

aspect

Ett opensource verktyg för
loggvisualisering

Fredrik Söderblom, XPD AB
fredrik@xpd.se



Problem

- Stooooora mängder loggar
 - Även en mindre site kan generera mellan 10 till 50MiB loggar per dag
- En bra administrerad site har ofta multipla loggfiler
 - Vilket gör det hela en smula värre ...

Problem

- Analys av loggar
 - Måste göras regelbundet
 - Idealiskt var 24:e timme
 - "Kan inte se skogen för träden"

Vad letar vi efter?

- Tre huvudsakliga kategorier:
 - Normal trafik
 - Abnormal trafik, men harmlös
 - Abnormal trafik av elak natur/syfte

Det traditionella sättet

- more, less
- `grep -Ev "pat|tern" /var/log/* | grep -V ...`
 - Ad infinitum
- tail
- sed/awk/perl
- swatch/logsurfer
- etc etc

```
elak.rtfm.as - PuTTY
Mar 30 06:26:32 elak syslogd: restart
Mar 30 06:26:48 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
0 SRC=82.99.xx.xxx DST=213.88.xx.xxx LEN=1500 TOS=0x00 PREC=0x00 TTL=58 ID=30649 DF PROTO=
TCP SPT=36881 DPT=40526 SEQ=4283853822 ACK=2112545902 WINDOW=1448 RES=0x00 ACK URGP=0 OPT
(0101080A07FA1F7A629A7C12)
Mar 30 06:26:48 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
0 SRC=82.99.xx.xxx DST=213.88.xx.xxx LEN=1500 TOS=0x00 PREC=0x00 TTL=58 ID=30649 DF PROTO=
TCP SPT=36881 DPT=40526 WINDOW=1448 RES=0x00 ACK URGP=0
Mar 30 06:27:51 elak tripwire[24388]: Integrity Check Complete: /var/lib/tripwire/elak.twd
TWReport elak 20050330062632 V:6523 S:100 A:464 R:87 C:5972
Mar 30 06:27:51 elak nullmailer[1780]: Trigger pulled.
Mar 30 06:27:51 elak nullmailer[1780]: Rescanning queue.
Mar 30 06:27:51 elak nullmailer[1780]: Starting delivery, 1 message(s) in queue.
Mar 30 06:27:51 elak nullmailer[1780]: Starting delivery: protocol: smtp host: vresig.rtfm
.as file: 1112156871.24408
Mar 30 06:27:53 elak nullmailer[24409]: smtp: Succeeded: 250 Ok: queued as 083F86420
Mar 30 06:27:53 elak nullmailer[1780]: Sent file.
Mar 30 06:27:53 elak nullmailer[1780]: Delivery complete, 0 message(s) remain.
Mar 30 06:30:01 elak /USR/SBIN/CRON[24437]: (www-data) CMD ((cd /usr/share/cacti; php4 /us
r/share/cacti/poller.php) > /dev/null 2>&1)
Mar 30 06:30:06 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
0 SRC=82.99.xx.xxx DST=213.88.xx.xxx LEN=1500 TOS=0x00 PREC=0x00 TTL=58 ID=50005 DF PROTO=
TCP SPT=36889 DPT=40532 SEQ=251904463 ACK=2877271334 WINDOW=1448 RES=0x00 ACK URGP=0 OPT (
0101080A07FD252D62A4CCC4)
Mar 30 06:30:06 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
0 SRC=82.99.xx.xxx DST=213.88.xx.xxx LEN=1500 TOS=0x00 PREC=0x00 TTL=58 ID=50005 DF PROTO=
TCP SPT=36889 DPT=40532 WINDOW=1448 RES=0x00 ACK URGP=0
Mar 30 06:32:07 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
0 SRC=82.99.xx.xxx DST=213.88.xx.xxx LEN=1500 TOS=0x00 PREC=0x00 TTL=58 ID=50007 DF PROTO=
TCP SPT=36889 DPT=40532 SEQ=251904463 ACK=2877271334 WINDOW=1448 RES=0x00 ACK URGP=0 OPT (
0101080A07FEF9ED62A4CCC4)
Mar 30 06:32:07 elak kernel: ipt:IN=eth0 OUT= MAC=00:0c:6e:04:2c:ef:00:c0:7b:a3:1c:1c:08:0
--More--
```

