

Agenda 9. HAMNET-Treffen 17.10.17 in Wesseling

- Begrüßung (DJ5KP)**
- Abstimmung der Tagesordnung (alle)**
- Aktueller Stand Linkstrecken und HAMNET-Knoten (alle SYSOP)**
- Neues zu CACTI (DJ5KP)**
- Rückblick auf den Umstieg von OSPF- auf BGP-Routing (DJ5KP)**
- Vorstellung des Tools "Graylog" (DO2KSM)**
- Erläuterungen zum Thema "torrent" (DH3WR)**
- Neues von der HamNet-Tagung in Stuttgart (DH3WR)**
- Fragen zu HamCloud und HF Linkstrecken (DL8UE)**
- Anderer Wochentag für das HamNet-Treffen? (alle)**
- Termin nächstes Treffen (alle)**
- Allgemeiner Erfahrungsaustausch (alle)**

Aktueller Stand HamNet-Knoten: (Meldung von Carsten (DM1CG))

Wir werden in den nächsten Wochen alle Anträge die mit DB0EU zusammenhängen zur BNetzA schicken, DB0KWE, DB0NIS, DB0EU, DB0HAN, DB0NOR, DB0GIE, DB0UHC. DB0NIS verzichtet auf alle Linkstrecken, damit der Standort vom DL1KFS Störungsfrei ist – seit Abbau aller UBNTs kann man dort wieder funken. DB0NIS bleibt mit z.Zt. 200Mbits an DB0EU angebunden, via ISM Link. Nach DB0KWE, DB0UHC, DB0HAN werden wir 2 x 10 MHz nebeneinander liegende Frequenzen beantragen. Nach HAN läuft der Links schon mit 2 x 10 MHz, nach UHC wurde erfolgreich getestet und nach DB0KWE lief auch ein 2h Test.

Der Router für DB0EU ist an dem Router von DB0NOR angeschlossen und kann fürs BGP installiert werden.

soweit von hier
vy 73 de Carsten

DM1CG

neues in CACTI: (Router Voltage&Temperature)

