

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38



Kamu telah memiliki **qmail** server beserta **spamassassin** dan **clamav**? Ada baiknya kita **memonitor statistic**

dari traffic email, spam, virus yang ada. Dengan adanya statistic ini, maka kita akan bisa mengetahui progress dari operasional server kita dari waktu ke waktu, dan bisa membantu kita di dalam mengambil keputusan apakah kita perlu menambah resource server (seperti ram, harddisk, dll), atau apakah sudah saatnya kita mengupgrade komponen2 qmail kita.

Qmailmrtg7 ini adalah paket yang bekerja sama dengan mrtg untuk menghasilkan report yang bisa kita lihat melalui web. Adapun paket2 yang kita perlukan adalah:

1. qmail, spamassassin, dan clamav. Pastikan bahwa sudah berjalan dengan baik. Tutorial ini hanya akan membahas instalasi qmailmrtg7.
2. mrtg beserta library2nya. Sesuaikan dengan distro yang kamu pakai.
3. qmailmrtg7 dari <http://www.inter7.com/index.php?page=qmailmrtg7>
4. Script untuk memungkinkan qmailmrtg7 membaca format log spamd dan clamd.

Contohnya dapat dilihat di http://www.qmailrocks.org/extra/qmailmrtg_full.gif

Berikut ini adalah step-by-stepnya:

1. Extract qmailmrtg7 itu dan install:

```
make
```

```
make install
```

Ia akan menginstall file binarynya di /usr/local/bin

2. Copy file2 ini ke dalam direktori webnya, kalau perlu sediakan direktori sendiri, misalnya: /var/www/html/qmailmrtg7

```
index.html
```

```
qmail.mrtg.cfg
```

3. Setel file qmail.mrtg.cfg tersebut.

Lewati dahulu bagian yang mengenai spamd dan clamd. Sebab untuk kedua komponen ini perlu tambahan paket sedikit.

