ELK – Stack
Elasticsearch, Logstash, Kibana
INTRODUCTION
Bernd Erk

- CEO at NETWAYS GmbH
- Co-Founder Icinga
- @gethash
- info@netways.de
NETWAYS GmbH

- Open Source Service Provider
- Located in Nuremberg
- About 45 employees right now

- Technical areas
  - Open Source Systems Management
  - Open Source Datacenter
- Custom Open Source solutions
We love Open Source

NETWAYS Products

- Icinga
- Puppet
- Foreman
- OpenNebula
- Bareos
- Tibco Jaspersoft
- Redmine
- Logstash
- Ceph
INTRODUCTION LOGS & EVENTS
Logs -> Flow of unstructured data

Oct 4 16:57:24 web sshd[25828]: Received disconnect from 10.10.0.31: 11: disconnected by user

Consists of timestamp and message
**Event** -> Flow off **structured** data

Event {
  Time: Oct 4 16:57:24
  Process: sshd
  State: Received disconnect from 10.10.0.31
  Client: 10.10.0.31
}

consists of detailed attributes
Log & Eventmanagement

Logs > Event > Analyse (Correlation) > Action
Tools

- Nagios & Icinga Addons
  - Check_logfiles
  - EventDB

- Check_MK Event Console

- Logmanagement-Tools
  - ELK-Stack
  - Graylog
  - Fluentd

ELK Stack
Overview

Shipper → redis → Broker → Indexer → Elasticsearch → Search & Storage → Webinterface
Logstash

- Logmanagement based on JRuby
- Configurable “Pipe”
- Flexible Plugin-Architecture for
  - Input
  - Filter
  - Output
- Single File Deployment
Logstash - IO

**Outputs**
- amqp
- boundary
- circonus
- cloudwatch
- datadog
- datadog_metrics
- elasticsearch
- elasticsearch_http
- elasticsearch_river
- email
- exec
- file
- ganglia
- gelf
- gemfire
- google_cloud_storage
- graphite
- graphtastic
- hipchat
- relp
- s3
- snmptrap
- sqlite
- sqs
- stdin
- stomp
- syslog
- tcp
- twitter
- udp
- unix
- varnishlog
- websocket
- wmi
- xmpp
- zenoss
- zeromq

**Inputs**
- amqp
- drupal_dblog
- elasticsearch
- eventlog
- exec
- file
- ganglia
- gelf
- gemfire
- generator
- graphite
- heroku
- imap
- irc
- log4j
- lumberjack
- metriccatcher
- mongodb
- nagios
- nagios_nsca
- null
- opentsdb
- pagerduty
- pipe
- rabbitmq
- redis
- riak
- riemann
- s3
- sns
- sqs
- statsd
- stdout
- stomp
- syslog
- tcp
- udp
- websocket
- xmpp
- zabbix
- zeromq
Logstash - Installation

- Download - www.elastic.co/downloads/logstash
- bin/logstash agent -f <config-file>
Redis

- NoSQL in memory based on C
- Support for various “Datatypes”
  - Strings / Hashes / Lists
  - Sets and Sorted Sets
- Support for various replication scenarios
- Very high performance

$ ./redis-benchmark -r 1000000 -n 2000000 -t get,set,lpush,lpop -q
SET: 122556.53 requests per second
GET: 123601.76 requests per second
LPUSH: 136752.14 requests per second
LPOP: 132424.03 requests per second
Redis - Installation

- Download - http://redis.io/download
- make
- make test
- make install
- /usr/local/bin/redis-server
Elasticsearch

- Schema free RESTful server based on Java
- Based on Lucene Core
- “Comparable” with Apache Solr
- Distributed Architecture using
  - Shards
  - Replicas
  - Gateways
- Realtime search base for Kibana
Elasticsearch – Installation

- Download – www.elastic.co/downloads/elasticsearch
- Unpack the archive
- Run bin/elasticsearch
INPUT OFF LOGS
Overview - Logshipping

