Es werde Licht!

Monitoring jenseits von `tail` und `grep`

// Berlin Expert Days // 2014-04-04 //

Oliver B. Fischer

Beruf ☑

Blog ☑

Twitter ☑

Vorsichtige Annäherung

Behutsame Annäherung an das Objekt

2013 - Die Kontaktaufnahme

```
silberbrett:~ plexus$ ssh -l ofischer server01
Linux server01 3.4.4-guest #1 SMP Thu Jan 31 13:17:15 EST 2013 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar 31 21:57:24 2014 from 192.168.179.170
Hallo Oliver!
ofischer@ server01:~$ sudo -i
root@ server01:~$
```

2013 - Die Kontaktaufnahme

```
top - 22:55:49 up 10 days, 16:03,  3 users,  load average: 4.96, 5.06, 4.17
Tasks: 126 total,   6 running, 120 sleeping,   0 stopped,   0 zombie
Cpu(s): 98.5%us,  0.2%sy,  0.0%ni,  0.1%id,  0.0%wa,  0.0%hi,  0.0%si,  1.2%st
Mem:  37076628k total, 36837744k used,   238884k free,   895216k buffers
Swap:  4095996k total,    75012k used,  4020984k free, 19399636k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 4284 postgres  20   0  500m 318m 316m R   86  0.9  17:45.21 postgres
 4285 postgres  20   0  500m 318m 316m R   83  0.9  17:48.26 postgres
 4438 postgres  20   0  501m 319m 316m R   81  0.9  17:44.19 postgres
 3923 postgres  20   0  501m 411m 409m R   79  1.1  17:56.93 postgres
 4439 postgres  20   0  501m 402m 400m R   66  1.1  17:29.13 postgres
15899 ofischer  20   0 13.2g 6.3g  22m S    4 17.9 530:24.44 java
 4577 cmeier    20   0  688m 123m 6200 S    0  0.3   0:06.22 node
 5383 ofischer  20   0 19116 1280  940 R    0  0.0   0:00.08 top
36918 elastics  20   0 8782m 8.4g  20m S    0 23.8 818:26.48 java
    1 root      20   0  8404  652  616 S    0  0.0   0:18.85 init
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:43.93 ksoftirqd/0
    4 root      20   0     0    0    0 S    0  0.0   1:12.16 kworker/0:0
    5 root      20   0     0    0    0 S    0  0.0   0:00.00 kworker/u:0
    6 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/0
    7 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/1
    8 root      20   0     0    0    0 S    0  0.0   2:43.16 kworker/1:0
    9 root      20   0     0    0    0 S    0  0.0   0:50.40 ksoftirqd/1
   11 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/2
   12 root      20   0     0    0    0 S    0  0.0   0:00.00 kworker/2:0
   13 root      20   0     0    0    0 S    0  0.0   0:50.63 ksoftirqd/2
   14 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/3
   16 root      20   0     0    0    0 S    0  0.0   0:54.34 ksoftirqd/3
   17 root       0 -20     0    0    0 S    0  0.0   0:00.00 cpuset
   18 root       0 -20     0    0    0 S    0  0.0   0:00.00 khelper
   19 root      20   0     0    0    0 S    0  0.0   0:00.00 kdevtmpfs
```

2013 - Die Kontaktaufnahme

```
  1  [                                                      0.0%]     Tasks: 80 total, 1 running
  2  [                                                      0.0%]     Load average: 0.26 0.22 0.36
  3  [|                                                     0.7%]     Uptime: 10 days, 02:14:53
  4  [                                                      0.0%]
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||||22053/36207MB]
  Swp[||                                                   75/3999MB]

    PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
  48703 logstash   20   0  579M  258M 11004 S  0.0  0.7  1h20:21 /usr/bin/java -Xmx256m -Djava.io.tmpdir=/var/lib/logstash/ -jar /opt/lo
  65145 app        20   0 13648   964   764 S  0.0  0.0  0:00.08 /usr/bin/pager
   2105 root       20   0 10588   820   776 S  0.0  0.0  1:01.27 /usr/bin/rsync --no-detach --daemon --config /etc/rsyncd.conf
  36918 elastics   20   0 8782M 8622M 20704 S  0.0 23.8  6h37:53 /usr/lib/jvm/java-7-oracle/bin/java -Xms8g -Xmx8g -Xss256k -Djava.awt.h
  45692 ofischer   20   0 13.3G 12.2G 11588 S  0.0 34.5  9h19:21 /usr/lib/jvm/java-7-oracle/bin/java -cp /srv/application/mm/
   2227 root       20   0 37224  1660  1544 S  0.0  0.0  0:11.08 /usr/lib/postfix/master
  39080 postgres   20   0  499M 24884 24588 S  0.0  0.1  1:26.67 /usr/lib/postgresql/9.1/bin/postgres -D /var/lib/postgresql/9.1/main -c
   1841 db         20   0 71408  3800  2640 S  0.0  0.0  0:10.83 /usr/lib/postgresql/9.1/bin/psql db_prod
   1755 root       20   0  3968   468   464 S  0.0  0.0  0:00.00 /usr/sbin/acpid
   1765 daemon     20   0 18764   228   216 S  0.0  0.0  0:00.02 /usr/sbin/atd
   1775 root       20   0  5964   204   200 S  0.0  0.0  0:00.00 /usr/sbin/collectdmon -P /var/run/collectdmon.pid -- -C /etc/collectd/c
   1803 root       20   0 23872   980   816 S  0.0  0.0  0:03.10 /usr/sbin/cron
   1931 ntp        20   0 38388  1664  1508 S  0.0  0.0  1:19.34 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 105:109
   1722 root       20   0  127M  1120   988 S  0.0  0.0  0:15.92 /usr/sbin/rsyslogd -c4
   2113 root       20   0 49224   696   588 S  0.0  0.0  0:00.86 /usr/sbin/sshd
   1712 ofischer   20   0 26632  1492  1000 S  0.0  0.0  0:00.04 SCREEN
   1713 ofischer   20   0 22900  4316  1612 S  0.0  0.0  0:00.40 bash -l
   1776 root       20   0  202M  1324   960 S  0.0  0.0  8:24.87 collectd -C /etc/collectd/collectd.conf -f
   7724 ofischer   20   0 19892  1636  1076 R  0.0  0.0  0:00.06 htop
      1 root       20   0  8404   652   616 S  0.0  0.0  0:18.21 init [2]
   5775 postfix    20   0 39288  2360  1864 S  0.0  0.0  0:00.02 pickup -l -t fifo -u -c
  39085 postgres   20   0  500M 15144 14224 S  0.0  0.0  1:43.75 postgres: autovacuum launcher process
   7462 postgres   20   0  500M  3876  2516 S  0.0  0.0  0:00.00 postgres: app db_prod 127.0.0.1(39173) idle
   7463 postgres   20   0  500M  3872  2512 S  0.0  0.0  0:00.00 postgres: app db_prod 127.0.0.1(39174) idle
   7464 postgres   20   0  500M  3872  2512 S  0.0  0.0  0:00.00 postgres: app db_prod 127.0.0.1(39175) idle
```

