

## ELK log analysis hands-on

*Wednesday, August 28, 2019 1:15 PM (4h 45m)*

This tutorial is aimed at intermediate linux users who are interested in a modern way of log collection and analysis.

You will learn how to setup an Elastic Search cluster with a few tuning recommendation. Next you will learn how to collect and process log data with Filebeat. Than we will focus on advanced log processing with Logstash, where you will learn how to categorise, transform and store data. Kibana aided data visualization will guide us through the whole workshop progress.

You will need a laptop with ssh client (Putty on windows) and web browser. Knowledge of basic linux CLI is an advantage but not a necessity.

**Presenter:** MIKULA, Alexandr (Czech Academy of Sciences)

**Session Classification:** Tutorials