

---

# Splunk User Guide

If you are craving such a referred **Splunk User Guide** book that will manage to pay for you worth, get the no question best seller from us currently from several preferred authors. If you want to entertaining books, lots of novels, tale, jokes, and more fictions collections are after that launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every ebook collections Splunk User Guide that we will extremely offer. It is not just about the costs. Its approximately what you habit currently. This Splunk User Guide, as one of the most working sellers here will very be in the course of the best options to review.



Splunk {Power User Knowledge Manager} Certification Guide Packt Publishing Ltd

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 This easy-to-follow, practical book can be used by anyone, even if you have never managed any data before Who This Book Is For This book will be perfect for you if you are a Software engineer or developer or System administrators or Business analyst who seek to correlate machine data with business metrics and provide intuitive real-time and statistical visualizations. Some knowledge or experience of previous versions of Splunk will be helpful but not essential. 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. 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. Style and approach This fast-paced, example-rich guide will help you analyze and visualize machine data with Splunk through simple, practical instructions.

**Splunk 9 Enterprise Certified Administration Guide** Packt Publishing Ltd

Transform machine data into powerful analytical intelligence using Splunk About This Book Analyze and visualize machine data to step into the world of Splunk! Leverage the exceptional analysis and visualization capabilities to make informed decisions for your business This easy-to-follow, practical book can be used by anyone - even if you have never managed data before Who This Book Is For This book is for the

beginners who want to get well versed in the services offered by Splunk 7. If you want to be a data/business analyst or want to be a system administrator, this book is what you want. No prior knowledge of Splunk is required. What You Will Learn Install and configure Splunk for personal use Store event data in Splunk indexes, classify events into sources, and add data fields Learn essential Splunk Search Processing Language commands and best practices Create powerful real-time or user-input dashboards Be proactive by implementing alerts and scheduled reports Tips from the Fez: best practices using Splunk features and add-ons Understand security and deployment considerations for taking Splunk to an organizational level In Detail Splunk is a search, reporting, and analytics software platform for machine data, which has an ever-growing market adoption rate. More organizations than ever are adopting Splunk to make informed decisions in areas such as IT operations, information security, and the Internet of Things. The first two chapters of the book will get you started with a simple Splunk installation and set up of a sample machine data generator, called Eventgen. After this, you will learn to create various reports, dashboards, and alerts. You will also explore Splunk's Pivot functionality to model data for business users. You will then have the opportunity to test-drive Splunk's powerful HTTP Event Collector. After covering the core Splunk functionality, you'll be provided with some real-world best practices for using Splunk, and information on how to build upon what you've learned in this book. Throughout the book, there will be additional comments and best practice recommendations from a member of the SplunkTrust Community, called "Tips from the Fez". Style and approach This fast-paced, example-rich guide will help you analyze and visualize machine data with Splunk through simple, practical instructions and recommendations. Downloading the example code for this book You can download the example code files for all Packt books you have purc ...

**Splunk Best Practices** Packt Publishing Ltd

This book will cover Splunk's offerings to efficiently capture, index, and correlate data from a searchable repository all in real-time to generate insightful graphs, reports, dashboards, and alerts. Developers and architects alike can be in high demand if they become experts with this tool.

**Building Splunk Solutions** Packt Publishing Ltd

Leverage Splunk's operational intelligence capabilities to unlock new hidden business insights and drive success Key Features Tackle any problems related to searching and analyzing your data with Splunk Get the latest information and business insights on Splunk 7.x Explore the all new machine learning

