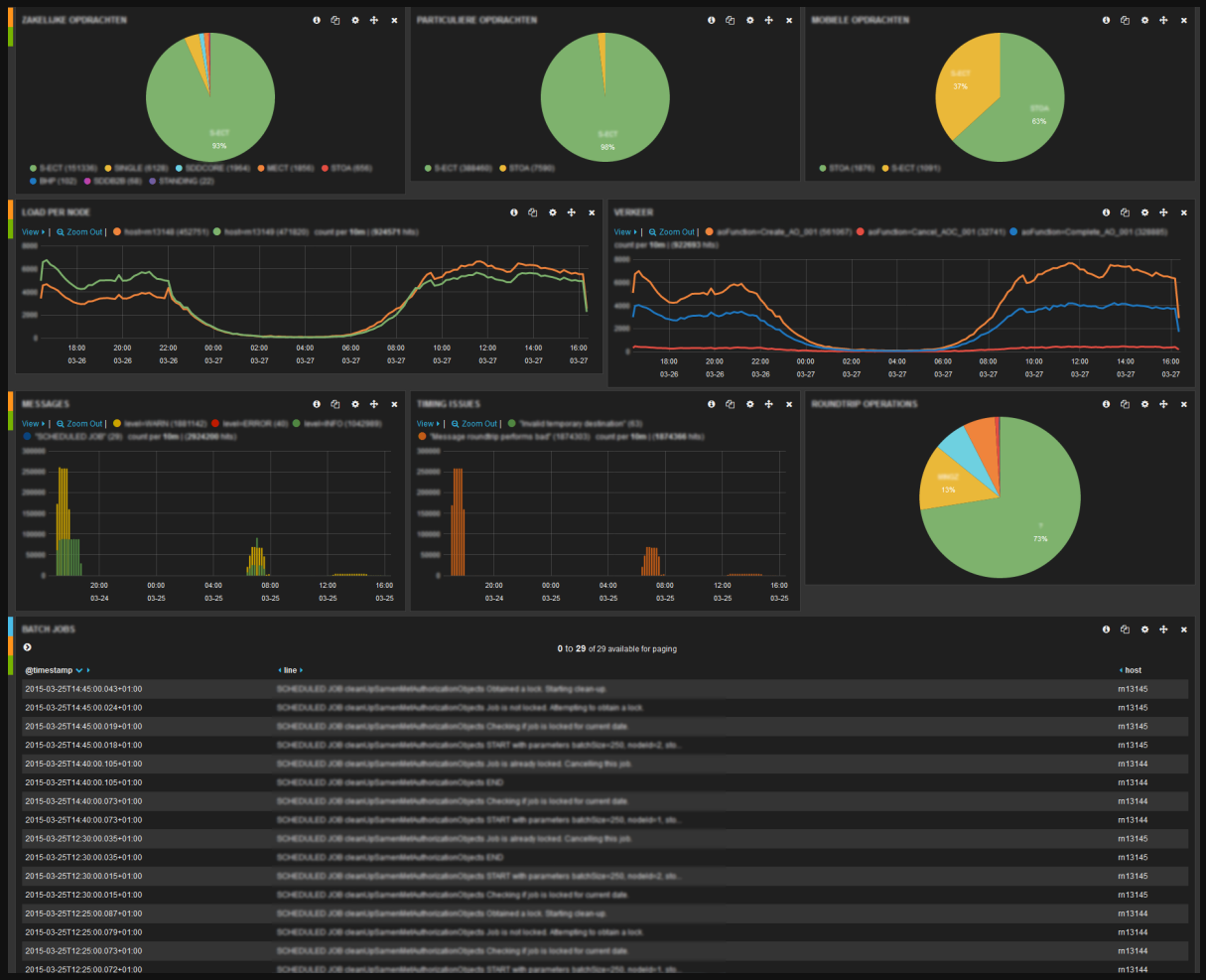
Deploying ELK in the real world

JavaCro '16 // May 19, 2016

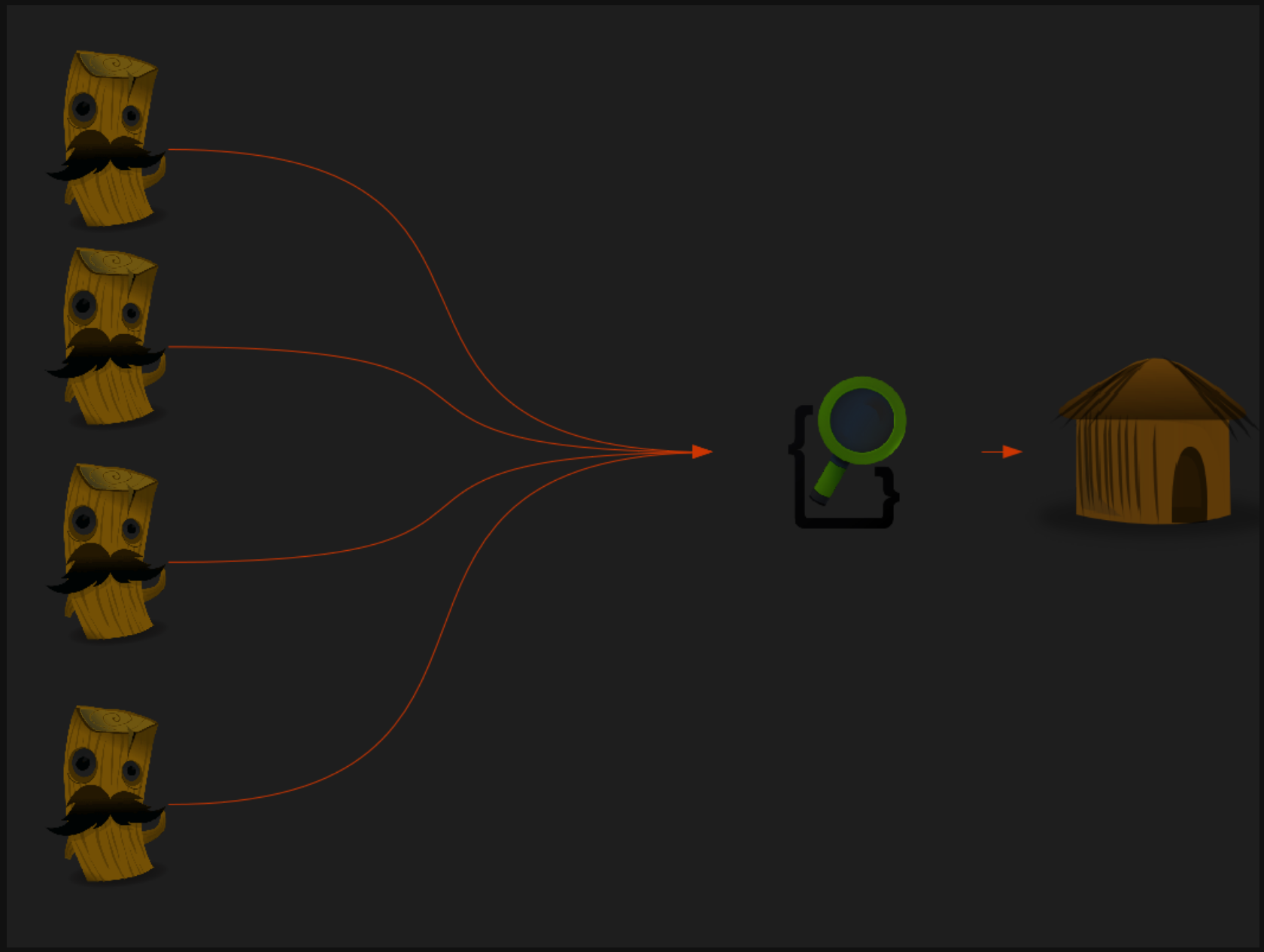
Maarten Mulders // @mthmulders

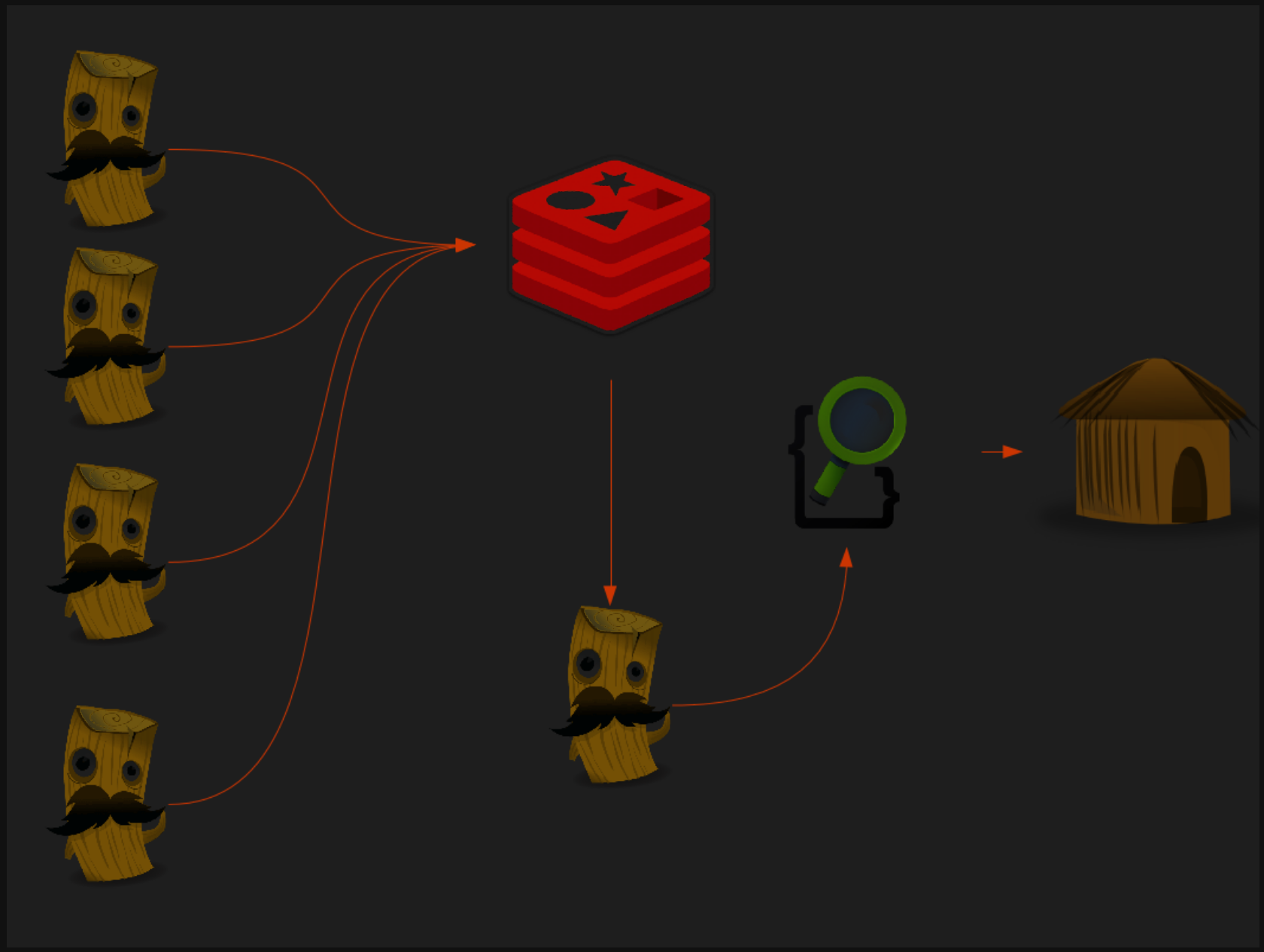
Agenda

- Intro
- Setup
- Sensitive data
- Usage patterns
- Q & A


ZAKELIJKE OPDRACHTEN
PARTICULIERE OPDRACHTEN
MOBIELE OPDRACHTEN
LOAD PER NODE
VERKEER
MESSAGES
TIMING ISSUES
ROUNDTRIP OPERATIONS
BATCH JOBS
0 to 29 of 29 available for paging
@timestamp
line
host

```
input {
  file {
    path => "/path/to/file.log"
  }
}
output {
  file {
    path => "/path/to/copied.log"
  }
}
```





Logstash

Processess technical logging and audit logging

Adds information

Removes information

Transforms information to a more usable form

Ship events to redis

Second Logstash

Uniforming data from heterogeneous sources

input: read events from redis

filter: fix timezones, transform xml into json

output: send events to elastic

Elastic

Large cluster that contains log data

Keeps one month of history

Also stores Kibana config

Kibana

Filters based on environment and timestamp (last 24h)

Automatically refreshed

Queries for 'error', 'orange cell', specific errors

Uses rows and panels for optimal screen usage

Sensitive data

Logstash input

```
input {
  file {
    path => "/path/to/application.log"
    codec => multiline {
      pattern => "^%{TIMESTAMP_ISO8601} "
      negate => true
      what => previous
    }
    type => "application"
  }
  file {
    path => "/path/to/audit.log"
    type => "audit"
  }
}
```

