The sys admin's daily grind: phpLogCon

MILKING MACHINE 2.0

Using SQL to sift syslog data out of a database is an admittedly universal, but also fairly convoluted approach. phpLogCon, with its web interface, gives admins an easier option. **BY CHARLY KÜHNAST**

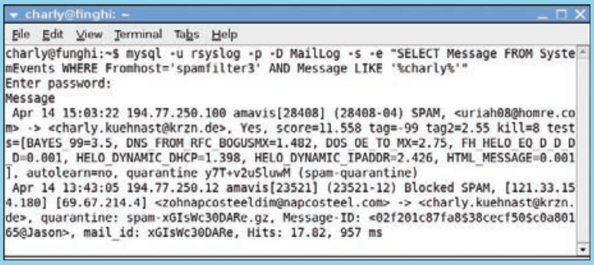
In last month's issue, I talked about RSyslog, a replacement for the syslog daemons [1]. Instead of referencing the standard logfiles in */var/log*, RSyslog works with one or multiple databases in which it logs local results or data supplied by remote servers. I always use one database, Maillog, for the mail facility, and a second database, syslog, for all other messages.

A couple of scripts extract statistics on spam filter performance from the Maillog DB.

Quick Queries

All of this works perfectly, but it's not much use if I just need to check some information from the database quickly – for example, if a colleague is missing an email.

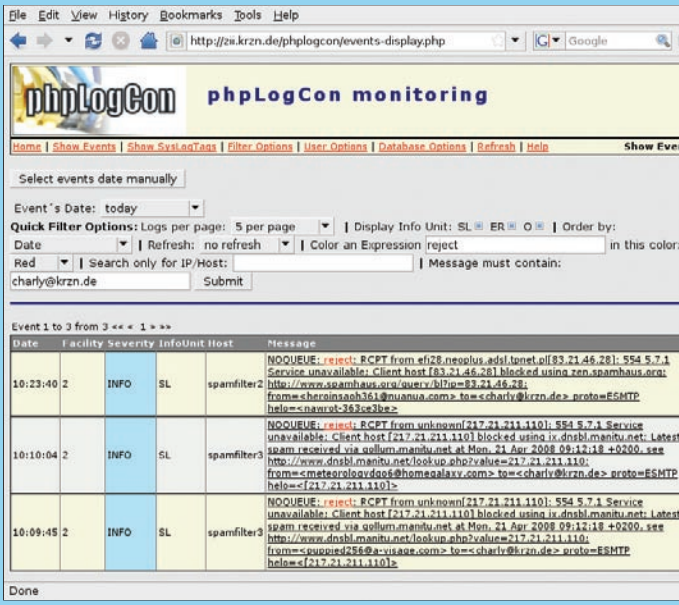
Or maybe I just want to know which spam filter is blocking the most mail to my address. (Incidentally, it's Backup MX, which spammers seem to favor as a general rule.) In cases like this, I turn to phpLogCon [2], a web front end for quick queries. If you happen to be sitting in front of somebody else's machine and only have access to a browser, the software gives you easy access to the most popular database queries.



```
charly@funghi:~$ mysql -u rsyslog -p -D MailLog -s -e "SELECT Message FROM Syste
mEvents WHERE Fromhost='spamfilter3' AND Message LIKE '%charly%'"
Enter password:
Message
 Apr 14 15:03:22 194.77.250.100 amavis[28408] (28408-04) SPAM, <uriah08@homre.co
m> -> <charly.kuehnast@krzn.de>, Yes, score=11.558 tag=-99 tag2=2.55 kill=8 test
s=[BAYES_99=3.5, DNS_FROM_RFC_BOGUSMX=1.482, DOS_OE_TO_MX=2.75, FH_HELO_EQ_D_D_D
_D=0.001, HELO_DYNAMIC_DHCP=1.398, HELO_DYNAMIC_IPADDR=2.426, HTML_MESSAGE=0.001
], autolearn=no, quarantine y7T+v2uSluwM (spam-quarantine)
 Apr 14 13:43:05 194.77.250.12 amavis[23521] (23521-12) Blocked SPAM, [121.33.15
4.180] [69.67.214.4] <zohnapcosteeldim@napcosteel.com> -> <charly.kuehnast@krzn.
de>, quarantine: spam-xGIsWc30DARe.gz, Message-ID: <02f201c87fa8$38cecf50$c0a801
65@Jason>, mail_id: xGIsWc30DARe, Hits: 17.82, 957 ms
```

Figure 1: If phpLogCon throws in the towel in the face of complex queries, it's back to the command line for Charly.

phpLogCon offers simple, web-based installation and is geared for working with multiple logfiles and for multiple, authorized users.


