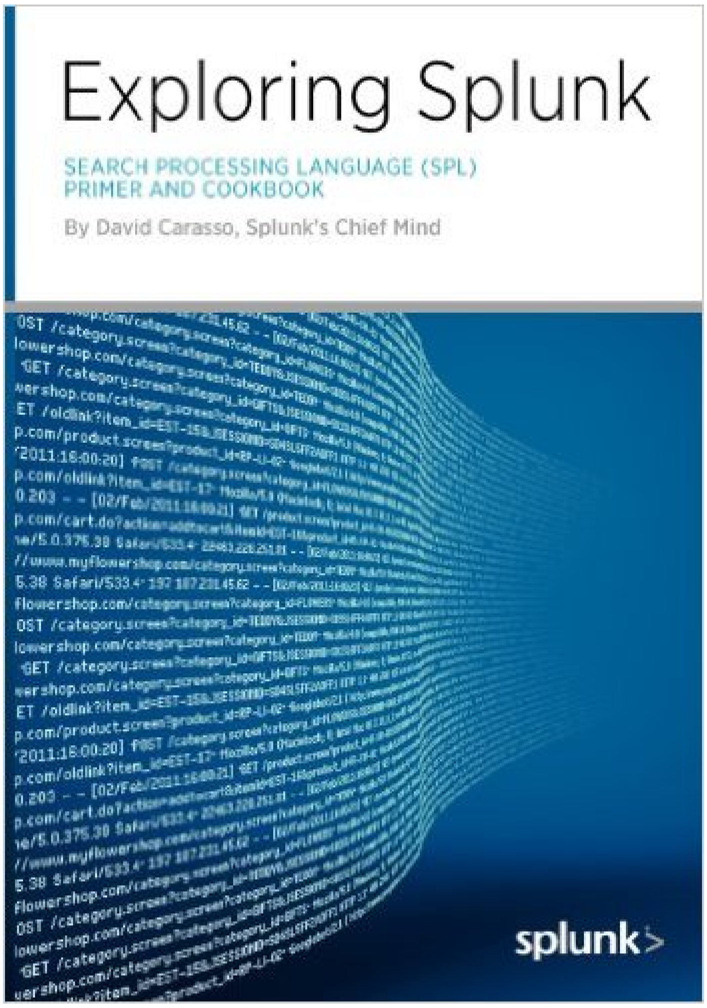
Exploring Splunk


Exploring Splunk
SEARCH PROCESSING LANGUAGE (SPL)
PRIMER AND COOKBOOK
By David Carasso, Splunk's Chief Mind
splunk>

Synopsis

Big data has incredible business value, and Splunk is the best tool for unlocking that value. Exploring Splunk shows you how to pinpoint answers and find patterns obscured by the flood of machinegenerated data. This book uses an engaging, visual presentation style that quickly familiarizes you with how to use Splunk. You’ll move from mastering Splunk basics to creatively solving real-world problems, finding the gems hidden in big data. Â Part I: Exploring Splunk Chapter 1 tells you what Splunk is and how it can help you. Chapter 2 discusses how to download Splunk and get started. Chapter 3 discusses the search user interface and searching with Splunk. Chapter 4 covers the most commonly used search commands. Chapter 5 explains how to visualize and enrich your data with knowledge. Part II: Solution Recipes Chapter 6 covers the most common monitoring and alerting solutions. Chapter 7 covers the most common transaction solutions. Chapter 8 covers the most common lookup table solutions.

Book Information

Paperback: 168 pages

Publisher: CITO Research (August 6, 2012)

Language: English

ISBN-10: 0982550677

ISBN-13: 978-0982550670

Product Dimensions: 7 x 0.4 x 10 inches

Shipping Weight: 9.6 ounces (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (16 customer reviews)

Best Sellers Rank: #643,463 in Books (See Top 100 in Books)   #369 inÂ Books > Computers & Technology > Databases & Big Data > Data Mining

Customer Reviews

This book is available from the Spunk website for free in many forms, including for Kindle.I do recommend it as a great resource as well. Just not sure you need to pay for it   ˆ‰[...]

I wish I had this book when I began working with Splunk. For those who don’t know what Splunk is, be patient. Splunk is many things: logging tool, log correlation tool, SIEM, operations and maintenance tool, monitoring, log search, etc. I have not seen a direct competitor than can compete in more than one or two market spaces with Splunk. It is flexible, simple to ramp up on, scalable, and powerful. I can replace scripts, each script having take weeks to build and debug, within minutes with Splunk. More importantly, another tech can follow behind me later without needing to be a Perl programmer.This book condenses the learning stages contained on the Splunk site into a primer. Yes, a version is free on splunk.com for ebook readers. But I like having the paper copy in my hands. This is for Splunkers what Scott Kelby publishes for photographers: dense, to the point, and recipe format solutions. The "Chief Mind" covers lots of concepts, commands, functions, etc, and provides some real solutions for functionality, such as monitoring for devices that have not logged in a given window of time.

I bought this book because there was some talks about moving towards Splunk and I thought I would get a head start. I had never had any prior experience with it before I ordered the book. The first couple of chapters are an introduction but as you progress you will need to download Splunk to get user friendly with it. Over all this book is good and based on what I have seen may be the best book on Splunk out there right now.

"Exploring Splunk", the first book about Splunk is spot on. It is for both the beginning user who’s just wondering what Splunk is all about to the experienced user who could use just a few more arrows in their quiver.Author David Carasso does an excellent job of giving us a bit of Splunk history, and helps us understand how Splunk works, he does not force us to read the whole book to get value of out of this publication. One can use this as a tutorial, or a quick reference guide. Exploring Splunk explains a lot about the product, but more importantly provides enough examples in each area so that the commands you’re interested in using are easy to follow. Whats really great about Exploring Splunk is nearly half of the book are "recipes" on how to accomplish tasks or "solve word problems" with Splunk.If you didn’t make it to the end, skip to it right now! Appendix E: has a great Quick Reference Guide that you’ll use all the time. Well done!

I just wanted to say thank you to the Author, David Carasso, for this first book on Splunk! If you are scratching your head when it comes to creating simple searches as a new user or you need something more complicated to analyze all that data that Splunk just indigested, then "Exploring Splunk" is all that you need. The book is full of examples and "recipes" just like the other reviewer stated and it’s extremely comprehensive,I recommend this book to any "Splunkologist".

I installed Splunk, got started with the tutorial, read the documentation and the help forum...Still it was this book that helped me to map data without a timestamp and showed me examples of the true power of Splunk.I feel I am now totally up-to-speed and on my way to become a Splunk expert!

While this book is pretty old for a technology book, it has aged well. A great deal for the price. It is the first published Splunk book, written by the late David Carasso, Splunk's Chief Mind. David was one of the very first Splunk employees and a key designer of the SPL.If any book about Splunk technology can become a classic, this one might. (Although a book about a specific technology, like Splunk, probably won't ever really be a classic...) The book is partly about how to do things in Splunk, but it is also pretty general; it probably serves best as an introduction. It was written for a fairly wide audience; most non-technical people will probably only want/need to read the first few chapters.

The material in the book didn't seem to deviate much from the publicly available documentation. I was expecting to get a better insight on the internals of Splunk but instead was presented with a user manual.

Download to continue reading...

Dmca