idh
The open system company

Infrastructure Analytics

mit

idh logging Framework ILF

Roger Zimmermann | Consulting | Informatik Projektleiter FA | Tel +41 52 366 39 01 | Mobile +41 79 932 18 96
roger.zimmermann@idh.ch | www.idh.ch | IDH GmbH | Lauchefeld 31 | CH-9548 Matzingen

Agenda

idh	Roger Zimmermann
Einführung Infrastruktur Data Logging	Roger Zimmermann
Aufbau Übersicht	Roger Zimmermann
Servicemodelle	Roger Zimmermann
Fragen ?	alle

idh Logging Framework

Wer sind wir ?

1996	Gründung der idh GmbH Schwerpunkt IT Infrastruktur
2005	Start mit Linux
2012	Start mit Partnerschaften im Hardwarebereich
2013	Start mit eigenen Produkten
	> idh logging Framework
	> idh monitoring Framework
2014	> idh cloud Framework

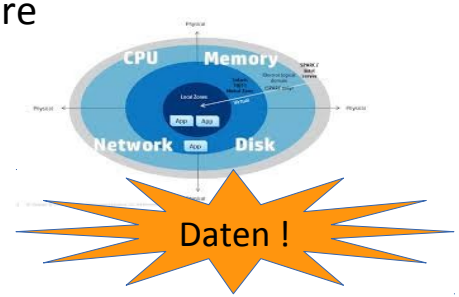
Wir sind ein Unternehmen welches mit hochqualifizierten Spezialisten den Kunden und Partnern helfen will, die immer komplexer und spezifisch werdenden Infrastrukturthemen in höchster Qualität zu planen, aufzubauen und in einen geordneten Betrieb zu bringen.
Durch breite Vernetzung stellen wir die richtigen Spezialisten für die jeweilige Herausforderung zur Verfügung.

Unser Portfolio deckt Bereiche ab, welche von den klassischen Herstellern nicht optimal vertreten werden.
Dabei wählen wir den Weg mit lizenzpflichtigen und/oder opensource Komponenten.

Durch die Kombination, gelingt es uns kostengünstig und mit hoher Qualität Leistungen an den Markt zu bringen.

Herausforderung

Hardware



Datenbanken

Applikationen

Infrastruktur

Daten ?

Betriebsysteme

Flexibilität

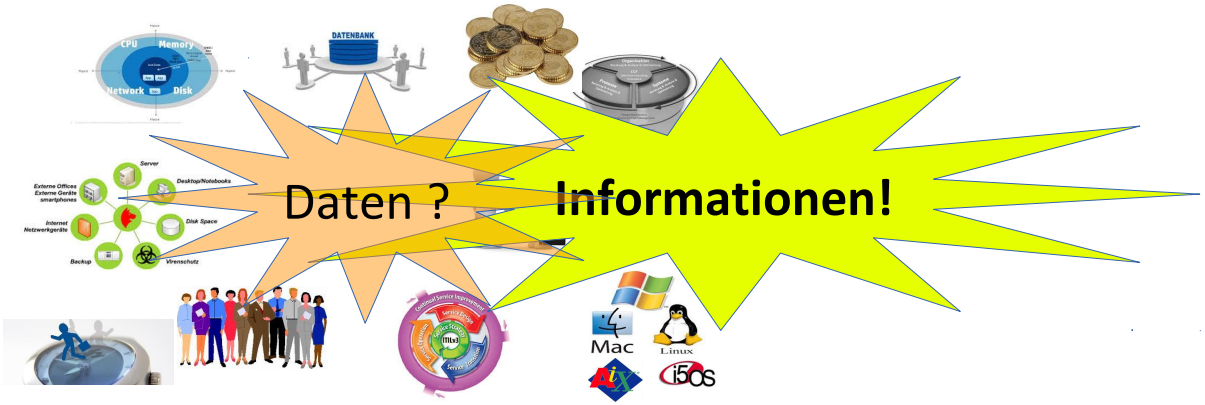
Ressourcen

Kundenanforderung

Prozesse

Kosten

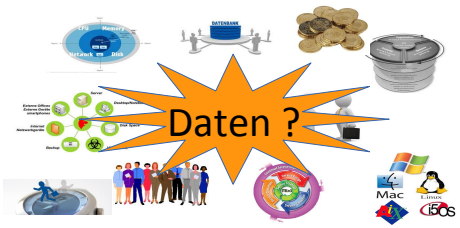
Herausforderung



Wie komme ich von vorhandenen Daten zu verwertbaren Informationen ?

