

Дребни мръсни hack-ове

Васил Колев
<vasil@ludost.net>

Идея на лекцията

- Дребни неща
- Вредни за ползване в реални условия
 - все пак ползвани....
- Интересни от техническа и патологична гледна точка
- Авторът не носи грам отговорност за последиците от лекцията си.

Използвани инструменти

- shell scripting
- coreutils
- gnuplot
- postgresql
- Всичко друго, попаднало под ръка и неуспяло да избяга

Първи hack

- Задача – да се анализира log таблица и да се нарисува резултата
- Структура на таблицата:
 - поле datetime
 - поле с тип на събитието (изброим)

Решение, първа част

```
SELECT
    ((EXTRACT(epoch FROM timestamp)::int/90)*90) AS
period,
    SUM((event_id=1)::int) AS type_1,
    SUM((event_id=2)::int) AS type_2,
    SUM((event_id=3 OR event_id=4)::int) AS
type_rest,
    SUM(1) AS all
FROM
    log
WHERE
    timestamp => '2006-08-28 00:00:00'
    AND timestamp < '2006-08-29 00:00:00'
GROUP BY
    period
ORDER BY
    period ASC;
```

Решение, вторая часть

```
# Извеждане и рисуване
```

```
psql -A -q -t -F ' ' $DB -c "$QUERY" > data
```

```
set title "Events through the day"
```

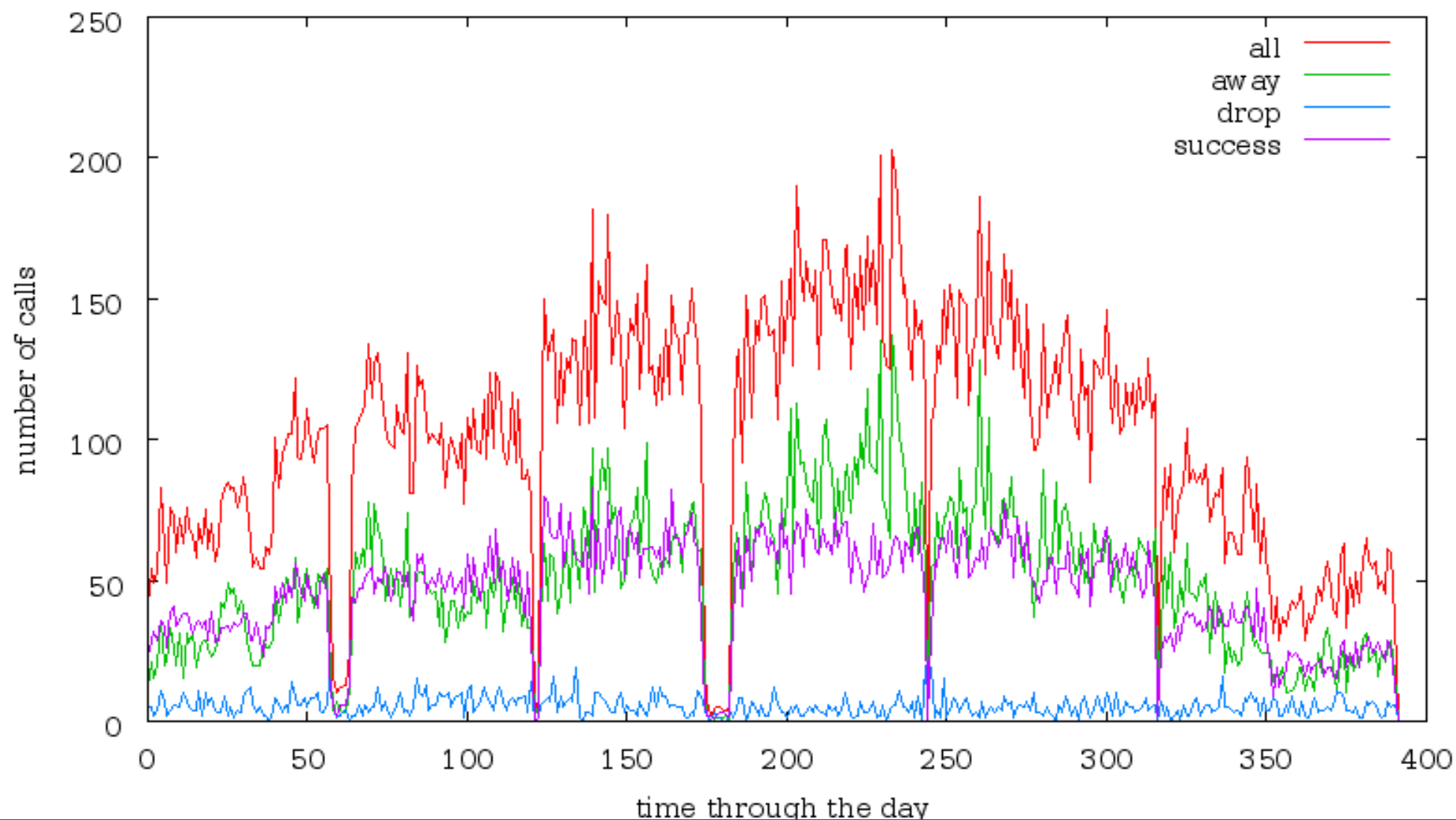
```
set ylabel "number of events"
```

```
set xlabel "time through the day"
```

```
plot "data" using 5 with lines title "all", "data"\  
      using 4 with lines title "rest", \  
      "data" using 3 with lines title "type_1", "data"\  
      using 2 with lines title "type_1"
```

