Elasticsearch Watcher Hands-on: Ein Use Case der anderen Art

Bianca Schlüter, SHI GmbH

Ihre Referentin

Bianca Schlüter

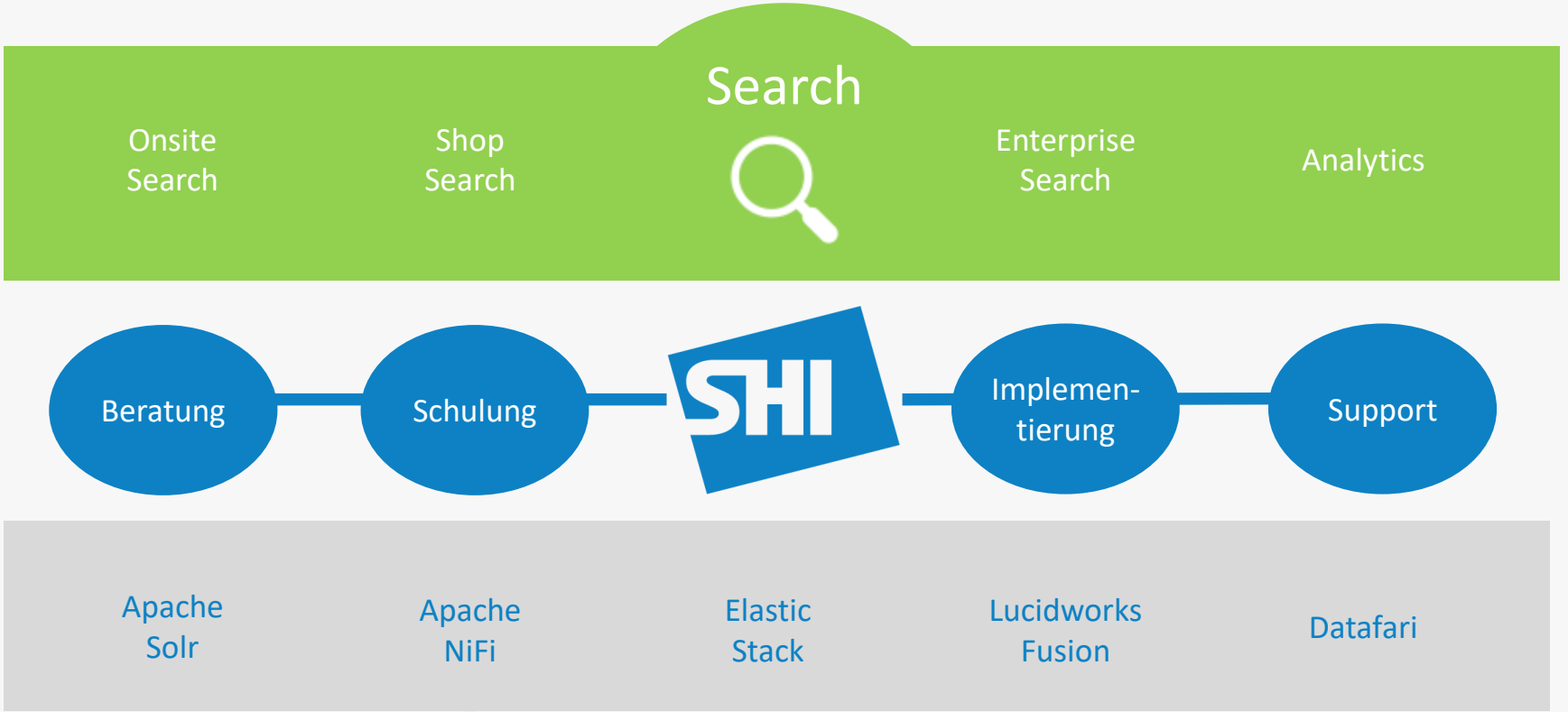
Senior Consultant Search & Analytics
Bianca.Schlueter@shi-gmbh.com

- Unterstützt Unternehmen bei der Integration und Optimierung von Such- und Analytics-Lösungen
- Toolkit: Elastic Stack, Apache NiFi, Apache Solr, …

www.shi-gmbh.com

Search | Analytics | Big Data

Die SHI auf einen Blick



Agenda

1. Was ist der Elastic Stack?
2. Was sind Watcher?
3. Ein Watcher-Use-Case der anderen Art
4. Demo

Was ist der Elastic Stack?