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

Berikut ini adalah isi dari file qmail.mrtg.cfg tersebut (yang telah saya modifikasi, juga beberapa bagian seperti ftp dan ssl saya matikan sebab saya tidak memakainya):

```
WorkDir: /var/www/html/qmailmrtg7/
```

```
#####
```

```
Title[msg]: Messages - FQDN
MaxBytes[msg]: 10000
AbsMax[msg]: 20000
Options[msg]: gauge
Target[msg]: `/usr/local/bin/qmailmrtg7 m /var/log/qmail/qmail-send`
PageTop[msg]: <B>FQDN Messages</B><br>
ShortLegend[msg]: msg
YLegend[msg]: msg/hour
Legend1[msg]: Total Msg&nbsp;
LegendI[msg]: Deliveries:&nbsp;
LegendO[msg]: Attempts:&nbsp;
WithPeak[msg]: ymwd
XSize[msg]: 350
YSize[msg]: 150
```

```
#-----
```

```
Title[queue-size]: Queue Size - FQDN
MaxBytes[queue-size]: 10000
AbsMax[queue-size]: 100000
Options[queue-size]: gauge
Target[queue-size]: `/usr/local/bin/qmailmrtg7 q /var/qmail/queue`
PageTop[queue-size]: <B>FQDN Queue Size</B><br>
ShortLegend[queue-size]: Msg
YLegend[queue-size]: msg total
Legend1[queue-size]: msg&nbsp;
LegendI[queue-size]: msg&nbsp;
LegendO[queue-size]: unprocessed msg:&nbsp;
WithPeak[queue-size]: ymwd
XSize[queue-size]: 350
YSize[queue-size]: 150
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

#-----

Title[clamd]: clamd - FQDN
MaxBytes[clamd]: 10000
AbsMax[clamd]: 100000
Options[clamd]: gauge
Target[clamd]: `/usr/local/bin/mrtgclamd`
PageTop[clamd]: FQDN ClamAV

ShortLegend[clamd]: Msg
YLegend[clamd]: viri/hour
Legend1[clamd]: a
LegendI[clamd]: found
LegendO[clamd]: errors:
WithPeak[clamd]: ymwd
XSize[clamd]: 350
YSize[clamd]: 150

#-----

Title[spamd]: spamd - FQDN
MaxBytes[spamd]: 10000
AbsMax[spamd]: 100000
Options[spamd]: gauge
Target[spamd]: `/usr/local/bin/mrtgspam`
PageTop[spamd]: FQDN SpamAssassin

ShortLegend[spamd]: Msg
YLegend[spamd]: spam/hour
Legend1[spamd]: a
LegendI[spamd]: clean
LegendO[spamd]: spam:
WithPeak[spamd]: ymwd
XSize[spamd]: 350
YSize[spamd]: 150

#-----

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

Title[concurrency]: Local/Remote Concurrency - FQDN
MaxBytes[concurrency]: 500
AbsMax[concurrency]: 10000
Options[concurrency]: gauge
Target[concurrency]: `/usr/local/bin/qmailmrtg7 c /var/log/qmail/qmail-send`
PageTop[concurrency]: FQDN - Local/Remote Concurrency

ShortLegend[concurrency]: concurrency
YLegend[concurrency]: max concurrency
Legend1[concurrency]: concurrency
LegendI[concurrency]: local
LegendO[concurrency]: remote
WithPeak[concurrency]: ymwd
XSize[concurrency]: 350
YSize[concurrency]: 150

#-----

Title[messstatus]: Message Status - FQDN
MaxBytes[messstatus]: 10000
AbsMax[messstatus]: 100000
Options[messstatus]: gauge
Target[messstatus]: `/usr/local/bin/qmailmrtg7 s /var/log/qmail/qmail-send`
