LI300 Logfile-Analyse mit Elasticsearch, Logstash, Kibana

Kurzbeschreibung:

Der Kurs **LI300 Logfile-Analyse mit Elasticsearch, Logstash, Kibana** vermittelt praxisnah, wie Protokoll-Daten aus Linux-, UNIX- und Windows-Systemen sicher transportiert, gespeichert und ausgewertet werden können. Nach einer Einführung in klassische und moderne Logfile-Analyse-Ansätze lernen die Teilnehmenden Tools wie Logstash, Elasticsearch, Kibana, Graylog und weitere kennen.

Verschiedene Log-Quellen, Transportwege, Formate und Oberflächen werden vorgestellt und in Workshops verglichen. Die Teilnehmenden üben dabei die Integration, flexible Kombination und reale Anwendungsszenarien (z. B. Volltextsuche, statistische Analyse, Langzeit-Analysen) und erhalten konkrete Handlungsempfehlungen für den Alltag. Für Systemadministratoren mit Erfahrung an der Linux-Konsole besonders geeignet.

Zielgruppe:

Das Seminar **LI300 Logfile-Analyse mit Elasticsearch, Logstash, Kibana** ist besonders geeignet für:

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

Voraussetzungen:

Um Kursinhalten und Lerntempo im Workshop **LI300 Logfile-Analyse mit Elasticsearch, Logstash, Kibana** 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 **LI300 Logfile-Analyse mit Elasticsearch, Logstash, Kibana** 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 Training schließt mit Empfehlungen für unterschiedliche Anwendungsfälle ab.

Inhalte/Agenda:

- **Einführung**
  - Traditionelle Ansätze Protokolle zu analysieren
  - Welche Probleme gehen damit einher?

- **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

-