#: Stand 10.10.2017 18:00 Uhr

A: Analyse

DB0KO HF Ports

DB0KO HF User Traffic

DB0KPG HF Ports

DB0NDK HF Ports

DJ5KP Traffic

Router CPU Load

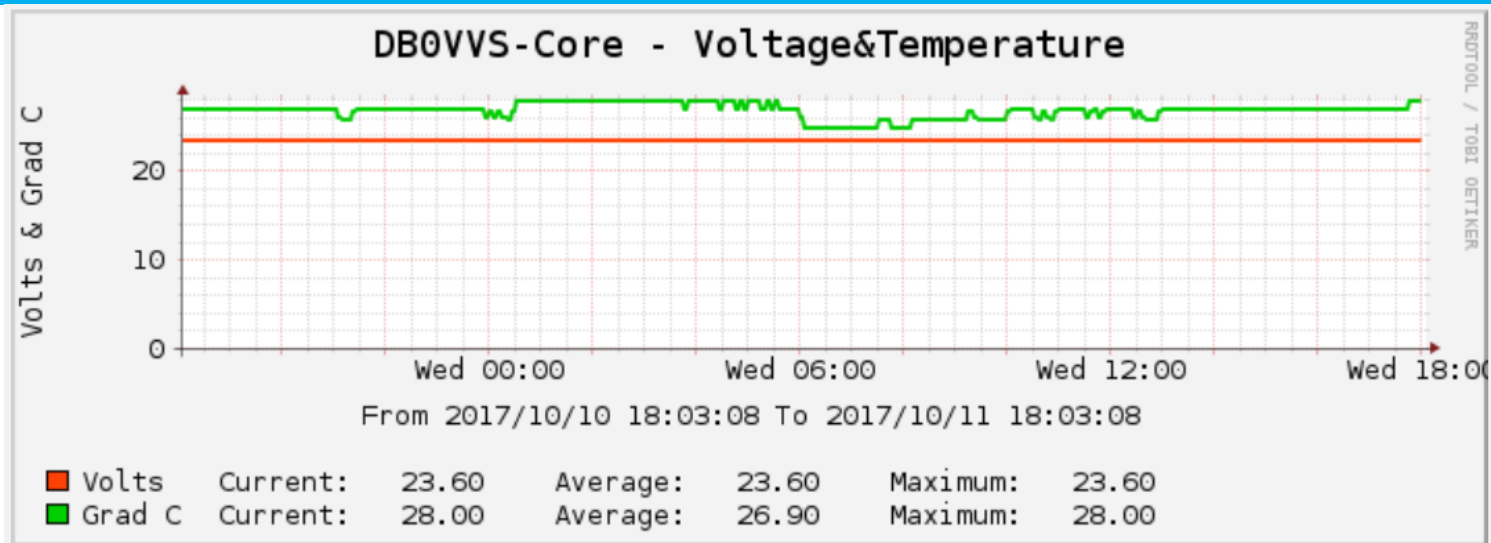
Router Memory Usage

Router Ping Zeiten

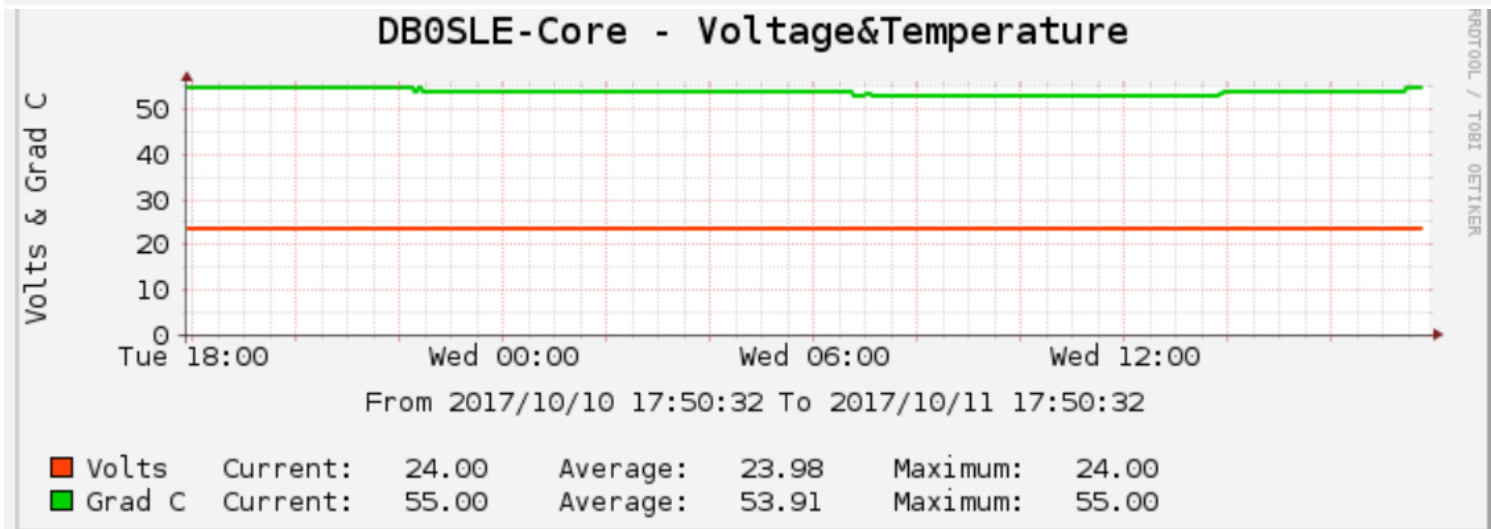
Router Routes

Router Uptimes

Router Voltage&Temperature

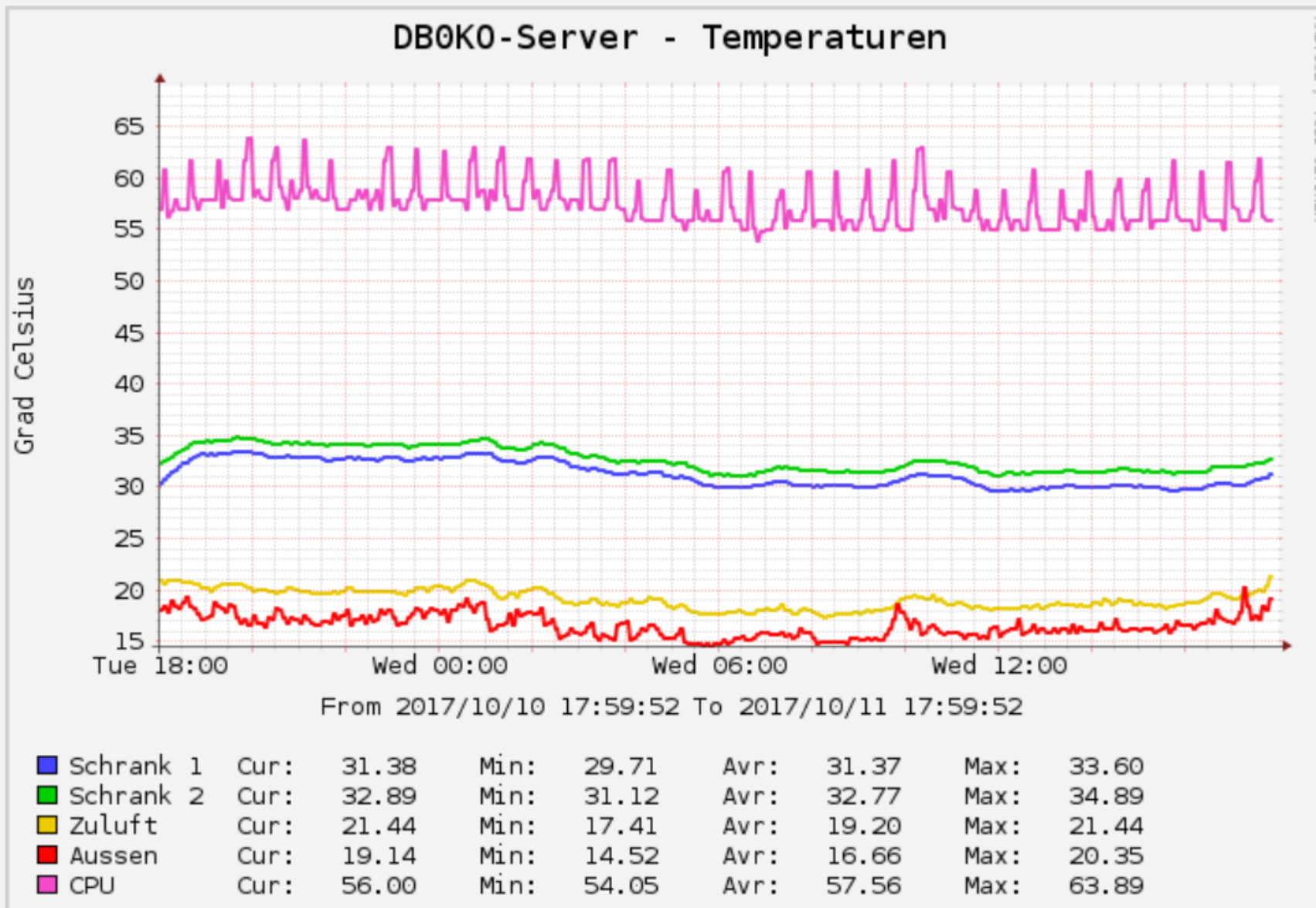


OK

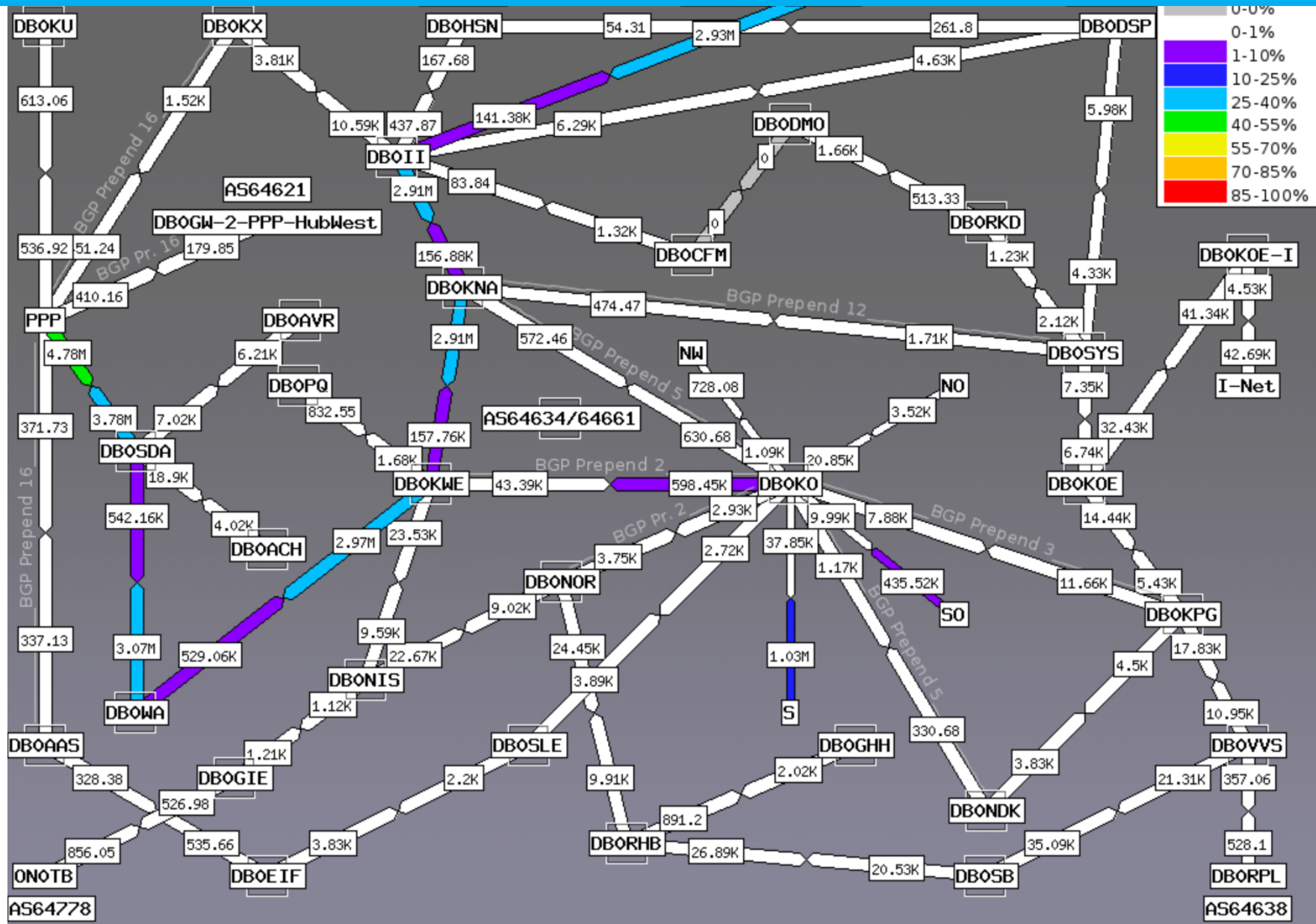


Nicht optimal

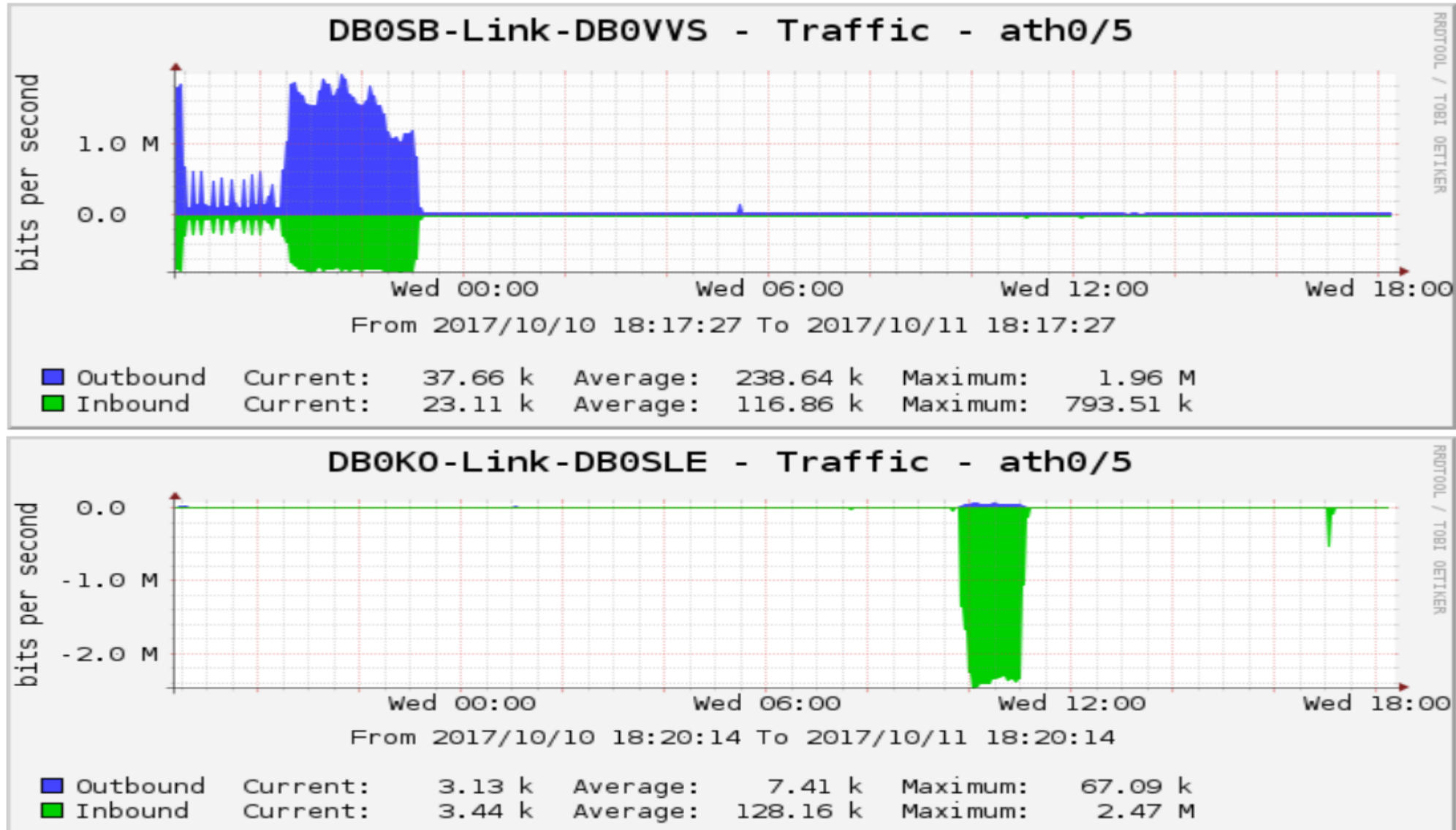
neues in CACTI: (DB0KO-Server-Temperaturen)



Neues in CACTI: (Weathermap (BGP Prepend))



Neues in CACTI: Darstellung Traffic



Graylog

Ein Vorschlag für zentrales Log-Management im HAMNET

Sebastian Muszynski, D02KSM

17.10.2017



■ Zentrales Log-Management

- Meldungen sammeln
- Meldungen verarbeiten
- Daten suchen
- Daten analysieren
- Eintauchen (Drill-Down)
- Visualisieren
- Auslöser und Alarmfunktion
- freie Lizenz, leicht zu installieren, skaliert

The image shows the Graylog website. The top section features the Graylog logo and navigation links: Overview, Docs, Blog, Enterprise, Community, and Download. A prominent headline reads "Trusted full-featured log management." followed by the tagline "Open Source. Built for Security, Operations, and DevOps." Below this, there's a "Correlate all D" button and a large red "Download now" button. A banner at the bottom of the top section shows "25,000 active installations", "3,200 Stars on Github", and "@graylog2 on Twitter".

The lower section is titled "USE CASE" and focuses on "Computer & Network Security". It describes perimeter security using firewalls and malware scanners, emphasizing observability and monitoring. It includes sub-sections for "Network Security Monitoring" (observing established or rejected network connections) and "Intrusion Detection" (integrating with IDS like Snort or Bro). A "Learn more" button is present.