toolkit in Splunk 7.x Book Description Splunk makes it easy for you to take control of your data, and with Splunk Operational Cookbook, you can be confident that you are taking advantage of the Big Data revolution and driving your business with the cutting edge of operational intelligence and business analytics. With more than 80 recipes that demonstrate all of Splunk's features, not only will you find quick solutions to common problems, but you'll also learn a wide range of strategies and uncover new ideas that will make you rethink what operational intelligence means to you and your organization. You'll discover recipes on data processing, searching and reporting, dashboards, and visualizations to make data shareable, communicable, and most importantly meaningful. You'll also find step-by-step demonstrations that walk you through building an operational intelligence application containing vital features essential to understanding data and to help you successfully integrate a data-driven way of thinking in your organization. Throughout the book, you'll dive deeper into Splunk, explore data models and pivots to extend your intelligence capabilities, and perform advanced searching with machine learning to explore your data in even more sophisticated ways. Splunk is changing the business landscape, so make sure you're taking advantage of it. What you will learn Learn how to use Splunk to gather, analyze, and report on data Create dashboards and visualizations that make data meaningful Build an intelligent application with extensive functionalities Enrich operational data with lookups and workflows Model and accelerate data and perform pivot-based reporting Apply ML algorithms for forecasting and anomaly detection Summarize data for long term trending, reporting, and analysis Integrate advanced JavaScript charts and leverage Splunk's API Who this book is for This book is intended for data professionals who are looking to leverage the Splunk Enterprise platform as a valuable operational intelligence tool. The recipes provided in this book will appeal to individuals from all facets of business, IT, security, product, marketing, and many more! Even the existing users of Splunk who want to upgrade and get up and running with Splunk 7.x will find this book to be of great value.

### *Mastering Splunk Apress*

Master the art of getting the maximum out of your machine data using Splunk About This Book A practical and comprehensive guide to the advanced functions of Splunk,, including the new features of Splunk 6.3 Develop and manage your own Splunk apps for greater insight from your machine data Full coverage of high-level Splunk techniques including advanced searches, manipulations, and visualization Who This Book Is For This book is for Splunk developers looking to learn advanced strategies to deal with big data from an enterprise architectural perspective. It is expected that readers have a basic understanding and knowledge of using Splunk Enterprise. What You Will Learn Find out how to develop and manage apps in Splunk Work with important search commands to perform data analytics on uploaded data Create visualizations in Splunk Explore tweaking Splunk Integrate Splunk with any pre-existing application to perform data crunching efficiently and in real time Make your big data speak with analytics and visualizations using Splunk Use SDK and Enterprise integration with tools such as R and Tableau In Detail Master the power of Splunk and learn the advanced strategies to get the most out of your machine data with this practical advanced guide. Make sense of the hidden data of your organization – the insight of your servers, devices, logs, traffic and clouds. Advanced Splunk shows you how. Dive deep into Splunk to find the most efficient solution to your data problems. Create the robust Splunk solutions you need to make informed decisions in big data machine analytics. From visualizations to enterprise integration, this well-organized high level guide has everything you need for Splunk mastery. Start with a complete overview of all the new features and advantages of the latest version of Splunk and the Splunk Environment. Go hands on with uploading

data, search commands for basic and advanced analytics, advanced visualization techniques, and dashboard customizing. Discover how to tweak Splunk to your needs, and get a complete on Enterprise Integration of Splunk with various analytics and visualization tools. Finally, discover how to set up and use all the new features of the latest version of Splunk. Style and approach This book follows a step by step approach. Every new concept is built on top of its previous chapter, and it is full of examples and practical scenarios to help the reader experiment as they read.

### **Splunk a Complete Guide - 2019 Edition Apress**

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis. This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers. Comprehensive coverage of log management including analysis, visualization, reporting and more Includes information on different uses for logs -- from system operations to regulatory compliance Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

### **Practical Splunk Search Processing Language Newnes**

Use this practical guide to the Splunk operational data intelligence platform to search, visualize, and analyze petabyte-scale, unstructured machine data. Get to the heart of the platform and use the Search Processing Language (SPL) tool to query the platform to find the answers you need. With more than 140 commands, SPL gives you the power to ask any question of machine data. However, many users (both newbies and experienced users) find the language difficult to grasp and complex. This book takes you through the basics of SPL using plenty of hands-on examples and emphasizes the most impactful SPL commands (such as eval, stats, and timechart). You will understand the most efficient ways to query Splunk (such as learning the drawbacks of subsearches and join, and why it makes sense to use tstats). You will be introduced to lesser-known commands that can be very useful, such as using the command rex to extract fields and erex to generate regular expressions automatically. In addition, you will learn how to create basic visualizations (such as charts and tables) and use prescriptive guidance on search optimization. For those ready to take it to the next level, the author introduces advanced commands such as predict, kmeans, and cluster. What You Will Learn Use real-world scenarios (such as analyzing a web access log) to search, group, correlate, and create reports using SPL commands Enhance your search results using lookups and create new lookup tables using SPL commands Extract fields from your search results Compare data from multiple time frames in one chart (such as comparing your current day application performance to the average of the past 30 days) Analyze the

performance of your search using Job Inspector and identify execution costs of various components of your search Who This Book Is For Application developers, architects, DevOps engineers, application support engineers, network operations center analysts, security operations center (SOC) analysts, and cyber security professionals who use Splunk to search and analyze their machine data

