Splunk User Guide

Thank you certainly much for downloading **Splunk User Guide**.Maybe you have knowledge that, people have look numerous times for their favorite books taking into account this Splunk User Guide, but stop going on in harmful downloads.

Rather than enjoying a fine ebook afterward a mug of coffee in the afternoon, otherwise they juggled considering some harmful virus inside their computer. **Splunk User Guide** is user-friendly in our digital library an online right of entry to it is set as public as a result you can download it instantly. Our digital library saves in compound countries, allowing you to acquire the most less latency era to download any of our books taking into account this one. Merely said, the Splunk User Guide is universally compatible in the manner of any devices to read.

Improving Your Splunk Skills Packt Publishing Ltd
Take your analytics online with the ease and power of the Splunk Web Framework About 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 projects Who This Book Is For This 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 website In Detail Building 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 approach This 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.

Building Splunk Solutions **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.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.

Logging and Log Management Orange Education Pvt 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 9.x Enterprise Certified Admin Guide Packt Publishing Ltd

Mastering Splunk: A Comprehensive Guide for Beginners Transform raw machine data into operational gold with Splunk! This hands-on guide is your ticket to taming the vast amounts of data generated by modern IT environments, unlocking a world of valuable insights to streamline operations, pinpoint security risks, and drive business success. Key Benefits: Dive into Splunk Fundamentals: Explore the core components of the Splunk platform and understand how it empowers your data analysis journey. Get Practical: Hands-on exercises and practical chapters reinforce your learning, making even complex concepts easy to grasp. Unleash Data's Power: Master data ingestion, search techniques, field extractions, powerful visualizations, and dashboard creation to turn information into actionable insights. Achieve Advanced Mastery: Delve into user management, configuration file customization, knowledge objects like lookups, and even push the boundaries of Splunk to solve unique data challenges. Why This Book Designed for Beginners, Ideal for Experienced Users: Start with the basics and progress to truly advanced techniques in a structured way. In-Depth, but Accessible: Detailed explanations without sacrificing clarity make this the ideal Splunk reference book for any skill level. Go beyond Theory: Real-world scenarios and practical examples demonstrate how Splunk is used to solve common IT, security, and business problems. Topics Covered Splunk architecture and deployment options Data indexing and search processing Field extractions and transformations Reporting and visualizations Dashboards and alerts Data models User management and security Configuration files and lookups Splunk Apps and add-ons Upgrade your data analysis skills and unlock the full potential of Splunk. Get your copy of "Mastering Splunk" today!

Implementing Splunk - Big Data Reporting and Development for Operational Intelligence Packt Publishing Ltd

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's 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. What You Will Learn 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 Who This Book Is For People looking to pass the User, Power User, and Enterprise Admin exams. It is also useful for Splunk administrators and support engineers for managing an existing deployment.

Data Analytics Using Splunk 9. X Packt Publishing Ltd

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.

Learning Splunk Web Framework Packt Publishing

Learn how to architect, implement, and administer a complex Splunk Enterprise environment and extract valuable insights from business data. Key FeaturesUnderstand the various components of Splunk and how they work together to provide a powerful Big Data analytics solution. Collect and index data from a wide variety of common machine data sourcesDesign searches, reports, and dashboard visualizations to provide business data insightsBook Description Splunk is a leading platform and solution for collecting, searching, and extracting value from ever increasing amounts of big data - and big data is eating the world! This book covers all the crucial Splunk topics and gives you the information and examples to get the

