
GRAYLOG

EINFÜHRUNG (1)

Unter Logging versteht man in der Informatik generell das (automatische) Speichern von Prozessen oder Datenänderungen. Diese werden in sogenannten Logdateien hinterlegt bzw. gespeichert.

Wikipedia - Logging

EINFÜHRUNG (2)

Außer dem Betriebssystem selbst schreiben meist Hintergrundprogramme […] in Logdateien, um Aktionsmeldungen, Fehlermeldungen und Hinweise persistent (dauernd) oder temporär verfügbar zu halten. Ähnliches gilt für Installationsprogramme, Firewalls, Virenscanner und dergleichen.

Wikipedia - Logging

EINFÜHRUNG (3)

Logs geben die Möglichkeit Dinge zu einem späteren Zeitpunkt nachzuvollziehen.

EINFÜHRUNG (4)

SECURITY (1)

A theme in this article will be: "what separates standard incidents from horrifying nightmares?"

A good or bad story around logging will dictate the rest of the incident.

Learning From A Year of Security Breaches

SECURITY (2)

I recommend that any security or infrastructure team putting off a comprehensive approach to logging drop nearly everything to invest in it.

Learning From A Year of Security Breaches

WHAT'S IN A LOG MESSAGE? (1)

Minimale Lognachricht:

- Zeitstempel (idealerweise ISO 8601-kompatibel)
- Daten

WHAT'S IN A LOG MESSAGE? (2)

```
Mar 27 18:15:23 Example Message
```

WHAT'S IN A LOG MESSAGE? (2)

```
2017-03-27T16:15:23.012Z Example Message
```

WHAT'S IN A LOG MESSAGE? (3)

```
2017-03-27T16:15:23.012Z joschi-mbp15 joschi[47088]: \
  Example Message
```

WHAT'S IN A LOG MESSAGE? (4)

```
{
  "version": "1.1",
  "host": "joschi-mbp15",
  "short_message": "Example Message",
  "full_message": "Multiline\nStacktrace\nhere",
  "timestamp": 1490631323.012,
  "level": 6,
  "_user": "joschi",
  "_user_id": 1001,
  "_process_id": "47088",
  "_some_env_var": "bar"
}
```

STRUCTURED LOGGING

- Strukturierte Informationen in einer Lognachricht
- Idealerweise mit definiertem Schema (Datentyp, Datenbereich etc.)
- Structured Syslog: RFC 5424
- Alternativen: GELF, CEF (Common Event Format), JSON

BEST PRACTICES

- Structured Logging verwenden
- Daten normalisieren und gemeinsames Vokabular für alle Systeme definieren
- Logmeldungen an zentraler Stelle sammeln
- Sinnvolle Daten loggen (nein, keine 32 GiB große Coredumps…)

GRAYLOG

- Freie Software (kostenlos und Open Source)
- Einfach zu installieren
- Leistungsfähig (bei entsprechender Hardware)
- Erweiterbar durch Plugins

GRAYLOG (KOMMERZIELLER EINSATZ)

- Kommerzieller Support
- Enterprise Features (Archiving, Audit Log)

GRAYLOG (INPUTS)

- GELF (UDP, TCP, AMQP, Kafka)
- Syslog (UDP, TCP, AMQP, Kafka)
- Raw/Plaintext (UDP, TCP, AMQP, Kafka)
- Beats (Filebeat, Metricbeat, etc.)

GRAYLOG (INPUTS, COMMUNITY)

- Redis
- NATS
- MQTT
- SNMP
- Netflow
- …und viele mehr im Graylog Marketplace

graylog Marketplace

Explore | Submit | Sign out

Hundreds of Add-ons for Graylog.

How would you like to extend Graylog today?

Search Marketplace

Browse Add-ons by Type

- Plugin
- Content Pack
- GELF Library
- Other Solutions

Space weather input

free!

