Logmonitoring with ELK and Icinga 2

2016-02-16 | Icinga Camp San Francisco

Thomas Widhalm | NETWAYS GmbH

About me

- Thomas Widhalm
  - Senior Consultant
  - @NETWAYS since 2013
  - "Elk Head" - ELK trainings, consulting, workshops
  - Icinga (2) - consulting, trainings, author

1 Introducing: ELK Stack

ELK Stack

+

+

=

Consists of:

- Elasticsearch
- Logstash
- Kibana

ELK Stack

Does:

- Forward log events from various sources to various targets
- Collects log events in a centralised storage
- Parses and enriches logs
- Provide search interface for log events
- Create graphs from logged information
- A lot more
- All this with all sorts of events not just logs

Elasticsearch

- Stores Events
- Is elastic
- HA / LB Cluster
- Robust

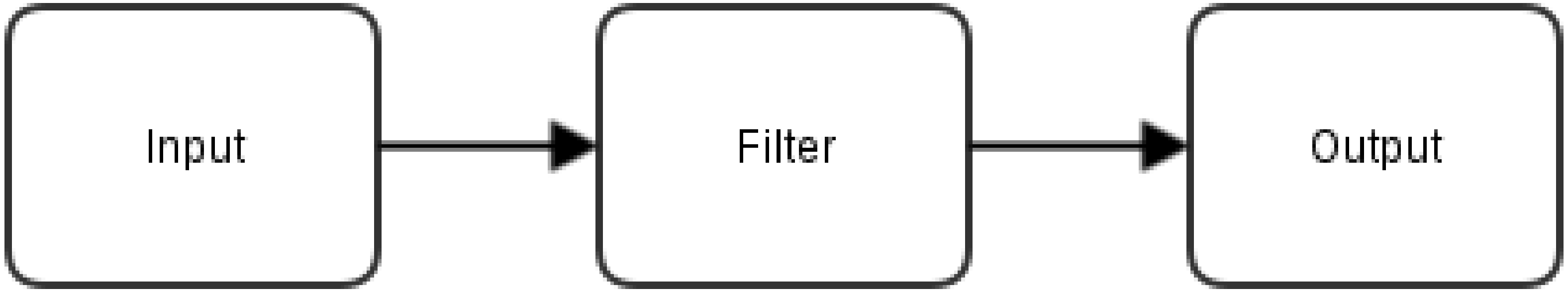
Elasticsearch

- NoSQL Search Server based on Apache Lucene
- RESTful Interface
- Easy to set up
- Redundant per default

Logstash

- Moves Events from sources to targets
- Parses and splits events into fields
- Enriches and transforms events
- Drops unwanted events

HA/ELK ELK Stack



Logstash

Transport

- Many sources
  - **Syslog**
  - Windows Eventlog
  - Log4j
  - Generic (`tcp`/`udp` Port, `exec`)
  - E-Mail
  - Jabber
  - JDBC
  - Twitter
  - Lots more

Logstash

Transport

- Many targets
    - Elasticsearch
    - **Icinga (2)**
    - Graphite
    - E-Mail
    - Jabber
    - IRC
    - JIRA
    - Lots more

Logstash

Parsing and splitting

- By Regex
- By included Regex Pattern (`SYSLOGLINE`, `IPV6`,…)
- Key-Value
- CSV
- http Useragent
- Syslog Priority
- Lots more

Logstash

Before:

```
192.168.1.10 – guest [04/Dec/2013:08:54:23 +0100] "POST /icinga-web/web/api/
jsonHTTP/1.1" 200 788 "https://icinga-private.demo.netways.de/icinga-web/
modules/web/portal" "Mozilla/5.0 (X11; Linux x86_64; rv:22.0)"
```

After:

```
"http_clientip"    : "192.168.1.10",
"http_ident"       : "-",
"http_auth"        : "guest",
"timestamp"        : "04/Dec/2013:08:54:23 +0100",
"http_verb"        : "POST",
"http_request"     : "/icinga-web/web/api/json",
"http_httpversion" : "1.1",
"http_response"    : "200",
"http_bytes"       : "788",
"http_referrer"    : "https://icinga-private.demo.netways.de/icinga-web/...",
"http_agent"       : "Mozilla/5.0 (X11; Linux x86_64; rv:22.0)"
```

Logstash

Enrich and transform

- Transform timestamps
- DNS resolution
- GeoIP resolution
- Anonymize or encrypt
- sflow / netflow
- Lots more

Logstash

Custom Plugins

- Plugins written in (j)Ruby
- It's easy to build your own (if you know Ruby)
- Contributions are welcome

