1ST EDITION

Kibana 8.x – A Quick Start Guide to Data Analysis

Learn about data exploration, visualization, and dashboard building with Kibana

KRISHNA SHAH

Kibana 8.x – A Quick Start Guide to Data Analysis

Learn about data exploration, visualization, and dashboard building with Kibana

Krishna Shah

‹packt›

Kibana 8.x – A Quick Start Guide to Data Analysis

Associate Group Product Manager: Kaustubh Manglurkar
Associate Publishing Product Manager: Heramb Bhavsar
Book Project Manager: Kirti Pisat
Senior Editor: Tiksha Lad
Technical Editor: Rahul Limbachiya
Copy Editor: Safis Editing
Proofreader: Safis Editing
Indexer: Pratik Shirodkar
Production Designer: Joshua Misquitta
Senior DevRel Marketing Coordinator: Nivedita Singh

First published: February 2024
Production reference: 2280224

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-80323-216-4

www.packtpub.com

For Ashok Shah,

In the library of your memory, I shelve this work, papa. May the whispers of data echo your passion for stories, and may you be proud of the chapters I write with your unseen hand, guiding me still.

- Krishna Shah

Contributors

About the author

Krishna Shah is a data architect from Melbourne, Australia with 9+ years of experience, and she knows how to make data work. She's been an official trainer for Elasticsearch and Kibana, crafting the courses that empower people to unlock the secrets of data. Prior to that, she worked for a start-up in India as the data engineer behind building and maintaining data engineering pipelines, then transforming that raw information into stunning visuals and insights using Kibana and other data engineering technologies. Today, she's an advocate, a mentor, and a bridge-builder, inviting everyone to find their own rhythm in the data's dance. Whether you're a novice or seasoned analyst, brace yourself for her infectious enthusiasm and knack for making the driest of datasets sing!

About the reviewer

Peter Steenbergen is a principal solutions architect at Elastic. Peter was one of the first people to receive the Elastic Certified Professional of the Year award and has many years of experience in building solutions with the Elastic Stack. He enjoys helping people in the community to solve their search and observability use cases leveraging the Elastic Stack. This could be through in-company training, knowledge-sharing workshops, or on-site consultative sessions. If he's not behind a computer, you can find him riding his mountain bike, running through the woods, or, with his latest hobby, playing on a padel court.

Table of Contents

Part 2: Visualizations in Kibana

4

How About We Visualize? 37

5

Powering Visualizations with Near Real-Time Updates 63

Part 3: Analytics on a Dashboard

6

Data Analysis with Machine Learning 81

10

Preface

Seven years ago, I stumbled upon Elasticsearch – not as a technical instructor but as a wide-eyed data detective. It was after that I discovered Kibana; I was captivated by its ability to transform cold, numerical figures into vibrant stories, each query a brushstroke painting the canvas of insights. As I delved deeper, its power to democratize data analysis, making it accessible not just to elite statisticians but to anyone with a curious mind, ignited a passion within me.

This passion led me to the world of official Kibana 8 training, where I witnessed firsthand the transformative impact it had on individuals and organizations. But a nagging feeling persisted – the existing resources, while comprehensive, felt like dense tomes for seasoned explorers, leaving newcomers lost in the wilderness of data.

That's where the seed of this book was sown. I envisioned a guide that didn't just explain the "what" and "how" of Kibana but also captured the "why." I wanted to translate the magic I saw in classrooms onto the page, making Kibana not just a tool but a bridge to a world of data-driven discovery.

Researching this book wasn't just about combing through documentation and tutorials; it was about reliving the journey of my students. I revisited the challenges they faced, the "aha!" moments they experienced, and the questions that lingered long after the training ended. I talked to data enthusiasts, industry experts, and fellow Kibana instructors, gathering their insights and weaving them into a tapestry of practical knowledge.

Each chapter became a brushstroke on the canvas of my vision. I crafted exercises that mirrored real-world scenarios, using familiar datasets to make the learning process relatable and engaging. I translated complex concepts into digestible language, using humor and anecdotes to keep the journey as enjoyable as it is informative.

This book is more than just a compilation of Kibana functionalities; it's an invitation to embark on a data-driven adventure. It's for the curious mind, the aspiring analyst, or anyone who wants to unlock the secrets hidden within their data. It's my way of sharing the magic I witnessed, igniting that spark of data passion in others, and guiding them on their own journey from data novice to empowered data detective.

Ready to transform raw data into captivating stories? This book is your Rosetta Stone, unlocking the power of Kibana 8.x. Delve into Discover, craft visual symphonies with dashboards, and unveil hidden patterns with **Machine Learning** (**ML**) and **Time Series Visual Builder** (**TSVB**). Master ES|QL's precise sculpting, bend data with dynamic runtime fields, and learn to manage your domain with ease. Let Kibana be your data maestro, conducting insights with elegance and precision. Now, turn the page and let the analysis begin!

