Evaluation, Installation, Konfiguration und Inbetriebnahme eines zentralisierten Logging-Systems

durchgeführt von:
Kai Müller

Ausbildungsberuf:
Fachinformatiker für Systemintegration

cewe

Agenda

1. Einführung

- Das Projektumfeld
- Ziele des Projekts

2. Planung

- Ist-Zustand
- Soll-Konzept
- Auswahl der Software
- Auswahl der Hardware

3. Umsetzung

- Vorbereitung
- Der Elastic-Stack
- Konfiguration

4. Abschluss

- Projekt- & Folgekosten
- Amortisation
- Fazit & Ausblick

Einführung

Das Projektumfeld
Die CEWE Stiftung & Co. KGaA

Abb. 2 CEWE Hauptsitz Oldenburg

https://company.cewe.de/de/ueber-uns/unternehmensgruppe/standorte/standort-oldenburg.html

- Größtes Fotoentwicklungsunternehmen in Europa
- Hauptsitz und größte Produktionsstätte in Oldenburg
- Rund 4.000 Mitarbeiter
- 14 Produktionsstätten
- Lieferung in 21 Länder Europas
- Beliebte Fotoprodukte
  - Handyhüllen
  - Art Prints
  - CEWE Fotobuch

Ziele des Projekts
Ein zentrales Logging-System

- Ablösen des zeitintensiven Arbeitslaufes
  - Arbeitszeitersparnis der Mitarbeiter
  - Weniger fehleranfälliger Ablauf
  - Einheitlicher Workflow
- Kostenersparnis

Planung

Ist-Zustand

- Über 200 zu administrierende Geräte
- Verschiedene Dienste, in-house Software und Betriebssysteme
- Log-Dateien werden von Hand aufgerufen:
  - Linux-Maschinen: Zugriff via SSH
  - Windows-Maschinen: Zugriff via Remote Desktop
  - Navigation durch Ordnerstrukturen zeitaufwändig

Soll-Konzept

- Zentrales System für das Log-Management
- Log-Dateien sollen zentral gesammelt werden
- Zugriff via Weboberfläche
  - Zugang über Benutzeranmeldung
- Filtermöglichkeiten
- On-Premise, keine Cloud-Lösung

Auswahl der Software

Eigenschaft	Gewichtung	Elastic-Stack		Graylog	
		Pkt.	Gew.	Pkt.	Gew.
Log-Parsing	35%	5	1,75	3	1,05
Visualisierung	10%	5	0,50	1	0,10
Einrichten von Suchmustern	10%	4	0,40	2	0,20
Dokumentation, Anleitung	30%	5	1,50	3	0,90
Auswahl an Log-Shippern	10%	3	0,30	2	0,20
Verfügbarkeit von Plugins	5%	4	0,20	3	0,15
	Ergebnis	26	4,65	14	2,60

0 = nicht vorhanden, 1 = schlecht, 2 = ausreichend, 3 = befriedigend, 4 = gut, 5 = sehr gut

Auswahl der Hardware

	Anschaffungskosten	Kosten pro Jahr	Gesamtkosten über zwei Jahre Nutzungsdauer
physischer Server	2.842,17€	1.388,57€	5.619,31€
virtuelle Maschine	-	339,45€	678,90€

- Es wurde ein Angebot für einen Server bei Thomas Krenn eingeholt
- Die virtuelle Maschine kann auf dem Produktionscluster gehostet werden
- Kostenersparnis von 4.940,41€ gegenüber einem physischen Server
- Anschaffungskosten der Virtualisierung in VM-Kosten berücksichtigt

-> Aufgrund des Preises habe ich mich für die virtuelle Maschine entschieden

Umsetzung

Vorbereitung
Erstellen der virtuellen Maschine

- Vorteile durch Skalierbarkeit
- Einfache Erweiterung der Kapazitäten bei Bedarf
- Schnelles Replizieren der Maschine
- Einfache Erstellung von Backups während der Laufzeit

