



Contribution ID: 57

Type: **not specified**

## Elastic Search, Logstash and Kibana

*Wednesday, September 9, 2015 1:00 PM (5 hours)*

Elasticsearch, Logstash and Kibana, known as the ELK stack, are three open source projects designed to ship, parse, search, analyse and visualize your data, from Apache logs to Twitter streams. A short description of the components is the following:

- Logstash allows you to ship and parse your data using a great variety of plugins. It is highly scalable.
- Elasticsearch is a search server based on Apache Lucene. It is distributed and highly scalable.
- Kibana is the visualization platform available through a web browser with a nice interface and easy to customize directly from the browser.

<br/>

In this course we will explain to you these three components and we will guide you through their installation and configuration. Several different data logs will be analyzed in order to finally create your own Kibana dashboards.

<p/>

Basic Linux knowledge and be familiar with vim is required. Some regular expressions knowledge would be a plus.

**Authors:** Mr PATHOMKEERATI, Kajorn (KIT/IAI); Mr AMBROJ PEREZ, Samuel (KIT/SCC)

**Presenters:** Mr PATHOMKEERATI, Kajorn (KIT/IAI); Mr AMBROJ PEREZ, Samuel (KIT/SCC)

**Session Classification:** Elastic Search, Logstash, Kibana

**Track Classification:** Data Center Management