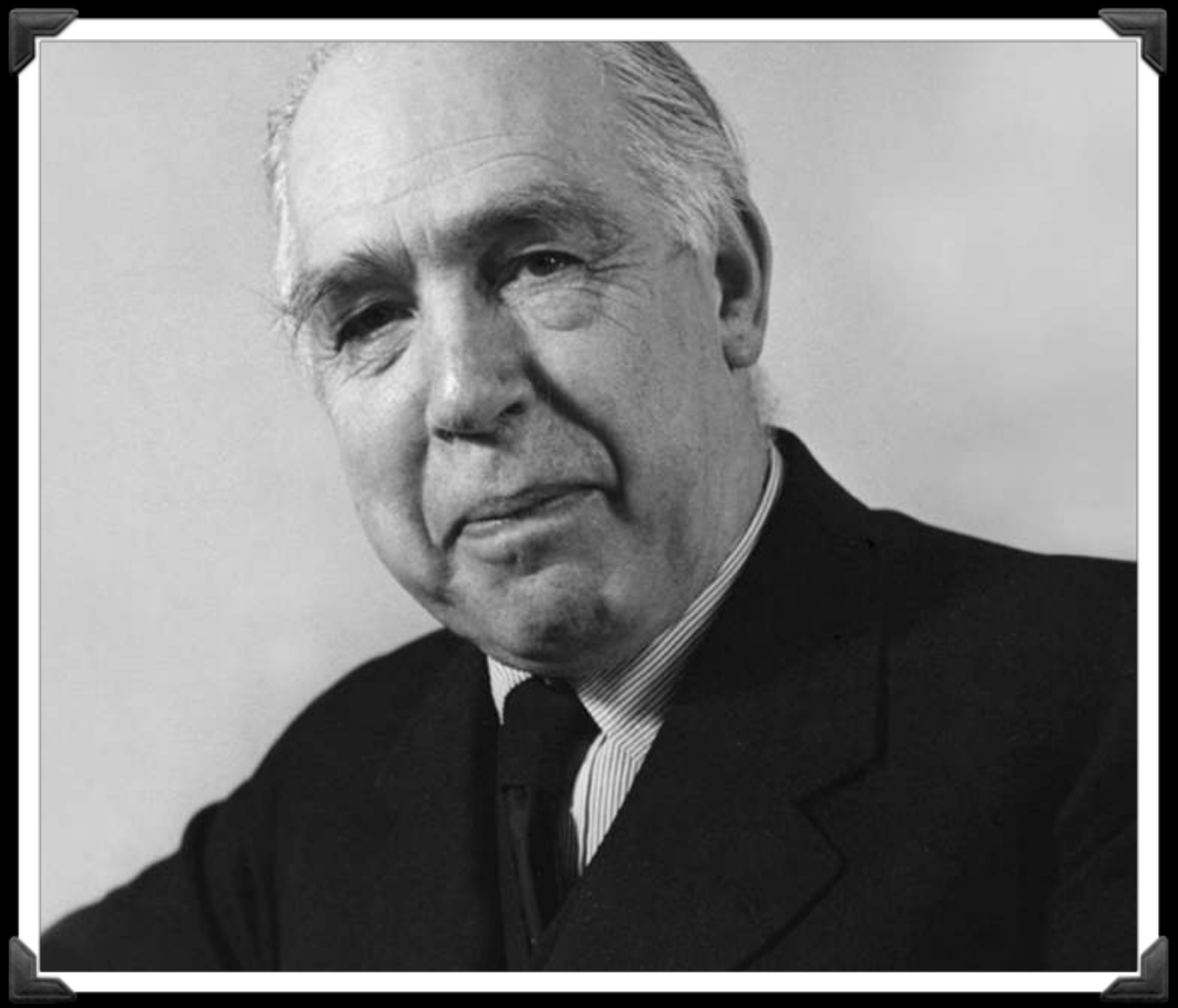

GrayLog

# Wer Wie Was
# Wieso Weshalb Warum

… eine Suchmaschine für Logfiles Sinn macht.



**prediction is very difficult,
especially if it's about the future**

**— Niels Bohr**

# Worum geht’s?

**“Eine Logdatei enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem.”**

—wikipedia

“Außer dem **Betriebssystem** selbst schreiben meist **Hintergrundprogramme** (z. B. ein E-Mail-Server, ein Proxyserver und anderes) in **Logdateien,** um **Aktionsmeldungen, Fehlermeldungen** und **Hinweise** persistent (dauernd) oder temporär verfügbar zu halten. Ähnliches gilt für **Installationsprogramme, Firewalls, Virenscanner** und dergleichen.”

—wikipedia

# Struktur des Vortrags

# Problem

Wir haben ein Problem

# Idee

Die Experten hacken schnell was zusammen

# Implementierung

Reboot vom Server

# Effekt

Skalierungsprobleme

Das kannste
schon so
machen,
aber dann isses
halt Kacke

# Logfails aus der Hölle

# Problem

Wenn die Kunden das Formular ausfüllen,
kommt das nicht immer in der Datenbank an

# Idee

Ops soll Dev automatisch informieren

# Implementierung

Email vom Webserver an die Devs-Mailingliste
mit den Fehlern

# Effekt

Sie haben Post


# SIE HABEN POST

Ca. 6000 Stück pro <Zeiteinheit>

# Problem

Devs haben zu viele Emails vom Webserver

# Idee

Das kann man doch weg filtern in Ordner

# Implementierung

Outlook

# Effekt

Wo in den 6000 Spam-Mails
war jetzt die Email vom Chef?

# Idee

Sammeln und nur eine Email schreiben

# Implementierung

Webserver schreibt es in ein Logfile,
das wird einmal am Tag an die Devs geschickt

# Effekt

Sie haben **keine** Post,
weil Email größer als 10 MB ist.

# Idee

Sammeln, **filtern** und nur dann eine Email schreiben

# Implementierung

Webserver schreibt es in ein Logfile,
ein **Perl-Skript filtert** es dann und
das wird einmal am Tag an die Devs geschickt


WHENEVER I LEARN A NEW SKILL I CONCOCT ELABORATE FANTASY SCENARIOS WHERE IT LETS ME SAVE THE DAY.
OH NO! THE KILLER MUST HAVE FOLLOWED HER ON VACATION!
BUT TO FIND THEM WE'D HAVE TO SEARCH THROUGH 200 MB OF EMAILS LOOKING FOR SOMETHING FORMATTED LIKE AN ADDRESS!
IT'S HOPELESS!
EVERYBODY STAND BACK.
I KNOW REGULAR EXPRESSIONS.
PERL!
TAP TAP

# Effekt

Sie haben Post,
die nur bereits bekannte Probleme meldet.

# Problem

Wenn die Kunden das Formular ausfüllen,
kommt das nicht immer in der Datenbank an (2)

# Idee

Statt es auf jedem Server zu speichern,
könnte man es zentral speichern.

# Implementierung

Logfiles via NFS auf Fileserver

# Effekt

Der Fileserver glüht langsam vor sich hin.


# R.I.P.

Fileserver003.example.tld

# Idee

Statt es auf jedem Server zu speichern,
könnte man es zentral sammeln.

# Implementierung

syslog via syslog-Protokoll auf Fileserver

# Effekt

Mit anderen Worten:

**BIG DATA**

# Tod

Durch Informationsüberfluß

# Was kann man tun?

# Problem

Wenn die Kunden das Formular ausfüllen,
kommt das nicht immer in der Datenbank an (3)

# Idee

Statt es auf jedem Server zu speichern,
könnte man es zentral sammeln.

# Implementierung

syslog via syslog-Protokoll
in eine Logfile-Suchmaschine schieben

# Effekt

# BIG DATA

Aber mit Sauce und scharf!

# Daten

das neue Öl

# Womit?

- Closed-Source:
  - Splunk
- Open-Source:
  - ELK-Stack
  - GrayLog

Collect & Process

Analyse & Research

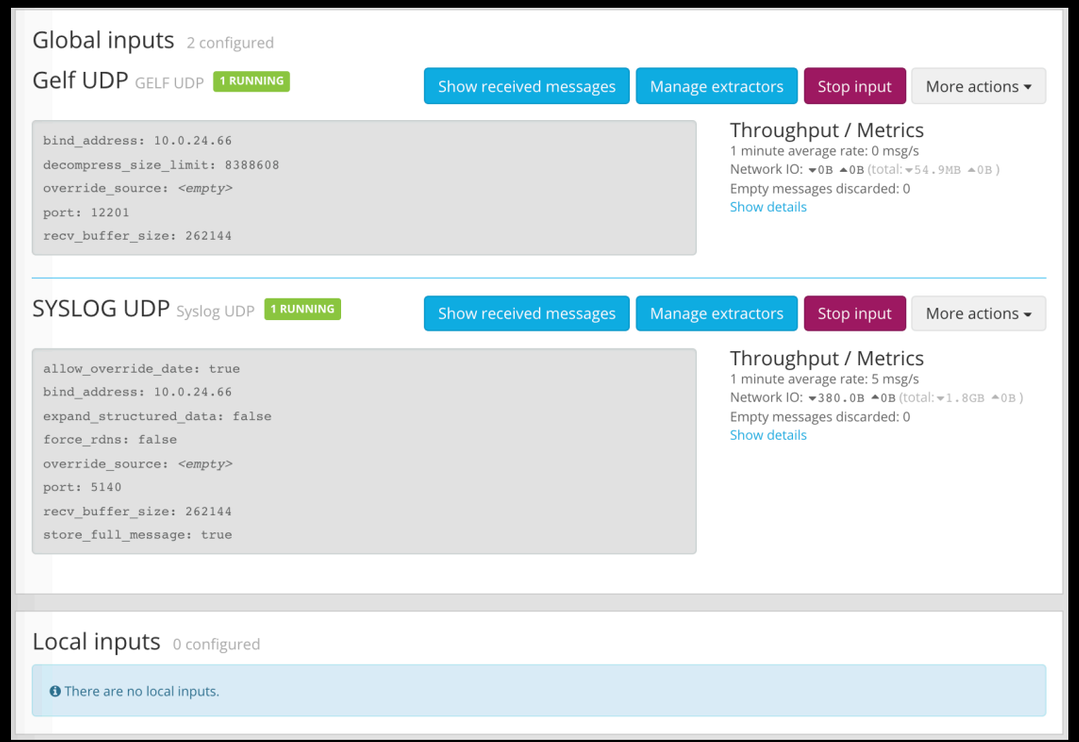
# GrayLog

Drill Down & Visualize

Alert & Trigger

# Collect & Process

- GrayLog kann über viele Wege mit Daten gefüttert werden:
- RFC 3164, RFC 5424, CEF, AWS, CloudTrail, PacketBeat, WinlogBeat, FileBeat und Raw Socket



# Global inputs 2 configured

## Gelf UDP GELF UDP 1 RUNNING

Show received messages | Manage extractors | Stop input | More actions

```
bind_address: 10.0.24.66
decompress_size_limit: 8388608
override_source: <empty>
port: 12201
recv_buffer_size: 262144
```

### Throughput / Metrics

1 minute average rate: 0 msg/s
Network IO: ▼0B ▲0B (total: ▼54.9MB ▲0B )
Empty messages discarded: 0
Show details

