

Splunk Forwarders

The Benefits of Deploying Splunk

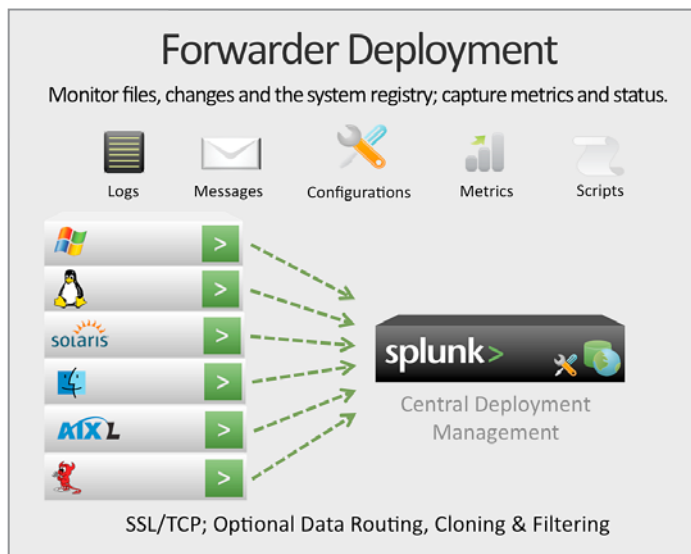
Some Data Is Not Available Remotely

No one likes deploying more software but sometimes there isn't another way to get the data that you need. Splunk forwarders are not like traditional agents: they are light weight and can be deployed in minutes at no additional cost.

Each component in your infrastructure generates data locally but very few provide the built-in capabilities for pushing that data to a central location. For a few technologies there are agentless solutions that claim to achieve this—however they typically don't cover all the data you need. WMI for Windows is one exception but it can quickly run into scalability issues. Syslog for network devices is another but since a syslog process must be running locally syslog is, in effect, an agent too.

There are also many agent-based solutions. Third-party vendors provide agents for specific data types or sources, such as Snare for Windows Event Logs or Tripwire for change monitoring. Many organizations also script their own custom processes to batch-upload logs to a central location. All these solutions result in a proliferation of agents, each of which is limited in scope, costly to implement and expensive to maintain.

Splunk forwarders can replace multiple specialized agents and help meet different monitoring objectives, from performance to change monitoring and security. Best of all, Splunk does not charge on a per-agent basis.



Options to Fit Your Data Collection Needs

Splunk Enterprise supports virtually any data format and runs on all modern operating systems. There is no database schema and no parsers or connectors to design, deploy or pay for.

Forwarder Options	Universal Forwarder	Heavy Forwarder
Monitor All Supported Inputs	•	•
Routing, Filtering, Cloning	•	•
Splunk Web		•
Python Libraries		•
Event-Based Routing		•
Enterprise support		•

Splunk as a forwarder provides a wide variety of data input mechanisms:

- Monitor Windows Event Logs and poll Windows performance counters
- Monitor Unix environments by capturing output from scripts or commands such as iostat, ps, top, etc.; get stats on other services and applications
- Tail local files and directories
- Detect file changes, Windows registry, and Active Directory change events

Reliable and Secure

Data is reliably transmitted with a Splunk forwarder. Communications occur on TCP sockets rather than best-effort and unsecured UDP network ports, so message delivery is guaranteed. Moreover, 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, Splunk indexers can be configured to provide index-side acknowledgement that data was received.

Data can be securely sent from a Splunk forwarder via SSL. Splunk forwarders can communicate between forwarder and receiver using SSL authentication and encryption.

Flexible Data Routing

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

Light Resource Footprint

Splunk forwarders place minimal load on the local host. Deploy the Universal Forwarder for the smallest overhead, typically less than 1% of a single CPU. Deploy the Heavy Forwarder when increased manageability and flexibility are required but system resources are not quite so limited.

Centralized Management

Splunk provides a central Deployment Server to simplify the administration of hundreds or thousands of forwarders in your environment and a Deployment Monitoring App to keep tabs on your distributed Splunk architecture. More information is available at: <http://docs.splunk.com/Documentation/Splunk/4.2.4/Deploy/Aboutforwardingandreceivingdata>

Free Download

Download [Splunk](#) for free. You'll automatically get all of the Enterprise features of Splunk for 60 days and you can index up to 500 megabytes of data per day. Or if you want to get started right away with an Enterprise license contact sales@splunk.com.