Plugin v1.0

Ever needed a proof that a solar storm made a bit flip and your code crash? Now you can! Correlate proton density to the response time of your app and the ion temperature to your exception rate.

space weather fun

lennartkoopmann

Download from Github | View on Github | 0 | ☆ 59

Published	Last Push	Marketplace Rating	Discussion
23 Oct 16:11	28 Apr 05:44		3 Comments

Readme from Github

Graylog Spaceweather plugin (Solar data)

(This is not actually providing any value at all - except fun and the possibility to decently nerd out)

graylog

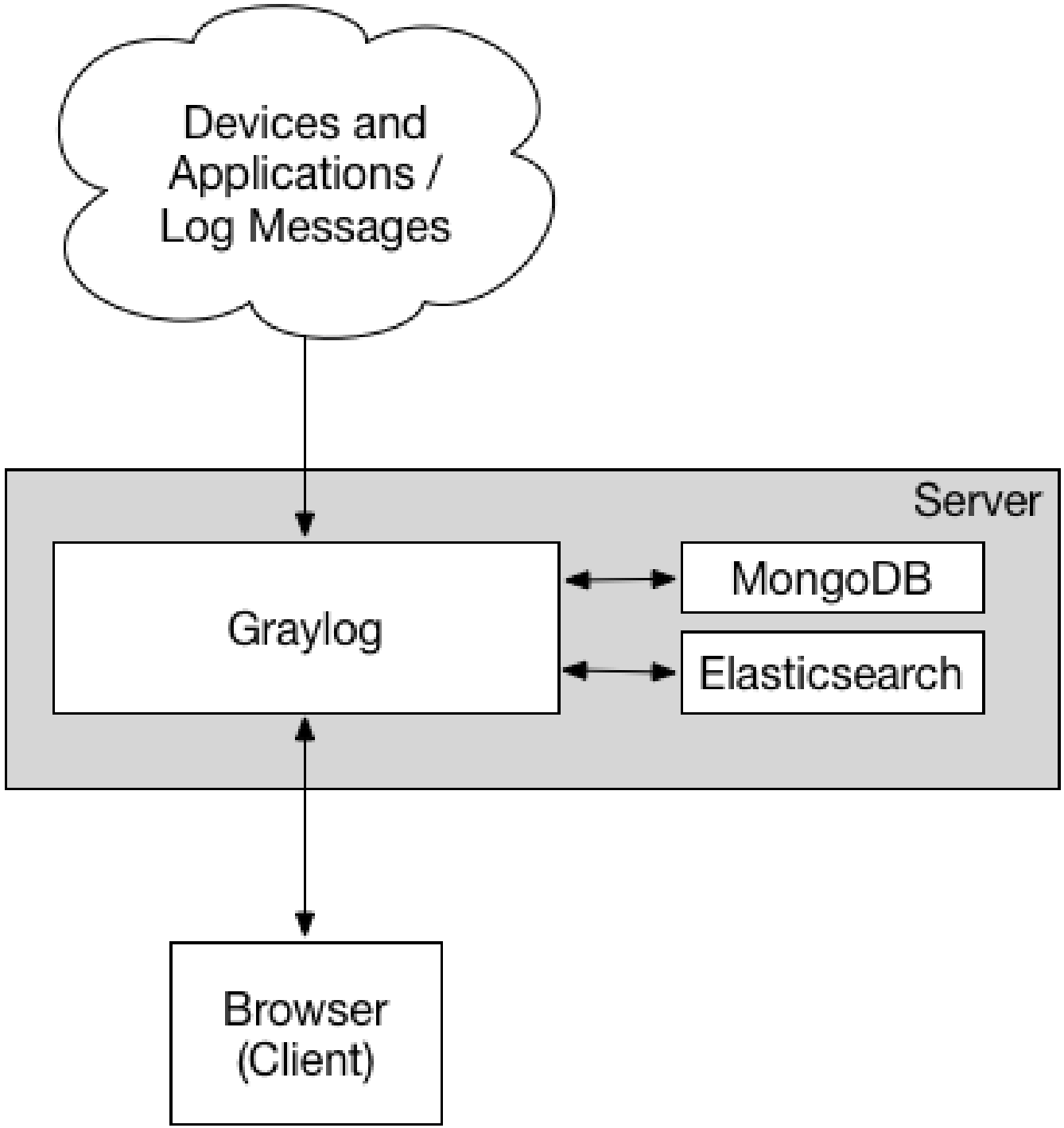
all categories | Categories | Latest | New (4) | Unread (2) | Top | + New Topic