## SYSLOG UDP Syslog UDP 1 RUNNING

Show received messages | Manage extractors | Stop input | More actions

```
allow_override_date: true
bind_address: 10.0.24.66
expand_structured_data: false
force_rdns: false
override_source: <empty>
port: 5140
recv_buffer_size: 262144
store_full_message: true
```

### Throughput / Metrics

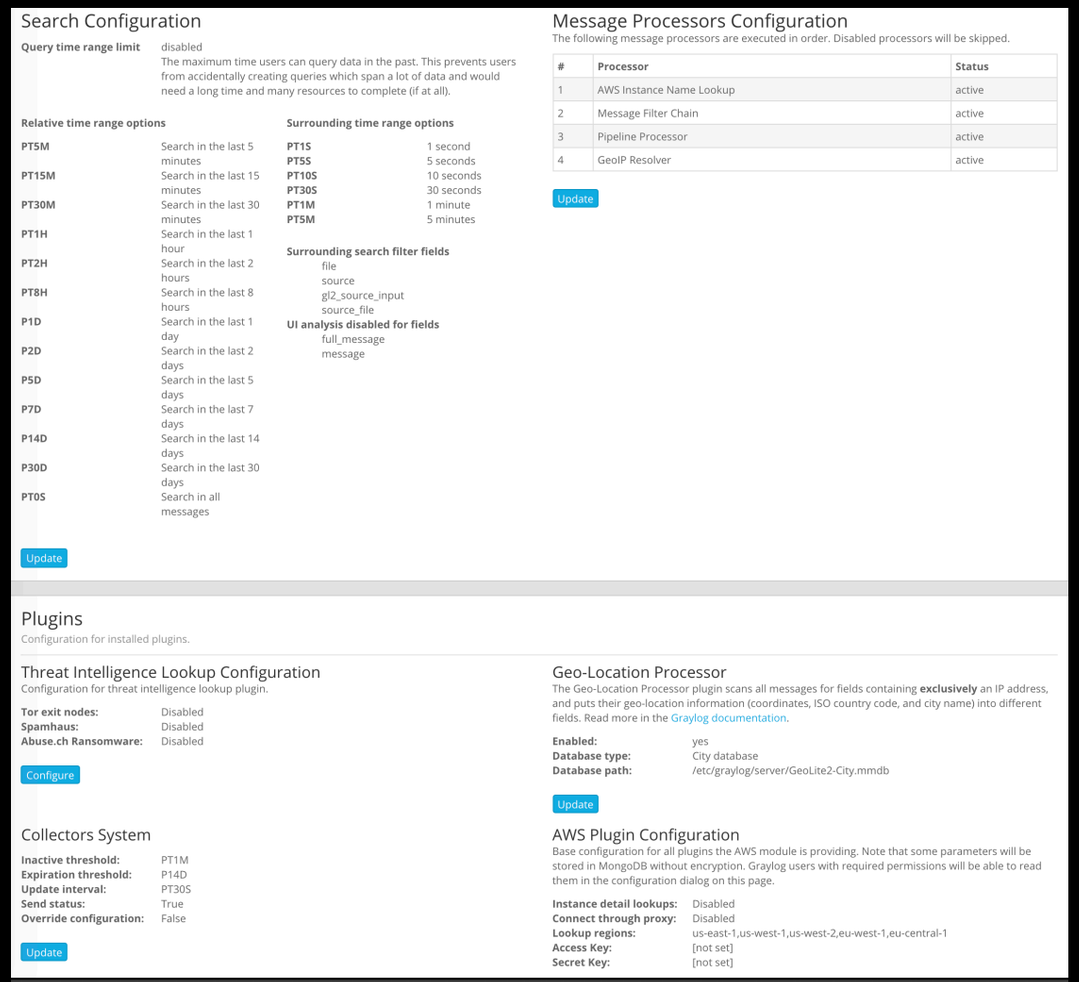
1 minute average rate: 5 msg/s
Network IO: ▼380.0B ▲0B (total: ▼1.8GB ▲0B )
Empty messages discarded: 0
Show details

# Local inputs 0 configured

There are no local inputs.

# Collect & Process

- Mit den GrayLog Plugins kann man Datenaufbereitung, z.B. GeoIP Unterstützung hinzufügen.



## Search Configuration

**Query time range limit** disabled
The maximum time users can query data in the past. This prevents users from accidentally creating queries which span a lot of data and would need a long time and many resources to complete (if at all).

**Relative time range options**

| | |
|---|---|
| **PT5M** | Search in the last 5 minutes |
| **PT15M** | Search in the last 15 minutes |
| **PT30M** | Search in the last 30 minutes |
| **PT1H** | Search in the last 1 hour |
| **PT2H** | Search in the last 2 hours |
| **PT8H** | Search in the last 8 hours |
| **P1D** | Search in the last 1 day |
| **P2D** | Search in the last 2 days |
| **P5D** | Search in the last 5 days |
| **P7D** | Search in the last 7 days |
| **P14D** | Search in the last 14 days |
| **P30D** | Search in the last 30 days |
| **PT0S** | Search in all messages |

**Surrounding time range options**

| | |
|---|---|
| **PT1S** | 1 second |
| **PT5S** | 5 seconds |
| **PT10S** | 10 seconds |
| **PT30S** | 30 seconds |
| **PT1M** | 1 minute |
| **PT5M** | 5 minutes |

**Surrounding search filter fields**
file
source
gl2_source_input
source_file

**UI analysis disabled for fields**
full_message
message

Update

## Message Processors Configuration

The following message processors are executed in order. Disabled processors will be skipped.

| # | Processor | Status |
|---|---|---|
| 1 | AWS Instance Name Lookup | active |
| 2 | Message Filter Chain | active |
| 3 | Pipeline Processor | active |
| 4 | GeoIP Resolver | active |

Update

# Plugins

Configuration for installed plugins.

## Threat Intelligence Lookup Configuration

Configuration for threat intelligence lookup plugin.

**Tor exit nodes:** Disabled
**Spamhaus:** Disabled
**Abuse.ch Ransomware:** Disabled

Configure

## Collectors System

**Inactive threshold:** PT1M
**Expiration threshold:** P14D
**Update interval:** PT30S
**Send status:** True
**Override configuration:** False

Update

## Geo-Location Processor

The Geo-Location Processor plugin scans all messages for fields containing **exclusively** an IP address, and puts their geo-location information (coordinates, ISO country code, and city name) into different fields. Read more in the Graylog documentation.

**Enabled:** yes
**Database type:** City database
**Database path:** /etc/graylog/server/GeoLite2-City.mmdb

Update

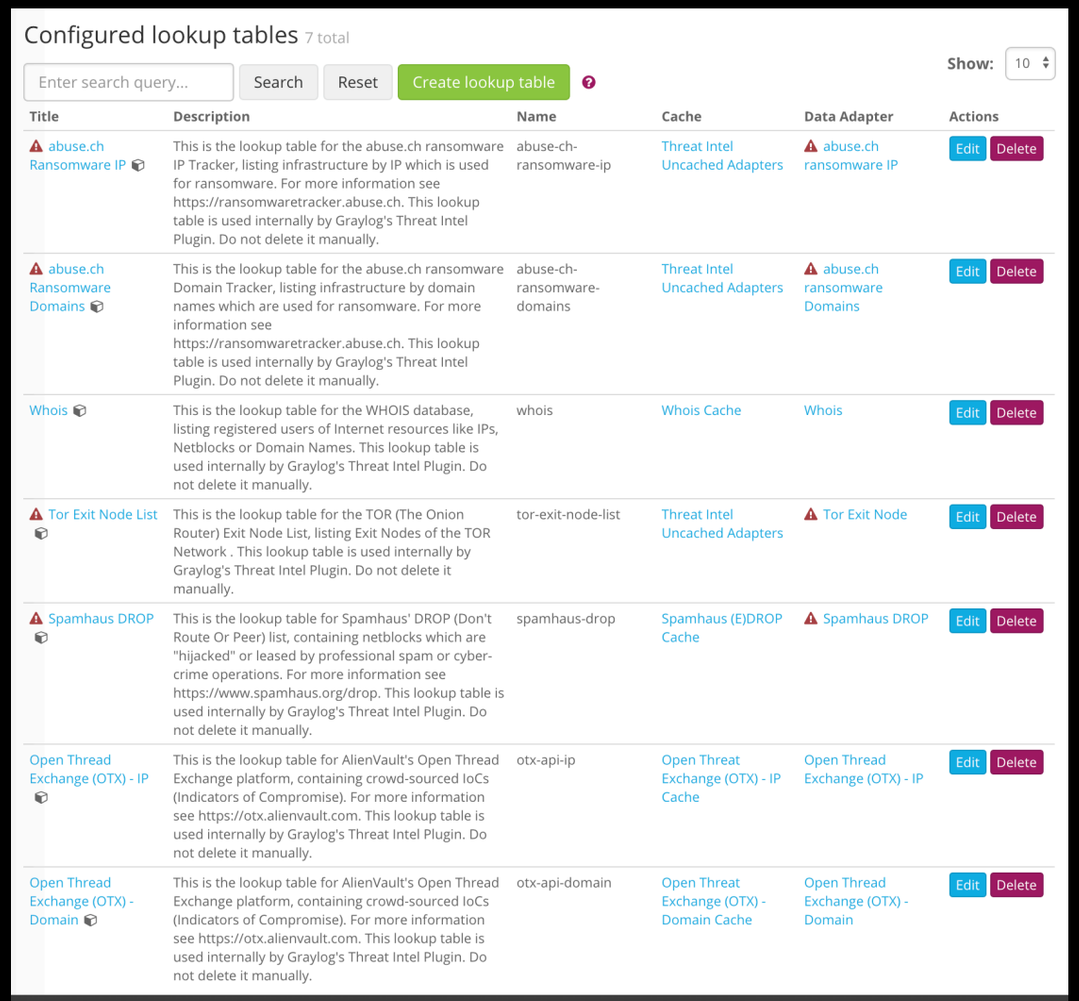
## AWS Plugin Configuration

Base configuration for all plugins the AWS module is providing. Note that some parameters will be stored in MongoDB without encryption. Graylog users with required permissions will be able to read them in the configuration dialog on this page.

