
LOGGING BEST PRACTICES

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.

---

https://de.wikipedia.org/wiki/Logging

EINFÜHRUNG (2)

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.

EINFÜHRUNG (3)

Logs geben die Möglichkeit Dinge zu einem späteren Zeitpunkt nachzuvollziehen.

WHAT'S IN A LOG MESSAGE? (1)

Minimale Lognachricht:

- Zeitstempel (idealerweise ISO 8601-kompatibel)
- Daten

WHAT'S IN A LOG MESSAGE? (2)

```
Oct 17 18:15:17 Example Message
```

WHAT'S IN A LOG MESSAGE? (3)

```
Oct 17 18:15:17 joschi-mbp15 joschi[47088]: Example Message
```

WHAT'S IN A LOG MESSAGE? (4)

```
2016-10-17T16:15:17.012Z joschi-mbp15 joschi[47088]: Example Message
```

STRUCTURED LOGGING

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

BEST PRACTICES

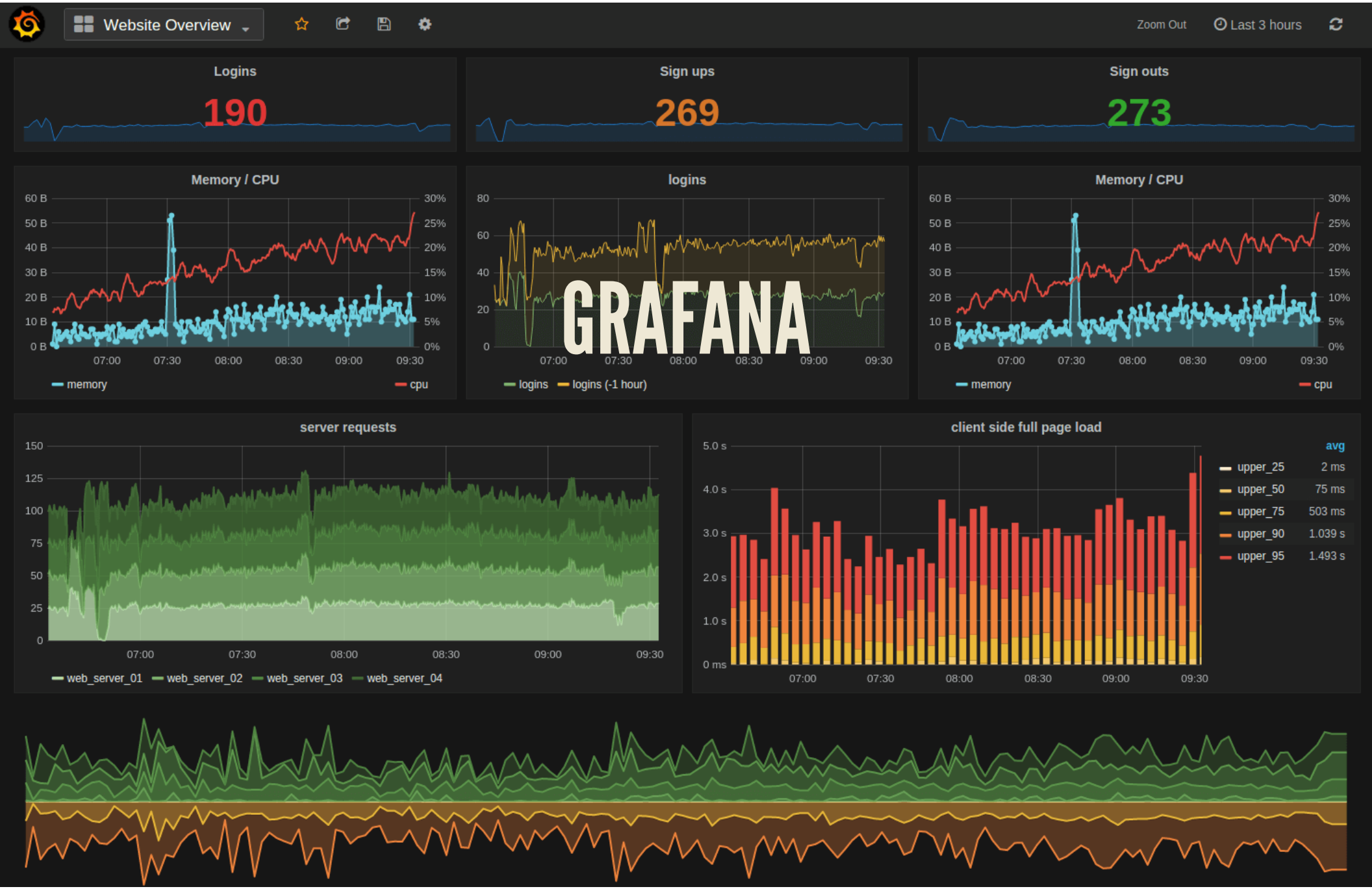
- Structured Logging verwenden
- Logmeldungen an zentraler Stelle sammeln
- Gemeinsames Vokabular für alle Systeme definieren
- Sinnvolle Daten loggen (nein, keine 32 GiB große Coredumps…)
- Log Levels nicht inflationär verwenden (es ist nicht alles ein ERROR)
- Request ID an den Systemgrenzen erzeugen