immediate job done. You will find enough insights to support further research and use Splunk to suit any business environment or situation. Splunk 7.x Quick Start Guide gives you a thorough understanding of how Splunk works. You will learn about all the critical tasks for architecting, implementing, administering, and utilizing Splunk Enterprise to collect, store, retrieve, format, analyze, and visualize machine data. You will find step-by-step examples based on real-world experience and practical use cases that are applicable to all Splunk environments. There is a careful balance between adequate coverage of all the critical topics with short but relevant deep-dives into the configuration options and steps to carry out the day-to-day tasks that matter. By the end of the book, you will be a confident and proficient Splunk architect and administrator. What you will learnDesign and implement a complex Splunk Enterprise solutionConfigure your Splunk environment to get machine data in and indexedBuild searches to get and format data for analysis and visualizationBuild reports, dashboards, and alerts to deliver critical insightsCreate knowledge objects to enhance the value of your dataInstall Splunk apps to provide focused views into key technologiesMonitor, troubleshoot, and manage your Splunk environmentWho this book is for This book is intended for experienced IT personnel who are just getting started working with Splunk and want to quickly become proficient with its usage. Data analysts who need to leverage Splunk to extract critical business insights from application logs and other machine data sources will also benefit from this book.

Advanced Splunk 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 Packt Publishing Ltd

While Robotic Process Automation (RPA) has been around for about 20 years, it has hit an inflection point because of the convergence of cloud computing, big data and AI. This book shows you how to leverage RPA effectively in your company to automate repetitive and rules-based processes, such as scheduling, inputting/transferring data, cut and paste, filling out forms, and search. Using practical aspects of implementing the technology (based on case studies and industry best practices), you'll see how companies have been able to realize substantial ROI (Return On Investment) with their implementations, such as by lessening the need for hiring or outsourcing. By understanding the core concepts of RPA, you'll also see that the technology significantly increases compliance – leading to fewer issues with regulations – and minimizes costly errors. RPA software revenues have recently soared by over 60 percent, which is the fastest ramp in the tech industry, and they are expected to exceed $1 billion by the end of 2019. It is generally seamless with legacy IT environments, making it easier for companies to pursue a strategy of digital transformation and can even be a gateway to AI. The Robotic Process Automation Handbook puts everything you need to know into one place to be a part of this wave. What You'll Learn Develop the right strategy and planDeal with resistance and fears from employeesTake an in-depth look at the leading RPA systems, including where they are most effective, the risks and the costsEvaluate an RPA system Who This Book Is For IT specialists and managers at mid-to-large companies

Splunk 7 Essentials, Third Edition Packt Publishing Ltd

Make the most of Splunk 9.x to build insightful reports and dashboards with a detailed walk-through of its extensive features and capabilities Key Features Be well-versed with the Splunk 9. x architecture, installation, onboarding, and indexing data features Create advanced visualizations using the Splunk search processing language Explore advanced Splunk administration techniques, including clustering, data modeling, and container management Book DescriptionSplunk 9 improves on the existing Splunk tool to include important features such as federated search, observability, performance improvements, and dashboarding. This book helps you to make the best use of the impressive and new features to prepare a Splunk installation that can be employed in the data analysis process. Starting with an introduction to the different Splunk components, such as indexers, search heads, and forwarders, this Splunk book takes you through the step-by-step installation and configuration instructions for basic Splunk components using Amazon Web Services (AWS) instances. You'll import the BOTS v1 dataset into a search head and begin exploring data using the Splunk Search Processing Language (SPL), covering various types of Splunk commands, lookups, and macros. After that, you'll create tables, charts, and dashboards using Splunk's new Dashboard Studio, and then advance to work with clustering, container management, data models, federated search, bucket merging, and more. By the end of the book, you'll not only have learned everything about the latest features of Splunk 9 but also have a solid understanding of the performance tuning techniques in the latest version.What you will learn Install and configure the Splunk 9 environment Create advanced dashboards using the flexible layout options in Dashboard Studio Understand the Splunk licensing models Create tables and make use of the various types of charts available in Splunk 9.x Explore the new configuration management features Implement the performance improvements introduced in Splunk 9.x Integrate Splunk with Kubernetes for optimizing CI/CD management Who this book is for The book is for data analysts, Splunk users, and administrators who want to become well-versed in the data analytics services offered by Splunk 9. You need to have a basic understanding of Splunk fundamentals to get the most out of this book.

