splunk>

TECH BRIEF

Splunk® Enterprise 6.2: 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
- Supports collection of thousands of different machine data formats
- Forwarders integrate with data onboarding wizard and advanced field extraction to streamline data preparation
- Centrally monitor thousands of remote systems across multiple geographies from Splunk Enterprise or Splunk Cloud

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 various sources and deliver the data to Splunk Enterprise or Splunk Cloud for indexing and analysis. They support universal installation and do not require customization for the vast array of machine data sources that exist in your technology infrastructure. The Splunk Deployment Monitor can scale to tens of thousands of forwarders, providing centralized management and configuration.

Key Capabilities

Forwarders can be deployed rapidly using either an existing deployment solution like SCCM, Chef or Puppet. Once deployed, forwarders gather machine data securely from up to tens of thousands of remote systems

Key features include:

- Tagging of metadata (source, sourcetype and host)
- Configurable buffering
- Data compression
- SSL security
- Use of any available network ports
- Ability to run scripted inputs locally
- Ability to persist data in case of intermittent connectivity
- Availability on all OS platforms including Windows, Linux and Unix

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 self-contained software that enables the secure, reliable delivery of data to Splunk Enterprise instances. It provides 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

Forwarders communicate using 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 indexer can be configured to use SSL authentication and encryption.

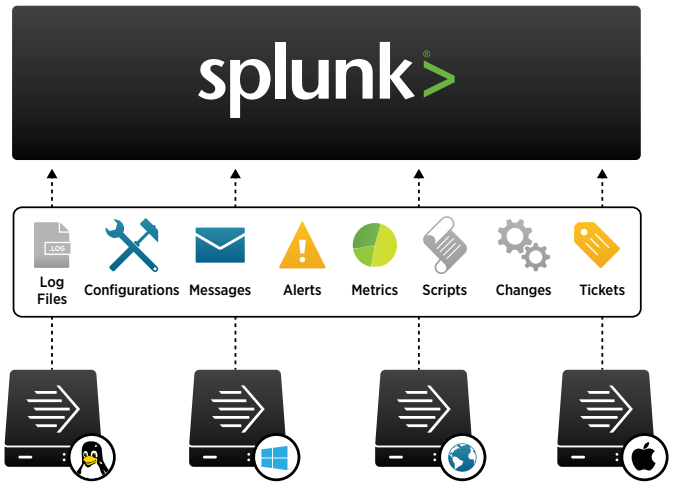

Figure 1: Machine data can be forwarded to Splunk Enterprise from remote sources.

Flexible Data Routing

Splunk Enterprise supports many different data architectures and footprints. 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 multitenant environments.

Centralized Management

Splunk Enterprise 6.2 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. Forwarders can also be remotely managed and configured via the Splunk REST API.

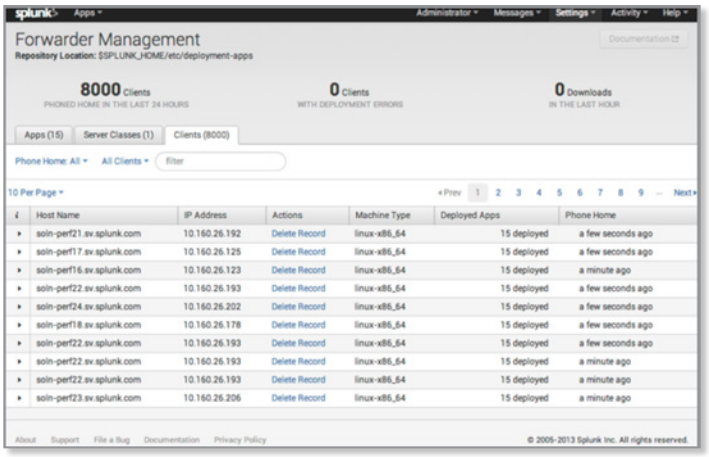

Figure 2: Forwarder management simplifies the administration of thousands of forwarders around the world.

Splunk Enterprise 6.2 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

Splunk Enterprise. Download Splunk Enterprise for free. You'll get a Splunk Enterprise 6.2 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.

Splunk Cloud. Sign up for Splunk Cloud, which delivers Splunk Enterprise as a service. Currently available in the U.S.A. and Canada.

Features	Splunk Free	Splunk Enterprise	Splunk Cloud
Indexing Volume	500MB/day	Unlimited According to license	5GB/day to TB/day According to license
Data Onboarding	•	•	•
Universal Indexing	•	•	•
Search	•	•	•
Distributed Search		•	
Monitoring and Alerting		•	•
Reporting	•	•	•
Knowledge Mapping	•	•	•
Dashboards	•	•	•
Data Model	•	•	•
Pivot	•	•	•
Event Pattern Detection	•	•	•
High Performance Analytics Store	•	•	•
Report Acceleration	•	•	•
Embedded Reports	•	•	•
PDF Delivery		•	•
Access Control & Single Sign-On		•	•
Single-Site Clustering		•	
Multisite Clustering		•	
Distributed Management Console		•	
Universal Forwarder	•	•	•
Forwarder Management	•	•	•
Rich Developer Environment	•	•	•
Apps	•	•	•
Premium Apps		•	•
Standard Support	•		
Enterprise Support		•	•

*Splunk Cloud is currently available in the U.S.A. and Canada

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

Splunk Product Features & Descriptions

Features	Definitions
Indexing Volume	Maximum indexing volume per day
Data Onboarding	Wizard-based workflow to simplify onboarding of any data source
Universal Indexing	Universal real-time indexing of machine data
Search	Ad hoc search across real-time and historical data
Distributed Search	Search across multiple Splunk deployments; supports load balancing and failover
Monitoring and Alerting	Monitor and alert for individual and correlated real-time events
Reporting	Ad hoc reports across real-time and historical data
Knowledge Mapping	Knowledge mapped to machine data artifacts
Dashboards	Highly customizable and interactive dashboards integrating real-time machine data and charts, reports and tables
Data Model	Used to define consistent relationships in machine data
Pivot	Drag-and-drop UI to explore, manipulate and visualize machine data
Event Pattern Detection	Automatically discovers patterns and commonalities in your data with a single click
High Performance Analytics Store	High performance analytics technology
Report Acceleration	Transparent data summarization technology
Embedded Reports	Embed charts and reports in other third-party business applications external to Splunk Enterprise
PDF Delivery	Scheduled and automated PDF generation and delivery of reports and dashboards
Access Control & Single Sign-On	Integrated role-based access control and user authentication with LDAP directory and single sign-on integration
Single-Site Clustering	High availability architecture for machine data availability in a single site deployment
Multisite Clustering	High availability architecture for disaster recovery in a multisite deployment
Distributed Management Console	Centrally manage the health and performance of distributed Splunk deployments
Universal Forwarder	Forwarding of data securely and reliably from remote systems in real time
Forwarder Management	UI for monitoring and deploying forwarder configurations
Rich Developer Environment	Developer platform for building enterprise apps that leverage Splunk software with modern web languages
Apps	Access to hundreds of partner, community and Splunk Apps from apps.splunk.com
Premium Apps	Access to premium Splunk Apps
Standard Support	Access full product documentation, Splunk Apps, Splunk Answers and IRC channel
Enterprise Support	Direct access to Splunk customer support, ability to manage cases online, tailored support levels

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

Item # TB-Splunk-Forwarder-110