2013 - Die Kontaktaufnahme

```
  1  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||98.0%]     Tasks: 81 total, 1 running
  2  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||96.1%]     Load average: 8.78 1.28 1.51
  3  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||97.4%]     Uptime: 10 days, 02:57:48
  4  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||96.0%]     Hostname: billing1
  Mem[|||||||||||||||||||||||||||||||||||||||||||||||||22984/36207MB]     Time: 09:50:33
  Swp[||                                                    75/3999MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
48703 logstash  20   0  579M  253M 11004 S  0.0  0.7  1h20:58  `- /usr/bin/java -Xmx256m -Djava.io.tmpdir=/var/lib/logstash/ -jar /op
45692 ofischer  20   0 13.3G 12.2G 11588 S 307. 34.5  9h47:41  `- /usr/lib/jvm/java-7-oracle/bin/java -cp /srv/application
39080 postgres  20   0  499M 24884 24588 S  0.0  0.1  1:26.85  `- /usr/lib/postgresql/9.1/bin/postgres -D /var/lib/postgresql/9.1/mai
39086 postgres  20   0 70416  1248   416 S  0.0  0.0  4:13.34  |    `- postgres: stats collector process
39085 postgres  20   0  500M 15144 14224 S  0.0  0.0  1:43.90  |    `- postgres: autovacuum launcher process
39084 postgres  20   0  499M 13572 13288 S  0.0  0.0  3:52.65  |    `- postgres: wal writer process
39083 postgres  20   0  500M  421M  420M S  0.0  1.2  7:54.67  |    `- postgres: writer process
 9235 postgres  20   0  500M  3856  2496 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39774) idle
 9234 postgres  20   0  500M  3864  2500 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39773) idle
 9075 postgres  20   0  500M  3868  2504 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39770) idle
 9074 postgres  20   0  500M  3864  2500 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39769) idle
 9073 postgres  20   0  500M  3868  2504 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39768) idle
 9072 postgres  20   0  501M 10772  8600 S  0.0  0.0  0:00.05  |    `- postgres: moneymaker db_prod 127.0.0.1(39767) idle
 9071 postgres  20   0  501M 20592 18356 S  1.0  0.1  0:00.49  |    `- postgres: moneymaker db_prod 127.0.0.1(39766) idle
 9070 postgres  20   0  501M 43680 41140 S  9.0  0.1  0:02.37  |    `- postgres: moneymaker db_prod 127.0.0.1(39765) idle
 9069 postgres  20   0  501M 61428 58868 S 22.0  0.2  0:05.53  |    `- postgres: moneymaker db_prod 127.0.0.1(39764) idle
 9068 postgres  20   0  501M  193M  190M S 37.0  0.5  0:29.92  |    `- postgres: moneymaker db_prod 127.0.0.1(39763) idle
 9067 postgres  20   0  500M  3864  2504 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39762) idle
 9066 postgres  20   0  500M  3868  2508 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39761) idle
 9065 postgres  20   0  500M  3856  2496 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39760) idle
 9064 postgres  20   0  500M  3864  2500 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39759) idle
 9063 postgres  20   0  500M  3860  2496 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39758) idle
 9062 postgres  20   0  500M  3868  2504 S  0.0  0.0  0:00.00  |    `- postgres: moneymaker db_prod 127.0.0.1(39757) idle
 1842 postgres  20   0  509M  416M  411M S  0.0  1.2  0:34.82  |    `- postgres: moneymaker db_prod [local] idle
36918 elastics  20   0 8782M 8622M 20704 S  0.0 23.8  6h38:36  `- /usr/lib/jvm/java-7-oracle/bin/java -Xms8g -Xmx8g -Xss256k -Djava.a
 6476 cfrei     20   0 53432 13760   788 S  0.0  0.0  8:26.40  `- SCREEN -c /usr/share/byobu/profiles/byoburc shell
61637 cfrei     20   0 26288  1264  1260 S  0.0  0.0  0:01.30  |    `- /bin/bash
  636 cfrei     20   0 74684  3164  3140 S  0.0  0.0  0:00.75  |    |    `- /usr/lib/postgresql/9.1/bin/psql -h db02.pb.local -U cfrei
56274 cfrei     20   0 26204  7488  1476 S  0.0  0.0  0:00.38  |    `- /bin/bash
 1839 root      20   0 26008  1116   876 S  0.0  0.0  0:00.00  |    |    `- sudo -u moneymaker psql db_prod
 1841 db        20   0 71408  3800  2640 S  0.0  0.0  0:10.83  |    |         `- /usr/lib/postgresql/9.1/bin/psql db_prod
65144 db        20   0 10720   776   620 S  0.0  0.0  0:00.00  |    |              `- sh -c /usr/bin/pager
65145 db        20   0 13648   964   764 S  0.0  0.0  0:00.08  |    |                   `- /usr/bin/pager
```

2013 - Die Kontaktaufnahme

tail -F /var/log/glassfish/server.log

```
[2014-03-31T23:01:01.144+0000] [glassfish 4.0] [INFO] [NCLS-CORE-00087] [javax.enterprise.system.core] [tid: _ThreadID=20
_ThreadName=RunLevelControllerThread-1396306859234] [timeMillis: 1396306861144] [levelValue: 800] [[
  Grizzly Framework 2.3.11 started in: 2ms - bound to [/0.0.0.0:3700]]]

[2014-03-31T23:01:01.867+0000] [glassfish 4.0] [INFO] [AS-WEB-GLUE-00198] [javax.enterprise.web] [tid: _ThreadID=19
_ThreadName=RunLevelControllerThread-1396306859229] [timeMillis: 1396306861867] [levelValue: 800] [[
  Created HTTP listener http-listener-1 on host/port 0.0.0.0:8080]]

[2014-03-31T23:01:01.908+0000] [glassfish 4.0] [INFO] [AS-WEB-GLUE-00198] [javax.enterprise.web] [tid: _ThreadID=19
_ThreadName=RunLevelControllerThread-1396306859229] [timeMillis: 1396306861908] [levelValue: 800] [[
  Created HTTP listener http-listener-2 on host/port 0.0.0.0:8181]]

[2014-03-31T23:01:01.960+0000] [glassfish 4.0] [INFO] [AS-WEB-GLUE-00198] [javax.enterprise.web] [tid: _ThreadID=19
_ThreadName=RunLevelControllerThread-1396306859229] [timeMillis: 1396306861960] [levelValue: 800] [[
  Created HTTP listener admin-listener on host/port 0.0.0.0:4848]]

[2014-03-31T23:01:02.131+0000] [glassfish 4.0] [INFO] [AS-WEB-GLUE-00200] [javax.enterprise.web] [tid: _ThreadID=19
_ThreadName=RunLevelControllerThread-1396306859229] [timeMillis: 1396306862131] [levelValue: 800] [[
  Created virtual server server]]

[2014-03-31T23:01:02.139+0000] [glassfish 4.0] [INFO] [AS-WEB-GLUE-00200] [javax.enterprise.web] [tid: _ThreadID=19
_ThreadName=RunLevelControllerThread-1396306859229] [timeMillis: 1396306862139] [levelValue: 800] [[
  Created virtual server __asadmin]]
```

2013 - Die Kontaktaufnahme

```
#!/bin/bash
echo -n "Script started at: "; date -u

echo
echo "This script lists the events with the largest number of „
echo "updates"

echo

sql="select * from view_events_mult_events_help order by c_event_cnt desc limit 10;"
echo "$sql" | /usr/bin/psql -d db_prod

echo -n "Script finished at: "; date -u
echo
printf "%5s[#By#the#way#]%56s\n" |tr " " "-" | tr "#" " "
/usr/games/fortune -s
printf "%75s\n" |tr " " "-"
```

2013 - Die Kontaktaufnahme

```
crontab -l
```

```
0 8 * * *      /home/user/scripts/show-trend 2>&1 | mail -s "JOB: Trend"
0 18 * * *     /home/user/scripts/show-youngest 2>&1 | mail -s "JOB: Youngest"
0 18 * * *     /home/user/scripts/show-status 2>&1 | mail -s "JOB: Status Overview"
0 8 * * *      /home/user/scripts/show-versions 2>&1 | mail -s "JOB: Event versions"
1 8 * * *      /home/user/scripts/show-versions_per-day 2>&1 | mail -s "JOB: Events per Day"
23 */2 * * *   /home/user/scripts/show-diffs 2>&1 | mail -s "JOB: Diffs"
0 0 * * *      /home/user/scripts/show-discusage 2>&1 | mail -s "JOB: Diskusage"
0 0 * * *      /home/user/scripts/show-databases 2>&1 | mail -s "JOB: Existing databases"
0 16 * * *     /home/user/scripts/show-strange-stuff 2>&1 | mail -s "JOB: Strange stuff"
0 16 * * *     /home/user/scripts/show-illegal-stuff 2>&1 | mail -s "JOB: Illegal events"
```

Bin ich der Einzige?

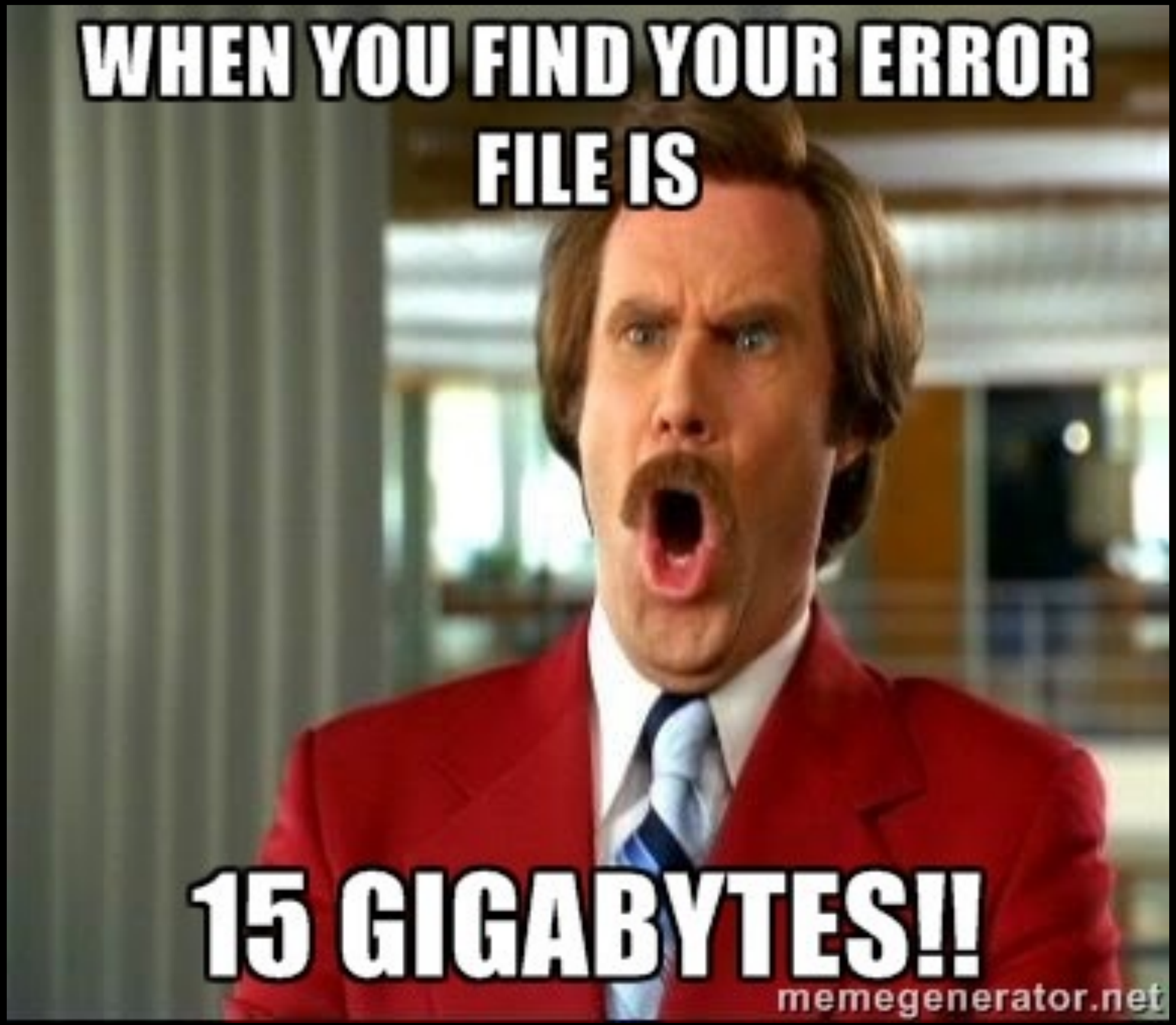
Oder gibt es viele in dieser Situation?

