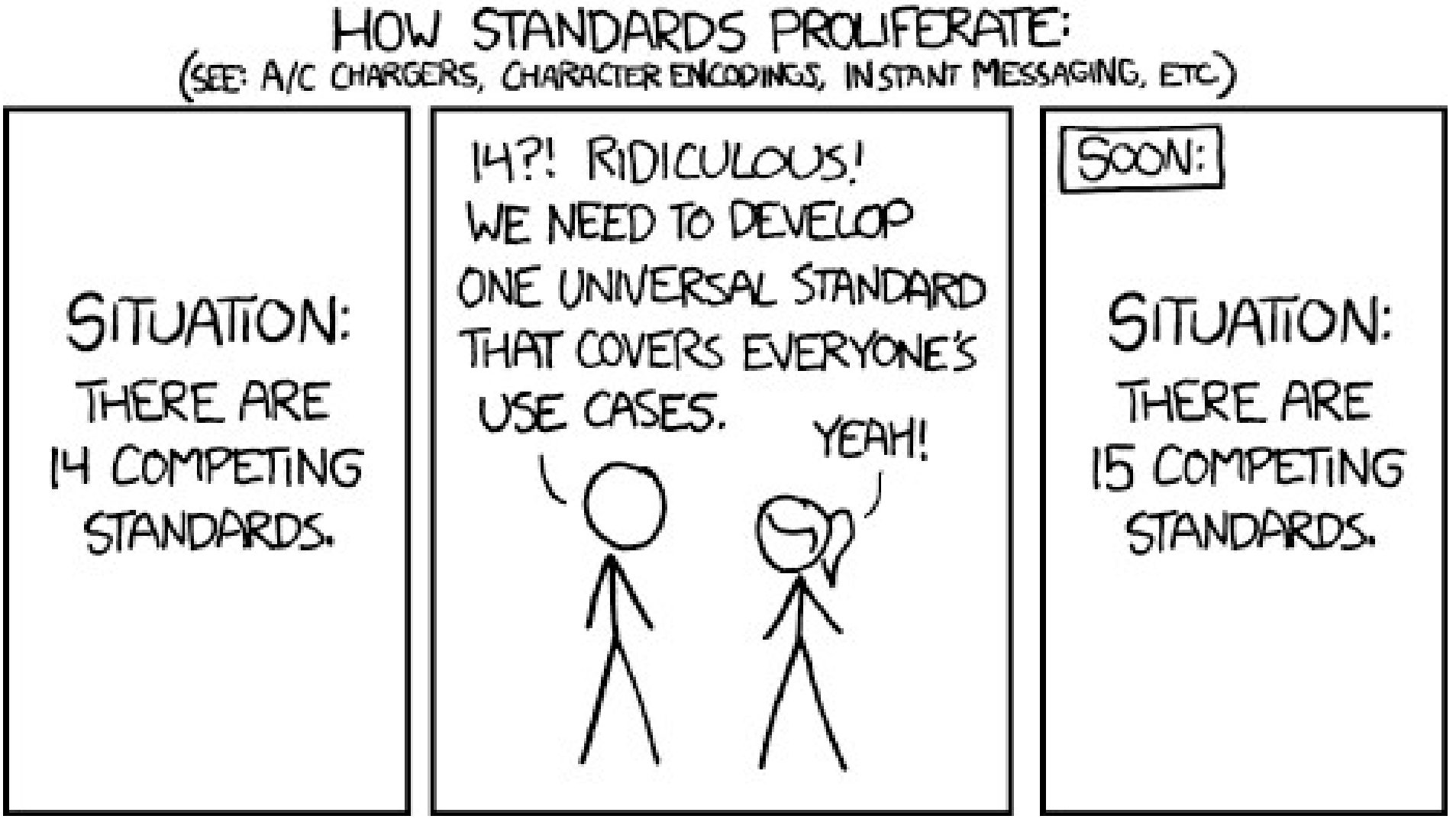
Zentrales strukturiertes Logging

oder wie kann ich 1000 Server überwachen

von
Jens Kühnel

syslog vs. strukturiertes Logging

Formate


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Formate

syslog BSD und IETF

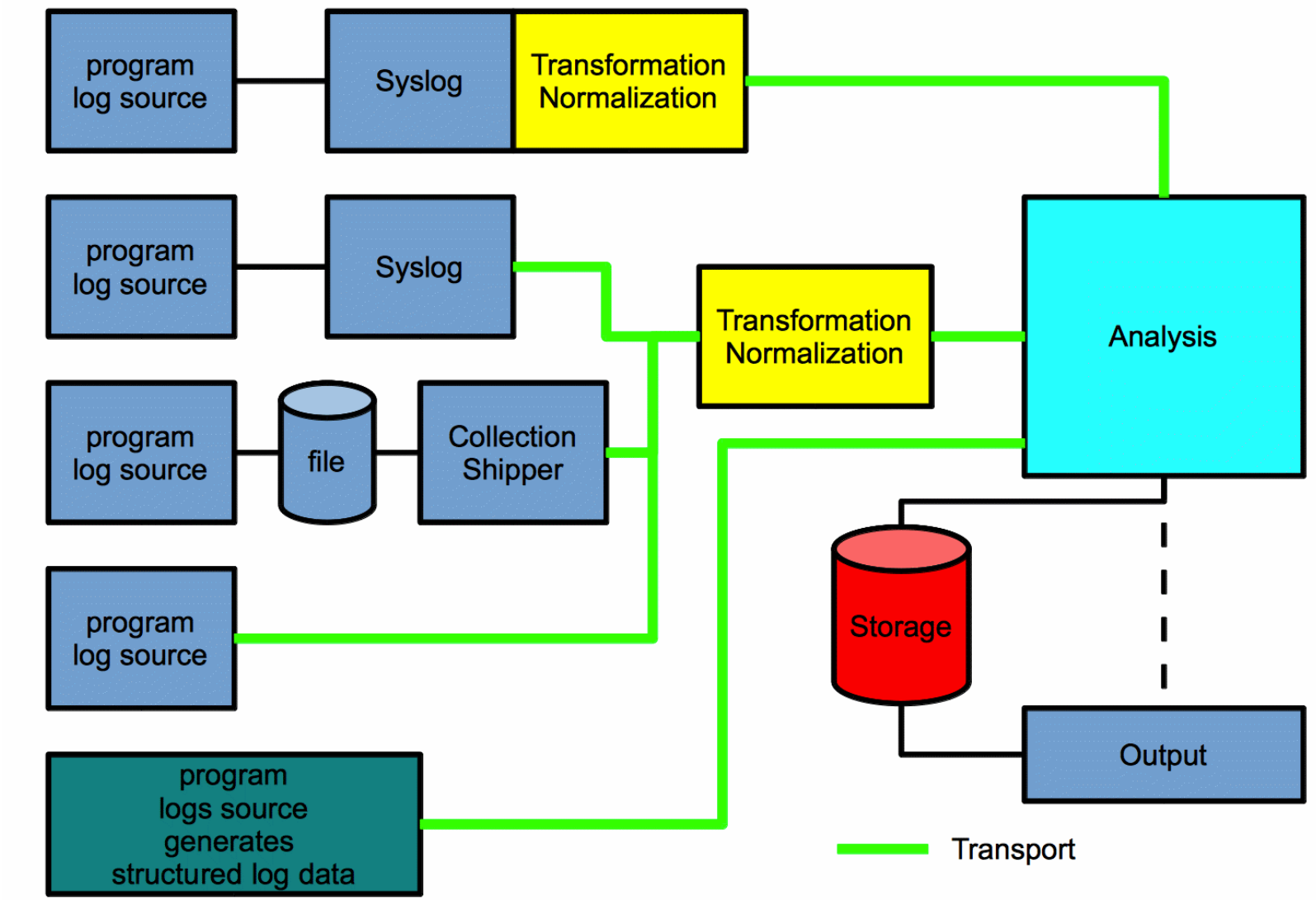
CEE / Project Lumberjack

JSON

- GELF
- logstash

systemd Journal

Ways of the log message



Transport

syslog (RELP)

redis

AMQP/STOMP (ActiveMQ/RabbitMQ)

0mq

Lumberjack

Storage

MySQL

Elasticsearch

(MongoDB)

Shipper

syslog-ng

rsyslog

fluentd

logstash

Logstash-forwarder (Lumberjack)

nxlog

Analyse und Normalisieren

syslog-ng

rsyslog

logstash

octopussy

nxlog

Output

Kibana 2+3

Graylog2

ELSA

octopussy

Überblick 1

ELSA

Speed is king

Struktur kommt doch eh nicht

Du brauchst Google!

graylog2

wir wollen Struktur

aber bis dahin muss es auch laufen

logstash

Schweizer Taschenmesser

mit Kibana echt cool

octopussy

alles muss Struktur habe, aber Logdateien sind cool!

fluentd

Wir bringen es zu dir, egal was es ist

und verpacken es dir auch noch hübsch

nxlog

Wir bringen es zu dir

aber wenn du mehr willst kauf mich.