Nöden är uppfinningarnas moder

- Oeffektivt
- Tidsödande
- "Kan inte se skogen för träden"
- Stor risk att missa intressanta anomaliteter

Nöden är uppfinningarnas moder

- Det måste finnas ett bättre sätt att göra det på

Nöden är uppfinningarnas moder

- 3 stycken "grundstenar"

Nöden är uppfinningarnas moder

1. En SQL databas kan vara idealisk för att spara sysloggar i
 - Lätt och relativt snabbt att söka i (med god indexering)
2. Använd SQL som en "arbetsyta" för "datamining"
 - Innehåller 60 dagar av löpande loggar
 - Behåll vanliga text baserade loggar och arkivera enligt gammal god sed

Nöden är uppfinningarnas moder

3. Visualisera loggarna med hjälp av någon form av grafik ..
 - Ögat kan snabbare fånga abnormaliteter
 - Lättare att navigera
 - Bättre överblick

Nöden är uppfinningarnas moder

- Loggvisualiseringen är inspirerad från det gamla Seelog projektet (HP et al)

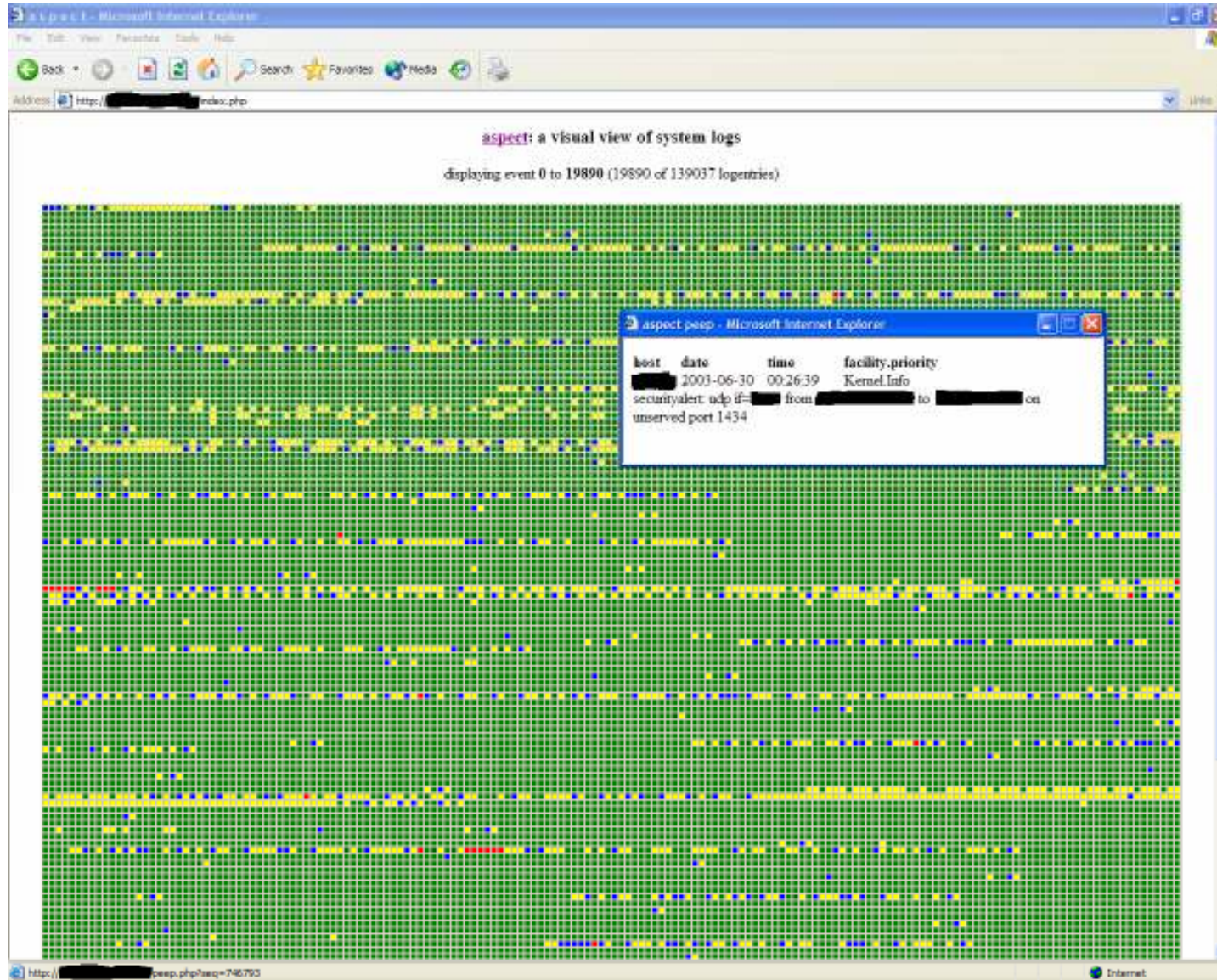
Nöden är uppfinningarnas moder

- Men mha LAMP så kan det göras generellt
- Första prototypen var klar sent hösten 2003
 - Ren HTML
 - Långsam
 - Ful 😊

LAMP

- Linux
- Apache
- MySQL
- PHP





Designmål för version 1

- 2 vyer
 - Loggvisualisering
 - Sökverktyg

Designmål för version 1

- Loggvisualisering
 - Snabb/are
 - Åtminstone snabbare än prototypen :)
 - Enkel att använda
 - Mer intuitivt användargränssnitt
 - Rollbaserad åtkomstkontroll

Designmål för version 1

- Sökverktyg
 - Enklare att använda än en SQL monitor
 - Stöd för att spara ofta återkommande frågor
 - Enkelt att begränsa sökningen

Version 1

- Peter Nolin kommer med i projektet
 - Varde ljus! :)

≡ legend
≡ view rules
≡ search
≡ user admin
≡ my page
≡ logout
ASPECT

Legend

from 2004-06-17
☐
☒ update

normal
blind
cute
fatty
amazing

Log details

date: 2004-06-20
time: 11:50:08
facility: local2
priority: info
host: elak
message: named[9748]: shutting down: flushing changes

Capturing rule

color	severity	facility	priority	host
yellow	2	%	%	%

named[%]: shutting down: flushing changes

:: legend ::
view rules ::
search ::
user admin ::
my page ::
logout

:: ASPECT ::

Search

from

to

limit

host

facility

priority

2004-06-17 00:00

2005-10-13 21:58

50 lines

all

all

all

saved queries

