By Falko Timme

Published: 2006-07-03 16:52

Postfix Monitoring With Mailgraph And pflogsumm

Version 1.0
Author: Falko Timme <ft [at] falkotimme [dot] com>
Last edited 06/23/2006

This article describes how you can monitor your Postfix mailserver with the tools Mailgraph and pflogsumm. Mailgraph creates daily, weekly, monthly, and yearly graphs of sent, received, bounced, and rejected emails and also of spam and viruses, if SpamAssassin and ClamAV are integrated into Postfix. These graphs can be accessed with a browser, whereas pflogsumm ("Postfix Log Entry Summarizer") can be used to send reports of Postfix activity per email.

In the following I will describe how to install and configure Mailgraph and pflogsumm on Debian Sarge, Ubuntu Dapper Drake (6.06 LTS), and Fedora Core 5.

I want to say first that this is not the only way of setting up such a system. There are many ways of achieving this goal but this is the way I take. I do not issue any guarantee that this will work for you!

1 Preliminary Note

In this tutorial my Linux system has the IP address *`192.168.0.100`* and hosts the web site *`http://www.example.com`* with the document root *`/var/www/www.example.com/web`* and a cgi-bin directory of *`/var/www/www.example.com/cgi-bin`*, and I will send the pflogsumm reports to the email address *`postmaster@example.com`*.

2 Debian Sarge

2.1 Mailgraph

Debian Sarge has packages for Mailgraph and pflogsumm, so we simply install these. We also install rrdtool that stores the data which is needed by Mailgraph to draw the graphs:

```
apt-get install rrdtool mailgraph
```

You will be asked a few questions:

```
Should Mailgraph start on boot? <--
 Which logfile should be used by mailgraph? <--
 Remove RRD files on purge? <--
```

Then there's also this question:

```
Count incoming mail as outgoing mail?
```

If you have integrated a content filter like amavisd (for spam and virus scanning) into Postfix (like in this tutorial: **Virtual Users And Domains With Postfix, Courier And MySQL (+ SMTP-AUTH, Quota, SpamAssassin, ClamAV)**), then answer to avoid that Mailgraph counts your emails twice (because Postfix delivers emails to amavisd which then - after successful scanning - delivers the mails back to Postfix). If you don't use a content filter, then answer .

During the installation, the system startup links for Mailgraph are created automatically, and Mailgraph also gets started automatically, so we don't need to start it manually.

Now we must copy the `mailgraph.cgi` script (which draws the graphs and creates the output for our web browsers) to the cgi-bin directory of our `www.example.com` web site:

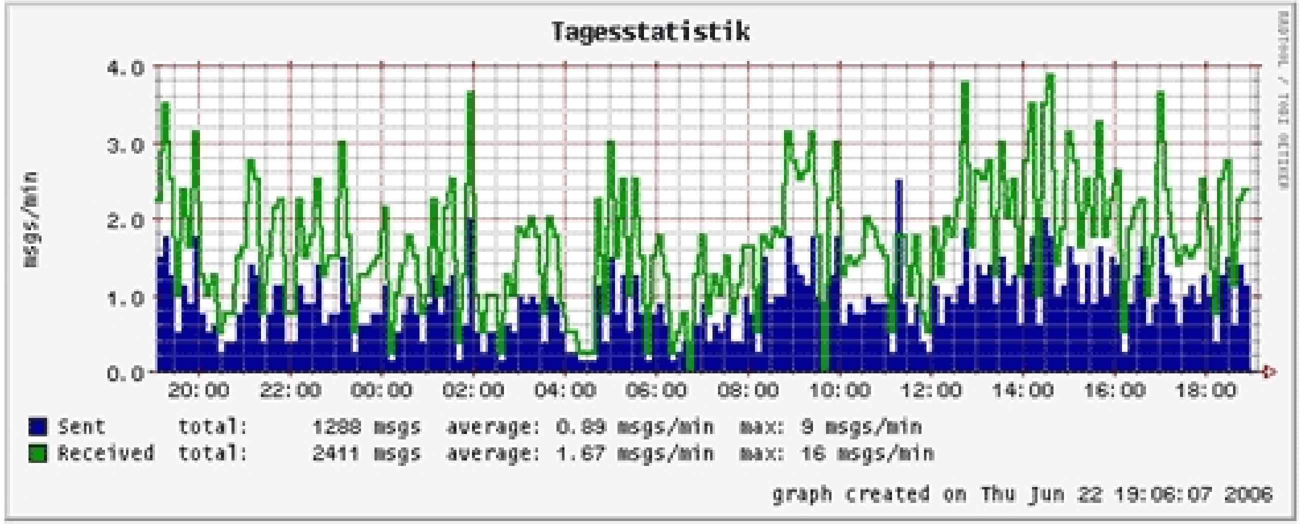
```
cp -p /usr/lib/cgi-bin/mailgraph.cgi /var/www/www.example.com/cgi-bin
```