Elastic Stack: Use Cases

Application and Website Search

Logging and Log Analytics

Enterprise Search

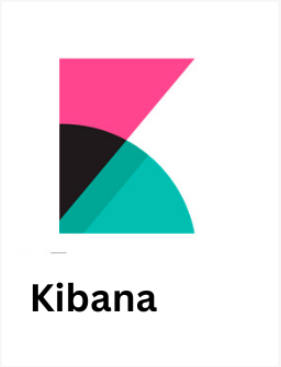
Data Analytics

Business Analytics

Geospatial Data Analysis

Security Analysis

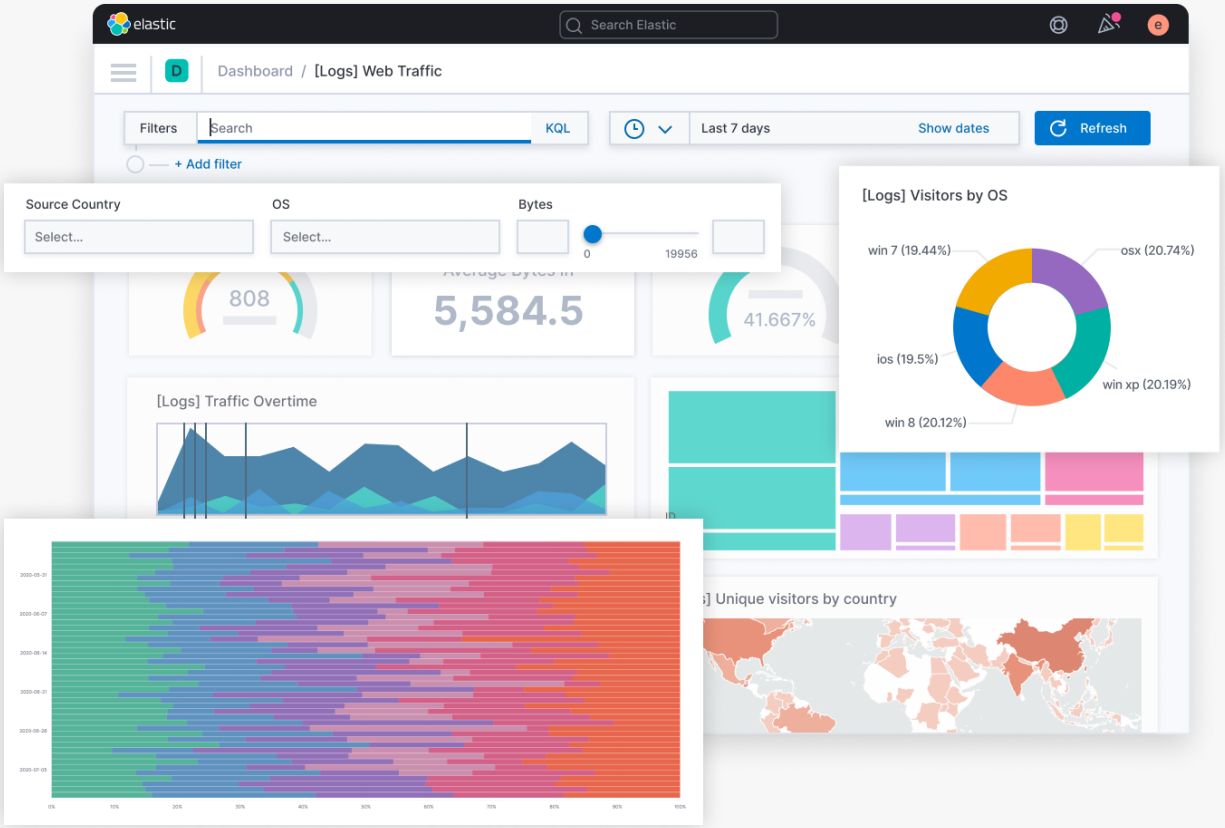
Was ist der Elastic Stack?