Who this book is for

Calling all data curious, analysis enthusiasts, and visualization voyagers! Whether you're a seasoned data wrangler or a wide-eyed newbie, this book welcomes you with open arms (and dashboards!). This book is your launchpad to unlock the power of Kibana, the interactive data visualization platform that transforms raw numbers into captivating stories. If you're hungry to explore hidden patterns, unearth trends from your data, and paint vibrant pictures of insights, then this guide is your compass. Whether you're a marketer charting customer journeys, an IT whiz troubleshooting server logs, or a scientist diving into research findings, Kibana has a seat for you at its analysis table. So, ditch the spreadsheets and dive into the dynamic world of data visualization – we'll start with baby steps and soon have you dancing with dashboards.

What this book covers

Chapter 1, *Introduction to Kibana*, unlocks the power of Kibana by diving into the vibrant world of data visualization. This chapter lays the foundation, introducing you to Kibana – an interactive platform that transforms raw data into captivating stories. You'll learn its purpose, its core features, and why it's the go-to tool for data explorers. Moreover, you will be guided through the exciting process of setting up your own Kibana environment, from installing and configuring the software to connecting it to your data source.

Chapter 2, *Creating Data Views and Introducing Spaces*, unlocks two powerful features that elevate your analysis game. You'll be guided through crafting tailored data views and personalized dashboards that focus on specific aspects of your data, letting you zero in on critical insights by creating a data view that helps you select and work on a specific type of data in Kibana. Then, you will be prepared to explore the revolutionary concept of Kibana spaces. This chapter unlocks doors to efficient data sharing, streamlined workflows, and a world where collaboration takes center stage.

Chapter 3, *Discovering Data through Discover*, equips you with the tools to explore your datasets like a seasoned detective, sifting through raw information to uncover hidden patterns and unveil compelling insights. You'll master the powerful search bar, unleashing precise queries to pinpoint specific data points. You'll learn the Kibana Query Language to search through your data and also create filters. You'll see how Discover helps us explore the data before you begin your analytics journey on your dataset.

Chapter 4, *How About We Visualize?*, unlocks the visual language of data in Kibana, transforming cold numbers into captivating stories. Forget static spreadsheets – here, you'll wield diverse charts and graphs like magic wands, revealing hidden patterns and trends within your information. You'll get to explore the power of bar charts, line graphs, and heatmaps, learning how each Lens editing tool paints a unique picture of your data's essence. You'll master the art of selecting the right visual for the job, ensuring your insights resonate with clarity and impact.

Chapter 5, *Powering Visualizations with Near-Real-Time Updates*, dives into the exciting world of near real-time data visualization with TSVB. You'll learn to craft visualizations that update seamlessly as new information flows in, revealing hidden patterns and trends as they unfold. You get to explore TSVB's powerful features, such as expressions, aggregations, and bucket scripting, empowering you to transform raw data into captivating stories that update with the pulse of your live systems.

Chapter 6, *Data Analysis with Machine Learning*, will delve into the exciting realm of ML within Kibana. Imagine using data patterns and algorithms to uncover hidden insights, predict trends, and automate anomaly detection. You'll get to explore tools such as anomaly detection, outlier analysis, and even supervised learning, all within your familiar Kibana interface. It is a powerful fusion of data analysis and ML, unlocking a whole new layer of understanding and actionable insights from your data.

Chapter 7, *Graph Visualization*, will help you learn to untangle the web of your data! This chapter equips you with the power of graphs to unveil hidden connections, trace relationships, and spot patterns lurking beneath the surface of numbers.

Chapter 8, *Finally, the Dashboard*, teaches you how to transform raw data into visually captivating dashboards that tell a clear and compelling story. You will craft interactive layouts, weave together powerful visualizations, and apply custom filters to empower anyone to explore and understand your data with ease. This is where information comes alive, guiding informed decisions and sparking insightful conversations.

Chapter 9, *ES|QL and Advanced Kibana Concepts*, explores the power of data manipulation where you dive into ES|QL, crafting custom Elasticsearch queries to sculpt your insights. You will unleash runtime fields, dynamically generating data points for deeper analysis on the fly. Finally, you will master advanced Kibana settings to understand how to fine-tune your environment for maximum visual impact and intuitive exploration.

Chapter 10, *Query DSL and Management through Kibana*, takes a deep dive into the pulse of your data with Query DSL. You will craft precise searches, sculpt results, and bend information to your will. We'll explore Kibana's data management tools, keeping your information kingdom organized and secure. Prepare to master both precision and control, one query and setting at a time!

