I Love Logging

Structured Logging with
Free/OpenSource Tools

Jens Kühnel

About Jens Kühnel

Freelancing Trainer, System Administrator, Consultant and Author since 2000

Bachelor of Science in Computer Science

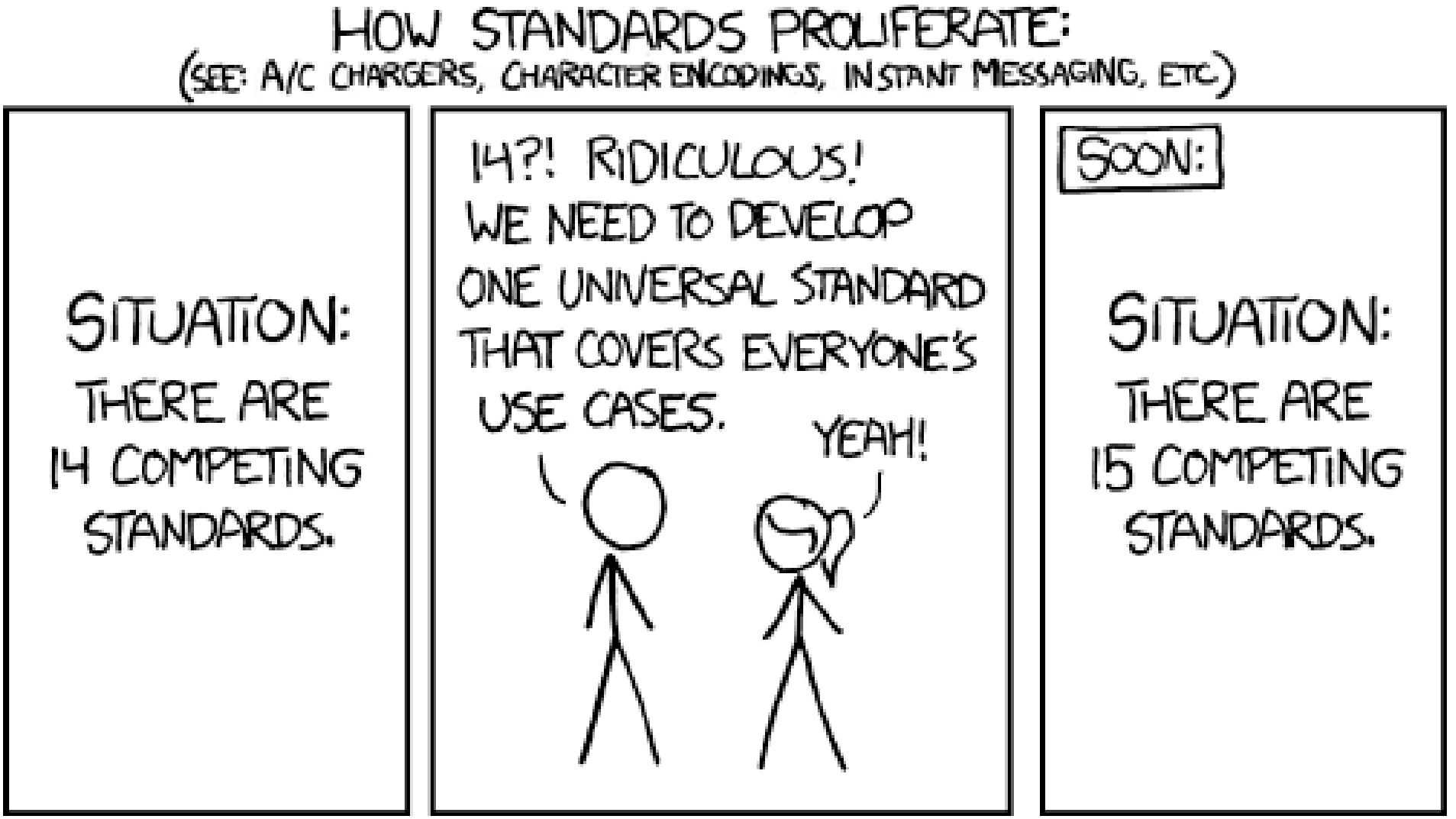
This is based on my thesis

I Love Logging

Informal Mailinglist of people interested in OpenSource Logging using different tools.

