Using Elasticsearch Logstash And Kibana To Create

Deliver end-to-end real-time distributed data processing solutions by leveraging the power of Elastic Stack 6.0 Key Features - Get to grips with the new features introduced in Elastic Stack 6.0 - Get valuable insights from your data by working with the different components of the Elastic stack such as Elasticsearch, Logstash, Kibana, X-Pack, and Beats - Includes handy tips and techniques to build, deploy and manage your Elastic applications efficiently on-premise or on the cloud Book Description The Elastic Stack is a powerful combination of tools for distributed search, analytics, logging, and visualization of data from medium to massive data sets. The newly released Elastic Stack 6.0 brings new features and capabilities that empower users to find unique, actionable insights through these techniques. This book will give you a fundamental understanding of what the stack is all about, and how to use it efficiently to build powerful real-time data processing applications. After a quick overview of the newly introduced features in Elastic Stack 6.0, you'll learn how to set up the stack by installing the tools, and see their basic configurations. Then it shows you how to use Elasticsearch for distributed searching and analytics, along with Logstash for logging, and Kibana for data visualization. It also demonstrates the creation of custom plugins using Kibana and Beats. You'll find out about Elastic X-Pack, a useful extension for effective security and monitoring. We also provide useful tips on how to use the Elastic Cloud and deploy the Elastic Stack in production environments. On completing this book, you'll have a solid foundational knowledge of the basic Elastic Stack functionalities. You'll also have a good understanding of the role of each component in the stack to solve different data processing problems. What you will learn - Familiarize yourself with the different components of the Elastic Stack - Get to know the new functionalities introduced in Elastic Stack 6.0 - Effectively build your data pipeline to get data from terabytes or petabytes of data into Elasticsearch and Logstash for searching and logging - Use Kibana to visualize data and tell data stories in real-time - Secure, monitor, and use the alerting and reporting capabilities of Elastic Stack - Take your Elastic application to an on-premise or cloud-based production environment Who this book is for This book is for data professionals who want to get amazing insights and business metrics from their data sources. If you want to get a fundamental understanding of the Elastic Stack for distributed, real-time processing of data, this book will help you. A fundamental knowledge of JSON would be useful, but is not mandatory. No previous experience with the Elastic Stack is required.

This book highlights the emerging field of intelligent computing and developing smart systems. It includes chapters discussing the outcome of challenging research related to distributed computing, smart machines and their security related research, and also covers next-generation communication techniques and the networking technologies that have the potential to build the future communication infrastructure. Bringing together computing, communications and other aspects of intelligent and smart computing, it contributes to developing a roadmap for future research on intelligent systems.

A beginner's guide to analyzing and visualizing your Elasticsearch data using Kibana 7 and Timelion Key Features Gain a fundamental understanding of how Kibana operates within the Elastic Stack Explore your data with Elastic Graph and create rich dashboards in Kibana Learn scalable data visualization techniques in Kibana 7 Book Description Kibana is a window into the Elastic Stack, that enables the visual exploration and real-time analysis of your data in Elasticsearch. This book will help you understand the core concepts of the use of Kibana 7 for rich analytics and data visualization. If you're new to the tool or want to get to grips with the latest features introduced in Kibana 7, this book is the perfect beginner's guide. You'll learn how to set up and configure the Elastic Stack and understand where Kibana sits within the architecture. As you advance, you'll learn how to ingest data from different sources using Beats or Logstash into Elasticsearch, followed by exploring and visualizing data in Kibana. Whether working with time series data to create complex graphs using Timelion or embedding visualizations created in Kibana into your web applications, this book covers it all. It also covers topics that every Elastic developer needs to be aware of, such as installing and configuring Application Performance Monitoring (APM) servers and agents. Finally, you'll also learn how to create effective machine learning jobs in Kibana to find anomalies in your data. By the end of this book, you'll have a solid understanding of Kibana, and be able to create your own visual analytics solutions from scratch. What you will learn Explore the data-driven architecture of the Elastic Stack Install and set up Kibana 7 and other Elastic Stack components Use Beats and Logstash to get input from different data sources Create different visualizations using Kibana Build enterprise-grade Elastic dashboards from scratch Use Timelion to play with time series data Install and configure APM servers and APM agents Work with Dev Tools, Spaces, Graph, and other important tools Who this book is for If you're an aspiring Elastic developer or data analysts, this book is for you. You'll also find it useful if you want to get up to speed with the new features of Kibana 7 and perform data visualization on enterprise data. No prior knowledge of Kibana is expected, but some experience with Elasticsearch will be helpful.

This book gathers the proceedings of the 9th International Conference on Frontier Computing, held in Kyushu, Japan on July 9–12, 2019, and provides comprehensive coverage of the latest advances and trends in information technology, science and engineering. It addresses a number of broad themes, including communication networks, business intelligence and knowledge management, web intelligence, and related fields that inspire the development of information technology. The respective contributions cover a wide range of topics: database and data mining, networking and communications, web and internet of things, embedded systems, soft computing, social network analysis, security and privacy, optical communication, and ubiquitous/pervasive computing. Many of the papers outline promising future research directions, and the book will benefit students, researchers and professionals alike. Further, it offers a useful reference guide for newcomers to the field.

Build mesmerizing visualizations, analytics, and logs from your data using Elasticsearch, Logstash, and KibanaAbout This Book• Solve all your data analytics problems with the ELK stack• Explore the power of Kibana4 search and visualizations built over Elasticsearch queries and learn about the features and plugins of Logstash• Develop a complete data pipeline using the ELK stackWho This Book Is ForIf you are a developer or DevOps engineer interested in building a system that provides amazing insights and business metrics out of data sources, of various formats and types, using the open source technology stack that ELK provides, then this book is for you. Basic knowledge of Unix or any programming language will be helpful to make the most out of this book.What You Will Learn• Install, configure, and run Elasticsearch, Logstash, and Kibana• Understand the need for log analytics and the current challenges in log analysis• Build your own data pipeline using the ELK stack• Familiarize yourself with the key features of Logstash and the variety of input, filter, and output plugins it provides• Build your own custom