Logstash filters

```
filter {
  if [type] == "application" {
    grok {
      match => {
        "message" => "(?m)%{TIMESTAMP_ISO8601:timestamp} \[%DATA\]
          %{LOGLEVEL:level} %{JAVACLASS} %{GREEDYDATA:line}"
      }
      remove_field => "message"
    }
  }
}
```

```
2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
   eventId=1401751935098~|~inChannel=MINGZ~|~odBeneficiaryAccount=NL28INGB0000000001
```

```
filter {
  if [type] == "audit" {









  }
}
```

```
{ message: "2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
       eventId=1401751935098~|~inChannel=MINGZ~|~
       odBeneficiaryAccount=NL28INGB0000000001" }
```

```
2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
   eventId=1401751935098~|~inChannel=MINGZ~|~odBeneficiaryAccount=NL28INGB0000000001
```

```
filter {
  if [type] == "audit" {
    grok {
      match => {
        "message" => "(?m)%{TIMESTAMP_ISO8601:timestamp} \[%DATA\]
          %{LOGLEVEL} %{JAVACLASS} %{GREEDYDATA:audit_message}"
      }
      remove_field => "message"
    }









  }
}
```

```
{ timestamp: "2015-01-28 01:32:15,098",
  audit_message: "eventId=1401751935098~|~inChannel=MINGZ~|~
    odBeneficiaryAccount=NL28INGB0000000001" }
```

```
2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
   eventId=1401751935098~|~inChannel=MINGZ~|~odBeneficiaryAccount=NL28INGB0000000001
```

```
filter {
  if [type] == "audit" {
    grok {
      match => {
        "message" => "(?m)%{TIMESTAMP_ISO8601:timestamp} \[%DATA\]
          %{LOGLEVEL} %{JAVACLASS} %{GREEDYDATA:audit_message}"
      }
      remove_field => "message"
    }
    mutate { gsub => ["audit_message", "\~\|\~", "`"] }









  }
}
```

```
{ timestamp: "2015-01-28 01:32:15,098",
  audit_message: "eventId=1401751935098`inChannel=MINGZ`
    odBeneficiaryAccount=NL28INGB0000000001" }
```

```
2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
   eventId=1401751935098~|~inChannel=MINGZ~|~odBeneficiaryAccount=NL28INGB0000000001
```

```
filter {
  if [type] == "audit" {
    grok {
      match => {
        "message" => "(?m)%{TIMESTAMP_ISO8601:timestamp} \[%DATA\]
          %{LOGLEVEL} %{JAVACLASS} %{GREEDYDATA:audit_message}"
      }
      remove_field => "message"
    }
    mutate { gsub => ["audit_message", "\~\|\~", "`"] }
    kv {
      source => "audit_message"
      field_split => "`"
      remove_field => "audit_message"
    }

  }
}
```

```
{ timestamp: "2015-01-28 01:32:15,098",
  eventId: "1401751935098",
  inChannel: "MINGZ",
  odBeneficiaryAccount: "NL28INGB0000000001" }
```

```
2015-01-28 01:32:15,098 [thread-1] INFO nl.ing.application.Class
   eventId=1401751935098~|~inChannel=MINGZ~|~odBeneficiaryAccount=NL28INGB0000000001
```

```
filter {
  if [type] == "audit" {
    grok {
      match => {
        "message" => "(?m)%{TIMESTAMP_ISO8601:timestamp} \[%DATA\]
          %{LOGLEVEL} %{JAVACLASS} %{GREEDYDATA:audit_message}"
      }
      remove_field => "message"
    }
    mutate { gsub => ["audit_message", "\~\|\~", "`"] }
    kv {
      source => "audit_message"
      field_split => "`"
      remove_field => "audit_message"
    }
    prune { blacklist_names => "^od.+$" }
  }
}
```

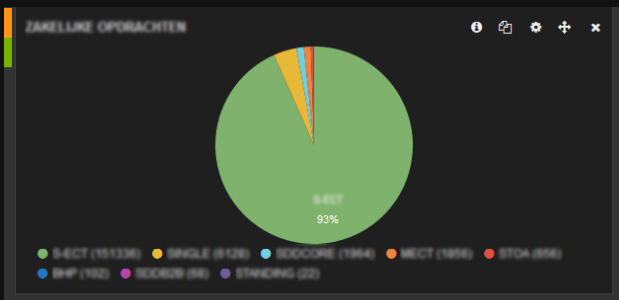
```
{ timestamp: "2015-01-28 01:32:15,098",
  eventId: "1401751935098",
  inChannel: "MINGZ" }
```

