Pushing IT forward!

KoSSE KOMPETENZVERBUND SOFTWARE SYSTEMS ENGINEERING SCHLESWIG-HOLSTEIN

CONSIST Business Information Technology

Was haben Logdaten mit dem Unternehmenserfolg zu tun?

30.11.2012
Kieker-Days
Matthias Bauer

CONSIST

Consist World Group im Überblick

- Mission
  - IT-Services für die individuellen Geschäftsprozesse unserer Kunden
- 1.200 Mitarbeiter, 100 Mio $ Umsatz
- Gegründet in 1972, in privater Hand
- Mit 12 Standorten weltweit in Europa, Amerika und Asien
- Kunden in über 30 Ländern weltweit

Aktuelle Fakten: Consist GmbH

- Gesellschafter: Consist Software Solutions Inc. (USA)
- Standorte: Kiel (Sitz), Hamburg, Berlin und Darmstadt
  - Ca. 210 Mitarbeiter in Deutschland
- Tochter: Consist ITU Environmental Software GmbH (100%)

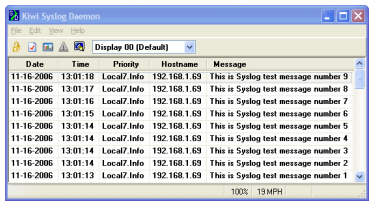
Stammsitz
in Kiel, Eigentum seit 1997

Consist Referenzen

Was haben Logdateien mit dem Unternehmenserfolg zu tun?

Monitoring

- Applikations-, Filter-, Interceptorlogs
- Logs der Laufzeitumgebung
- Syslog
- Betriebssystem
- Datenbank
- Clusterbetrieb?
- Virtualisierung?
- ……



Logdaten sind semi-strukturiert

CONSIST
Business Information Technology

ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

---

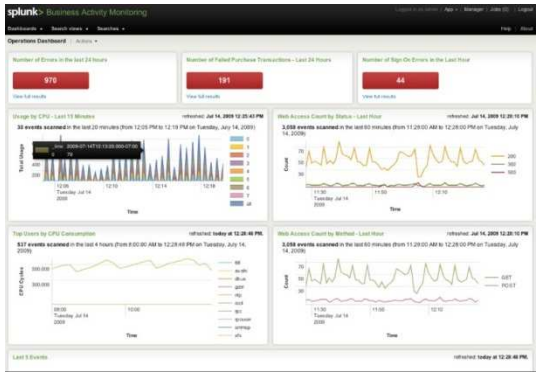
05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link: "http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place”}, objectType:"person”,preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!”,objectType:"activity”,postedTime:"2012-05-21T16:39:40.647-0600”}

Was geht noch?

- Können Logdaten über das Monitoring hinaus weiteren Mehrwert liefern?
- Z.B.: Daten eines Webserver-Logs
  - Enthalten alle Zugriffe auf das System
  - Enthalten Statusinformationen
  - Enthalten Aufrufparameter
  - Enthalten Einzelzugriffe, die zusammen einen Prozess ergeben
- Können Logdaten aktuelle Geschäftsinformationen liefern?

Verschiedene Sichten auf dieselben Daten



ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

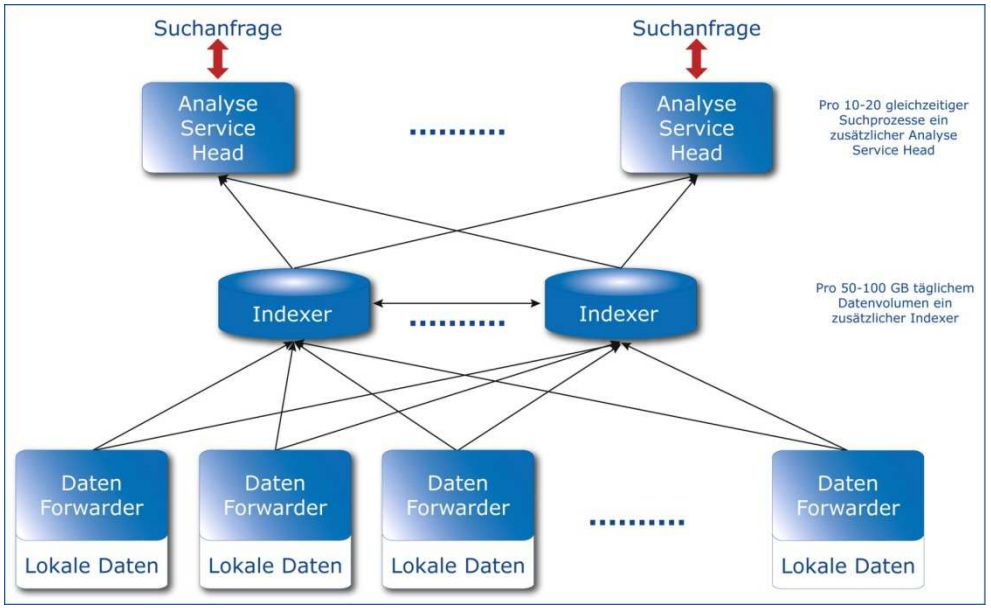
May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

---

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link: "http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"}, objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}

Technologiepartner: splunk



- 70 MB Software
  - Installiert in Minuten
- Keine Datenbank
- Skalierbar
  - Map/Reduce
  - Scale-Out statt Scale-Up
  - Verarbeitet mehr als 100 TB Daten/Tag
- Commodity Hardware
- Splunkbase
  - Appstore

Mehrwert durch Korrelation

- Logdaten werden in dem Moment geschrieben, in dem die Aktion passiert.
  - Liefern damit zeitnahe (realtime) Einblicke in aktuelle Geschäftsinformationen
- Logdaten sind vielseitig auswertbar
  - Application Management
  - Operational Intelligence
  - Marketing Controlling
  - Reputation Management
  - .....
- Mehrwert der Logdaten entsteht über Korrelation strukturell verschiedener aber zeitlich zusammenhängender Logevents

Pushing IT forward!

CONSIST
Business Information Technology

Herzlichen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

CONSIST