Below the security section, there's another "USE CASE" for "IT Operations", which describes centrally collecting syslog and EventLog messages to spot and resolve issues faster. It also includes a "Monitor & Alert" section for preventing downtime and a "Compliance" section for information security standards.

The bottom right of the image shows a screenshot of the Graylog interface, displaying a search bar, a search result count (18,536 messages), a histogram of message counts over time, and a list of fields for filtering.

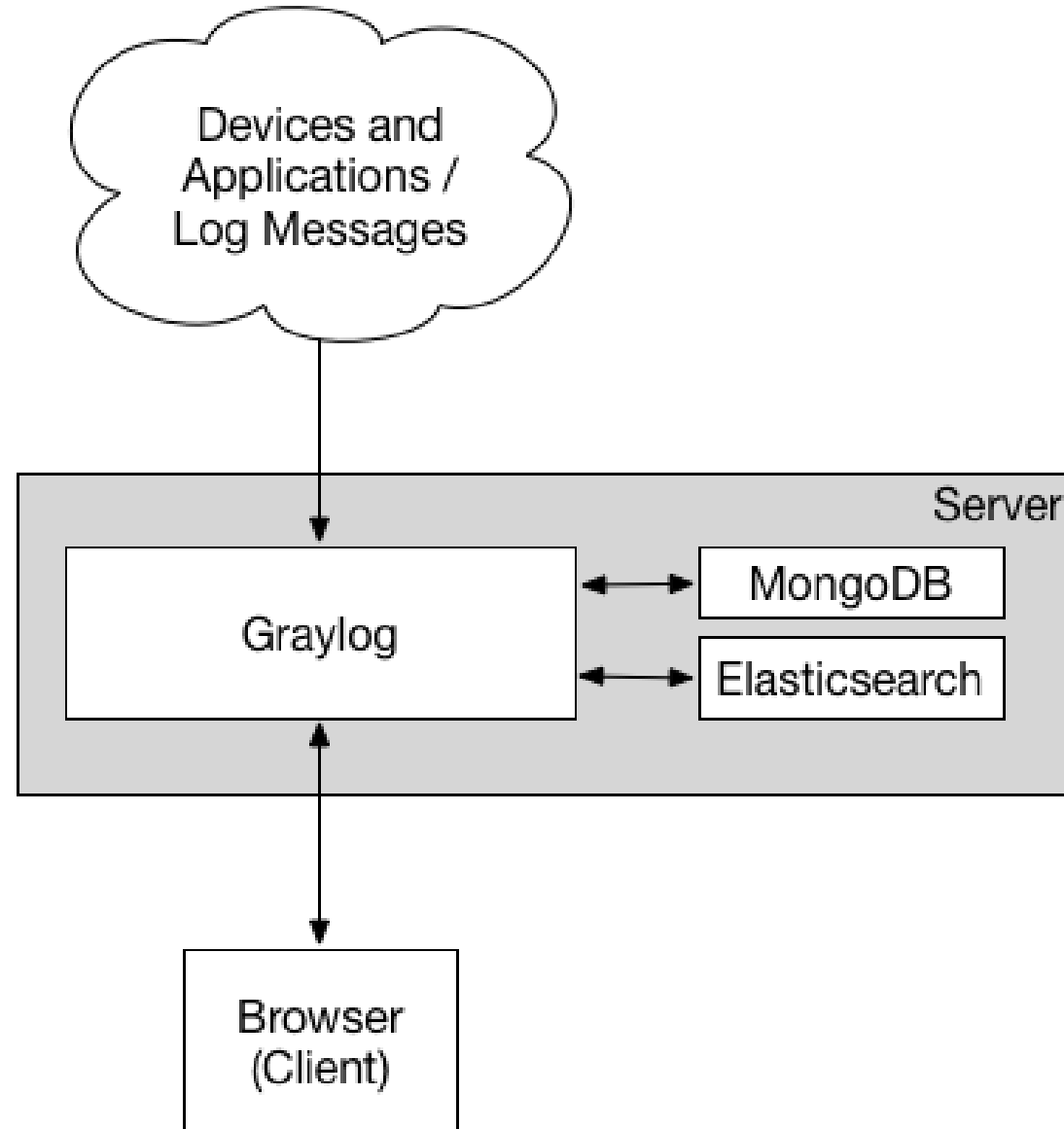
Motivation

- Zentrale Sammelstelle für Logmeldungen unterschiedlicher Quellen
- Visualisierung der Häufigkeit von Ereignissen entlang der Zeitachse

The screenshot displays the LogAnalyzer web interface. The browser address bar shows the URL `192.168.1.127/loganalyzer/index.php`. The page title is "LogAnalyzer ANALYSIS & REPORTING". The interface includes a navigation bar with buttons for Search, Show Events, Statistics, Reports, Help, Search in Knowledge Base, Admin Center, and Logoff. A search filter is set to "admin". The main content area shows "Recent syslog messages" with a table of log entries. The table has columns for Date, Facility, Severity, Host, Syslogtag, ProcessID, Messagetype, and Message. The messages are sorted by date, showing events from "Today 03:01:01". The messages include CRON jobs (cron.hourly, anacron) and a KERN message (kernel).