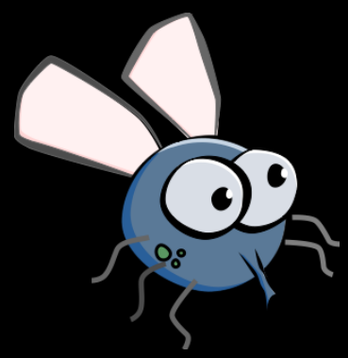
```
tail -f /var/log/server.log | grep -A 20 Exception
```

```
cat /var/log/server.log_* | grep -A 20 Exception
```

```
find . -name „server*" | parallel -P 8 grep sync {}
```

Mein `grep` ist größer als Dein `grep`?


WHEN YOU FIND YOUR ERROR FILE IS
15 GIGABYTES!!
memegenerator.net



Vielleicht Hadoop?

Das integrierte Monitoring

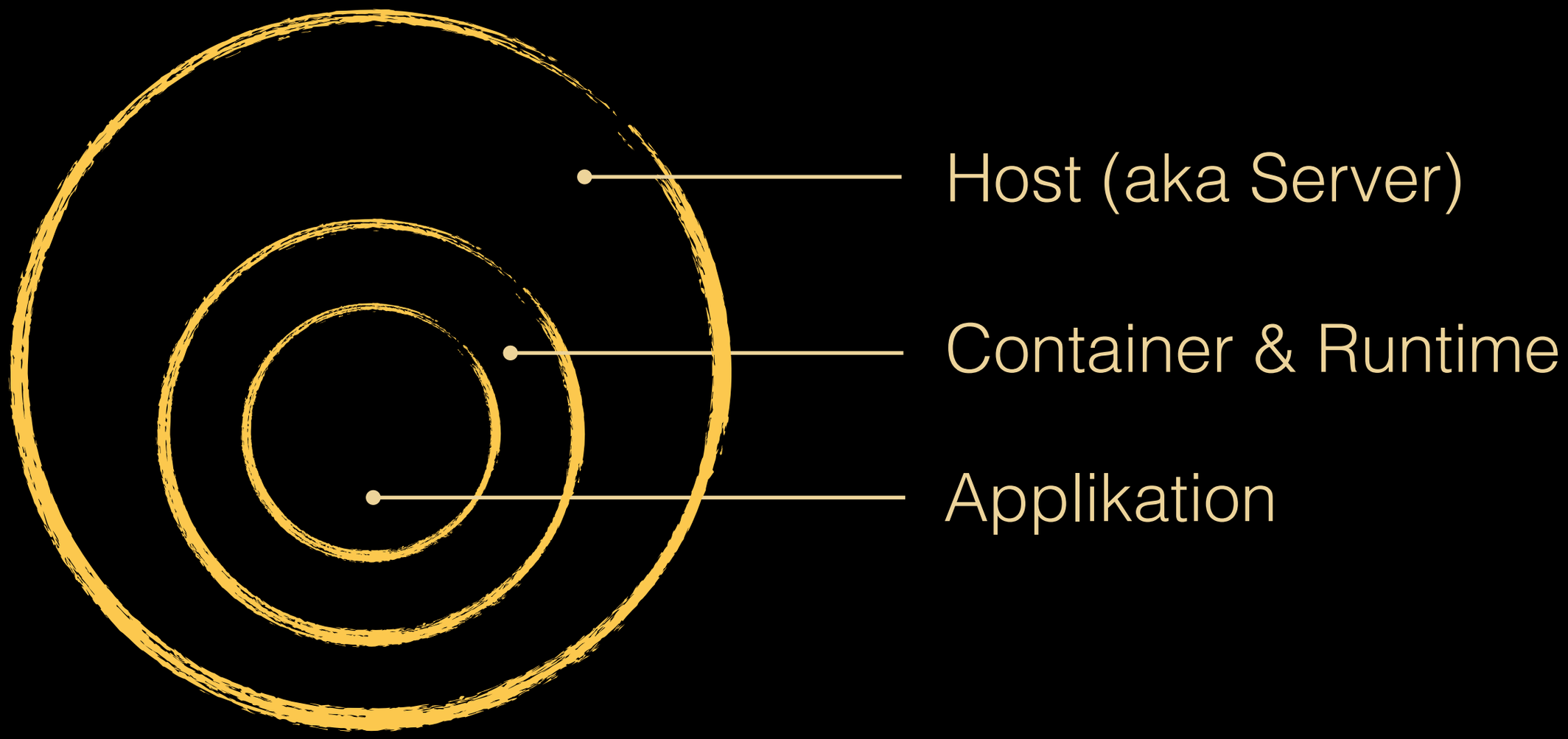
Es wächst zusammen, was zusammen gehört

Was wir gerne hätten

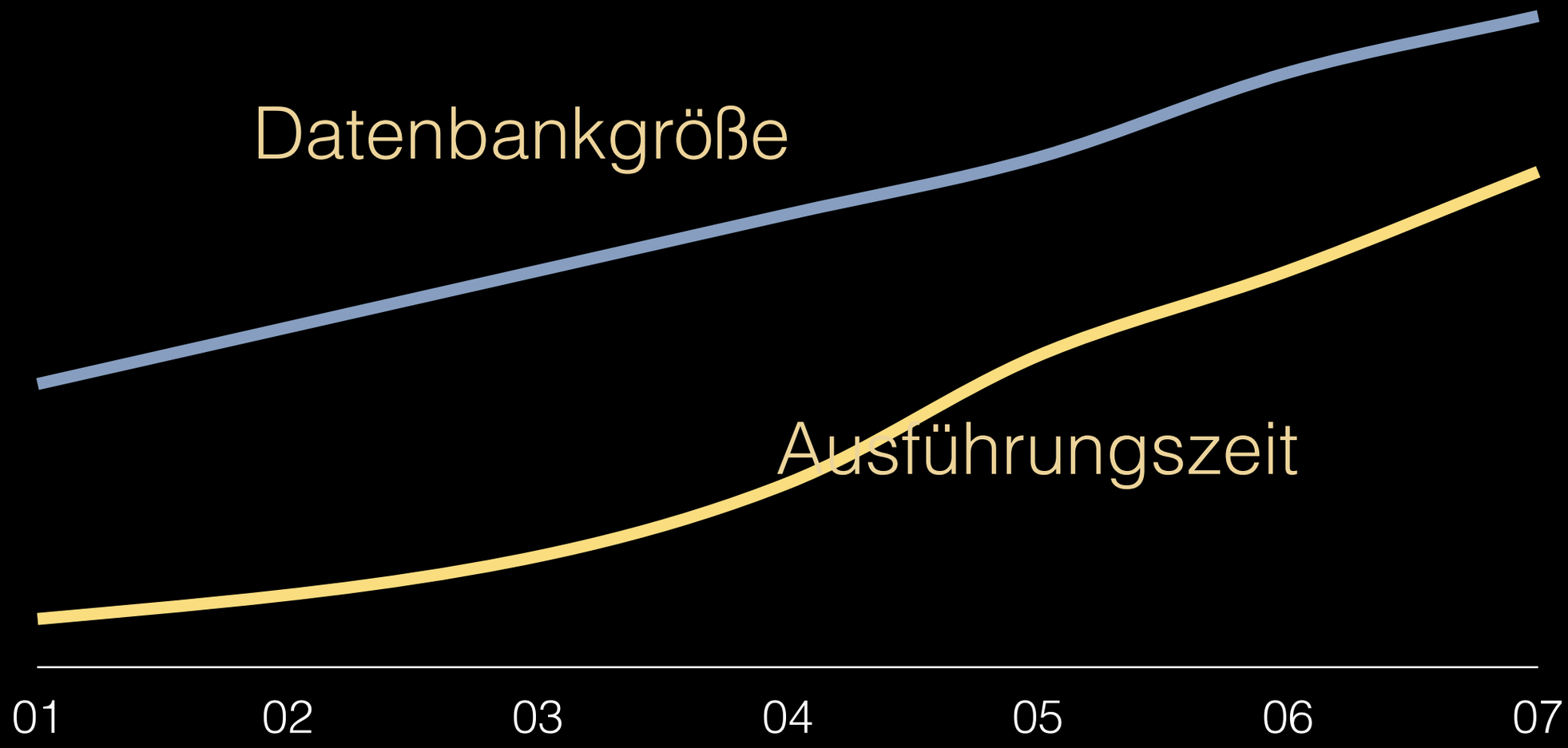
Was wir oft haben

Womit wir zufriednen wären

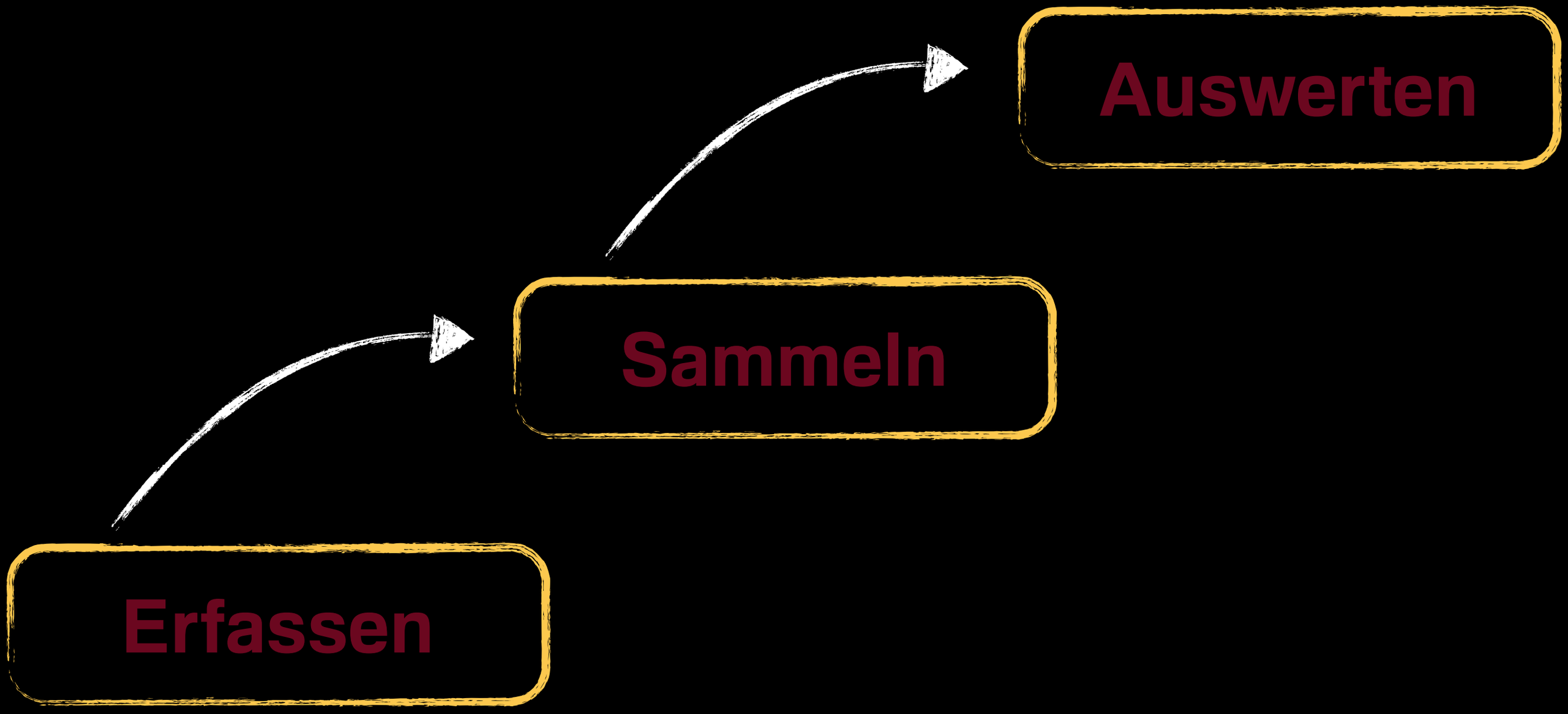
Was müssen wir wissen?



Zusammenhänge erkennen



Dreisprung…



Metriken identifzieren

- Was ist kritisch für uns?
- Was ist schon einmal kaputt gegangen?
- Verdienen wir damit Geld?
- Kostet uns das Geld?
- Gibt es ein Service Level Agreement?
- Was sagt mir mein Bauchgefühl?

Design for Diagnostability

Funktionalität
Zweckdienlichkeit
Robustheit
Sicherheit
Verfügbarkeit
Geschwindigkeit
Zuverlässigkeit
Portierbarkeit

Untersuchbarkeit

Datenhaltung

- Drei Kategorien: kurzfristige, mittel- und langfristige Daten
- Ältere Daten zusammenfassen
- Daten für historische Vergleich vergleichbar halten
- Anzahl der dauerhaften Metriken beschränken

Eventsourcing

„Capture all changes to an application state as a sequence of events.“

```
{ time => 2014-02-03T00:09, action => UPDATE, value => 16, user => foobar }
{ time => 2014-02-08T00:09, action => UPDATE, value => 19, user => snafu }
{ time => 2014-02-09T10:09, action => UPDATE, value => 16, user => foobar }
```

- „Loggen“ auf Architekturebene
- Replay der Events möglich

Butter bei die Fische

Lasset den Worten Taten folgen

Richtig loggen

- Einfacher Text
- JSON
- XML
- Key-Value-Paare

Logmessages müssen maschinenlesbar sein

Logmessages müssen menschenlesbar sein

Richtig loggen

```
logger.info("Interval intervalStart='{}' - intervalEnd='{}' for eventType='{}' " +
            "does not need synchronisation since state='insync' ." +
            "Found eventsES='{}' events in ElasticSearch and " +