syslog vs. structured Logging

Formats



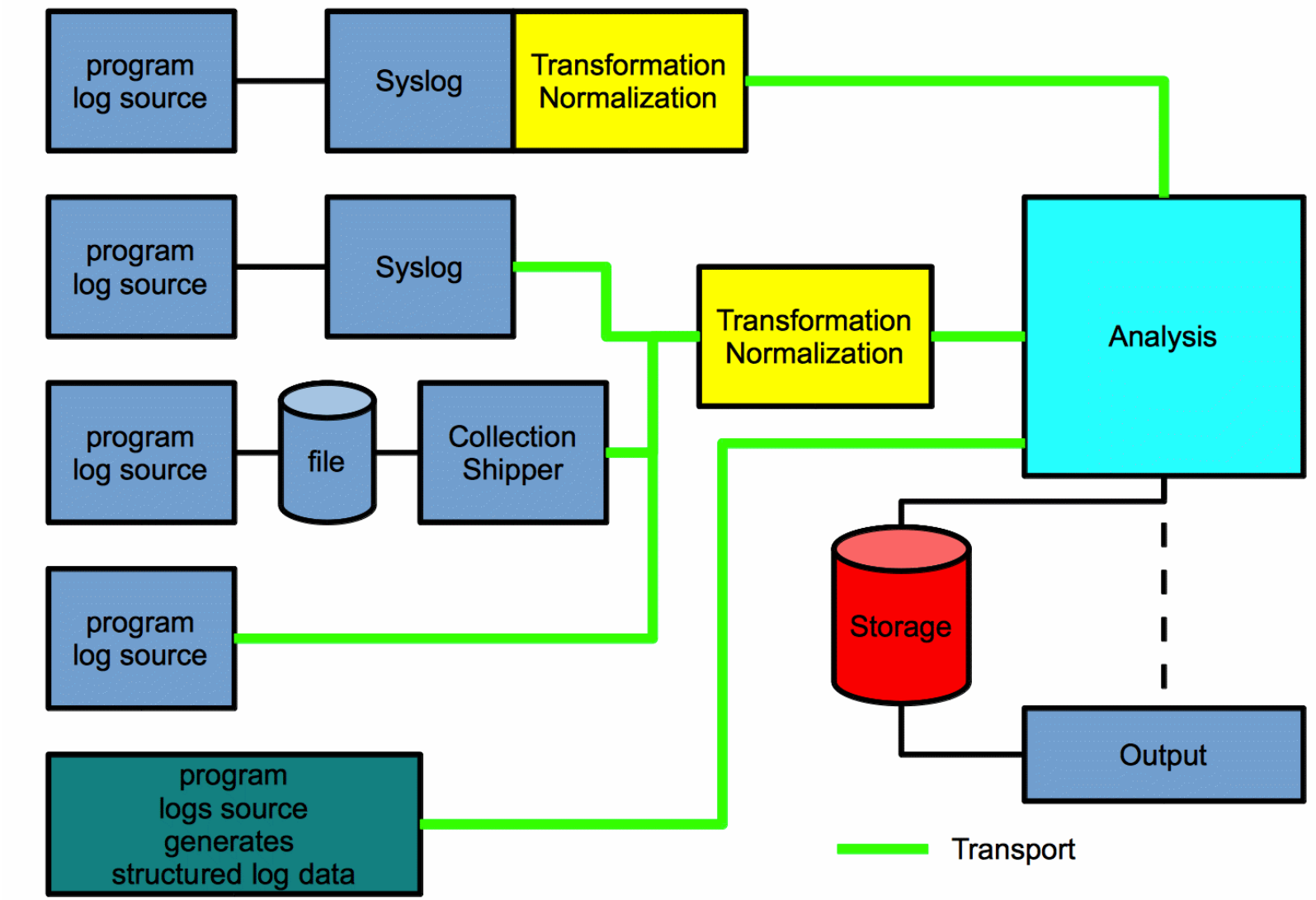
Source: http://xkcd.com/927/

Formats

- syslog BSD and IETF

- JSON
  - CEE / Project Lumberjack
  - GELF
  - logstash
  - systemd Journal
  - Nested vs. Flat

Ways of the log message



Transport

syslog IETF/BSD TCP/UDP/(RELP)

redis

AMQP/STOMP (ActiveMQ/RabbitMQ)