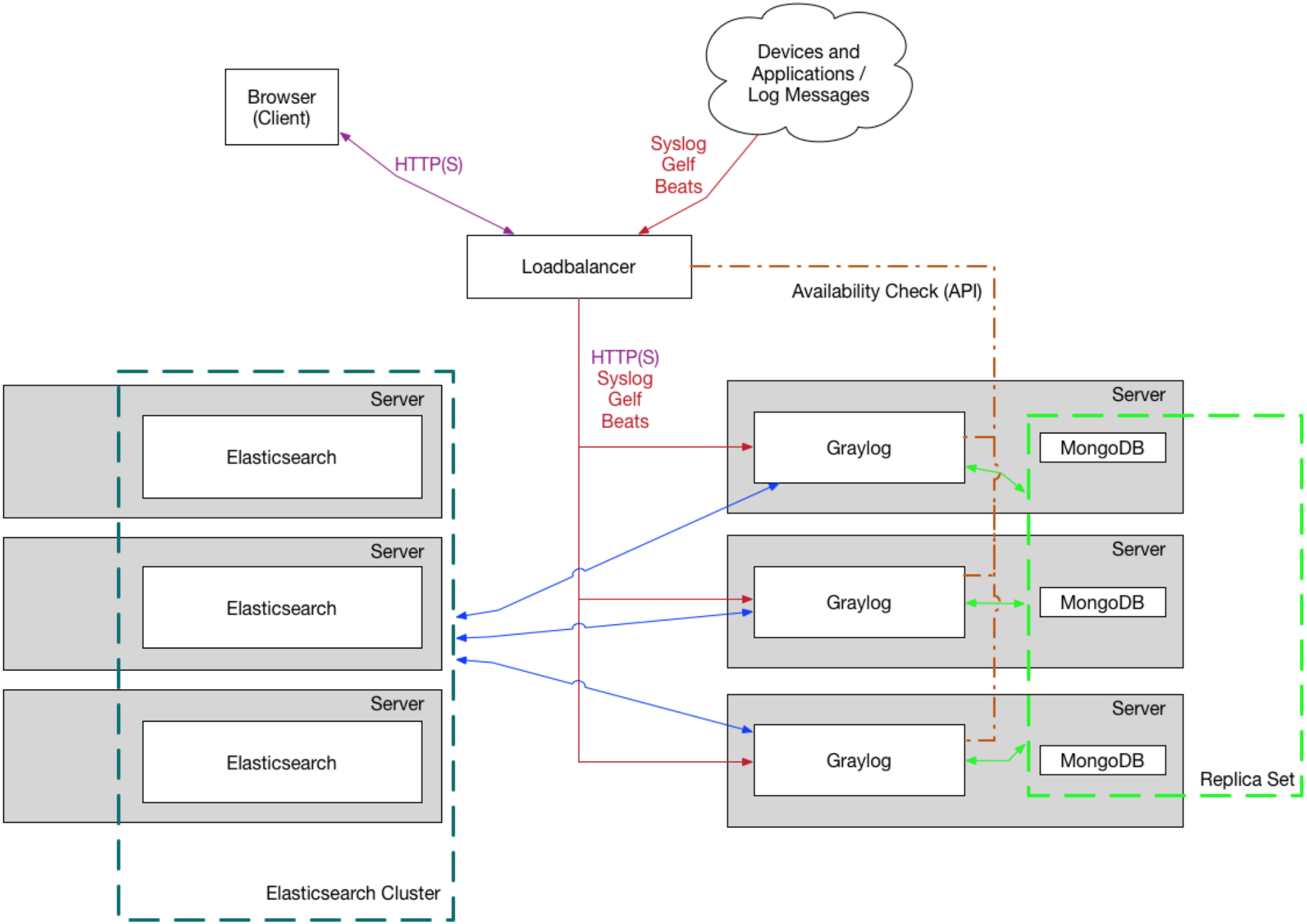
Category	Topics
Announcements This is where we'll post important Graylog updates, such as new releases, product updates, and other useful information.	1 / month
Installation New to Graylog? We've created this category for discussions on installing your Graylog setup.	41 / month 1 unread
Maintenance Have questions on maintaining Graylog after installation? Post it here.	93 / month 1 unread 4 new
Development This is the place to discuss and ask questions about the development of a Graylog-related project	11 / month
Graylog Add-ons Use this category for all things related to add-ons from the Graylog Marketplace such as installation and usage of plugins, content packs, etc.	11 / month

