System Logging & Logs Management in Linux

The system log daemon is responsible for logging the system messages generated by applications or kernel. The system log daemon also supports the remote logging. The messages are differentiated by facility and priority. In principle, the logs handled by syslog are available in the /var/log/ directory on Linux system:

```
[root@NehraClasses ~]# ls -l /var/log
total 1956
drwxr-xr-x.  2 root   root      263 Mar  7 15:08       anaconda
drwx------.   2 root   root       23 Mar  7 15:11       audit
-rw-------.    1 root   root    70472 Mar 16 00:40      boot.log
-rw-rw----.  1 root   utmp      384 Mar 15 12:05      btmp
drwxr-xr-x. 2 chrony chrony       6 May 22  2019      chrony
-rw-------.    1 root   root     6021 Mar 16 00:40      cron
drwxr-xr-x. 2 lp     sys        57 Mar  7 15:02       cups
-rw-r--r--.   1 root   root    11530 Mar 15 20:00      dnf.librepo.log
-rw-r--r--.   1 root   root    43385 Mar 15 20:00      dnf.log
-rw-r--r--.  1 root   root     2124 Mar 15 20:00      dnf.rpm.log
-rw-r-----.  1 root   root     1488 Mar 16 00:40      firewalld
drwx--x--x.2 root   gdm         6 Sep 16 20:06       gdm
drwxr-xr-x.2 root   root        6 Sep  8  2020       glusterfs
-rw-r--r--.  1 root   root      918 Mar 15 20:00      hawkey.log
drwx------. 2 root   root       41 Mar 14 16:36       httpd
drwxr-xr-x.2 root   root        6 Aug 21  2020       insights-client
-rw-rw-r--. 1 root   utmp    292292 Mar 16 00:40      lastlog
drwx------. 3 root   root       18 Mar  7 15:02       libvirt
-rw-------. 1 root   root        0 Mar  7 14:59       maillog
-rw-------. 1 root   root  1664151 Mar 16 00:42      messages
drwx------. 2 root   root        6 Mar  7 14:58       private
drwxr-xr-x. 2 root   root        6 Sep  9  2020       qemu-ga
drwxr-xr-x. 2 root   root       43 Mar  7 15:11       rhsm
drwx------. 3 root   root       17 Mar  7 14:59       samba
-rw-------. 1 root   root    18723 Mar 16 00:38      secure
```

```
drwx------. 2 root   root        6 Dec 11  2018          speech-dispatcher
-rw-------. 1 root   root        0 Mar  7 14:59          spooler
drwxr-x---. 2 sssd   sssd       93 Mar  7 15:38          sssd
drwxr-xr-x. 3 root   root       21 Mar  7 15:02          swtpm
drwxr-xr-x. 2 root   root       23 Mar  7 15:11          tuned
-rw-rw-r--. 1 root   utmp    19968 Mar 16 00:38          wtmp
-rw-r--r--. 1 root   root    22294 Mar  7 15:12          Xorg.9.log
```

where some of the logs are dumped under a subdirectory like cups, samba, httpd. Among the logs under /var/log the /var/log/messages is the most common one as the kernel / core system logs are held there. The kernel modules generally dump there too. So, for problem diagnosis / monitoring the /var/log/messages is the primary log file to examine.

The following are the 20 different log files that are located under /var/log/ directory. Some of these log files are distribution specific. For example, you'll see dpkg.log on Debian based systems (for example, on Ubuntu).

/var/log/messages – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.

/var/log/dmesg – Contains kernel ring buffer information. When the system boots up, it prints number of messages on the screen that displays information about the hardware devices that the kernel detects during boot process. These messages are available in kernel ring buffer and whenever the new message comes the old message gets overwritten. You can also view the content of this file using the dmesg command.

/var/log/auth.log – Contains system authorization information, including user logins and authentication mechanism that were used.

/var/log/boot.log – Contains information that are logged when the system boots

/var/log/daemon.log – Contains information logged by the various background daemons that runs on the system

/var/log/dpkg.log – Contains information that are logged when a package is installed or removed using dpkg command

/var/log/kern.log – Contains information logged by the kernel. Helpful for you to troubleshoot a custom-built kernel.

/var/log/lastlog – Displays the recent login information for all the users. This is not an ascii file. You should use lastlog command to view the content of this file.

/var/log/maillog /var/log/mail.log – Contains the log information from the mail server that is running on the system. For example, sendmail logs information about all the sent items to this file

/var/log/user.log – Contains information about all user level logs

/var/log/Xorg.x.log – Log messages from the X

/var/log/alternatives.log – Information by the update-alternatives are logged into this log file. On Ubuntu, update-alternatives maintains symbolic links determining default commands.