**Instance detail lookups:** Disabled
**Connect through proxy:** Disabled
**Lookup regions:** us-east-1,us-west-1,us-west-2,eu-west-1,eu-central-1
**Access Key:** [not set]
**Secret Key:** [not set]

# Collect & Process

- GrayLog unterstützt Lookup-Tables um Daten auch nach dem Import aufzubereiten



Configured lookup tables 7 total

Enter search query... | Search | Reset | Create lookup table | Show: 10

| Title | Description | Name | Cache | Data Adapter | Actions |
|---|---|---|---|---|---|
| abuse.ch Ransomware IP | This is the lookup table for the abuse.ch ransomware IP Tracker, listing infrastructure by IP which is used for ransomware. For more information see https://ransomwaretracker.abuse.ch. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | abuse-ch-ransomware-ip | Threat Intel Uncached Adapters | abuse.ch ransomware IP | Edit Delete |
| abuse.ch Ransomware Domains | This is the lookup table for the abuse.ch ransomware Domain Tracker, listing infrastructure by domain names which are used for ransomware. For more information see https://ransomwaretracker.abuse.ch. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | abuse-ch-ransomware-domains | Threat Intel Uncached Adapters | abuse.ch ransomware Domains | Edit Delete |
| Whois | This is the lookup table for the WHOIS database, listing registered users of Internet resources like IPs, Netblocks or Domain Names. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | whois | Whois Cache | Whois | Edit Delete |
| Tor Exit Node List | This is the lookup table for the TOR (The Onion Router) Exit Node List, listing Exit Nodes of the TOR Network . This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | tor-exit-node-list | Threat Intel Uncached Adapters | Tor Exit Node | Edit Delete |
| Spamhaus DROP | This is the lookup table for Spamhaus' DROP (Don't Route Or Peer) list, containing netblocks which are "hijacked" or leased by professional spam or cyber-crime operations. For more information see https://www.spamhaus.org/drop. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | spamhaus-drop | Spamhaus (E)DROP Cache | Spamhaus DROP | Edit Delete |
| Open Thread Exchange (OTX) - IP | This is the lookup table for AlienVault's Open Thread Exchange platform, containing crowd-sourced IoCs (Indicators of Compromise). For more information see https://otx.alienvault.com. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | otx-api-ip | Open Threat Exchange (OTX) - IP Cache | Open Thread Exchange (OTX) - IP | Edit Delete |
| Open Thread Exchange (OTX) - Domain | This is the lookup table for AlienVault's Open Thread Exchange platform, containing crowd-sourced IoCs (Indicators of Compromise). For more information see https://otx.alienvault.com. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | otx-api-domain | Open Threat Exchange (OTX) - Domain Cache | Open Thread Exchange (OTX) - Domain | Edit Delete |

# Configured lookup tables 7 total

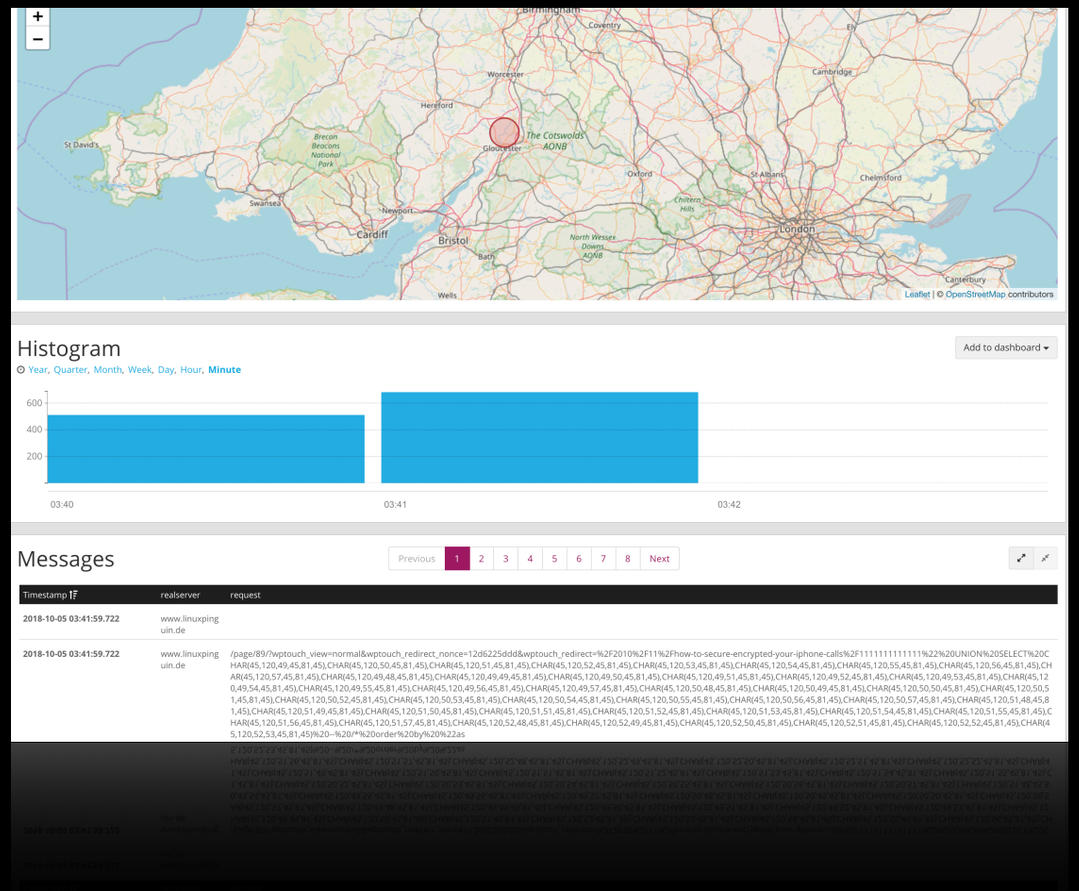
Enter search query... | Search | Reset | Create lookup table

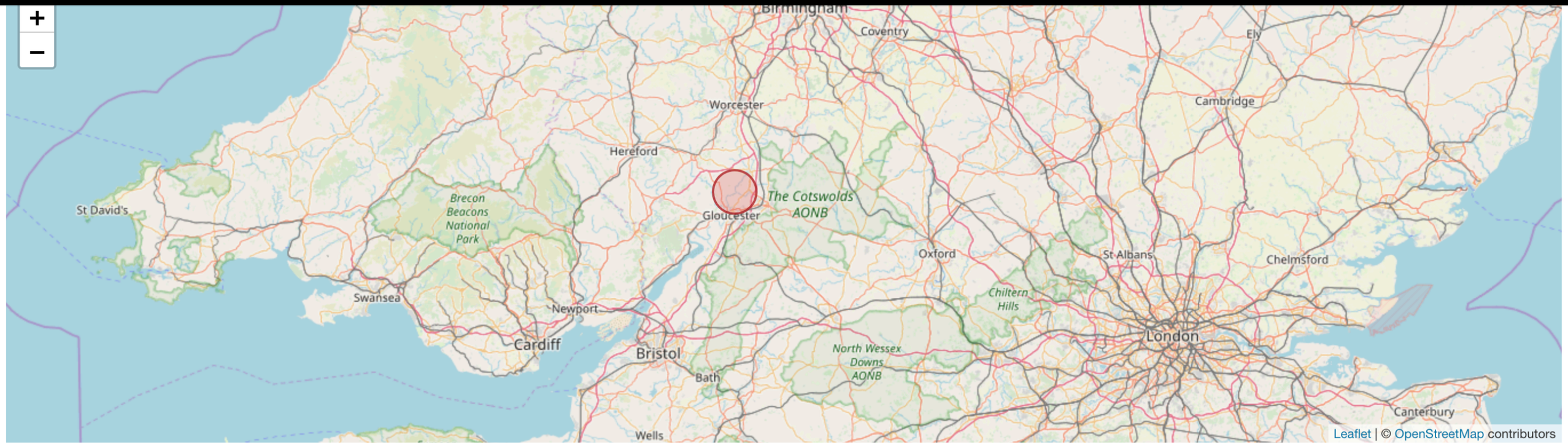
Show: 10

| Title | Description | Name | Cache | Data Adapter | Actions |
|---|---|---|---|---|---|
| abuse.ch Ransomware IP | This is the lookup table for the abuse.ch ransomware IP Tracker, listing infrastructure by IP which is used for ransomware. For more information see https://ransomwaretracker.abuse.ch. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | abuse-ch-ransomware-ip | Threat Intel Uncached Adapters | abuse.ch ransomware IP | Edit Delete |
| abuse.ch Ransomware Domains | This is the lookup table for the abuse.ch ransomware Domain Tracker, listing infrastructure by domain names which are used for ransomware. For more information see https://ransomwaretracker.abuse.ch. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | abuse-ch-ransomware-domains | Threat Intel Uncached Adapters | abuse.ch ransomware Domains | Edit Delete |
| Whois | This is the lookup table for the WHOIS database, listing registered users of Internet resources like IPs, Netblocks or Domain Names. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | whois | Whois Cache | Whois | Edit Delete |
| Tor Exit Node List | This is the lookup table for the TOR (The Onion Router) Exit Node List, listing Exit Nodes of the TOR Network . This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | tor-exit-node-list | Threat Intel Uncached Adapters | Tor Exit Node | Edit Delete |
| Spamhaus DROP | This is the lookup table for Spamhaus' DROP (Don't Route Or Peer) list, containing netblocks which are "hijacked" or leased by professional spam or cyber-crime operations. For more information see https://www.spamhaus.org/drop. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | spamhaus-drop | Spamhaus (E)DROP Cache | Spamhaus DROP | Edit Delete |
| Open Thread Exchange (OTX) - IP | This is the lookup table for AlienVault's Open Thread Exchange platform, containing crowd-sourced IoCs (Indicators of Compromise). For more information see https://otx.alienvault.com. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | otx-api-ip | Open Threat Exchange (OTX) - IP Cache | Open Thread Exchange (OTX) - IP | Edit Delete |
| Open Thread Exchange (OTX) - Domain | This is the lookup table for AlienVault's Open Thread Exchange platform, containing crowd-sourced IoCs (Indicators of Compromise). For more information see https://otx.alienvault.com. This lookup table is used internally by Graylog's Threat Intel Plugin. Do not delete it manually. | otx-api-domain | Open Threat Exchange (OTX) - Domain Cache | Open Thread Exchange (OTX) - Domain | Edit Delete |

# Analyse & Research

- Durchsuche mit GrayLog die TeraBytes an Logdaten.
- Entdecke und analysiere die wichtigen Punkte.
- Was war kam da aus Glocester?

