heinlein

Akademie

Logfile-Analyse mit dem OpenSearch Stack

System-Administratoren in heterogenen Umgebungen verwalten oft große Mengen an Protokolldaten verschiedener Systeme in unterschiedlichen Formaten. Bei Fehlern sind diese Protokolle oft der einzige Hinweis auf die Ursache, doch deren manuelle Analyse über viele Server hinweg ist zeitaufwendig. Der Kurs konzentriert sich auf eine bewährte, freie Softwarelösung, die effiziente Datenanalyse ermöglicht. Eine passende Vorauswahl an Werkzeugen erleichtert den Einstieg in die Logfile-Analyse.

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

Der OpenSearch Stack bietet eine Alternative zum Elastic Stack mit Elasticsearch, Kibana, Elastic Beats, Logstash und mehr. Diese Alternative besteht komplett aus freier Software. Das betrifft auch erweiterte Funktionen, die bei anderen Lösungen oft unter proprietären Lizenzen stehen.

Im Rahmen des Kurses installieren Sie einen OpenSearch Cluster und die Web-Oberfläche OpenSearch Dashboards. Mit ausgewählten Lösungen wie Fluentd und Logstash transportieren Sie Protokoll-Daten in den Cluster, die Sie dann mit OpenSearch Dashboards näher auswerten. Sie lernen die Möglichkeiten von OpenSearch Dashboards und ausgewählter Plugins kennen.

Einführung

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

Konzepte und Begriffe

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

Erste Schritte: Installation und Konfiguration eines OpenSearch Clusters

OpenSearch im Vergleich zu anderen Lösungen zur Logfile-Analyse

Gängige Log-Quellen

- Syslog
- Webserver, Mailserver, MariaDB, PostgreSQL
- Windows Event Log, Windows-Dienste
- Netzwerk-Komponenten

Transport und Verarbeitung von Protokoll-Meldungen

- Fluentd
- Fluent Bit
- Rsyslog
- Dataprepper
- Logstash

Speicherung in OpenSearch

- Einzeln und als Cluster
- Monitoring mit OpenSearch Dashboards
- Performance-Aspekte
- Alte Daten aufräumen
- Backup

Oberflächen

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

Suche

- Lucene
- OpenSearch Dashboards Query Language

Ziel

Am Ende des Kurses sind Sie in der Lage, ein professionelles Logfile-Analyse-Setup aufzubauen und auf verschiedenen Systeme anfallende Protokoll-Daten auszuwerten. Mit Hilfe des OpenSearch Stacks und ausgewählter zusätzlicher Lösungen wie Fluentd oder Logstash wandeln Sie Protokoll-Daten in unterschiedlichen Formaten in ein einheitliches Format, das sich leicht auswerten lässt.

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

Leider gibt es für diese Schulung momentan keinen festen Termin. Bei Interesse an einer Schulungsteilnahme oder an einer Inhouse-Schulung zu diesem Thema, wenden Sie sich bitte per Mail an uns. Vielen Dank.

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-opensearch-stack**