-add-ons).

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

   ```splunk
   | mstats min(Processor.%_Idle_Time) AS "processor_idle_time" WHERE index="<name of Windows metrics index>" host="<name of host to check>" (instance="_Total" AND object="Processor") BY host span=30s
   | eval processor_active_time=100-processor_idle_time
   | timechart span=1m max(processor_active_time) AS processor_active_time BY host
   ```

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>mstats min(Processor.%_Idle_Time) AS</td>
<td>Search metrics index(s) where CPU utilization data is</td>
</tr>
</tbody>
</table>
Next steps

Set up an alert based on this search so you can proactively manage potential stability issues.

To alert when a CPU utilization is nearing max capacity, you can configure one of the following two recommendations:

- Use the SPL from this procedure to configure a Core Splunk alert.
- Configure the Average CPU Usage vital metric for the Windows entity type in IT Essentials Work to alert when the CPU Utilization percentage is at or near 100.

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 the cpu.utilization streaming metric and filter down to the desired hosts.

   ```
   A = data('cpu.utilization', filter=filter('host.name', '<name of host to check>')).publish(label='A')
   ```

Next steps

To alert when CPU utilization is nearing max capacity for the selected host(s), use the SignalFlow from this procedure to configure a detector with an alert condition of "Static Threshold" and alert settings of:

- Alert when: Above
- Threshold: 95
- Trigger sensitivity: Duration
- Duration: 5m

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

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.
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.