SerNet

Elasticsearch goes BIRT
Praxisbericht einer Zweckentfremdung

17. September 2015, BED-Con

Sebastian Hagedorn

SerNet GmbH, Göttingen - Berlin

Agenda

SerNet

- Theorie
  - verinice
  - BIRT
  - Elasticsearch
  - Schnittstelle BIRT ↔ Elasticsearch
- Praxis
  - vDesigner, Reporttemplate
  - Code
  - Report ausführen
- Ergebnisse und Fazit

Sebastian Hagedorn

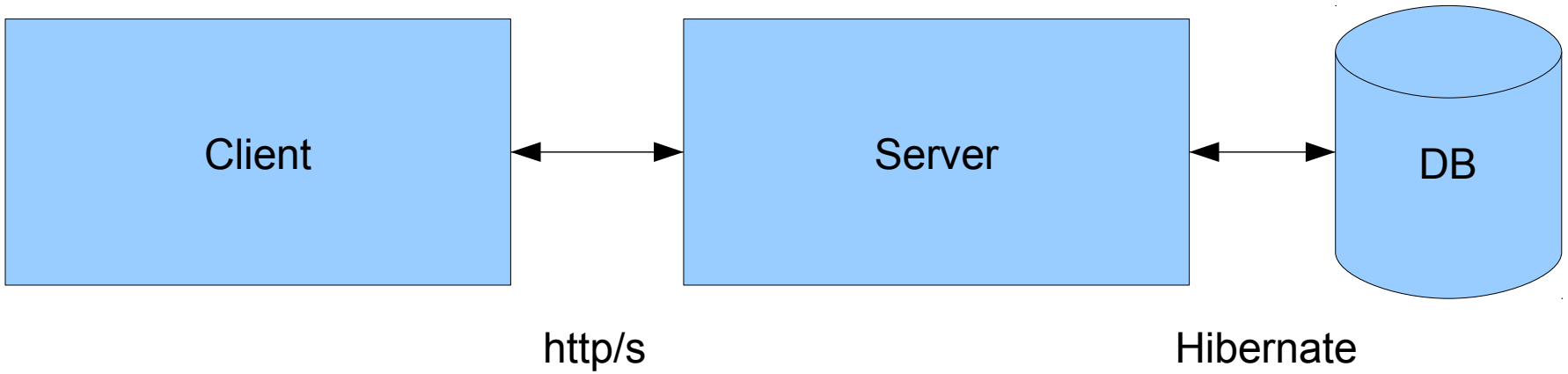
SerNet

- angestellt bei SerNet seit 2011
- Software-Entwickler im verinice.TEAM
- Bugfixing, Feature-Entwicklung, Customizing, Reports