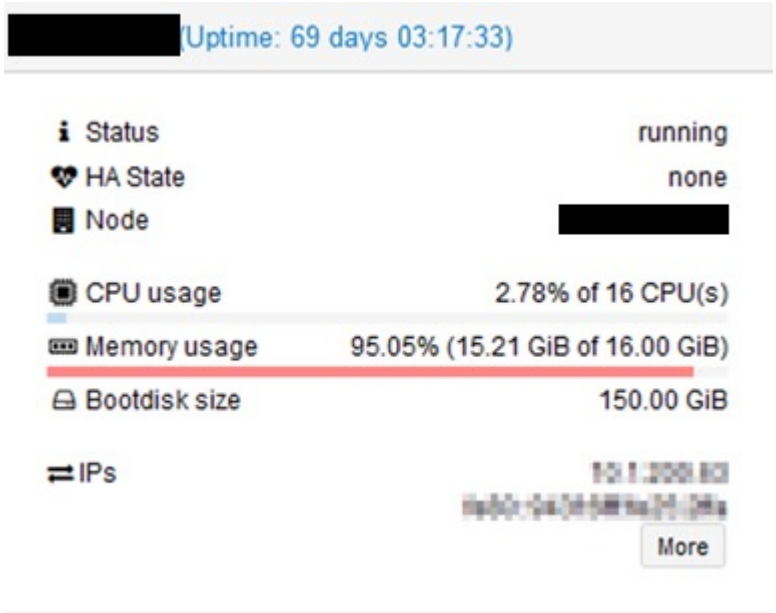

Abb. 3 Zusammenfassung der Projekt-VM

Der Elastic-Stack
Die Komponenten

- Sammlung von Open-Source Produkten der Firma ***Elastic***
- Komponenten bauen aufeinander auf und erfüllen verschiedene Rollen
- Beats ist eine offene Plattform für anwendungsspezifische Datenübertragung
- Früher ELK-Stack aber seit Einführung von Beats nur noch Elastic-Stack

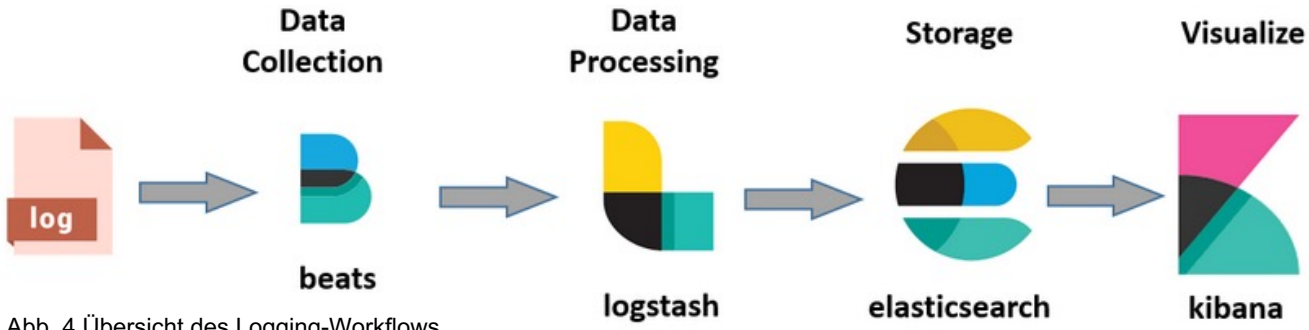

Abb. 4 Übersicht des Logging-Workflows

Konfiguration

- Konfiguration wird in .yml oder .yaml Dateien vorgenommen
- Standardmäßig in z.B. /etc/kibana/kibana.yml zu finden
- Filebeat wird auf jedem Client installiert und konfiguriert

```
# ============================== Filebeat inputs ===============================
filebeat.inputs:
- type: log
  # Change to true to enable this input configuration.
  enabled: true
  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /home/[redacted]
  include_lines:
    - 'FATAL'
    - 'JdfHubController'
  fields:
    sourcefiletype: [redacted]
  fields_under_root: false

# ---------------------------- Logstash Output -----------------------------
output.logstash:
  # The Logstash hosts
  hosts: [redacted]
```

Abb. 5 Auszug der Filebeat.yml

Fertige Umsetzung

- Log-Shipper senden die Log-Dateien an den Logging-Server
- Anwender greifen auf Logging-Server zu
- Nutzerrechte beschränken Sichtbarkeit der Log-Dateien