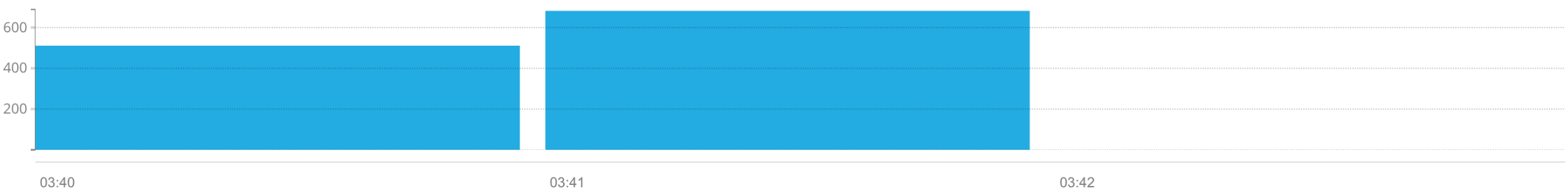





# Histogram

Add to dashboard

Year, Quarter, Month, Week, Day, Hour, **Minute**



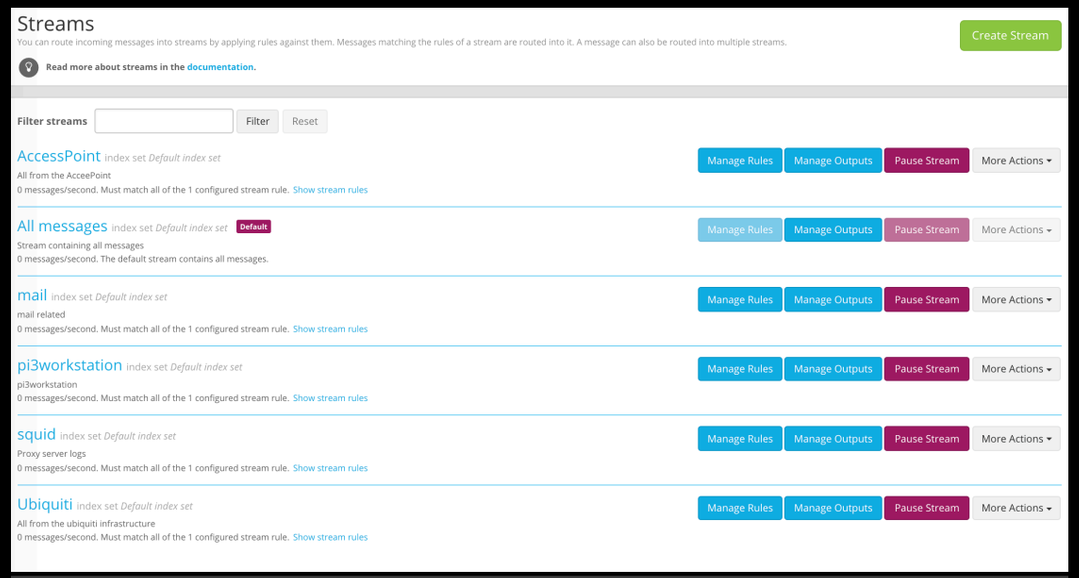

# Messages

Previous 1 2 3 4 5 6 7 8 Next

| Timestamp | realserver | request |
|---|---|---|
| **2018-10-05 03:41:59.722** | www.linuxpinguin.de | |
| **2018-10-05 03:41:59.722** | www.linuxpinguin.de | /page/89/?wptouch_view=normal&wptouch_redirect_nonce=12d6225ddd&wptouch_redirect=%2F2010%2F11%2Fhow-to-secure-encrypted-your-iphone-calls%2F1111111111111%22%20UNION%20SELECT%20CHAR(45,120,49,45,81,45),CHAR(45,120,50,45,81,45),CHAR(45,120,51,45,81,45),CHAR(45,120,52,45,81,45),CHAR(45,120,53,45,81,45),CHAR(45,120,54,45,81,45),CHAR(45,120,55,45,81,45),CHAR(45,120,56,45,81,45),CHAR(45,120,57,45,81,45),CHAR(45,120,49,48,45,81,45),CHAR(45,120,49,49,45,81,45),CHAR(45,120,49,50,45,81,45),CHAR(45,120,49,51,45,81,45),CHAR(45,120,49,52,45,81,45),CHAR(45,120,49,53,45,81,45),CHAR(45,120,49,54,45,81,45),CHAR(45,120,49,55,45,81,45),CHAR(45,120,49,56,45,81,45),CHAR(45,120,49,57,45,81,45),CHAR(45,120,50,48,45,81,45),CHAR(45,120,50,49,45,81,45),CHAR(45,120,50,50,45,81,45),CHAR(45,120,50,51,45,81,45),CHAR(45,120,50,52,45,81,45),CHAR(45,120,50,53,45,81,45),CHAR(45,120,50,54,45,81,45),CHAR(45,120,50,55,45,81,45),CHAR(45,120,50,56,45,81,45),CHAR(45,120,50,57,45,81,45),CHAR(45,120,51,48,45,81,45),CHAR(45,120,51,49,45,81,45),CHAR(45,120,51,50,45,81,45),CHAR(45,120,51,51,45,81,45),CHAR(45,120,51,52,45,81,45),CHAR(45,120,51,53,45,81,45),CHAR(45,120,51,54,45,81,45),CHAR(45,120,51,55,45,81,45),CHAR(45,120,51,56,45,81,45),CHAR(45,120,51,57,45,81,45),CHAR(45,120,52,48,45,81,45),CHAR(45,120,52,49,45,81,45),CHAR(45,120,52,50,45,81,45),CHAR(45,120,52,51,45,81,45),CHAR(45,120,52,52,45,81,45),CHAR(45,120,52,53,45,81,45)%20--%20/*%20order%20by%20%22as |

# Analyse & Research

- Mit den Streams von GrayLog kann man Zugriff auf einzelne Datenströme ermöglichen.
- Auf diese kann man dann mit ACL geschützt Benutzer zugreifen lassen.



# Streams

You can route incoming messages into streams by applying rules against them. Messages matching the rules of a stream are routed into it. A message can also be routed into multiple streams.

Create Stream

**Read more about streams in the documentation.**

**Filter streams** Filter Reset

## AccessPoint index set *Default index set*

Manage Rules | Manage Outputs | Pause Stream | More Actions

All from the AcceePoint

0 messages/second. Must match all of the 1 configured stream rule. Show stream rules

## All messages index set *Default index set* Default

Manage Rules | Manage Outputs | Pause Stream | More Actions

Stream containing all messages

0 messages/second. The default stream contains all messages.

## mail index set *Default index set*

Manage Rules | Manage Outputs | Pause Stream | More Actions

mail related

0 messages/second. Must match all of the 1 configured stream rule. Show stream rules

## pi3workstation index set *Default index set*

Manage Rules | Manage Outputs | Pause Stream | More Actions

pi3workstation

0 messages/second. Must match all of the 1 configured stream rule. Show stream rules

## squid index set *Default index set*

Manage Rules | Manage Outputs | Pause Stream | More Actions

Proxy server logs

0 messages/second. Must match all of the 1 configured stream rule. Show stream rules

## Ubiquiti index set *Default index set*

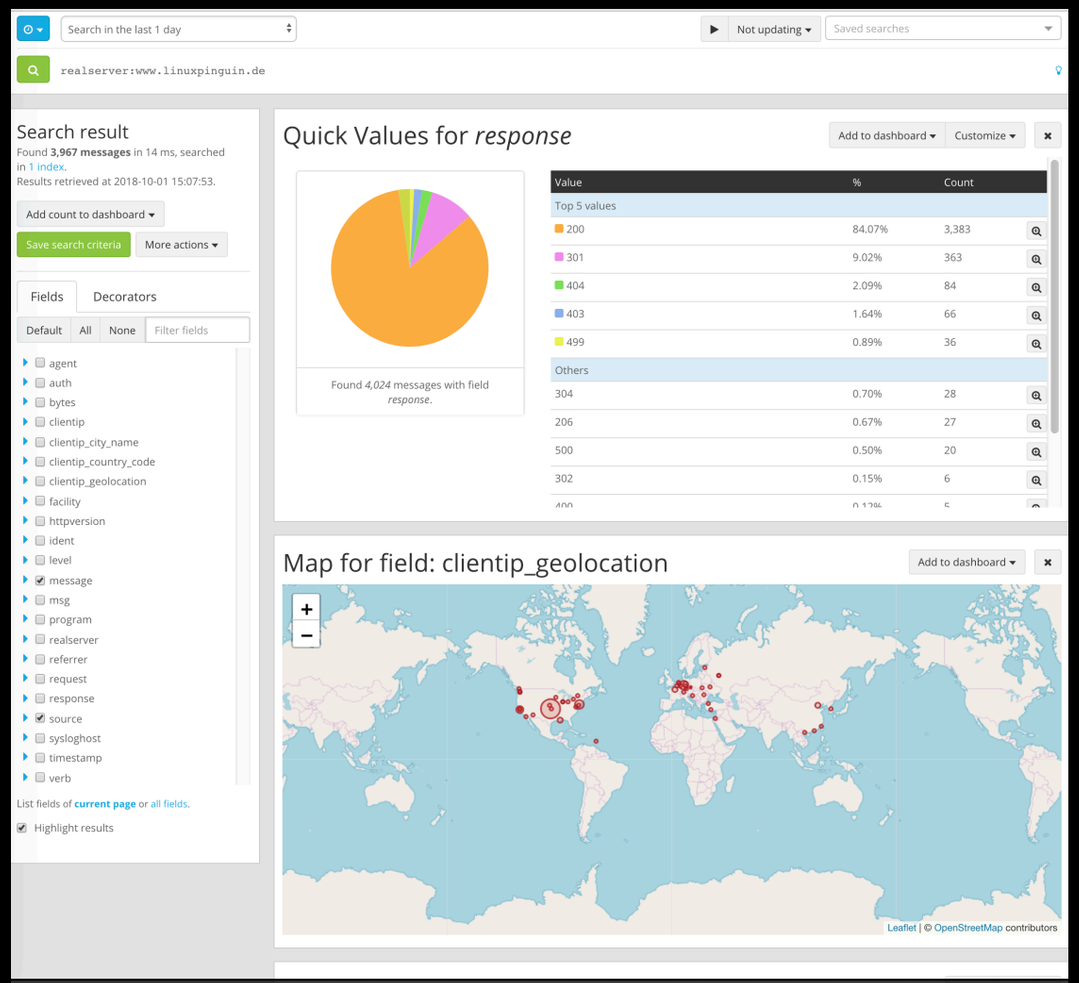
Manage Rules | Manage Outputs | Pause Stream | More Actions

All from the ubiquiti infrastructure

0 messages/second. Must match all of the 1 configured stream rule. Show stream rules

# Drill down & Visualize

- Grab dich mit GrayLog in die Tiefe deiner Daten.
- GeoIP Karten und Tortendiagramme geben einen guten  Überblick.



Search in the last 1 day

Not updating

Saved searches

realserver:www.linuxpinguin.de

## Search result

Found **3,967 messages** in 14 ms, searched in 1 index.
Results retrieved at 2018-10-01 15:07:53.

Add count to dashboard

Save search criteria

More actions

Fields | Decorators

Default | All | None | Filter fields

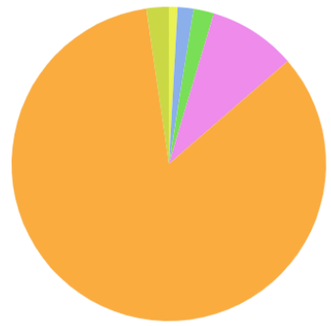
- agent
- auth
- bytes
- clientip
- clientip_city_name
- clientip_country_code
- clientip_geolocation
- facility
- httpversion
- ident
- level
- [x] message
- msg
- program
- realserver
- referrer
- request
- response
- [x] source
- sysloghost
- timestamp
- verb

List fields of **current page** or all fields.

[x] Highlight results

## Quick Values for *response*

Add to dashboard | Customize



Found *4,024* messages with field *response*.