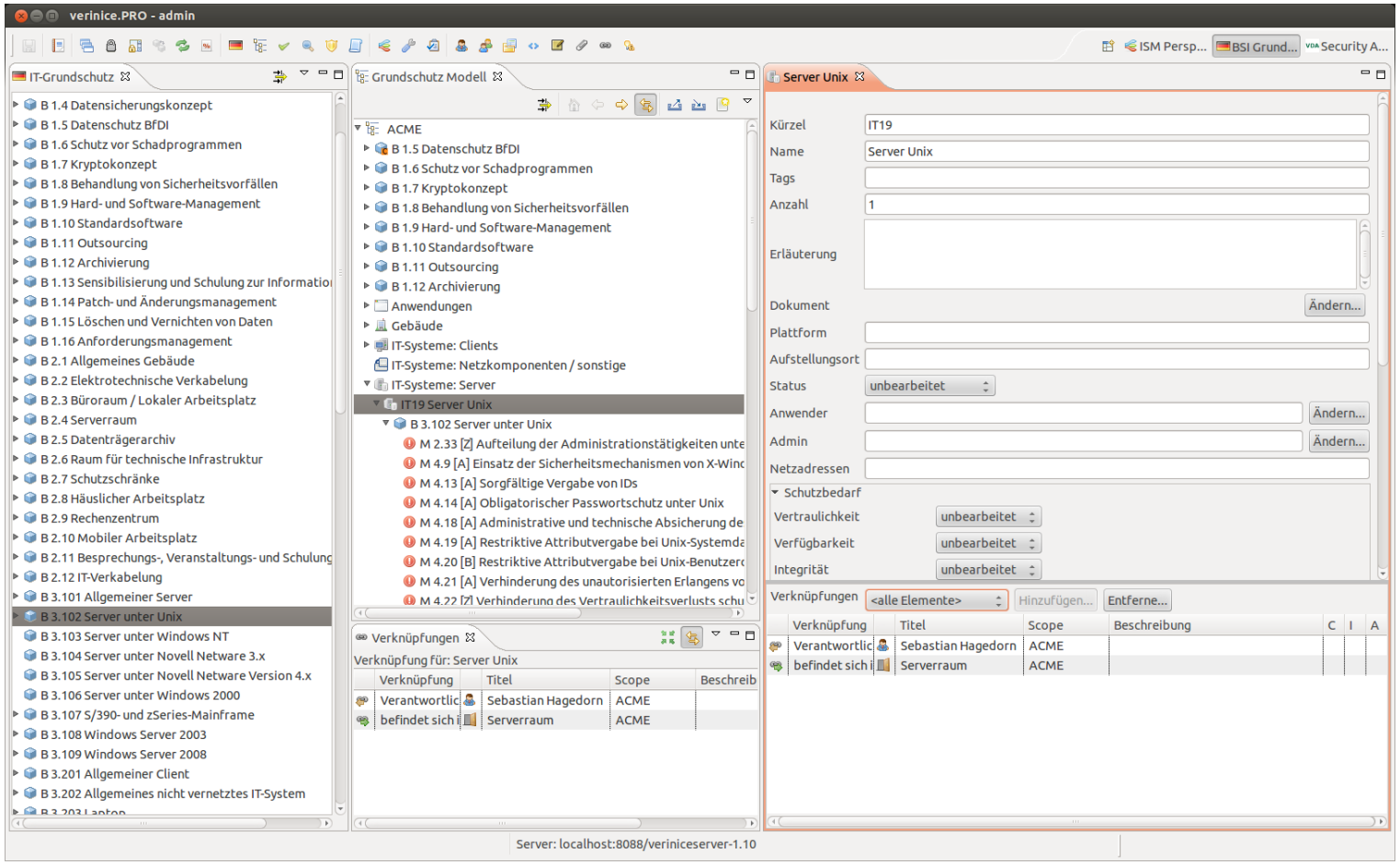
- ISMS – Informationssicherheitsmanagement-Tool
- Rich-Client / Webclient, Server (Tomcat-Servlet)
- Open Source
- setzt viele Open Source-Bibliotheken und Frameworks ein, unter anderem BIRT für Reporting und Elasticsearch zur Volltextsuche
- hauptsächlich in Java geschrieben (Eclipse RCP/PDE)