#### **Splunk Essentials** Packt Publishing Ltd

Most programmers' fear of user interface (UI) programming comes from their fear of doing UI design. They think that UI design is like graphic design—the mysterious process by which creative, latte-drinking, all-black-wearing people produce cool-looking, artistic pieces. Most programmers see themselves as analytic, logical thinkers instead—strong at reasoning, weak on artistic judgment, and incapable of doing UI design. In this brilliantly readable book, author Joel Spolsky proposes simple, logical rules that can be applied without any artistic talent to improve any user interface, from traditional GUI applications to websites to consumer electronics. Spolsky's primary axiom, the importance of bringing the program model in line with the user model, is both rational and simple. In a fun and entertaining way, Spolsky makes user interface design easy for programmers to grasp. After reading *User Interface Design for Programmers*, you'll know how to design interfaces with the user in mind. You'll learn the important principles that underlie all good UI design, and you'll learn how to perform usability testing that works.

#### **Learning Splunk Web Framework** CreateSpace

This guide follows a Splunk software engineering team on a journey to build solutions with partners, focusing on the real world use cases to showcase various technologies of the Splunk Developer Platform. Like a documentary, it captures our story from envisioning and user experience prototyping to development, packaging and multiple production deployments. It includes the diverse perspectives of developers and testers, administrators and product owners, security experts and release engineers. As on any real journey, we make mistakes, have arguments, and change our minds along the way. So in addition to showing you how best to do things, we highlight the pitfalls and issues that we encounter, and the solutions we find. The key element of this guidance, of course, is the code. We've made the code repos open, and recommend you study the source code of the reference apps and the associated tests. In fact, you can see and replay the code in motion, as it was developed. We encourage you to reuse and learn from it.

#### **The Product is Docs** Packt Publishing Ltd

This book is for those Splunk developers who want to learn advanced strategies to deal with big data from an enterprise architectural perspective. You need to have good working knowledge of Splunk.

#### **SPLUNK Core Certified User Exam Practice Questions & Dumps** Packt Publishing Ltd

*Big Data Analytics Using Splunk* is a hands-on book showing how to process and derive business value from big data in real time. Examples in the book draw from social media sources such as Twitter (tweets) and Foursquare (check-ins). You also learn to draw from machine data, enabling you to analyze, say, web server log files and patterns of user access in real time, as the access is occurring. Gone are the days when you need be caught out by shifting public opinion or sudden changes in customer behavior. Splunk's easy to use engine helps you recognize and react in real time, as events are occurring. Splunk is a powerful, yet simple analytical tool fast gaining traction in the fields of big data and operational intelligence. Using Splunk, you can monitor data in real time, or mine your data after the fact. Splunk's stunning visualizations aid in locating the needle of value in a haystack of a data. Geolocation support spreads your data across a map, allowing you to drill down to geographic areas of interest. Alerts can run in the background and trigger to warn you of shifts or events as they are taking place. With Splunk you can immediately recognize and react to changing trends and shifting public opinion as expressed through social media, and to new patterns of eCommerce and customer behavior. The ability to immediately recognize and react to changing trends provides a tremendous advantage in today's fast-paced world of Internet business. *Big Data Analytics Using Splunk* opens the door to an

exciting world of real-time operational intelligence. Built around hands-on projects Shows how to mine social media Opens the door to real-time operational intelligence

#### **Splunk Operational Intelligence Cookbook** Apress

This guide follows a Splunk software engineering team on a journey to build solutions with partners, focusing on the real world use cases to showcase various technologies of the Splunk Developer Platform. Like a documentary, it captures our story from envisioning and user experience prototyping to development, packaging and multiple production deployments. It includes the diverse perspectives of developers and testers, administrators and product owners, security experts and release engineers. As on any real journey, we make mistakes, have arguments, and change our minds along the way. So in addition to showing you how best to do things, we highlight the pitfalls and issues that we encounter, and the solutions we find. The key element of this guidance, of course, is the code. We've made the code repos open, and recommend you study the source code of the reference apps and the associated tests. In fact, you can see and replay the code in motion, as it was developed. We encourage you to reuse and learn from it.