Herausforderung

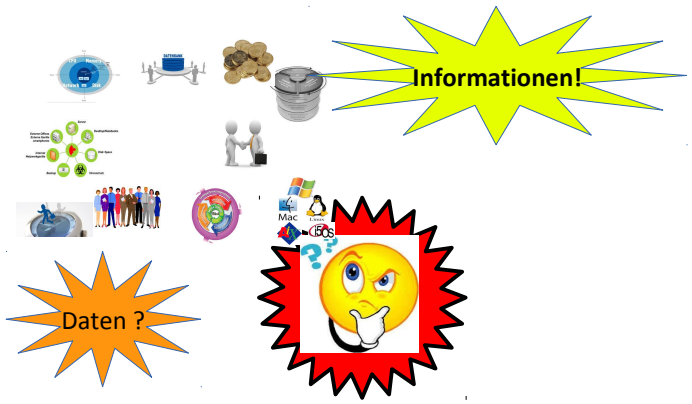
- Vernetzte Applikationen, welche (logging) Daten dezentral schreiben
- Vernetzte Infrastruktur, welche heterogen (logging) Daten schreiben
- Dezentrales Fehlersuchen erschwert Kommunikation unter den Teams
- Optimierung von Prozessen durch Daten-Fragmentierung kaum möglich
- Zeit und Kosten



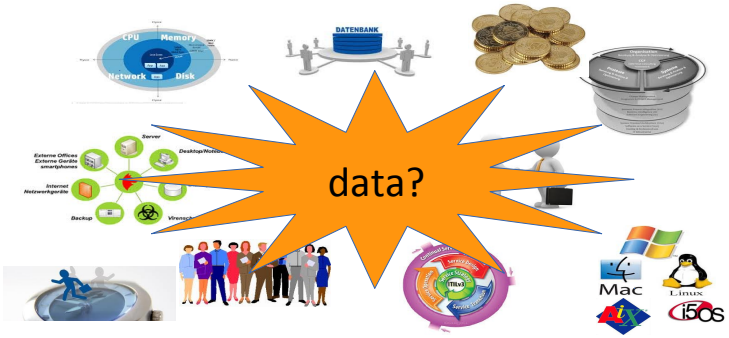
Wie komme ich von vorhandenen Daten zu verwertbaren Informationen ?

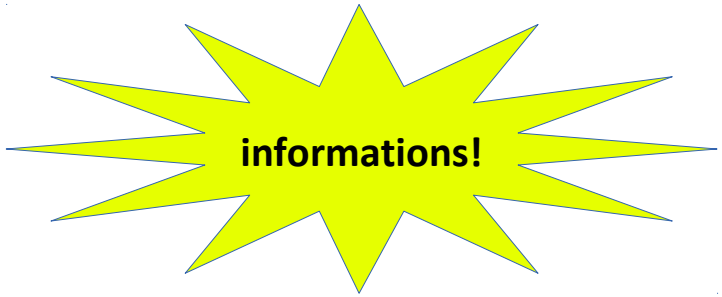
Motivation

- Vereinfachtes Troubleshooting
  - Zentrales Verwalten von (Infrastruktur)-Log's
  - Gesamtheitliche und übergreifende Fehleranalyse
- IT Grundschutz
  - Audit und Compliance
  - Forensik
- Alarming und Monitoring
  - Korrelationen aus verschiedenen logging Daten und Weiterleitung an Monitoring
- Planung
  - Trendanalyse
  - Reporting
  - Analytik
- Kosten
  - Keine Lizenzkosten
  - Kurze Implementationszeit
  - Support bei Bedarf