10 entries containing the searchstring.

Run

Recall

Delete

SQL statements

SELECT * FROM syslog WHERE message LIKE '%\$ARG1%' LIMIT 0, 10;

Run Query

Save Query

Reset

show query

show facility/prio

search from end

Query: SELECT * FROM syslog WHERE message LIKE '%grsec%' LIMIT 0, 10;

2004-06-17	01:59:59	elak:	kernel: 1>grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java_vm[java_vm:16262] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java_vm[java_vm:21515] uid/euid:500/500 gid/egid:500/500	(kern/warn)
2004-06-17	02:03:28	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:13903] uid/euid:500/500 gid/egid:500/500, parent /home/frso/dl/azureus/azureus[azureus:26875] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:28	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:13903] uid/euid:500/500 gid/egid:500/500, parent /home/frso/dl/azureus/azureus[azureus:26875] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:32	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:17687] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:7637] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:46	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:29198] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:7637] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:46	elak:	kernel: <<<1>grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:29198] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:7637] uid/euid:500/500 gid/egid:500/500	(uucp/info)
2004-06-17	02:03:47	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:13903] uid/euid:500/500 gid/egid:500/500, parent /home/frso/dl/azureus/azureus[azureus:26875] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:48	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:17687] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:7637] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:48	elak:	kernel: grsec: signal 11 sent to /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:17687] uid/euid:500/500 gid/egid:500/500, parent /usr/lib/mozilla-firebird/plugins/j2re1.4.2/bin/java[java:7637] uid/euid:500/500 gid/egid:500/500	(kern/alert)
2004-06-17	02:03:48	elak:	kernel: grsec: more alerts, logging disabled for 10 seconds	(kern/alert)