Результат

Calls through the day, quantized at 90 sec. (fig. 1)



Втори hack

- Задача: разбивка на списък от ip адреси по държави заедно с общия брой срещания
- Използва се базата от ip.ludost.net
- Не знам perl :)

Решение, първа част

Таблицы в базата:

cnt – начален адрес, краен, държава

iplist – адрес, брой срещания

final – адрес, държава, брой срещания

Решение, част втора

Зареждане на базата с държави:

```
sed 's/ /,/g' country.db |sed \  
's/^\//";s/,/" /g;s/$/"/' |\  
psql DBN -c 'COPY cnt FROM STDIN;'
```

Решение, трета част

Анализ на всеки 5 минути

PQ='psql -A -q -t DBN -c'

sort iplist|uniq -c |awk '{print \$2"\t"\$1}'\$1 | psql
-A \ -q -t dbn -c 'DELETE FROM iplist;COPY iplist FROM
STDIN' "

\$PQ "DROP TABLE final"

\$PQ "SELECT ip, att, (SELECT ctr FROM cip WHERE ip>beg
AND ip<fns) AS cnt INTO final FROM iplist"

all=`\$PQ "SELECT sum(att) FROM final"`

psql -q DBN -c "SELECT
cnt,SUM(att),((SUM(att)*100/\$all)::int) AS pct FROM
final GROUP BY cnt ORDER BY SUM(att) DESC" > cnt.txt

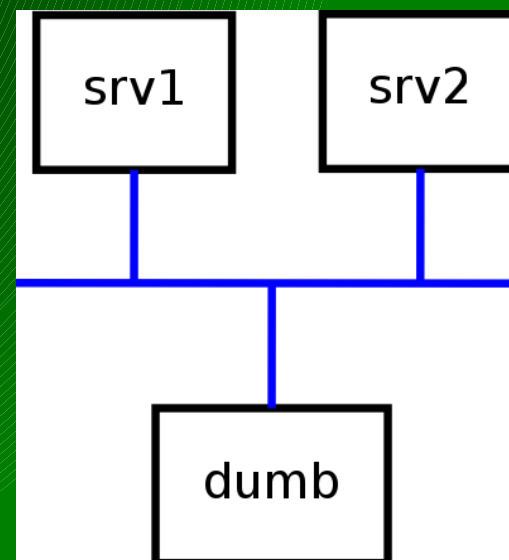
Результат

cnt	sum	pct
bg	123	60
us	58	28
nz	11	5
de	6	2
ru	2	0
nl	2	0
hu	1	0

(7 rows)

Трети hack

- Разправия с учудващо глупав хардуер
- High-availability система с drbd



Решение, част първа

```
#!/bin/sh
cd ~/krokodilski || exit 2
echo $$ > /var/run/kmq.pid

tcpdump -Slni eth0.51 src host 10.0.0.16 and src
port 5001 and not dst port 0 2>/dev/null | (
while read i; do
    k=`echo $i|awk '{print $6}'`
    p=`echo $i|awk '{print $4}'|cut -d . -f 5`
    if [ $k = "ack" ]; then
        continue;
    fi
    k1=`echo $k |cut -d: -f 1`
    echo $p$k1 > file.tmp
    mv file.tmp file.seq
done )
```

Решение, част втора

```
cd ~/krokodilski || exit 2
./spoof 10.0.0.16 5001 10.0.0.5 `cat file.seq |
cut -d : -f 1` `cat file.seq |cut -d : -f 2` 10
```

```
# spoof е измъкнато от една лекция по
# мрежова сигурност
```

Резултат

ами работи

Въпроси?

... или всички се чудят защо им губих
досега времето?

Край

Благодаря за (незаслуженото)
внимание!