LI121 Elasticsearch, Logstash, Kibana Logfile-Analyse mit OpenSource Tools

Kurzbeschreibung:

Im Kurs **L121 Elasticsearch, Logstash, Kibana Logfile-Analyse mit OpenSource Tools** erhalten Sie eine Übersicht über Software-Lösungen zur Logfile-Analyse (Linux, UNIX, Windows).

Zielgruppe:

Das Seminar **L121 Elasticsearch, Logstash, Kibana Logfile-Analyse mit OpenSource Tools** ist besonders geeignet für:

- Linux-/Windows Systemadministratoren
- Administratoren von heterogenen Umgebungen mit vielen unterschiedlichen Protokoll-Formaten

Voraussetzungen:

Um Kursinhalten und Lerntempo im Workshop **L121 Elasticsearch, Logstash, Kibana Logfile-Analyse mit OpenSource Tools** gut folgen zu können, sind gute Erfahrungen mit der jeweiligen System-Administration und Grundkenntnisse zum Arbeiten mit der Befehlszeile von Linux nötig.

Sonstiges:

Dauer: 4 Tage

Preis: 2390 Euro plus Mwst.

Ziele:

Der Kurs **L121 Elasticsearch, Logstash, Kibana Logfile-Analyse mit OpenSource Tools** gibt eine Übersicht über gängige Software-Lösungen, um im Betrieb anfallende Protokoll-Daten zu transportieren, zu speichern und auszuwerten.
Das beispielhafte Einrichten und Vergleichen der besprochenen Werkzeuge anhand verschiedener Einsatz-Szenarien ermöglicht einen Überblick über deren Möglichkeiten und Einschränkungen.
Das Linux-Training LI121 schließt mit Empfehlungen für unterschiedliche Anwendungsfälle ab.

Inhalte/Agenda:

- ♦ **Einführung**
  - ◊ Traditionelle Ansätze Protokolle zu analysieren
  - ◊ Was für Probleme gibt es damit?

♦ **Konzepte und Begriffe**
- ◊ Der Weg einer Protokoll-Meldung
- ◊ Das JSON-Format

♦ **Gängige Log-Quellen**
- ◊ Syslog
- ◊ Elastic Beats und Fluent Bit
- ◊ Spezifische Dienste wie Webserver, MySQL, PostgreSQL
- ◊ Netzwerk-Komponenten
- ◊ Windows Event Log, Windows-Dienste

♦ **Transport und Speicherung von Protokoll-Meldungen**
- ◊ Logstash
- ◊ Fluentd
- ◊ Graylog
- ◊ Zentraler rsyslog/syslog-ng-Server

♦ **Speicherung und Suche**
- ◊ ElasticSearch
- ◊ MongoDB

♦ **Oberflächen**
- ◊ Kibana
- ◊ Graylog

♦ **Sinnvolle Kombinationen und integrierte Lösungen**
- ◊ Logstash + Elasticsearch + Kibana
- ◊ Fluentd + Elasticsearch + Kibana
- ◊ Graylog + Elasticsearch

♦ **VMware Log Insight**
- ◊ Splunk

♦ **Einsatz-Szenarien**
- ◊ Volltextsuche
- ◊ Korrelationen, mehrere Abfragen
- ◊ Statistische Analyse: Häufigkeiten, Trends
- ◊ Langzeit-Analysen
- ◊ Heuristiken
- ◊ Skriptgesteuerte Auswertung
- ◊ Rollenverteilung

♦ ◊