Logstash plugin• Create actionable insights using charts, histograms, and quick search features in Kibana4• Understand the role of Elasticsearch in the ELK stackIn DetailThe ELK stack—Elasticsearch, Logstash, and Kibana, is a powerful combination of open source tools. Elasticsearch is for deep search and data analytics. Logstash is for centralized logging, log enrichment, and parsing. Kibana is for powerful and beautiful data visualizations. In short, the Elasticsearch ELK stack makes searching and analyzing data easier than ever before.This book will introduce you to the ELK (Elasticsearch, Logstash, and Kibana) stack, starting by showing you how to set up the stack by installing the tools, and basic configuration. You'll move on to building a basic data pipeline using the ELK stack.Next, you'll explore the key features of Logstash and its role in the ELK stack, including creating Logstash plugins, which will enable you to use your own customized plugins. The importance of Elasticsearch and Kibana in the ELK stack is also covered, along with various types of advanced data analysis, and a variety of charts, tables ,and maps.Finally, by the end of the book you will be able to develop full-fledged data pipeline using the ELK stack and have a solid understanding of the role of each of the components.Style and approachThis book is a step-by-step guide, complete with various examples to solve your data analytics problems by using the ELK stack to explore and visualize data. Master the intricacies of Elasticsearch 7.0 and use it to create flexible and scalable search solutions Key Features Master the latest distributed search and analytics capabilities of Elasticsearch 7.0 Perform searching, indexing, and aggregation of your data at scale Discover tips and techniques for speeding up your search query performance Book Description Building enterprise-grade distributed applications and executing systematic search operations call for a strong understanding of Elasticsearch and expertise in using its core APIs and latest features. This book will help you master the advanced functionalities of Elasticsearch and understand how you can develop a sophisticated, real-time search engine confidently. In addition to this, you'll also learn to run machine learning jobs in Elasticsearch to speed up routine tasks. You'll get started by learning to use Elasticsearch features on Hadoop and Spark and make search results faster, thereby improving the speed of query results and enhancing the customer experience. You'll then get up to speed with performing analytics by building a metrics pipeline, defining queries, and using Kibana for intuitive visualizations that help provide decision-makers with better insights. The book will later guide you through using Logstash with examples to collect, parse, and enrich logs before indexing them in Elasticsearch. By the end of this book, you will have comprehensive knowledge of advanced topics such as Apache Spark support, machine learning using Elasticsearch and scikit-learn, and real-time analytics, along with the expertise you need to increase business productivity, perform analytics, and get the very best out of Elasticsearch. What you will learn Pre-process documents before indexing in ingest pipelines Learn how to model your data in the real world Get to grips with using Elasticsearch for exploratory data analysis Understand how to build analytics and RESTful services Use Kibana, Logstash, and Beats for dashboard applications Get up to speed with Spark and Elasticsearch for real-time analytics Explore the basics of Spring Data Elasticsearch, and understand how to index, search, and query in a Spring application Who this book is for This book is for Elasticsearch developers and data engineers who want to take their basic knowledge of Elasticsearch to the next level and use it to build enterprise-grade distributed search applications. Prior experience of working with Elasticsearch will be useful to get the most out of this book.

This book features high-quality research papers presented at the International Conference on Advanced Computing and Intelligent Engineering (ICACIE 2017). It includes sections describing technical advances in the fields of advanced computing and intelligent engineering, which are based on the presented articles. Intended for postgraduate students and researchers working in the discipline of computer science and engineering, the proceedings also appeal to researchers in the domain of electronics as it covers hardware technologies and future communication technologies.

"This course is a step-by-step guide to using Elasticsearch in combination with the rest of the ELK stack (now called Elastic Stack) to ship, parse, store, and analyze logs. You'll start this course by getting an understanding of what ElasticSearch is, what it's used for, and why it's important. Then, you'll be introduced to the new features in ElasticSearch 5.0. We'll go through each of the fundamental concepts of ElasticSearch such as queries, indices, and aggregation. You'll find out how to add more power to your searches using filters, ranges, and more. You'll also see how ElasticSearch can be used with the other components of the Elastic Stack such as LogStash, Kibana, and Beats. Finally, we'll take a walk through getting ElasticSearch up and running on the popular logstash Apache web log analysis. Aside from learning how to add more power to your searches with filters, ranges, and more, you'll also see how ElasticSearch can be used with the other components of the Elastic Stack such as LogStash, Kibana and Beats. Finally, we'll build, test and run our first Logstash pipeline to analyze Apache web logs. This step combines all the understanding of ElasticSearch, Logstash, Kibana and the lightweight data shipper FileBeat that we acquired from previous sections. By the end of this course, you will have a firm understanding of all the fundamentals of ElasticSearch 5.0, along with knowledge of practical real world usage."--Resource description page.

A step-by-step guide that will teach you how to use Elasticsearch in your application effectively KEY FEATURES ? Get familiar with the core concepts of Elasticsearch. ? Understand how the search engine works and how Elasticsearch is different from other similar tools. ? Learn to install Elasticsearch on different operating systems. ? Get familiar with the components of Elastic Stack such as Kibana, Logstash, and Beats, etc. ? Learn how to import data from different sources such as RDBMS, and files, etc DESCRIPTION In the modern Information Technology age, we are flooded with loads of data so we should know how to handle those data and transform them to fetch meaningful information. This book is here to help you manage the data using Elasticsearch. The book starts by covering the fundamentals of Elasticsearch and the concept behind it. After the introduction, you will learn how to install Elasticsearch on different platforms. You will then get to know about Index Management where you will learn to create, update, and delete Elasticsearch indices. Then you will understand how the Query DSL works and how to write some complex search queries using the Query DSL. After completing these basic features, you will move to some advanced topics. Under advanced topics, you will learn to handle Geodata which can be used to plot the data on a map. The book then focuses on Data Analysis using Aggregation. You will then learn how to tune Elasticsearch performance. The book ends with a chapter on Elasticsearch administration. WHAT YOU WILL LEARN ? Learn how to create and manage a cluster ? Work with different components of Elastic Stack ? Review the list of top Information Security certifications. ? Get to know more about Elasticsearch Index Management. ? Understand how to improve the performance by tuning Elasticsearch WHO THIS BOOK IS FOR This book is for

developers, architects, DBA, DevOps, and other readers who want to learn Elasticsearch efficiently and want to apply that in their application whether it is a new one or an existing one. It is also beneficial to those who want to play with their data using Elasticsearch. Basic computer programming is a prerequisite. TABLE OF CONTENTS 1 Getting started with Elasticsearch 2 Installation Elasticsearch 3 Working with Elastic Stack 4 Preparing your data 5 Importing Data into Elasticsearch 6 Managing Your Index 7 Apply Search on Your Data 8 Handling Geo with Elasticsearch 9 Aggregating Your Data 10 Improving the Performance 11 Administer Elasticsearch

When it comes to an architectural job role, that particular individual should be able to understand any infrastructure and should be capable of designing an efficient environment. This book will help you understand and achieve the level of knowledge required to architect and implement various IT solutions based on Linux.

Elastic has announced the integration of Prelert machine learning technology within its ecosystem allowing real-time generation of business insights from the Elasticsearch data without it leaving the cluster at all. This book will demonstrate these unique features and teach you to perform machine learning on the Elastic Stack without any hassle.

