Logwatch

Logwatch (http://www.logwatch.org/) is a powerful and versatile log parser and analyzer. Logwatch is designed to give a unified report of all activity on a server, which can be delivered through the command line or email.

Contents

Installation

Install `logwatch` (https://www.archlinux.org/packages/?name=logwatch).

In addition to the logwatch binaries, scripts and config files, the pacman package also includes a cron job that is installed as `/etc/cron.daily/0logwatch`. Also note that logwatch scripts use perl, which is a dependency of the logwatch package.

Configuration

Logwatch has a tiered configuration approach. There are several locations where configuration details can be specified, with each one superseding the previous one:

- /usr/share/logwatch/default.conf/*
- /etc/logwatch/conf/dist.conf/*
- /etc/logwatch/conf/*
- The script / command line arguments

Logwatch will parse all these location when called.

Within these directories, there are several areas of configuration. The logwatch.conf files are where most of the high-level settings are, which allow you to set where your reports are sent, how they are formatted, etc. The conf file at /usr/share/logwatch/default.conf/logwatch.conf contains all the default settings and comments on what they do. It is recommended to leave the default conf alone and instead re-define a setting variable you want to change in /etc/logwatch/conf/logwatch.conf.

Within the logfiles/ directory of any of the conf locations are config files detailing specific log files. By default, most of the common log files found in a Linux system are already accounted for. If you have some esoteric application that does not have a log file conf already, copy an existing one from the default.conf/logfiles/ directory and customize it for your application.

The services/ folder contains similar conf definitions, but these one define the various services reported by logwatch. This is necessary because often multiple services will report to the same log (e.g. messages, dmesg, boot, etc.). For more information, examine some of the default services/ conf files.

Note that if you want logwatch messages delivered by email, you need to install a package that provides a sendmail frontend. **Postfix** is a good choice.

There is a helpful document supplied with the package to give further information on configuration. It is located at /usr/share/logwatch/HOWTO-Customize-LogWatch.

Cron Job

The default install also includes a cron job, placed in cron.daily. This job will use the configuration settings from all the config locations, as detailed above. The script can be moved to a different cron folder for different report frequencies or set up as a custom cron job in a crontab file.

systemd journal support

Logwatch 7.4.3-3 now supports querying the systemd journal via journalctl. See **Logwatch dist.conf files for Arch Linux (https://bbs.archlinux.org/viewtopic.php?id=227516)** for details

Older versions of Logwatch do not support querying the systemd journal directly. For this reason, a logger like syslog-ng is required to duplicate the journal output into external log files (such as in `/var/log`). A **patch (http://sourceforge.net/p/logwatch/patches/34/)** is under development to support the systemd journal. Alternately, a custom script could duplicate some of the logwatch functionality by directly querying the journal and sending email(s), as done in a Python script in **this blog post (https://tim.siosm.fr/blog/2014/02/24/journald-log-scanner-python/)**.

Retrieved from "https://wiki.archlinux.org/index.php?title=Logwatch&oldid=482239"

- This page was last edited on 18 July 2017, at 08:42.
-