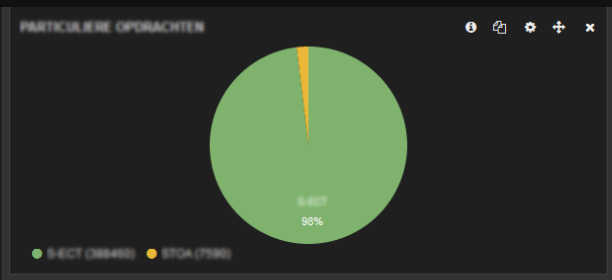
```
filter {
  if "_grokparsefailures" in [tags] {
    prune {
      blacklist_names => [ "message", "audit_message" ]
    }
  }
}
```

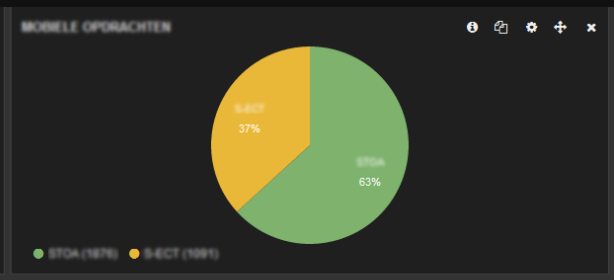
Logstash

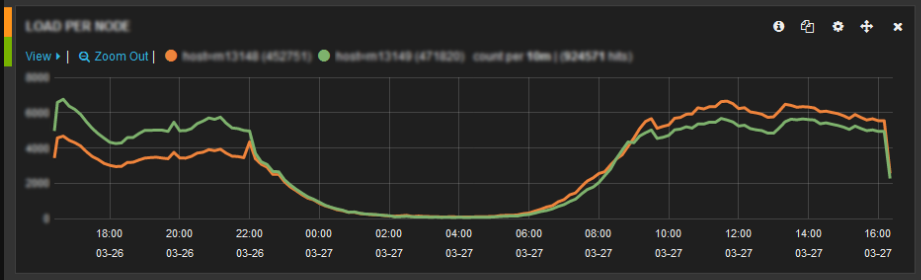
```
output {
  redis {
    host => "redis-host"
    data_type => "list"
    key => "logstash"
  }
}
```

