Working with Elasticsearch 7.0

Days: 2

Prerequisites: To ensure a smooth learning experience and maximize the benefits of attending this course, you should have the following prerequisite skills:

- Ability to use computers to start programs, open and save files, navigate application menus and interfaces
- Knowledge of basic data analysis concepts, including how to work with and interpret data sets, is necessary.
- Familiarity with basic IT and computer concepts, including operating systems and networks, will facilitate understanding of course content.
- Since Elastic Stack is used for data processing and analysis, understanding how databases function, and basic SQL skills are beneficial.
- Some basic programming knowledge, particularly in a language such as Python or Java, will help in understanding and implementing certain concepts, although it's not a hard prerequisite.
- Experience with command-line interfaces (CLI) would be advantageous, as Elastic Stack often involves interactions via CLI.
- Basic Linux skills, including familiarity with command-line options such as ls, cd, cp, and su

Audience: This training is ideally suited for data analysts, IT professionals, and software developers who seek to augment their data processing and analytics capabilities. It will also benefit system administrators and data engineers who wish to harness Elastic Stack's functionalities for efficient system logging, monitoring, and robust data visualization. With a focus on practical application, this course is perfect for those aspiring to solve complex data challenges in real-time environments across diverse industry verticals.

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. Geared for experienced data analysts, IT professionals, and software developers who seek to augment their data processing and analytics capabilities, **Working with Elasticsearch** will explore how to use Elastic Stack and Elasticsearch efficiently to build powerful real-time data processing applications.

Throughout the two-day hands-on course, you'll explore the power of this robust toolset that enables advanced distributed search, analytics, logging, and visualization of data, enabled by new features in Elastic Stack 7.0. You'll delve into the core functionalities of Elastic Stack, understanding the role of each component in constructing potent real-time data processing applications. You'll gain proficiency in Elasticsearch for distributed searching and analytics, Logstash for logging, and Kibana for compelling data visualization. You'll also explore the art of crafting custom plugins using Kibana and Beats, and familiarize yourself with Elastic X-Pack, a vital extension for effective security and monitoring.

The course also covers essentials like Elasticsearch architecture, solving full-text search problems, data pipeline building, and creating interactive Kibana dashboards. Learn how to deploy Elastic Stack in production environments and explore the powerful analytics capabilities offered through Elasticsearch aggregations. The course will also touch upon securing, monitoring, and utilizing Elastic Stack's alerting and reporting capabilities. Hands-on labs, captivating demonstrations, and interactive group activities enrich your learning journey throughout the course.

For teams with specific requirements, our team is ready to tailor the course content to your unique learning objectives and goals. Upon completion, you will be well-equipped with a deep understanding of Elastic Stack's fundamental functionalities and how each component contributes to solving various data processing challenges.

Working with Elasticsearch 7.0

Course Objectives: This course combines engaging instructor-led presentations and useful demonstrations with valuable hands-on labs and engaging group activities. Throughout the course you'll explore:

- Fundamentals of Elastic Stack including Elasticsearch, Logstash, and Kibana
- Useful tips for using Elastic Cloud and deploying Elastic Stack in production environments
- How to install and configure an Elasticsearch architecture
- How to solve the full-text search problem with Elasticsearch
- Powerful analytics capabilities through aggregations using Elasticsearch
- How to build a data pipeline to transfer data from a variety of sources into Elasticsearch for analysis
- How to create interactive dashboards for effective storytelling with your data using Kibana
- How to secure, monitor and use Elastic Stack's alerting and reporting capabilities

OUTLINE:

LESSON 1: INTRODUCING ELASTIC STACK

- What is Elasticsearch, and why use it?
- Exploring the components of the Elastic Stack
- Use cases of Elastic Stack
- Downloading and installing

LESSON 2: GETTING STARTED WITH ELASTICSEARCH

- Using the Kibana Console UI
- Core concepts of Elasticsearch
- CRUD operations
- Creating indexes and taking control of mapping
- REST API overview

LESSON 3: SEARCHING - WHAT IS RELEVANT

- The basics of text analysis
- Searching from structured data
- Searching from the full text
- Writing compound queries
- Modeling relationships

LESSON 4: ANALYTICS WITH ELASTICSEARCH

- The basics of aggregations
- Preparing data for analysis
- Metric aggregations
- Bucket aggregations
- Pipeline aggregations
- Substantial Lab and Case Study

LESSON 5: ANALYZING LOG DATA

- Log analysis challenges
- Using Logstash
- The Logstash architecture
- Overview of Logstash plugins
- Ingest node

LESSON 6: VISUALIZING DATA WITH KIBANA

- Downloading and installing Kibana
- Preparing data
- Kibana UI
- Timelion
- Using plugins