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 03:01:01	CRON	NOTICE	centos7	run-parts(/etc/cron.hourly)[29...		Syslog	finished 0anacron
Today 03:01:01	CRON	NOTICE	centos7	anacron[29281]:		Syslog	Jobs will be executed sequentially
Today 03:01:01	CRON	NOTICE	centos7	anacron[29281]:		Syslog	Will run job 'cron.daily' in 35 min.
Today 03:01:01	CRON	NOTICE	centos7	anacron[29281]:		Syslog	Anacron started on 2017-02-05
Today 03:01:01	CRON	NOTICE	centos7	run-parts(/etc/cron.hourly)[29...		Syslog	starting 0anacron
Today 03:01:01	KERN	DEBUG	centos7	kernel:		Syslog	[17415.062066] SELinux: initialized (dev tmpfs, type tmpfs), uses transition SID ...

Architektur



graylog

SearchStreamsDashboardsSourcesSystem1

In 2 / Out 2 msg/sHelpSebastian Muszynski

Last Hour

Saved searches

Q

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

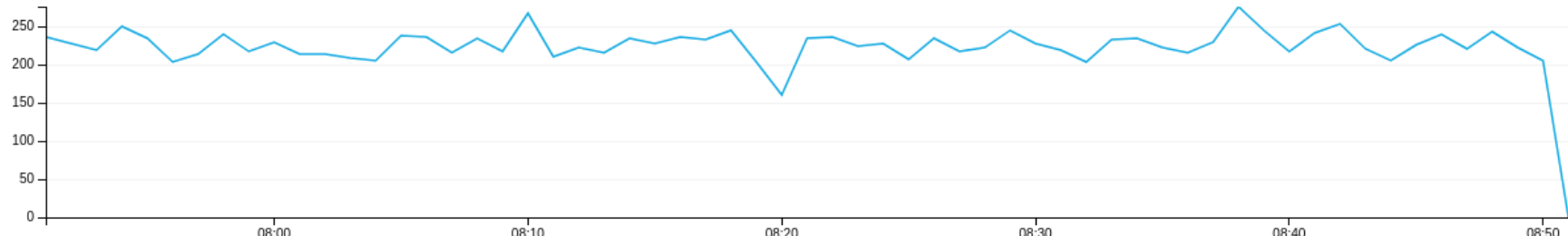
Sources

Last Hour

This is a list of all sources that sent in messages to Graylog. Note that the list is cached for a few seconds so you might have to wait a bit until a new source appears.

Use your mouse to interact with the table and graphs on this page, and get a better overview of the sources sending data into Graylog.

Messages per minute



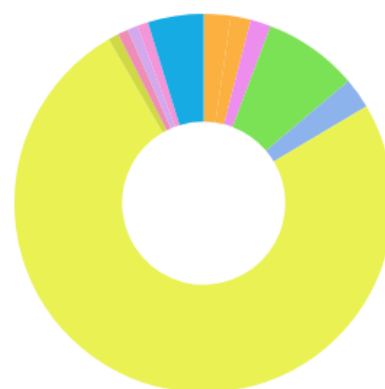
Selected sources

Search

Show: 100

Name	Percentage	Message count	
Top sources			
db0sda-core	75.18%	10,197	
db0kx-core	8.10%	1,098	
db0nor-core	2.62%	356	
db0gie-core	2.29%	311	
db0koe-core	1.75%	237	
db0kna-core	1.71%	232	

Messages per source



graylog

SearchStreamsDashboardsSourcesSystem1

In 12 / Out 12 msg/sHelpSebastian Muszynski

Search in all messages

Updating search results...

▶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 31,342,474 messages in 1,667 ms, searched in 2 indices. Results retrieved at 2017-10-17 08:54:50.

Add count to dashboard

Save search criteriaMore actions

FieldsDecorators

DefaultAllNoneFilter fields

▶streams

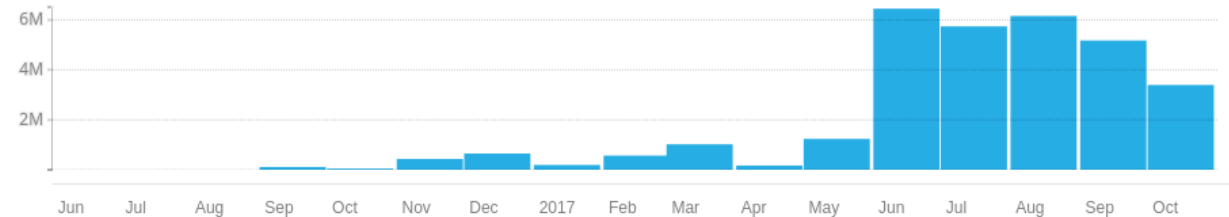
▶time

List fields of current page or all fields.

Histogram

Add to dashboard

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



Messages

Previous12345678910Next

Timestampsource

2017-10-17 08:54:50.205DB0SDA-Core

respond new phase 1 (Aggressive): 137.226.79.99[500]<=>92.72.15.72[500]

2017-10-17 08:54:50.109DB0SDA-Core

84.141.229.91 failed to pre-process ph2 packet.