Learn advanced analytical techniques and leverage existing tool kits to make your analytic applications more powerful, precise, and efficient. This book provides the right combination of architecture, design, and implementation information to create analytical systems that go beyond the basics of classification, clustering, and recommendation. Pro Hadoop Data Analytics emphasizes best practices to ensure coherent, efficient development. A complete example system will be developed using standard third-party components that consist of the tool kits, libraries, visualization and reporting code, as well as support glue to provide a working and extensible end-to-end system. The book also highlights the importance of end-to-end, flexible, configurable, high-performance data pipeline systems with analytical components as well as appropriate visualization results. You'll discover the importance of mix-and-match or hybrid systems, using different analytical components in one application. This hybrid approach will be prominent in the examples. What You'll Learn Build big data analytic systems with the Hadoop ecosystem Use libraries, tool kits, and algorithms to make development easier and more effective Apply metrics to measure performance and efficiency of components and systems Connect to standard relational databases, noSQL data sources, and more Follow case studies with example components to create your own systems Who This Book Is For Software engineers, architects, and data scientists with an interest in the design and implementation of big data analytical systems using Hadoop, the Hadoop ecosystem, and other associated technologies.

DevOps for VMware® Administrators is the first book focused on using DevOps tools and practices with VMware technologies. The authors introduce high-value tools from third parties and VMware itself, and guide you through using them to improve the performance of all your virtualized systems and applications. You'll walk through automating and optimizing configuration management, provisioning, log management, continuous integration, and more. The authors also offer step-by-step coverage of deploying and managing applications at scale with Docker containers and Google Kubernetes. They conclude with an up-to-the-minute discussion of VMware's newest DevOps initiatives, including VMware vRealize Automation and VMware vRealize Code Stream. Coverage includes • Understanding the challenges that DevOps tools and practices can help VMware administrators to solve • Using Vagrant to quickly deploy Dev and Test environments that match production system specifications • Writing Chef "recipes" that streamline server configuration and maintenance • Simplifying Unix/Linux configuration management and orchestration with Ansible • Implementing Docker containers for faster and easier application management • Automating provisioning across the full lifecycle with Razor • Integrating Microsoft PowerShell Desired State Configuration (DSC) and VMware PowerCLI to automate key Windows Server and vSphere VM admin tasks • Using Puppet to automate infrastructure provisioning, configuration, orchestration, and reporting • Supercharging log management with ELK (Elasticsearch, Logstash, Kibana) • Supporting DevOps source code management with Git and continuous integration practices with Jenkins • Achieving continuous integration, delivery, and deployment with VMware's vRealize Code Stream

Summary Elasticsearch in Action teaches you how to build scalable search applications using Elasticsearch. You'll ramp up fast, with an informative overview and an engaging introductory example. Within the first few chapters, you'll pick up the core concepts you need to implement basic searches and efficient indexing. With the fundamentals well in hand, you'll go on to gain an organized view of how to optimize your design. Perfect for developers and administrators building and managing search-oriented applications. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Modern search seems like magic—you type a few words and the search engine appears to know what you want. With the Elasticsearch real-time search and analytics engine, you can give your users this magical experience without having to do complex low-level programming or understand advanced data science algorithms. You just install it, tweak it, and get on with your work. About the Book Elasticsearch in Action teaches you how to write applications that deliver professional quality search. As you read, you'll learn to add basic search features to any application, enhance search results with predictive analysis and relevancy ranking, and use saved data from prior searches to give users a custom experience. This practical book focuses on Elasticsearch's REST API via HTTP. Code snippets are written mostly in bash using cURL, so they're easily translatable to other languages. What's Inside What is a great search application? Building scalable search solutions Using Elasticsearch with any language Configuration and tuning About the Reader For developers and administrators building and managing search-oriented applications. About the Authors Radu Gheorghe is a search consultant and software engineer. Matthew Lee Hinman develops highly available, cloud-based systems. Roy Russo is a specialist in predictive analytics. Table of Contents PART 1 CORE ELASTICSEARCH FUNCTIONALITY Introducing Elasticsearch Diving into the functionality Indexing, updating, and deleting data Searching your data Analyzing your data Searching with relevancy Exploring your data with aggregations Relations among documents PART 2 ADVANCED ELASTICSEARCH FUNCTIONALITY Scaling out Improving performance Administering your cluster

Learn how to install, configure and implement the Elastic Stack (Elasticsearch, Logstash and Kibana) – the invaluable tool for anyone deploying a centralized log management solution for servers and apps. You will see how to use and configure Elastic Stack independently and alongside Puppet. Each chapter includes real-world examples and practical troubleshooting tips, enabling you to get up and running with Elastic Stack in record time. Fully customizable and easy to use, Elastic Stack enables you to be on top of your servers all the time, and resolve problems for your clients as fast as possible. Supported by Puppet and available with various plugins. Get started with Beginning Elastic Stack today and see why many consider Elastic Stack the best option for server log management. What You Will Learn: Install and configure Logstash Use Logstash with Elasticsearch and Kibana Use Logstash with Puppet and Foreman Centralize data processing Who This Book Is For: Anyone working on multiple servers who needs to search their logs using a web interface. It is ideal for server administrators who have just started their job and need to look after multiple servers efficiently.

Cyber-physical systems (CPS) and the Internet of Things (IoT) are rapidly developing technologies that are transforming our society. The disruptive transformation of the economy and society is expected due to the data collected by these systems, rather than the technological aspects of such as networks, embedded systems, and cloud technology. However, to create value out of the data, it must be transformed into information and therefore, expertise in data analytics and machine learning is the key component of future smart systems in cities and other applications. Big Data Analytics in Cyber-Physical Systems examines sensor signal processing, IoT gateways, optimization and decision making, intelligent mobility, and implementation of machine learning algorithms in embedded systems. This book focuses on the interaction between IoT technology and the mathematical tools to evaluate the extracted data of those systems. Each chapter provides different tools and applications in order to present a broad list of data analytics and machine learning tools in multiple IoT applications. Additionally, this volume addresses the education transfer needed to incorporate these technologies into our society by examining new platforms for IoT in schools, new courses and concepts for universities and adult education on IoT and data science. Fills the gap between IoT, CPS, and mathematical modeling Numerous use cases that discuss how concepts are applied in different domains and applications Provides "best practices," "real developments", and "winning stories" to complement technical information Uniquely covers contents within the context of mathematical foundations of signal processing and machine learning in CPS and IoT

"In the recent years - the term big data has been gaining popularity. And there has been a paradigm shift in the volume of information and the ways in which it can be extracted from this data. ELK is one of the few new-age frameworks which is capable of handling Big Data demands and scale. Over the years the ELK stack has become quite popular. And for a good reason. It is a very robust, mature and feature rich framework. ELK is used by large enterprises, government organizations and startups alike. The ELK stack has a very rich and active community behind it. They develop, share and support tons of source code, components, plugins and knowledge about these tools freely and openly. Imagine a large organization, which has information coming in from varied sources, at varied frequencies, and in various formats. It will be a herculean task to sort and sift through this data and normalize it to use for any comprehensive analysis. We will need a pretty versatile and flexible tool to deal with all these permutations of data streams. In this course, we will focus on one such enterprise data collection and collation tool, the LogStash which is one of the core components of the ELK stack. We will look at the overview and explore the technology that goes behind this tool."--Resource description page.