PageTop[messstatus]: FQDN - Message Status

ShortLegend[messstatus]: msg
YLegend[messstatus]: msg/hour
Legend1[messstatus]: msg
LegendI[messstatus]: success
LegendO[messstatus]: failures
WithPeak[messstatus]: ymwd
XSize[messstatus]: 350
YSize[messstatus]: 150

#-----

Title[bits]: Bits Transferred - FQDN
MaxBytes[bits]: 1540000
AbsMax[bits]: 100000000
Options[bits]: gauge

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

Target[bits]: `/usr/local/bin/qmailmrtg7 b /var/log/qmail/qmail-send`
PageTop[bits]: FQDN - Bits Transferred

ShortLegend[bits]: bits
YLegend[bits]: bits/sec
Legend1[bits]: bits
LegendI[bits]: bits
LegendO[bits]: bits
WithPeak[bits]: ymwd
XSize[bits]: 350
YSize[bits]: 150

#-----

Title[smtp]: SMTP Concurrency - FQDN
MaxBytes[smtp]: 100
AbsMax[smtp]: 500
Options[smtp]: gauge
Target[smtp]: `/usr/local/bin/qmailmrtg7 t /var/log/qmail/qmail-smtpd`
PageTop[smtp]: FQDN - SMTP Concurrency

ShortLegend[smtp]: SMTP
YLegend[smtp]: max SMTP
Legend1[smtp]: SMTP
LegendI[smtp]: SMTP
LegendO[smtp]: SMTP
WithPeak[smtp]: ymwd
XSize[smtp]: 350
YSize[smtp]: 150

#-----

Title[smtpad]: SMTP Totals - FQDN
MaxBytes[smtpad]: 1000
AbsMax[smtpad]: 100000
Options[smtpad]: gauge
Target[smtpad]: `/usr/local/bin/qmailmrtg7 a /var/log/qmail/qmail-smtpd`
PageTop[smtpad]: FQDN - SMTP Totals

ShortLegend[smtpad]: SMTP
YLegend[smtpad]: SMTP/hour

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

Legend1[smtpad]: SMTP
LegendI[smtpad]: Allow
LegendO[smtpad]: Deny
WithPeak[smtpad]: ymwd
XSize[smtpad]: 350
YSize[smtpad]: 150

#-----
Title[pop3]: POP3 Concurrency - FQDN
MaxBytes[pop3]: 100
AbsMax[pop3]: 500
Options[pop3]: gauge
Target[pop3]: `/usr/local/bin/qmailmrtg7 t /var/log/qmail/qmail-pop3d`
PageTop[pop3]: FQDN POP3 Concurrency

ShortLegend[pop3]: POP3
YLegend[pop3]: max POP3
Legend1[pop3]: POP3
LegendI[pop3]: POP3
LegendO[pop3]: POP3
WithPeak[pop3]: ymwd
XSize[pop3]: 350
YSize[pop3]: 150

#-----

Title[pop3ad]: POP3 Totals - FQDN
MaxBytes[pop3ad]: 1000
AbsMax[pop3ad]: 100000
Options[pop3ad]: gauge
Target[pop3ad]: `/usr/local/bin/qmailmrtg7 a /var/log/qmail/qmail-pop3d`
PageTop[pop3ad]: FQDN - POP3 Totals

ShortLegend[pop3ad]: POP3
YLegend[pop3ad]: POP3/hour
Legend1[pop3ad]: POP3
LegendI[pop3ad]: Allow
LegendO[pop3ad]: Deny
WithPeak[pop3ad]: ymwd
XSize[pop3ad]: 350
YSize[pop3ad]: 150

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#-----  
Title[cpu0]: CPU 0 Usage - FQDN  
MaxBytes[cpu0]: 100  
AbsMax[cpu0]: 1000  
Options[cpu0]: bits  
Target[cpu0]: `/usr/bin/awk '/cpu0 /{print $2+$3; print $2+$3+$4; print &quot;quite some  
time&quot;; print &quot;home&quot;}'</proc/stat`  
PageTop[cpu0]: CPU 0 Usage - FQDN  
ShortLegend[cpu0]: %x100  
Ylegend[cpu0]: %x100  