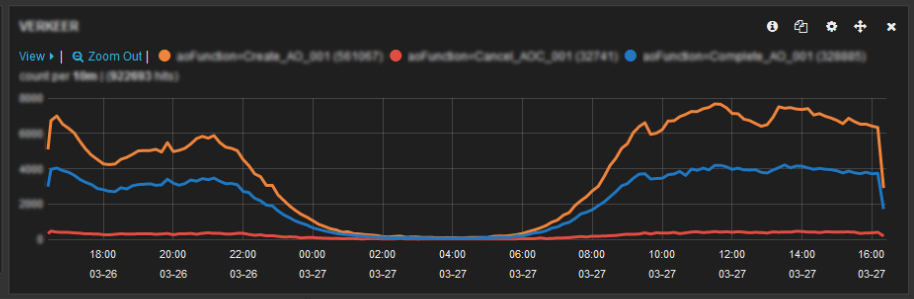
Usage patterns

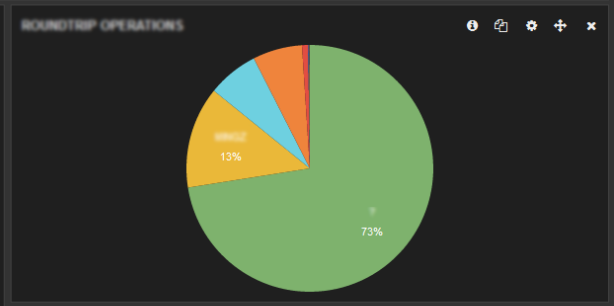










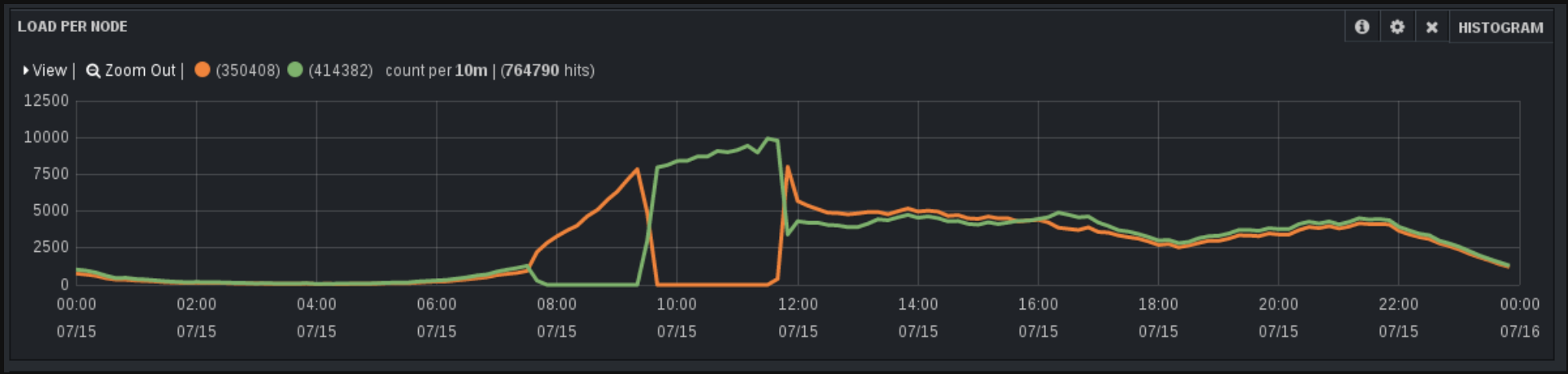


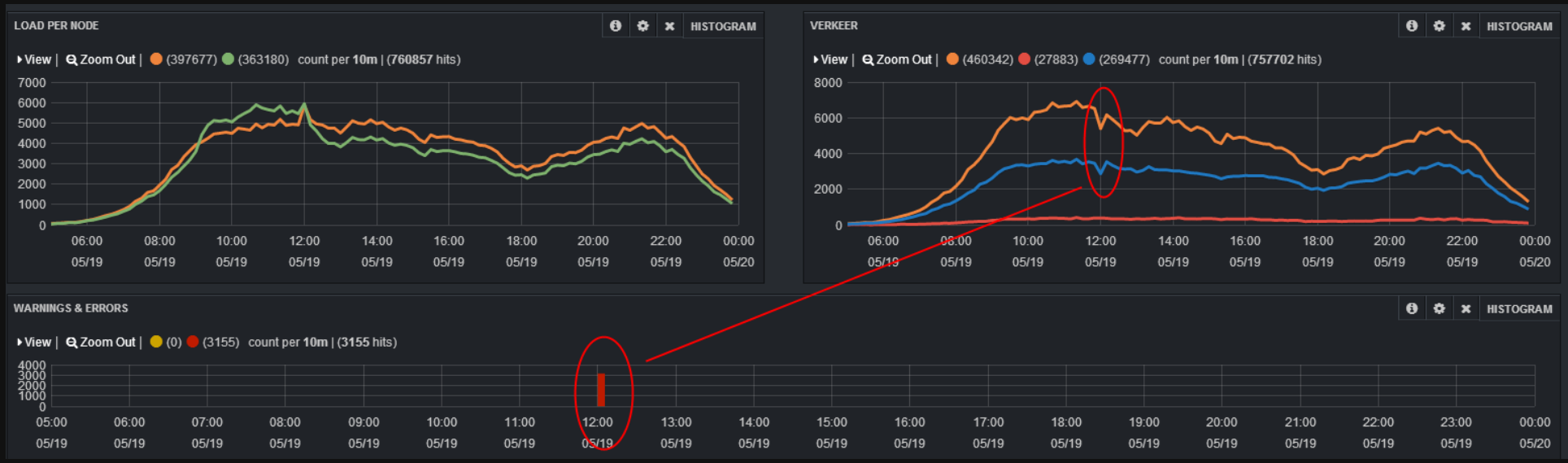
BATCH JOBS

0 to **29** of 29 available for paging

@timestamp	line	host
2015-03-25T14:45:00.043+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Obtained a lock. Starting clean-up.	rn13145
2015-03-25T14:45:00.024+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Job is not locked. Attempting to obtain a lock.	rn13145
2015-03-25T14:45:00.019+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Checking if job is locked for current date.	rn13145
2015-03-25T14:45:00.018+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects START with parameters batchSize=250, nodeId=2, sto...	rn13145
2015-03-25T14:40:00.105+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Job is already locked. Cancelling this job.	rn13144
2015-03-25T14:40:00.105+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects END	rn13144
2015-03-25T14:40:00.073+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Checking if job is locked for current date.	rn13144
2015-03-25T14:40:00.073+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects START with parameters batchSize=250, nodeId=1, sto...	rn13144
2015-03-25T12:30:00.035+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects Job is already locked. Cancelling this job.	rn13145
2015-03-25T12:30:00.035+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects END	rn13145
2015-03-25T12:30:00.015+01:00	SCHEDULED JOB cleanUpSamenWerkAuthorizationObjects START with parameters batchSize=250, nodeId=2, sto...	rn13145