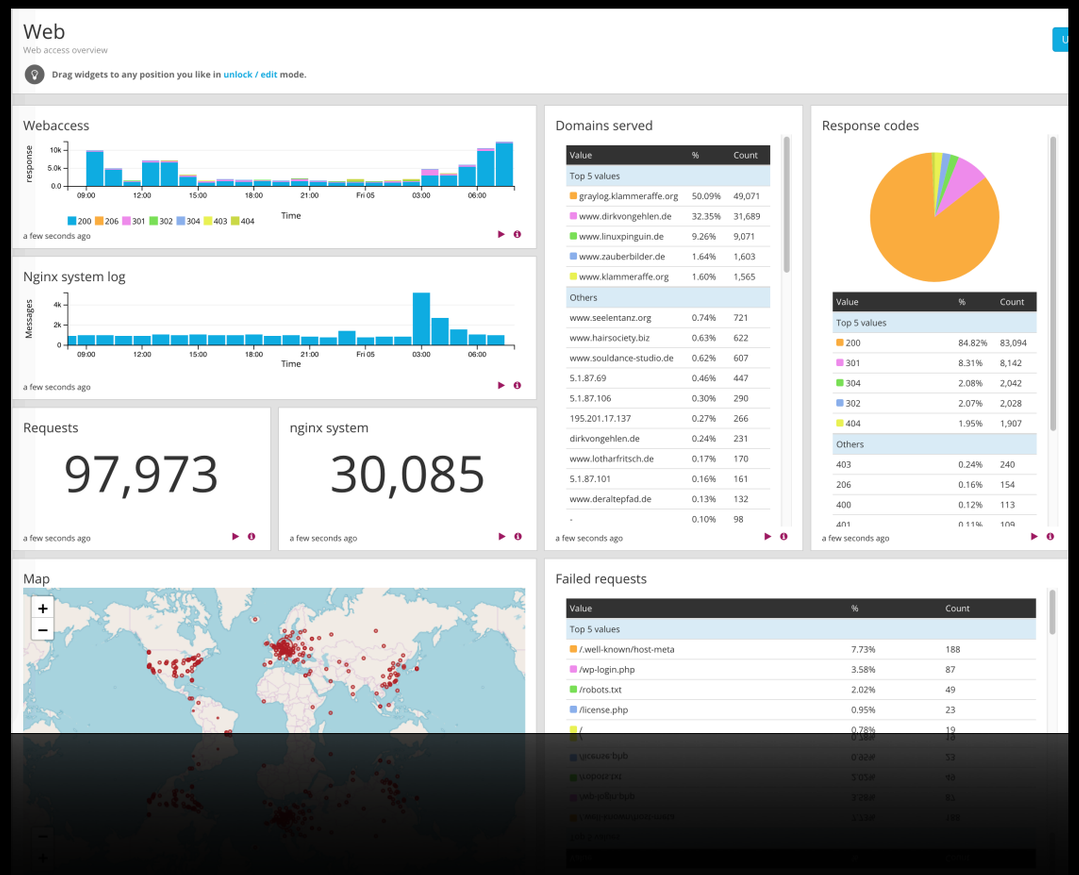
| Value | % | Count |
|---|---|---|
| Top 5 values | | |
| 200 | 84.07% | 3,383 |
| 301 | 9.02% | 363 |
| 404 | 2.09% | 84 |
| 403 | 1.64% | 66 |
| 499 | 0.89% | 36 |
| Others | | |
| 304 | 0.70% | 28 |
| 206 | 0.67% | 27 |
| 500 | 0.50% | 20 |
| 302 | 0.15% | 6 |
| 400 | 0.12% | 5 |

## Map for field: clientip_geolocation

Add to dashboard

# Drill down & Visualize

- Dashboards kann man mit GrayLog ziemlich einfach zusammen stellen.
- Und sie geben einen guten Rundumblick auf die zeitliche Entwicklung.

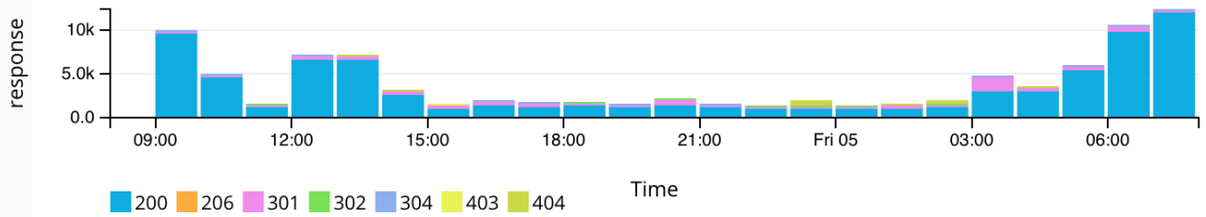


# Web

Web access overview

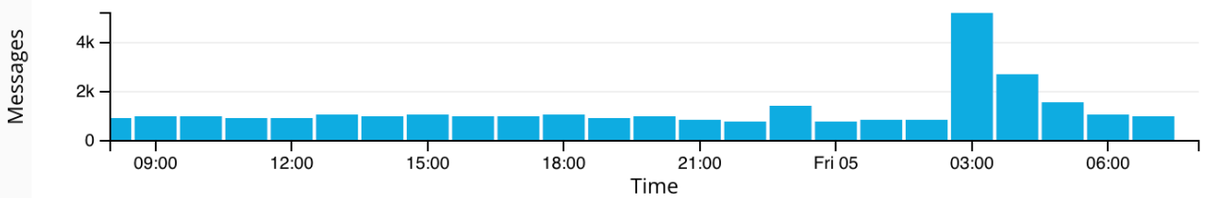
Drag widgets to any position you like in unlock / edit mode.

## Webaccess




a few seconds ago

## Nginx system log




a few seconds ago

## Requests

97,973

a few seconds ago

## nginx system

30,085

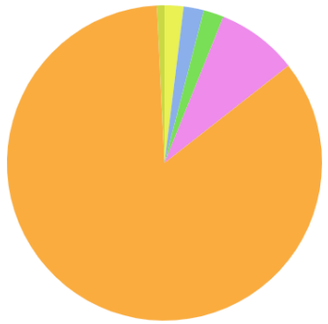
a few seconds ago

## Domains served

| Value | % | Count |
|---|---|---|
| Top 5 values | | |
| graylog.klammeraffe.org | 50.09% | 49,071 |
| www.dirkvongehlen.de | 32.35% | 31,689 |
| www.linuxpinguin.de | 9.26% | 9,071 |
| www.zauberbilder.de | 1.64% | 1,603 |
| www.klammeraffe.org | 1.60% | 1,565 |
| Others | | |
| www.seelentanz.org | 0.74% | 721 |
| www.hairsociety.biz | 0.63% | 622 |
| www.souldance-studio.de | 0.62% | 607 |
| 5.1.87.69 | 0.46% | 447 |
| 5.1.87.106 | 0.30% | 290 |
| 195.201.17.137 | 0.27% | 266 |
| dirkvongehlen.de | 0.24% | 231 |
| www.lotharfritsch.de | 0.17% | 170 |
| 5.1.87.101 | 0.16% | 161 |
| www.deraltepfad.de | 0.13% | 132 |
| - | 0.10% | 98 |

a few seconds ago

## Response codes



| Value | % | Count |
|---|---|---|
| Top 5 values | | |
| 200 | 84.82% | 83,094 |
| 301 | 8.31% | 8,142 |
| 304 | 2.08% | 2,042 |
| 302 | 2.07% | 2,028 |
| 404 | 1.95% | 1,907 |
| Others | | |
| 403 | 0.24% | 240 |
| 206 | 0.16% | 154 |
| 400 | 0.12% | 113 |
| 401 | 0.11% | 109 |

a few seconds ago

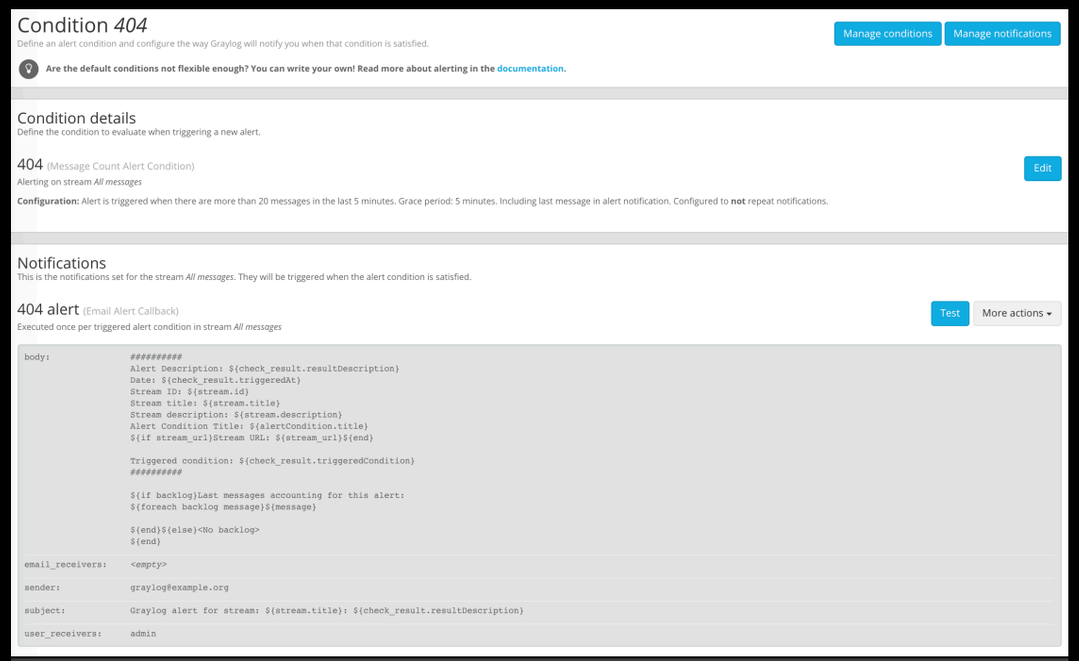
## Map

## Failed requests

| Value | % | Count |
|---|---|---|
| Top 5 values | | |
| /.well-known/host-meta | 7.73% | 188 |
| /wp-login.php | 3.58% | 87 |
| /robots.txt | 2.02% | 49 |
| /license.php | 0.95% | 23 |
| / | 0.78% | 19 |

# Alert & Trigger

- Mit Alerts kann GrayLog dann eine per Email oder anderen Wege (Slack, etc.) über Probleme informieren.



# Condition *404*

Define an alert condition and configure the way Graylog will notify you when that condition is satisfied.

Manage conditions | Manage notifications

**Are the default conditions not flexible enough? You can write your own! Read more about alerting in the documentation.**

## Condition details

Define the condition to evaluate when triggering a new alert.

### 404 (Message Count Alert Condition)

Edit

Alerting on stream *All messages*

**Configuration:** Alert is triggered when there are more than 20 messages in the last 5 minutes. Grace period: 5 minutes. Including last message in alert notification. Configured to **not** repeat notifications.

## Notifications

This is the notifications set for the stream *All messages*. They will be triggered when the alert condition is satisfied.