Latest	
 Indices routing • new Maintenance	5 1m
L Msg from one stream stored not only in configured index set, but also in default one • new Maintenance	0 1h
 Could not execute search after new installation 3 Installation	4 1h
A Not getting data on Collector-Sidecar • new Maintenance	0 2h
 Unable to load user list after upgrade to 2.2.2 1 Maintenance	2 2h
F Graylog not processing data • new Maintenance	0 2h
Pipeline: Create new message, set this message with new	

GRAYLOG CLUSTER: KOMPONENTEN

- Graylog
- Elasticsearch 2.x
- MongoDB 2.4 oder höher
- Optional: Graylog Collector


Devices and
Applications /
Log Messages
Server
Graylog
MongoDB
Elasticsearch
Browser
(Client)


Devices and
Applications /
Log Messages
Browser
(Client)
HTTP(S)
Syslog
Gelf
Beats
Loadbalancer
Availability Check (API)
HTTP(S)
Syslog
Gelf
Beats
Server
Elasticsearch
Server
Elasticsearch
Server
Elasticsearch
Elasticsearch Cluster
Server
Graylog
MongoDB
Server
Graylog
MongoDB
Server
Graylog
MongoDB
Replica Set

FOF/WOF system aggregates

Events below the Drupal layer

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

Update in background | Fullscreen | Unlock / Edit

Sec events > warning

in a few seconds

11,745

Message count

in a few seconds

173,429

Failed login attempts

in a few seconds

Value	%	Count
Top values		
teamspeak	5.25%	151
admin	4.10%	118
1pute	3.82%	110
ec----	3.82%	110
amazonaws	3.82%	110
Others		
ec2-54-247-89-36	3.82%	110
eu-west-pute	3.82%	110
pute	3.82%	110
eu-west-1pute	3.82%	110

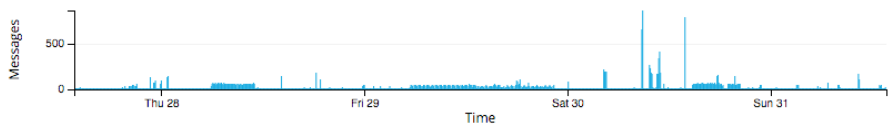
Chatty applications

in a few seconds

Value	%	Count
Top values		
sshd	28.08%	47,820
CRON	24.61%	41,921
postfix	21.49%	36,601
uptime	10.14%	17,266
pop3d	7.88%	13,421
Others		
imapd	6.42%	10,931
proftpd	1.03%	1,749
ntpd	0.21%	364
pop3d-ssl	0.04%	70
sudo	0.03%	58
su	0.03%	48
dhclient	0.02%	27
imapd-ssl	0.01%	22
rsyslogd	0.01%	15
logger	0.00%	4

