System performance data

Performance logs provide a real-time indication of system health by showing resource usage that, when compared with historical norms, flags performance problems. When measurements deviate from standard or typical parameters, it’s a warning for IT admins to do further investigation. While primarily used for keeping infrastructure up and running, monitoring system performance can also be used to uncover potential security incidents by detecting abnormal activity in performance. In the Common Information Model, system performance data is typically mapped to the Performance data model.

Measures of system activity such as CPU load, memory and disk usage, and I/O traffic are vital signs that show system health. Recording these measures provides a record of system activity over time that shows normal, baseline levels, and unusual events. By registering myriad system parameters, performance logs also can highlight mismatches between system capacity and application requirements, such as a database using all available system memory and frequently swapping to disk.

Application

When your Splunk deployment is ingesting system performance data, you can use it to accomplish observability use cases.

- Maintaining *nix systems
- Maintaining Microsoft Windows systems
- Recovering lost visibility of IT infrastructure

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with system performance data.

- Splunk Add-on for Microsoft Windows
- Splunk Add-on for Unix and Linux