2017-10-17 08:54:49.763DB0SDA-Core

94.134.69.113 peer sent packet for dead phase2

2017-10-17 08:54:49.594DB0SDA-Core

46.92.32.210 failed to pre-process ph2 packet.

2017-10-17 08:54:47.773DB0SDA-Core

94.134.69.113 failed to pre-process ph2 packet.

2017-10-17 08:54:46.818DB0SDA-Core

TCP connection established from 87.138.193.75

2017-10-17 08:54:46.524DB0KNA-Core

Failed to open TCP connection: No route to host

2017-10-17 08:54:46.524DB0KNA-Core

12

graylog

SearchStreamsDashboardsSourcesSystem1

In 12 / Out 12 msg/sHelpSebastian Muszynski

Search in all messages

Updating search results...

▶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 31,342,474 messages in 1,667 ms, searched in 2 indices. Results retrieved at 2017-10-17 08:54:50.

Add count to dashboard

Save search criteriaMore actions

FieldsDecorators

DefaultAllNoneFilter fields

▶

streams

▶

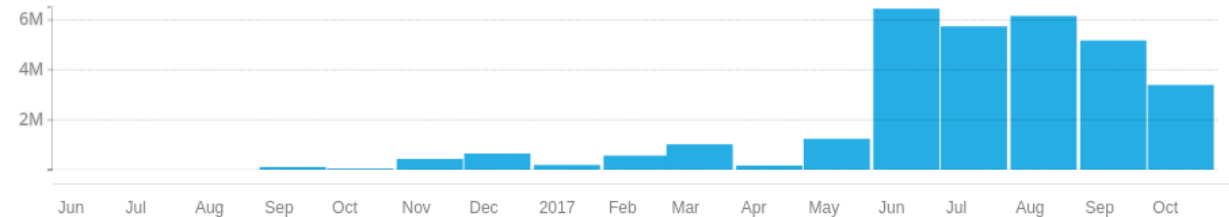
time

List fields of current page or all fields.

Histogram

Add to dashboard

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



Messages

Previous12345678910Next

Timestamp	source
2017-10-17 08:54:50.205	DB0SDA-Core
respond new phase 1 (Aggressive): 137.226.79.99[500]<=>92.72.15.72[500]	
2017-10-17 08:54:50.109	DB0SDA-Core
84.141.229.91 failed to pre-process ph2 packet.	
2017-10-17 08:54:49.763	DB0SDA-Core
94.134.69.113 peer sent packet for dead phase2	
2017-10-17 08:54:49.594	DB0SDA-Core
46.92.32.210 failed to pre-process ph2 packet.	
2017-10-17 08:54:47.773	DB0SDA-Core
94.134.69.113 failed to pre-process ph2 packet.	
2017-10-17 08:54:46.818	DB0SDA-Core
TCP connection established from 87.138.193.75	
2017-10-17 08:54:46.524	DB0KNA-Core
Failed to open TCP connection: No route to host	

Auslöser und Alarmierungen

graylog

Search

Streams

Dashboards

Sources

System

1

In 7 / Out 7 msg/s

Help

Lennart Koopmann

Alerts configuration for stream »Exceptions on all platforms«

You can define thresholds on any message field or message count of a stream and be alerted based on this definition.

Learn more about alerts in the [documentation](#).

Add new alert condition

Message count condition

Configure new alert condition

Trigger alert when there are ☒ more ☐ less

than messages in the last minutes and

then wait at least minutes until triggering a new alert. (grace period)

When sending an alert, include the last messages of the stream evaluated for this alert condition.

Add alert condition

Configured alert conditions

Field value condition

Alert is triggered when the field millis has a higher mean value than 250 in the last 3 minutes. Grace period: 0 minutes. Not including any messages in alert notification.

Edit condition

Delete condition

Callbacks

The following callbacks will be performed when this stream triggers an alert.

