



DIG IN THE DIRT

# SERVUS, OSMC!

OPEN SOURCE  
**MONITORING**  
CONFERENCE

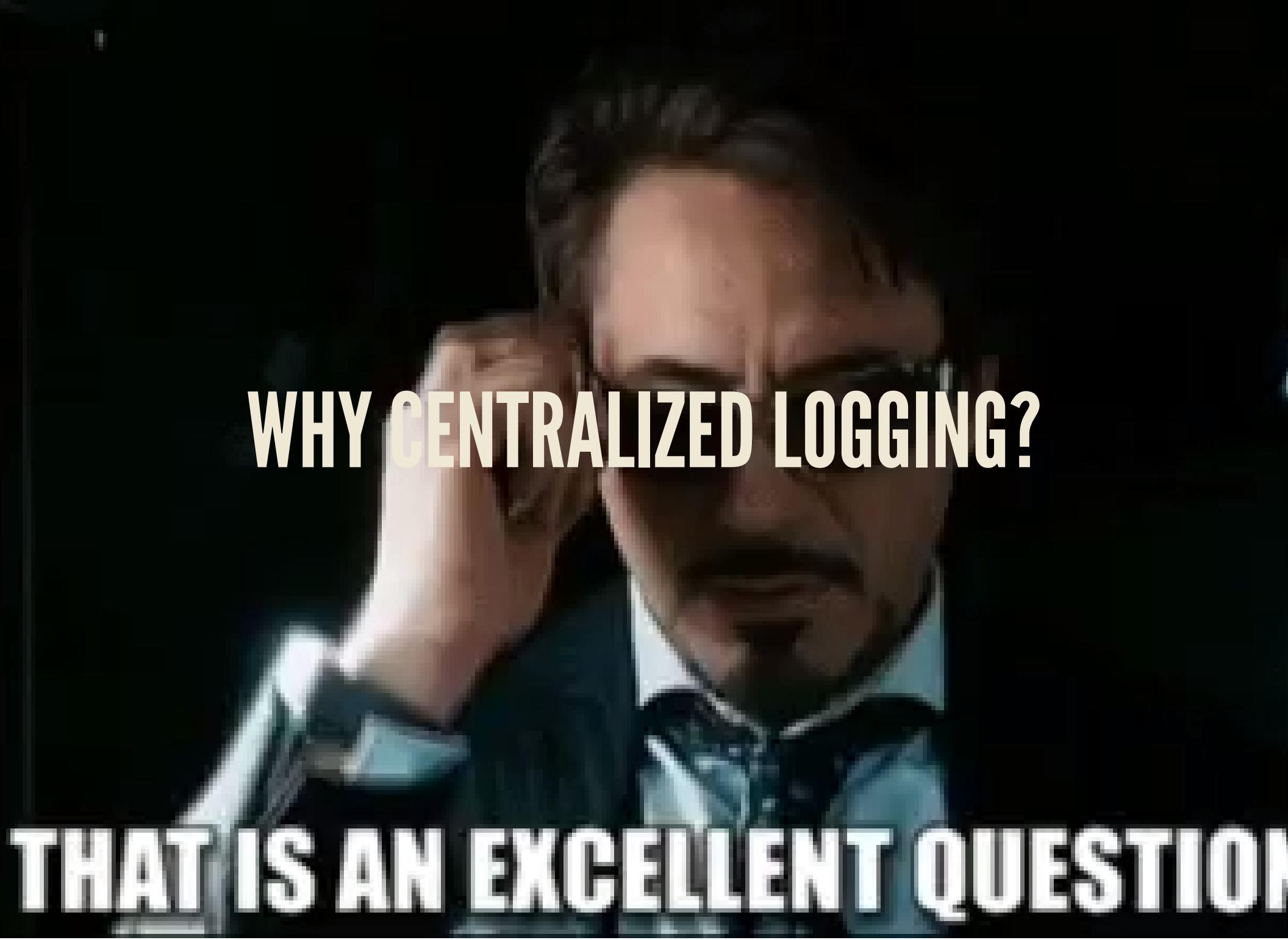
November 21 – 24, 2017 | Nuremberg

# POPULAR VOTE



Who's using...