#### **Improving Your Splunk Skills** Packt Publishing Ltd

Together, Big Data, high-performance computing, and complex environments create unprecedented opportunities for organizations to generate game-changing insights that are based on hard data. *Business Analytics: An Introduction* explains how to use business analytics to sort through an ever-increasing amount of data and improve the decision-making cap

#### **Mastering Splunk** Packt Publishing Ltd

Empower Your Digital Shield with Splunk Expertise! KEY FEATURES ? In-depth Exploration of Splunk's Security Ecosystem and Capabilities ? Practical Scenarios and Real-World Implementations of Splunk Security Solutions ? Streamline Automation and Orchestration in Splunk Operations DESCRIPTION The Ultimate Splunk for Cybersecurity is your practical companion to utilizing Splunk for threat detection and security operations. This in-depth guide begins with an introduction to Splunk and its role in cybersecurity, followed by a detailed discussion on configuring inputs and data sources, understanding Splunk architecture, and using Splunk Enterprise Security (ES). It further explores topics such as data ingestion and normalization, understanding SIEM, and threat detection and response. It then delves into advanced analytics for threat detection, integration with other security tools, and automation and orchestration with Splunk. Additionally, it covers cloud security with Splunk, DevOps, and security operations. Moreover, the book provides practical guidance on best practices for Splunk in cybersecurity, compliance, and regulatory requirements. It concludes with a summary of the key concepts covered throughout the book. WHAT WILL YOU LEARN ? Achieve advanced proficiency in Splunk Enterprise Security to bolster your cyber defense capabilities comprehensively. ? Implement Splunk for cutting-edge cybersecurity threat detection and analysis with precision. ? Expertly integrate Splunk with leading cloud platforms to enhance security measures. ? Seamlessly incorporate Splunk with a variety of security tools for a unified defense system. ? Employ Splunk's robust data analytics for sophisticated threat hunting. ? Enhance operational efficiency and accuracy by automating security tasks with Splunk. ? Tailor Splunk dashboards for real-time security monitoring and insightful analysis. WHO IS THIS BOOK FOR? This book is designed for IT professionals, security analysts, and network administrators possessing a foundational grasp of cybersecurity principles and a basic familiarity with Splunk. If you are an individual seeking to enhance your proficiency in leveraging Splunk for advanced cybersecurity applications and integrations, this book is crafted with your skill development in mind. TABLE OF CONTENTS 1. Introduction to Splunk and Cybersecurity 2. Overview of Splunk Architecture 3. Configuring Inputs and Data Sources 4. Data Ingestion and Normalization 5. Understanding SIEM 6. Splunk Enterprise Security 7. Security Intelligence 8. Forensic Investigation in Security Domains 9. Splunk Integration with Other Security Tools 10. Splunk

for Compliance and Regulatory Requirements 11. Security Orchestration, Automation and Response (SOAR) with Splunk 12. Cloud Security with Splunk 13. DevOps and Security Operations 14. Best Practices for Splunk in Cybersecurity 15. Conclusion and Summary Index