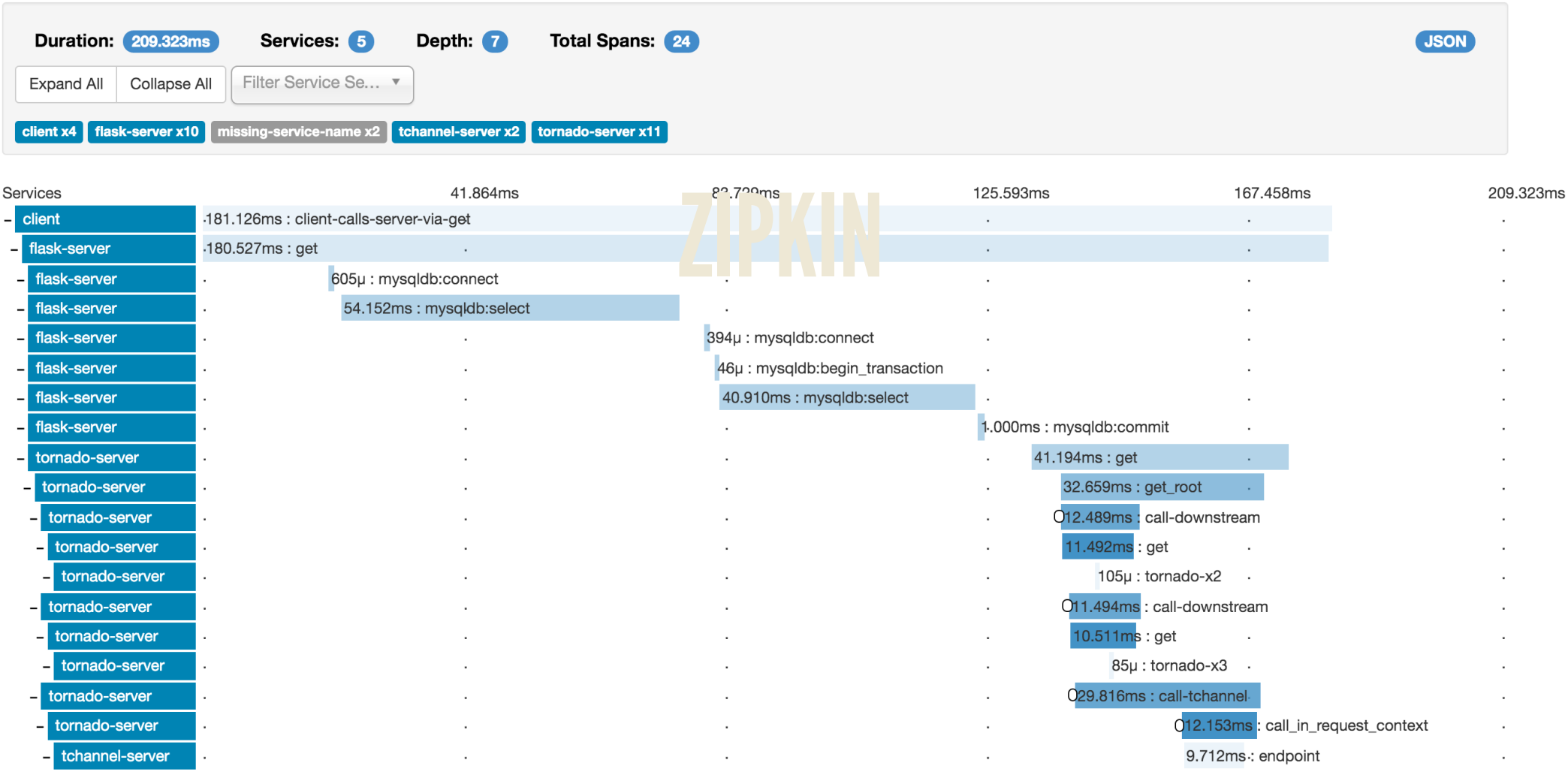
REQUEST IDS

- Request ID (eindeutige Kennung für eine Benutzerinteraktion)
- An den Systemgrenzen erzeugen und weiterreichen
- Bei verteiltem System: Request ID und Span ID (siehe Dapper oder Zipkin)
- Unschätzbar wertvoll bei Fehleranalyse, Sicherheitsaudits und Performance-Analysen