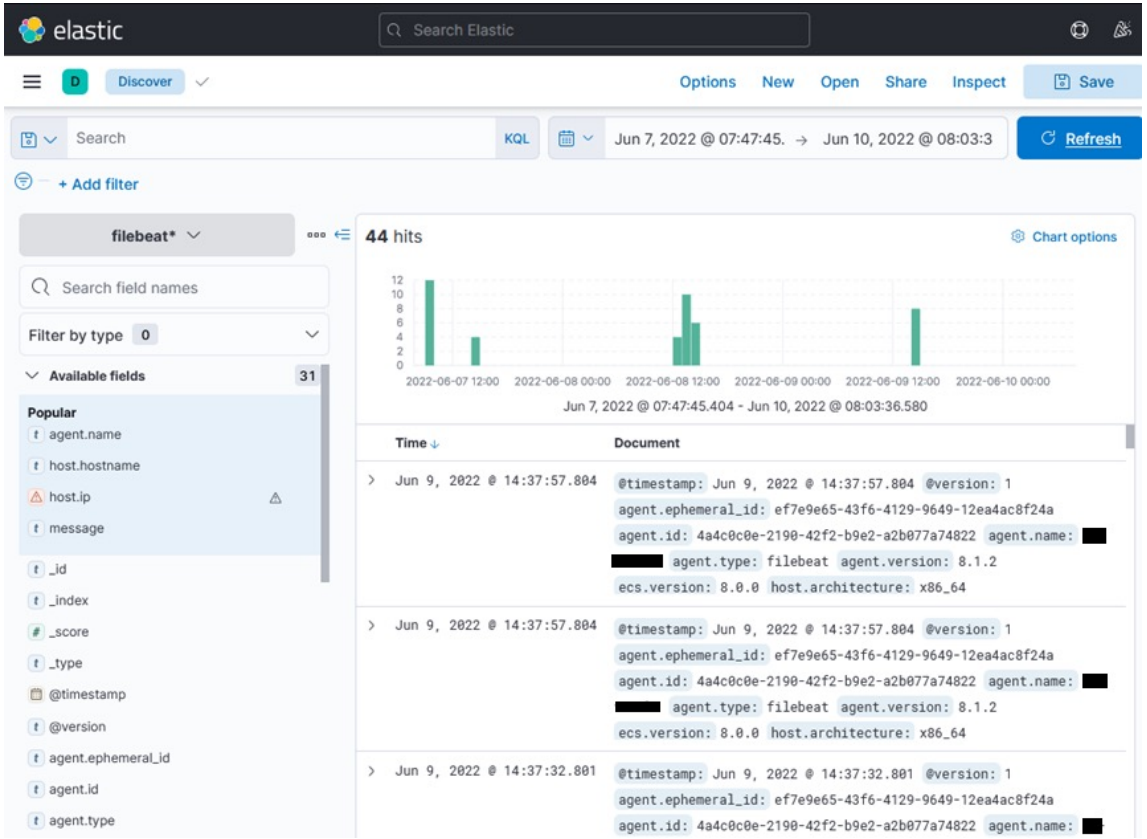

Abb. 6 Kibana Übersicht

Abschluss

Projekt- & Folgekosten

Gesamtprojektkosten über 2 Jahre

Aufwendungen	Kosten
Kosten der VM über 2 Jahre	678,90€
Erfassung neuer Systeme [redacted] Stunden á [redacted]	3.060,00€
Administration [redacted] Stunden á [redacted]	2.040,00€
Arbeitszeit Kai Müller [redacted] Stunden á [redacted]	1.590,00€
Personalkosten	127,50€
	7.496,40€

Kosten des alten Workflows pro Monat

Aufwendungen	Kosten pro Monat
[redacted] Fehlersuche pro Monat á [redacted]	892,50€

Kosten des neuen Workflows pro Monat

Aufwendungen	Kosten pro Monat
[redacted] Fehlersuche pro Monat á [redacted]	357,20€

Amortisation

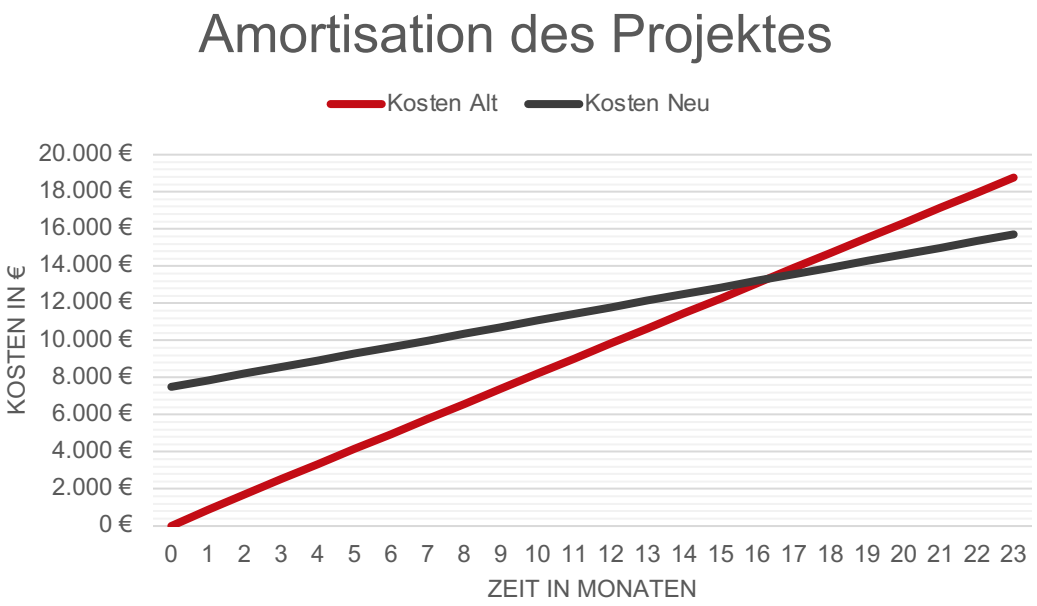

Abb. 7 Amortisationsrechnung

- Erwartete Amortisation ab dem 16. Monat
- Hohe Investitionskosten aber ca. 60% Reduktion der Arbeitszeit
- Projekt schon innerhalb der Testphase rentabel

Fazit & Zukunft

- Zeitaufwendiges Setup
- Erfolgreiche Umsetzung der Teststellung in 35h möglich
- Erhebliche Entlastung der Mitarbeiter der Produktions-IT erwartet
- Nicht nur Zeit- sondern auch Kostenersparnis

- Zukunft:
  - System lässt sich weiter ausbauen, z.B. Failover, Cluster, Entwicklung eigener Filter
  - Überführung der ausbleibende Systeme wird nach Abschlussprüfung durchgeführt

Abbildungsverzeichnis