OMB No. 5078458112469

Splunk User Guide

Splunk Tutorial for Beginners (Cyber Security Tools) Splunk Basics Tutorial for Beginners | Cyber Security MUST WATCH ! Complete Guide in HD : Splunk Core Certified User | Detailed explanation with examples Splunk SIEM Crash Course | Free Spunk Training for Security Analyst Practical #Splunk - Zero to Hero #cybersecnerd Splunk ASAP Module 1 - What is Splunk? (beginner) Splunk Core Certified Power User SPLK 1002 - Practice Questions and Answers Splunk Training Video for Beginners | What is Splunk? | Spelkers E-Learning! | Part-1 Free Splunk Courses with Completion certificates from Splunk Basic Searching in Splunk 6.X Splunk Cybersecurity Defense Analyst (Beta) Bootcamp 1st session. Splunk Enterprise Security Training | Splunk Security Training | Intelllipaat Splunk Architecture | Splunk Components | Splunk Training for Beginners \u0026 Experienced | Splunk How To Pass The Splunk Core Certified User Exam | Everything You Need To Study and Pass SPLK 1001 Splunk Core Certified User 2024 Splunk Certification | Splunk Certification Path | Splunk Certified Power User and Admin Training Basic Searching in Splunk Enterprise Your First Splunk Certification Should be|Splunk Fundamentals 1|Splunk Core Certified User Splunk SIEM Basics For Beginners | TryHackMe Splunk: Basics Splunk Tutorial for Beginners | Splunk Installation and Configuration | Splunk Training | Edureka

Splunk Developer's Guide - Second Edition
Splunk 7 Essentials - Third Edition
Building Splunk Solutions (Second Edition)
Splunk 7 Essentials - Third Edition
Splunk 9.x Enterprise Certified Admin Guide
Improving Your Splunk Skills
Cyber Resiliency with Splunk Enterprise and IBM FlashSystem Storage Safeguarded Copy with IBM Copy Services Manager
Building Splunk Solutions
Implementing Splunk
Practical Docker with Python
Site Reliability Engineering
Building Splunk Solutions (. Conf2015 Edition)
Practical Splunk Search Processing Language
Splunk Essentials
Introduction to IBM Common Data Provider for z Systems
Splunk Operational Intelligence Cookbook
Splunk: Enterprise Operational Intelligence Delivered
SPLUNK Core Certified User Exam Practice Questions & Dumps
Splunk {Power User Knowledge Manager} Certification Guide
Mastering Splunk
Splunk Certified Study Guide
Advanced Splunk
User Interface Design for Programmers
Learning Splunk Web Framework

BECKER HOPE

OMB No. 5078458112469 edited by

Splunk Developer's Guide - Second Edition Apress
Learn to effectively use, configure, deploy and extend Splunk and implement its powerful

capabilities.

Splunk 7 Essentials - Third Edition

Packt Publishing Ltd
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 such areas as IT Operations, Information Security and the Internet of Things. This book is for anyone who needs to get reports and analytics from machine data. The first two chapters of the book will quickly get you started with a simple Splunk installation and set up of a sample machine data generator, called Eventgen. You will then learn about searching machine data and enriching it with additional fields to provide analytical value. 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,who can then create visualizations with point and click ease. You will also 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 in using Splunk, and information on how to build upon what you've learned in this book to take Splunk to your organization. Throughout the book, there will be additional comments and best practice recommendations from a member of the Splunk Trust community, called "Tips from the Fez". Splunk Trust is a Splunk-sponsored community of the top Splunk talent in the marketplace
Building Splunk Solutions (Second Edition) 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 forThis 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.

Splunk 7 Essentials - Third Edition

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 9.x Enterprise Certified Admin Guide

IBM Redbooks
This book will provide you with questions and answers that will prepare you for Splunk Power User (previously called Knowledge Manager) Certification Exam.
CreateSpace
Maximize the impact and precision of your message! Now in its fourth edition, the Microsoft Manual of Style provides essential guidance to content creators, journalists, technical writers, editors, and everyone else who writes about computer technology. Direct from the Editorial Style Board at Microsoft—you get a comprehensive glossary of both general technology terms and those specific to Microsoft; clear, concise usage and style guidelines with helpful examples and alternatives; guidance on grammar, tone, and voice; and best practices for writing content for the web, optimizing for accessibility, and communicating to a worldwide audience. Fully updated and optimized for ease of use, the Microsoft Manual of Style is designed to help you communicate clearly, consistently, and accurately about technical topics—across a range of audiences and media.