Shipper → Broker → Indexer → Search & Storage → Webinterface
We love Open Source

Logstash - Shipper

- Shipment of logs to Logstash
  - Logstash
  - Logstash Forwarder
  - Syslog
  - Log4J
  - Gelf
  - File-Read
  - Many more
Logstash – Shipper - Configuration

• Configuration

    input {
        file {
            path => "/root/demodata/access.log.1"
            type => "apache-access"
        } } 

    output {
        stdout {
            debug => true
        } 
        redis {
            host => "127.0.0.1"
            data_type => "list"
            key => "logstash.apache"
        } 
    } 

• bin/logstash agent –f logstash_shipper.conf
EVENT INDEXING
We love Open Source

Overview - Indexing

- **Shipper**
  - Redis

- **Shipper**
  - Indexer

- **Shipper**
  - Elasticsearch

- **Shipper**
  - Webinterface
Logstash - Indexer

• Configuration

```ruby
input {
  redis {
    host => "127.0.0.1"
    type => "redis-input"
    # these settings should match the output of the agent
    data_type => "list"
    key => "logstash.apache"
  }
}

output {
  stdout {
    debug => true
  }
  elasticsearch_http {
    host => "127.0.0.1"
  }
}
```
Bring your stuff in order

- We need more than a timestamp and message
- We need structured and queryable information
- We need grok
Grok - Example

55.3.244.1 GET /index.html 15824 0.043

client: 55.3.244.1
method: GET
request: /index.html
bytes: 15824
duration: 0.043
Demo

http://grokconstructor.appspot.com/do/match#result
Logstash – Indexer- Apache

• Configuration for Apache-Logs

input {
  redis {
    host => "127.0.0.1"
    type => "apache-access"
    data_type => "list"
    key => "logstash.apache"
    format => "json_event"
  }
}

filter {
  if [type] == "apache-access" {
    grok {
      match => [ "message", "%{COMBINEDAPACHELOG}" ]
    }
  }
}

output {
  elasticsearch_http {
    host => "127.0.0.1"
  }
}
Logstash – Indexer - GEOIP

- Configuration for Geo-Data

```yaml
input {
  redis {
    host => "127.0.0.1"
    type => "apache-access"
    data_type => "list"
    key => "logstash.apache"
  }
}
filter {
  grok {
    type => "apache-access"
    pattern => "%{COMBINEDAPACHELOG}"
  }
  geoip {
    source => "clientip"
    add_tag => ["geotag"]
  }
}
output {
  elasticsearch_http {host => "127.0.0.1"}
}
```
INTERFACES & API
We love Open Source

Kibana

**TOP10 CLIENTS**

<table>
<thead>
<tr>
<th>Term</th>
<th>Count</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>91.198.2.65</td>
<td>520516</td>
<td></td>
</tr>
<tr>
<td>95.91.81.184</td>
<td>57627</td>
<td></td>
</tr>
<tr>
<td>66.249.78.140</td>
<td>12630</td>
<td></td>
</tr>
<tr>
<td>91.198.2.70</td>
<td>12144</td>
<td></td>
</tr>
<tr>
<td>66.249.67.224</td>
<td>9596</td>
<td></td>
</tr>
<tr>
<td>66.249.67.237</td>
<td>9332</td>
<td></td>
</tr>
<tr>
<td>66.249.67.211</td>
<td>9064</td>
<td></td>
</tr>
<tr>
<td>91.198.2.112</td>
<td>5728</td>
<td></td>
</tr>
<tr>
<td>66.249.79.154</td>
<td>5118</td>
<td></td>
</tr>
<tr>
<td>66.249.78.166</td>
<td>4799</td>
<td></td>
</tr>
</tbody>
</table>

**TOP USERAGENTS**

- "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.75.4 (KHTML ML, like Gecko) Version/7.0.4 Safari/537.76.4" (2688:1)
- "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0" (2480:5)
- "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36" (568:37)
- "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
  (34:66)
- "Googlebot-Image/1.0" (176:19)

**RESPONSE**

- 200 (619:4:4)
- 304 (25:9:5)
- 302 (9:8:6)
- 403 (4:6:14)
- 301 (4:1:23)
- 500 (5:83)
- 404 (4:4:46)
- 401 (4:20)
- 400 (2)