Indexierung & Speicherung

Analyse & Visualisierung

Kibana Dashboards



Was sind Watcher?

Was sind Watcher?

- Feature von Elasticsearch
- Verfügbar in Platinum und Enterprise Version
- Alerting und Monitoring

Überwachen von Änderungen oder Anomalien in den Daten und als Konsequenz Durchführen von erforderlichen **Aktionen**.

Beispielhafte Use Cases

- Versenden Sie täglich per E-Mail einen Report, der die Verkaufszahlen des Vortages Ihres Onlineshops beinhaltet.
- Überwachen Sie den Status Ihres Elasticsearch Clusters durch regelmäßiges Aufrufen der Cluster-Health-API. Bei Problemen wird eine Nachricht in einen Slack Channel gepostet.
- Überwachen Sie die Festplattennutzung Ihrer Server. Wenn ein gewisser Schwellwert überschritten wird, wird automatisch ein Helpdesk-Ticket eröffnet.

Wann eignen sich Watcher für meinen Use Case?

Die relevanten Daten können mit einer regelmäßigen **Elasticsearch-Abfrage** identifiziert werden

Die Ergebnisse der Abfrage können anhand einer **Bedingung** überprüft werden.

Durchführen von einer oder mehrerer **Aktionen** (z.B. Senden einer E-Mail, Speicherung der Abfrageergebnisse).

Konfigurationselemente von Watchern

Schedule

Ein Zeitplan für die Ausführung des Watchers, etwa alle x Sekunden / Minuten oder eine Cron.

Input

Typischerweise Search Input, kann aber auch ein HTTP-Input sein.

Auf den Input kann in den folgenden Conditions und Actions zugegriffen werden.

Condition

Legt fest, ob die Aktionen ausgeführt werden sollen oder nicht. Kann bei komplexeren Szenarien Skripte beinhalten. Ansonsten typischerweise ein Schwellwertabgleich.

Payload Transform (optional)

Manipuliert den Payload (etwa die Response der Input Query) für die Watcher-Aktion(en).

Action

Eine oder mehrere Aktionen, wie z. B. das Versenden von E-Mails, die Weiterleitung von Daten an Drittsysteme über einen Webhook oder die Indexierung der Abfrageergebnisse.

Flexibilität von Watchern

Mehrere Input-Quellen möglich durch sogenannte Chain Inputs

Mehrere Aktionen möglich

Bedingungen können global oder pro Aktion definiert werden

Transformationen können global oder pro Aktion definiert werden

Genau diese Flexibilität ermöglicht es, Watcher sehr vielseitig einzusetzen!

Ein Watcher-Use-Case der anderen Art

Enterprise Search

- Komponente A: Indexierung der Inhalte
- Komponente B: Suche in den Inhalten

Ziel

- Bestimmung des Gesundheitszustand der Enterprise Search und ihrer zwei Subkomponenten
- Darstellung des Gesundheitsstatus in einem Dashboard
- Integriertes Alerting

Berechnungslogik

Status der Indexierung: Hier interessieren wir uns für das maximale CPU aller für die Indexierung verantwortlichen Server

- Max(CPU) > 90%: Status lautet "rot"
- Ansonsten lautet Status "grün"