Architektur

SerNet



SerNet


verinice.PRO - admin
ISM Persp...
BSI Grund...
Security A...
IT-Grundschutz
B 1.4 Datensicherungskonzept
B 1.5 Datenschutz BfDI
B 1.6 Schutz vor Schadprogrammen
B 1.7 Kryptokonzept
B 1.8 Behandlung von Sicherheitsvorfällen
B 1.9 Hard- und Software-Management
B 1.10 Standardsoftware
B 1.11 Outsourcing
B 1.12 Archivierung
B 1.13 Sensibilisierung und Schulung zur Informatio
B 1.14 Patch- und Änderungsmanagement
B 1.15 Löschen und Vernichten von Daten
B 1.16 Anforderungsmanagement
B 2.1 Allgemeines Gebäude
B 2.2 Elektrotechnische Verkabelung
B 2.3 Büroraum / Lokaler Arbeitsplatz
B 2.4 Serverraum
B 2.5 Datenträgerarchiv
B 2.6 Raum für technische Infrastruktur
B 2.7 Schutzschränke
B 2.8 Häuslicher Arbeitsplatz
B 2.9 Rechenzentrum
B 2.10 Mobiler Arbeitsplatz
B 2.11 Besprechungs-, Veranstaltungs- und Schulung
B 2.12 IT-Verkabelung
B 3.101 Allgemeiner Server
B 3.102 Server unter Unix
B 3.103 Server unter Windows NT
B 3.104 Server unter Novell Netware 3.x
B 3.105 Server unter Novell Netware Version 4.x
B 3.106 Server unter Windows 2000
B 3.107 S/390- und zSeries-Mainframe
B 3.108 Windows Server 2003
B 3.109 Windows Server 2008
B 3.201 Allgemeiner Client
B 3.202 Allgemeines nicht vernetztes IT-System
Grundschutz Modell
ACME
B 1.5 Datenschutz BfDI
B 1.6 Schutz vor Schadprogrammen
B 1.7 Kryptokonzept
B 1.8 Behandlung von Sicherheitsvorfällen
B 1.9 Hard- und Software-Management
B 1.10 Standardsoftware
B 1.11 Outsourcing
B 1.12 Archivierung
Anwendungen
Gebäude
IT-Systeme: Clients
IT-Systeme: Netzkomponenten / sonstige
IT-Systeme: Server
IT19 Server Unix
B 3.102 Server unter Unix
M 2.33 [Z] Aufteilung der Administrationstätigkeiten unte
M 4.9 [A] Einsatz der Sicherheitsmechanismen von X-Winc
M 4.13 [A] Sorgfältige Vergabe von IDs
M 4.14 [A] Obligatorischer Passwortschutz unter Unix
M 4.18 [A] Administrative und technische Absicherung de
M 4.19 [A] Restriktive Attributvergabe bei Unix-Systemda
M 4.20 [B] Restriktive Attributvergabe bei Unix-Benutzerc
M 4.21 [A] Verhinderung des unautorisierten Erlangens vo
Verknüpfungen
Verknüpfung für: Server Unix
Verknüpfung
Titel
Scope
Beschreib
Verantwortlic
Sebastian Hagedorn
ACME
befindet sich i
Serverraum
ACME
Server Unix
Kürzel
IT19
Name
Server Unix
Tags
Anzahl
1
Erläuterung
Dokument
Ändern...
Plattform
Aufstellungsort
Status
unbearbeitet
Anwender
Ändern...
Admin
Ändern...
Netzadressen
Schutzbedarf
Vertraulichkeit
unbearbeitet
Verfügbarkeit
unbearbeitet
Integrität
unbearbeitet
Verknüpfungen
<alle Elemente>
Hinzufügen...
Entferne...
Verknüpfung
Titel
Scope
Beschreibung
C
I
A
Verantwortlic
Sebastian Hagedorn
ACME
befindet sich i
Serverraum
ACME
Server: localhost:8088/veriniceserver-1.10

Datenmodell

SerNet

- Baumstruktur, dynamisch anpassbar
- Worst-Case (für Reporting): beliebige Tiefe des Baums kann modelliert werden
- Abfragen von Eltern-Kind-Beziehung über mehrere Ebenen durch verschachtelte for-Schleifen implementiert
  → langsam
- Nicht nur Eltern-Kind Beziehungen sondern auch Verknüpfungen der Elemente untereinander möglich (ternäre Beziehungen)

BIRT

SerNet

- Business Intelligence Reporting Tool
- Eclipse-Projekt
- einfach in JEE-Projekte integrierbar
- JDBC
- versucht auf „einfache“ Art Daten visualisierbar zu machen
- Design der Report-Templates über eigenständiges Tool („WYSIWYG“)

Open Data Access (ODA)

SerNet

- Data Access Framework
- Eclipse-Projekt
- BIRT-Connectoren – ODA-Driver
- Daten und UI-Plugin
- verinice ODA-Driver stellt BSH-Interpreter in Query bereit
- beliebiger Java-Code innerhalb von Query ausführbar

BeanShell

SerNet

- dynamische Skriptsprache für die Java-VM
- erlaubt es, nahezu unveränderten Java-Code durch einen Interpreter auszuführen
- dynamische Typisierung
- Funktionen, globale Variablen
- Syntax stark an Java angelehnt
- in IQuery-Implementierung eingebettet
- ermöglicht Ansprechen der Java-/Verinice-API aus einem Report-Data-Set heraus