LegendI[cpu0]: &nbsp;user:  
LegendO[cpu0]: &nbsp;total:  
Legend1[cpu0]: Time spent in user mode  
Legend2[cpu0]: Time spent in user mode + time spent in system mode  
Legend3[cpu0]: Maximum occurance of time spent in user mode  
Legend4[cpu0]: Maximum occurance of (time spent in user mode + time spent in system mode)  
XSize[cpu0]: 350  
YSize[cpu0]: 150
```

```
#-----  
Title[eth0]: eth0 bits - FQDN  
Options[eth0]: bits  
Target[eth0]: `grep eth0 /proc/net/dev | sed 's/eth0:/' | awk '{print $1; print $9; print  
&quot;&quot;; print &quot;&quot;}'`  
PageTop[eth0]: eth0 bits - FQDN  
MaxBytes[eth0]: 100000000  
Ylegend[eth0]: bits  
ShortLegend[eth0]: bits  
XSize[eth0]: 350  
YSize[eth0]: 150  
Legend1[eth0]: bits&nbsp;  
LegendI[eth0]: input&nbsp;  
LegendO[eth0]: output&nbsp;  
WithPeak[eth0]: ymwd
```

```
#-----  
Title[eth0p]: eth0 packets - FQDN  
Options[eth0p]: bits  
Target[eth0p]: `grep eth0 /proc/net/dev | sed 's/eth0:/' | awk '{print $2; print $10; print  
&quot;&quot;; print &quot;&quot;}'`  
PageTop[eth0p]: eth0 packets - FQDN
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

MaxBytes[eth0p]: 100000000
Ylegend[eth0p]: bits
ShortLegend[eth0p]: bits
XSize[eth0p]: 350
YSize[eth0p]: 150
Legend1[eth0p]: bits
LegendI[eth0p]: input
LegendO[eth0p]: output
WithPeak[eth0p]: ymwd

#-----

Title[mem]: memory used/free - FQDN
Target[mem]: `free | /usr/bin/awk '/Mem: /{print \$3*1000; print \$4*1000; print ""; print ""}`
PageTop[mem]: memory used/free - FQDN
Options[mem]: gauge
MaxBytes[mem]: 5000000000
Ylegend[mem]: mem
ShortLegend[mem]: mem
XSize[mem]: 350
YSize[mem]: 150
Legend1[mem]: mem
LegendI[mem]: used
LegendO[mem]: free
WithPeak[mem]: ymwd

#-----

Title[swap]: memory swap - FQDN
Target[swap]: `free | /usr/bin/awk '/Swap: /{print \$3; print \$3; print ""; print ""}`
PageTop[swap]: memory swap - FQDN
Options[swap]: gauge
MaxBytes[swap]: 500000
Ylegend[swap]: mem
ShortLegend[swap]: mem
XSize[swap]: 350
YSize[swap]: 150
Legend1[swap]: mem
LegendI[swap]: swap
LegendO[swap]: swap
WithPeak[swap]: ymwd

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#-----  
Title[load]: system load - FQDN  
Target[load]: `uptime | sed 's/,//g' | awk '{print $10*100; print $11*100 ; print &quot;&quot;}'`  
PageTop[load]: system load - FQDN  
Options[load]: gauge  
MaxBytes[load]: 100000  
Ylegend[load]: load x100  
ShortLegend[load]: load  
XSize[load]: 350  
YSize[load]: 150  
Legend1[load]: load nbsp;  
LegendI[load]: 5min nbsp;  
LegendO[load]: 15min nbsp;  
WithPeak[load]: ymwd
```

```
#-----  
#Title[ftpd]: ftpd concurrency - FQDN  
#MaxBytes[ftpd]: 100  
#AbsMax[ftpd]: 500  
#Options[ftpd]: gauge  
#Target[ftpd]: `/usr/local/bin/qmailmrtg7 t /var/log/ftpd`  