Splunk Certified Study Guide Newnes

Over 70 practical recipes to gain operational data intelligence with Splunk Enterprise About This Book This is the most up-to-date book on Splunk 6.3 and teaches you how to tackle real-world operational intelligence scenarios efficiently Get business insights using machine data using this easy-to-follow guide Search, monitor, and analyze your operational data skillfully using this recipe-based, practical guide Who This Book Is For This book is intended for users of all levels 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! Also, existing users of Splunk who want to upgrade and get up and running with Splunk 6.3 will find this book invaluable. What You Will Learn Use Splunk to gather, analyze, and report on data Create dashboards and visualizations that make data meaningful Build an operational intelligence application with extensive features and functionality Enrich operational data with lookups and workflows Model and accelerate data and perform pivot-based

reporting Build real-time, scripted, and other intelligence-driven alerts Summarize data for longer term trending, reporting, and analysis Integrate advanced JavaScript charts and leverage Splunk's API In Detail 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 70 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 to explore your data in even more sophisticated ways. Splunk is changing the business landscape, so make sure you're taking advantage of it. Style and approach Splunk is an excellent platform that allows you to make sense of machine data with ease. The adoption of Splunk has been huge and everyone who has gone beyond installing Splunk wants to know how to make most of it. This book will not only teach you how to use Splunk in real-world scenarios to get business insights, but will also get existing Splunk users up to date with the latest Splunk 6.3 release.

Splunk 7 Essentials - Third Edition 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.

Splunk Best Practices Apress

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

Splunk Operational Intelligence Cookbook 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, Spolky 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.

The Adventures of Johnny Bunko 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.

Ultimate Splunk for Cybersecurity Packt Publishing Ltd

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

Mastering Splunk Packt Publishing Ltd

This book is intended for users of all levels 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 a business – IT, Security, Product, Marketing, and many more!

Splunk Developer's Guide - Second Edition Penguin

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

Splunk Essentials 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.

Practical Splunk Search Processing Language IBM Redbooks

Learn the A to Z of building excellent Splunk applications with the latest techniques using this comprehensive guide About This Book This is the most up-to-date book on Splunk 6.3 for developers Get ahead of being just a Splunk user and start creating custom Splunk applications as per your needs Your one-stop-solution to Splunk application development Who This Book Is For This book is for those who have some familiarity with Splunk and now want to learn how to develop an efficient Splunk application. Previous experience with Splunk, writing searches, and designing basic dashboards is expected. What You Will Learn Implement a Modular Input and a custom D3 data visualization Create a directory structure and set view permissions Create a search view and a dashboard view using advanced XML modules Enhance your application using eventtypes, tags, and macros Package a Splunk application using best practices Publish a Splunk application to the Splunk community In Detail Splunk provides a platform that allows you to search data stored on a machine, analyze it, and visualize the analyzed data to make informed decisions. The adoption of Splunk in enterprises is huge, and it has a wide range of customers right from Adobe to Dominos. Using the Splunk platform as a user is one thing, but customizing this platform and creating applications specific to your needs takes more than basic knowledge of the platform. This book will dive into developing Splunk applications that cater to your needs of making sense of data and will let you visualize this data with the help of stunning dashboards. This book includes everything on developing a full-fledged Splunk application right from designing to implementing to publishing. We will design the fundamentals to build a Splunk application and then move on to creating one. During the course of the book, we will cover application data, objects, permissions, and more. After this, we will show you how to enhance the application, including branding, workflows, and enriched data. Views, dashboards, and web frameworks are also covered. This book will showcase everything new in the latest version of Splunk including the latest data models, alert actions, XML forms, various dashboard enhancements, and visualization options (with D3). Finally, we take a look at the latest Splunk cloud applications, advanced integrations, and development as per the latest release. Style and approach This book is an easy-to-follow guide with lots of tips and tricks to help you master all the concepts necessary to develop and deploy your Splunk applications.