Splunk User Guide

When somebody should go to the ebook stores, search opening by shop, shelf by shelf, it is in reality problematic. This is why we give the books compilations in this website. It will extremely ease you to look guide **Splunk User Guide** as you such as.

By searching the title, publisher, or authors of guide you in point of fact want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best area within net connections. If you goal to download and install the Splunk User Guide, it is completely simple then, back currently we extend the connect to purchase and make bargains to download and install Splunk User Guide for that reason simple!

Mastering Splunk 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.

```
SPLUNK Core Certified User Exam Practice
Questions & Dumps 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.

Splunk Certified Study Guide Apress
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 Developer's Guide - Second Edition 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.

The Robotic Process Automation Handbook Apress
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.

User Interface Design for Programmers Packt Publishing Ltd
Design, implement, and publish custom Splunk applications by following best practices About This Book This is the most up-to-date guide on the market and will help you finish your tasks faster, easier, and more efficiently. Highly practical guide that addresses common and not-so-common pain points in Splunk. Want to explore shortcuts to perform tasks more efficiently with Splunk? This is the book for you! Who This Book Is For This book is for administrators, developers, and search ninjas who have been using Splunk for some time. A comprehensive coverage makes this book great for Splunk veterans and newbies alike. What You Will Learn Use Splunk effectively to gather, analyze, and report on operational data throughout your environment Expedite your reporting, and be empowered to present data in a meaningful way Create robust searches, reports, and charts using Splunk Modularize your programs for better reusability. Build your own Splunk apps and learn why they are important Learn how to integrate with enterprise systems Summarize data for longer term trending, reporting, and analysis In Detail This book will give you an edge over others through insights that will help you in day-to-day instances. When you're working with data from various sources in Splunk and performing analysis on this data, it can be a bit tricky. With this book, you will learn the best practices of working with Splunk. You'll learn about tools and techniques that will ease your life with Splunk, and will ultimately save you time. In some cases, it will adjust your thinking of what Splunk is, and what it can and cannot do. To start with, you'll get to know the best practices to get data into Splunk, analyze data, and package apps for distribution. Next, you'll discover the best practices in logging, operations, knowledge management, searching, and reporting. To finish off, we will teach you how to troubleshoot Splunk searches, as well as deployment, testing, and development with Splunk. Style and approach If you're stuck or want to find a better way to work with Splunk environment, this book will come handy. This easy-to-follow, insightful book contains step-by-step instructions and examples and scenarios that you will connect to.

Mastering Splunk Apress
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.

Practical Splunk Search Processing Language Orange Education Pvt Ltd
Transform machine-generated data into valuable business insights using the powers of Splunk Key FeaturesExplore the all-new machine learning toolkit in Splunk 7.xTackle any problems related to searching and analyzing your data with SplunkGet the latest information and business insights on Splunk 7.xBook Description Splunk makes it easy for you to take control of your data and drive your business with the cutting edge of operational intelligence and business analytics. Through this Learning Path, you'll implement new services and utilize them to quickly and efficiently process machine-generated big data. You'll begin with an introduction to the new features, improvements, and offerings of Splunk 7. You'll learn to efficiently use wildcards and modify your search to make it faster. You'll learn how to enhance your applications by using XML dashboards and configuring and extending Splunk. You'll also find step-by-step demonstrations that'll walk you through building an operational intelligence application. As you progress, you'll explore data models and pivots to extend your intelligence capabilities. By the end of this Learning Path, you'll have the skills and confidence to implement various Splunk services in your projects. This Learning Path includes content from the following Packt products: Implementing Splunk 7 - Third Edition by James MillerSplunk Operational Intelligence Cookbook - Third Edition by Paul R Johnson, Josh Diakun, et alWhat you will learnMaster the new offerings in Splunk: Splunk Cloud and the Machine Learning ToolkitCreate efficient and effective searchesMaster the use of Splunk tables, charts, and graph enhancementsUse Splunk data models and pivots with faster data model accelerationMaster all aspects of Splunk XML dashboards with hands-on applicationsApply ML algorithms for forecasting and anomaly detectionIntegrate advanced JavaScript charts and leverage Splunk's APIWho this book is for This Learning Path is for data analysts, business analysts, and IT administrators who want to leverage the Splunk enterprise platform as a valuable operational intelligence tool. Existing Splunk users who want to upgrade and get up and running with Splunk 7.x will also find this book useful. Some knowledge of Splunk services will help you get the most out of this Learning Path.

Learning Splunk Web Framework Packt Publishing
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 ...

Datadog Cloud Monitoring Quick Start Guide Apress
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.

Implementing Splunk - Big Data Reporting and Development for Operational Intelligence 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 {Power User Knowledge Manager} Certification Guide 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

Logging and Log Management 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.

Building Splunk Solutions 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

Improving Your Splunk Skills Packt Publishing Ltd
The 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.

Splunk Best Practices CreateSpace
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 8 5starcooks
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

Learning Splunk Web Framework 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. Downloading the example code for this book. You can download the example code files for all Packt books you have purchased from your account at http://www.Packt...

Splunk Certified Study Guide Newnes
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.

Splunk 7.x Quick Start Guide 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.