### 404 alert (Email Alert Callback)

Test | More actions

Executed once per triggered alert condition in stream *All messages*

```
body:               ##########
                    Alert Description: ${check_result.resultDescription}
                    Date: ${check_result.triggeredAt}
                    Stream ID: ${stream.id}
                    Stream title: ${stream.title}
                    Stream description: ${stream.description}
                    Alert Condition Title: ${alertCondition.title}
                    ${if stream_url}Stream URL: ${stream_url}${end}

                    Triggered condition: ${check_result.triggeredCondition}
                    ##########

                    ${if backlog}Last messages accounting for this alert:
                    ${foreach backlog message}${message}

                    ${end}${else}<No backlog>
                    ${end}

email_receivers:    <empty>

sender:             graylog@example.org

subject:            Graylog alert for stream: ${stream.title}: ${check_result.resultDescription}

user_receivers:     admin
```

Zentrales Logmanagement

ACL basierter Zugriff

Suchmaschine

Dashboards

Imports

Exports

Alerting

Geo-IP

JSON

GrokPatterns

Marketplace

Plugins

Archivierung

Elasticsearch

Collect & Process

Analyse & Research

# GrayLog

Drill Down & Visualize

Alert & Trigger

Apache Kafka

GELF

TCP

UDP

VPN

Skalierbar

Site-resilient

CSV

Syslog

Raw-Sockets

RFC 3164

RFC 5424

CEF

AWS

CloudTrail

PacketBeat

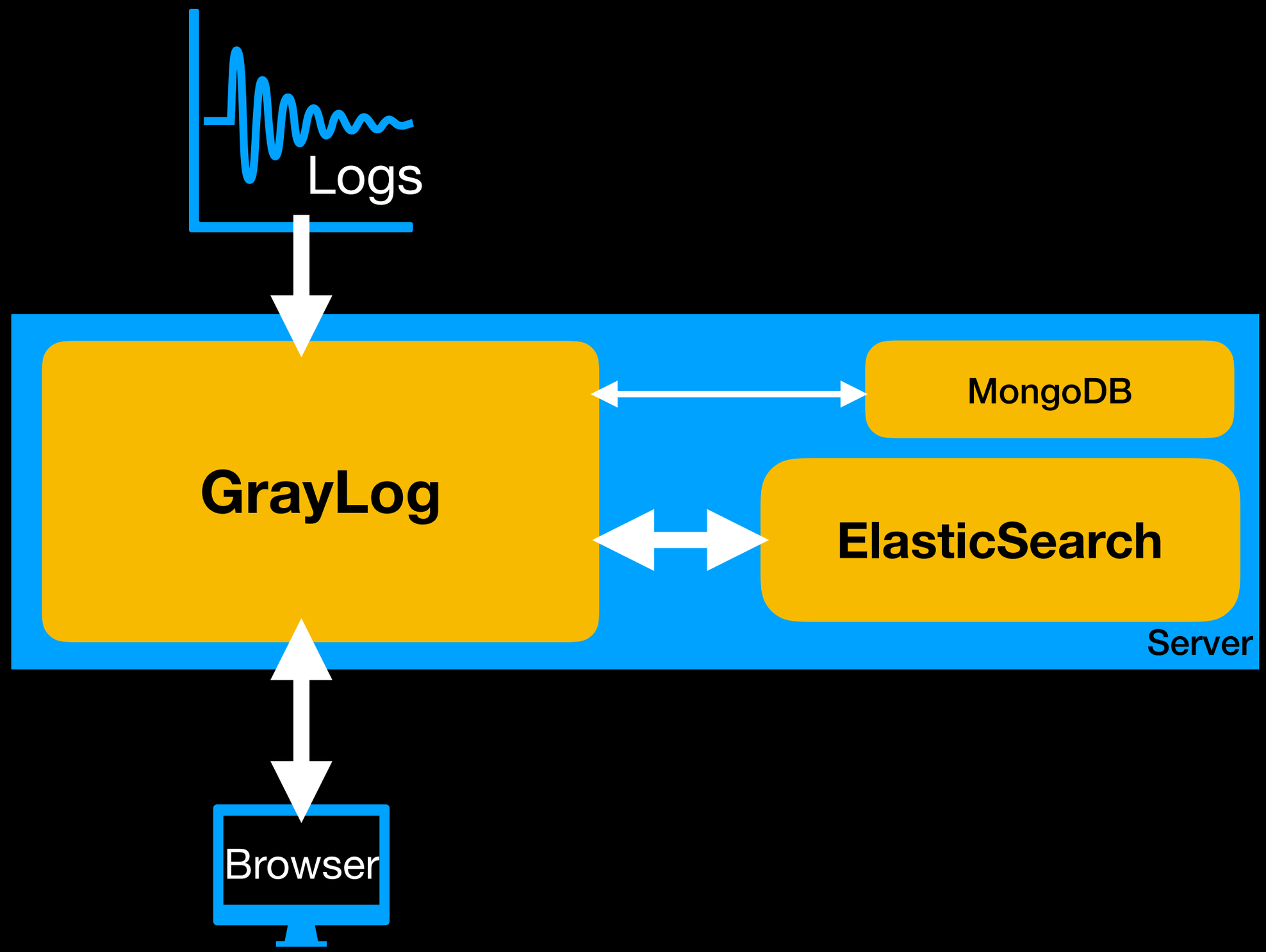
WinlogBeat

FileBeat

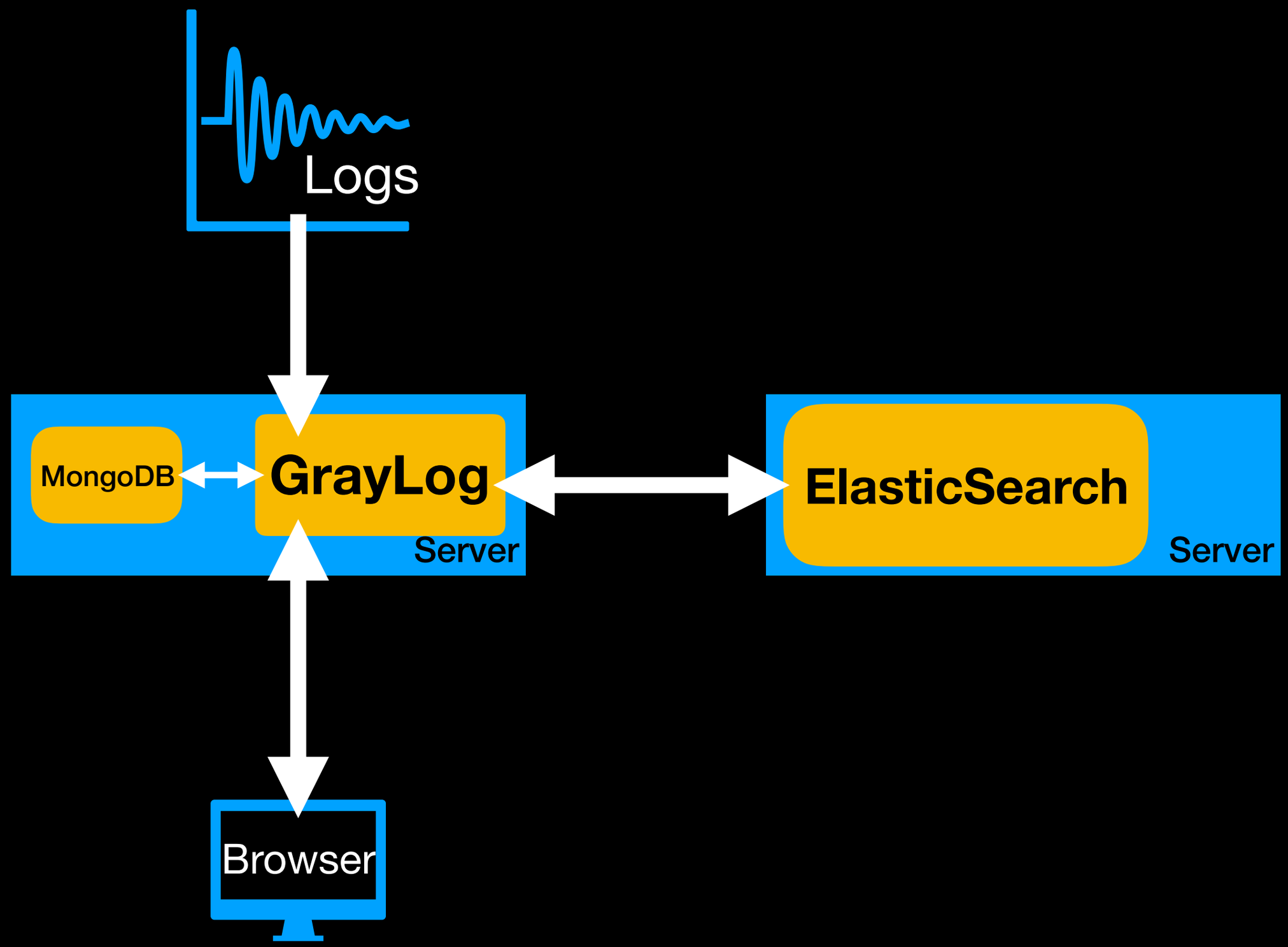
# GrayLog

- **Server Aufbau**
  - Einfacher Server
  - Etwas aufwendiger
  - Vollausbau

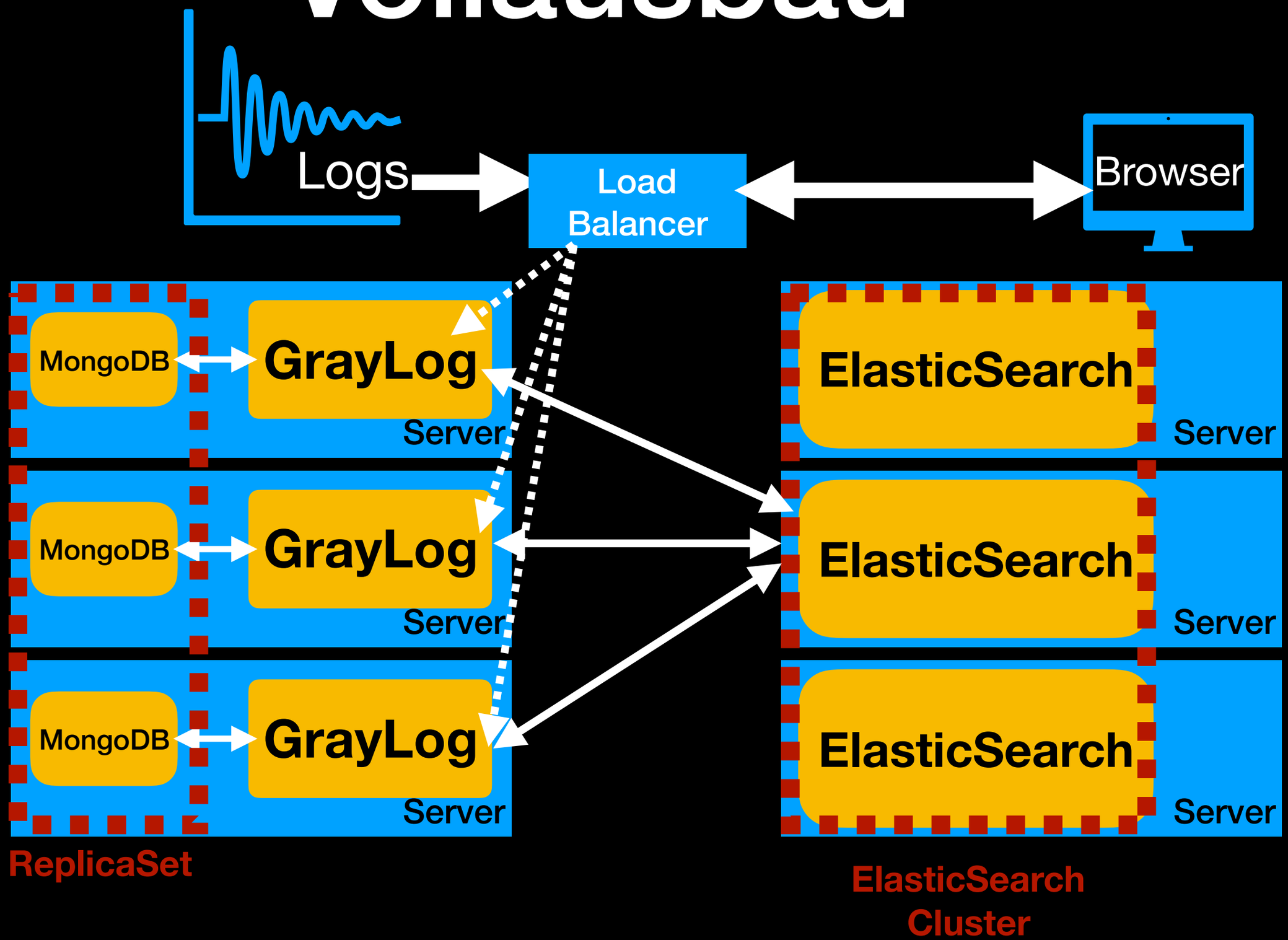
# Einfacher Server



# Etwas aufwendiger



# Vollausbau


Logs
Load Balancer
Browser
MongoDB
GrayLog
Server
MongoDB
GrayLog
Server
MongoDB
GrayLog
Server
ElasticSearch
Server
ElasticSearch
Server
ElasticSearch
Server
ReplicaSet
ElasticSearch Cluster

# GrayLog

## Ein Anwendungsbeispiel

# GrayLog

- Apache Statistiken erfassen
- JSON als Datenformat
- Per Syslog melden
- JSON Felder in GrayLog anlegen
- Stream anlegen
- Dashboard anlegen
- Alarmierung bei Ausfall

# Apache Statistiken erfassen

- Ein PHP-Skript konvertiert die Ausgabe von: ***http://127.0.0.1/server-status?auto***

- Das wird minütlich über cron aufgerufen.

```
Total Accesses: 58
Total kBytes: 2308
CPULoad: 5.55869
Uptime: 213
ReqPerSec: .2723
BytesPerSec: 11095.7
BytesPerReq: 40748.1
BusyWorkers: 1
IdleWorkers: 6
Scoreboard: ____W__.....................................................
.......................................................................
