Splunk Essentials - Second Edition

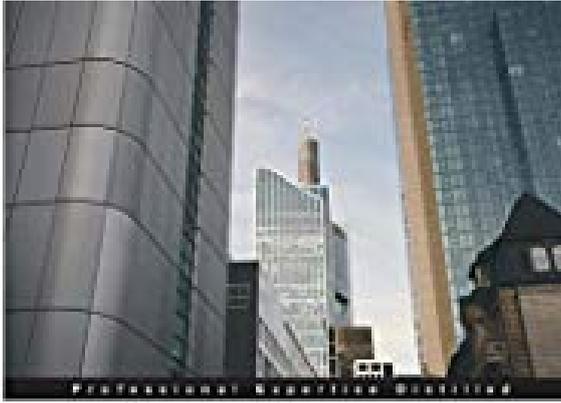|	
Pages:	236
ASIN	B01AJST0TY
Language	English
Author:	Betsy Page Sigman
Genre:	Uncategorized
Goodreads Rating:	3.82
Published:	September 30th 2016 by Packt Publishing

Splunk Essentials - Second Edition.pdf

Splunk Essentials - Second Edition.epub

A fast-paced and practical guide to demystifying big data and transforming it into operational intelligence About This Book   Want to get started with Splunk to analyze and visualize machine data? Open this book and step into the world of Splunk Leverage the exceptional analysis and visualization capabilities to make informed decisions for your business with the help of this example-rich guide This easy-to-follow, practical book can be used by anyone, even if you have never managed any data before This book will be perfect for you if you are a Software engineer or developer who needs real-time access to log files, performance counters, and trending analysis to assist in their development pipeline.

 It is also suitable for System administrators who require visibility on the state of all systems to conform with operational SLAs and to hasten incident resolution. It is also useful to Business analyst who seek to correlate machine data with business metrics and provide intuitive real-time and statistical visualizations. It can also be used as a companion book by Students who wish to learn about a technical tool that is widely used in all enterprises. What You Will Learn   Install and configure Splunk Gather data from different sources, isolate them by indexes, classify them into source types, and tag them with the essential fields Be comfortable with the Search Processing Language and get to know the best practices in writing search queries Create stunning and powerful dashboards Be proactive by implementing alerts and scheduled reports Use the Splunk SDK and integrate Splunk data into other applications Implement the best practices in using Splunk In Detail Splunk is a search, analysis, and reporting platform for machine data, which has a high adoption on the market. More and more organizations want to adopt Splunk to use their data to make informed decisions. With the release of 6.3, Splunk has become more robust and has better analytics. This book is for anyone who wants to manage data with Splunk.

You'll start with very basics of Splunk— installing Splunk—and then move on to searching machine data with Splunk. You will gather data from different sources, isolate them by indexes, classify them into source types, and tag them with the essential fields. After this, you will learn to create various reports, XML forms, and alerts. You will then continue using the Pivot Model to transform the data models into visualization. You will also explore visualization with D3 in Splunk. Finally you'll be provided with some real-world best practices in using Splunk.