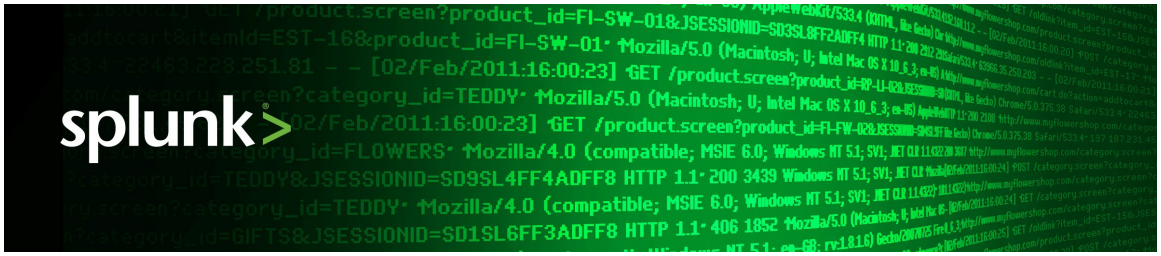


Splunk® Enterprise Search Manual 7.2.4

Get started with Search

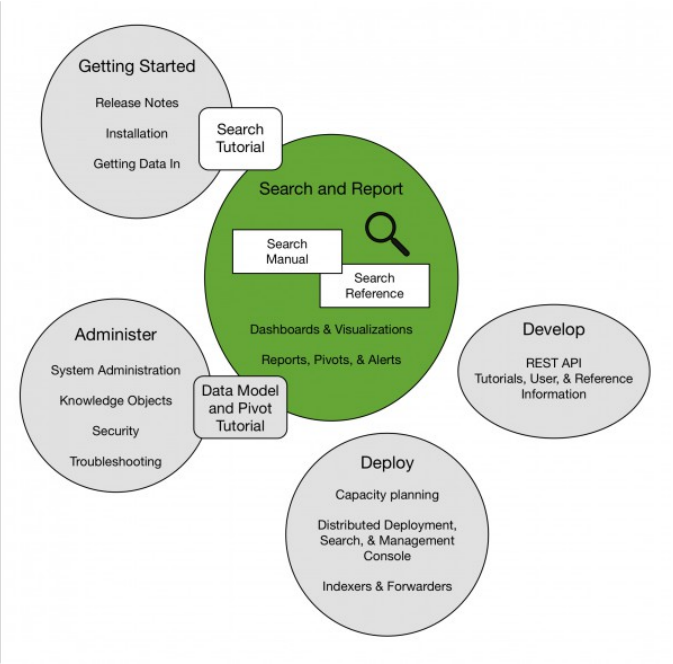
Generated: 11/20/2019 7:21 pm

Copyright (c) 2019 Splunk Inc. All Rights Reserved

Get started with Search

This manual discusses the **Search & Reporting app** and how to use the Splunk search processing language (**SPL**).

The Search app, the short name for the Search & Reporting app, is the primary way you navigate the data in your Splunk deployment. The Search app consists of a web-based interface (Splunk Web), a command line interface (CLI), and the Splunk SPL.



Start Here

If you are new to Splunk Search, the best way to get acquainted is to start with the Search Tutorial. The Search Tutorial introduces you to the Search and Reporting app and guides you through adding data, searching your data, and building simple reports and dashboards.

The Search Tutorial provides a great foundation for understanding Splunk Search.

Getting started in your own environment

After you complete the Search Tutorial, you should learn about the types of data you can explore, how Splunk software indexes data, and about Splunk knowledge objects.

Here are the resources to look at:

- Upload data to your Splunk deployment. See the Getting Data In manual.
- Understand how indexing works. See the Managing Indexers and Clusters of Indexers manual.
- Understand fields and knowledge objects, such as host, source type, and event type. See the Knowledge Manager Manual.

Use the Search app effectively

And of course you need to learn how to use the Search app effectively, which is the focus of this manual. This manual contains detailed information about how to search your data.

Basic Search app skills

- Navigating Splunk Web
- Using the Search app
- Types of searches
- Types of commands

Detailed Search information

- Retrieving events
- Specifying time ranges
- Optimizing searches

- Creating tables and charts
- Evaluating and manipulating fields
- Calculating statistics and advanced statistics
- Grouping and correlating events
- Managing search jobs

Search command reference

For a catalog of search commands and arguments that make up the Splunk SPL, see the *Search Reference*.

Distributed Search

If you are using Splunk Enterprise, **distributed search** provides a way to scale your deployment by separating the search management and presentation layer from the indexing and search retrieval layer. For an introduction to distributed search, see the *Distributed Search Manual*.

See also

Navigating Splunk Web
Using Splunk Search