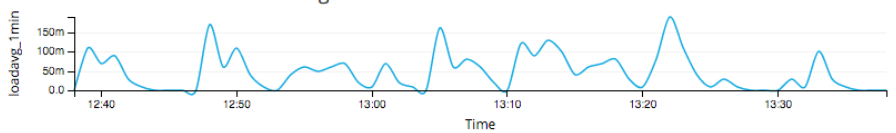
Global event rate

in a few seconds



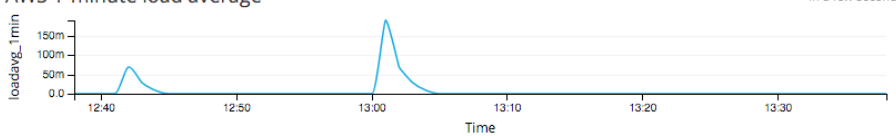
Private cloud 1-minute load average

in a few seconds



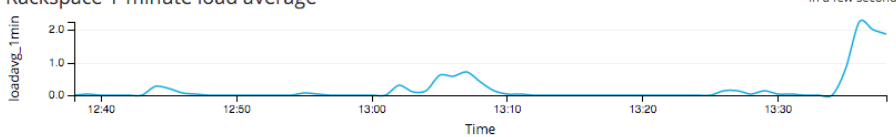
AWS 1-minute load average

in a few seconds



Rackspace 1-minute load average

in a few seconds



AWS Networks

AWS network FlowLog overview

Update in background | Fullscreen | Unlock / Edit

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

Top rejected packet sources

a few seconds ago

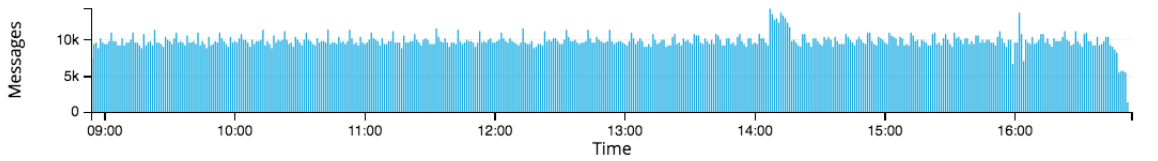
Rejected packet sources

a few seconds ago

Value	%	Count
Top values		
172.30.1.147	17.24%	8,496
172.30.2.187	17.01%	8,383
93.174.93.136	0.83%	409
89.163.144.243	0.80%	395
163.172.206.209	0.74%	366
Others		
61.164.149.128	0.44%	217
54.239.39.130	0.39%	191
54.239.39.230	0.37%	184
176.32.118.53	0.33%	164

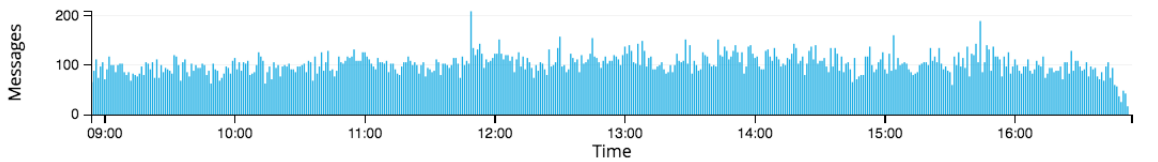
Global activity

a few seconds ago



Global rejected packets

a few seconds ago



Rejected packet ports

a few seconds ago

Value	%	Count
Top values		
23	14.91%	7,348
0	4.24%	2,087
5358	3.60%	1,775
22	2.89%	1,425
7547	2.37%	1,166
Others		
5060	1.56%	768
3389	1.34%	662
2323	1.24%	610
33434	0.89%	438

graylog Search Streams Alerts Dashboards Sources System In 0 / Out 0 msg/s Help Jochen Schalanda

WiFi IDS

WiFi IDS

Update in background Fullscreen Unlock / Edit

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

All channels in use

a few seconds ago

Value	%	Count
Top values		
1	34.76%	28,156
11	27.98%	22,664
6	27.92%	22,615
4	4.74%	3,841
9	2.03%	1,646
Others		
3	1.50%	1,219
8	0.39%	316
5	0.32%	257
7	0.18%	146
10	0.17%	138
2	0.00%	3

