heinlein

Akademie

Logfile-Analyse mit Elasticsearch, Logstash und Kibana

Der Logfile-Analyse-Kurs der Heinlein Akademie: In diesem Training lernen Sie, wie Sie die Protokoll-Daten verschiedenster Systeme (Linux, UNIX, Windows) effizient auswerten und welche Software-Lösungen sich zur Logfile-Analyse bewährt haben.

Experte | 4 Tage | Martin Steigerwald | Berlin / Online

Vorkenntnisse

Voraussetzung für die Schulung sind gute Kenntnisse der jeweiligen System-Administration sowie Grundkenntnisse im Arbeiten mit der Linux-Befehlszeile und Netzwerk-Grundkenntnisse. Der Kurs richtet sich an Linux / Windows Systemadministratoren und an Administratoren von heterogenen Umgebungen mit vielen unterschiedlichen Protokoll-Formaten.

Kursinhalt

Einführung:

- Traditionelle Ansätze, Protokolle zu analysieren
- Welche Probleme gibt es damit?
- Wie löst Logfile-Analyse diese?

Konzepte und Begriffe:

- Der Weg einer Protokoll-Meldung
- Das JSON-Format
- Rest API

Sinnvolle Kombinationen und integrierte Lösungen:

- Der Elastic Stack: Logstash, Elasticsearch, Kibana und Beats
- OpenSearch und OpenSearch Dashboards
- Fluentd, Fluent Bit, Elasticsearch, Kibana
- Graylog

Gängige Log-Quellen:

- Syslog
- Elastic Beats und Fluent Bit
- Webserver, Mailserver, MariaDB, PostgreSQL
- Netzwerk-Komponenten
- Windows Event Log, Windows-Dienste

Transport und Verarbeitung von Protokoll-Meldungen:

- Logstash
- Fluentd
- Graylog
- Rsyslog

Speicherung mit Elasticsearch:

- einzeln und als Cluster
- Monitoring mit Cerebro und Kibana
- Performance-Aspekte
- alte Daten aufräumen
- Backup

Suche:

- Lucene
- Kibana Query Language
- Graylog

Oberflächen:

- Kibana, OpenSearch Dashboards, Graylog
- Protokoll-Daten auswerten
- Graphen und Dashboards bauen
- Administrative Aufgaben erledigen

Ziel

Viele System-Administratoren heterogener Umgebung haben es mit Unmengen an Protokoll-Daten verschiedenster Systeme zu tun, die diese in unterschiedlichen Formaten speichern. Tritt ein Fehler auf, sind diese Logfiles oft der einzige Zugang zur Problem-Ursache. Gerade bei hunderten von Servern ist deren manuelle Analyse und Korrelation über verschiedene Systeme hinweg immens zeitaufwendig. Beschäftigt sich ein Administrator nun mit effizienteren Wegen, sich einen Überblick über diese Daten-Mengen zu verschaffen, findet er eine ganze Reihe unterschiedlicher Software-Lösungen, deren Hersteller oder Entwickler anpreisen, das Problem zu lösen. Ein konzentrierter Überblick über deren Merkmale sowie Vor- und Nachteile fehlt jedoch. Der Kurs hat den Zweck, diese Lücke zu schließen, und ermöglicht den Teilnehmern, verschiedene Lösungen Hands On anzuschauen.

Am Ende des Kurses sind Sie in der Lage, ein professionelles Logfile-Analyse-Setup aufzubauen und auf verschiedenen Systeme anfallende Protokoll-Daten auszuwerten. Durch das Einrichten und Vergleichen unterschiedlicher Lösungen haben Sie einen Überblick über deren Möglichkeiten und Einschränkungen. Dadurch können Sie eine qualifizierte Entscheidung treffen, welche Lösungen Sie einsetzen möchten.

Dozenten

Martin Steigerwald beschäftigt sich seit Mitte der 90er Jahre mit Linux. Er ist langjähriger Autor von Artikeln für verschiedene Computer-Magazine wie die LinuxUser (linuxuser.de) und das Linux-Magazin (linux-magazin.de). Seit Herbst 2004 ist er als Consultant für solide Server-Infrastruktur auf Linux-Basis und als Trainer für Linux-Themen bei der Proact Deutschland GmbH in Nürnberg tätig.

Termine

KW	Datum	Dozent
24	10.06.–13.06.2024	Martin Steigerwald
49	02.12.–03.12.2024	Martin Steigerwald

Weitere Termine auf Anfrage.

Preise

Komplett-Paket
2.360,00 EUR
zuzüglich 19% Ust. (=2.808,40 EUR brutto)
inkl. Hotel, Abendessen und Abendprogramm

Standard-Paket / Online-Paket
2.000,00 EUR
zuzüglich 19% Ust. (=2.380,00 EUR brutto)
ohne Hotel, Abendessen und Abendprogramm.

Komplett-Paket + Zusatznacht am Vortag
2.480,00 EUR
zuzüglich 19% Ust. (=2.951,20 EUR brutto)
inkl. Hotel, Abendessen und Abendprogramm sowie einer zusätzlichen Hotelnacht am Vortag zum Preis von 120,00 EUR (zzgl. 19% USt = 142,80 EUR brutto).

Wenn Sie Fragen haben oder einen Platz reservieren möchten erreichen Sie uns telefonisch unter **030-405051-40** oder per Mail unter **mail@heinlein-akademie.de**.

Die Schulungen finden, sofern nicht anders angegeben, in den Räumlichkeiten der Heinlein Support GmbH, **Schwedter Str. 8/9B, 10119 Berlin** statt.

Anmeldung unter: http://www.heinlein-support.de/schulung/logfile-analyse-mit-elasticsearch-logstash-und-kibana

Heinlein Support GmbH
Schwedter Straße 8/9B
10119 Berlin

Tel.: +49 (0)30 40 50 51-0
Fax: +49 (0)30 40 50 51-19
mail@heinlein-support.de
www.heinlein-support.de