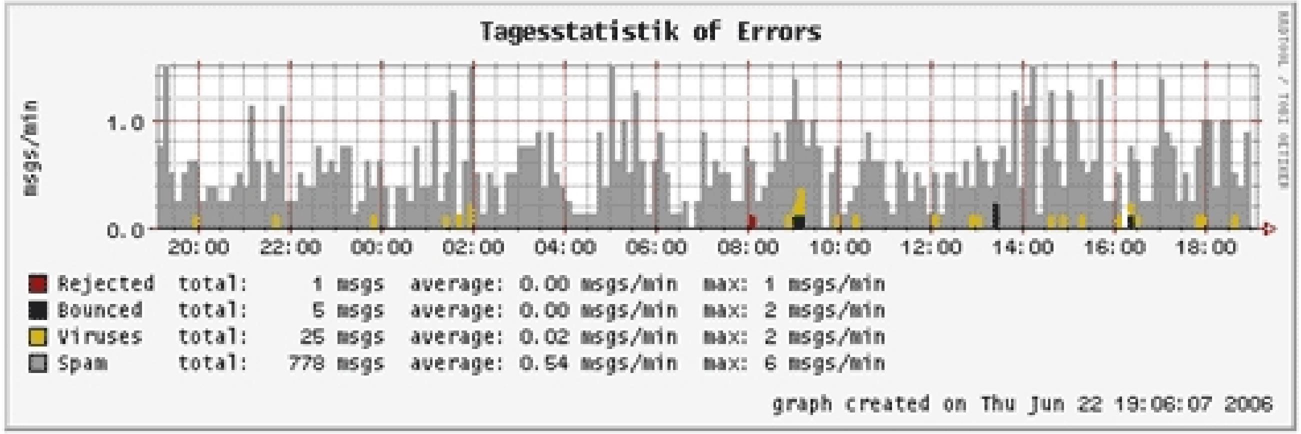
The script is already executable, so we don't need to *chmod* it. If you use suExec for the `www.example.com` web site, you must *chown* `mailgraph.cgi` to the appropriate owner and group.

Now direct your browser to *`http://www.example.com/cgi-bin/mailgraph.cgi`*, and you should see some graphs. Of course, there must be some emails going through your system before you see the first results, so be patient.

After some time your graphs could look like this (the following output is customized, so it doesn't look exactly like yours):