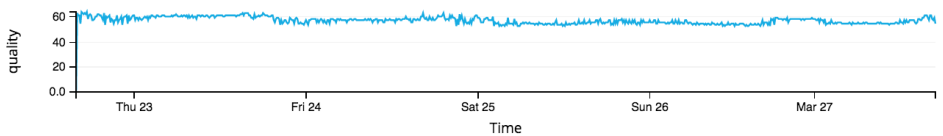
Networks in reach

a few seconds ago

Value	%	Count
Top values		
SH_Utility 2	16.96%	32,346
SH_Guest	16.85%	32,138
SH_Office	15.90%	30,324
HIDDEN	7.85%	14,984
Wemap	3.77%	7,200
Others		
Free Karma by Women In Tech	3.77%	7,194
\x00\x00\x00\x00\x00\x00\x00\x00	3.50%	6,685
Effort Guest	2.92%	5,567
HTXLabs_Guest	2.64%	5,032

Signal Quality

a few seconds ago



Access Points

a few seconds ago

Value	%	Count
Top values		
E2:55:7D:AE:B5:81	23.74%	7,200
E2:55:7D:AD:F8:21	23.74%	7,200
E2:55:7D:B0:A5:51	23.68%	7,181
02:18:4A:13:8B:11	23.63%	7,166
E2:55:7D:AF:BF:91	4.86%	1,475
Others		
02:18:4A:13:92:C1	0.34%	102

Our Channels

a few seconds ago

Value	%	Count
Top values		
11	38.22%	11,590
6	33.28%	10,091

Encrypted Corporate Netwo...

a few seconds ago

Value	%	Count
Top values		
true	100.00%	30,324

graylog | Search | Streams | Alerts | Dashboards | Sources | System | In 0 / Out 0 msg/s | Help | Jochen Schalanda

Search in the last 1 day | Not updating | Saved searches

Type your search query here and press enter. ("not found" AND http) OR http_response_code:[400 TO 404]

Search result

Found **13,958,769 messages** in 1,342 ms, searched in 8 indices.
Results retrieved at 2017-03-27 16:50:52.

Add count to dashboard | Save search criteria | More actions

Fields | Decorators

Default | All | None | Filter fields

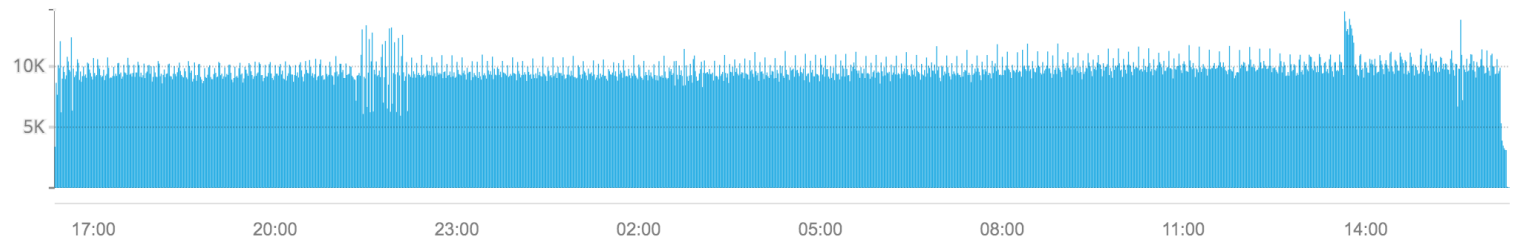
- account_id
- action
- application_name
- aws_source
- bssid
- bytes
- capture_window_duration_seconds
- channel
- dns_op_code
- dns_question
- dns_question_class
- dns_question_type
- dns_response_code