#PageTop[ftpd]: <font face=arial size=3><B>FQDN</B> - ftpd (concurrency)</font><br>  
#ShortLegend[ftpd]: ftpd  
#YLegend[ftpd]: ftpd  
#Legend1[ftpd]: ftpd  
#LegendI[ftpd]: &nbsp;ftpd:  
#LegendO[ftpd]:  
#WithPeak[ftpd]: ymwd  
#XSize[ftpd]: 350  
#YSize[ftpd]: 150
```

```
#-----  
  
#Title[ftpdad]: ftpd allow/deny - FQDN  
#MaxBytes[ftpdad]: 1000  
#AbsMax[ftpdad]: 10000  
#Options[ftpdad]: gauge  
#Target[ftpdad]: `/usr/local/bin/qmailmrtg7 a /var/log/pureftpd.log`  
#PageTop[ftpdad]: <font face=arial size=3><B>FQDN</B> - ftpd (allow/deny)</font><br>  
#ShortLegend[ftpdad]: ftpd
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#YLegend[ftpdad]: ftpd
#Legend1[ftpdad]: ftpd
#LegendI[ftpdad]: &nbsp;Allow:
#LegendO[ftpdad]: &nbsp;Deny:
#WithPeak[ftpdad]: ymwd
#XSize[ftpdad]: 350
#YSize[ftpdad]: 150
```

```
#-----
```

```
#Title[smtps]: SMTP SSL Concurrency - FQDN
#MaxBytes[smtps]: 100
#AbsMax[smtps]: 500
#Options[smtps]: gauge
#Target[smtps]: `/usr/local/bin/qmailmrtg7 t /var/log/qmail/qmail-smtpd`
#PageTop[smtps]: <B>FQDN - SMTP Concurrency</B><BR>
#ShortLegend[smtps]: SMTP
#YLegend[smtps]: max SMTP
#Legend1[smtps]: SMTP&nbsp;
#LegendI[smtps]: SMTP&nbsp;
#LegendO[smtps]: SMTP&nbsp;
#WithPeak[smtps]: ymwd
#XSize[smtps]: 350
#YSize[smtps]: 150
```

```
#-----
```

```
#Title[smtpsad]: SMTP SSL Totals - FQDN
#MaxBytes[smtpsad]: 1000
#AbsMax[smtpsad]: 100000
#Options[smtpsad]: gauge
#Target[smtpsad]: `/usr/local/bin/qmailmrtg7 a /var/log/qmail/qmail-smtpd`
#PageTop[smtpsad]: <B>FQDN - SMTP Totals</B><BR>
#ShortLegend[smtpsad]: SMTP
#YLegend[smtpsad]: SMTP/hour
#Legend1[smtpsad]: SMTP&nbsp;
#LegendI[smtpsad]: Allow&nbsp;
#LegendO[smtpsad]: Deny&nbsp;
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#WithPeak[smtpsad]: ymwd
#XSize[smtpsad]: 350
#YSize[smtpsad]: 150
```

```
#-----
#Title[pop3s]: POP3 SSL Concurrency - FQDN
#MaxBytes[pop3s]: 100
#AbsMax[pop3s]: 500
#Options[pop3s]: gauge
#Target[pop3s]: `/usr/local/bin/qmailmrtg7 t /var/log/qmail/qmail-pop3d`
#PageTop[pop3s]: <B>FQDN POP3 Concurrency</B><BR>
#ShortLegend[pop3s]: POP3
#YLegend[pop3s]: max POP3
#Legend1[pop3s]: POP3&nbsp;
#LegendI[pop3s]: POP3&nbsp;
#LegendO[pop3s]: POP3&nbsp;
#WithPeak[pop3s]: ymwd
#XSize[pop3s]: 350
#YSize[pop3s]: 150
```

```
#-----

#3Title[pop3sad]: POP3 SSL Totals - FQDN
#MaxBytes[pop3sad]: 1000
#AbsMax[pop3sad]: 100000
#Options[pop3sad]: gauge
#Target[pop3sad]: `/usr/local/bin/qmailmrtg7 a /var/log/qmail/qmail-pop3d`
#PageTop[pop3sad]: <B>FQDN - POP3 Totals</B><BR>
#ShortLegend[pop3sad]: POP3
#YLegend[pop3sad]: POP3/hour
#Legend1[pop3sad]: POP3&nbsp;
#LegendI[pop3sad]: Allow&nbsp;
#LegendO[pop3sad]: Deny&nbsp;
#WithPeak[pop3sad]: ymwd
#XSize[pop3sad]: 350
#YSize[pop3sad]: 150
```