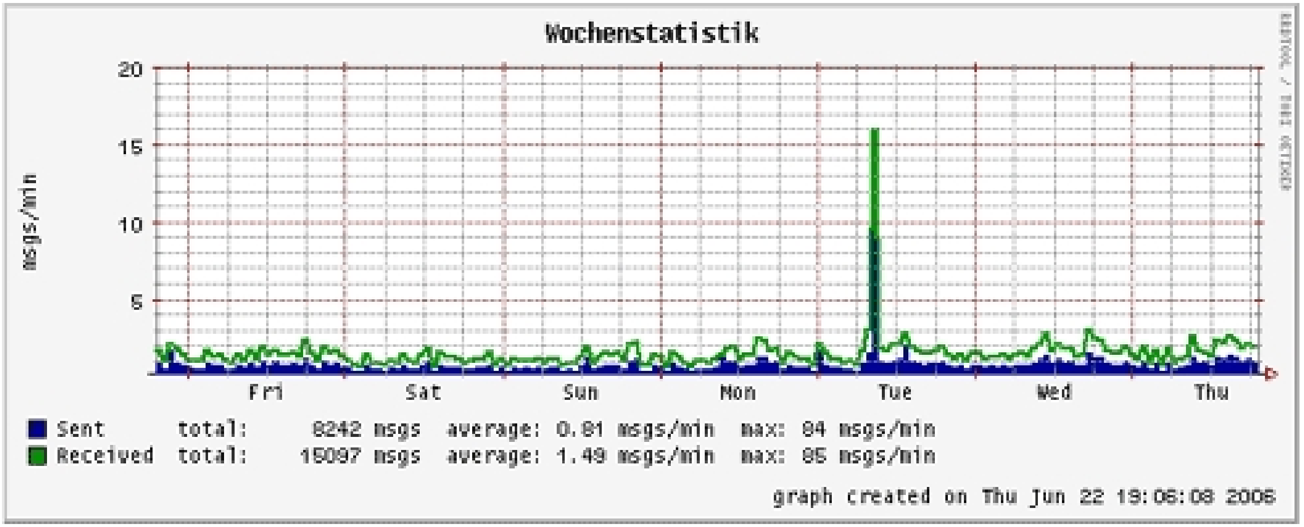
Tagesstatistik



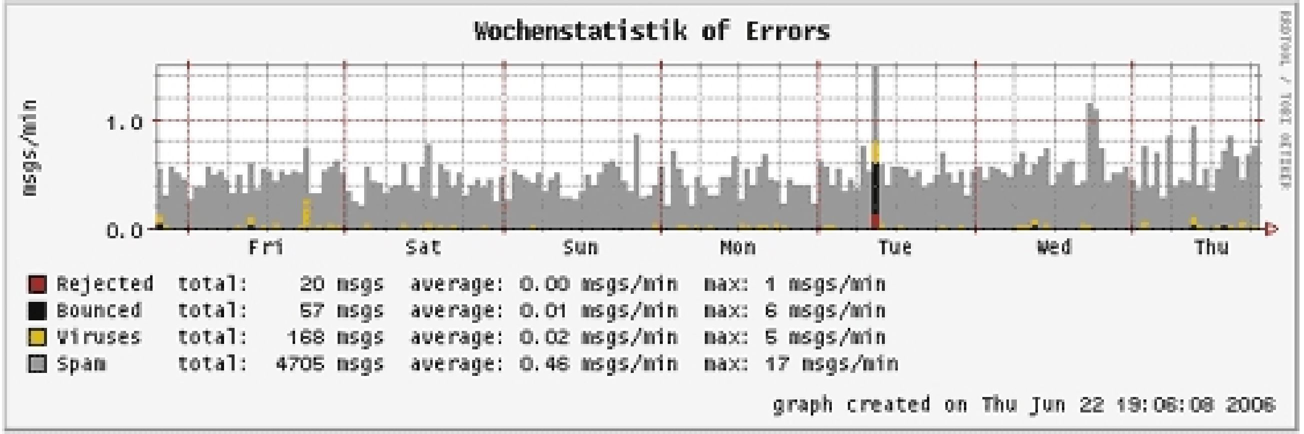


Daily Statistics.

Wochenstatistik

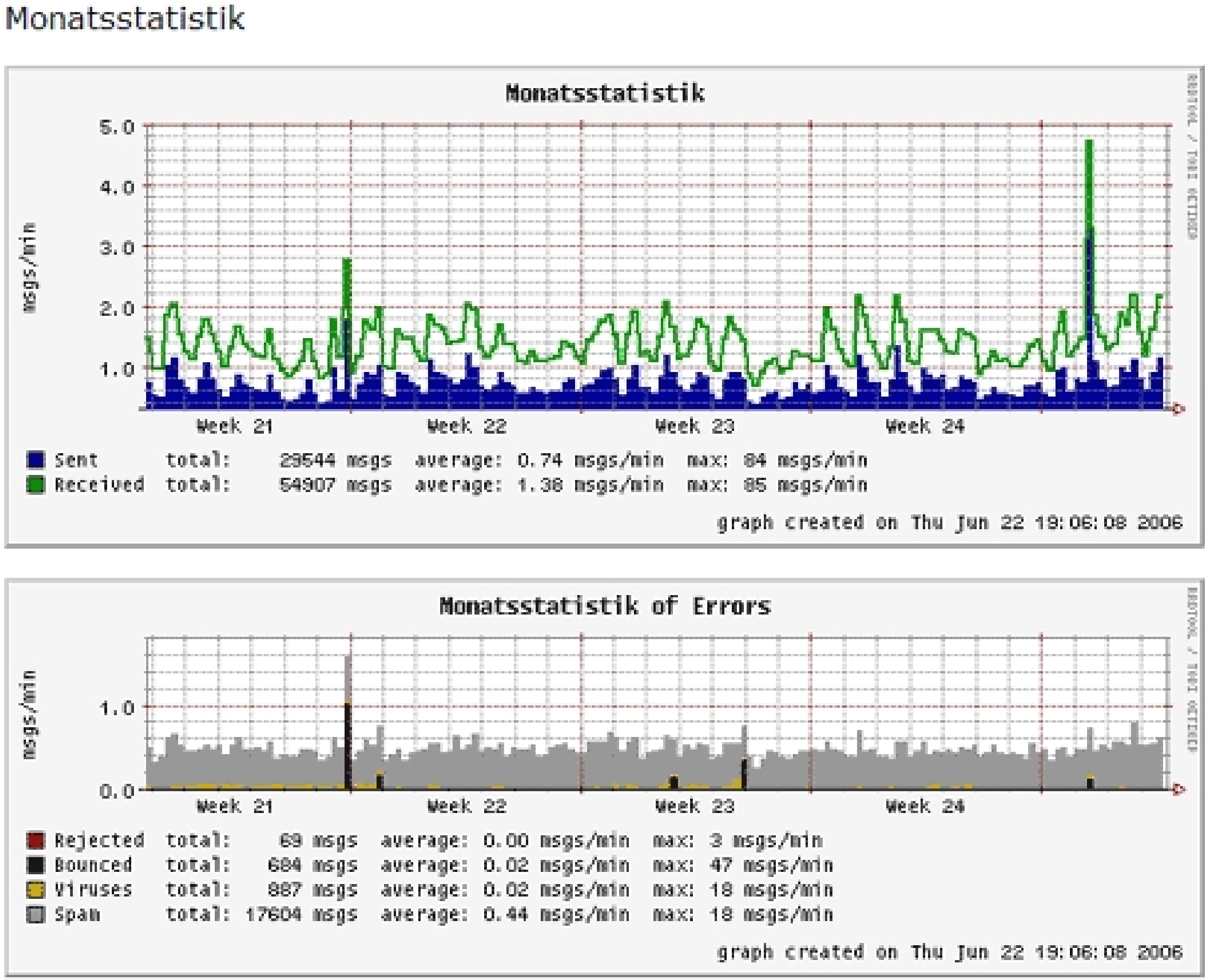


```
■ Sent      total:    8242 msgs  average: 0.81 msgs/min  max: 84 msgs/min
■ Received  total:   15097 msgs  average: 1.49 msgs/min  max: 85 msgs/min
                                          graph created on Thu Jun 22 19:06:08 2006
```



```
■ Rejected  total:   20 msgs  average: 0.00 msgs/min  max: 1 msgs/min
■ Bounced   total:   57 msgs  average: 0.01 msgs/min  max: 6 msgs/min
■ Viruses   total:  168 msgs  average: 0.02 msgs/min  max: 5 msgs/min
■ Spam      total: 4705 msgs  average: 0.46 msgs/min  max: 17 msgs/min
                                          graph created on Thu Jun 22 19:06:08 2006
```