0mq

logstash-forwarder (Lumberjack)

Storage

Elasticsearch

(mongo)

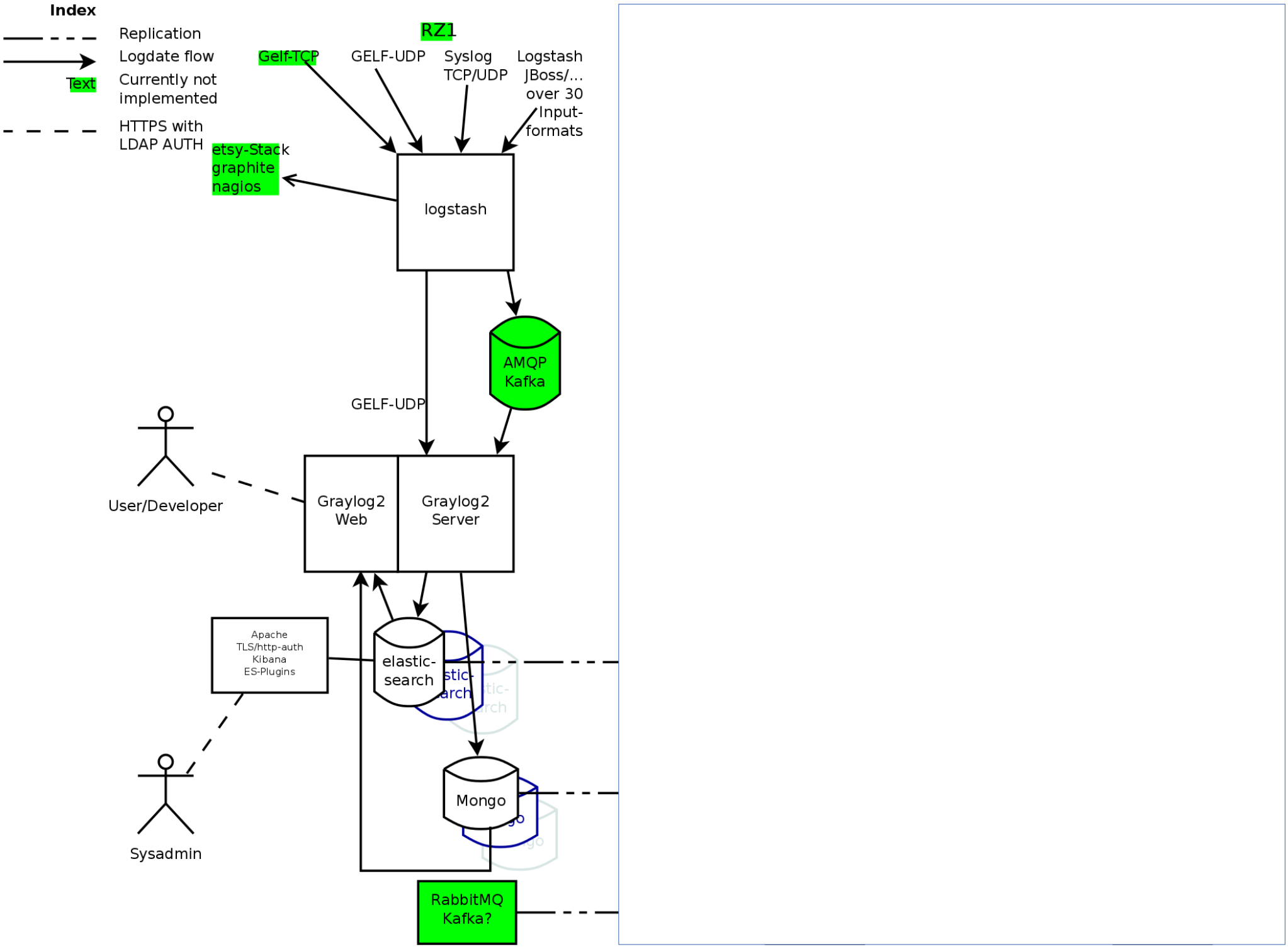
Major Tools

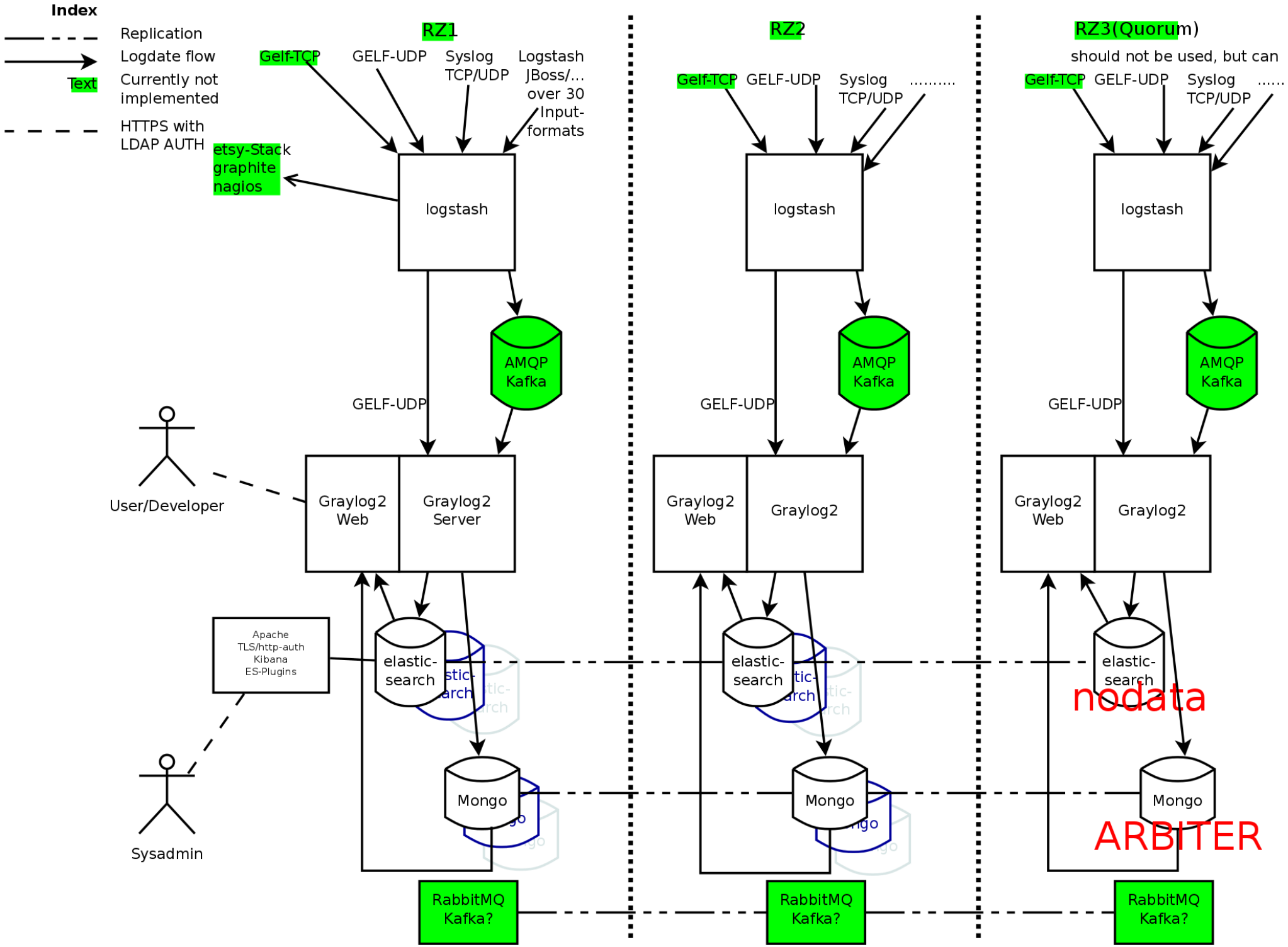
- Rsyslog TSN
- Syslog-ng TSN
- Graylog2 NO
- Logstash TSN
- Kibana O

T=Transport, S=Shipper, N=Normalization, O=Output

My search for a logging solution

- Requirements
  - User separation
  - Interactive search
  - Automatic normalization
  - Widespread use
- Used Tools at the Moment:
  - Graylog2
  - (Logstash)
  - rsyslog
  - ....


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

I Love logging

Join the logging fun :-)
http://Ilovelogging.org/

My bachelor thesis will be available there soon.