            "eventsDB='{}' in the database.",
            interval.getStart()  interval.getEnd(),
            clazz.getSimpleName()
            inElasticSearch, inDatabase);
```

```
[2014-04-02T13:10:42.569+0000] [glassfish 4.0] [INFO] []
[application.elasticsearch.indexer] [tid: _ThreadID=167 _ThreadName=__ejb-thread-pool11]
[timeMillis: 303848789833] [levelValue: 800] [[ Interval
intervalStart=2014-04-02T09:10:00.005Z - intervalEnd=2014-04-02T13:10:00.005Z for
eventType=FooBarEvent does not need synchronisation since state='insync'. Found
eventsES='8' events in ElasticSearch and eventsDB='8' in the database.]]
```

Richtig loggen

java.util.logging ⟷ SLF4J

Formatiert Zahlen	Formatiert Zahlen nicht
3.340.393,89	3340393.89
3,340,393.89	3340393.89

Richtig loggen

```
2014-04-04T10:15:00.000
2014-04-04T10:15:00.000+08:00
2014-04-04T10:15:00.000+02:00
2014-04-04T10:15:00.000+01:00
2014-04-04T10:15:00.000-01:00
2014-04-04T10:15:00.000+00:00
```

Don’t make me think! Nimm UTC!

Richtig loggen

```
12 582 912

12 582 912 MiB

12 884 901 888 Bytes
```

Don’t make me think!

Nutze Einheiten!

Vermeide Umrechnungen!

Messen

```
public void doSomeCriticalStuff()
{
    long start = System.currentTimeMillis();

     // do critical stuff

    long end = System.currentTimeMillis();

    logger.debug("Operation took execTime={} ms.", end - start);
}
```

```
public void doSomeCriticalStuff()
{
    StopWatch watch = new StopWatch();

    watch.start();

    // do critical stuff

    watch.stop();

    logger.debug("Operation took execTime={} ms.", watch.getTime());
}
```

Metriken erheben

„Metrics is a Java library which gives you unparalleled insight into what your code does in production.“

Counter

Meter

Gauges

Timer

Histogramme

Metriken erheben

Gauges	The instantaneous value of something.
Counter	An incrementing and decrementing value.
Meter	The average rate of events over a period of time.
Timer	A histogram of durations and a meter of calls.
Histogramms	The statistical distribution of values in a stream of data.