Weekly Statistics.



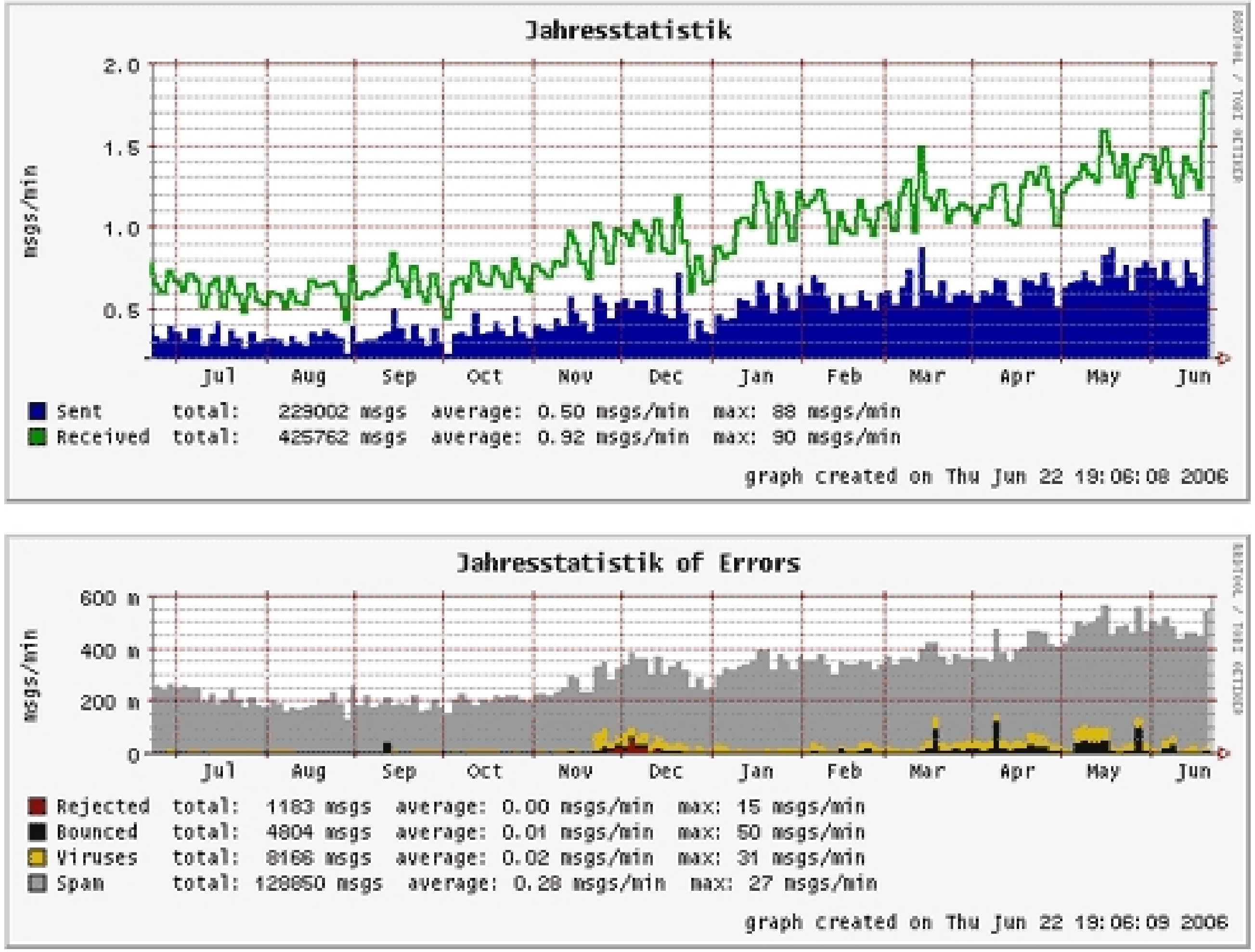
Monatsstatistik

```
■ Sent      total:    29544 msgs  average: 0.74 msgs/min  max: 84 msgs/min
■ Received  total:    54907 msgs  average: 1.38 msgs/min  max: 85 msgs/min
                                      graph created on Thu Jun 22 19:06:08 2006
```

```
■ Rejected  total:    69 msgs  average: 0.00 msgs/min  max: 3 msgs/min
■ Bounced   total:   684 msgs  average: 0.02 msgs/min  max: 47 msgs/min
■ Viruses   total:   887 msgs  average: 0.02 msgs/min  max: 18 msgs/min
■ Spam      total: 17604 msgs  average: 0.44 msgs/min  max: 18 msgs/min
                                      graph created on Thu Jun 22 19:06:08 2006
```

