Logwatch gibt Systeminformationen und -status aufbereitet über Email oder auf der Kommandozeile aus.

Installation

```
sudo apt-get install logwatch
```

Anpassen

```
#Die Basic-Konfiguration
sudo vim /usr/share/logwatch/default.conf/
logwatch.conf
#So sieht das ausführungsscript aus
sudo vim /etc/cron.daily/00logwatch
```

meine **logwatch.conf**

```
########################################################
# This was written and is maintained by:
#    Kirk Bauer <kirk@kaybee.org>
#
# Please send all comments, suggestions, bug reports,
#    etc, to kirk@kaybee.org.
#
########################################################
# NOTE:
#   All these options are the defaults if you run logwatch with no
#   command-line arguments.  You can override all of these on the
#   command-line.
# You can put comments anywhere you want to.  They are effective for the
# rest of the line.
# this is in the format of <name> = <value>.  Whitespace at the beginning
# and end of the lines is removed.  Whitespace before and after the = sign
# is removed.  Everything is case *insensitive*.
# Yes = True  = On  = 1
# No  = False = Off = 0
# Default Log Directory
# All log-files are assumed to be given relative to this directory.
LogDir = /var/
log
# You can override the default temp directory (/tmp) here
TmpDir = /var/cache/
logwatch
#Output/Format Options
##By default Logwatch will print to stdout in text with no encoding.
```

```
##To make email Default set Output = mail to save to file set Output = file
Output = mail##To make Html the default formatting Format = html
Format = html##To make Base64 [aka uuencode] Encode = base64
#Encode = none
#
## Default person to mail reports to.  Can be a local account or a
## complete email address.  Variable Print should be set to No to
## enable mail feature.
MailTo = "root"
# Default person to mail reports to.  Can be a local account or a
# complete email address.  Variable Print should be set to No to
# enable mail feature.
#MailTo = root
# WHen using option --multiemail, it is possible to specify a different
# email recipient per host processed.  For example, to send the report
# for hostname host1 to user@example.com, use:
#Mailto_host1 = user@example.com
# Multiple recipients can be specified by separating them with a space.
# Default person to mail reports from.  Can be a local account or a
# complete email address.
MailFrom = Logwatch
# If set to 'Yes', the report will be sent to stdout instead of being
# mailed to above person.
#Print = Yes
# if set, the results will be saved in <filename> instead of mailed
# or displayed.
#Save = /tmp/logwatch
# Use archives?  If set to 'Yes', the archives of logfiles
# (i.e. /var/log/messages.1 or /var/log/messages.1.gz) will
# be searched in addition to the /var/log/messages file.
# This usually will not do much if your range is set to just
# 'Yesterday' or 'Today'... it is probably best used with
# By default this is now set to Yes. To turn off Archives uncomment this.
#Archives = No
# Range = All
# The default time range for the report...
# The current choices are All, Today, Yesterday
Range = yesterday
# The default detail level for the report.
# This can either be Low, Med, High or a number.
# Low = 0
# Med = 5
# High = 10
Detail = Med
# The 'Service' option expects either the name of a filter
# (in /usr/share/logwatch/scripts/services/*) or 'All'.
# The default service(s) to report on.  This should be left as All for
# most people.
```

```
Service = All# You can also disable certain services (when specifying all)
Service = "-zz-network"
# Prevents execution of zz-network service, which
                            # prints useful network configuration info.
Service = "-zz-sys"         # Prevents execution of zz-sys service, which
                            # prints useful system configuration info.
Service = "-eximstats"      # Prevents execution of eximstats service, which
                            # is a wrapper for the eximstats program.
# If you only cared about FTP messages, you could use these 2 lines
# instead of the above:
#Service = ftpd-messages   # Processes ftpd messages in /var/log/messages
#Service = ftpd-xferlog    # Processes ftpd messages in /var/log/xferlog
# Maybe you only wanted reports on PAM messages, then you would use:
#Service = pam_pwdb        # PAM_pwdb messages - usually quite a bit
#Service = pam             # General PAM messages... usually not many
# You can also choose to use the 'LogFile' option.  This will cause
# logwatch to only analyze that one logfile.. for example:
#LogFile = messages
# will process /var/log/messages.  This will run all the filters that
# process that logfile.  This option is probably not too useful to
# most people.  Setting 'Service' to 'All' above analyizes all LogFiles
# anyways...
#
# By default we assume that all Unix systems have sendmail or a sendmail-like s
# The mailer code Prints a header with To: From: and Subject:.
# At this point you can change the mailer to any thing else that can handle tha
# stream. TODO test variables in the mailer string to see if the To/From/Subjec
# From here with out breaking anything. This would allow mail/mailx/nail etc...
mailer = "/usr/sbin/sendmail -t"
#
# With this option set to 'Yes', only log entries for this particular host
# (as returned by 'hostname' command) will be processed.  The hostname
# can also be overridden on the commandline (with --hostname option).  This
# can allow a log host to process only its own logs, or Logwatch can be
# run once per host included in the logfiles.
#
# The default is to report on all log entries, regardless of its source host.
# Note that some logfiles do not include host information and will not be
# influenced by this setting.
#
#HostLimit = Yes
# vi: shiftwidth=3 tabstop=3 et
```