Updated 03/06/2024

Sign up

EFK Training

3 days (21 hours)

Presentation

EFK (ElasticSearch, Fluentd and Kibana) is a popular centralized logging solution. With our EFK training you'll be able to collect, process and visualize logs.

In this course, you'll learn about the services that help to quickly sort and analyze large volumes of log data produced by pods.

With Elasticsearch, you'll be able to perform full-text and structured searches as well as analyses, Kibana for data visualization, Fluentd to collect, transform and send log data to the Elasticsearch backend.

Thanks to this training, you'll be able to manage large quantities of data and provide real-time information on the behavior of complex systems.

As with all our training courses, this one will include the latest tool features.

Objectives

- Understanding EFK Stack components and architecture
- Install and configure Elasticsearch, Fluentd and Kibana
- Create and manage visualizations and dashboards in Kibana
- Optimize and monitor the performance of log pipelines in production

Target audience

- Developers
- Data engineers
- Architects

Prerequisites

- Knowledge of databases
- Familiarity with log formats and logging systems

OUR EFK TRAINING PROGRAM

INTRODUCTION TO EFK

- EFK Stack presentation
- Use cases
- Advantages of EFK over other solutions
- Overview of Elastic, Fluentd and Kibana components
- Architecture and data flow

INSTALLATION AND CONFIGURATION

- Installing and configuring Elastic
- Key concepts: Indexes, Shards and Replicas
- Data backup and restoration
- Securing the installation

DISCOVER FLUENTD

- Introduction to Fluentd and its architecture
- Installing Fluentd
- Inputs and outputs configuration
- Use filters to transform data
- Best practices for optimizing Fluentd performance

VISUALIZATION WITH KIBANA

- Installing and configuring Kibana
- Navigating the Kibana interface
- Creating basic visualizations
- Dashboards and panels: creation and management
- Using Kibana for log analysis

FLUENTD INTEGRATION WITH ELASTICSEARCH

- Configuring Fluentd to send logs to Elasticsearch
- Data schema and index template management

- Monitoring and troubleshooting log pipelines
- Performance optimization and parameter tuning
- Case study: application log ingestion with Fluentd and Elastic

ADVANCED ANALYSIS AND MONITORING WITH KIBANA

- Advanced queries and data analysis with Lucene
- Use alerts and notifications correctly
- Real-time log exploration
- Integration with other monitoring and warning tools
- Case study: creating complex dashboards

BEST PRACTICES AND PRODUCTION DEPLOYMENT

- Strategies for deploying the EFK Stack in production
- Data backup and recovery
- Security and access management
- Updating and managing EFK Stack versions

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 is used to check correct acquisition.

skills.

Sanction

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