Monthly Statistics.

Jahresstatistik



Yearly Statistics.

Please note: Mailgraph will report spam and viruses only if you have integrated a content filter like amavisd into Postfix which is configured to use

SpamAssassin and ClamAV to tag spam and virus mails. If you don't do this, you will still see graphs, but without the spam and virus report.

2.2 pflogsumm

To install pflogsumm, we run

```
apt-get install pflogsumm
```

We want pflogsumm to be run by a cron job each day and send the report to `postmaster@example.com`. Therefore we must configure our system that it writes one mail log file for 24 hours, and afterwards starts the next mail log so that we can feed the old mail log to pflogsumm. Therefore we configure logrotate (that's the program that rotates our system's log files) like this: open `/etc/logrotate.conf` and append the following stanza to it, after the line `# system-specific logs may be configured here`:

```
vi /etc/logrotate.conf
```

```
/var/log/mail.log {
   missingok
   daily
   rotate 7
   create
   compress
   start 0
}
```

There's a `logrotate` script in `/etc/cron.daily`. This script is called everyday between 06:00h and 07:00h. With the configuration we just made, it will copy the current Postfix log `/var/log/mail.log` to `/var/log/mail.log.0` and compress it, and the compressed file will be `/var/log/mail.log.0.gz`. It will also create a new, empty `/var/log/mail.log` to which Postfix can log for the next 24 hours.

Now we create the script `/usr/local/sbin/postfix_report.sh` which invokes pflogsumm and makes it send the report to `postmaster@example.com`:

```
vi /usr/local/sbin/postfix_report.sh
```

```
#!/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
gunzip /var/log/mail.log.0.gz

pflogsumm /var/log/mail.log.0 | formail -c -I"Subject: Mail Statistics" -I"From: pflogsumm@localhost" -I"To: postmaster@example.com" -I"Received: from www.example.com ([192.168.0.100])" | sendmail postmaster@example.com

gzip /var/log/mail.log.0
exit 0
```

We must make this script executable:

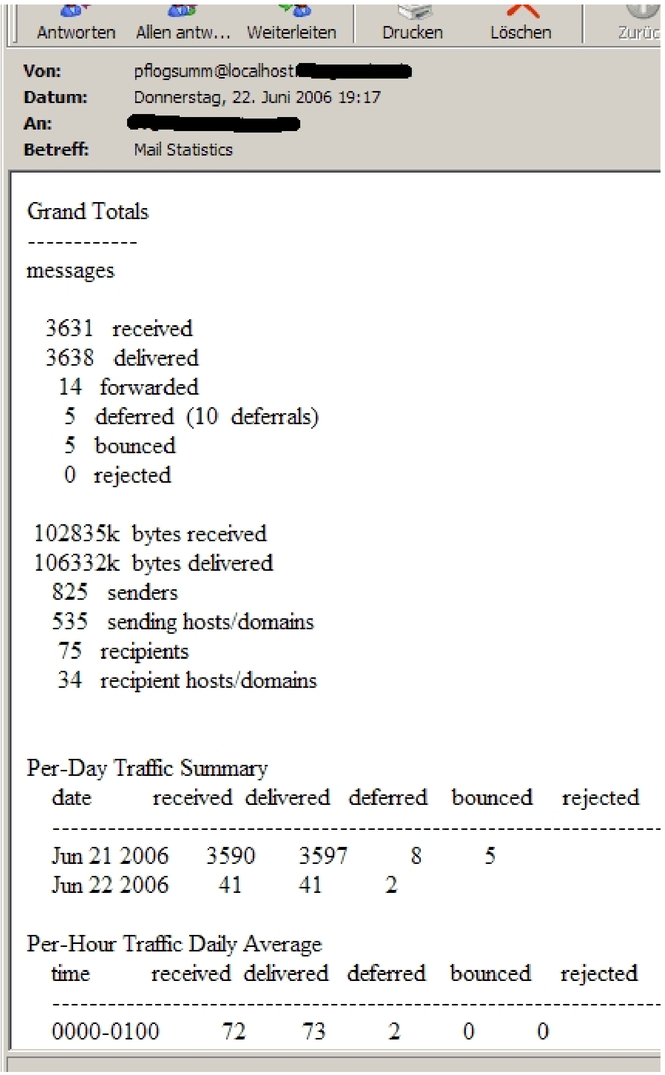
```
chmod 755 /usr/local/sbin/postfix_report.sh
```

Then we create a cron job which calls the script everyday at 07:00h:

```
crontab -e
```

```
0 7 * * * /usr/local/sbin/postfix_report.sh &> /dev/null
```

This will send the report to `postmaster@example.com`. It looks like this in an email client:



Von: pflogsumm@localhost[redacted]
Datum: Donnerstag, 22. Juni 2006 19:17
An: [redacted]
Betreff: Mail Statistics

```
Grand Totals
------------
messages

  3631   received
  3638   delivered
    14   forwarded
     5   deferred  (10  deferrals)
     5   bounced
     0   rejected

 102835k  bytes received
 106332k  bytes delivered
   825   senders
   535   sending hosts/domains
    75   recipients
    34   recipient hosts/domains


Per-Day Traffic Summary
    date          received  delivered   deferred    bounced     rejected
    ------------------------------------------------------------------------
    Jun 21 2006     3590      3597         8          5
    Jun 22 2006       41        41         2

Per-Hour Traffic Daily Average
    time          received  delivered   deferred    bounced     rejected
    ------------------------------------------------------------------------
    0000-0100        72        73          2          0          0
```

3 Ubuntu Dapper Drake (6.06 LTS)

3.1 Mailgraph

To install Mailgraph, we run

```
apt-get install rrdtool mailgraph
```

Ubuntu doesn't ask us questions. Nevertheless, we have to make the differentiation if we use a content filter like amavisd in Postfix or not. Open `/etc/default/mailgraph`:

```
vi /etc/default/mailgraph
```

If you use a content filter like amavisd, the file should have the following contents:

```
MAIL_LOG=/var/log/mail.log
IGNORE_LOCALHOST=true
```

If you don't, then it should look like this:

```
MAIL_LOG=/var/log/mail.log
IGNORE_LOCALHOST=false
```

Ubuntu doesn't create the system startup links for Mailgraph automatically, so we do it now:

```
update-rc.d mailgraph defaults
```

Also, we have to start Mailgraph now:

```
/etc/init.d/mailgraph start
```

Now we must copy the `mailgraph.cgi` script (which draws the graphs and creates the output for our web browsers) to the cgi-bin directory of our `www.example.com` web site:

```
cp -p /usr/lib/cgi-bin/mailgraph.cgi /var/www/www.example.com/cgi-bin
```

The script is already executable, so we don't need to `chmod` it. If you use suExec for the `www.example.com` web site, you must `chown mailgraph.cgi` to the appropriate owner and group.

Now direct your browser to `http://www.example.com/cgi-bin/mailgraph.cgi`, and you should see some graphs. Of course, there must be some emails going through your system before you see the first results, so be patient.