- Elastic Stack (ex-ELK)
- Splunk?
- Some Logging SaaS (Loggly, Scalyr, etc.)
- Graylog?



**WHY CENTRALIZED LOGGING?**

**THAT IS AN EXCELLENT QUESTION**

# DEBUGGING



Jan Lehnardt  
@janl

Folgen



Debugging in three easy steps:

1. look at the logs.
2. if you don't have logs, add logs.
3. look at the logs.

Original (Englisch) übersetzen

RETWEETS

344

GEFÄLLT

467



DONT  
PANIC



14:26 - 10. Okt. 2016

# 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

# SECURITY (3)

## *A10:2017 Insufficient Logging & Monitoring*

*Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident.*

OWASP Top 2017

## A to Z Departures

Next train to	Plat	Due	Expted
Abbey Wood	4	17:29	On time
Albany Park	4	17:25	On time
Rishworth Internl		Please ask staff	
Barnhurst	4	17:45	On time
Battersea Park	-	17:41	On time
Beckenham Jnc		Please ask staff	
Bedford		Please ask staff	
Belvedere	4	17:48	
Bexley		17:45	
Bexleyheath		17:45	
Blackfriars		Please ask staff	
Blackheath		17:45	
Brighton		17:45	
Brockley		17:45	
Cannon Street		17:45	
Canterbury West		17:45	
Catford Bridge		17:45	
Charing Cross		17:45	
Charlton		17:45	
Chatham		17:45	

A to Z Departures

A to Z Despatch  
West London

卷之三

1

A large digital flight information board displaying arrival and departure times for various flights. The board is oriented vertically and shows multiple columns of flight details, including flight numbers, arrival/departure times, and gate numbers. The text is in yellow on a dark background.

# FAHRPLAN



- Capture DNS, HTTP, and ICMP packets
- Send connection/packet metadata to Graylog
- Clean up and consolidate data
- Check against threat databases
- Show stats on dashboard A small icon of a bar chart with three bars (green, red, blue) on a grey background.
- Alert on threat

# GRAYLOG

- Open source log management platform
- Built for security and operations
- Easy to set up, powerful features
- Extensible via plugins



- Graylog Enterprise
- Commercial plugins (Audit log, Archiving)
- Professional support

# GRAYLOG (INPUTS)

- GELF
- Syslog
- CEF
- Beats (Filebeat, Metricbeat, etc.)
- Netflow (v5 and v9)

# GRAYLOG (INPUTS, COMMUNITY)

- Redis
- MQTT
- SNMP
- NATS
- Many more on the Graylog Marketplace

# Hundreds of Add-ons for Graylog.

How would you like to extend Graylog today?



## Browse Add-ons by Type



Plugin



Content Pack



GELF Library



Other Solutions

[← Back to listing](#)

## 👤 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**

23 Oct 16:11

**Last Push**

28 Apr 05:44

**Marketplace Rating****Discussion**

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 )

[all categories ▶](#)**Categories**[Latest](#)[New \(4\)](#)[Unread \(2\)](#)[Top](#)[+ New Topic](#)

## Category

## Topics

**Announcements**

1 / month

This is where we'll post important Graylog updates, such as new releases, product updates, and other useful information.

**Installation**

41 / month

1 unread

New to Graylog? We've created this category for discussions on installing your Graylog setup.

**Maintenance**

93 / month

1 unread

4 new

Have questions on maintaining Graylog after installation? Post it here.

**Development**

11 / month

This is the place to discuss and ask questions about the development of a Graylog-related project

**Graylog Add-ons**

11 / month

Use this category for all things related to add-ons from the [Graylog Marketplace](#) such as installation and usage of plugins, content packs, etc.

