XING
DAS PROFESSIONELLE NETZWERK

Strukturierte Aufbereitung zentraler Logdaten bei XING

SLAC 2013 – Florian Speidel

Inhalt

XING

- Vorstellung
- Anekdote
- Ausgangssituation
- Anforderungen
- Eingesetzte Komponenten
- Das Setup
- Workshop

Vorstellung Unternehmen

XING

XING ist das soziale Netzwerk für berufliche Kontakte

Rund 13 Millionen Mitglieder weltweit nutzen die Plattform für Geschäft, Job und Karriere, davon über 6 Millionen im deutschsprachigen Raum (Stand: Dezember 2012)

Mitglieder tauschen sich online in rund 50.000 Fachgruppen aus und treffen sich persönlich auf XING Events.

Vorstellung Person

XING

Florian Speidel

34 Jahre alt

Senior System Administrator bei XING

Schwerpunkte Email. – Logging Infrastruktur

Anekdote

XING

Ausgangssituation

XING

- 50.000 bis 300.000 Events pro Sekunde
- Suche via grep auf zentralen Logservern
- Zweidimensionales Suchen
- Kein roter Faden
- Unterschiedliche Timestamps
- Viele Scripte und Cron-Jobs

Anforderungen

XING

- Verarbeitung in Echtzeit
- Keine doppelten / verlorenen Daten
- Volltextindizierung + einfache Suchmöglichkeit
- Sammlung von Performancedaten
- Flexibilitaet
- Erweiterbarkeit
- Skalierbarkeit

Eingesetzte Komponenten

XING

syslog-ng

- **Standard Syslog Daemon**
- **Einsammeln aller Logs auf dem Client**
- **Zentraler Logserver**

syslog-ng

Eingesetzte Komponenten

XING

Graylog2

Was ist Graylog2?

- Open Source Log Management

Typische / Unsere Einsatzzwecke

- Zentraler Logserver
- Darstellung von Logdaten
- Analyse von Events
- Auslösen von Aktionen bei Events
- Alarmierung

Eingesetzte Komponenten

XING

Logstash

Was ist Logstash?

- Open Source Log Management

Typische / Unsere Einsatzzwecke

- Datenkonvertierung / Transport
- Datenmanipulation
- Darstellung von Logdaten
- Extrahieren von Metriken
- …