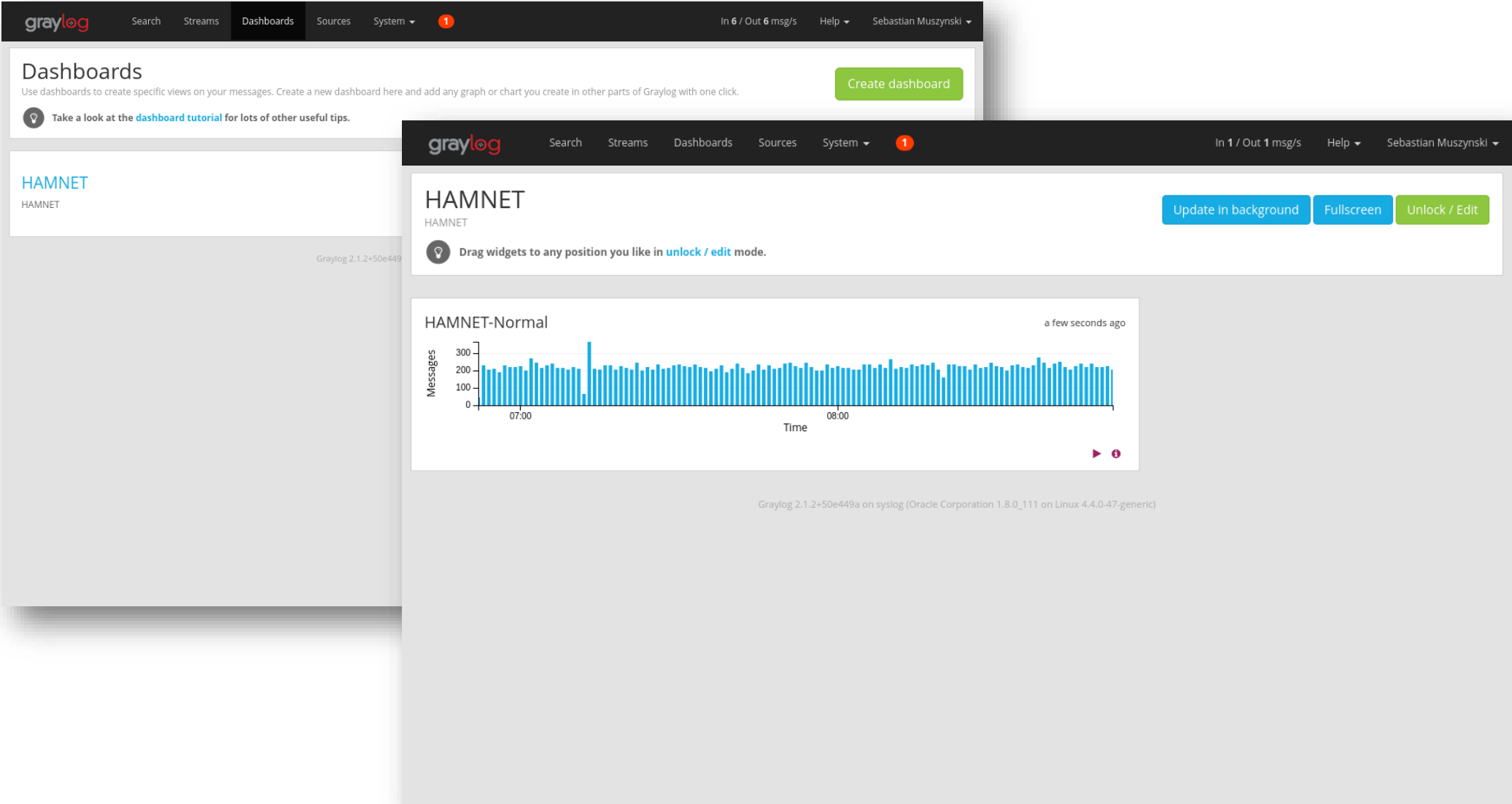
Select Callback Type

Add callback

Find more callbacks

No configured alarm callbacks.

Zusammenhänge in Dashboards darstellen



Nutzung

- Web-Oberfläche erreichbar unter <http://syslog.db0sda.ampr.org>
- Zugangsdaten bei Michael (DJ5KP) anfordern
- Ziel-Host für Syslog-Meldungen: 44.225.164.22:5141

Vielen Dank!

Fragen?

Sebastian Muszynski, D02KSM

basti@linkt.de

github.com/syssi

twitter.com/syssi84

17.10.2017



HAMNET-Tagung 23.09.17 in Stuttgart

Status des HAMNET-Backbone in DL

DD9QP

Kurzüberblick der bisher gewonnenen Erkenntnisse für ein Standarddeployment von HAMNET-Knoten

Team
IP-Koordination DL

Die HamCloud im Detail

DG8NGN, DL9SAU

Netzdesign von Amateurfunkanwendungsnetzen basierend auf HAMNET, HamCloud und Internet

DG8NGN

Themenblock "Monitoring im HAMNET"

Diverse

Kurze Einführung in "The Dude" von Mikrotik

DL8SCU

Monitoring im AS64643/AS64661 mit "Cacti"

DJ5KP

Netzwerk- und Applikationsmonitoring mit "OpenNMS"

DL8MFU

Diskussion "lokales vs. globales" Monitoring

OE2LSP, DG8NGN

IP-Ressourcen & Internetanbindung

Gesamtnetz: 44.224.128.0/17 (AS64680)

- 44.224.128.0/19 Datacenter #1 (z.Z. in Nürnberg)
- 44.224.160.0/19 Datacenter #2 (z.Z. in Aachen)
- 44.224.192.0/19 Datacenter #3 (z.Z. in Duisburg)
- 44.224.224.0/19 Standortunabhängiger Netzbereich

Anbindung: Alle Standorte sind mit Gigabit an das DFN (Deutsches Forschungsnetz) angebunden.

Anbindung

Es sollen möglichst viele HAMNET-Knoten mit Internetzugang an die HamCloud angebunden werden.

Anbindungstechnologien:

PPtP, L2TP (bevorzugt), SSTP

DNS-Round-Robin Terminierung der VPN-Tunnel:

tun.hc.r1.ampr.org has address 137.226.79.124

tun.hc.r1.ampr.org has address 141.75.245.252

tun.hc.r1.ampr.org has address 134.91.19.149

IP-Ressourcen:

/30-Netze aus 44.224.240.0/20 (max. 1024 VPN-Links)

Routing-Filter – eBGP visualisiert

