

Linux System Log Administration

Syslog listens by default on **UDP port 514**.

Verify syslog is running:
>netstat -an | grep 514

Syslogd daemon

Background running job waiting for some event to trigger it to perform some action. (**syslogd** package)

Configuration Settings

(**/etc/syslog.conf**)

Comment lines are denoted with “#” hash mark symbol.

Multiple “selectors” maybe listed per action if separated by a semicolon (;)

facility . priority action

selector

Facility – Code word for type of program / tool that generated the message

Priority – Importance code word

Action – File, remote computer or other location

Facility codes

- ❖ auth, authpriv, cron, **daemon**, kern, lpr, mail, mark, news, **security**, syslog, user, uucp, local0-7
- ❖ Most servers that aren't covered by more specific codes use the daemon facility
- ❖ security and auth are the same, **auth** is preferred
- ❖ mark is reserved for internal use
- ❖ An asterisk (*) refers to all facilities
- ❖ You can specify multiple facilities with commas (,)

Priority codes

debug, info, notice, warning, **warn**, error, **err**, crit, alert, emerg, **panic**

- ❖ The system logger includes the priority code
- ❖ Debug logs the most information
- ❖ Logs messages to the level used listed
- ❖ An asterisk (*) refers to all priorities

Action

Mostly a filename in the **/var**

- ❖ Also maybe a device
- ❖ Or a remote machine
- ❖ Or a list of log files
- ❖ Or a list of log files
- ❖ Or a list of log files
- ❖ Or a list of log files
- ❖ Or a list of log files
- ❖ Or a list of log files
- ❖ Or a list of log files

mail.*	/var/log/mail
Sends all log entries identified by the originating program as related to mail to the listed log file	
kern.*	/var/log/kernel
kern.crit	@logger.n-cg.net
kern.crit	/dev/console
kern.info;kern.err	/var/log/kernel-info

Activating L

logrotate

If

Rotating Log Files

Log rotation tools – rename and optionally delete old log files, and force the log

(**logrotate** package – **cr**)

Configuration Settings

(**/etc/logrotate**)

Sample log

Rot

W

(displays log messages on the screen as they occur)

© Copyright Nickerson Consulting Group 2005-2006