Ziel

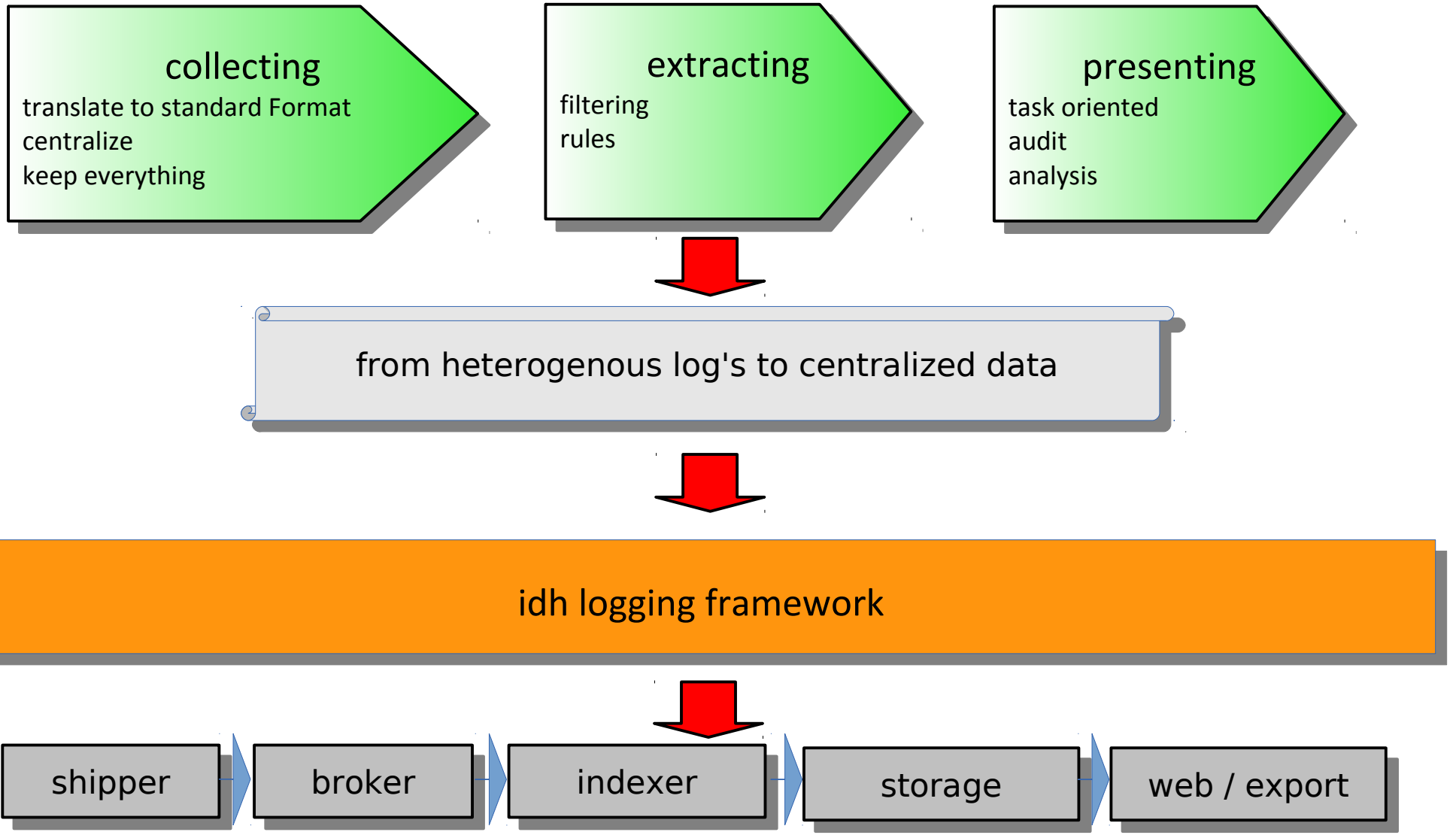




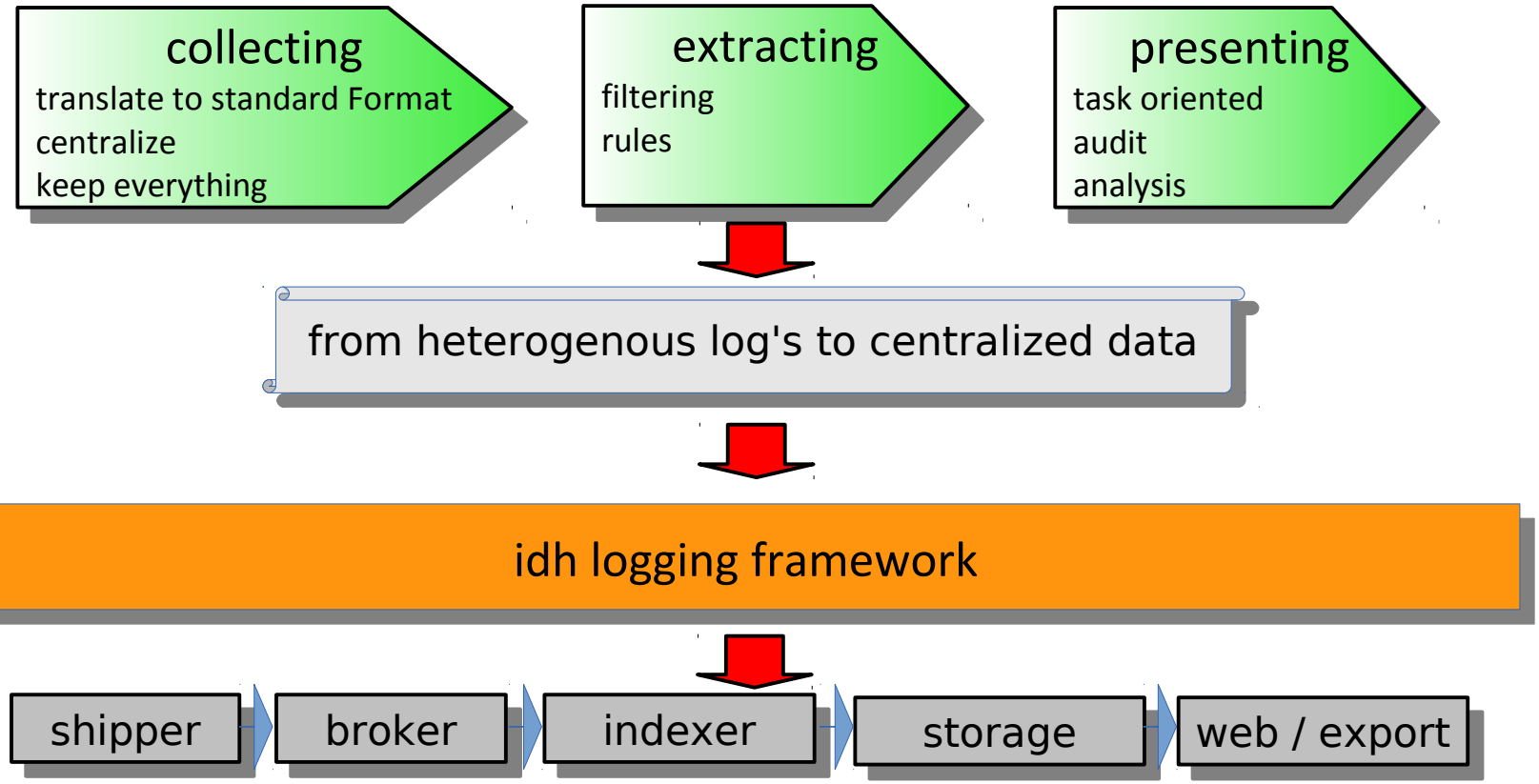
infrastructure analytics

from heterogenous log's to centralized data

Lösung

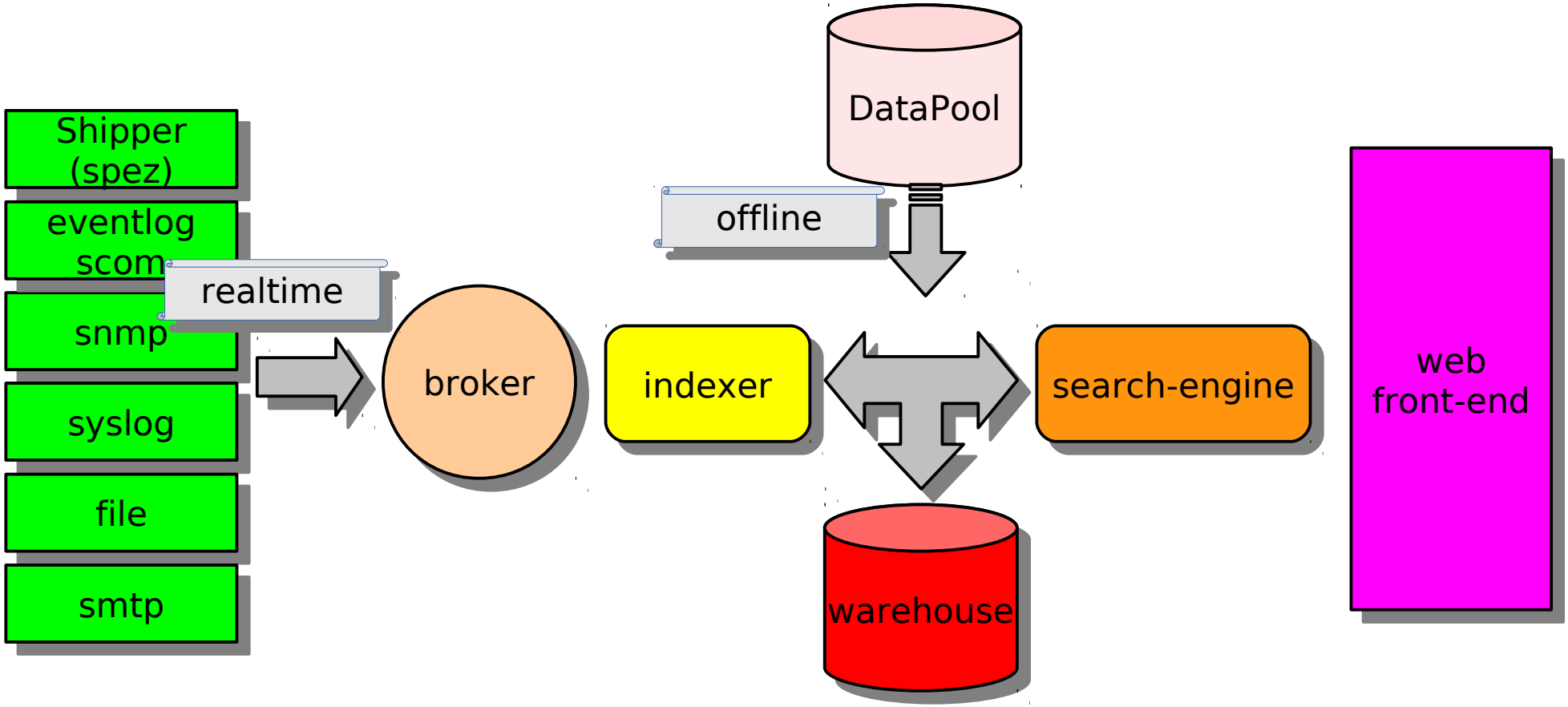

collecting
translate to standard Format
centralize
keep everything
extracting
filtering
rules
presenting
task oriented
audit
analysis
from heterogenous log's to centralized data