4. Setelah itu, sebagai root kita jalankan ini:

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

/usr/bin/mrtg /var/www/html/qmailmrtg7/qmail.mrtg.cfg

Kamu akan melihat error message. Jalankan command itu 3-4 kali. Kamu masih akan menemukan error message, terutama yang mengenai spamd dan clamd. Tidak apa2. Sekarang coba kamu buka webnya yang telah kamu buat sebelumnya, misalnya di <http://domainkamu/qmailmrtg7/>

Maka kamu akan mulai melihat grafik2 qmail dan system kamu. Grafik spamd dan clamd belum muncul. Happy? :)

5. Jangan terlalu happy dulu. Hehe.. Langkah selanjutnya adalah bagaimana menghasilkan grafik spamd dan clamd itu. Grafik ini menurut saya sangat membantu, sebab kita tahu belakangan ini serangan virus dan spam sangat mengganggu, jadi kita perlu tahu berapa besar serangan yg diterima server kita.

6. Nah langkah ke-6 ini yang rada tricky. Saya harus beberapa kali coba2 baru berhasil. Kita harus menginstall beberapa buat script yang akan membantu kita di dalam mem-parse log yang dihasilkan oleh spamassassin dan clamav.

Script2 tersebut adalah:

clammrtg.pl

glmrtg.pl

mrtgclamd

mrtgspam

Buatlah file2 tersebut dan isikan ini ke dalamnya masing2:

----- pembatas script -----

Untuk clammrtg.pl :

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#!/usr/bin/perl
#-----#
#glmrtg - Grab Logs from syslog files for MRTG
#Copyright (C) 2002 Chadwick L. Sorrell ( csorrell@hrtc.net )
#
#-----#
#
#Version: 0.3
#
#
#Based on which facility you use in syslog and what interval you have set in mrtg
#you might need to modify the default variables $interval and $facility
#
#Syntax: glmrtg logfile 'unique phrase' [interval]
#
#Example: glmrtg /var/log/maillog 'sendmail'
# -This would give you the number of messages sendmail sent/received during the last 5
minutes.
#
#MRTG Example:
#...
#Target[spam]: `perl glmrtg.pl /var/log/maillog identified && perl glmrtg.pl /var/log/maillog clean`
#...
#
use Date::Parse;
use POSIX qw(strftime);

# Default interval is 5 minutes #
$interval = 300;

# Default facility in syslog #
$facility = &quot;clamdscan&quot;;

# Initialize start time and end time #
$edate = time();

# If specified via commandline change the default interval #
if($ARGV[2])
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
{
$interval = $ARGV[2];
}$sdate = $edate - $interval;
$count=0;
# End Initialize #

# Narrow the grep to just the recent and current hour. #
if($interval < 3600)
{
$pg1 = strftime '%H', localtime $sdate;
$pg2 = strftime '%H', localtime ($sdate - 3600);

$grep_add = &quot;| grep -E '( $pg2| $pg1)'&quot;;
}

# Generate the filtered log #
#print &quot;grep '$ARGV[1]' $ARGV[0] $grep_add > spamd.mln&quot;;
system(&quot;grep '$ARGV[1]' $ARGV[0] $grep_add > virus.ml&quot;);

#
# Iterate through the file and if the line is between the start and end time increment the count #
open(GDATA, &quot;<virus.ml&quot;) or die &quot;couldn't open virus.ml for reading&quot;;
while($line = <GDATA>)
{
#$line = $_;;
$line =~ s/$facility (.*)$//;
#print &quot;$line&quot;;
$curtime=0;
$curtime = str2time(substr(&quot;$line&quot;,8, 3).&quot;
&quot;.substr(&quot;$line&quot;,5,3).substr(&quot;$line&quot;,17,8));
$foo = substr(&quot;$line&quot;,8,3).&quot; &quot;.substr(&quot;$line&quot;,5,
3).substr(&quot;$line&quot;,17,8);
#print &quot;$foo&quot;;
#print &quot;curtime - $curtime&quot;;
#print &quot;sdate - $sdate&quot;;
#print &quot;edate - $edate&quot;;
#print &quot;if (curtime >= sdate && curtime < edate)n&quot;;
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
if($curtime >= $sdate && $curtime < $edate)
{
$count++;
}
}
close(GDATA);
```

```
# Print total #
print &quot;$countn&quot;;
```

----- pembatas script -----

Untuk qmrtg.pl:

```
#!/usr/bin/perl
#-----#
#glmrtg - Grab Logs from syslog files for MRTG
#Copyright (C) 2002 Chadwick L. Sorrell ( csorrell@hrtc.net )
#
#This program is free software; you can redistribute it and/or
#modify it under the terms of the GNU General Public License
#as published by the Free Software Foundation; either version 2
#of the License, or (at your option) any later version.
#
#This program is distributed in the hope that it will be useful,
#but WITHOUT ANY WARRANTY; without even the implied warranty of
#MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
#GNU General Public License for more details.
#
#You should have received a copy of the GNU General Public License
#along with this program; if not, write to the Free Software
#Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
#-----#
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
#
#Version: 0.3
#
#
#Based on which facility you use in syslog and what interval you have set in mrtg
#you might need to modify the default variables $interval and $facility
#
#Syntax: glmrtg logfile 'unique phrase' [interval]
#
#Example: glmrtg /var/log/maillog 'sendmail'
# -This would give you the number of messages sendmail sent/received during the last 5
minutes.
#
#MRTG Example:
#...
#Target[spam]: `perl glmrtg.pl /var/log/maillog identified && perl glmrtg.pl /var/log/maillog clean`
#...
#
use Date::Parse;
use POSIX qw(strftime);