2015-03-25T12:30:00.015+01:00	SCHEDULED JOB cleanUpSamenMetAuthorizationObjects Checking if job is locked for current date	rn13145
2015-03-25T12:25:00.087+01:00	SCHEDULED JOB cleanUpSamenMetAuthorizationObjects Obtained a lock. Starting clean-up.	rn13144
2015-03-25T12:25:00.079+01:00	SCHEDULED JOB cleanUpSamenMetAuthorizationObjects Job is not locked. Attempting to obtain a lock.	rn13144
2015-03-25T12:25:00.073+01:00	SCHEDULED JOB cleanUpSamenMetAuthorizationObjects Checking if job is locked for current date	rn13144
2015-03-25T12:25:00.072+01:00	SCHEDULED JOB cleanUpSamenMetAuthorizationObjects START with parameters batchSize=250, nodeId=1, slo	rn13144

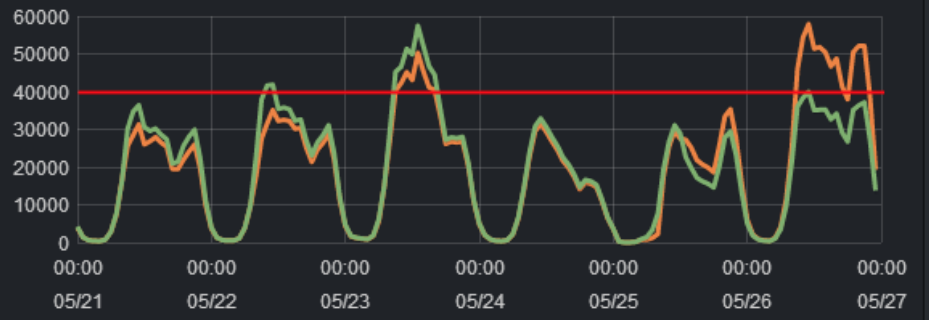

LOAD PER NODE
HISTOGRAM
View | Zoom Out | (350408) (414382) count per 10m | (764790 hits)
12500
10000
7500
5000
2500
0
00:00 07/15
02:00 07/15
04:00 07/15
06:00 07/15
08:00 07/15
10:00 07/15
12:00 07/15
14:00 07/15
16:00 07/15
18:00 07/15
20:00 07/15
22:00 07/15
00:00 07/16


LOAD PER NODE
HISTOGRAM
View | Zoom Out | (397677) (363180) count per 10m | (760857 hits)
7000
6000
5000
4000
3000
2000
1000
0
06:00 05/19
08:00 05/19
10:00 05/19
12:00 05/19
14:00 05/19
16:00 05/19
18:00 05/19
20:00 05/19
22:00 05/19
00:00 05/20
VERKEER
HISTOGRAM
View | Zoom Out | (460342) (27883) (269477) count per 10m | (757702 hits)
8000
6000
4000
2000
0
06:00 05/19
08:00 05/19
10:00 05/19
12:00 05/19
14:00 05/19
16:00 05/19
18:00 05/19
20:00 05/19
22:00 05/19
00:00 05/20
WARNINGS & ERRORS
HISTOGRAM
View | Zoom Out | (0) (3155) count per 10m | (3155 hits)
4000
3000
2000
1000
0
05:00 05/19
06:00 05/19
07:00 05/19
08:00 05/19
09:00 05/19
10:00 05/19
11:00 05/19
12:00 05/19
13:00 05/19
14:00 05/19
15:00 05/19
16:00 05/19
17:00 05/19
18:00 05/19
19:00 05/19
20:00 05/19
21:00 05/19
22:00 05/19
23:00 05/19
00:00 05/20

