splunk>

Getting Started with Splunk

Take Splunk for a Test Drive

The best way to experience Splunk is to use it for yourself. This guide walks you through step by step in installing Splunk, adding data, searching the data, saving the searches as reports, and creating dashboards. If you're new to Splunk or would like to simply learn more about the platform, this is the place to start!

Total time to complete the guide is about an hour but we encourage you to explore and spend as much time on each step as you see fit. Splunk provides sample data so all you need is a laptop or server to get started.

Lets get started!

- **(5-10min**)** **Part 1: Downloading and installing Splunk Enterprise**
  Takes you through the steps to download, install, and start Splunk on your platform. This chapter is directed towards users who are downloading and starting Splunk for the first time.
  *** depends on the network connection speed*

- **(5 min)** **Part 2: Getting started with Splunk Enterprise**
  Describes Splunk Web, which is the interface for using Splunk Enterprise and Search. Read this chapter to familiarize yourself with Splunk Home and how to navigate the different views in Splunk Web.

- **(6 min)** **Part 3: Getting data into Splunk Enterprise**
  Walks you through adding the tutorial data into Splunk Enterprise. The tutorial data, which is a sample data set composed of web server and MySQL logs for a fictional online game store, is included for download in this chapter. Follow the detailed instructions to add this data to your Splunk instance.

- **(8 min)** **Part 4: Using Splunk Search**
  Describes the parts of Splunk Web you need to to run searches, including the search dashboards, the timerange picker, search actions, and other options. If you've used Splunk Search in previous releases, you should still read this chapter familiarize yourself with new options and other changes.

- **(25 min)** **Part 5: Searching the tutorial data**
  Teaches different ways to search and includes using fields, using the search language, subsearches, and field lookups.

- **(7 min)** **Part 6: Saving and sharing reports**
  Describes the steps to save and share your searches as reports. This chapter also includes mode search examples.

- **(5 min)** **Part 7: Creating dashboards**
  Discusses how to create dashboards targeted to meet different business needs.

splunk>

Getting Started with Splunk

Useful Technical Resources

How To Videos

- Splunk Installation Videos:
  - Installing Splunk on Linux (Video - 4:59)
  - Installing Splunk on Windows (Video - 5:50)
- Splunk Getting Data In Videos:
  - Getting Unix/ Linux Data into Splunk (Video - 2:14)
  - Getting Windows Data into Splunk (Video - 3:14)
- Splunk Basics
  - Splunk Basic Searching (Video – 11:48)
  - Splunk Creating Dashboards (Video – 7:59)

Product Resources

Download Splunk - Multiple operating systems supported (e.g. Linux, Mac, Windows, Solaris, etc.)

Installation guide – Install Splunk Enterprise and the Splunk Forwarder(s)

Getting data into Splunk - Point Splunk Enterprise at data and in moments, you can start searching the data, or use it to create charts, reports, alerts, and other interesting outputs

Common Search Queries/Functions - Frequently used Splunk search commands with descriptions and examples.

Quick Reference Resources

Search Language Quick Reference Card - Available only as a PDF file, is a six-page reference card that provides fundamental search concepts, commands, functions, and examples.

Splunk Search Cheat Sheet – Online quick reference guide and cheat sheet for learning the Splunk Search Language. Also available as a downloadable PDF (8 pages).

Answers

Splunk Answers – Have questions on how to do something with Splunk? Get answers fast.

Social Media

Splunk Online Blogs – All topics Splunk; tips and tricks, customers, dev, customers, etc.
The Splunk Book - Exploring Splunk - Search Processing Language (SPL) Primer and Cookbook
IRC - The Splunk community is 100,000 strong and active 24/7. If you have interest in chatting live with online community members, try out our IRC channel. It consists of people who are experts in Splunk as well as people who are just getting started. What ever your level or interest is, there is always an active discussion happening in our IRC channel.

Best Practices

Getting Data In - When first testing a new data source, it is often easier to just have the file monitored on the local Splunk instance. However, eventually be sure to use the Universal Forwarder to collect the data.

Testing inputs - Use a test index so you can easily test and, if needed, clean the data.

Data Prerequisites – there are a few default fields you must get right at index time; everything else you can create/modify after indexing (aka schema on the fly)

Event breaking – Splunk generally does this automatically, but it is best practice to check that Splunk correctly detected the beginning and end of an event. When you search the index and see that the count is different than what you expect you likely may have multi-line events. Splunk can easily handle this with some simple configuration.

Time stamp – Splunk automatically detects the time stamp but if your log format has a strange time stamp you may need to manually configure the time stamp.

Host - Generally dedicated from the universal forwarder so really only a concern if you are using a syslog server with data from multiple hosts.

Source type: Splunk knows about many source types (ie. access_combined, IIS, syslog, etc) but if you have a custom data source you should set this so that you can easily find it later on by doing queries like sourcetype=my_mobile_api

Index Separation/Customizing - Use a test index when starting out. Eventually, you will want separate indexes based on whether the data has specific retention requirements or if you want to prevent certain users from being able to query the data.

If you can't find what you are looking for or need further assistance please don't hesitate to reach out.

Happy Splunking!