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

Histogram

Add to dashboard

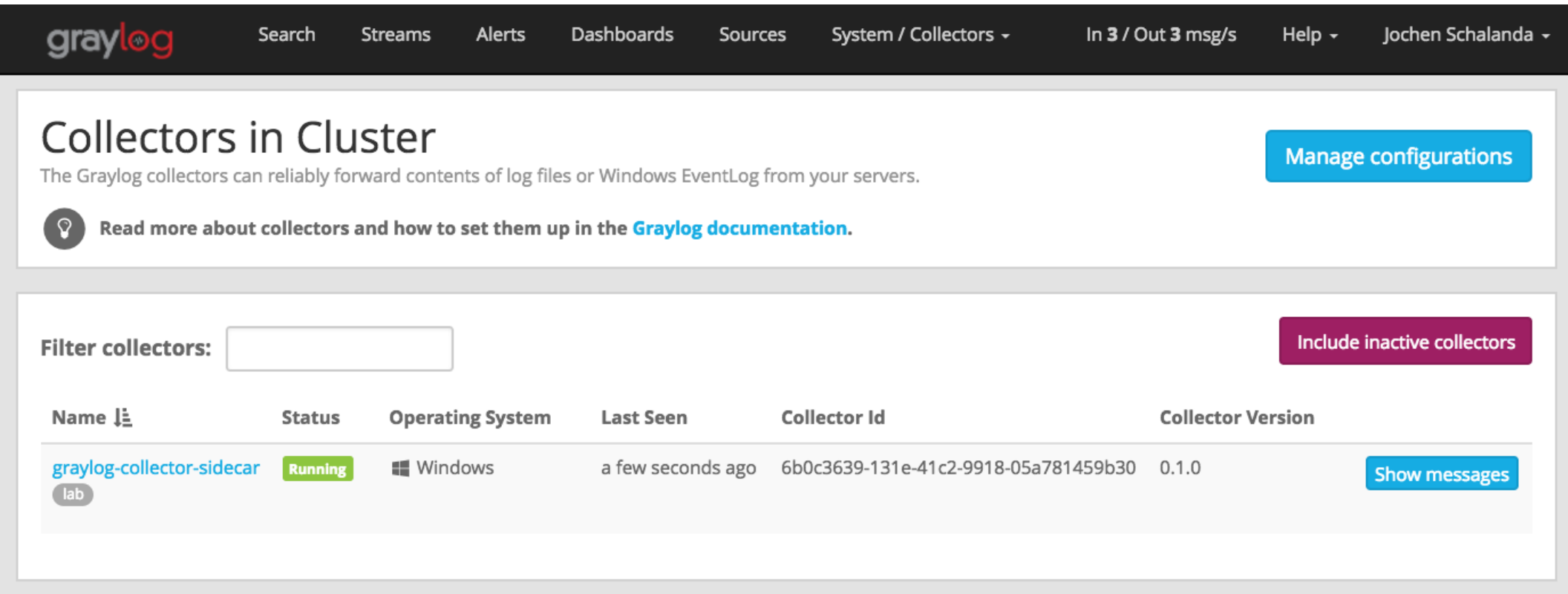
Year, Quarter, Month, Week, Day, Hour, **Minute**