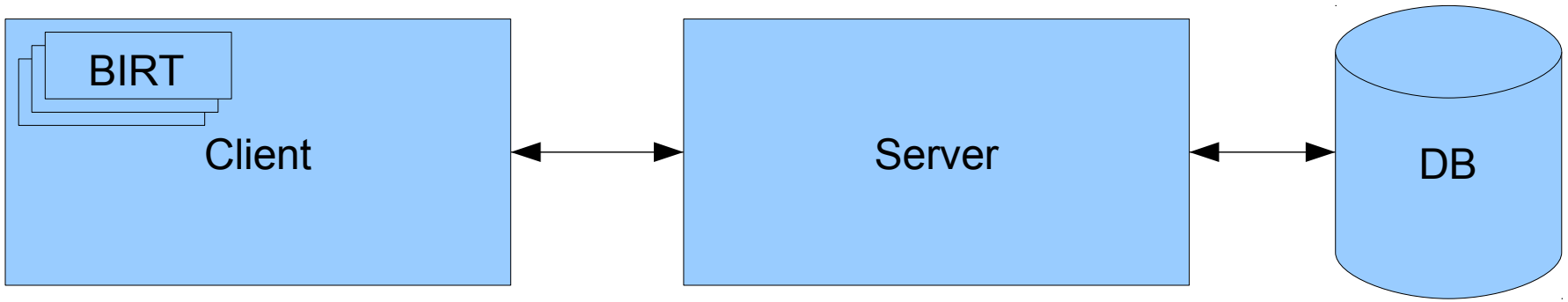
Elasticsearch

SerNet

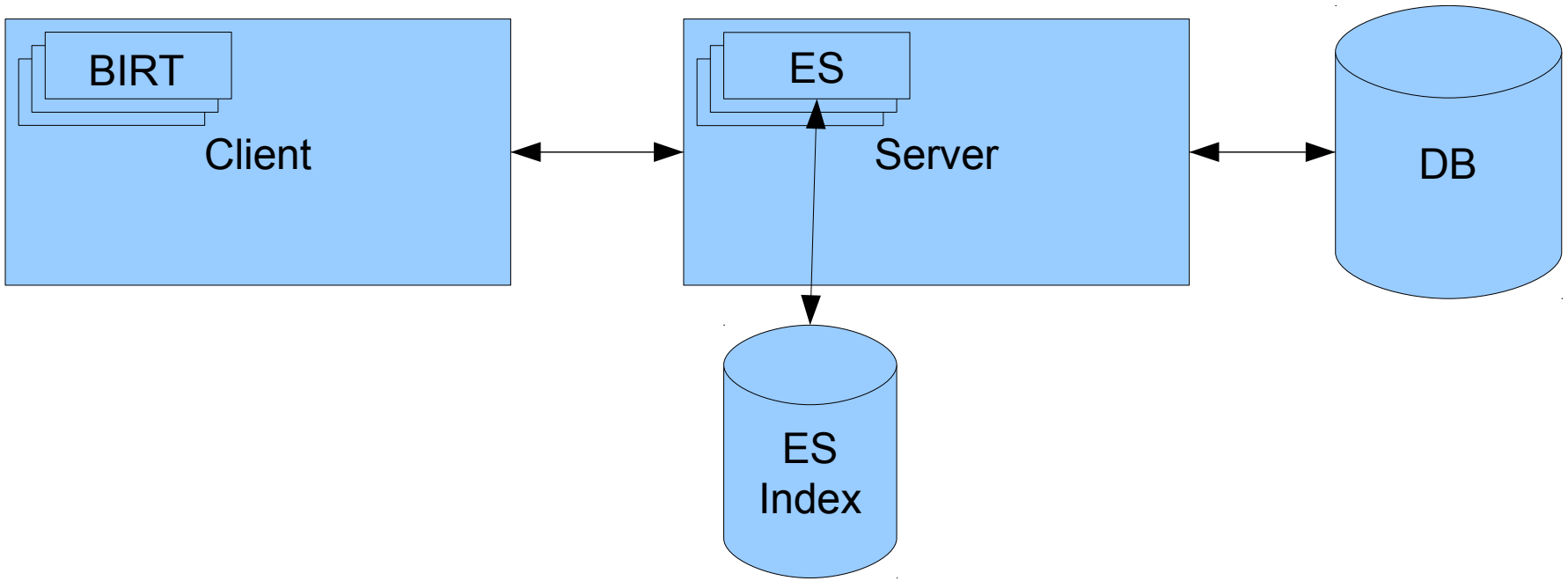
- performante Volltextsuche auf Basis von Lucene
- einfache, aber umfangreiche Java-API
- Suche auf Basis eines Index
- in verinice implementiert über ein DAO und einen Service
  - SearchService über ApplicationContext (Spring) zugreifbar
- Abstraktion der Suche über eigene Klassen
  - Query, ResultRow, ResultTable, Occurence, ...