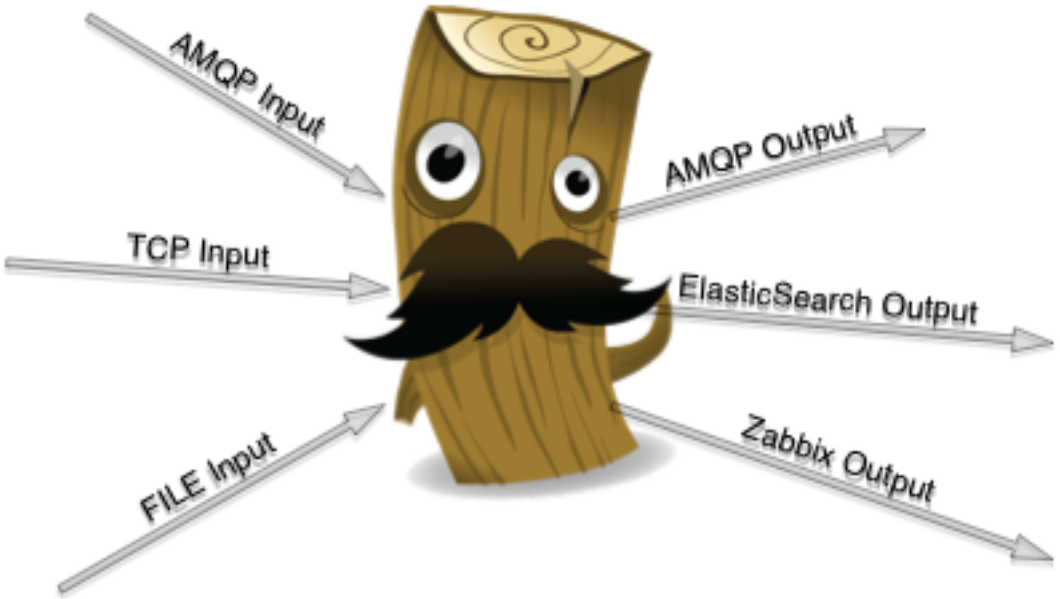
Eingesetzte Komponenten

XING

Logstash

Die Besonderheit

- Konfiguration von Plugins
- Datenkonvertierung



Konfiguration

- Input {…}
- Filter {…} (optional)
- Output {…}

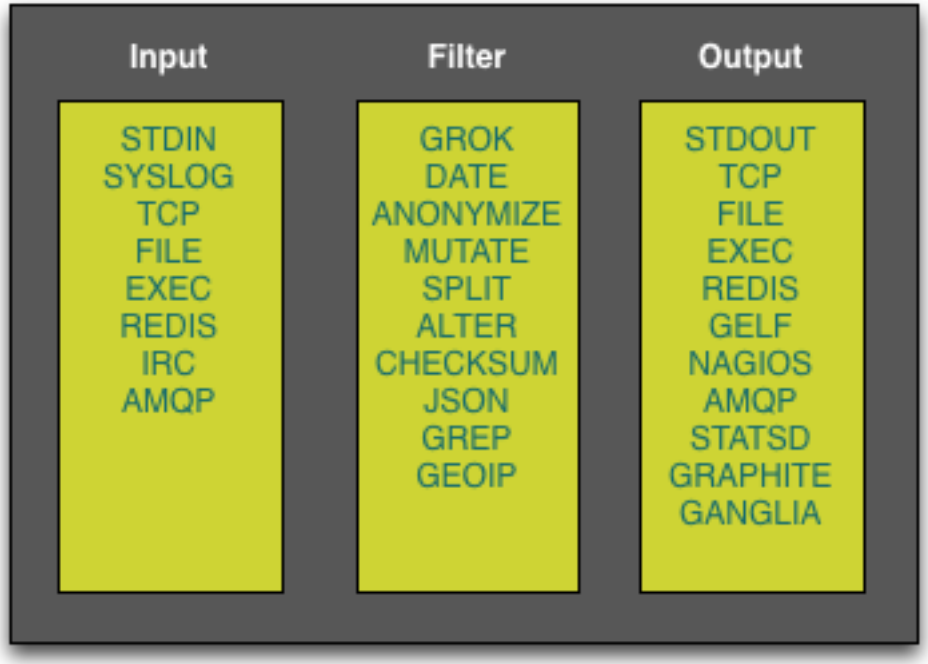
Eingesetzte Komponenten

XING

Logstash

Plugins

- 43 Input Plugins
- 35 Filter Plugins
- 51 Output Plugins



Eingesetzte Komponenten

XING

syslog-ng

Soviele Überschneidungen?

Eingesetzte Komponenten

XING

syslog-ng

Jede Komponente hat seine Vorteile

- **Syslog-ng -> Client und Rohdatenspeicher**
- **Graylog2 -> Visualisierung und Analyse**
- **Logstash -> Datenmanipulation / Transport**