Metriken erheben

```
metricsRegistry = new MetricRegistry();

metricsRegistry.registerAll(new MemoryUsageGaugeSet());
```

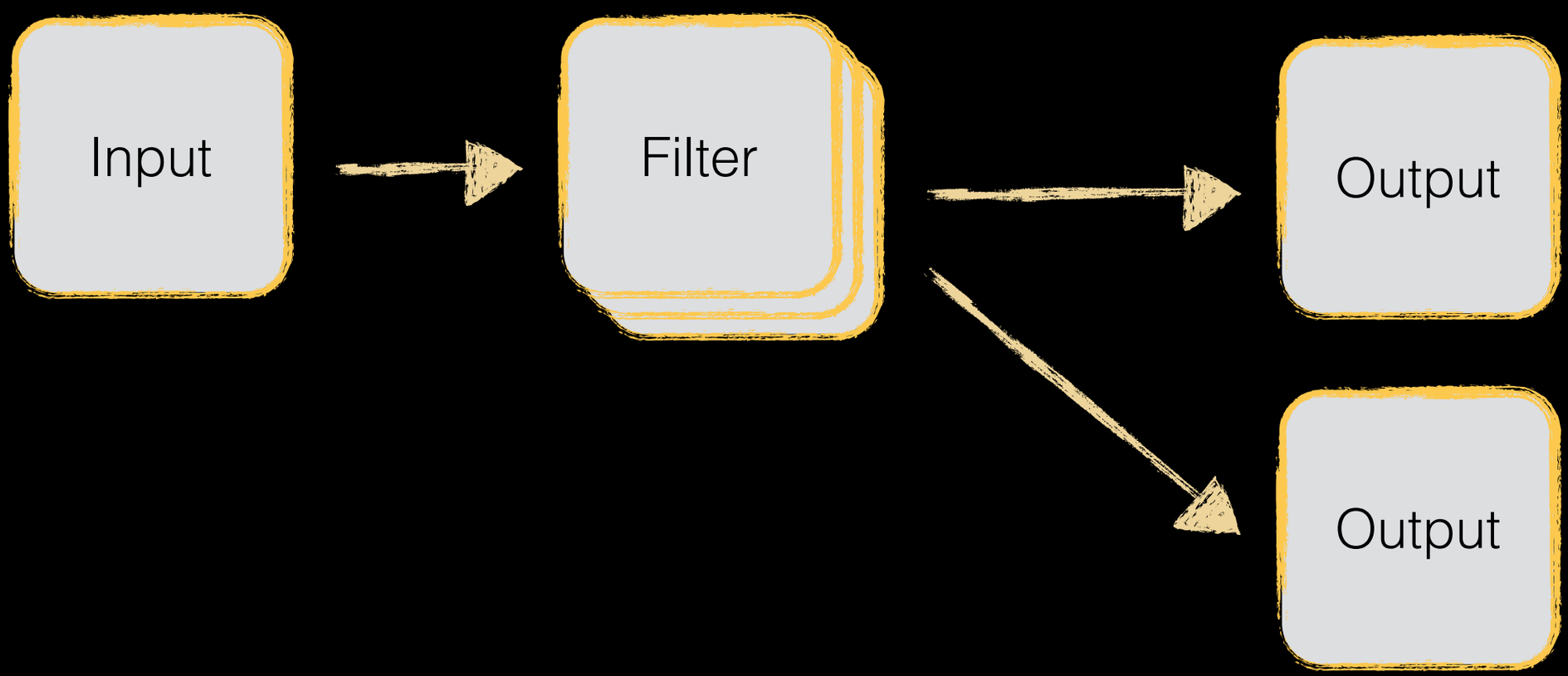
```
metricsRegistry.register(name(OperationService.class, "customers"), new Gauge<Integer>()
{
    @Override
    public Integer getValue() {
        return database.getCustomerCountByState(ACTIVE);
    }
});
```

```
@POST
@Path("api/event")
public Response handleEvent(EventJTO e) throws InvalidEventException
{
   Meter restRequests = metricsRegistry.meter(name(Resource.class, "events", "requests"));
   restRequests.mark();

   // process the event

}
```

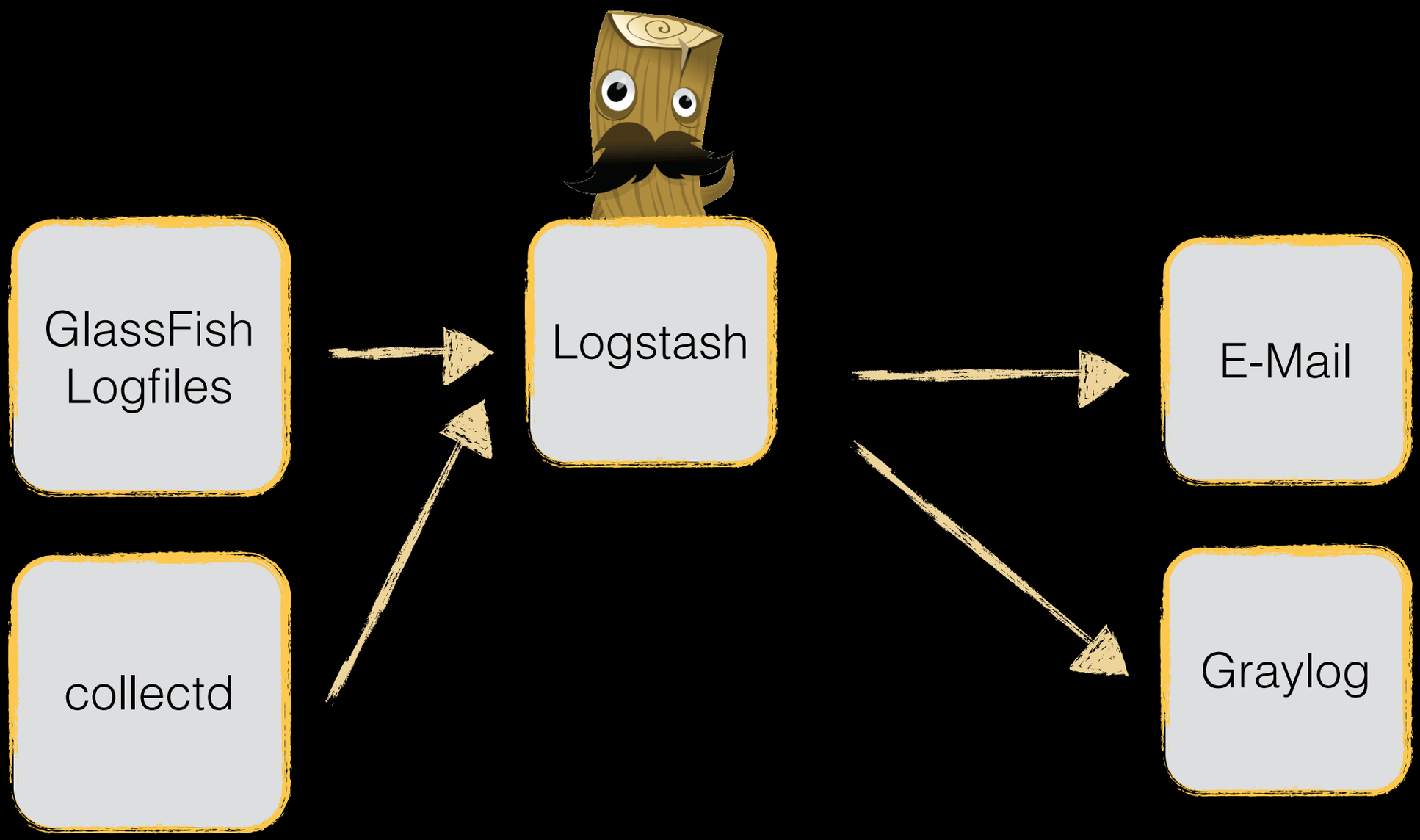
Logstash - Daten sammeln

„Unix pipes on sterioids“

Logstash - Daten sammeln



Logstash - Daten sammeln



Logstash - Daten sammeln

```
input {
  file {
    path => "/var/log/glassfish/server.log"
    type => "glassfish4"
  }
}



filter {
    # Das Logfile wird zeilenweise eingelesen. Eine Zeile ist ein Event.
     # Jetzt machen wir aus mehreren Zeilen ein Event!
     multiline {
       pattern => "^\[%{TIMESTAMP_ISO8601:timestamp}"
       negate => true
       what => previous
     }
}
```