Store, search, and analyze your data with ease using Elasticsearch 5.x About This Book Get to grips with the basics of Elasticsearch concepts and its APIs, and use them to create efficient applications Create large-scale Elasticsearch clusters and perform analytics using aggregation This comprehensive guide will get you up and running with Elasticsearch 5.x in no time Who This Book Is For If you want to build efficient search and analytics applications using Elasticsearch, this book is for you. It will also benefit developers who have worked with Lucene or Solr before and now want to work with Elasticsearch. No previous knowledge of Elasticsearch is expected. What You Will Learn See how to set up and configure Elasticsearch and Kibana Know how to ingest structured and unstructured data using Elasticsearch Understand how a search engine works and the concepts of relevance and scoring Find out how to query Elasticsearch with a high degree of performance and scalability Improve the user experience by using autocomplete, geolocation queries, and much more See how to slice and dice your data using Elasticsearch aggregations. Grasp how to use Kibana to explore and visualize your data Know how to host on Elastic Cloud and how to use the latest X-Pack features such as Graph and Alerting In Detail Elasticsearch is a modern, fast, distributed, scalable, fault tolerant, and open source search and analytics engine. You can use Elasticsearch for small or large applications with billions of documents. It is built to scale horizontally and can handle both structured and unstructured data. Packed with easy-to- follow examples, this book will ensure you will have a firm understanding of the basics of Elasticsearch and know how to utilize its capabilities efficiently. You will install and set up Elasticsearch and Kibana, and handle documents using the Distributed Document Store. You will see how to query, search, and index your data, and perform aggregation-based analytics with ease. You will see how to use Kibana to explore and visualize your data. Further on, you will learn to handle document relationships, work with geospatial data, and much more, with this easy-to-follow guide. Finally, you will see how you can set up and scale your Elasticsearch clusters in production environments. Style and approach This comprehensive guide will get you started with Elasticsearch 5.x, so you build a solid understanding of the basics. Every topic is explained in depth and is supplemented with practical examples to enhance your understanding.

Get the most out of the Elastic Stack for various complex analytics using this comprehensive and practical guide About This Book Your one-stop solution to perform advanced analytics with Elasticsearch, Logstash, and Kibana Learn how to make better sense of your data by searching, analyzing, and logging data in a systematic way This highly practical guide takes you through an advanced implementation on the ELK stack in your enterprise environment Who This Book Is For This book cater to developers using the Elastic stack in their day-to-day work who are familiar with the basics of Elasticsearch, Logstash, and Kibana, and now want to become an expert at using the Elastic stack for data analytics. What You Will Learn Build a pipeline with help of Logstash and Beats to visualize Elasticsearch data in Kibana Use Beats to ship any type of data to the Elastic stack Understand Elasticsearch APIs, modules, and other advanced concepts Explore Logstash and it's plugins Discover how to utilize the new Kibana UI for advanced analytics See how to work with the Elastic Stack using other advanced configurations Customize the

Elastic Stack and plugin development for each of the component Work with the Elastic Stack in a production environment Explore the various components of X-Pack in detail. In Detail Even structured data is useless if it can't help you to take strategic decisions and improve existing system. If you love to play with data, or your job requires you to process custom log formats, design a scalable analysis system, and manage logs to do real-time data analysis, this book is your one-stop solution. By combining the massively popular Elasticsearch, Logstash, Beats, and Kibana, elastic.co has advanced the end-to-end stack that delivers actionable insights in real time from almost any type of structured or unstructured data source. If your job requires you to process custom log formats, design a scalable analysis system, explore a variety of data, and manage logs, this book is your one-stop solution. You will learn how to create real-time dashboards and how to manage the life cycle of logs in detail through real-life scenarios. This book brushes up your basic knowledge on implementing the Elastic Stack and then dives deeper into complex and advanced implementations of the Elastic Stack. We'll help you to solve data analytics challenges using the Elastic Stack and provide practical steps on centralized logging and real-time analytics with the Elastic Stack in production. You will get to grip with advanced techniques for log analysis and visualization. Newly announced features such as Beats and X-Pack are also covered in detail with examples. Toward the end, you will see how to use the Elastic stack for real-world case studies and we'll show you some best practices and troubleshooting techniques for the Elastic Stack. Style and approach This practical guide shows you how to perform advanced analytics with the Elastic stack through real-world use cases. It includes common and some not so common scenarios to use the Elastic stack for data analysis.
Learning ELK StackPackt Publishing Ltd
A developer's field-guide to designing scalable services using Kubernetes Key Features Develop and run your software using containers within a Kubernetes environment Get hands-on experience of using Kubernetes with DevOps concepts such as continuous integration, benchmark testing, monitoring, and so on Pragmatic example-based approach showing how to use Kubernetes in the development process Book Description Kubernetes is documented and typically approached from the perspective of someone running software that has already been built. Kubernetes may also be used to enhance the development process, enabling more consistent testing and analysis of code to help developers verify not only its correctness, but also its efficiency. This book introduces key Kubernetes concepts, coupled with examples of how to deploy and use them with a bit of Node.js and Python example code, so that you can quickly replicate and use that knowledge. You will begin by setting up Kubernetes to help you develop and package your code. We walk you through the setup and installation process before working with Kubernetes in the development environment. We then delve into concepts such as automating your build process, autonomic computing, debugging, and integration testing. This book covers all the concepts required for a developer to work with Kubernetes. By the end of this book, you will be in a position to use Kubernetes in development ecosystems. What you will learn Build your software into containers Deploy and debug software running in containers within Kubernetes Declare and add configuration through Kubernetes Define how your application fits together, using internal and external services Add feedback to your code to help Kubernetes manage your services Monitor and measure your services through integration testing and in production deployments Who this book is for If you are a full-stack or back-end software developers interested, curious, or being asked to test as well as run the code you're creating, you can leverage Kubernetes to make that process simpler and consistent regardless of where you deploy. If you're looking for developer focused examples in NodeJS and Python for how to build, test, deploy, and run your code with Kubernetes, this is perfect for you.
Build mesmerizing visualizations, analytics, and logs from your data using Elasticsearch, Logstash, and Kibana About This Book Solve all your data analytics problems with the ELK stack Explore the power of Kibana4 search and visualizations built over Elasticsearch queries and learn about the features and plugins of Logstash Develop a complete data pipeline using the ELK stack Who This Book Is For If you are a developer or DevOps engineer interested in building a system that provides amazing insights and business metrics out of data sources, of various formats and types, using the open source technology stack that ELK provides, then this book is for you. Basic knowledge of Unix or any programming language will be helpful to make the most out of this book. What You Will Learn Install, configure, and run Elasticsearch, Logstash, and Kibana Understand the need for log analytics and the current challenges in log analysis Build your own data pipeline using the ELK stack Familiarize yourself with the key features of Logstash and the variety of input, filter, and output plugins it provides Build your own custom Logstash plugin Create actionable insights using charts, histograms, and quick search features in Kibana4 Understand the role of Elasticsearch in the ELK stack In Detail The ELK stack—Elasticsearch, Logstash, and Kibana, is a powerful combination of open source tools. Elasticsearch is for deep search and data analytics. Logstash is for centralized logging, log enrichment, and parsing. Kibana is for powerful and beautiful data visualizations. In short, the Elasticsearch ELK stack makes searching and analyzing data easier than ever before. This book will introduce you to the ELK (Elasticsearch, Logstash, and Kibana) stack, starting by showing you how to set up the stack by installing the tools, and basic configuration. You'll move on to building a basic data pipeline using the ELK stack. Next, you'll explore the key features of Logstash and its role in the ELK stack, including creating Logstash plugins, which will enable you to use your own customized plugins. The importance of Elasticsearch and Kibana in the ELK stack is also covered, along with various types of advanced data analysis, and a variety of charts, tables ,and maps. Finally, by the end of the book you will be able to develop full-fledged data pipeline using the ELK stack and have a solid understanding of the role of each of the components. Style and approach This book is a step-by-step guide, complete with various examples to solve your data analytics problems by using the ELK stack to explore and visualize data.
A beginner's guide to storing, managing, and analyzing data with the updated features of Elastic 7.0 Key Features Gain access to new features and updates introduced in Elastic Stack 7.0 Grasp the fundamentals of Elastic Stack including Elasticsearch, Logstash, and Kibana Explore useful tips for using Elastic Cloud and deploying Elastic Stack in production environments Book Description The Elastic Stack is a powerful combination of tools for techniques such as distributed search, analytics, logging, and visualization of data. Elastic Stack 7.0 encompasses new features and capabilities that will enable you to find unique insights into analytics using these techniques. This book will give you a fundamental understanding of what the stack is all about, and help you use it efficiently to build powerful real-time data processing applications. The first few sections of the book will help you understand how to set up the stack by installing tools, and exploring their basic configurations. You'll then get up to speed with using Elasticsearch for distributed searching and analytics, Logstash for logging, and Kibana for data visualization. As you

