Splunk App for Unix and Linux

The Splunk App for Unix and Linux provides data inputs, searches, reports, alerts, and dashboards for Linux and Unix management. From any place, you can monitor and troubleshoot *nix operating systems of any size. The app includes a set of scripted inputs for collecting CPU, disk, I/O, memory, log, configuration, and user data:

- Get information about who is logged into your system, including last login times and unauthorized login attempts.
- Find out how much network throughput and bandwidth your system is using.
- Determine the status of current running processes on your system, and who is running them.
- Learn what software is installed on your system.

Monitored system metrics

The Splunk App for Unix and Linux runs with a Splunk platform instance to gather system metrics, including the following:

- Hardware information: CPU type, count, and cache; hard drives; network interface cards, count, and memory, as well as CPU statistics.
- Disk information, including available disk space and associated input/output statistics for devices and partitions.
- Information about the configured network interfaces, including connections, routing tables, and TCP/UDP transfer statistics.
- User statistics, including last login times for system accounts, user attributes, and security-related information.
- Information about processes, the files they open, and other resources they use.

The app has pre-built reports and dashboards for visibility into your system's operation.

App Features

Features of the Splunk App for Unix and Linux include the following:

Central Visibility Into Operational Health

Get instant visibility into the operational health of Unix and Linux environments. Organize your hosts by groups of services specific to your environment. Use NOC-like dashboards for central insight into problems and visualize resource consumption of selected systems for easy detection of outliers and anomalies.

Performance and Resource Utilization Analytics

Set multiple customizable thresholds for your CPU and memory utilization across your groups of hosts to easily spot trends and spikes in resource utilization in your infrastructure. Isolate problems with configurable statistical comparisons, using 42 important host and OS metrics. Visualize trends and display side-by-side performance comparisons of the several hosts of interest to understand trends, establish baselines and optimize resource allocations. Quickly cross-compare CPU, RAM and disk historical capacity utilization across many different hosts to identify increased resource consumption.

Threshold-Based Alerts

Get real-time notifications of important events from your Unix and Linux environment using the app's threshold-based alerts. Quickly assess the business impact of events and conduct remediation actions through insight into snapshots of various OS metrics around the time-specific alert fired. Compare the behavior of hosts in your systems and create long-term trends based on the alerts activity in your environment.
**Correlation Across Technologies**

Combine your OS data with data from all other technology tiers, such as applications, virtual, storage, networks and servers to gain a complete, centralized view of KPIs across your enterprise. Use Splunk search language, visualizations and correlations to find causal links across technologies. Get an accurate picture of resource usage and performance across multiple tiers of your IT stack.

**Common Information Model Compatibility**

This app provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security, the Splunk App for PCI Compliance, and Splunk IT Service Intelligence.

**Additional Information**

Download the Splunk App for Unix and Linux from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk App for Unix and Linux.

See Questions related to the Splunk App for Unix and Linux on Splunk Answers.