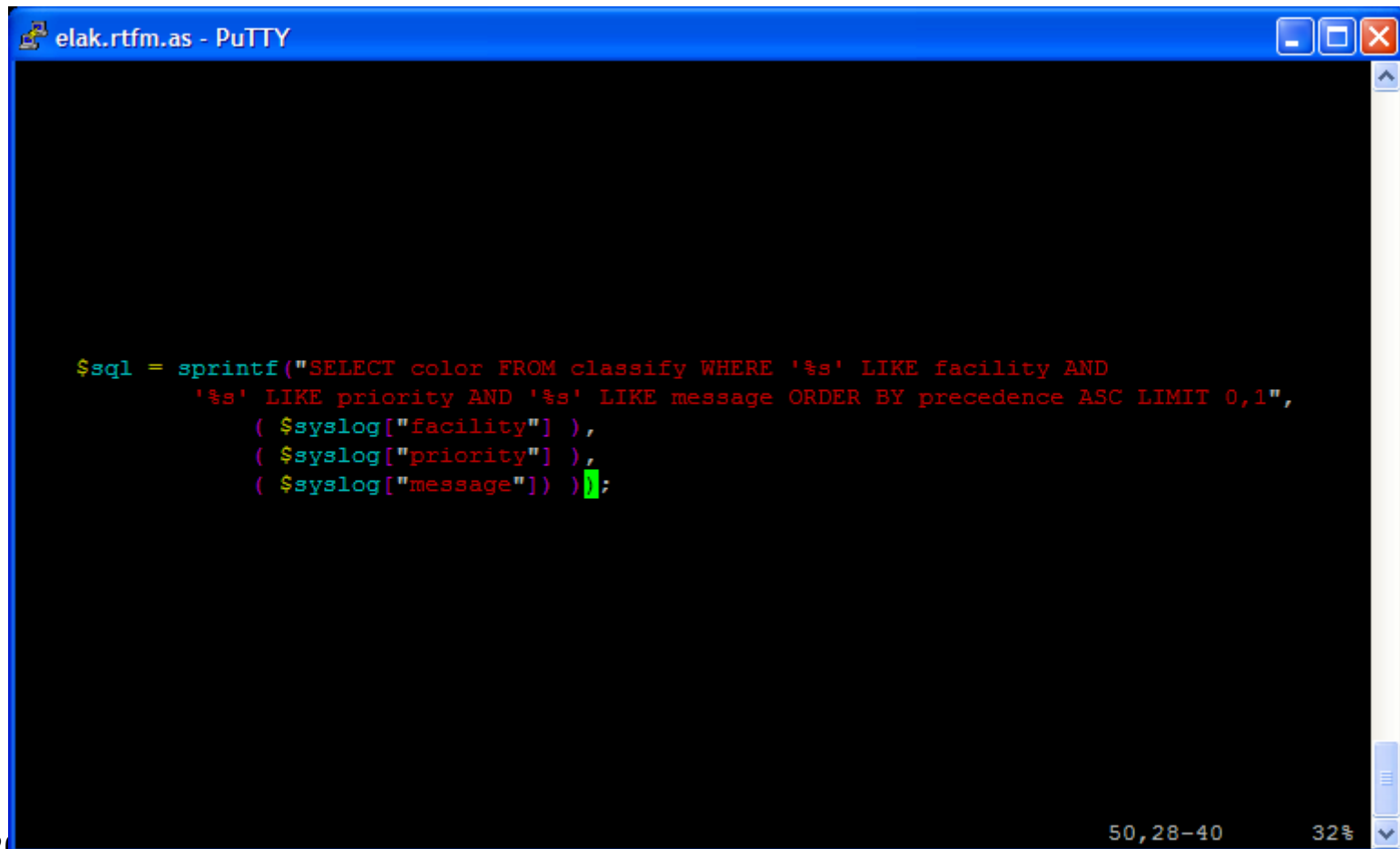
prev

next

[0 to 50 (of 1417)]

Demo

SQL backwards



```
$sql = sprintf("SELECT color FROM classify WHERE '%s' LIKE facility AND  
            '%s' LIKE priority AND '%s' LIKE message ORDER BY precedence ASC LIMIT 0,1",  
            ( $syslog["facility"] ),  
            ( $syslog["priority"] ),  
            ( $syslog["message"] ) );
```

50,28-40 32%

Referenser

- <http://aspect.sf.net>
- <http://sourceforge.net/projects/msyslog/>
- <http://dynarch.com/mishoo/calendar.epl>

Författare

- Fredrik Söderblom
- Peter Nolin

Relaterade projekt

- <http://sourceforge.net/projects/msyslogui/>
- http://www.balabit.com/products/syslog_ng/