## Latest



Indices routing • new

Maintenance

5

1m



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



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



Graylog not processing data • new

Maintenance

0

2h

Bindings: Create new messages, not this message with now



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**.

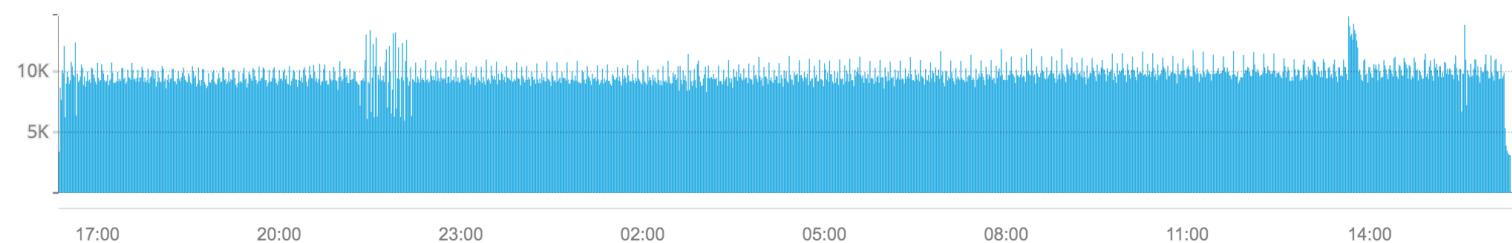
Results retrieved at 2017-03-27 16:50:52.

[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

[Year](#), [Quarter](#), [Month](#), [Week](#), [Day](#), [Hour](#), [Minute](#)[Add to dashboard ▾](#)

## 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

## FOF/WOF system aggregates

Events below the Drupal layer

Update in background

Fullscreen

Unlock / Edit

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

Sec events &gt; warning in a few seconds

11,745



Message count in a few seconds

173,429



Failed login attempts in a few seconds

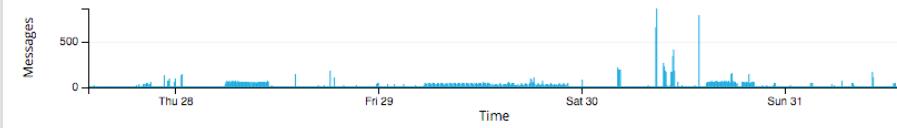
Value	%	Count
Top values		
teamspeak	5.25%	151
admin	4.10%	118
1pute	3.82%	110
ec----	3.82%	110
amazonaws	3.82%	110
Others		
ec2-54-247-89-36	3.82%	110
eu-west-pute	3.82%	110
pute	3.82%	110
eu-west-1oute	3.82%	110

Chatty applications in a few seconds

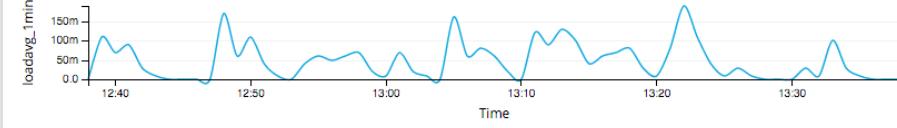


Value	%	Count
Top values		
sshd	28.08%	47,820
CRON	24.61%	41,921
postfix	21.49%	36,601
uptime	10.14%	17,266
pop3d	7.88%	13,421
Others		
imapd	6.42%	10,931
proftpd	1.03%	1,749
ntpd	0.21%	364
pop3d-ssl	0.04%	70
sudo	0.03%	58
su	0.03%	48
dhclient	0.02%	27
imapd-ssl	0.01%	22
rsyslogd	0.01%	15
logger	0.00%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