ohne Elasticsearch

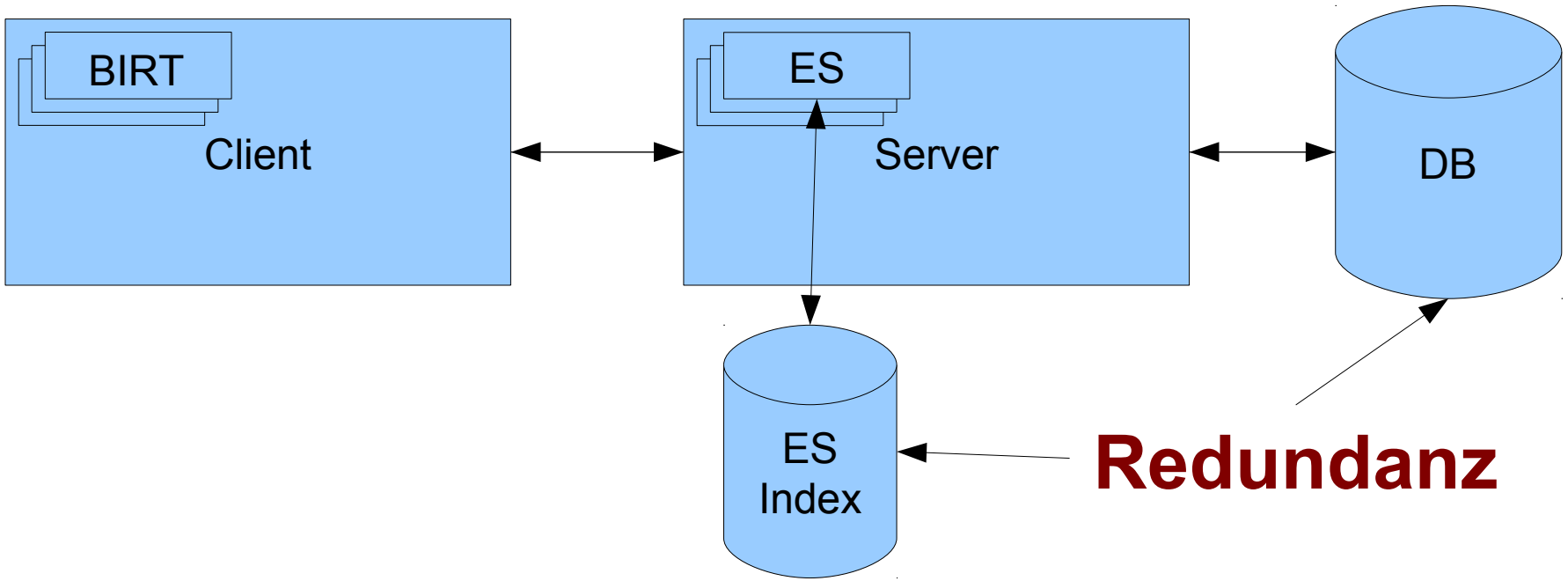
SerNet



SerNet



SerNet



Zweckentfremdung

SerNet

- Ausnutzen der Redundanz
- ES-Index speichert Objekte im JSON-Format
- (meist) schneller als langwieriges Ausführen von Commands die mit der DB kommunizieren
- Umgehen von Flaschenhals Hibernate (Cascadierung, kein Lazy-Loading, keine Proxy-Initialisierung)

Anbindung BIRT ↔ ES

SerNet

- Anbindung über eigenen ODA-Treiber nicht notwendig, aber möglich
- Erweiterung der Suchimplementierung um Filter nach Scope-Id
- Zugriff auf Elasticsearch über Data-Set in Report-Template