idh logging framework
shipper
broker
indexer
storage
web / export

Lösung



Infrastructure Analytics

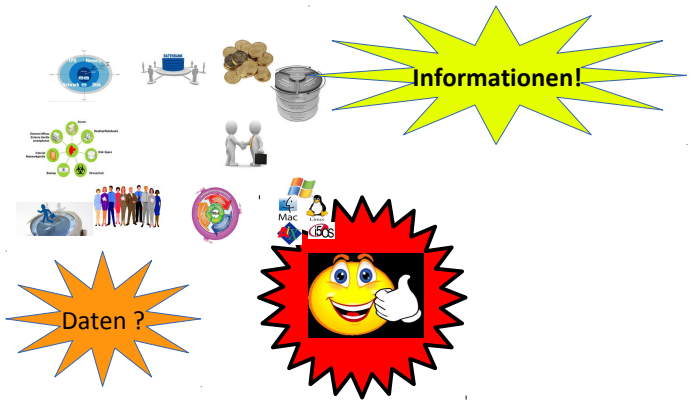
Komponente


DataPool
offline
Shipper (spez)
eventlog
scom
realtime
snmp
syslog
file
smtp
broker
indexer
search-engine
web front-end
warehouse
Reliability / Availability / Scaleability
idh Logging Framework

Eigenschaften

- Höchste Perfomance
  - Indexierung > 1 Mio Indexes/h
  - Cluster aware
- Multi Threading Architektur
  - Multi Threading Architektur
- Offene Architektur
  - Linux
  - UNIX
  - Windows
- Flexibel
  - Verschiedenste Module für die Indexierung
    - CSV / Math / etc
    - Modifikationen
  - Cli Interface
  - Monitoring Anbindung
    - SCOM
    - Nagios
    - Tivoli etc