.......................................................................
...................
root@atorg-fra:~#
```

# Umwandlung in JSON

- Die erzeugte Datenstruktur wird per **JSON** weiterverarbeitet

```
Array
(
    [curlTotalTime] => 0.000386
    [TotalAccesses] => 135
    [TotalkBytes] => 14685
    [CPULoad] => 5.91463
    [Uptime] => 246
    [ReqPerSec] => .548781
    [BytesPerSec] => 61127.8
    [BytesPerReq] => 111388
    [BusyWorkers] => 4
    [IdleWorkers] => 4
    [Scoreboard] => W__W_KK_.....................................................
.......................................................................................
.......................................................................................
...........................
)
apachestats[4446]: {"curlTotalTime":0.000386,"TotalAccesses":135,"TotalkBytes":1468
5,"CPULoad":5.91463,"Uptime":246,"ReqPerSec":0.548781,"BytesPerSec":61127.8,"BytesP
erReq":111388,"BusyWorkers":4,"IdleWorkers":4,"Scoreboard":"W__W_KK_..............
.......................................................................................
.......................................................................................
......................................................................................"}
```

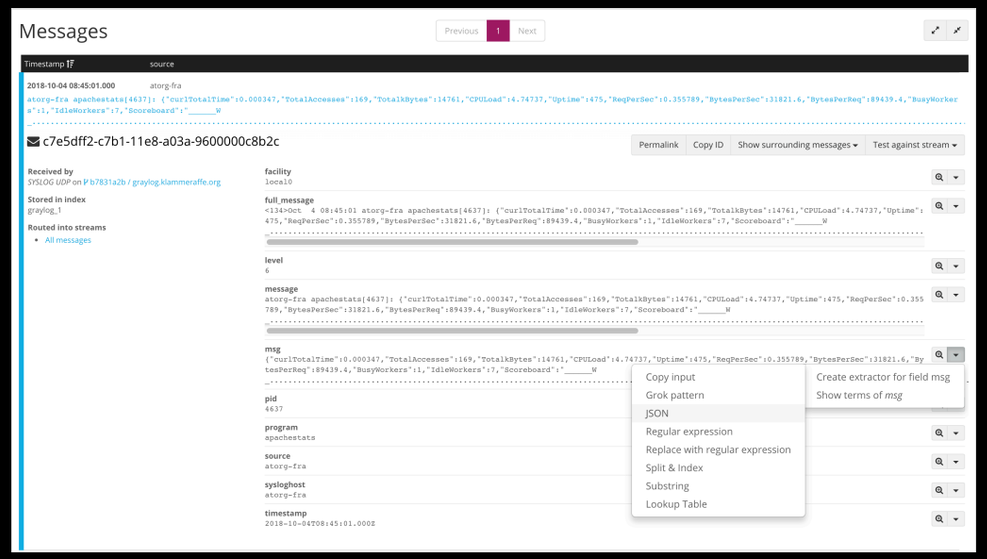
# Per Syslog melden

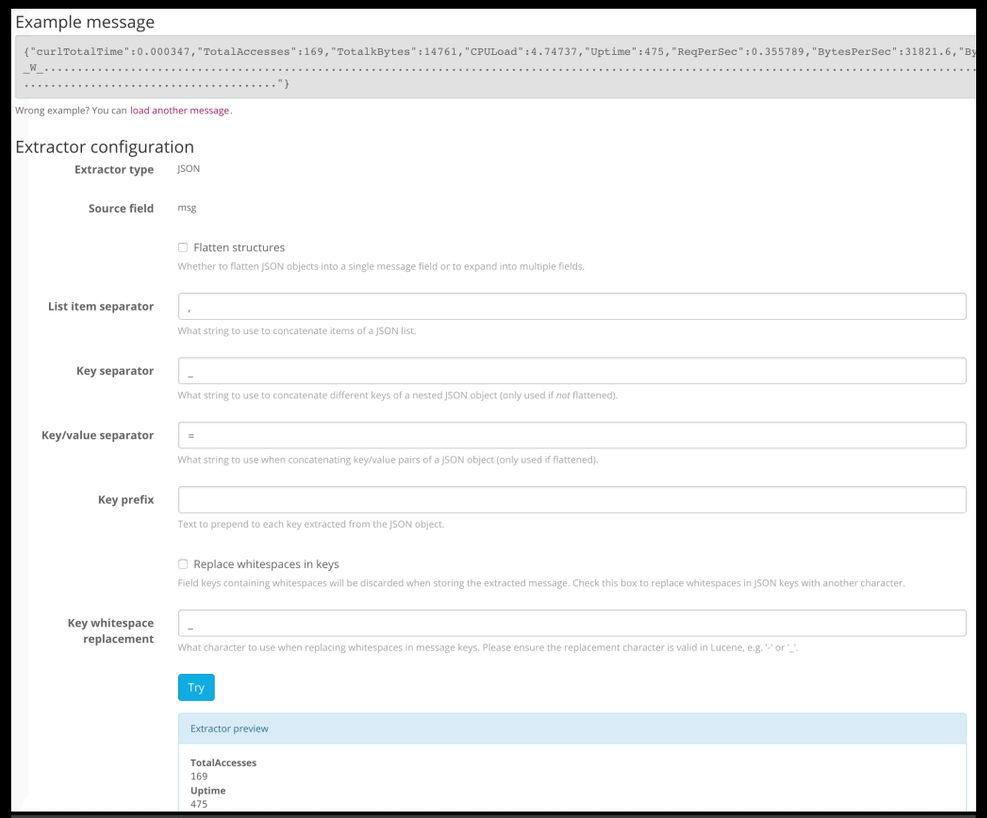
- Per **syslog** (514/udp) wird es dann an den GrayLog Server geschickt.
- Hier wäre auch 514/tcp oder viele andere Methoden möglich

```
Oct  4 08:38:11 atorg-fra apachestats[4295]: {"curlTotalTime":0.000467,"TotalAccess
es":23,"TotalkBytes":23,"CPULoad":7.83333,"Uptime":66,"ReqPerSec":0.348485,"BytesPe
rSec":356.848,"BytesPerReq":1024,"BusyWorkers":1,"IdleWorkers":6,"Scoreboard":"___W
___.......................................................................
.......................................................................
.......................................................................
..."}
Oct  4 08:41:11 atorg-fra apachestats[4446]: {"curlTotalTime":0.000386,"TotalAccess
es":135,"TotalkBytes":14685,"CPULoad":5.91463,"Uptime":246,"ReqPerSec":0.548781,"By
tesPerSec":61127.8,"BytesPerReq":111388,"BusyWorkers":4,"IdleWorkers":4,"Scoreboard
":"W__W_KK_...............................................................
.......................................................................
.......................................................................
.........."}
```

# JSON zu GrayLog Felder

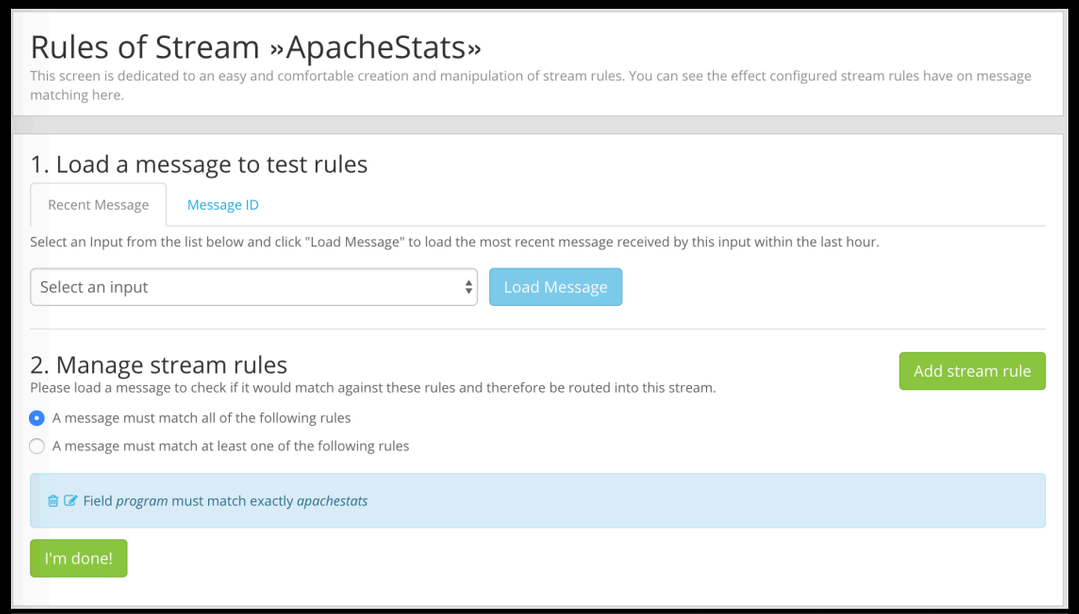
- Durch die Anwendung des Filters wird aus dem **JSON** Eintrag einzelne **Felder**
- Diese können dann gezielt durchsucht werden.