Improving Your Splunk Skills

Packt Publishing Ltd
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

Cyber Resiliency with Splunk Enterprise and IBM FlashSystem Storage Safeguarded Copy with IBM Copy Services Manager

Packt Publishing Ltd
Transform machine data into powerful analytical intelligence using Splunk Key Features 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 Book Description 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". 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 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.
Building Splunk Solutions Packt Publishing Ltd
IBM Common Data Provider for z Systems collects, filters, and formats IT operational data in near real-time and provides that data to target analytics solutions. IBM Common Data Provider for z Systems enables authorized IT operations teams using a single web-based interface to specify the IT operational data to be gathered and how it needs to be handled. This data is provided to both on- and off-platform analytic solutions, in a consistent, consumable format for analysis. This Redpaper discusses the value of IBM Common Data Provider for z Systems, provides a high-level reference architecture for IBM Common Data Provider for z Systems, and introduces key components of the architecture. It shows how IBM Common Data Provider for z Systems provides operational data to various analytic solutions. The publication provides high-level integration guidance, preferred practices, tips on planning for IBM Common Data Provider for z Systems, and example integration scenarios.
Implementing Splunk IBM Redbooks
You want to build a more diverse organization, but how will you shift your hiring practices? Learn the playbook from the world’s top talent executives and the global leader in diversity recruiting. Hiring for Diversity: The Guide to Building an Inclusive and Equitable Organization brings together the most cutting-edge practices for implementing a diversity hiring strategy that leaves your organization with a comprehensive view and an actionable plan. Using the author’s research-backed Equal Hiring Index ® and work with hundreds of leading employers, the book offers readers the most actionable examples of the policies and practices that inclusive hiring leaders employ today. You’ll learn: How to take stock of your existing hiring and retention practices to identify the most urgent and high impact opportunities Where to enact tactical changes to your hiring practices and policies that will reduce bias and improve accessibility How to develop a comprehensive diversity sourcing strategy by building a holistic understanding of underrepresented communities How to shift the mindset and behavior of people in your organization to collectively advance your diversity hiring efforts How to measure your progress and report your impact in your diversity hiring Perfect for human resources professionals, managers, executives, and board members, and existing and aspiring leaders passionate about diversity, Hiring for Diversity will also earn a prominent spot on the bookshelves of anyone interested in making the company they work in more inclusive, fair, and equitable.
Practical Docker with Python John Wiley & Sons

Learn the key differences between containers and virtual machines. Adopting a project based approach, this book introduces you to a simple Python application to be developed and containerized with Docker. After an introduction to Containers and Docker you'll be guided through Docker installation and configuration. You'll also learn basic functions and commands used in Docker by running a simple container using Docker commands. The book then moves on to developing a Python based Messaging Bot using required libraries and virtual environment where you'll add Docker Volumes to your project, ensuring your container data is safe. You'll create a database container and link your project to it and finally, bring up the Bot-associated database all at once with Docker Compose. What You'll Learn Build, run, and distribute Docker containers Develop a Python App and containerize it Use Dockerfile to run the Python App Define and run multi-container applications with Docker Compose Work with persisting data generated by and used by Docker containers Who This Book Is For Intermediate developers/DevOps practitioners who are looking to improve their build and release workflow by containerizing applications

Site Reliability Engineering Packt Publishing Ltd

Splunk Developer's GuidePackt Publishing Ltd

Building Splunk Solutions (. Conf2015 Edition) Apress

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.

Practical Splunk Search Processing Language 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.

Splunk Essentials 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 Description: Splunk 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.

Introduction to IBM Common Data Provider for z Systems Apress

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.

Splunk Operational Intelligence Cookbook Pearson Education

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.

Splunk: Enterprise Operational Intelligence Delivered Packt Publishing Ltd

Splunk is a type of analysis and reporting software for analyzing machine-generated Big Data. It captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations. It aims to make machine data

accessible across an organization for a variety of purposes. Implementing Splunk Second Edition is a learning guide that introduces you to all the latest features and improvements of Splunk 6.2. The book starts by introducing you to various concepts such as charting, reporting, clustering, and visualization. Every chapter is dedicated to enhancing your knowledge of a specific concept, including data models and pivots, speeding up your queries, backfilling, data replication, and so on. By the end of the book, you'll have a very good understanding of Splunk and be able to perform efficient data analysis.

SPLUNK Core Certified User Exam Practice Questions & Dumps 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 FeaturesBe well-versed with the Splunk 9. x architecture, installation, onboarding, and indexing data featuresCreate advanced visualizations using the Splunk search processing languageExplore advanced Splunk administration techniques, including clustering, data modeling, and container managementBook Description Splunk 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 learnInstall and configure the Splunk 9 environmentCreate advanced dashboards using the flexible layout options in Dashboard StudioUnderstand the Splunk licensing modelsCreate tables and make use of the various types of charts available in Splunk 9.xExplore the new configuration management featuresImplement the performance improvements introduced in Splunk 9.xIntegrate Splunk with Kubernetes for optimizing CI/CD managementWho 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 {Power User Knowledge Manager} Certification Guide Packt Publishing Ltd

What external factors influence the analytics technology domain and how are they evolving? Do you need different combination of analysis to improve the quality of analytic output? Splunk has enabled your organization to ask harder questions in easier ways? Is there already a lot of Splunk documentation? What does Splunk collect? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are you really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Splunk investments work better. This Splunk All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Splunk Self-Assessment. Featuring 852 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Splunk improvements can be made. In using the questions you will be better able to: - diagnose Splunk projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Splunk and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Splunk Scorecard, you will develop a clear picture of which Splunk areas need attention. Your purchase includes access details to the Splunk self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Splunk Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.