- Frontend
  - Web Gui
  - Apache Webserver
  - Text Filter
  - CSV Export
  - Graphische Aufbereitung
  - User Authentifizierung
  - Role Based Access möglich

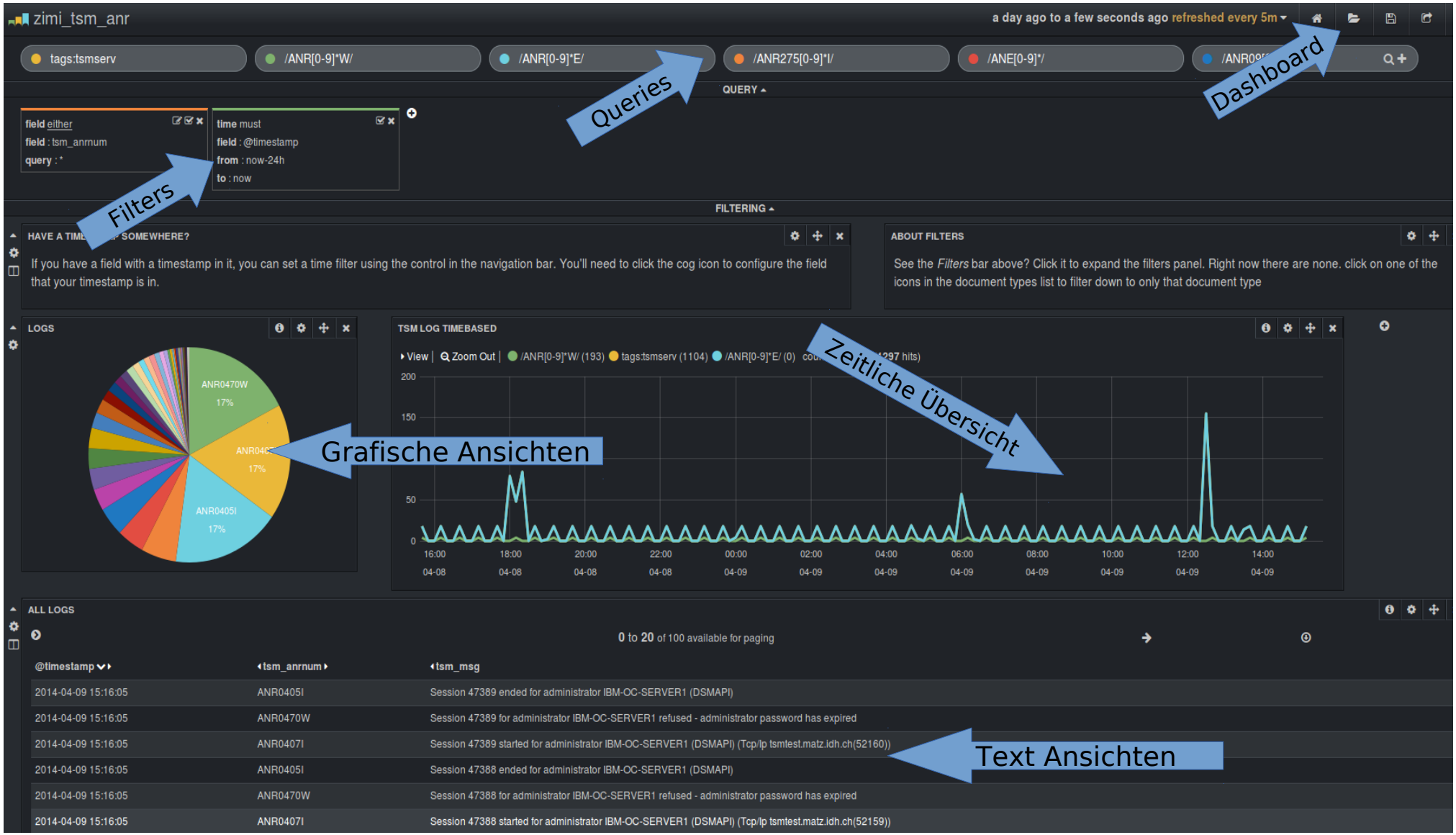


Infrastructure Analytics

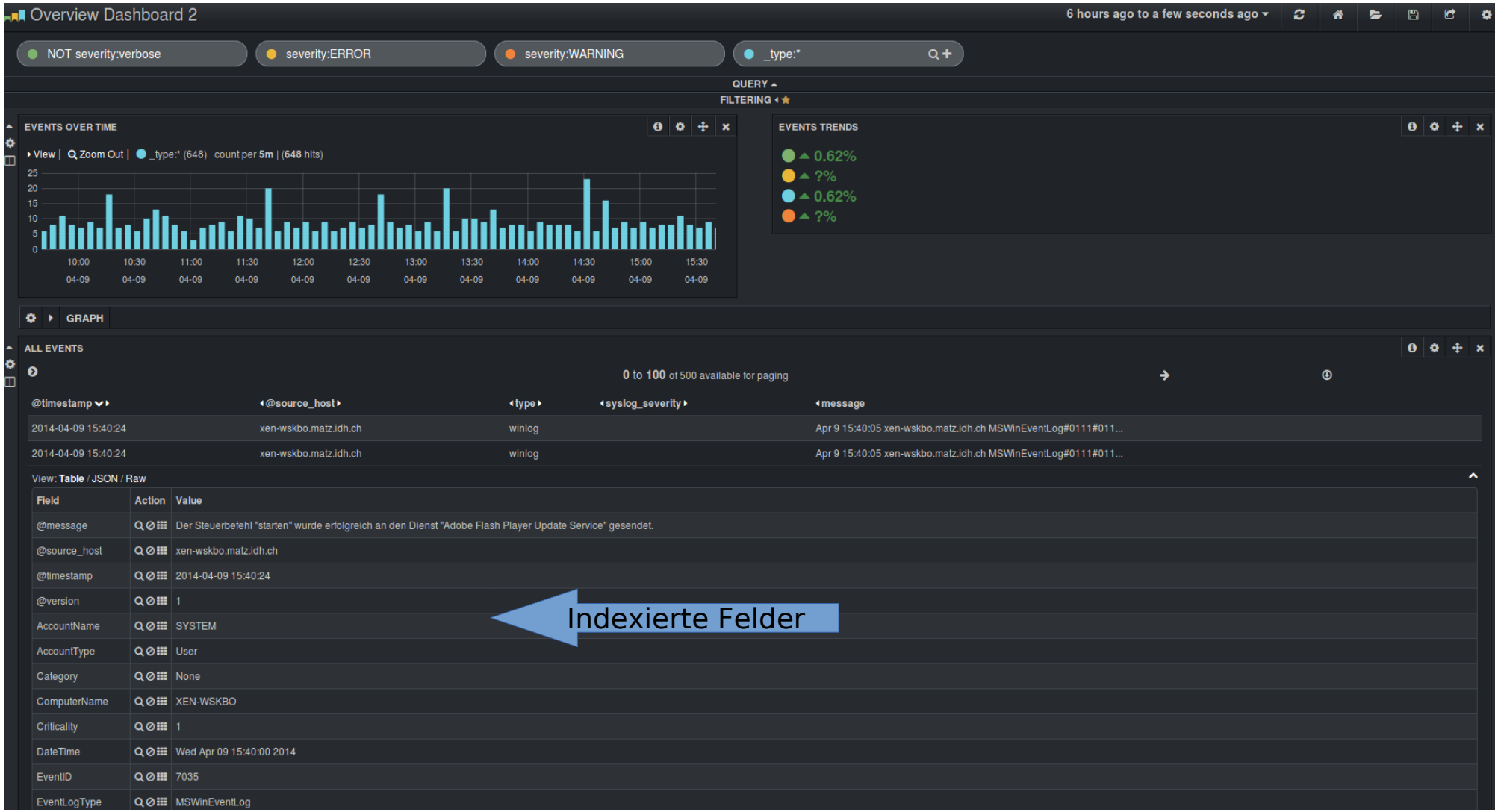
Dashboard


VOIP Overview
a day ago to a few seconds ago refreshed every 5m
type:"asterisk_cdr"
tags:incoming
tags:answered
tags:hangup_at_prompt
tags:outgoing
QUERY
FILTERING
EVENTS OVER TIME
HISTOGRAM
View | Zoom Out | (15) (2) (2) (0) (6) count per 10m | (25 hits)
12.5
10.0
7.5
5.0
2.5
0.0
12:00 01/12
16:00 01/12
20:00 01/12
00:00 01/13
04:00 01/13
08:00 01/13
CALL TYPE
PIE
outgoing (6)
_grokparsefailure (6)
incoming (2)
forwarded_at_prompt (2)
answered (2)
answered
11%
outgoing
33%
incoming
11%
_grokparsefailure
33%
BY NUMBER IN
PIE
0765374195 (1)
0445587134 (1)
0445587134