work through the book, you will discover the technique of creating custom plugins using Kibana and Beats. This is followed by coverage of the Elastic X-Pack, a useful extension for effective security and monitoring. You'll also find helpful tips on how to use Elastic Cloud and deploy Elastic Stack in production environments. By the end of this book, you'll be well versed with the fundamental Elastic Stack functionalities and the role of each component in the stack to solve different data processing problems. What you will learn Install and configure an Elasticsearch architecture Solve the full-text search problem with Elasticsearch Discover powerful analytics capabilities through aggregations using Elasticsearch Build a data pipeline to transfer data from a variety of sources into Elasticsearch for analysis Create interactive dashboards for effective storytelling with your data using Kibana Learn how to secure, monitor and use Elastic Stack's alerting and reporting capabilities Take applications to an on-premise or cloud-based production environment with Elastic Stack Who this book is for This book is for entry-level data professionals, software engineers, e-commerce developers, and full-stack developers who want to learn about Elastic Stack and how the real-time processing and search engine works for business analytics and enterprise search applications. Previous experience with Elastic Stack is not required, however knowledge of data warehousing and database concepts will be helpful. Use the ELK (Elasticsearch, Logstash, and Kibana) stack to build systems that provide actionable insights and business metrics from data sources, including creating amazing visualizations and dashboards. Learn how to set up the ELK stack, build a data pipeline, and create customized plugins. Applied ELK Stack will teach you to configure the software, install tools, and build a data pipeline. You will learn the key features of Logstash and its role in the ELK stack, including creating Logstash plugins, which will enable you to use your own customized plugins. The importance of Elasticsearch and Kibana in the ELK stack is covered, along with various types of advanced data analysis, including charts, tables, and maps. The simple and powerful nature of ELK stack has contributed to its quick adoption. With this book you will learn: The need for log analytics, and current challenges How to perform real-time data analytics on streaming data, and turn them into actionable insights How to create indexing and delete data The different components of ELK (Elasticsearch, Logstash, and Kibana) stack Shipping, Filtering, and Parsing Events with Logstash How to build amazing visualizations and dashboards using Data Discovery, Visualization, and Dashboard with Kibana

Use the functionalities of Kibana to discover data and build attractive visualizations and dashboards for real-world scenarios About This Book Perform real-time data analytics and visualizations, on streaming data, using Kibana Build beautiful visualizations and dashboards with simplicity and ease without any type of coding involved Learn all the core concepts as well as detailed information about each component used in Kibana Who This Book Is For Whether you are new to the world of data analytics and data visualization or an expert, this book will provide you with the skills required to use Kibana with ease and simplicity for real-time data visualization of streaming data. This book is intended for those professionals who are interested in learning about Kibana,its installations, and how to use it . As Kibana provides a user-friendly web page, no prior experience is required. What You Will Learn Understand the basic concepts of elasticsearch used in Kibana along with step by step guide to install Kibana in Windows and Ubuntu Explore the functionality of all the components used in Kibana in detail, such as the Discover, Visualize, Dashboard,and Settings pages Analyze data using the powerful search capabilities of elasticsearch Understand the different types of aggregations used in Kibana for visualization Create and build different types of amazing visualizations and dashboards easily Create, save, share, embed, and customize the visualizations added to the dashboard Customize and tweak the advanced settings of Kibana to ensure ease of use In Detail With the increasing interest in data analytics and visualization of large data around the globe, Kibana offers the best features to analyze data and create attractive visualizations and dashboards through simple-to-use web pages. The variety of visualizations provided, combined with the powerful underlying elasticsearch capabilities will help professionals improve their skills with this technology. This book will help you quickly familiarize yourself to Kibana and will also help you to understand the core concepts of this technology to build visualizations easily. Starting with setting up of Kibana and elasticsearch in Windows and Ubuntu, you will then use the Discover page to analyse your data intelligently. Next, you will learn to use the Visualization page to create beautiful visualizations without the need for any coding. Then, you will learn how to use the Dashboard page to create a dashboard and instantly share and embed the dashboards. You will see how to tweak the basic and advanced settings provided in Kibana to manage searches, visualizations, and dashboards. Finally, you will use Kibana to build visualizations and dashboards for real-world scenarios. You will quickly master the functionalities and components used in Kibana to create amazing visualizations based on real-world scenarios. With ample screenshots to guide you through every step, this book will assist you in creating beautiful visualizations with ease. Style and approach This book is a comprehensive step-by-step guide to help you understand Kibana. It's explained in an easy-to-follow style along with supporting images. Every chapter is explained sequentially , covering the basics of each component of Kibana and providing detailed explanations of all the functionalities of Kibana that appeal.