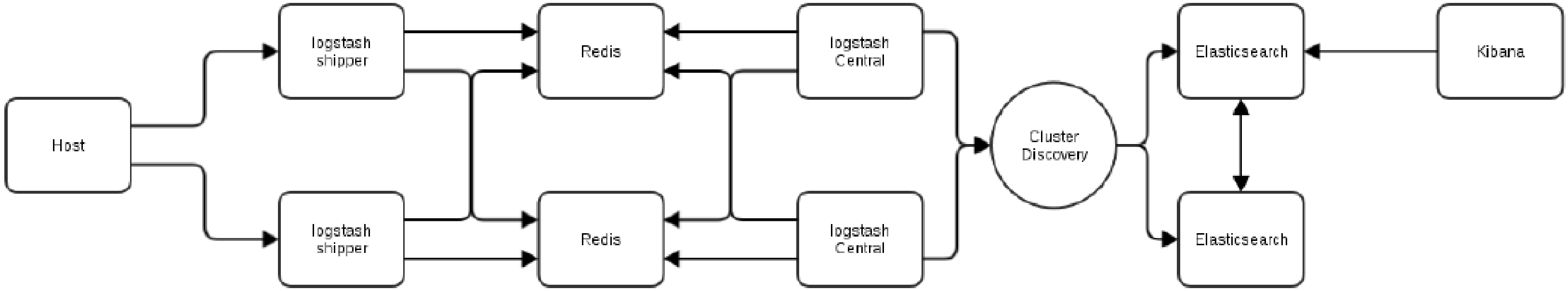
Kibana

- Webinterface for Queries and Graphs
- Interactive searches
- Dashboards with visualizations / graphs
- Interactive filters for queries and dashboards

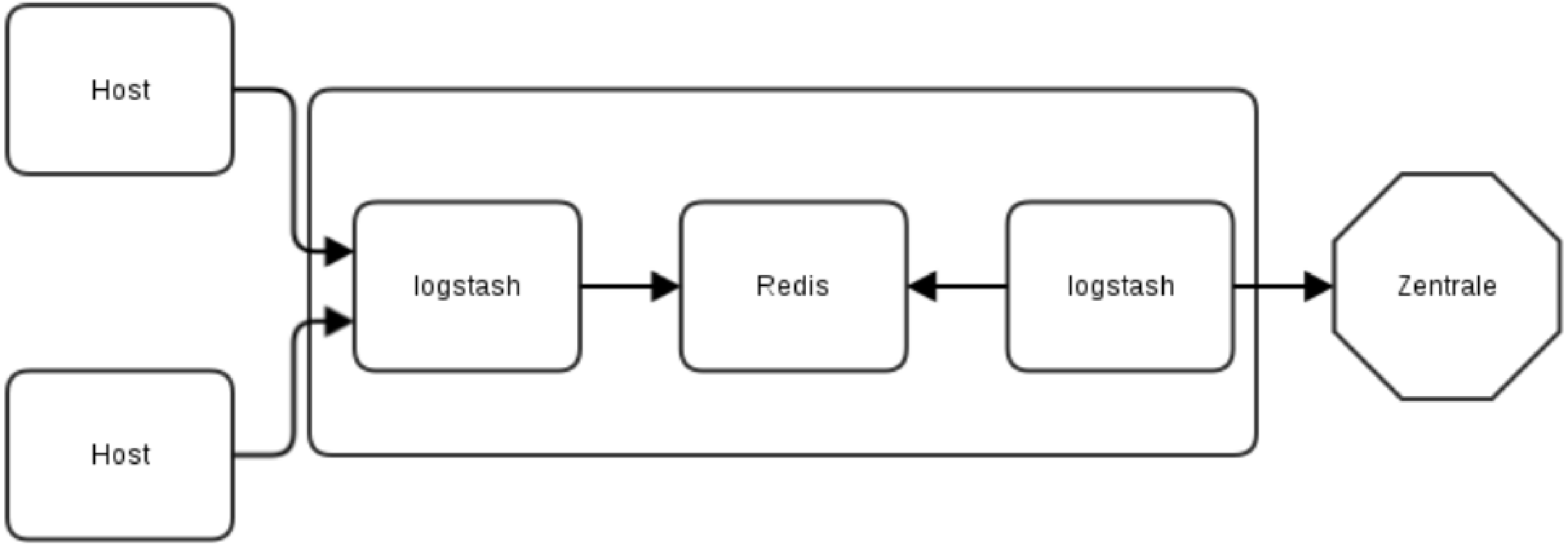
Kibana

- Query with Lucene Query Syntax
- Graphs from field values
  - Uses filters and aggregations within Elasticsearch ->
  - Scales with Elasticsearch