DIE LIEBE VERWANDTSCHAFT

- Metriken (z. B. Dropwizard Metrics)
- Request Tracing (z. B. Zipkin)
- Application Performance Monitoring (z. B. New Relic)


Website Overview
Zoom Out
Last 3 hours
Logins
190
Sign ups
269
Sign outs
273
Memory / CPU
60 B
50 B
40 B
30 B
20 B
10 B
0 B
30%
25%
20%
15%
10%
5%
0%
07:00
07:30
08:00
08:30
09:00
09:30
memory
cpu
logins
80
60
40
20
0
logins
logins (-1 hour)
GRAFANA
Memory / CPU
memory
cpu
server requests
150
125
100
75
50
25
0
web_server_01
web_server_02
web_server_03
web_server_04
client side full page load
5.0 s
4.0 s
3.0 s
2.0 s
1.0 s
0 ms
avg
upper_25 2 ms
upper_50 75 ms
upper_75 503 ms
upper_90 1.039 s
upper_95 1.493 s


Duration: 209.323ms
Services: 5
Depth: 7
Total Spans: 24
JSON
Expand All
Collapse All
Filter Service Se...
client x4
flask-server x10
missing-service-name x2
tchannel-server x2
tornado-server x11
Services
41.864ms
125.593ms
167.458ms
209.323ms
ZIPKIN
client
181.126ms : client-calls-server-via-get
flask-server
180.527ms : get
flask-server
605µ : mysqldb:connect
flask-server
54.152ms : mysqldb:select
flask-server
394µ : mysqldb:connect
flask-server
46µ : mysqldb:begin_transaction
flask-server
40.910ms : mysqldb:select
flask-server
1.000ms : mysqldb:commit
tornado-server
41.194ms : get
tornado-server
32.659ms : get_root
tornado-server
12.489ms : call-downstream
tornado-server
11.492ms : get
tornado-server
105µ : tornado-x2
tornado-server
11.494ms : call-downstream
tornado-server
10.511ms : get
tornado-server
85µ : tornado-x3
tornado-server
29.816ms : call-tchannel
tornado-server
12.153ms : call_in_request_context
tchannel-server
9.712ms : endpoint

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

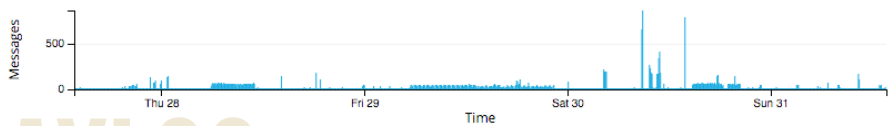
Chatty applications

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

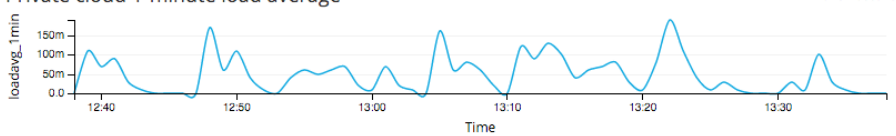
Global event rate

in a few seconds



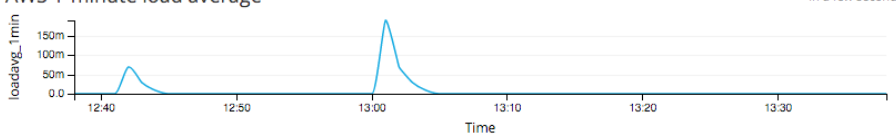
Private cloud 1-minute load average

in a few seconds



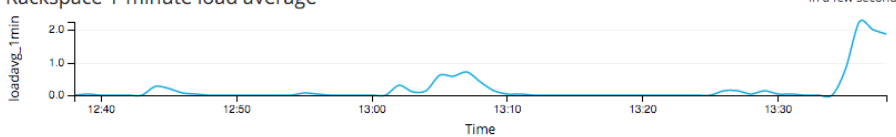
AWS 1-minute load average

in a few seconds



Rackspace 1-minute load average

in a few seconds



DEMO

Demo application on GitHub

KONTAKT


FRAGEN?

WEITERFÜHRENDE QUELLEN

- Graylog
- OWASP Logging Cheat Sheet
- 10 Tips for Proper Application Logging