Eingesetzte Komponenten

XING

Redis

- Persistenter Cache zwischen Logstash-Instanzen

Elasticsearch

- Storage-Backend für Graylog2
- Basis zur Entwicklung spezialisierter Tools

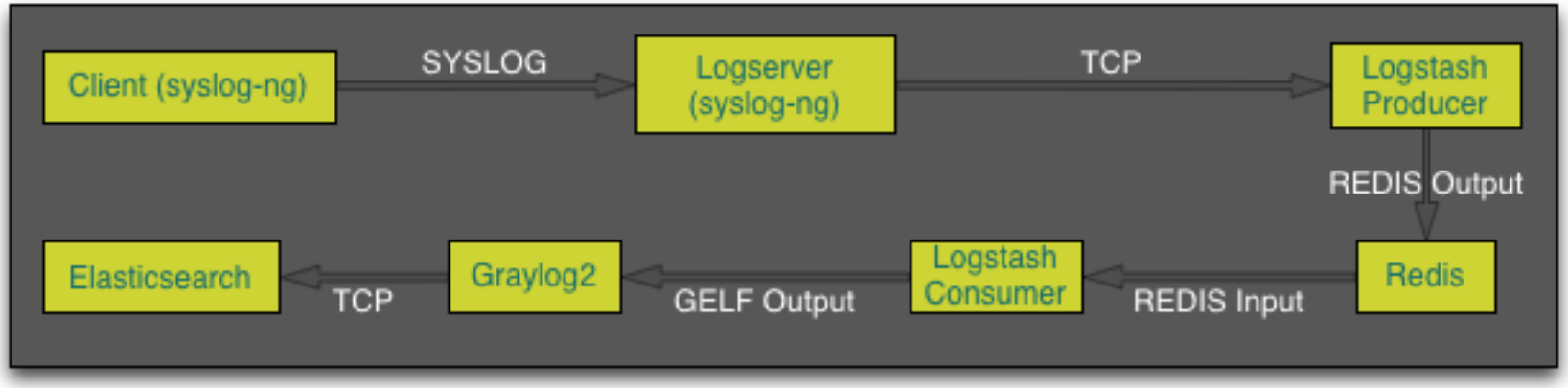
StatsD / Graphite

- Visualisierung von Metriken

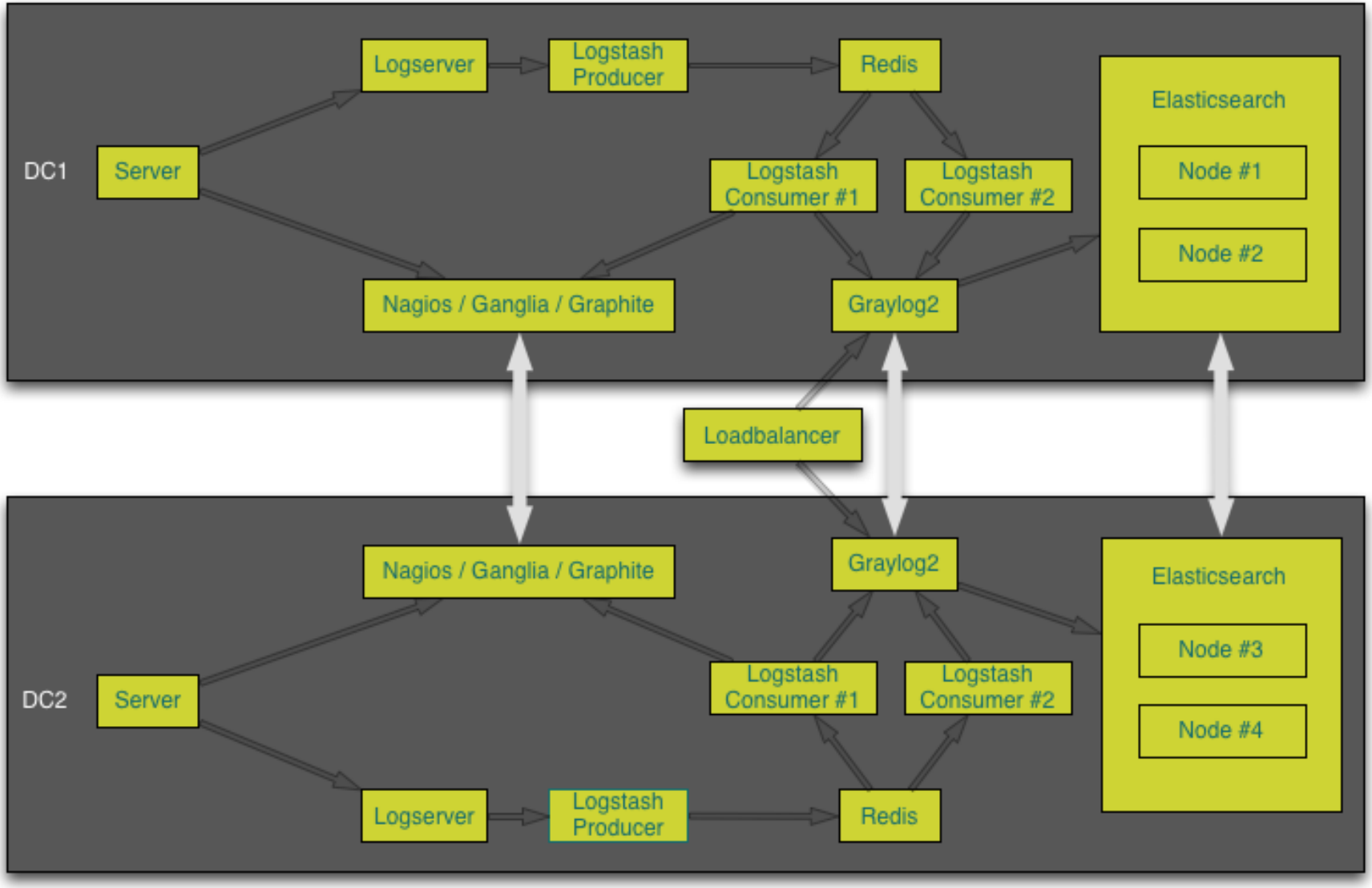
Nagios

- Aktive und eventbasierte Alarmierung

Das Setup


Client (syslog-ng)
SYSLOG
Logserver (syslog-ng)
TCP
Logstash Producer
REDIS Output
Redis
REDIS Input
Logstash Consumer
GELF Output
Graylog2
TCP
Elasticsearch

Das Setup


DC1
Server
Logserver
Logstash Producer
Redis
Logstash Consumer #1
Logstash Consumer #2
Elasticsearch
Node #1
Node #2
Nagios / Ganglia / Graphite
Graylog2
Loadbalancer
DC2
Server
Nagios / Ganglia / Graphite
Graylog2
Elasticsearch
Node #3
Node #4
Logstash Consumer #1
Logstash Consumer #2
Logserver
Logstash Producer
Redis

Workshop

XING

103.135.172.160 - - [28/May/2013:12:19:19 +0200] "GET /app/newsfeed?op=activitystream&want_html=1&_=1369736356281 HTTP/1.1" 200 3646 "https://www.xing.com/" "Mozilla/5.0 (Windows NT 6.1; rv:21.0) Gecko/20100101 Firefox/21.0"

Workshop

XING

utime:1369699271,sender:postmaster@xing.com,recipient:florian.speidel@xing.com,
returnpath:<postmaster@xing.com>,recipient_id:,content:,click_tracking:,message_id:
BD/51-03663-6C3F3A15,size:158949,injector:datacenter,binding:mailout1-104,
bindinggroup:mailout1,queuetime:0.031070,remote_ip:10.4.39.2,delivery_attempts:
0,esc:250 2.0.0 Ok: queued as EFE9E100B78D

Das Ergebnis

Syslog Dashboard in Graphite (Gesammelte Metriken)

Das Ergebnis

Eigenentwicklung zur Anzeige von Emaildaten

MailDB Custom log Reject log Help

sender:mailrobot@xing.com Field Go!

Date	Sender	Recipient	Recipient-UID	Message-ID	Injector	Content	Binding	Remote-IP	Status	Attempts	DSN Code / Enhanced Status Code