3.2 pflogsumm

The pflogsumm part is exactly the same as for Debian Sarge:

To install pflogsumm, we run

```
apt-get install pflogsumm
```

We want pflogsumm to be run by a cron job each day and send the report to `postmaster@example.com`. Therefore we must configure our system that it writes one mail log file for 24 hours, and afterwards starts the next mail log so that we can feed the old mail log to pflogsumm. Therefore we configure logrotate (that's the program that rotates our system's log files) like this: open `/etc/logrotate.conf` and append the following stanza to it, after the line `# system-specific logs may be configured here`:

```
vi /etc/logrotate.conf
```

```
/var/log/mail.log {
   missingok
   daily
```

```
    rotate 7
    create
    compress
    start 0
}
```

There's a *logrotate* script in */etc/cron.daily*. This script is called everyday between 06:00h and 07:00h. With the configuration we just made, it will copy the current Postfix log */var/log/mail.log* to */var/log/mail.log.0* and compress it, and the compressed file will be */var/log/mail.log.0.gz*. It will also create a new, empty */var/log/mail.log* to which Postfix can log for the next 24 hours.

Now we create the script */usr/local/sbin/postfix_report.sh* which invokes pflogsumm and makes it send the report to *postmaster@example.com*:

```
vi /usr/local/sbin/postfix_report.sh
```

```
#!/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
gunzip /var/log/mail.log.0.gz

pflogsumm /var/log/mail.log.0 | formail -c -I"Subject: Mail Statistics" -I"From: pflogsumm@localhost" -I"To: postmaster@example.com" -I"Received: from www.example.com ([192.168.0.100])" | sendmail postmaster@example.com

gzip /var/log/mail.log.0
exit 0
```

We must make this script executable:

```
chmod 755 /usr/local/sbin/postfix_report.sh
```

Then we create a cron job which calls the script everyday at 07:00h:

```
crontab -e
```

```
0 7 * * * /usr/local/sbin/postfix_report.sh &> /dev/null
```

This will send the report to `postmaster@example.com`.

4 Fedora Core 5

4.1 Mailgraph

There's no Mailgraph package available for Fedora Core 5, so we must install it manually. First, we need to install the prerequsities that Mailgraph requires:

```
yum install rrdtool rrdtool-perl perl-File-Tail
```

Then we download the Mailgraph sources and copy the Mailgraph scripts to the appropriate locations:

```
cd /tmp

wget http://people.ee.ethz.ch/~dws/software/mailgraph/pub/mailgraph-1.12.tar.gz

tar xvfz mailgraph-1.12.tar.gz

cd mailgraph-1.12

mv mailgraph.pl /usr/local/bin/mailgraph.pl

mv mailgraph-init /etc/init.d/mailgraph
```

Now we must adjust the Mailgraph init script */etc/init.d/mailgraph*:

```
vi /etc/init.d/mailgraph
```

On Fedora, the Postfix mail log is */var/log/maillog*, so we change

```
MAIL_LOG=/var/log/syslog
```

to

```
MAIL_LOG=/var/log/maillog
```

Then we add another variable to */etc/init.d/mailgraph*, *IGNORE_LOCALHOST*. If you have integrated a content filter like amavisd into Postfix, add this line

```
IGNORE_LOCALHOST="--ignore-localhost"
```

to the block where the variables like *MAIL_LOG* are defined. If you don't use a content filter, add this line instead:

```
IGNORE_LOCALHOST=""
```

In both cases, change

```
    nice -19 $MAILGRAPH_PL -l $MAIL_LOG -d \
        --daemon-pid=$PID_FILE --daemon-rrd=$RRD_DIR
```

to

```
    nice -19 $MAILGRAPH_PL -l $MAIL_LOG -d \
        --daemon-pid=$PID_FILE --daemon-rrd=$RRD_DIR $IGNORE_LOCALHOST
```

So the final script should look like this (in this case, with *`--ignore-localhost`* enabled):

```
#!/bin/sh

# $Id: mailgraph-init,v 1.4 2005/06/13 11:23:22 dws Exp $
# example init script for mailgraph
#
# chkconfig: 2345 82 28
# description: mailgraph postfix log grapher.
#
# processname: mailgraph.pl
# pidfile: /var/run/mailgraph.pid



PATH=/bin:/usr/bin
MAILGRAPH_PL=/usr/local/bin/mailgraph.pl
MAIL_LOG=/var/log/maillog
PID_FILE=/var/run/mailgraph.pid
RRD_DIR=/var/lib
IGNORE_LOCALHOST="--ignore-localhost"