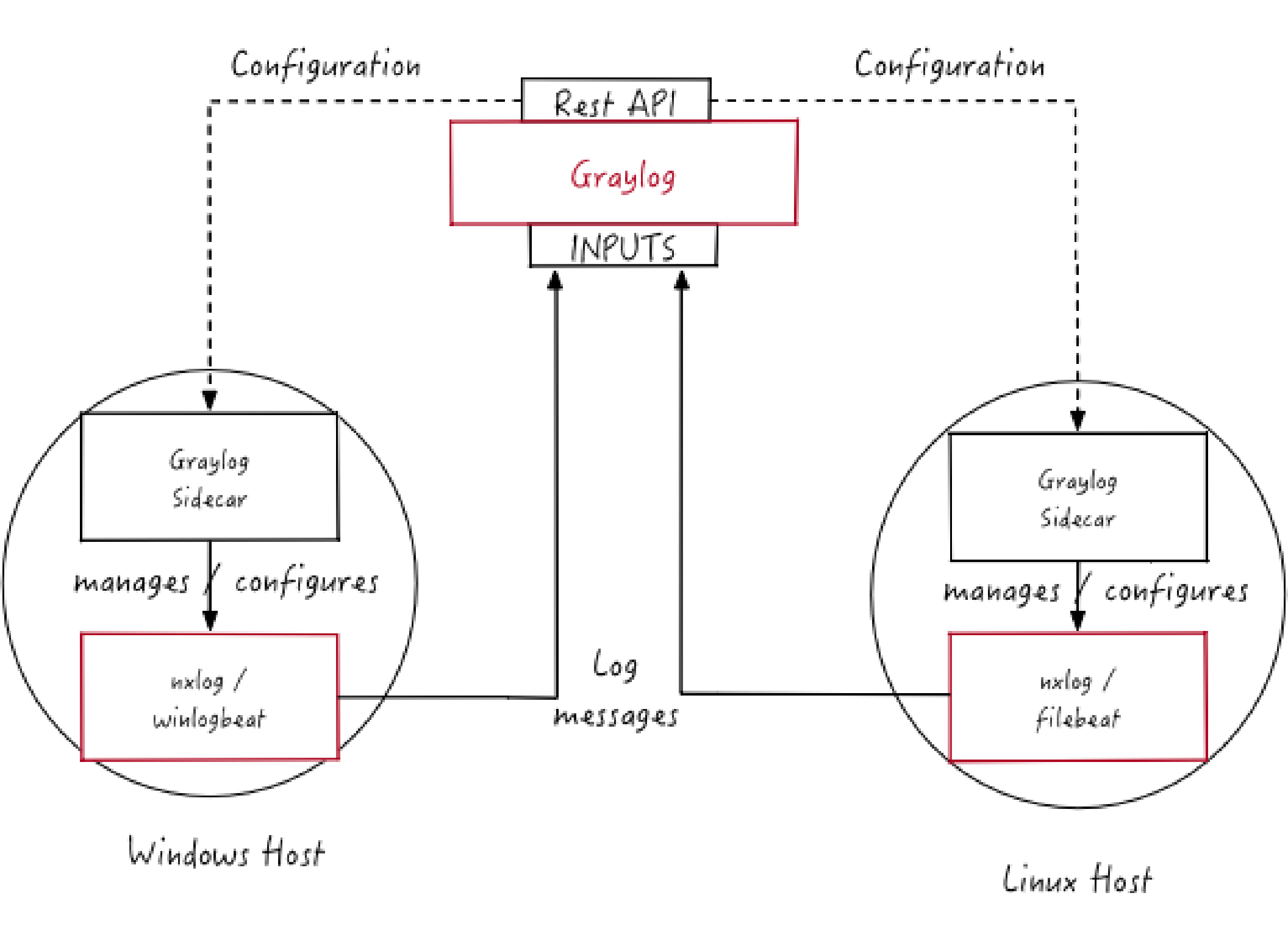


Messages

Previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Next

Timestamp	source
2017-03-27 16:50:47.360	EC2AMAZ-57J1961
An account failed to log on. Subject: Security ID: S-1-0-0	
2017-03-27 16:50:46.419	EC2AMAZ-57J1961
An account failed to log on. Subject: Security ID: S-1-0-0	
2017-03-27 16:50:43.068	graylog-defcon
DNS Query: collectd.librato.com	


graylog
Search
Streams
Alerts
Dashboards
Sources
System / Collectors
In 3 / Out 3 msg/s
Help
Jochen Schalanda
Collectors in Cluster
The Graylog collectors can reliably forward contents of log files or Windows EventLog from your servers.
Manage configurations
Read more about collectors and how to set them up in the Graylog documentation.
Filter collectors:
Include inactive collectors
Name
Status
Operating System
Last Seen
Collector Id
Collector Version
graylog-collector-sidecar
lab
Running
Windows
a few seconds ago
6b0c3639-131e-41c2-9918-05a781459b30
0.1.0
Show messages


Configuration
Rest API
Configuration
Graylog
INPUTS
Graylog
Sidecar
manages / configures
nxlog /
winlogbeat
Log
messages
Graylog
Sidecar
manages / configures
nxlog /
filebeat
Windows Host
Linux Host

DEMO

Demo on AWS (non-public)

KONTAKT


FRAGEN?

WEITERFÜHRENDE QUELLEN

- Graylog
- Graylog Documentation
- Graylog Marketplace
- Graylog Community Forums
- JAXenter: Logmanagement mit Graylog