Disclaimer:

This book, *Kibana 8. x: A Quick Start Guide to Data Analysis*, is not sponsored, endorsed, or affiliated with Elastic NV ("Elastic") or any of its subsidiaries or affiliates. The contributors to this book are independent authors and are not acting on behalf of or as representatives of, Elastic in any capacity. The content of this book is solely the responsibility of the authors and does not necessarily reflect the views or opinions of Elastic. Elastic makes no representations or warranties of any kind, express or implied, regarding the accuracy, completeness, or timeliness of the content of this book.

To get the most out of this book

It is recommended to have a basic understanding of data. Familiarity with data types, structures, and concepts will ease navigation through Kibana's data manipulation tools.

Some SQL knowledge is useful. While not essential, basic SQL skills can come in handy for writing simple queries in ES|QL, Kibana's query language.

Conceptual know-how on downloading, installing, and configuring Kibana and working with YAML files is essential.

If you are using the digital version of this book, we advise you to type the code yourself or access the code from the book's GitHub repository (a link is available in the next section). Doing so will help you avoid any potential errors related to the copying and pasting of code.

Download the example code files

You can download the example code files for this book from GitHub at `https://github.com/PacktPublishing/Kibana-8.x-A-Quick-Start-Guide-to-Data-Analysis`. If there's an update to the code, it will be updated in the GitHub repository.

We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`. Check them out!

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "For example, `GET _ml/info` will simply return the result of the current machine learning jobs on the cluster."

A block of code is set as follows:

```
GET _ml/memory/<node_id>/_stats
GET _ml/memory/_stats
```

Any command-line input or output is written as follows:

```
<iframe src="https://juxwycstgeesmshyp-xxxxxxxxxxx.rp.strigo.io/
app/r/s/xAwTf" height="600" width="800"></iframe>
```

Bold: Indicates a new term, an important word, or words that you see on screen. For instance, words in menus or dialog boxes appear in **bold**. Here is an example: "Inside the **Documents** layer, select **data view**/**Index pattern** you wish to work on and the **Geospatial** field, and then click on **Add layer** at the bottom."

> **Tips or important notes**
> Appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, email us at `customercare@packtpub.com` and mention the book title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata` and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Share your thoughts

Once you've read *Kibana 8.x: A Quick Start Guide to Data Analysis*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback.

`https://packt.link/r/1803232161`

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below

`https://packt.link/free-ebook/9781803232164`

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly

Part 1: Exploring Kibana

This part covers Kibana's core functionality: transforming raw data into captivating insights. We'll craft data views, which are customized lenses used to focus on specific data subsets. We will introduce you to spaces, which are collaborative containers for sharing and organizing dashboards. Finally, the **Discover** tab will become your playground, where queries unveil hidden patterns and trends, weaving data into stories that guide your decisions. Here, you also get equipped to explore, visualize, and understand the true power of Kibana in data exploration and discovery.

This part has the following chapters:

- *Chapter 1*, *Introduction to Kibana*
- *Chapter 2*, *Creating Data Views and Introducing Spaces*
- *Chapter 3*, *Discovering the Data through Discover*

1
Introduction to Kibana

Now is the time to kickstart our journey into the world of visualizing data. We are first going to start understanding the core concepts of Kibana, right from setting up, installing, and configuring to starting Kibana. We will also learn how Kibana acts as a window to your data stored in Elasticsearch. Kibana, being an open source application, is also a UI layer of Elastic Stack for visualizing and exploring data in Elasticsearch. It can also be used to manage the stack.

The following are the topics that we will cover in detail:

- Getting an overview of Kibana
- Understanding data integrations

Technical requirements

Kibana requires specific hardware specifications when installed on a server, which includes support for 64-bit operating systems. The installation process offers multiple package formats, such as `tar`, `deb`, `rpm`, and Docker. Kibana can be installed, configured, and started from an archive on Linux, macOS, or Windows.

The hardware requirements for Kibana may vary depending on the specific use-case requirements. However, it is generally recommended to allocate 1 GB to 2 GB of RAM and 2 CPUs for use cases involving PDF, CSV, and PNG reporting in Kibana.

Getting an overview of Kibana

Kibana is a powerful tool for data discovery, analysis, visualization, and security. It's designed for administrators, analysts, and business users to manage, monitor, and secure their Elastic Stack deployments. Kibana provides a comprehensive suite of features for searching, observing, and protecting data. It's easy to quickly find documents and uncover hidden insights, visualize results in charts, gauges, maps, graphs, and more, and combine them in a dashboard. Analysts can explore and analyze data with the help of Kibana's sophisticated query language, and administrators can manage and monitor the health of their Elastic Stack cluster.