NAME

logwatch − system log analyzer and reporter

SYNOPSIS

logwatch [--detail *level* **] [--logfile** *log-file-group* **] [--service** *service-name* **] [--mailto** *address* **] [--archives] [--range** *range* **] [--debug** *level* **] [--filename** *file-name* **] [--logdir** *directory* **] [--hostlimit** *hosts* **] [--hostname** *hostname* **] [--html_wrap** *number of characters* **] [--hostformat** *host based options* **] [--output** *output-type* **] [--format** *report format* **] [--encode** *encoding to use* **] [--numeric] [--no-oldfiles-log] [--version] [--help|--usage]**

DESCRIPTION

Logwatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Logwatch is being used for Linux and many types of UNIX.

OPTIONS

--detail level

This is the detail level of the report. *level* can be a positive integer, or high, med, low, which correspond to the integers 10, 5, and 0, respectively.

--logfile log-file-group

This will force Logwatch to process only the set of logfiles defined by *log-file-group* (i.e. messages, xferlog, ...). Logwatch will therefore process all services that use those logfiles. This option can be specified more than once to specify multiple logfile-groups.

--service service-name

This will force Logwatch to process only the service specified in *service-name* (i.e. login, pam, identd, ...). Logwatch will therefore also process any log-file-groups necessary to process these services. This option can be specified more than once to specify multiple services to process. A useful *service-name* is *All* which will process all services (and logfile-groups) for which you have filters installed.

--mailto address

Mail the results to the email address or user specified in *address.*

--range range

You can specify a date-range to process. Common ranges are *Yesterday, Today, All,* and *Help.* Additional options are listed when invoked with the *Help* parameter.

--archives

Each log-file-group has basic logfiles (i.e. /var/log/messages) as well as archives (i.e. /var/log/messages.? or /var/log/messages.?.gz). When used with "−−range all", this option will make Logwatch search through the archives in addition to the regular logfiles. For other values of −−range, Logwatch will search the appropriate archived logs.

--debug level

For debugging purposes. *level* can range from 0 to 100. This will *really* clutter up your output. You probably don’t want to use this.

--filename file-name

Save the output to *file-name* instead of displaying or mailing it.

--logdir directory

Look in *directory* for log subdirectories or log files first before looking in the default directories.

--hostlimit host1,host2

Limit report to hostname - host1, host2.

--hostname hostname

Use *hostname* for the reports instead of this system’s hostname. In addition, if HostLimit is set in the logwatch.conf configuration file (see **MORE INFORMATION**, below), then only logs from this hostname will be processed (where appropriate).

--html_wrap num-characters
Number of characters that html output should be wrapped to. Default is 80.

--numeric
Inhibits additional name lookups, displaying IP addresses numerically.

--no-oldfiles-log
Suppress the logwatch log, which informs about the old files in logwatch tmpdir.

--usage Displays usage information

--help same as −−usage.

FILES

/usr/share/logwatch/
This directory contains all the perl executables and configuration files shipped with the logwatch distribution.

/etc/logwatch
This directory contains local configuration files that override the default configuration. See **MORE INFORMATION** below for more information.

EXAMPLES

logwatch --service ftpd-xferlog --range all --detail high --archives
This will print out all FTP transfers that are stored in all current and archived xferlogs.

logwatch --service pam_pwdb --range yesterday --detail high
This will print out login information for the previous day...

MORE INFORMATION

The directory /usr/share/doc/logwatch-* contains several files with additional documentation:

HOWTO-Customize-LogWatch
Documents the directory structure of Logwatch configuration and executable files, and describes how to customize Logwatch by overriding these default files.

LICENSE
Describes the License under which Logwatch is distributed. Additional clauses may be specified in individual files.

README
Describes how to install, where to find it, mailing lists, and other useful information.

AUTHOR

Kirk Bauer <kirk@kaybee.org>
http://www.kaybee.org/˜kirk
http://logwatch.sourceforge.net