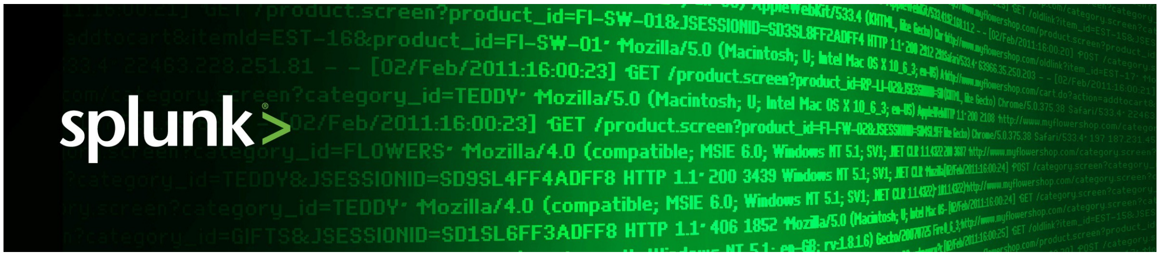


Splunk® Enterprise Installation Manual 7.1.0

Splunk Enterprise architecture and processes

Generated: 5/21/2018 9:07 am

Splunk Enterprise architecture and processes

This topic discusses the internal architecture and processes of Splunk Enterprise at a high level. If you're looking for information about third-party components used in Splunk Enterprise, see the credits section in the Release notes.

Splunk Enterprise Processes

A Splunk Enterprise server installs a process on your host, `splunkd`.

`splunkd` is a distributed C/C++ server that accesses, processes and indexes streaming IT data. It also handles search requests. `splunkd` processes and indexes your data by streaming it through a series of pipelines, each made up of a series of processors.

- **Pipelines** are single threads inside the `splunkd` process, each configured with a single snippet of XML.
- **Processors** are individual, reusable C or C++ functions that act on the stream of IT data that passes through a pipeline. Pipelines can pass data to one another through **queues**.
- New for version 6.2, `splunkd` also provides the Splunk Web user interface. It lets users search and navigate data and manage Splunk Enterprise deployment through a Web interface. It communicates with your Web browser through REpresentational State Transfer (REST).
- `splunkd` runs a Web server on port 8089 with SSL/HTTPS turned on by default.
- It also runs a Web server on port 8000 with SSL/HTTPS turned off by default.

`splunkweb` installs as a legacy service on Windows only. Prior to version 6.2, it provided the Web interface for Splunk Enterprise. Now, it installs and runs, but quits immediately. You can configure it to run in "legacy mode" by changing a configuration parameter.

On Windows systems, `splunkweb.exe` is a third-party, open-source executable that Splunk renames from `pythonservice.exe`. Because it is a renamed file, it does not contain the same file version information as other Splunk Enterprise for Windows binaries.

Read information on other Windows third-party binaries that come with Splunk Enterprise.

Splunk Enterprise and Windows in Safe Mode

If Windows is in Safe Mode, Splunk services do not start. If you attempt to start Splunk Enterprise from the Start Menu while in Safe Mode, Splunk Enterprise does not alert you to the fact that its services are not running.

Additional processes for Splunk Enterprise on Windows

On Windows instances of Splunk Enterprise, in addition to the two services described, Splunk Enterprise uses additional processes when you create specific data inputs on a Splunk Enterprise instance. These inputs run when configured by certain types of Windows-specific data input.

splunk.exe

`splunk.exe` is the control application for the Windows version of Splunk Enterprise. It provides the command-line interface (CLI) for the program. It lets you start, stop, and configure Splunk Enterprise, similar to the *nix `splunk` program.

The `splunk.exe` binary requires an elevated context to run because of how it controls the `splunkd` and `splunkweb` processes. Splunk Enterprise might not function correctly if this program does not have the appropriate permissions on your Windows system. This is not an issue if you install Splunk Enterprise as the Local System user.

splunk-admon

`splunk-admon.exe` runs whenever you configure an Active Directory (AD) monitoring input. `splunkd` spawns `splunk-admon`, which attaches to the nearest available AD domain controller and gathers change events generated by AD. Splunk Enterprise stores these events in an index.

splunk-perfmon

`splunk-perfmon.exe` runs when you configure Splunk Enterprise to monitor performance data on the local Windows machine. This binary attaches to the Performance Data Helper libraries, which query the performance libraries on the system and extract performance metrics both instantaneously and over time.

splunk-netmon

`splunk-netmon` runs when you configure Splunk Enterprise to monitor Windows network information on the local machine.

splunk-regmon

`splunk-regmon.exe` runs when you configure a Registry monitoring input in Splunk. This input initially writes a baseline for the Registry in its current state (if requested), then monitors changes to the Registry over time.

splunk-winevtlog

You can use this utility to test defined event log collections, and it outputs events as they are collected for investigation. Splunk Enterprise has a Windows event log input processor built into the engine.

splunk-winhostmon

`splunk-winhostmon` runs when you configure a Windows host monitoring input in Splunk. This input gets detailed information about Windows hosts.

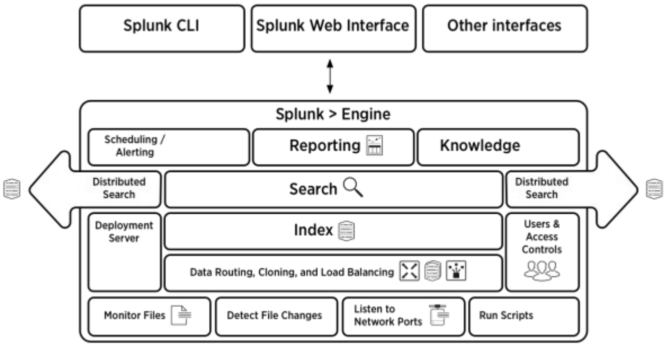
splunk-winprintmon

`splunk-winprintmon` runs when you configure a Windows print monitoring input in Splunk. This input gets detailed information about Windows printers and print jobs on the local system.

splunk-wmi

When you configure a performance monitoring, event log or other input against a remote computer, this program runs. Depending on how you configure the input, it either attempts to attach to and read Windows event logs as they come over the wire, or executes a Windows Query Language (WQL) query against the Windows Management Instrumentation (WMI) provider on the specified remote machine.

Architecture diagram


Splunk CLI
Splunk Web Interface
Other interfaces
Splunk > Engine
Scheduling / Alerting
Reporting
Knowledge
Distributed Search
Search
Distributed Search
Deployment Server
Index
Users & Access Controls
Data Routing, Cloning, and Load Balancing
Monitor Files
Detect File Changes
Listen to Network Ports
Run Scripts