Get to grips with Kibana and its advanced functions to create interactive visualizations and dashboards Key Features Explore visualizations and perform histograms, stats, and map analytics Unleash X-Pack and Timelion, and learn alerting, monitoring, and reporting features Manage dashboards with Beats and create machine learning jobs for faster analytics Book Description Kibana is one of the popular tools among data enthusiasts for slicing and dicing large datasets and uncovering Business Intelligence (BI) with the help of its rich and powerful visualizations. To begin with, Mastering Kibana 6.x quickly introduces you to the features of Kibana 6.x, before teaching you how to create smart dashboards in no time. You will explore metric analytics and graph exploration, followed by understanding how to quickly customize Kibana dashboards. In addition to this, you will learn advanced analytics such as maps, hits, and list analytics. All this will help you enhance your skills in running and comparing multiple queries and filters, influencing your data visualization skills at scale. With Kibana's Timelion feature, you can analyze time series data with histograms and stats analytics. By the end of this book, you will have created a speedy machine learning job using X-Pack capabilities. What you will learn Create unique dashboards with various intuitive data visualizations Visualize Timelion expressions with added histograms and stats analytics Integrate X-Pack with your Elastic Stack in simple steps Extract data from Elasticsearch for advanced analysis and anomaly detection using dashboards Build dashboards from web applications for application logs Create monitoring and alerting dashboards using Beats Who this book is for Mastering Kibana 6.x is for you if you are a big data engineer, DevOps engineer, or data scientist aspiring to go beyond data visualization at scale and gain maximum insights from their large datasets. Basic knowledge of Elasticstack will be an added advantage, although not mandatory.

A quick start guide to visualize your Elasticsearch data Key Features Your hands-on guide to visualizing the Elasticsearch data as well as navigating the Elastic stack Work with different Kibana plugins and create effective machine learning jobs using Kibana Build effective dashboards and reports without any hassle Book Description The Elastic Stack is growing rapidly and, day by day, additional tools are being added to make it more effective. This book endeavors to explain all the important aspects of Kibana, which is essential for utilizing its full potential. This book covers the core concepts of Kibana, with chapters set out in a coherent manner so that readers can advance their learning in a step-by-step manner. The focus is on a practical approach, thereby enabling the reader to apply those examples in real time for a better understanding of the concepts and to provide them with the correct skills in relation to the tool. With its succinct explanations, it is quite easy for a reader to use this book as a reference guide for learning basic to advanced implementations of Kibana. The practical examples, such as the creation of Kibana dashboards from CSV data, application RDBMS data, system metrics data, log file data, APM agents, and search results, can provide readers with a number of different drop-off points from where they can fetch any type of data into Kibana for the purpose of analysis or dashboarding. What you will

learn Explore how Logstash is configured to fetch CSV data Understand how to create index patterns in Kibana Become familiar with how to apply filters on data Discover how to create ML jobs Explore how to analyze APM data from APM agents Get to grips with how to save, share, inspect, and edit visualizations Understand how to find an anomaly in data Who this book is for Kibana 7 Quick Start Guide is for developers new to Kibana who want to learn the fundamentals of using the tool for visualization, as well as existing Elastic developers.

Learn to develop, test, and deploy your Spring Boot distributed application and explore various best practices. Key Features Build and deploy your microservices architecture in the cloud Build event-driven resilient systems using Hystrix and Turbine Explore API management tools such as KONG and API documentation tools such as Swagger Book Description Spring is one of the best frameworks on the market for developing web, enterprise, and cloud ready software. Spring Boot simplifies the building of complex software dramatically by reducing the amount of boilerplate code, and by providing production-ready features and a simple deployment model. This book will address the challenges related to power that come with Spring Boot's great configurability and flexibility. You will understand how Spring Boot configuration works under the hood, how to overwrite default configurations, and how to use advanced techniques to prepare Spring Boot applications to work in production. This book will also introduce readers to a relatively new topic in the Spring ecosystem – cloud native patterns, reactive programming, and applications. Get up to speed with microservices with Spring Boot and Spring Cloud. Each chapter aims to solve a specific problem or teach you a useful skillset. By the end of this book, you will be proficient in building and deploying your Spring Boot application. What you will learn Build logically structured and highly maintainable Spring Boot applications Configure RESTful microservices using Spring Boot Make the application production and operation-friendly with Spring Actuator Build modern, high-performance distributed applications using cloud patterns Manage and deploy your Spring Boot application to the cloud (AWS) Monitor distributed applications using log aggregation and ELK Who this book is for The book is targeted at experienced Spring and Java developers who have a basic knowledge of working with Spring Boot. The reader should be familiar with Spring Boot basics, and aware of its benefits over traditional Spring Framework-based applications.

"Elasticsearch is a powerful tool not only for powering search on big websites, but also for analyzing big data sets in a matter of milliseconds! It's an increasingly popular technology, and a valuable skill to have in today's job market. We'll cover setting up search indices on an Elasticsearch cluster, and querying that data in many different ways. Fuzzy searches, partial matches, search-as-you-type, pagination, sorting - you name it. And it's not just theory, every lesson has hands-on examples where you'll practice each skill using a virtual machine running Elasticsearch on your own PC. We cover, in depth, the often-overlooked problem of importing data into an Elasticsearch index. Whether it's via raw RESTful queries, scripts using Elasticsearch API's, or integration with other "big data" systems like Spark and Kafka - you'll see many ways to get Elasticsearch started from large, existing data sets at scale. We'll also stream data into Elasticsearch using Logstash and Filebeat - commonly referred to as the "ELK Stack" (Elasticsearch / Logstash / Kibana) or the "Elastic Stack". Elasticsearch isn't just for search anymore - it has powerful aggregation capabilities for structured data. We'll bucket and analyze data using Elasticsearch, and visualize it using the Elastic Stack's web UI, Kibana. Elasticsearch is positioning itself to be a much faster alternative to Hadoop, Spark, and Flink for many common data analysis requirements. It's an important tool to understand, and it's easy to use! Dive in with me and I'll show you what it's all about."--Resource description page.

