Performance Monitor inputs show maximum values of 100 percent usage for a process on multicore Microsoft Windows machines

Generated: 11/05/2019 3:34 am
Performance Monitor inputs show maximum values of 100 percent usage for a process on multicore Microsoft Windows machines

Introduction

This page discusses how to work around an issue where the standard Performance Data Helper (PDH) APIs cause Performance Monitor inputs to show maximum values of 100% usage for a process on multicore Windows machines, even when the process uses more than one core at a time.

Symptoms

Performance Monitor inputs display maximum values of 100% usage for a process on multicore Windows machines, even when the process uses more than one core at a time.

Cause

A problem was found in the PDH APIs that causes Performance Monitor inputs to show maximum values of 100% usage for a process on multicore Microsoft Windows machines, even when the process uses more than one core at a time. For example, if a process uses 5 of 8 cores on an 8-core machine, the input should return a value of approximately 500, rather than the incorrect 100.

Currently, the input uses the standard Performance Data Helper (PDH) APIs to calculate CPU usage for a process. On multicore systems, the maximum value that PDH APIs return is 100, regardless of the number of cores in the machine that the process uses.

Workaround

To work around this issue:

1. Identify how many processors are in your system. On your Windows deployment, navigate to System information to identify the total number of CPU cores in your deployment.
2. Navigate to $SPLUNK_HOME/etc/system/local/inputs.conf.
3. In the stanza for the Performance Monitor inputs where you want to use the kernel APIs to get process information, set the useWinApiProcStats function to true.
4. Restart Splunk Enterprise.

Each processor core in your system is equal to a maximum processor performance percentage of 100%. So for each core in a multicore windows deployment, 100% is added to the total maximum available processor performance percentage. For example, an 8 core windows environment will have a maximum process capability of 800%.

Total processor capability can be validated in your Splunk platform deployment by navigating to Data inputs > Local performance monitoring> Select system.

When this setting is configured to true, the Performance Monitor input uses process kernel mode and user mode times to calculate CPU usage for a process, and the input uses the GetProcessTime() function in the core Windows API to calculate CPU usage for a process, for the following Performance Monitor counters only:

- Processor Time
- User Time
- Privileged Time

The APIs this setting uses are English language only. If your Windows machine uses a non-English system locale, in the same stanza as the Performance Monitor inputs, configure the useEnglishOnly setting to true.