+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/28/2024

Sign up

Elastic Stack ELK Training: The Elastic Suite

3 days (21 hours)

Presentation

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

At the end of our course, you'll 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...). Document-oriented i n the NoSQL sense of the term, all data is stored as structured JSON documents.

ELK will play an important role in your company's IT infrastructure. You'll learn all about the ElasticSearch ecosystem, its role and use cases.

In this ELK training course, you'll learn how to use ELK V8, a combination of 4 tools: Elasticsearch, Logstash, Kibana and Beats.

You'll also discover Beats, a simple way of collecting and sending data. Logstash extracts logs, transfers them, parses them and indexes them in Elasticsearch. Kibana lets you exploit 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 additions to the Elastic suite
- Knowledge of the ELK suite (with Beats ELKB / BELK)

- Feed Elasticsearch with multiple data sources
- Structuring and enriching 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.

Recommendations for pre- and post-course reading

- A guide from the Elastic suite showing steps to improve search relevance
- The complete guide to the Elastic suite

Elastic Stack ELK training program

Introduction and overview

- The Elasticsearch ecosystem
- The role of Elasticsearch, Logstash, Kibana and Beats
- Simplify version management with The Elastic Stack version 7
- What's new in versions 6 & 7
- Principles and operation
- Examples of architectures
- Use cases

Elasticsearch - Data indexing, search and analysis

- Introduction to Elasticsearch
- Indexing and searching
- Data analysis
- Mappings and analysis configuration
- Querying with Elasticsearch
- Plugin system & Configuration
- Queries and Filters

- Approvals
- Replication and partitioning
- TP: 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...
- Inputs: File, Redis, RabbitMQ...
- Filters: Grok, Date, Mutate...
- Outputs: File, Elasticsearch, Redis...
- Threading and high availability

Kibana - Visualize Elasticsearch data and create your own reports

- Installation and configuration
- Data discovery and query construction / Queries
- Visualization aggregation and construction
- Panels
- Creating views
- Setting up a dashboard
- Practical work: Creating a report with real-time visualization

Beats - Simply collect, share and send your data

- Introduction to Data Shippers and real-time monitoring
- Monitor your network with PacketBeat
- Monitore your files with FileBeat
- Monitor your Windows event logs with WinlogBeat
- Retrieve important server metrics 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 be alerted with 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 covers the basic concepts of Elasticsearch and explores the main components of the "Elasic Stack": Beats, Logstash, Elasticsearch and Kibana. It covers several use cases and how to define an appropriate architecture and size clusters. Theory: 60% Practical: 40% Audience:

- Data Engineers
- Architects
- System Administrators
- DevOps

Prerequisites :

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

Elasticsearch: Getting Started

- Elasticsearch Overview
- Keys Features
- Basic Concepts
- Install Elasticsearch
- CRUD Operations
- First steps on Search API

Elasticsearch: Mappings and Templates

- Introduction
- Data Types
- Main parameters
- API mapping

- 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.

Companies concerned

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

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

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

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.