### **Building Splunk Solutions (Second Edition)** Apress

Make your Splunk certification easier with this exam study guide that covers the User, Power User, and Enterprise Admin certifications. This book is divided into three parts. The first part focuses on the Splunk User and Power User certifications starting with how to install Splunk, Splunk Processing Language (SPL), field extraction, field aliases and macros, and Splunk tags. You will be able to make your own data model and prepare an advanced dashboard in Splunk. In the second part, you will explore the Splunk Admin certification. There will be in-depth coverage of Splunk licenses and user role management, and how to configure Splunk forwarders, indexer clustering, and the security policy of Splunk. You'll also explore advanced data input options in Splunk as well as .conf file merging logic, btool, various attributes, stanza types, editing advanced data inputs through the .conf file, and various other types of .conf file in Splunk. The concluding part covers the advanced topics of the Splunk Admin certification. You will also learn to troubleshoot Splunk and to manage existing Splunk infrastructure. You will understand how to configure search head, multi-site indexer clustering, and search peers besides exploring how to troubleshoot Splunk Enterprise using the monitoring console and matrix.log. This part will also include search issues and configuration issues. You will learn to deploy an app through a deployment server on your client instance, create a server class, and carry out load balancing, socks proxy, and indexer discovery. By the end of the Splunk Certified Study Guide, you will have learned how to manage resources in Splunk and how to use REST API services for Splunk. This section also explains how to set up Splunk Enterprise on the AWS platform and some of the best practices to make them work efficiently together. The book offers multiple choice question tests for each part that will help you better prepare for the exam. You will: Study to pass the Splunk User, Power User, and Admin certificate exams Implement and manage Splunk multi-site clustering Design, implement, and manage a complex Splunk Enterprise solution Master the roles of Splunk Admin and troubleshooting Configure Splunk using AWS.

### Splunk 7 Essentials - Third Edition Packt Publishing Ltd

This guide follows a Splunk software engineering team on a journey to build solutions with partners, focusing on the real world use cases to showcase various technologies of the Splunk Developer Platform. Like a documentary, it captures our story from envisioning and user experience prototyping to development, packaging and multiple production deployments. It includes the diverse perspectives of developers and testers, administrators and product owners, security experts and release engineers. As on any real journey, we make mistakes, have arguments, and change our minds along the way. So in addition to showing you how best to do things, we highlight the pitfalls and issues that we encounter, and the solutions we find. The key element of this guidance, of course, is the code. We've made the code repos open, and recommend you study the source code of the reference apps and the associated tests. In fact, you can see and replay the code in motion, as it was developed. We encourage you to reuse and learn from it. The second edition is expanded with 10 new chapters, including 3 new ones in the Journey covering OAuth, alerting and high performance HTTP Event Collector. Additionally we include a new section - the Essentials where we've generalized the lessons learned from this Journey and other development projects into fundamental patterns and practices. We still cover the full spectrum of application development from getting data into Splunk Enterprise to packaging and distributing your app. Each topic combines design and implementation guidelines in a way that supports an iterativedevelopment process. These guidelines cover not only Splunk Enterprise operational and programming concepts that the application deals with directly, but also consider performance, quality, and maintenance issues in recommending particular approaches.

### Learning Splunk Web Framework Packt Publishing Ltd

Take your analytics online with the ease and power of the Splunk

Web FrameworkAbout This Book- Want to build rich applications on the Web using Splunk? This book will be your ultimate guide!- Learn to use web framework components with the help of this highly practical, example-rich guide- Perform excellent Splunk analytics on the Web and bring that knowledge to your own projectsWho This Book Is ForThis book will cater to Splunk developers and administrators who now wish to further their knowledge with Splunk Web Framework and learn to improve the way they present and visualize data in Splunk. A basic knowledge of JavaScript will be beneficial but is not a prerequisite.What You Will Learn- Master the fundamentals of Splunk Web Framework- Start thinking of Splunk as a complete development platform to build user-friendly apps- Extend the functionality of your apps using SimpleXML techniques- Set up dashboard layouts, navigation, and menus in your apps- Create simple dashboard elements including charts and tables- Master the art of interacting with searches and dashboards- Integrate SplunkJS to add visual appeal to your websiteIn DetailBuilding rich applications on the Web using Splunk is now simpler than ever before with the Splunk Web Framework. It empowers developers to build their own web applications with custom dashboards, tables, charts, form searches, and other functionalities in the datasets at their disposal. The book will start with the fundamentals of the Splunk Web Framework, teaching you the secrets of building interesting and user-friendly applications. In the first application, you will learn to analyze and monitor traffic hitting the NASA website and learn to create dashboards for it. You will then learn additional, and more detailed, techniques to enhance the functionalities of the app such as dashboards and forms, editing simple XML, using simple XML extensions, tokens, post-process searches, dynamic drill-downs, the Splunk Web Framework and REST API, and much more. The second app will use historical stock market data and will create custom dashboards using Splunk Web Framework; the book will now cover important topics such as creating HTML dashboards, enhancing the visual appeal of the app using CSS, and moving your app with SplunkJS. The book will provide different and interesting examples instead of the usual "Log, Index, Search, and Graph" so that Splunk will be the first tool readers think of to resolve a problem. Style and approachThis book will follow a step-by-step approach whereby every new concept is built on top of the previous chapter, and will be highly practical in nature; the reader will learn to build apps while reading about the Splunk Web framework.