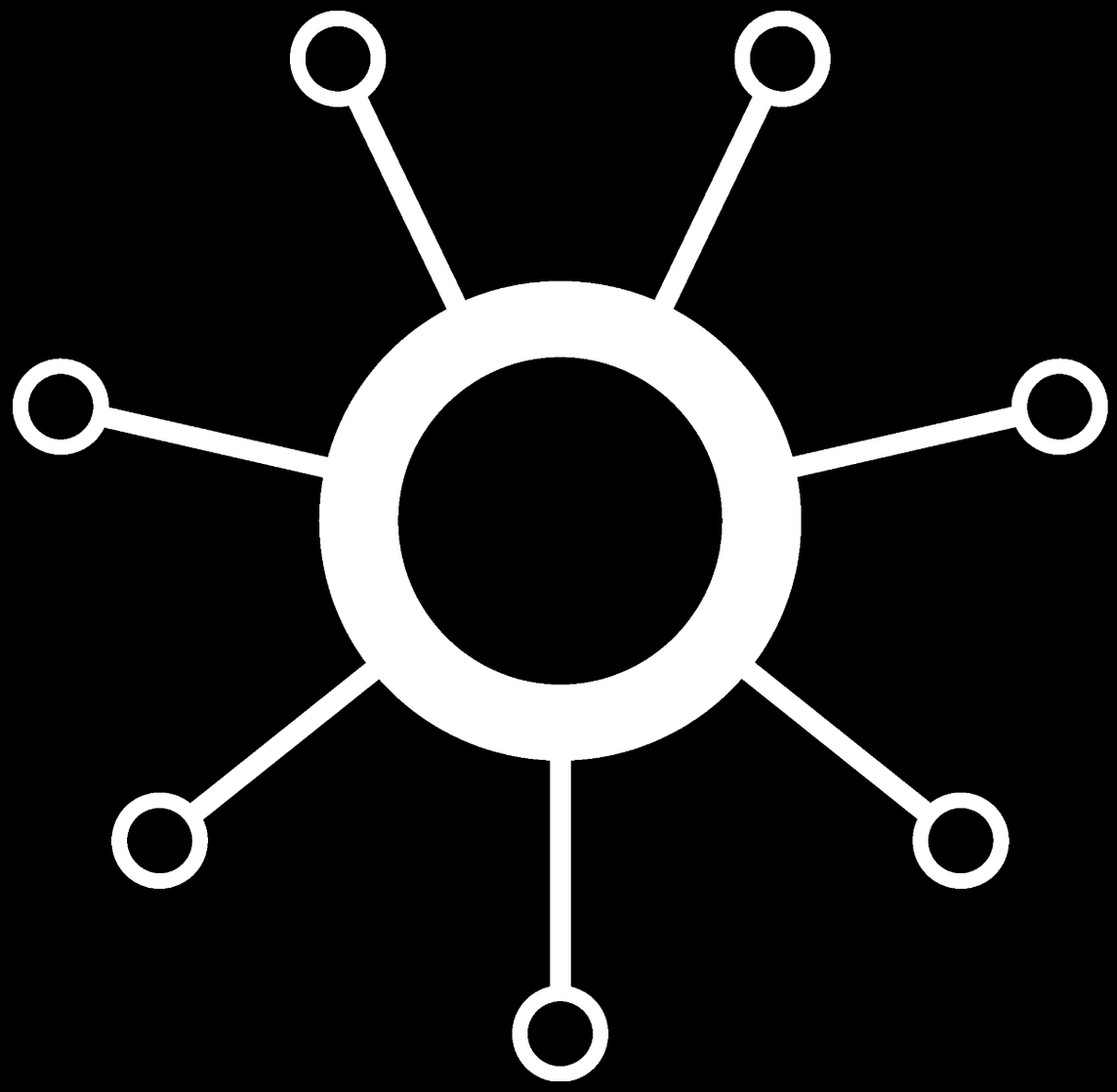
Logstash - Daten sammeln

```
grok {
   match => ["message",
             "\[%{TIMESTAMP_ISO8601:event_time}\]%{SPACE}\[%{DATA:product}\]%{SPACE}\[%
{WORD:loggerlevel}\]%{SPACE}\[%{DATA:messageid}\]%{SPACE}\[%{DATA:logger}\]%{GREEDYDATA}"
}

kv {
      prefix => "kv_"
      trim => "\[\]'"
}
```

Logstash - Daten sammeln

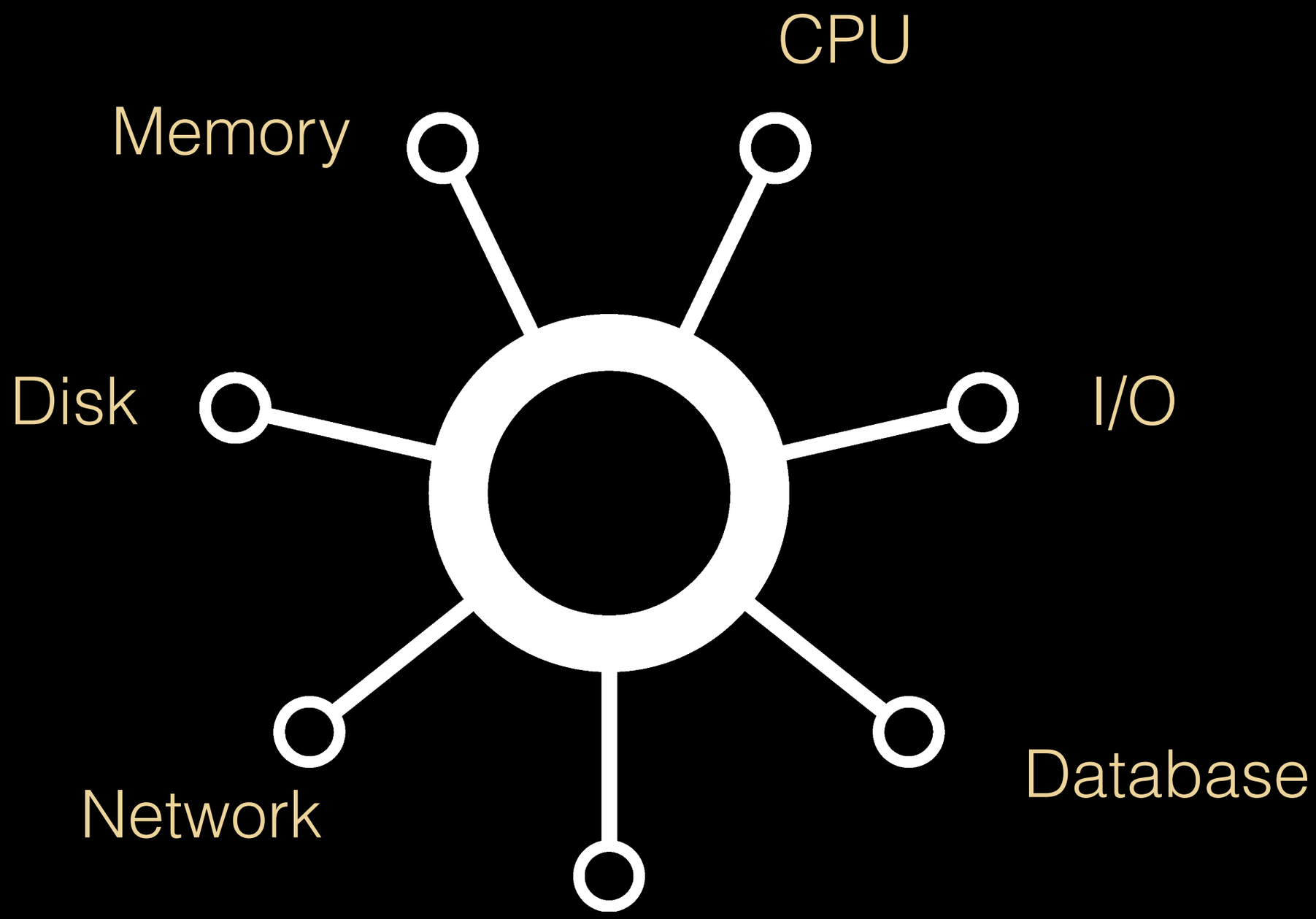
```
input {
  collectd {
    type => "collectd"
    add_field => { message => "This comes from collectd" }
  }
}
```

collectd



„The System statistics collection deamon“

collectd



… und viel viel mehr …

collectd

```
FQDNLookup true

# Load the logfile plugin to be able to write a logfile
LoadPlugin "logfile"

<Plugin logfile>
  LogLevel debug
</Plugin>


LoadPlugin "network"
<Plugin "network">
    Server "server01.pb.local" "25826"
</Plugin>

LoadPlugin "memory"
LoadPlugin "cpu"
LoadPlugin "vmem"
LoadPlugin "disk"
LoadPlugin "swap"
LoadPlugin "load"
LoadPlugin "df"

<Plugin "df">
        FSType "ext4"
</Plugin>
```

Auswertung

Kibana - visualize logs and time-stamped data

{ GRAYLOG 2

Graphite - Scalable Realtime Graphing

RIEMANN

Selfmade (HTML, JavaScript, Java, …)

Auswertung - Kibana

GlassFish

a month ago to a few seconds ago

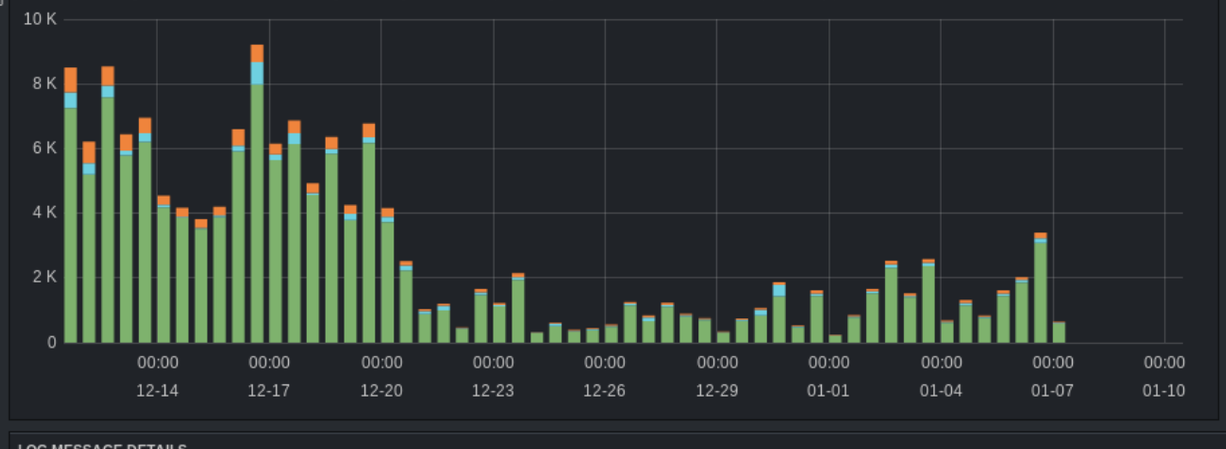
Pinned | Log (all) | Log: info level | Log: warning level | Log: severe level