# Default interval is 5 minutes #
$interval = 300;
# Default facility in syslog #
$facility = &quot;spamd&quot;;

# Initialize start time and end time #
$edate = time();

# If specified via commandline change the default interval #
if($ARGV[2])
{
$interval = $ARGV[2];
}

$sdate = $edate - $interval;
$count=0;
# End Initialize #
```


Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
# Narrow the grep to just the recent and current hour. #
```

```
if($interval < 3600)
```

```
{
```

```
$pg1 = strftime '%H', localtime $sdate;
```

```
$pg2 = strftime '%H', localtime ($sdate - 3600);
```

```
$grep_add = &quot;| grep -E '( $pg2| $pg1)'&quot;;
```

```
}
```

```
# Generate the filtered log #
```

```
#print &quot;grep '$ARGV[1]' $ARGV[0] $grep_add > spamd.mln&quot;;
```

```
system(&quot;grep '$ARGV[1]' $ARGV[0] $grep_add > spamd.ml&quot;);
```

```
#
```

```
# Iterate through the file and if the line is between the start and end time increment the count #
```

```
open(GDATA, &quot;<spamd.ml&quot;) or die &quot;couldn't open spamd.ml for
```

```
readingn&quot;;
```

```
while($line = <GDATA>)
```

```
{
```

```
#$line = $_;
```

```
$line =~ s/$facility (.*)$//;
```

```
#print &quot;$linen&quot;;
```

```
$curtime = str2time(substr(&quot;$line&quot;,0,15));
```

```
#$foo = substr(&quot;$line&quot;,0,15);
```

```
#print &quot;$foon&quot;;
```

```
#print &quot;curtime - $curtimen&quot;;
```

```
#print &quot;sdate - $sdaten&quot;;
```

```
#print &quot;edate - $edaten&quot;;
```

```
#print &quot;if (curtime >= sdate && curtime < edate)n&quot;;
```

```
if($curtime >= $sdate && $curtime < $edate)
```

```
{
```

```
$count++;
```

```
}
```

```
}
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
close(GDATA);
```

```
# Print total #  
print &quot;$countn&quot;;
```

----- pembatas script -----

Untuk mrtgclamd:

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

```
echo `perl /usr/local/bin/clammrtg.pl /var/spool/qmailscan/viruses.log`  
echo 0  
echo  
echo
```

----- pembatas script -----

Untuk mrtgspam:

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

```
echo `perl /usr/local/bin/glmrtg.pl /var/log/mail/info identified`
```

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

```
echo `perl /usr/local/bin/glmrtg.pl /var/log/mail/info clean`  
echo  
echo
```

----- script selesai -----

**7. Ok, untuk mudahnya, copykan file2 script tersebut ke dalam /usr/local/bin
Jangan lupa untuk di chmod 755 agar bisa dieksekusi.**

**8. Setelah itu jalankan lagi command berikut beberapa kali sampai tidak muncul error:
/usr/bin/mrtg /var/www/html/baseqmailmrtg/qmail.mrtg.cfg**

Command tersebut sebaiknya dimasukkan ke dalam cron job dengan interval 5 menit:
/etc/crontab

```
* /5 * * * * root /usr/bin/mrtg /var/www/html/qmailmrtg7/qmail.mrtg.cfg
```

Ok, selamat! Kamu telah memiliki statistik traffic email, spamd, dan clamd, serta system load yang dapat kamu akses melalui web.

Kalau ada kesulitan, silahkan tanya di forum yah :)

Bahan2 referensi:

<http://www.qmailrocks.org>

<http://www.inter7.com>

<http://www.google.com>



v.1.0 by ari_stress a.k.a tiger74

Jakarta, 24 Desember 2004. fajarpri at arinet.org

Penulis adalah Microsoft Certified Professional, yang jatuh cinta kepada Linux. Bekerja di

Cara menginstall qmailmrtg7 untuk memonitor traffic email, spam, virus, dan system

Written by ari

Friday, 24 December 2004 06:32 - Last Updated Wednesday, 29 December 2004 15:38

sebuah lembaga pendidikan di Jakarta