

Updated on 11/27/2025

Register

Elastic Stack ELK Training: The Elastic Suite

3 days (21 hours)

Overview

Our training course on the complete open source Elastic suite offered by The Elastic Stack will help you search for, extract, analyze, and visualize data to generate real-time dashboards.

By the end of our course, you will discover the many features offered by ELK, such as centralized logging, multiple hosting options, and scalability. [ElasticSearch](#) is a powerful search engine recognized and used by major international players (Sony, IGN, Stackoverflow, GitHub, SoundCloud, Mozilla, etc.). Document-oriented in the NoSQL sense of the term, all data is stored in the form of structured JSON documents.

ELK will play an important role in your companies' IT infrastructures. You will learn about the entire ElasticSearch ecosystem, its role, and its use cases.

In this ELK training course, you will learn how to use ELK V9, which combines four tools: Elasticsearch, Logstash, Kibana, and Beats.

You will also discover Beats, which allows you to easily collect and send data. Logstash allows you to extract logs, transfer them, parse them, and finally index them in Elasticsearch. Kibana allows you to exploit the data stored in Elasticsearch, produce queries, and create dashboards from a web browser.

As with all our training courses, this one will introduce you to the latest version of ELK / Elastic Stack.

Objectives

- Discover Elasticsearch and the latest features of the Elastic suite
- Learn about the ELK suite (with Beats ELKB / BELK)

- Feed Elasticsearch with multiple data sources
- Structure and enrich heterogeneous data
- Transfer raw data from a file or broker
- Produce dashboards with Kibana
- System monitoring, JMX, business, and BI
- Advanced Administration (Optional Module)

Target audience

Developers, System Administrators, DevOps.

Prerequisites

- Basic knowledge of a Unix system
- [Test My Knowledge](#)

Recommended reading before and after the training

- [A guide to the Elastic suite](#) that shows the steps to follow to improve search relevance
- The [complete guide](#) to the Elastic Stack

Elastic Stack ELK training program

Introduction and overview

- The Elasticsearch ecosystem
- The role of Elasticsearch, Logstash, Kibana, and Beats
- Simplifying version management with The Elastic Stack version 9
- What's new in version 9
- Principles and operation
- Architecture examples
- Use cases

Elasticsearch - Indexing, searching, and analyzing data

- Introduction to Elasticsearch
- Indexing and Search
- Data analysis
- Mappings and Analysis Configuration
- Querying with Elasticsearch
- Plugin System & Configuration
- Queries and filters
- Aggregations

- Replication and partitioning
- Practical work: Installation and configuration
 - ElasticSearch Server
 - Setting up a cluster
 - Node roles

Logstash - Transform and format your data for use in Elasticsearch

- Concepts: Input, Output, Filter, Codecs, etc.
- Inputs: File, [Redis](#), RabbitMQ...
- Filters: Grok, Date, Mutate...
- Outputs: File, Elasticsearch, [Redis](#)...
- Threading and high availability

Kibana - Visualize Elasticsearch data and create your reports

- Installation and configuration
- Data discovery and query building
- Aggregations and building visualizations
- Panels
- Creating views
- Setting up a dashboard
- Practical work: Creating a report with real-time visualization

Beats - Easily collect, parse, and send your data

- Introduction to Data Shippers and real-time monitoring
- Monitor your network with PacketBeat
- Monitor your files with FileBeat
- Monitor your Windows event logs with WinlogBeat
- Retrieve important metrics from your servers with Metricbeat

Monitoring and analysis

- Putting it into practice
- System monitoring
- JVM/JMX monitoring
- Log As A Service
- Business Analysis & BI (Business Intelligence)

Advanced Administration Modules (optional)

- X-Pack: Secure and protect your data and receive alerts thanks to reports on the health of your Elastic Stack services!
- ES-Hadoop

- Elastic Cloud: Elasticsearch as a Service
- Graph
- Advanced tuning and architectures
- Supervision (Kopf, Marvel) and monitoring (Cluster, Nodes, Cat)
- Backups: Snapshots and Restore

ADDITIONAL MODULE IN ENGLISH ON REQUEST (+2 DAYS)

- Training language: English
- Course level: Beginner to intermediate

This training course teaches the basic concepts of Elasticsearch and explores the main components of the Elastic Stack: Beats, Logstash, Elasticsearch, and Kibana. It covers several use cases and how to define an appropriate architecture and properly size clusters.

Theory: 60% Practice: 40% Audience:

- Data Engineers
- Architects
- System Administrators
- DevOps

Prerequisites:

- Knowledge of REST/HTTP, Json, Yaml is appreciated
- No knowledge required

Elasticsearch: Getting Started

- Elasticsearch Overview
- Key Features
- Basic Concepts
- Install Elasticsearch
- CRUD Operations
- First Steps on Search API

Elasticsearch: Mappings and Templates

- Introduction
- Data Types
- Main parameters
- Mapping API

- Analysis and Inverted Index
- Multi-Fields
- Dynamic Mapping
- Templates

Elasticsearch: Search and Aggregations

- Search API Overview
- Terms, Full Text, and Compound Queries
- Aggregations Overview
- Metrics, Aggregations
- Buckets Aggregations
- Pipelines Aggregations

Elasticsearch: Ingest and Pipelines

- Ingest Node
- Pipelines

Kibana

- Overview
- Management
- Discover
- Visualize and Dashboard
- More Features

Beats

- Overview
- Filebeat
- Metricbeat
- More Beats

Logstash

- Overview
- Pipeline Configuration
- Main settings

Architectures

- Elastic Stack-based Architecture
- Elastic Stack and Kafka Integration

- Monitoring using Elastic Stack.

Target companies

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.