50%
0765374195
50%
INCOMING CALLS
TABLE
0 to 2 of 2 available for paging
host
asterisk_channel
asterisk_answer
tags
idhvoip
"0765374195" <0765374195>
2014-01-13 07:32:36
_grokparsefailure,incoming,forv
idhvoip
"0445587134" <0445587134>
2014-01-13 08:20:35
_grokparsefailure,incoming,forv
OUTGOING CALLS
TABLE
0 to 6 of 6 available for paging
host
asterisk_channel
asterisk_dst
asterisk_answer
asterisk_billsec
idhvoip
"Remote Roger" <232>
0765374195
2014-01-13 08:28:00
31
idhvoip
"Remote Roger" <232>
0445587134
2014-01-13 08:12:31
43

Dashboard (tsm)

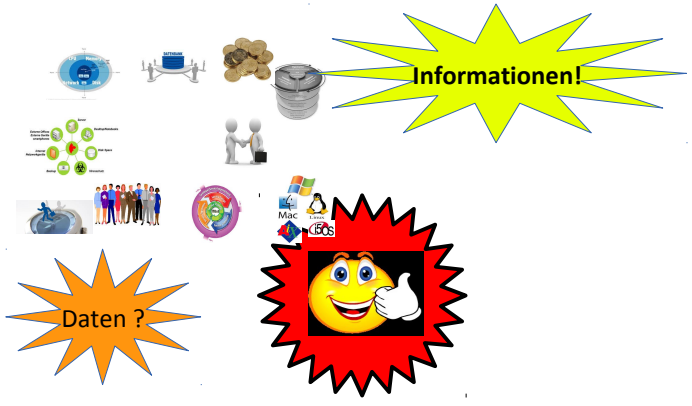


Dashboard (eventlog)



Business Cases

- IT Infrastruktur
  - Überwachen und Optimieren von Hardware Komponenten
- Netzwerk Infrastruktur
  - Zeitnahe Kontrolle, Analyse und Übersicht von Netzwerkverkehr
- Middleware
  - Zeitliche Korrelation von Abläufen