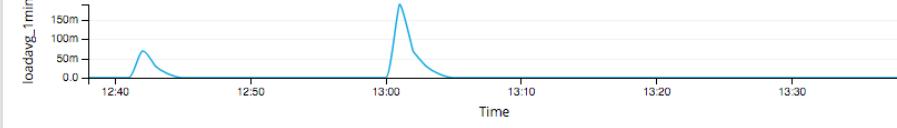
Global event rate in a few seconds



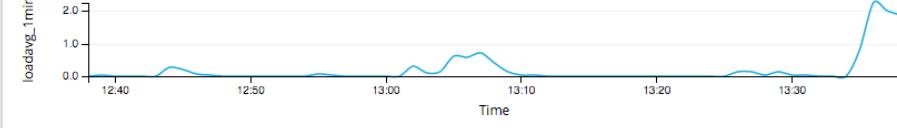
Private cloud 1-minute load average in a few seconds



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**.

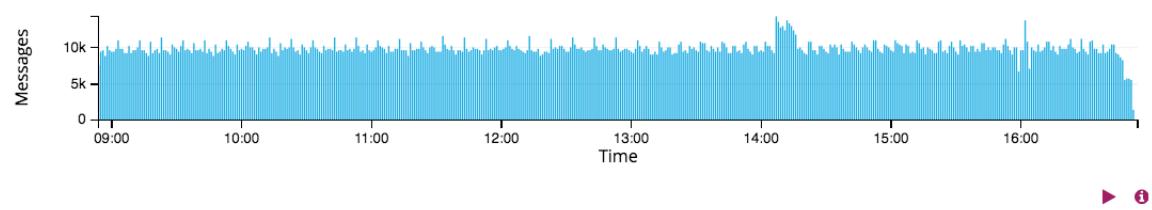
## Top rejected packet sources



## Rejected packet sources

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

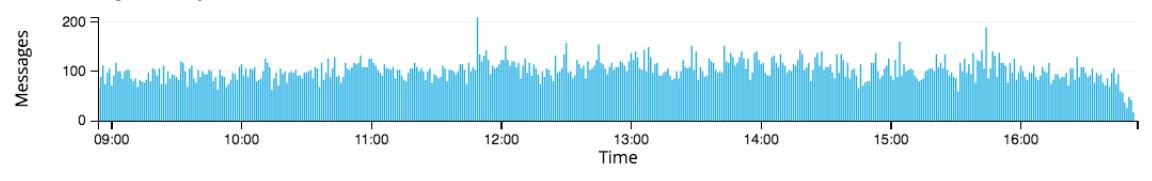
## Global activity



## Rejected packet ports

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

## Global rejected packets



WiFi IDS

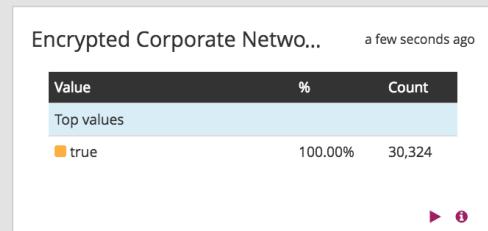
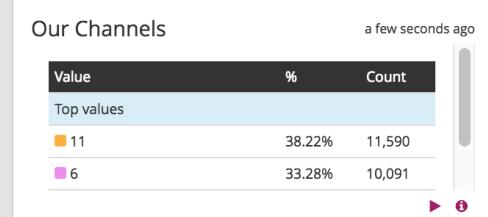
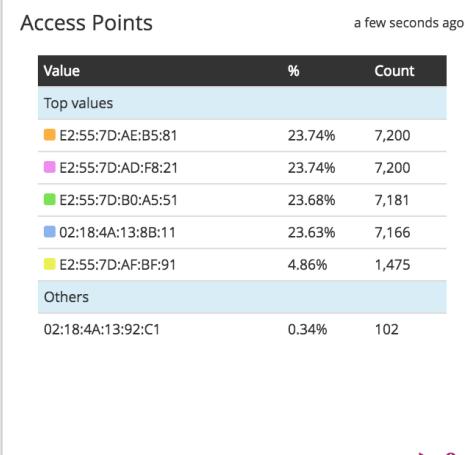
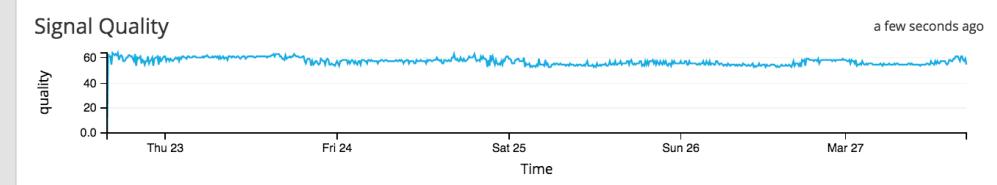
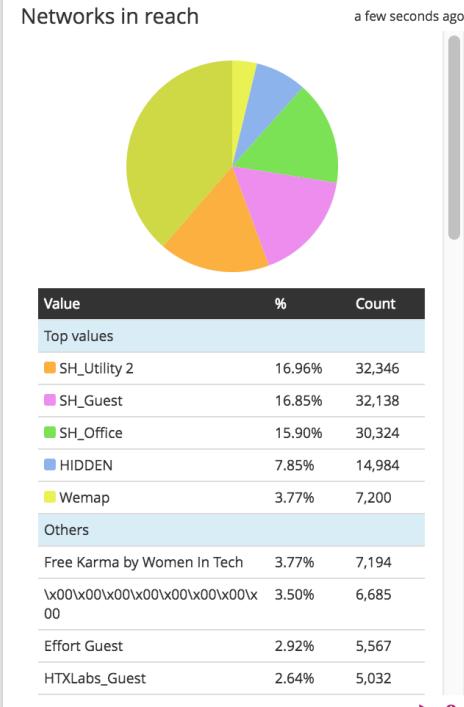
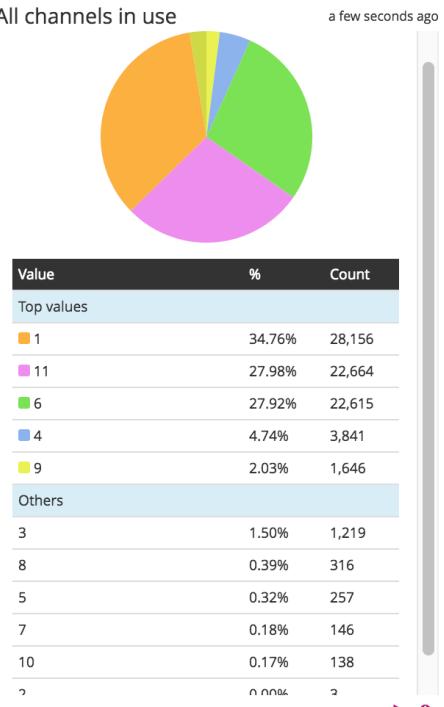
WiFi IDS

Update in background

Fullscreen

Unlock / Edit

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



## 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	<a href="#">Show messages</a>



LIVE DEMO



[Open Demo](#)



QUESTIONS? 🤔

# CONTACT DETAILS



[Twitter](#) – [GitHub](#) – [LinkedIn](#) – [X](#)



# ADDITIONAL LINKS

- [Graylog](#)
- [Graylog Documentation](#)
- [Graylog Marketplace](#)
- [Graylog Community Forums](#)

# IMAGE CREDITS

- “Digging” by Jeremy Schultz is licensed under CC BY 2.0
- Tony Stark GIF at Giphy
- “Train Timetables” by robertsharp is licensed under CC BY 2.0
- “Pearl ... dig, dig, dig” by sneakerdog is licensed under CC BY 2.0
- Lincoln Stoll (@lstoll)

# BACKUP SLIDES



# WHAT'S IN A GRAYLOG CLUSTER?

- Graylog
- Elasticsearch 5.x
- MongoDB 2.4 oder höher
- Optional: Graylog Collector

