splunk>

TECH BRIEF

Splunk Enterprise 6: Forwarders

Reliable and Secure Data Collection From Remote Sources

HIGHLIGHTS

- Forward data from remote systems securely in real time
- Minimal resource overhead and minimal impact on endpoint performance
- Universal install supports thousands of different machine data formats
- Monitor thousands of remote systems across multiple geographies from a central interface

Collecting Machine Data From Remote Sources

Machine data consists of all of the data generated by the applications, servers, network devices, security devices, sensors and other technologies that power your organization. But what about the data generated from remote systems? How do you collect remote data as it's being generated so you can analyze it?

Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk Enterprise for indexing and consolidation. They support universal installation and do not require customization for the hundreds or thousands of machine data sources that exist in your technology infrastructure. Forwarders can scale to tens of thousands of remote systems, collecting terabytes of data with minimal impact on performance.

Key Capabilities

Forwarders can be deployed rapidly using an existing deployment solution or by leveraging the Splunk Enterprise Deployment Server. Once deployed, Forwarders will gather machine data securely from remote systems.

Key features include:

- Tagging of metadata (source, sourcetype and host)
- Configurable buffering
- Data compression
- SSL security
- Use of any available network ports
- Running scripted inputs locally

Forwarders support virtually any machine data format and run on all modern operating systems (see *Figure 1*). There are no database schemas, parsers or connectors to design, deploy or purchase.

Types of Forwarders

- The Universal Forwarder is a streamlined, dedicated version of Splunk Enterprise that contains only the essential components needed to forward data. It has no searching, indexing or alerting features, does not parse data and does not include a bundled version of Python. Universal Forwarders have a default transfer rate of 256Kbps
- A Heavy Forwarder is a full Splunk Enterprise instance, with some features disabled to achieve a smaller footprint

Reliable and Secure Data Collection

Forwarder communications occur on TCP sockets, rather than best-effort and unsecured UDP network ports, so message delivery is guaranteed. Forwarders can detect a network outage and automatically failover to another target Indexer or buffer events locally until the target Indexer is available again. Additionally, Indexers can be configured to provide index-side acknowledgement that data was received. Communication between a Forwarder and receiver is completed using SSL authentication and encryption.

Flexible Data Routing

Splunk Enterprise supports many different data centralization architectures. Forwarders can load balance data between multiple Indexers, route data in raw format to integrate with third party systems, clone data to allow for high availability and conditionally route data to different locations to support multi-tenant environments.

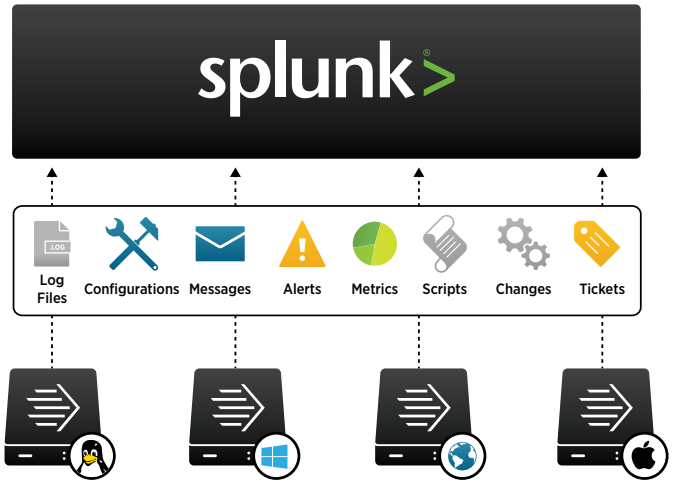

Figure 1: Machine data can be forwarded to Splunk Enterprise from remote sources.

Centralized Management

Splunk Enterprise 6 provides centralized Forwarder Management to simplify the administration of hundreds or thousands of Forwarders in your environment (see *Figure 2*). Forwarder Management includes a visual interface to deploy thousands of configurations, monitor the status of rollouts and track down errors.

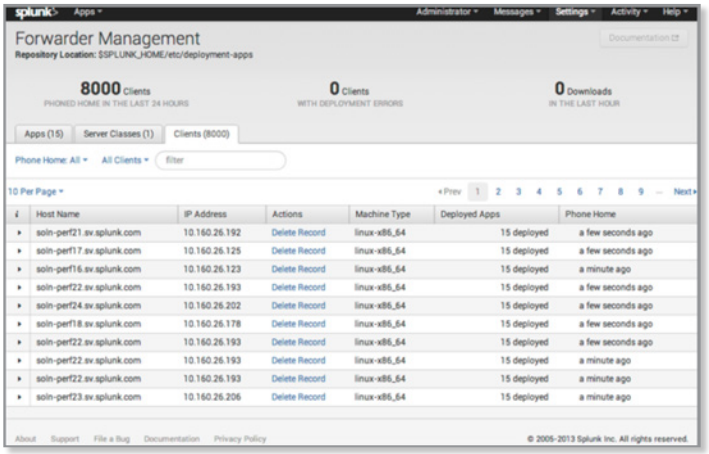

Figure 2: Forwarder Management simplifies the administration of thousands of Forwarders around the world.

Splunk Enterprise 6 is Software. Get Up and Running in Minutes. Forwarders are a key part of your deployment. Download and install Splunk Enterprise on your laptop or server in under five minutes. You'll be up and running with an intuitive web user interface and a powerful enterprise platform for indexing your machine data.

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.

Features	Splunk Free	Splunk Enterprise
Indexing Volume	500MB/day	Unlimited (According to license)
Universal Indexing	•	•
Search	•	•
Distributed Search		•
Monitoring and Alerting		•
Reporting	•	•
Knowledge Mapping	•	•
Dashboards	•	•
Data Model	•	•
Pivot	•	•
High Performance Analytics Store	•	•
Report Acceleration	•	•
PDF Delivery		•
Access Control and Single Sign-On		•
Clustering		•
Cluster Management		•
Universal Forwarder	•	•
Forwarder Management	•	•
Rich Developer Environment	•	•
Splunk Apps	•	•
Premium Apps		•
Standard Support	•	•
Enterprise Support		•

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

Item # TB-Splunk-Forwarder-106