File Edit View History Bookmarks Tools Help
Google
phpLogCon
phpLogCon monitoring
Home | Show Events | Show SysLogTags | Filter Options | User Options | Database Options | Refresh | Help
Show Eve
Select events date manually
Submit
Done

http://zii.krzn.de/phplogcon/events-display.php

Event´s Date: today

Quick Filter Options: Logs per page: 5 per page | Display Info Unit: SL ☒ ER ☒ O ☒ | Order by: Date | Refresh: no refresh | Color an Expression reject in this color: Red | Search only for IP/Host: | Message must contain: charly@krzn.de

Event 1 to 3 from 3 << < 1 > >>

Date	Facility	Severity	InfoUnit	Host	Message
10:23:40	2	INFO	SL	spamfilter2	NOQUEUE: reject: RCPT from efi28.neoplus.adsl.tpnet.pl[83.21.46.28]: 554 5.7.1 Service unavailable: Client host [83.21.46.28] blocked using zen.spamhaus.org; http://www.spamhaus.org/query/bl?ip=83.21.46.28; from=<heroinsaoh361@nuanua.com> to=<charly@krzn.de> proto=ESMTP helo=<nawrot-363ce3be>
10:10:04	2	INFO	SL	spamfilter3	NOQUEUE: reject: RCPT from unknown[217.21.211.110]: 554 5.7.1 Service unavailable: Client host [217.21.211.110] blocked using ix.dnsbl.manitu.net; Latest spam received via gollum.manitu.net at Mon, 21 Apr 2008 09:12:18 +0200, see http://www.dnsbl.manitu.net/lookup.php?value=217.21.211.110; from=<meteorologydgo6@homegalaxy.com> to=<charly@krzn.de> proto=ESMTP helo=<[217.21.211.110]>
10:09:45	2	INFO	SL	spamfilter3	NOQUEUE: reject: RCPT from unknown[217.21.211.110]: 554 5.7.1 Service unavailable: Client host [217.21.211.110] blocked using ix.dnsbl.manitu.net; Latest spam received via gollum.manitu.net at Mon, 21 Apr 2008 09:12:18 +0200, see http://www.dnsbl.manitu.net/lookup.php?value=217.21.211.110; from=<puppied256@a-visage.com> to=<charly@krzn.de> proto=ESMTP helo=<[217.21.211.110]>

Figure 2: The phpLogCon web might not win any beauty contests, but it does give administrators fast search results.

Web Interface

The web interface could be tidier, but at least it is not totally overloaded (Figure 2).

I can set the verbosity to between 5 and 2,000 entries per page and sort the results in ascending or descending order by date, facility, urgency, and host name.

Also, phpLogCon will highlight occurrences of a specified term in the results set.

Limiting a Search

Because I need to process fairly large logfiles, selecting the period of time I want to search is particularly useful. For example, if I already know that an error occurred some time between 2:00 and 4:00pm, it wouldn't make much sense to scour the whole log database – I can just set the search window in *Manual event date selection*.

Filter Options

On top of this, the *Filter options* let me set an urgency level (between *0* for Emergency and *7* for Debug). phpLogCon's author also kindly provides automatic updates and a readable FAQ.

What the phpLogCon web interface unfortunately does not offer is queries with multiply AND- or OR-linked search keys. For the time being, it's back to the command line for queries of this kind (see Figure 1), but on a brighter note, work on version 2.0 is in progress. ■

SYSADMIN

INFO

[1] "The sys admin's daily grind: RSyslog" by Charly Kühnast, *Linux Magazine*, June 2008.

[2] phpLogCon: *http://www.phplogcon.org*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).