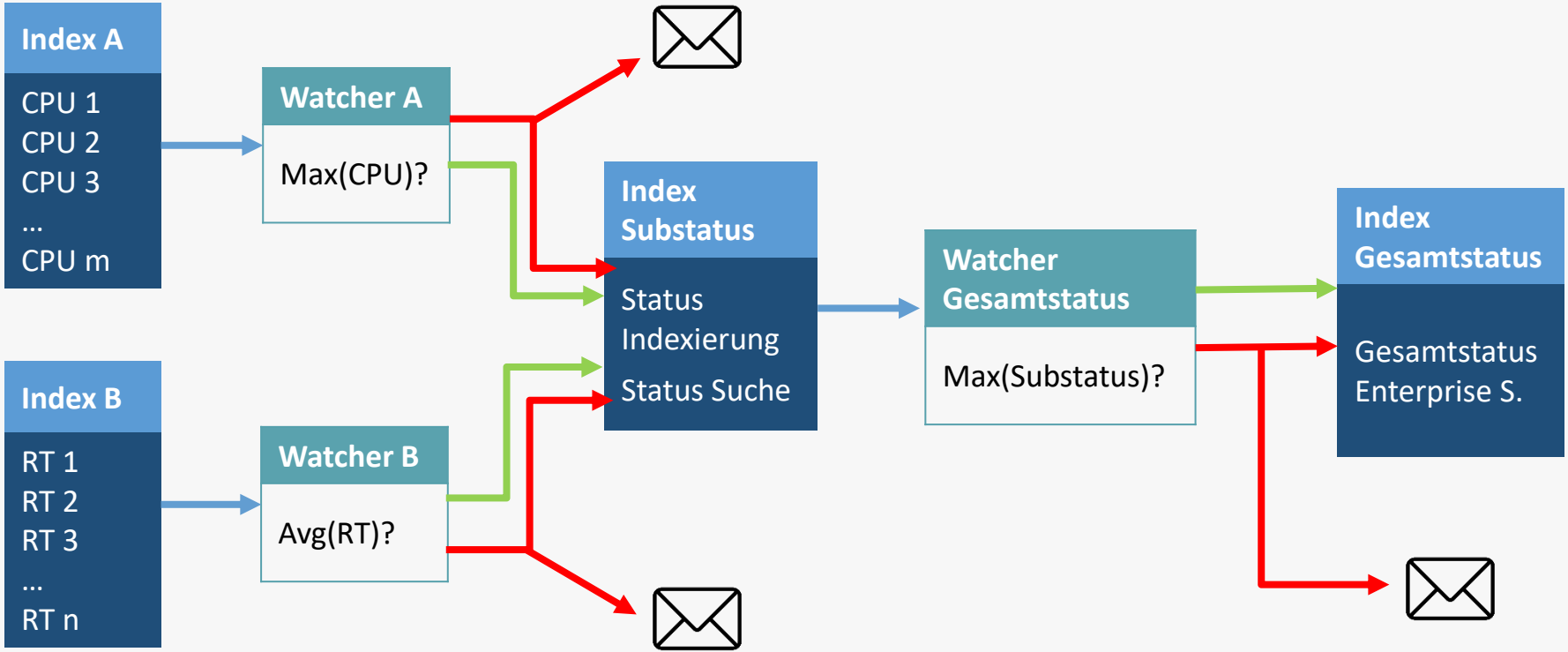
Status der Suche: Die durchschnittliche Responsetime aller Suchanfragen wird betrachtet

- Avg(Responsetime) > 500ms: Status lautet "rot"
- Ansonsten lautet Status "grün"

Gesamtstatus der Enterprise Search:

- Ist der Status beider Komponenten „grün“, dann ist auch der Gesamtstatus des Systems „grün“.
- Ist der Status mindestens einer Komponente "rot", dann ist auch der Gesamtstatus "rot".

Umsetzung mit Watchern



Demo Time!

Links

Watcher Doku: https://www.elastic.co/guide/en/elasticsearch/reference/current/xpack-alerting.html

Elastic Website: https://www.elastic.co/de/

Elasticsearch Doku: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

Kibana Doku: https://www.elastic.co/guide/en/kibana/current/index.html

Wir freuen uns auf Euch!

Unser Newsletter

Unser Blog und unsere Website

Die SHI auf LinkedIn

Danke für Eure Aufmerksamkeit!

KONTAKT

SHI GmbH

www.shi-gmbh.com

Konrad-Adenauer-Allee 15

86150 Augsburg

info@shi-gmbh.com

0821-74 82 633 - 0