Search, analyze, and manage data effectively with Elasticsearch 7 Key Features Extend Elasticsearch functionalities and learn how to deploy on Elastic Cloud Deploy and manage simple Elasticsearch nodes as well as complex cluster topologies Explore the capabilities of Elasticsearch 7 with easy-to-follow recipes Book Description Elasticsearch is a Lucene-based distributed search server that allows users to index and search unstructured content with petabytes of data. With this book, you'll be guided through comprehensive recipes on what's new in Elasticsearch 7, and see how to create and run complex queries and analytics. Packed with recipes on performing index mapping, aggregation, and scripting using Elasticsearch, this fourth edition of Elasticsearch Cookbook will get you acquainted with numerous solutions and quick techniques for performing both every day and uncommon tasks such as deploying Elasticsearch nodes, integrating other tools to Elasticsearch, and creating different visualizations. You will install Kibana to monitor a cluster and also extend it using a variety of plugins. Finally, you will integrate your Java, Scala, Python, and big data applications such as Apache Spark and Pig with Elasticsearch, and create efficient data applications powered by enhanced functionalities and custom plugins. By the end of this book, you will have gained in-depth knowledge of implementing Elasticsearch architecture, and you'll be able to manage, search, and store data efficiently and effectively using Elasticsearch. What you will learn Create an efficient architecture with Elasticsearch Optimize search results by executing analytics aggregations Build complex queries by managing indices and documents Monitor the performance of your cluster and nodes Design advanced mapping to take full control of index steps Integrate Elasticsearch in Java, Scala, Python, and big data applications Install Kibana to monitor clusters and extend it for plugins Who this book is for If you're a software engineer, big data infrastructure engineer, or Elasticsearch developer, you'll find this book useful. This Elasticsearch book will also help data professionals working in the e-commerce and FMCG industry who use Elastic for metrics evaluation and search analytics to get deeper insights for better business decisions. Prior experience with Elasticsearch will help you get the most out of this book.

Whether you need full-text search or real-time analytics of structured data—or both—the Elasticsearch distributed search engine is an ideal way to put your data to work. This practical guide not only shows you how to search, analyze, and explore data with Elasticsearch, but also helps you deal with the complexities of human language, geolocation, and relationships. If you're a newcomer to both search and distributed systems, you'll quickly learn how to integrate Elasticsearch into your application. More experienced users will pick up lots of advanced techniques. Throughout the book, you'll follow a problem-based approach to learn why, when, and how to use Elasticsearch features. Understand how Elasticsearch interprets data in your documents Index and query your data to take advantage of search concepts such as relevance and word proximity Handle human language through the effective use of analyzers and queries Summarize and group data to show overall trends, with aggregations and analytics Use geo-points and geo-shapes—Elasticsearch's approaches to geolocation Model your data to take advantage of Elasticsearch's horizontal scalability Learn how to configure and monitor your cluster in production

A new book designed for SysAdmins, Operations staff, Developers and DevOps who are interested in deploying a log management solution using the open source tool Logstash. In this book we will walk you through installing, deploying, managing and extending Logstash. We'll teach you how to: * Install and deploy Logstash. * Ship events from a Logstash Shipper to a central Logstash server. * Filter incoming events using a variety of techniques. * Output those events to a selection of useful destinations. * Use Logstash's awesome web interface Kibana. * Scale out your Logstash implementation as your environment grows. * Quickly and easily extend Logstash to deliver additional functionality you might need. By the end of the book you should have a functional and effective log management solution that you can deploy into your own environment.

Have you ever found yourself questioning whether your network is in good hands? Did you do everything you could to defend against exploits on your network? Is your employer safe because you have one of the best Security Information Event Management (SIEM) setups you can use monitoring the network for you? Or, maybe you are new to Information Security and you want to learn how to employ a robust Intrusion Detection System (IDS) but you do not know where to start. If you have ever asked yourself any of these questions, or you just want to learn about ELK Stack and Zeek (Bro), you have come to the right place. A quick Google search will show you there isn't a lot of information for configuring Zeek (Bro), ElasticSearch, Logstash, Filebeat, and Kibana- it is rather complicated because the websites will describe how to install, but they don't really lead you to specifics on what else you need to do, or they are really outdated. That is where you must piece together the information yourself, and really research -

lucky for you, I did the leg work for you and decided to write this book. Whether you have been in the Information Security industry for many years or you're just getting started this book has something for you. In my time studying over the years I've always found that a lot of books are interesting reads, but they add a lot of fluff. That was not my goal with this book; I wanted to provide you with a straight forward book without the fluff, that will show you exactly what you need - I cover the basics, and then explain the intricacies involved with configuring a SIEM that is reliable. I also provide a step-by-step process, while including any pertinent notes that you need to pay attention to, and lastly providing a breakdown of what is occurring at that time. Having background to each section and knowing what is happening is extremely important to learning and understanding what is happening on your network. Likewise, this book covers a brief overview of different programming languages, and their configuration nuances when applied to Zeek (Bro) and Elk Stack. I tried my best to approach this as if you did not know anything, so that anyone can read this and understand what is happening throughout the installation and configuration process. Let us get to the basics of what will be covered in this book so that you have a good idea of what you will learn. The first section of this book covers the Zeek(Bro) IDS installation and configuration. Furthermore, you will learn about the origin of Zeek (Bro), and the many features that Zeek (Bro) has to offer. This section will walk you through the entire installation process, while providing explanations for the configuration changes that we make on the system. There are a lot of dependencies needed to install Zeek (bro), and I will walk you through that entire process. We will also go over installing PF_ring - a tool for increased capture speeds and network capture optimization. The tool is very useful when capturing data on large networks, and from multiple nodes. In the next section we will go over installing Tor, and Privoxy for network anonymity. You're probably asking yourself why you would want to do that when setting up a SIEM or IDS. The simple answer is that in order to know what's traversing the network, you need to understand what it is doing and how to use it yourself. Sometimes the best defense comes from knowing what the offense is using. Once we install Tor, you can generate some Tor traffic on your network, and watch as one of the custom Zeek (Bro) signatures - I will teach you about in this book - detects this traffic so you can see what it looks like once a notice is generated. It's also good to know how to remain anonymous on the network if you're ever doing any type of forensic investigations too, so learning this is always a plus. ...