- Technik und Entwicklung
  - Technisch / Mathematische Auswertung von Daten



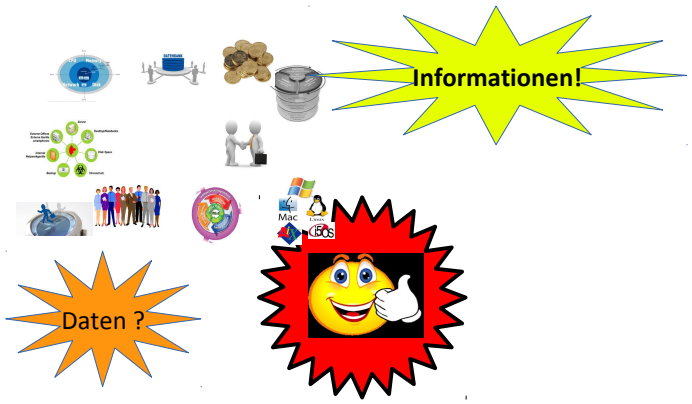
Infrastructure Analytics

Servicemodelle

- Pilot
  - Best practice
  - 3-5 Tage
  - Kosten sFr 4500.--
- Logging as a Service
  - Applikatorisches Sourcing
  - *Kosten / Mt sFr 650.--
- ilf basis
  - Service Abo
  - *Kosten / Mt sFr 680.--
- ilf enhanced
  - Service Abo inkl Engineering Support
  - *Kosten / Mt sFr 1050.--

idh Logging Framework

→ Keine Lizenzkosten
→ Support bei Bedarf
→ Subscription bei Bedarf



Infrastructure Analytics

* unverbindlicher Kostenvorschlag

Fragen ?

Wie komme ich von vorhandenen Daten zu verwertbaren Informationen ?

from heterogenous log's to centralized information

idh Logging Framework

Infrastructure Analytics !

Testen Sie uns !

Wir sind bereit mit ihnen den nächsten Schritt zu gehen