QUERY

FILTERING

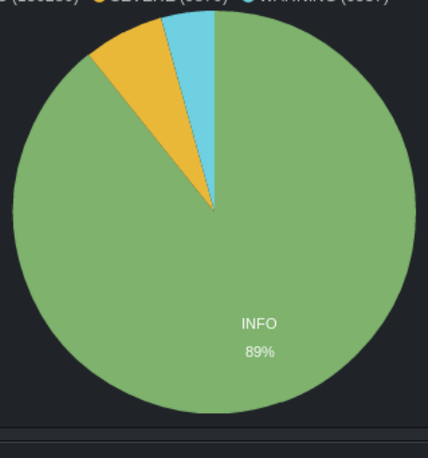
LOG SUMMARY

View | Log: info level (136273) Log: warning level (6535) Log: severe level (9868) count per **12h** | (**152676** hits)



LOG LEVEL DISTRIBUTION

INFO (136280) SEVERE (9870) WARNING (6537)



LOG LEVEL TREND (1D)

-6.66% (Log (all))
-6.85% (Log: info level)
-5.62% (Log: warning level)
-6.69% (Log: severe level)

LOG MESSAGE DETAILS

0 to **100** of 500 available for paging

event_time	logger	level	message
2014-01-07T05:43:31.853+0000	org.[redacted].engine.hooks	INFO	V[redacted]l: 3[redacted]c2...
2014-01-07T05:43:29.656+0000	[redacted]	INFO	([redacted])[#] [#|2014-01-07T05:43:29.656+0000|INFO|gla...
2014-01-07T05:42:38.802+0000	com.[redacted].dPersistenceImpl	INFO	gincredential" ></property> </properties>...
2014-01-07T05:42:28.599+0000	com.[redacted].tenceImpl	INFO	#|2014-01-07T05:42:23.439+0000|INFO|[redacted].resourc...
2014-01-07T05:41:16.213+0000	[redacted]CE	INFO	[redacted]=...
2014-01-07T05:41:07.996+0000	com.[redacted].ProvisioningSingleton	INFO	[redacted]
2014-01-07T05:40:36.225+0000	org.[redacted].engine.hooks	INFO	hreadID=148;_ThreadName=Thread-2;|Receiving process execution event from ac...
2014-01-07T05:37:45.218+0000	com.[redacted].BusinessProcessManagementServiceImpl	INFO	[redacted]able: task= [redacted]e Chang...
2014-01-07T05:37:41.944+0000	org.[redacted].engine.hooks	INFO	[redacted]ThreadID=60455;_ThreadName=Thread-2;|Prov...
2014-01-07T05:34:55.192+0000	com.[redacted].ProvisioningServiceImpl	INFO	55 state=AVAILABLE null(1047146796) count=1 size=1024 d...

Auswertung - Graylog 2

- Lucene-basierte Abfragesprache
- Dashboards
- Charts
- Berechtigungen
- LDAP-Unterstützung
- Explizite Endpunkte für Clients
- Extraktoren für Werte
- OpenSource @ GitHub
- …

Auswertung - Graylog 2

GRAYLOG2 Search Streams Dashboards Sources System 6 msg/s on 1 node.

Search in the last 8 hours | Choose a saved search

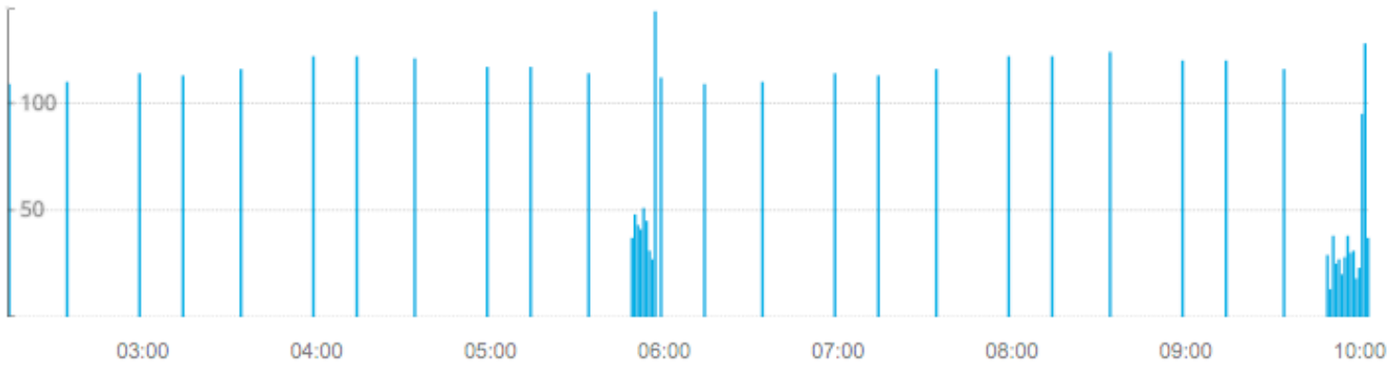
source:[redacted].glassfish4 AND logger:[redacted].elasticsearch.indexer AND rating:<7

Search results

Export | Save search

Found 3,719 messages.

Total result histogram



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

Timestamp	Source	Message
2014-04-03 08:14:22.438	[redacted]1.glassfish4	[2014-04-03T08:14:22.438+0000] [glassfish 4.0] [INFO] [] [[redacted]ch.indexer] [tid: _ThreadID=176 _ThreadName=__ejb-thread-pool7] [timeMillis: 1396512862438] [levelValue: 800] [[redacted]]
2014-04-03 08:14:22.437	[redacted].glassfish4	[2014-04-03T08:14:22.437+0000] [glassfish 4.0] [INFO] [] [moneymaker.elasticsearch.indexer] [tid: _ThreadID=176 _ThreadName=__ejb-thread-pool7] [timeMillis: 1396512862437] [[redacted]events DB=29 in the database.]]
2014-04-03 08:14:22.026	[redacted].glassfish4	[2014-04-03T08:14:22.026+0000] [glassfish 4.0] [INFO] [] [[redacted].elasticsearch.indexer] [tid: _ThreadID=176 _ThreadName=__ejb-thread-pool7] [timeMillis: 1396512862026] [[redacted]]

Search results

Found 3,719 messages in 80ms, searched in 1 index.

Message fields of current page / all

- [ ] event_recieved
- [ ] event_time
- [ ] facility
- [ ] fqdn
- [ ] kv__ThreadID
- [ ] kv__ThreadName
- [ ] kv_eventType
- [ ] kv_eventsDB
- [ ] kv_eventsES
- [ ] kv_execTime
- [ ] kv_indexedEvents
- [ ] kv_intervalEnd
- [ ] kv_intervalStart
- [ ] kv_state
- [ ] level
- [ ] logger
- [ ] loggerlevel
- [x] message
- [ ] nm_eventsDB
- [ ] nm_eventsES
- [ ] nm_execTime
- [ ] path
- [ ] product
- [ ] rating
- [x] source
- [ ] type
- [ ] version

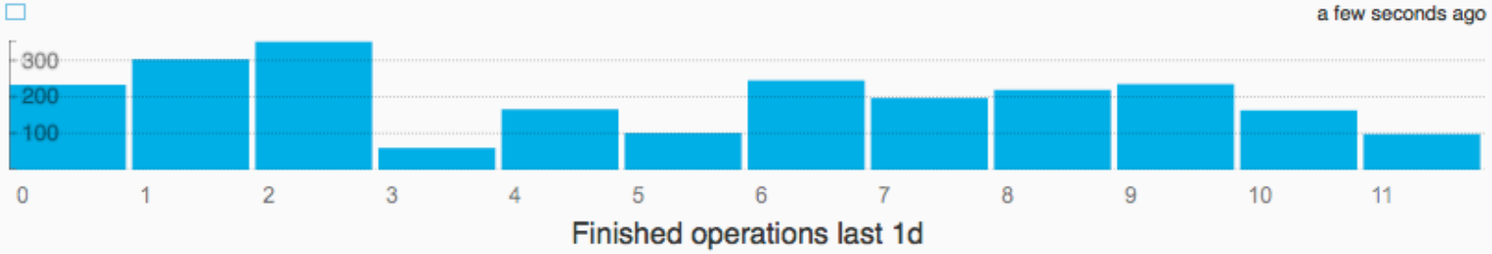
Auswertung - Graylog 2

Dashboards / Executed Operations

Executed Operations

A usefull description of the content of this dashboard (Unlock widget positions by clicking on the lock symbol on the top right. Then drag them to any position you like.)