### **Search Reference Guide** Packt Publishing Ltd

Find all the information, exercises, and tools to ace the Splunk Enterprise Certified Admin exam in one place Key Features Explore various administration topics including installation, configuration, and user management Gain a deep understanding of data inputs, parsing, and field extraction Excel in the Splunk Enterprise Admin exam with the help of self-assessment questions and mock exams Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionThe IT sector's appetite for Splunk and skilled Splunk developers continues to surge, offering more opportunities for developers with each passing decade. If you want to enhance your career as a Splunk Enterprise administrator, then Splunk 9.x Enterprise Certified Admin Guide will not only aid you in excelling on your exam but also pave the way for a successful career. You'll begin with an overview of Splunk Enterprise, including installation, license management, user management, and forwarder management. Additionally, you'll delve into indexes management, including the creation and management of indexes used to store data in Splunk. You'll also uncover config files, which are used to configure various settings and components in Splunk. As you advance, you'll explore data administration, including data inputs, which are used to collect data from various sources, such as log files, network protocols (TCP/UDP), APIs, and agentless inputs (HEC). You'll also discover search-time and index-time field extraction, used to create reports and visualizations, and help make the data in Splunk more searchable and accessible. The self-assessment questions and answers at the end of each chapter will help you gauge your understanding. By the end of this book, you'll be well versed in all the topics required to pass the Splunk Enterprise Admin exam and use Splunk features effectively. What you will learn Explore Splunk Enterprise 9.x features and usage Install, configure, and manage licenses and users for Splunk Create and manage indexes for data storage Explore Splunk

---

configuration files, their precedence, and troubleshooting Manage forwarders and source data into Splunk from various resources Parse and transform data to make it easy to use Extract fields from data at search and index time for data analysis Engage with mock exam questions to simulate the Splunk admin exam Who this book is for This book is for data professionals looking to gain certified Splunk administrator credentials. It will also help data analysts, Splunk users, IT experts, security analysts, and system administrators seeking to explore the Splunk admin realm, understand its functionalities, and become proficient in effectively administering Splunk Enterprise. This guide serves as both a valuable resource for learning and a practical manual for administering Splunk Enterprise, encompassing features beyond the scope of certification preparation.

*Logging and Log Management* Packt Publishing

Learn to effectively use, configure, deploy and extend Splunk and implement its powerful capabilities.

**Splunk 7 Essentials, Third Edition** CRC Press

This book provides a broad perspective about the essential aspects of creating technical documentation in today's product development world. It is a book of opinions and guidance, collected as short essays. You can read selectively about subjects that interest you, or you can read the entire collection in any order you like. Information development is a multidimensional discipline, and it is easy to theorize. We have written this book from our direct experience, using the concrete insights and practices we apply to our work every day. If you work as an information developer, a manager in a documentation team, or in another part of product development that collaborates with a doc team, there is information in this book for you. Perhaps you are a technical writer in a small, high-growth company that is figuring out its processes. Perhaps you are an information-development manager in a large enterprise company with an expanding product line and an ever more complex matrix of cross-functional dependencies. You might work at a medium-sized company where your management is asking you to do more with fewer people, and you want some additional perspective that will help you find a leaner and more effective way to deliver what your business demands. Or you might work outside the technical documentation world, in another part of product development, and are wondering how to collaborate most effectively with the documentation team. The purpose of *The Product is Docs* is to provoke discussion, shine light on some murky areas, and--we hope--inspire our colleagues to consider their processes and assumptions with new eyes. -- Amazon.