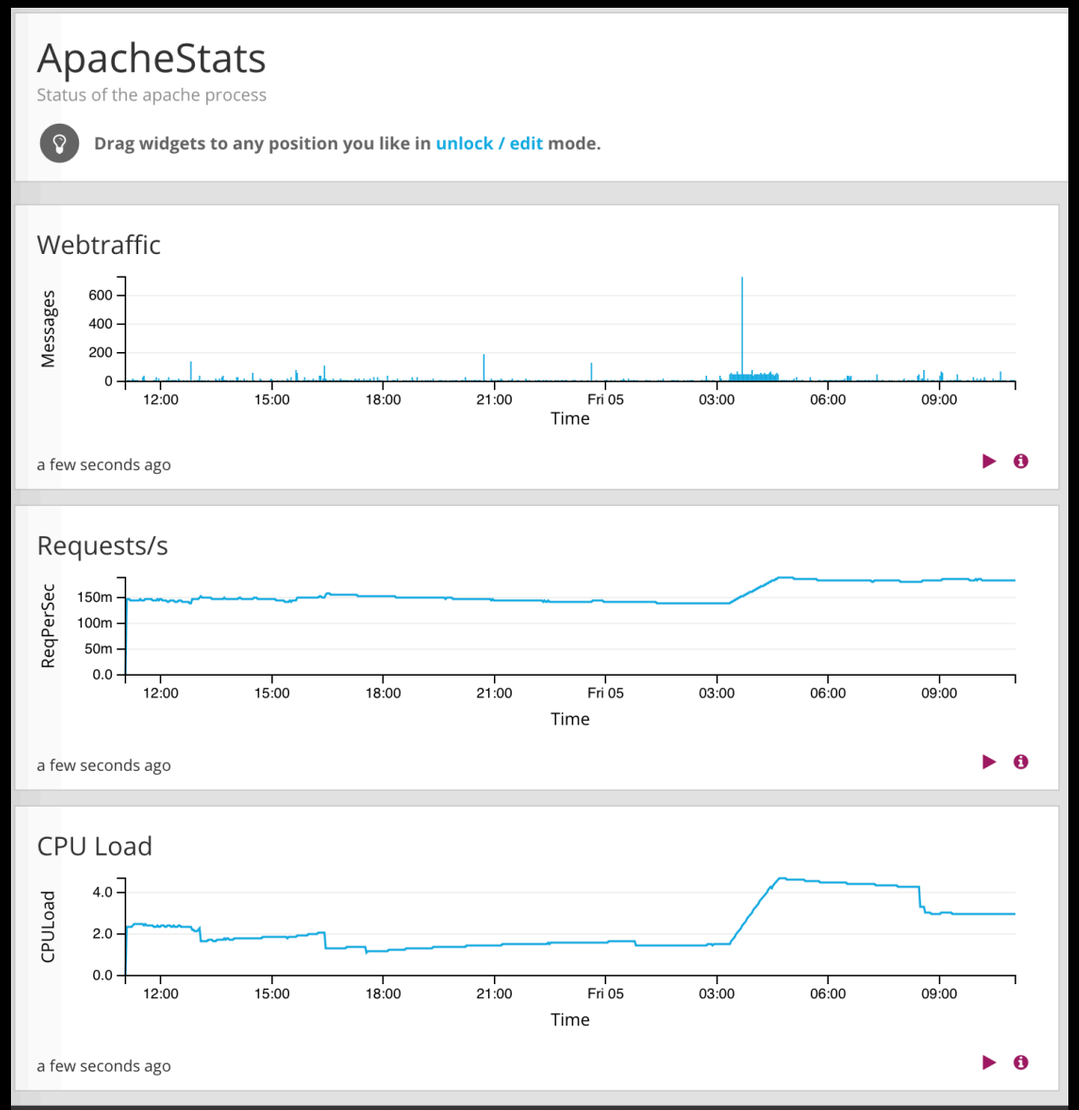
# Stream anlegen

- Ein **Stream** filtert alle relevanten Datenquellen in eine Datensicht.
- Darauf können wir dann unser Dashboard bauen
- Und wir können diesen **Stream** nur bestimmten Nutzergruppen sichtbar machen.



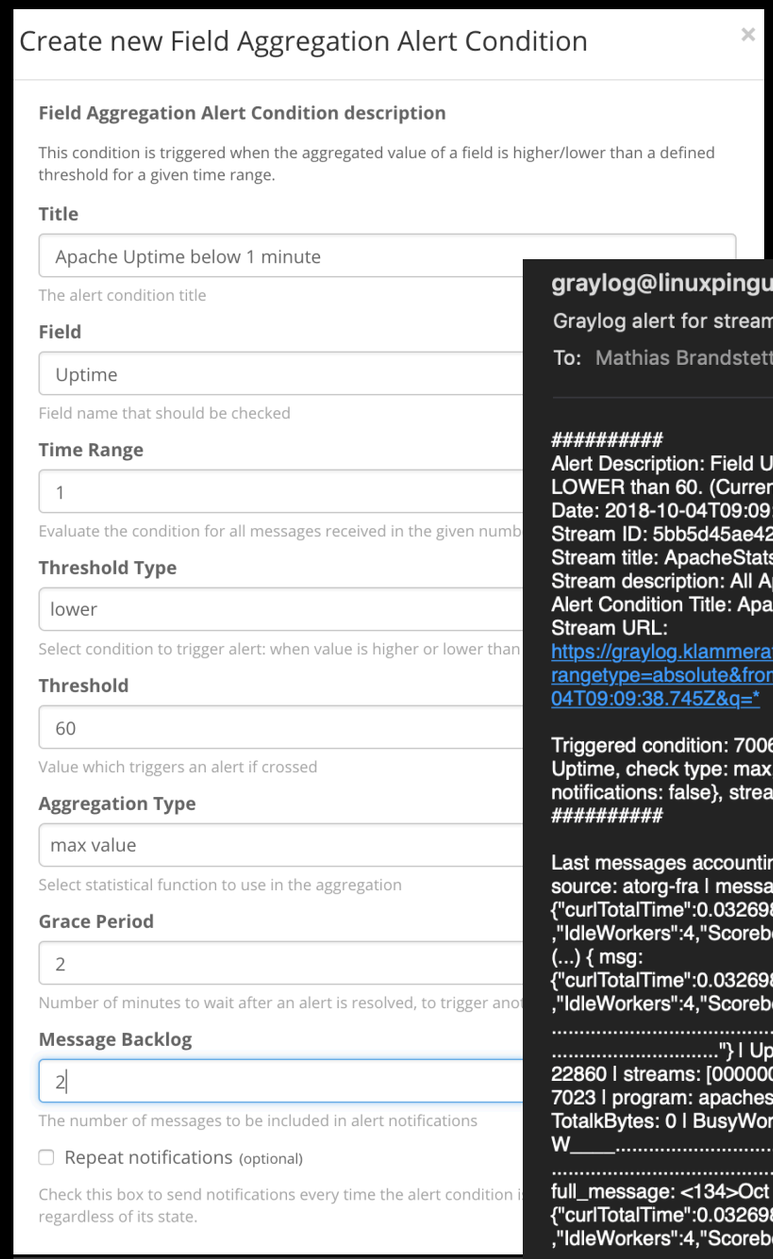
# Dashboard

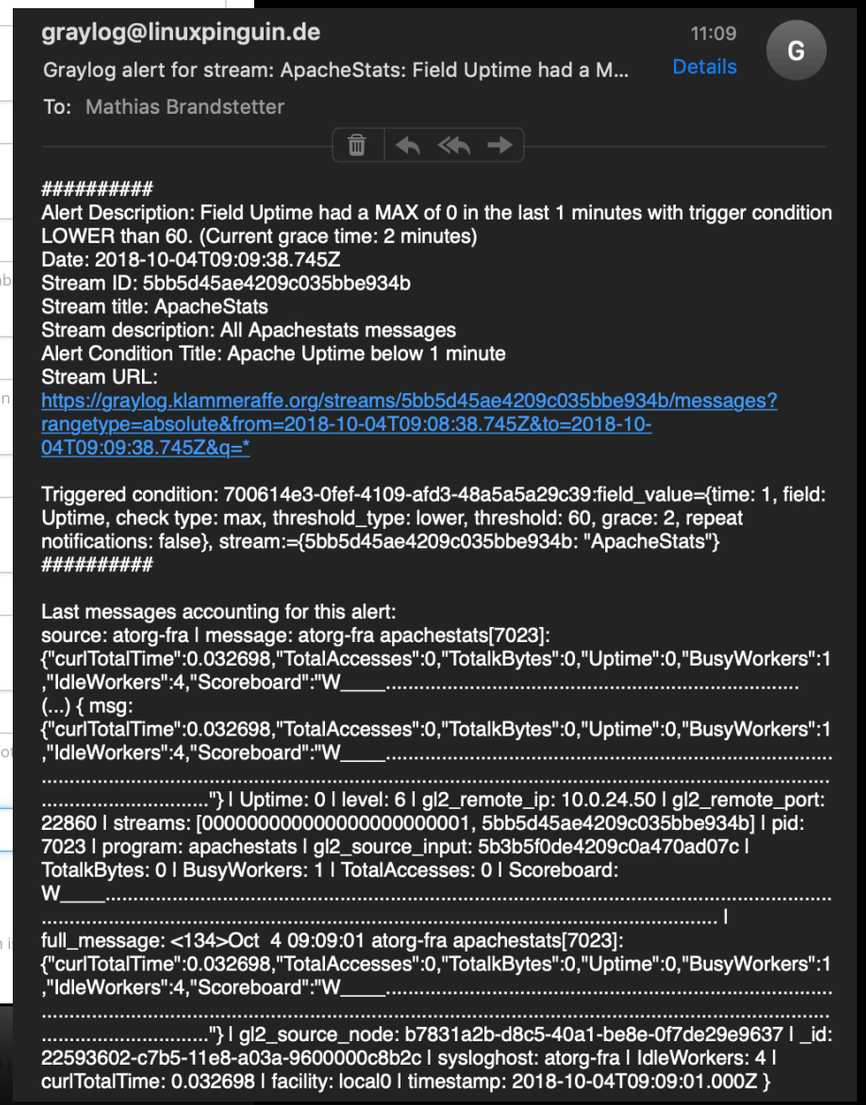
- Mit den Feldern aus dem Stream erzeugen wir dann folgendes Dashboard zur Übersicht.
- Auch dieses können wir nur bestimmten Nutzergruppen sichtbar machen.



# Alarmierung

- Bauen wir nun noch die Alarmierung ein.
- Wann immer nun von uns festgelegte Parameter nicht eingehalten werden, gibt es eine Nachricht.



# Fragen?

Mathias Brandstetter
info@linuxpinguin.de

@filid