Splunk Stream™ Installation and Configuration Manual 7.1.3

About Splunk Stream

Generated: 4/24/2019 5:25 am
About Splunk Stream

Splunk Stream lets you capture, filter, index, and analyze streams of network event data.

A "stream" is a grouping of events defined by a specific network protocol and set of fields. When combined with logs, metrics, and other information, the streams that you capture with Splunk Stream can provide valuable insight into activities and suspicious behavior across your network infrastructure.

Use Splunk Stream to:

- Passively capture live streams of network event data.
- Capture metadata and full packet streams for multiple network protocols.
- Collect NetFlow protocol data.
- Apply aggregation methods for statistical analysis of event data.
- Apply filters to minimize indexer requirements.
- Extract content from strings and generate hashes.
- Extract files from network traffic.
- Monitor network trends and app performance in pre-built dashboards.
- Deploy independent Stream forwarder to capture data on remote linux machines.
- Scale rapidly and unobtrusively with no need for tagging or instrumentation.

For Splunk Stream installation instructions, including a detailed overview of Splunk Stream components, see Install Splunk Stream.

To get started using Splunk Stream to capture network metadata and full network packets, see Configure Streams in the Splunk Stream User Manual.