LOAD PER NODE

HISTOGRAM

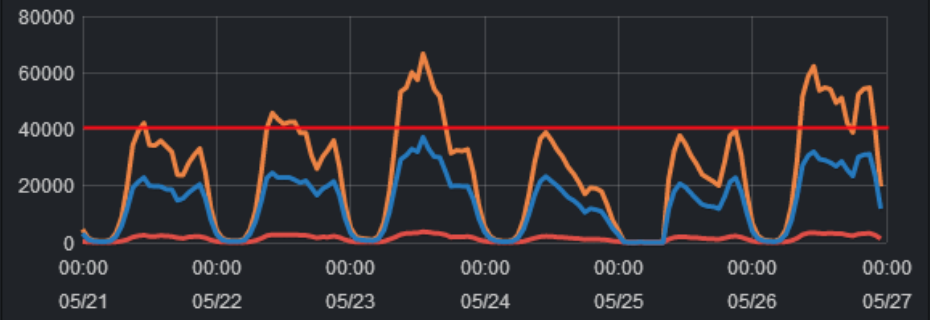
▸View | Zoom Out | (2883487) (2811663) count per **1h** | (**5695150** hits)

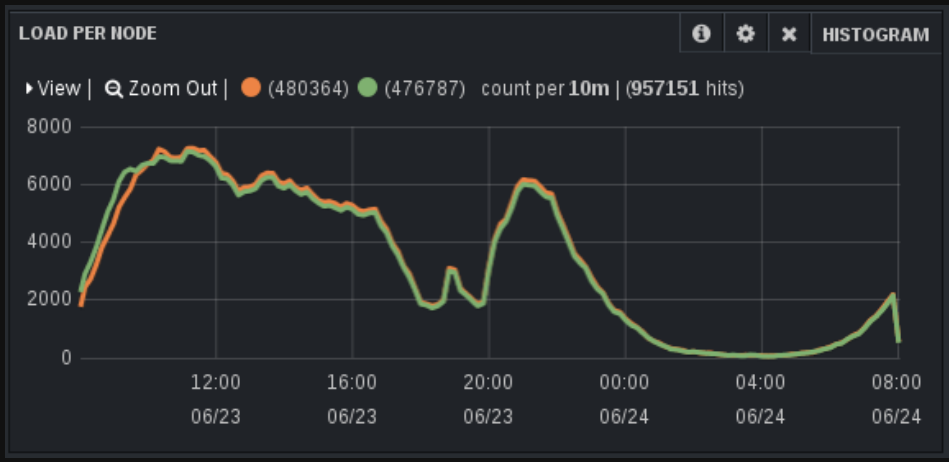


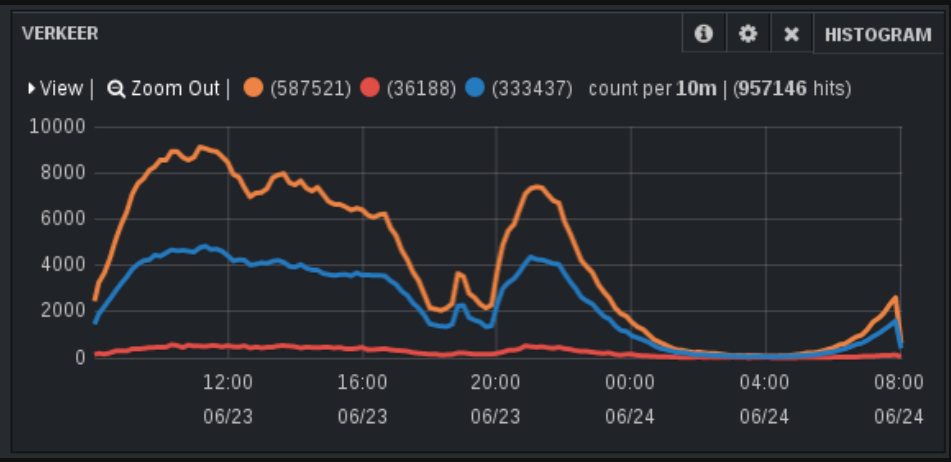
VERKEER

HISTOGRAM

▸View | Zoom Out | (3462339) (209086) (1995867) count per **1h** | (**5667292** hits)




LOAD PER NODE
HISTOGRAM
View | Zoom Out | (480364) (476787) count per 10m | (957151 hits)
8000
6000
4000
2000
0
12:00 06/23
16:00 06/23
20:00 06/23
00:00 06/24
04:00 06/24
08:00 06/24


VERKEER
HISTOGRAM
View | Zoom Out | (587521) (36188) (333437) count per 10m | (957146 hits)
10000
8000
6000
4000
2000
0
12:00 06/23
16:00 06/23
20:00 06/23
00:00 06/24
04:00 06/24
08:00 06/24

Questions?