ELK Stack

The ELK stack is an open source way to consolidate various logs gathered by **logstash** to a real-time search, analytics, and visualized form by way of **ElasticSearch** and **Kibana**.

From the web site—

- **Elasticsearch** is a flexible and powerful open source, distributed, real-time search and analytics engine
- **Logstash** helps you take logs and other time based event data from any system and store it in a single place for additional transformation and processing
- **Kibana** is Elasticsearch's data visualization engine, allowing native interaction with all the data in Elasticsearch via custom dashboards. Kibana's dynamic dashboard panels are savable, shareable and exportable, displaying changes to queries into Elasticsearch in real-time.

See also—

- Overview, **http://www.elasticsearch.org/overview/**
- Download, http://www.elasticsearch.org/overview/elkdownloads/
- Review, http://aarvik.dk/a-bit-on-elasticsearch-logstash-kibana-the-elk-stack/

Revision #1
Created Mon, Jul 21, 2014 7:23 PM by Postovoit, Philip
Updated Mon, Jul 21, 2014 7:23 PM by Postovoit, Philip