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-102	213.165.67.97	delivered	0	250 Requested mail action okay, completed: id=
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	contactadd_notify	mailout2-107	212.227.15.134	delivered	0	250 Message accepted by mxeu3.kundenserver.de
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	contactadd_notify	mailout2-106	194.25.134.72	delivered	0	250 2.0.0 Message accepted.
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	message_notify	mailout2-102	68.232.135.99	delivered	0	250 ok: Message accepted
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-119	212.227.17.175	delivered	0	250 Message accepted by mxbap0.kundenserver.de
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-108	65.54.188.72	delivered	0	250 Queued mail for delivery
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-119	213.165.67.115	delivered	0	250 Requested mail action okay, completed: id=
2013-05-28 10:05:13	mailrobot@xing.com				datacenter	message_notify	mailout2-107	62.209.51.136	delivered	0	250 2.0.0 Message accepted for delivery
2013-05-28 10:05:12	mailrobot@xing.com				datacenter	contactadd_notify	mailout2-116	160.83.90.10	delivered	0	250 2.0.0 Message accepted for delivery
2013-05-28 10:05:12	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-110	217.111.120.1	delivered	0	250 2.0.0 Message accepted for delivery
2013-05-28 10:05:12	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-116	195.47.247.192	delivered	0	250 2.0.0 Ok: queued as
2013-05-28	mailrobot@xing.com				datacenter	notification_newarticles	mailout2-	213.165.67.99	delivered	0	250 Requested mail action okay, completed: id=

XING

Fragen?

Das professionelle Netzwerk
www.xing.com

Vielen Dank für die Aufmerksamkeit!

Das professionelle Netzwerk
www.xing.com