HA/ELK ELK Stack



Remote Shipper



2 Why Logmonitoring?

Why

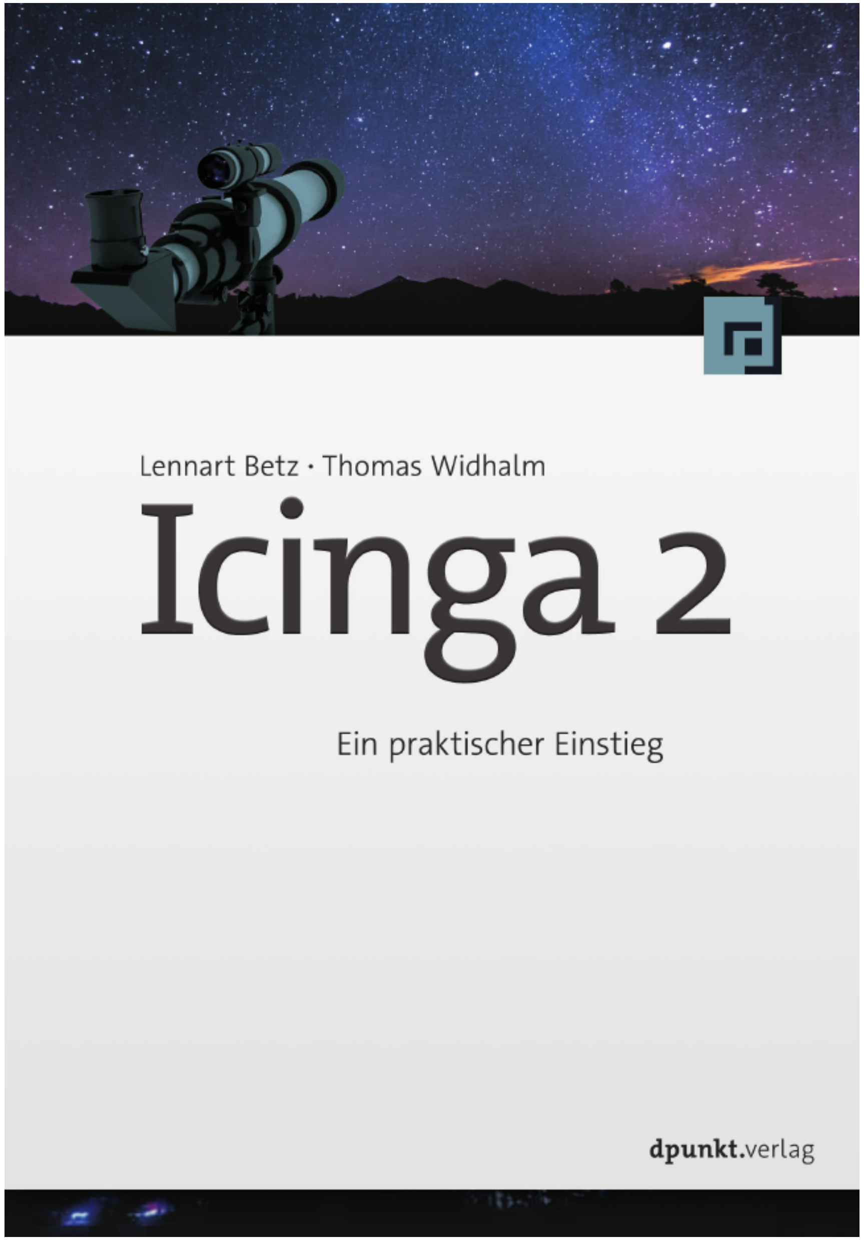
- Not all information is available for active monitoring
- Catch-all approach

Why Icinga 2

- Open Source / Free Software
- Very modular and ready to be enhanced with 3rd party tools
- Proven solution for alerting
- One more reason ->

Icinga 2

Gives you all a reason to learn German.



Lennart Betz · Thomas Widhalm

Icinga 2

Ein praktischer Einstieg

dpunkt.verlag

Why ELK

- "Logstash" is too long a word on the slides - writing "ELK" is more economic
- Logstash is great at forwarding messages from different sources
- Logstash can parse messages
- Elasticsearch and Kibana can be used for validating rules

3 Connecting ELK to Icinga

Icinga

Problems of every Logmonitoring

Not ELK specific

- Lots of different log formats
- Not every message occurs regularly
- Missing information
- Barely any "OK" messages
- Writing lots of rules

Solution to missing "OK" events

Solution A: Automatic recovery after some time

Solution B: List all events which qualify as alert and acknowledge each and every one

Icinga

A: Automatic OK

- Logstash `n-word` Output to Icinga
- Set to OK with `check_dummy`
- Alerts are sent a very short time after the logevent
- Send alerts after n logevents which match a filter or send an alert on every match

Icinga

B: list all events and tick them off

- Currently only prototype
- Integration in Icinga Web 2
- Queries Elasticsearch
- Acknowledges Events in Elasticsearch
- Takes more time to send alert but gives better overview over events
- Service is not OK before someone acknowledges the event

Icinga

What you need

- Match Events to Host and Service
  - Available in event text
  - Transforming event information (e.g. DNS resolution)
  - Metahost / Metaservice

- Decide wether an event should trigger an alert
  - By Severity of message
  - By regex matching on event text

Contact

NETWAYS GmbH
Deutschherrnstrasse 15-19, 90429 Nürnberg
Tel: +49 911 92885-0
Fax: +49 911 92885-77
Email: info@netways.de
Website: www.netways.de
Twitter: twitter.com/netways
Facebook: facebook.com/netways
Blog: blog.netways.de

Contakt

Thomas Widhalm
Email: thomas.widhalm@netways.de
Twitter: @widhalmt
GnuPG: 6265BAE6 / A84CB603
Threema: H7AV7D33 / Telegram: widhalmt
Jabber: widhalmt@widhalm.or.at

THANK YOU