```

```
case "$1" in
'start')
        echo "Starting mail statistics grapher: mailgraph";
        nice -19 $MAILGRAPH_PL -l $MAIL_LOG -d \
                --daemon-pid=$PID_FILE --daemon-rrd=$RRD_DIR $IGNORE_LOCALHOST
        ;;

'stop')
        echo "Stopping mail statistics grapher: mailgraph";
        if [ -f $PID_FILE ]; then
                kill `cat $PID_FILE`
                rm $PID_FILE
        else
                echo "mailgraph not running";
        fi
        ;;

*)
        echo "Usage: $0 { start | stop }"
        exit 1
        ;;

esac
exit 0
```

Next we make the script executable, create the appropriate system startup links and start Mailgraph:

```
chmod 755 /etc/init.d/mailgraph

chkconfig --levels 235 mailgraph on

/etc/init.d/mailgraph start
```

Still in the `/tmp/mailgraph-1.12` directory, we move `mailgraph.cgi` to our cgi-bin directory:

```
mv mailgraph.cgi /var/www/www.example.com/cgi-bin/
```

Now we open the file and adjust the locations of the two Mailgraph databases.

```
vi /var/www/www.example.com/cgi-bin/mailgraph.cgi
```

Change

```
my $rrd = 'mailgraph.rrd'; # path to where the RRD database is
my $rrd_virus = 'mailgraph_virus.rrd'; # path to where the Virus RRD database is
```

to

```
my $rrd = '/var/lib/mailgraph.rrd'; # path to where the RRD database is
my $rrd_virus = '/var/lib/mailgraph_virus.rrd'; # path to where the Virus RRD database is
```

Then we make the script executable:

```
chmod 755 /var/www/www.example.com/cgi-bin/mailgraph.cgi
```

If you use suExec for the `www.example.com` web site, you must `chown mailgraph.cgi` to the appropriate owner and group.

Now direct your browser to `http://www.example.com/cgi-bin/mailgraph.cgi`, and you should see some graphs. Of course, there must be some emails going through your system before you see the first results, so be patient.

4.2 pflogsumm

The steps differ only slightly from those on Debian and Ubuntu. The main difference is that Postfix logs to *`/var/log/maillog`* on Fedora instead of *`/var/log/mail.log`* (Debian/Ubuntu) (pay attention to the dot!).

First we install pflogsumm:

```
yum install postfix-pflogsumm
```

We want pflogsumm to be run by a cron job each day and send the report to *`postmaster@example.com`*. Therefore we must configure our system that it writes one mail log file for 24 hours, and afterwards starts the next mail log so that we can feed the old mail log to pflogsumm. Therefore we configure logrotate (that's the program that rotates our system's log files) like this: open *`/etc/logrotate.conf`* and append the following stanza to it, after the line *`# system-specific logs may be configured here`*:

```
vi /etc/logrotate.conf
```

```
/var/log/maillog {
    missingok
    daily
    rotate 7
    create
    compress
    start 0
}
```

Also change *`/etc/logrotate.d/syslog`*

```
vi /etc/logrotate.d/syslog
```

from

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

to

```
/var/log/messages /var/log/secure /var/log/spooler /var/log/boot.log /var/log/cron {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

There's a *logrotate* script in */etc/cron.daily*. This script is called everyday between 06:00h and 07:00h. With the configuration we just made, it will copy the current Postfix log */var/log/maillog* to */var/log/maillog.0* and compress it, and the compressed file will be */var/log/maillog.0.gz*. It will also create a new, empty */var/log/maillog* to which Postfix can log for the next 24 hours.

Now we create the script */usr/local/sbin/postfix_report.sh* which invokes pflogsumm and makes it send the report to *postmaster@example.com*:

```
vi /usr/local/sbin/postfix_report.sh
```

```
#!/bin/sh
```

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
gunzip /var/log/maillog.0.gz

pflogsumm /var/log/maillog.0 | formail -c -I"Subject: Mail Statistics" -I"From: pflogsumm@localhost" -I"To: postmaster@example.com" -I"Received: from www.example.com ([192.168.0.100])" | sendmail postmaster@example.com

gzip /var/log/maillog.0
exit 0
```

We must make this script executable:

```
chmod 755 /usr/local/sbin/postfix_report.sh
```

Then we create a cron job which calls the script everyday at 07:00h:

```
crontab -e
```

```
0 7 * * * /usr/local/sbin/postfix_report.sh &> /dev/null
```

This will send the report to `postmaster@example.com`.

5 Links

- Mailgraph: **http://people.ee.ethz.ch/~dws/software/mailgraph**
- pflogsumm: **http://jimsun.linxnet.com/postfix_contrib.html**
- RRDTool: **http://oss.oetiker.ch/rrdtool**
- Postfix: **http://www.postfix.org**