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

Kurzbeschreibung:

Übersicht über Software-Lösungen zur Logfile-Analyse (Linux, UNIX, Windows).

Zielgruppe:

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

Voraussetzungen:

Gute Erfahrungen mit der jeweiligen System-Administration. Grundkenntnisse zum Arbeiten mit der Befehlszeile von Linux.

Sonstiges:

Dauer: 4 Tage

Preis: 1990 Euro plus Mwst.

Ziele:

Der Kurs 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. Der Kurs schließt mit einem Fazit mit Empfehlungen für unterschiedliche Anwendungsfälle.
Geeignete Folge-Kurse:
LI146 Linux Datacenter Services.

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