a few seconds ago



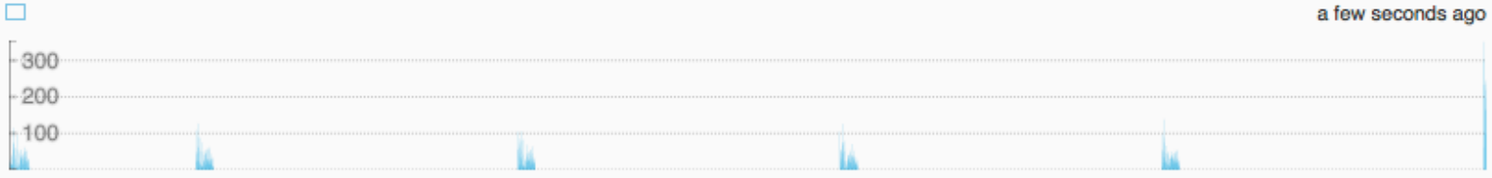
Finished operations last 1d

a few seconds ago

222.371

Finished operations last 1d

a few seconds ago



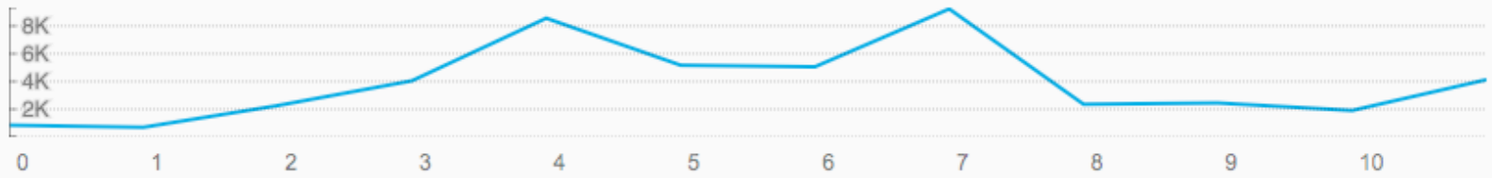
Finished operations last 5d

a few seconds ago

12

Failed operations last 1d

a few seconds ago



Execution time last 1d

a few seconds ago

1.434.168

Finished operations last 5d

a few seconds ago

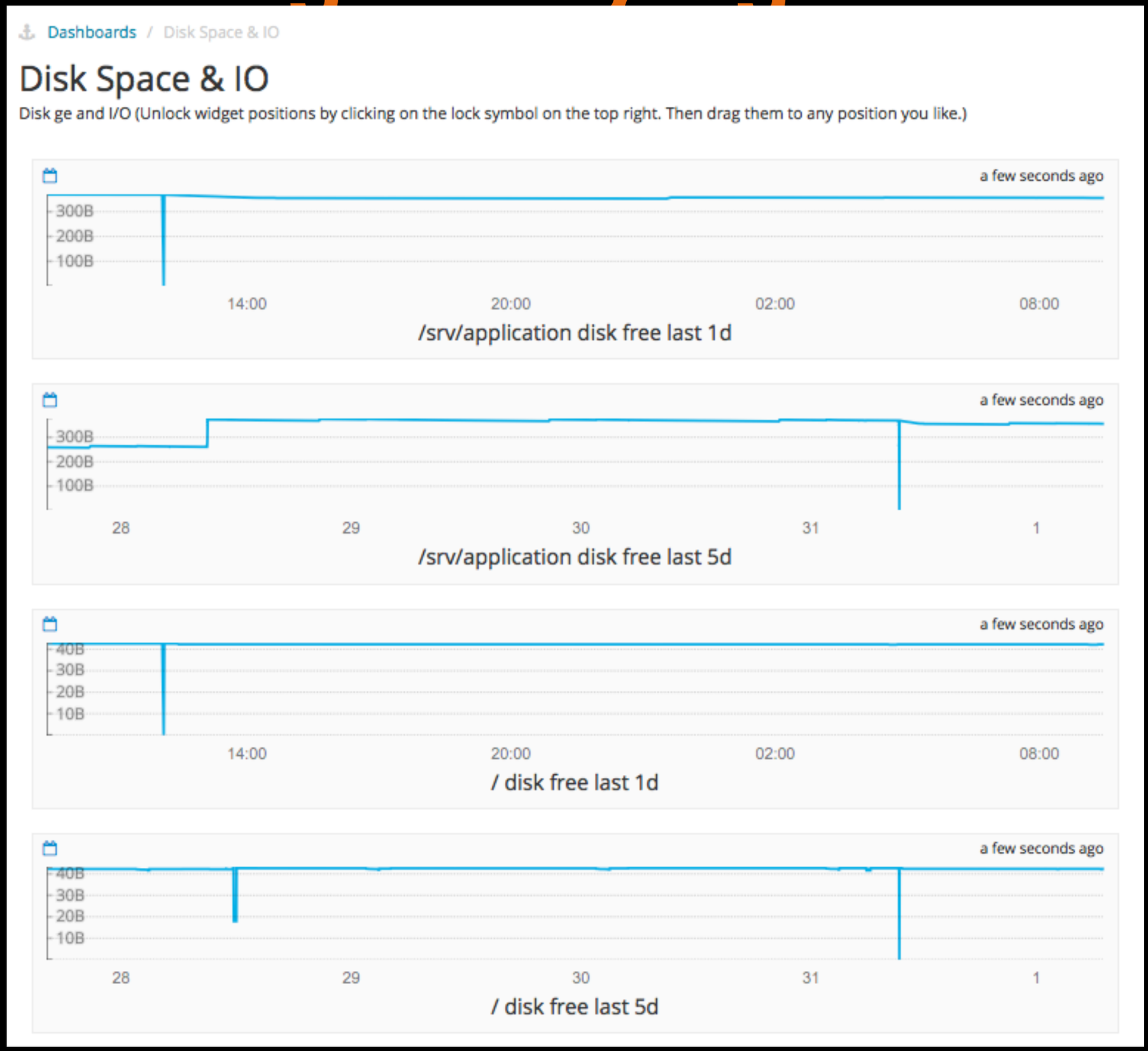
Execution time last 5d

a few seconds ago

52

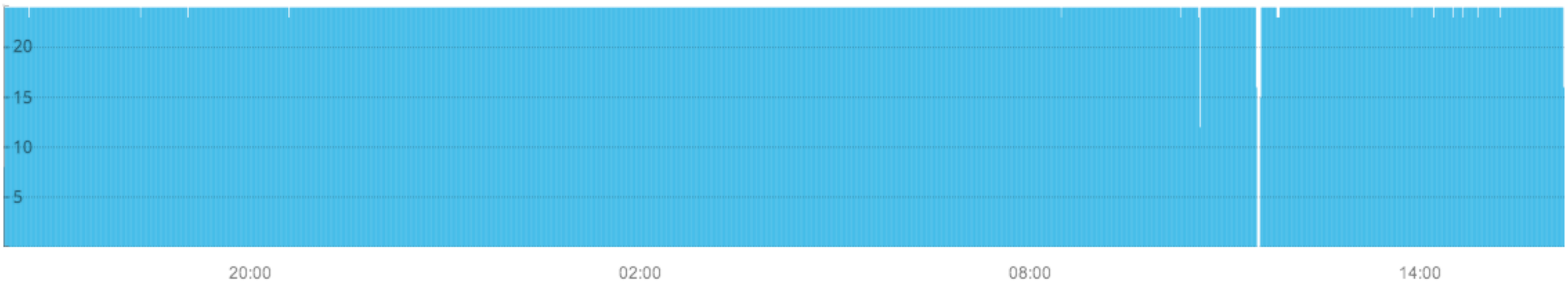
Failed operations last 5d

Auswertung - Graylog 2



Auswertung - Graylog 2

Total result histogram

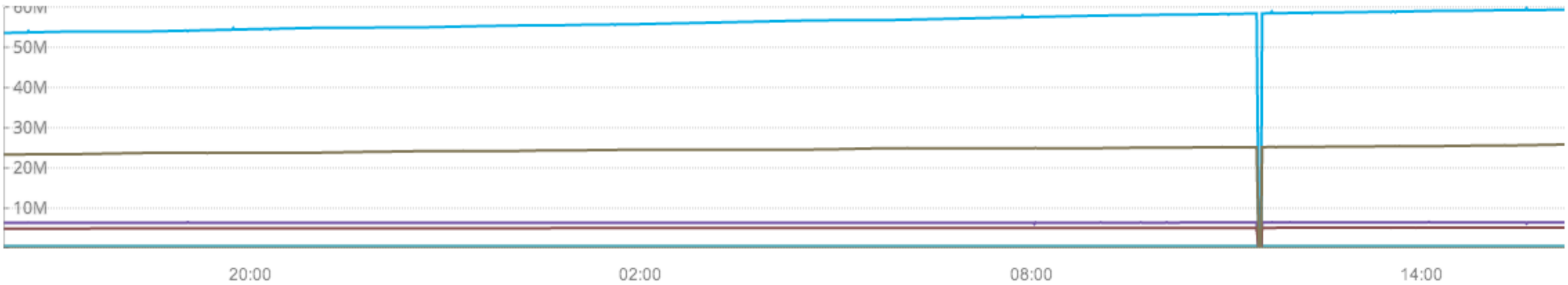


Resolution: Year, Quarter, Month, Week, Day, Hour, **Minute**

Combined chart

- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:idle`
- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:steal`
- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:wait`
- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:system`
- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:user`
- [mean] value, Query: `source: .collectd AND plugin:cpu AND type_instance:interrupt`

secret



Lessons Learned

Was bleibt

Monitoring ist ein First-Class-Citizen

Tools für professionelles Monitoring sind frei verfügbar.

Es gibt keine Entschuldigung es nicht zu tun.

Fragen

Zeit, die letzten Klarheiten zu beseitigen