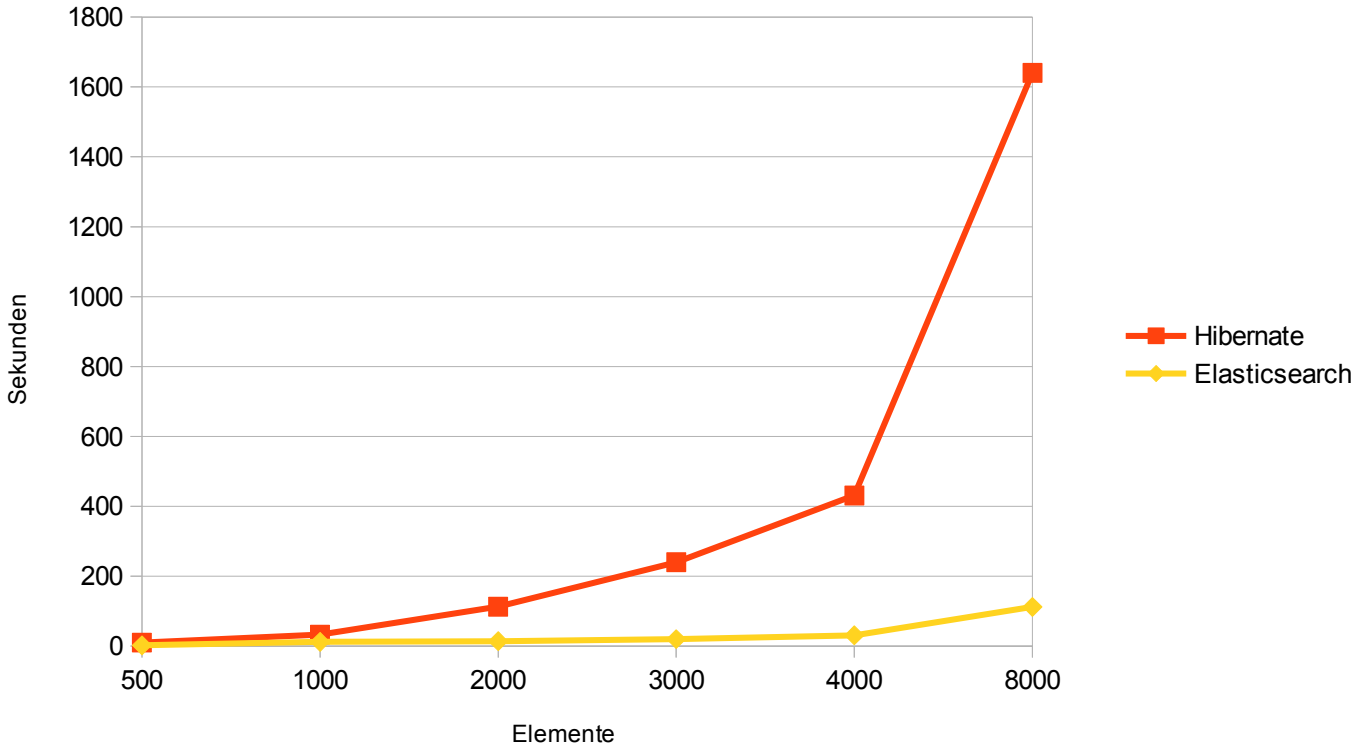
Praxis / Livedemo

SerNet

- Code SearchService + BaseDao
- BIRT / vDesigner
- verinice

Ergebnisse

SerNet



Fazit

SerNet

- einfache Integration / Implementierung einer Schnittstelle
- Abfrage von Daten über primitive Datentypen

  → Vermeiden von Overhead
- je komplexer die Anfrage, desto größer der Geschwindigkeitsgewinn
- Nachteile

Kontakt

SerNet

Sebastian Hagedorn, sh@sernet.de

SerNet GmbH

Bahnhofsallee 1b
37081 Göttingen

Torstrasse 6
10119 Berlin

tel +49 551 370000-0
fax +49 551 370000-9

+49 30 5 779 779 0
+49 30 5 779 779 9

http://svn.verinice.org
http://www.sernet.de