Exploit the visualization capabilities of Kibana and build powerful interactive dashboards About This Book Introduction to data-driven architecture and the Elastic stack Build effective dashboards for data visualization and explore datasets with Elastic Graph A comprehensive guide to learning scalable data visualization techniques in Kibana Who This Book Is For If you are a developer, data visualization engineer, or data scientist who wants to get the best of data visualization at scale then this book is perfect for you. A basic understanding of Elasticsearch and Logstash is required to make the best use of this book. What You Will Learn How to create visualizations in Kibana Ingest log data, structure an Elasticsearch cluster, and create visualization assets in Kibana Embed Kibana visualization on web pages Scaffold, develop, and deploy new Kibana & Timelion customizations Build a metrics dashboard in Timelion based on time series data Use the Graph plugin visualization feature and leverage a graph query Create, implement, package, and deploy a new custom plugin Use Prelert to solve anomaly detection challenges In Detail Kibana is an open source data visualization platform that allows you to interact with your data through stunning, powerful graphics. Its simple, browser-based interface enables you to quickly create and share dynamic dashboards that display changes to Elasticsearch queries in real time. In this book, you'll learn how to use the Elastic stack on top of a data architecture to visualize data in real time. All data architectures have different requirements and expectations when it comes to visualizing the data, whether it's logging analytics, metrics, business analytics, graph analytics, or scaling them as per your business requirements. This book will help you master Elastic visualization tools and adapt them to the requirements of your project. You will start by learning how to use the basic visualization features of Kibana 5. Then you will be shown how to implement a pure metric analytics architecture and visualize it using Timelion, a very recent and trendy feature of the Elastic stack. You will learn how to correlate data using the brand-new Graph visualization and build relationships between documents. Finally, you will be familiarized with the setup of a Kibana development environment so that you can build a custom Kibana plugin. By the end of this book you will have all the information needed to take your Elastic stack skills to a new level of data visualization. Style and approach This book takes a comprehensive, step-by-step approach to working with the visualization aspects of the Elastic stack. Every concept is presented in a very easy-to-follow manner that shows you both the logic and method of implementation. Real world cases are referenced to highlight how each of the key concepts can be put to practical use.

Get the most out of Elasticsearch 7's new features to build, deploy, and manage efficient applications Key Features Discover the new features introduced in Elasticsearch 7 Explore techniques for distributed search, indexing, and clustering Gain hands-on knowledge of implementing Elasticsearch for your enterprise Book Description Elasticsearch is one of the most popular tools for distributed search and analytics. This Elasticsearch book highlights the latest features of Elasticsearch 7 and helps you understand how you can use them to build your own search applications with ease. Starting with an introduction to the Elastic Stack, this book will help you quickly get up to speed with using Elasticsearch. You'll learn how to install, configure, manage, secure, and deploy Elasticsearch clusters, as well as how to use your deployment to develop powerful search and analytics solutions. As you progress, you'll also understand how to troubleshoot any issues that you may encounter along the way. Finally, the book will help you explore the inner workings of Elasticsearch and gain insights into queries, analyzers, mappings, and aggregations as you learn to work with search results. By the end of this book, you'll have a basic understanding of how to build and deploy effective search and analytics solutions using Elasticsearch. What you will learn Install Elasticsearch and use it to safely store data and retrieve it when needed Work with a variety of analyzers and filters Discover techniques to improve search results in Elasticsearch Understand how to perform metric and bucket aggregations Implement best practices for moving clusters and applications to production Explore various techniques to secure your Elasticsearch clusters Who this book is for This book is for software developers, engineers, data architects, system administrators, and anyone who wants to get up and running with Elasticsearch 7. No prior experience with Elasticsearch is required.

A beginner's guide to storing, managing, and analyzing data with the updated features of Elastic 7.0 Key Features Gain access to new features and updates introduced in Elastic Stack 7.0 Grasp the fundamentals of Elastic Stack including Elasticsearch, Logstash, and Kibana Explore useful tips for using Elastic Cloud and deploying Elastic Stack in production environments Book Description The Elastic Stack is a powerful combination of tools that help in performing distributed search, analytics, logging, and visualization of data. Elastic Stack 7.0 encompasses new features and capabilities that will enable you to find unique insights into analytics using these techniques. This book will give you a fundamental understanding of what the stack is all about, and guide you in using it efficiently to build powerful real-time data processing applications. The first few sections of the book will help you understand how to set up the stack by installing tools and exploring their basic configurations. You'll then get up to speed with using Elasticsearch for distributed search and analytics, Logstash for logging, and Kibana for data visualization. As you work through the book, you will discover the technique of creating custom plugins using Kibana and Beats. This is followed by coverage of the Elastic X-Pack, a useful extension for effective security and monitoring. You'll also find helpful tips on how to use Elastic Cloud and deploy Elastic Stack in production environments. By the end of this book, you'll be well-versed with fundamental Elastic Stack functionalities and the role of each component in the stack to solve different data processing problems. What you will learn Install and configure an Elasticsearch architecture Solve the full-text search problem with Elasticsearch Discover powerful analytics capabilities through aggregations using Elasticsearch Build a data pipeline to transfer data from a variety of sources into Elasticsearch for analysis Create interactive dashboards for effective storytelling with your data using Kibana Secure, monitor, and use Elastic Stack's alerting and reporting capabilities Take applications to an on-premise or cloud-based production environment with Elastic Stack Who this book is for This book is for entry-level data

professionals, software engineers, e-commerce developers, and full-stack developers who want to learn about Elastic Stack and understand how the real-time processing and search engine works for business ana ...

Use the ELK (Elasticsearch, Logstash, and Kibana) stack to build systems that provide actionable insights and business metrics from data sources, including creating amazing visualizations and dashboards. Learn how to set up the ELK stack, build a data pipeline, and create customized plugins. Practical ELK Stack will teach you to configure the software, install tools, and build a data pipeline. You will learn the key features of Logstash and its role in the ELK stack, including creating Logstash plugins, which will enable you to use your own customized plugins. The importance of Elasticsearch and Kibana in the ELK stack is covered, along with various types of advanced data analysis, including charts, tables, and maps. The simple and powerful nature of ELK stack has contributed to its quick adoption. Diverse scenarios are covered, ranging from social media analysis to grid monitoring at CERN. You will see how ELK stack is being used at companies such as Facebook, Github, and Netflix. With this book you will learn: The need for log analytics, and current challenges How to perform real-time data analytics on streaming data, and turn them into actionable insights How to create indexing and delete data The different components of ELK (Elasticsearch, Logstash, and Kibana) stack Shipping, Filtering, and Parsing Events with Logstash How to build amazing visualizations and dashboards using Data Discovery, Visualization, and Dashboard with Kibana Who this book is for: This book is for developers or DevOps Engineers interested in building systems that provide amazing insights and business metrics out of different data sources using the ELK stack.

Copyright: 8da3bae54e2e787c832324c505eba748