Überblick 2

syslog-ng

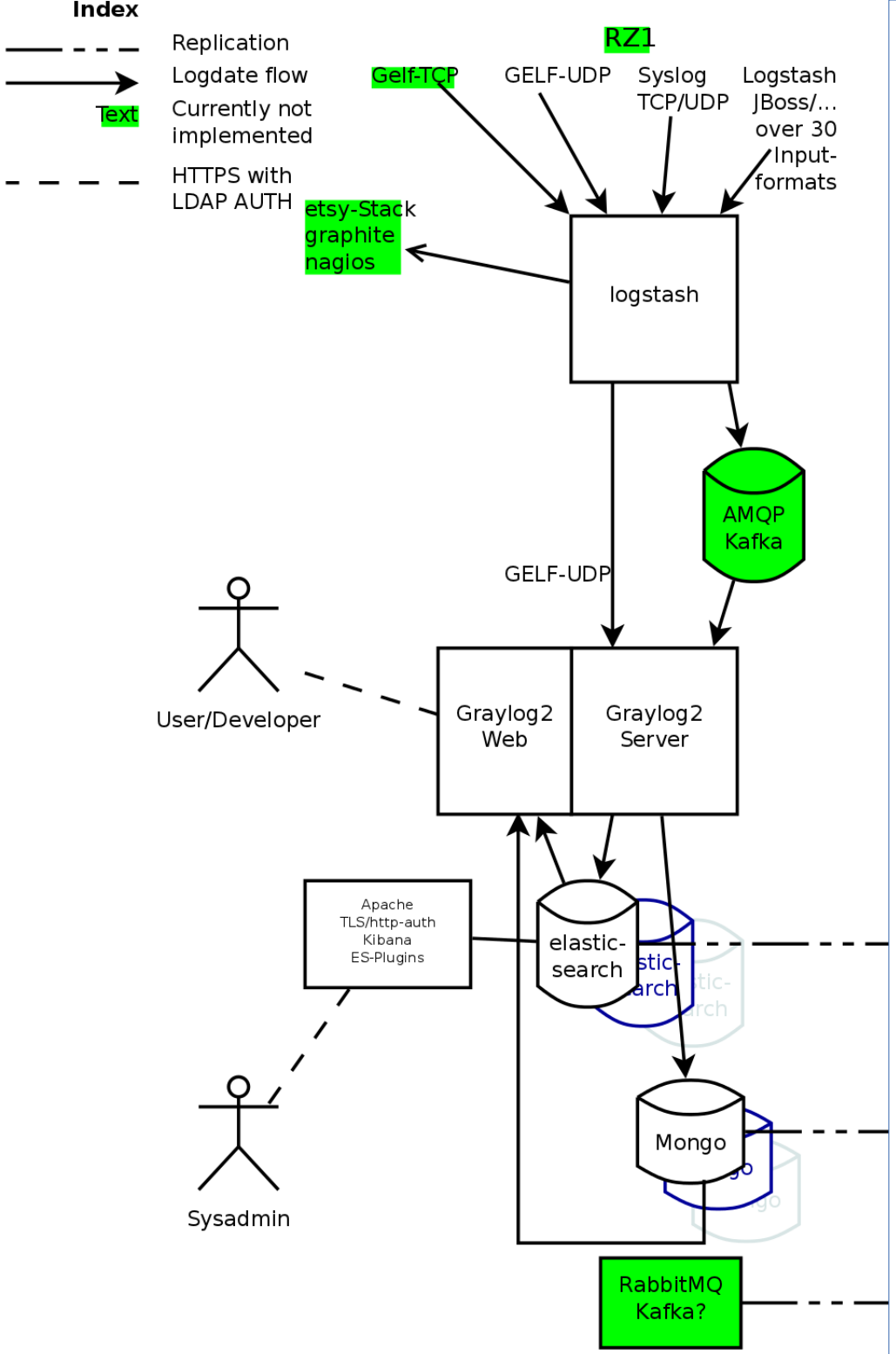
Wir machen alles

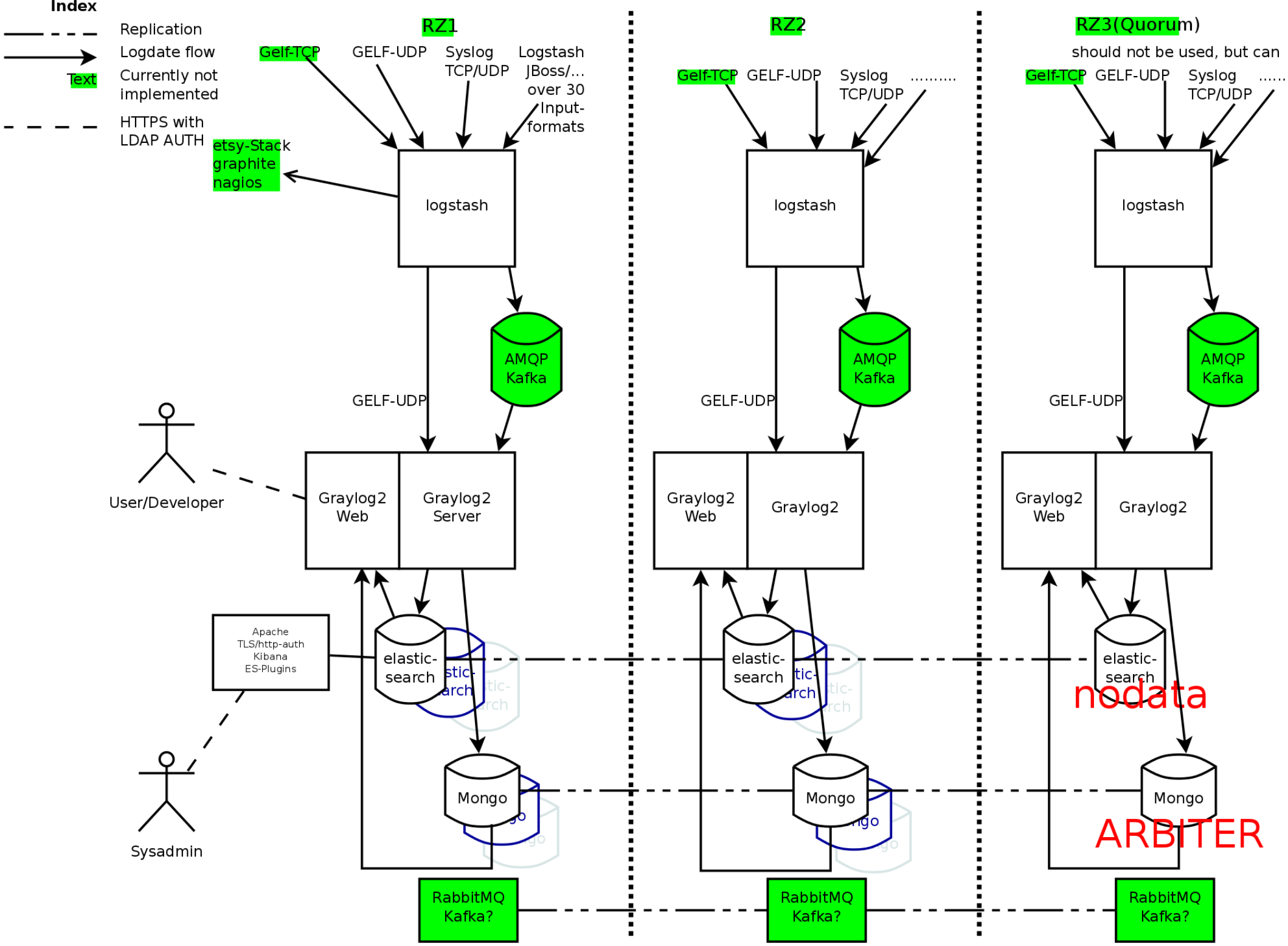
Aber wenn du deine Logdateien sicher brauchst, musst du zahlen

rsyslog

Wir machen auch alles

Wir sind wirklich Open Source, auch caching


Index
Replication
Logdate flow
Text
Currently not implemented
HTTPS with LDAP AUTH
RZ1
Gelf-TCP
GELF-UDP
Syslog TCP/UDP
Logstash JBoss/... over 30 Input-formats
etsy-Stack
graphite
nagios
logstash
AMQP
Kafka
GELF-UDP
User/Developer
Graylog2 Web
Graylog2 Server
Apache
TLS/http-auth
Kibana
ES-Plugins
elastic-search
Mongo
Sysadmin
RabbitMQ
Kafka?


Index
Replication
Logdate flow
Text
Currently not implemented
HTTPS with LDAP AUTH
RZ1
RZ2
RZ3(Quorum)
should not be used, but can
Gelf-TCP
GELF-UDP
Syslog TCP/UDP
Logstash JBoss/... over 30 Input-formats
.....
etsy-Stack
graphite
nagios
logstash
AMQP
Kafka
GELF-UDP
User/Developer
Graylog2 Web
Graylog2 Server
Graylog2
Apache
TLS/http-auth
Kibana
ES-Plugins
elastic-search
Mongo
Sysadmin
RabbitMQ
Kafka?
nodata
ARBITER

Bachelorarbeit

Verfügbar unter

http://it-hure.de/

Update Mai/Juni 2014