splunk>

FACT SHEET

Splunk® App for Stream

Enhance Operational Intelligence With Wire Data Capture

HIGHLIGHTS

- Expand the potential of machine data with real-time insights from wire data
- Augment operational intelligence for IT, security and the business, without instrumentation
- Gain visibility into any public, private or hybrid cloud infrastructure by collecting wire data with a single software solution
- Control the amount of wire data ingested with fine-grained protocol and attribute filtering
- Enable fast deployment, accelerate incident response, and scale-out wire data collection across the enterprise with interface-driven installation, management and customization

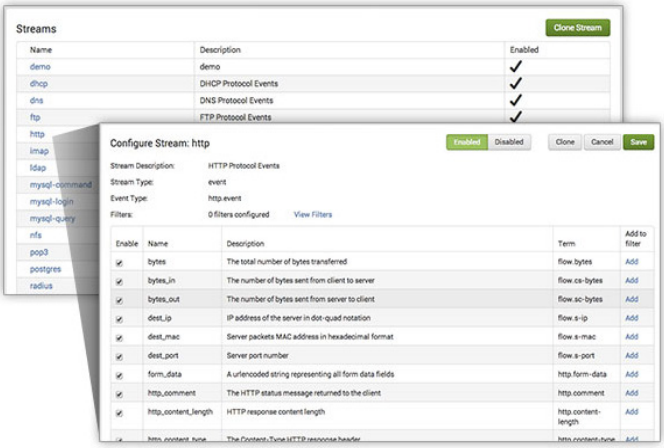
Wire data, the data communicated over the network, is an important source of information about business activity, application performance, security and infrastructure issues. This data can provide granular insights into payloads, web interactions, infrastructure and application response times, customer user/usage experiences and more. When correlated with other machine-generated data, wire data can enhance operational intelligence.

Given the high volume, velocity and variety of wire data, extracting real-time insights at scale presents several challenges. Traditional methods require manual instrumentation at routers, gateways and switches, and exporting slices of data into third-party tools. Alternatively, appliance-based solutions capture wire data from the network perimeter and are inflexible. Both methods make it difficult to acquire data from endpoints in public cloud infrastructures, creating data gaps. Furthermore, these solutions do not allow for on-the-fly configuration, customization and filtering.

Splunk App for Stream

The Splunk App for Stream is a simple and scalable software solution that captures real-time wire data from distributed infrastructures. These include private, public and hybrid clouds with on-the-fly deployment and fine-grained filtering capabilities.

Capture wire data from endpoints (such as physical or virtual machines), routers and switches, without instrumentation, so it can be analyzed in real time with Splunk software. Splunk customers can enhance operational intelligence by correlating this new class of data with other machine-generated data.



Using Wire Data to Support Splunk Use Cases

Wire data can extend every Splunk use case across IT and the business:

Application Management—gain granular visibility into application performance; transaction traces, paths and response times; network performance and even database queries, without the need for instrumenting applications or modifying application logs.

Infrastructure Operations—pinpoint the root cause of issues faster. Map dependencies of critical infrastructure services and ensure the delivery of services at the levels required by the business.

Combine application and infrastructure logs with granular wire data in Splunk software for a complete view of application availability, performance and usage in relation to the underlying infrastructure components. Accelerate time-to-resolution, establish better baselines and trends, and enable IT to make informed business decisions.

Security—proactively monitor and avoid attacks and exfiltration. Drive sophisticated analytics for threat detection, incident response, intelligence gathering and threat prevention with granular data on headers, payload and more. Accelerate incident response with simple and rapid deployment to collect wire data.

Business Analytics—capture all web interactions for a deeper understanding of user experience to improve customer satisfaction, prevent drop-offs, improve conversions and boost online revenues. Gain real-time business insights across critical business processes such as retail, provisioning in telecoms, trade execution in financial services and more.

Features of the Splunk App for Stream

Product/App Features

- Capture wire data across distributed infrastructures, from the network perimeter and endpoints in public, private or hybrid clouds using a single software solution
- Control and manage wire data volumes with fine-grained precision by selecting or deselecting protocols and associated attributes within the app interface
- Clone built-in streams, and define filters and aggregation rules to capture meaningful data for analyses
- Whitelist or blacklist data capture from specific IP addresses and subnets with the interface
- Decrypt SSL-encrypted traffic with private keys for data completeness
- Scale the installation and configuration with interface-driven installation and centralized management
- Correlate application and infrastructure data such as logs, events and metrics with wire data to gain valuable insights and enhance operational intelligence

Product Requirements:

All instances of the Splunk App for Stream must run Splunk Enterprise v6.0 or later. The Splunk App for Stream comes prepackaged with a Splunk Stream forwarder (v6.0). The Splunk forwarder is supported on Linux 32-/64-bit and Mac OSX 64-bit kernels (with limited protocol support on the Mac OSX platform).

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 apps.splunk.com

© 2014 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Hunk, Splunk Cloud, Splunk Storm and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.

Item # FS-Splunk-Stream-102