**TRAFFIC IN BYTES**

View | Zoom Out | http_bytes mean per 1h | http_bytes hits
DEMO
MONITORING ELK-STACK
Monitoring of the ELK-Stack

- Availability of services and resources
  - Shipment
  - Caching and Indexing
  - Storage
- Realtime monitor for Elasticsearch
NODE PING

- http://berk-logstash.demo.netways.de/es/

{
  "status" : 200,
  "name" : "Richard Fisk",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.5",
    "build_hash" : "2aaf797f2a571dc8779a3b61180afe8390ab61f9",
    "build_timestamp" : "2015-04-27T08:06:06Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
We love Open Source

ElasticHQ

Cluster Overview

<table>
<thead>
<tr>
<th>Cluster Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Nodes</td>
</tr>
<tr>
<td><strong>10</strong> Total Shards</td>
</tr>
<tr>
<td><strong>5</strong> Successful Shards</td>
</tr>
<tr>
<td><strong>1</strong> Indices</td>
</tr>
<tr>
<td><strong>19,368</strong> Documents</td>
</tr>
<tr>
<td><strong>11.5MB</strong> Size</td>
</tr>
</tbody>
</table>

Cluster Health

<table>
<thead>
<tr>
<th>Status</th>
<th>Yellow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timed Out?</td>
<td>false</td>
</tr>
<tr>
<td># Nodes</td>
<td>1</td>
</tr>
</tbody>
</table>

Indices

<table>
<thead>
<tr>
<th>Index</th>
<th># Docs</th>
<th>Primary Size</th>
<th># Shards</th>
<th># Replicas</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>logstash-2014.03.11</td>
<td>19,388</td>
<td>11.5MB</td>
<td>5</td>
<td>1</td>
<td>open</td>
</tr>
</tbody>
</table>
DEMO
INTEGRATION NAGIOS, ICINGA AND CHECK_MK
Realtime Loganalysis

- Analyse various in sources in realtime
- Check for patterns and states
  - Facilitites
  - Regex
  - Programs
- Submission as passive events
Overview Logstash and Nagios

- Indexer
- Search & Storage
- Webinterface
- Commandpipe
- Icinga -Web
Logstash - Nagios

• Configuration for Nagios-Alert

input {
...
}

filter {
  if [type] == "syslog" {
    grok {match => [ "message", "%{SYSLOGBASE}" ]}
    grep {
      match => [ "message", "Error" ]
      drop => false
      add_tag => "nagios-update"
      add_field => [
        # "nagios_host", "%@source_host",
        "nagios_host", "localhost",
        "nagios_service", "Logstash",
        "nagios_level", "2"
      ]
    }
  }
}

output {
  elasticsearch {host => "127.0.0.1"}
  nagios {
    commandfile => "/var/lib/icinga/rw/icinga.cmd"
  }
}
Overview Check_MK

Indexer -> Elasticsearch -> Search & Storage -> Webinterface

Multisite
Using the integrated Syslog-Server

- Enable the integrated Syslog server
  - omd config set MKEVENTD_SYSLOG on
- Since version 1.2.3i2 TCP is also available
Logstash -> Syslog

• Configuration for Syslog output

```ruby
input {
  ...
}

filter {
  if [type] == "syslog" {
    grok {match => [ "message", "%{SYSLOGBASE}" ]}
    grep {
      match => [ "message", "Error" ]
      drop => false
      add_tag => "checkmk"
    }
  }
}

output {
  elasticsearch {host => "127.0.0.1"}
  syslog {
    facility => "local0"
    host => 192.168.1.1
    port => tcp
    severity => "critical"
  }
}
```
CONCLUSION
Conclusion ELK-Stack

• Support for a huge number of APIs and programs
• Scalable storage backend with Elasticsearch
• Flexible Query-Interface with Kibana
• Highly integrable in all popular stacks
• Collect *everything* and analyse *later*!
THANK YOU

www.netways.de
blog.netways.de
www.netways.org

netways
netways
netways