/var/log/btmp – This file contains information about failed login attemps. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more”

/var/log/cups – All printer and printing related log messages

/var/log/anaconda.log – When you install Linux, all installation related messages are stored in this log file

/var/log/yum.log – Contains information that are logged when a package is installed using yum

/var/log/cron – Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file

/var/log/secure – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.

/var/log/wtmp or /var/log/utmp – Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information.

/var/log/faillog – Contains user failed login attemps. Use faillog command to display the content of this file.

Apart from the above log files, /var/log directory may also contain the following sub-directories depending on the application that is running on your system.

/var/log/httpd/ (or) /var/log/apache2 – Contains the apache web server access_log and error_log

/var/log/lighttpd/ – Contains light HTTPD access_log and error_log

/var/log/conman/ – Log files for ConMan client. conman connects remote consoles that are managed by conmand daemon.

/var/log/mail/ – This subdirectory contains additional logs from your mail server. For example, sendmail stores the collected mail statistics in /var/log/mail/statistics file

/var/log/prelink/ – prelink program modifies shared libraries and linked binaries to speed up the startup process. /var/log/prelink/prelink.log contains the information about the .so file that was modified by the prelink.

/var/log/audit/ – Contains logs information stored by the Linux audit daemon (auditd).

/var/log/setroubleshoot/ – SELinux uses setroubleshootd (SE Trouble Shoot Daemon) to notify about issues in the security context of files, and logs those information in this log file.

/var/log/samba/ – Contains log information stored by samba, which is used to connect Windows to Linux.

/var/log/sa/ – Contains the daily sar files that are collected by the sysstat package.

/var/log/sssd/ – Use by system security services daemon that manage access to remote directories and authentication mechanisms.

Instead of manually trying to archive the log files, by cleaning it up after x number of days, or by deleting the logs after it reaches certain size, you can do this automatically using logrotate as we discussed earlier.

The system log daemon/service and it’s configuration file differs depending on the version of Linux used i.e.:

RHEL 5: syslogd - /etc/syslog.conf
RHEL 6: rsyslogd - /etc/rsyslog.conf

Rsyslog

Rsyslog is the new logging daemon starting RHEL6 to compete with the old syslog-ng daemon. Few of the benefits rsyslog daemon provides over sysloging are:

1. Reliable Networking
– Rsyslog uses TCP instead of UDP which is more reliable. TCP uses the acknowledgment and retransmission capabilities.
– with Rsyslog daemon you can specify multiple destination hosts/files for messages delivery if rsyslogd is unable to deliver a message to aprticular destination.

2. Precision
– it is possible to filter messages on any part of log message rather than the priority of the message and the original facility.
– support for precise timestamps to log messages that the syslog daemon.

3. Other features
– TLS encryption
– ability to log to SQL databases.

The configuration file – **/etc/rsyslog.conf** for the rsyslogd daemon is used to handle all the messages. The configuration file basically provides rules statements which in turn provides 2 things:

1. Selectors
– what messages to match.
– selector consists of a facility and priority separated by a dot (.)(e.g. mail.info)
2. actions
– what to do with matched messages
– usually a destination to log the message (file on local machine or a remote host)

Selectors and actions

Selectors are made up of 2 things facilities and priorities. They specify which messages to match. The action field specifies what action to apply to the matched message. For Example :

```
kern.debug                    /var/log/kernlog
```

– The messages with with a facility of kernel and priority debug are logged into the file /var/log/kernlog.
– Priority statements are hierarchical in selectors. Rsyslog matches all the messages with specified priority and higher. So all the messages from kernel with priority debug and higher are logged. Debug being the lowest priority all the messages with facility kern are matched.
– Another way to do this is to use the asterisk (*). For example :

```
kern.*                    /var/log/kernlog
```

– multiple selectors can be specified on a single line separated by semicolons. This is useful when same action needs to be applied to multiple messages.
– when a file is listed in action field, the matched messages are written into the file.
– There can be other devices such as FIFO, terminal etc to write the messages to.
– If a username is listed in action field, the matched messages are printed to the users all the terminals if they are logged in.
– (*) in the action field specifies

Understanding rsyslog Actions

Facilities

The **facility** is used to specify which type of program or application is generating the message. Thus, enabling the syslog daemon to handle different sources differently. The table below lists the standard facilities and their description:

Facility	**Description**
auth/authpriv	security/authorization messages (private)
Cron	clock daemon (crond and atd messages)
Daemon	messages from system daemons without separate facility
Kern	kernel messages
local0 – local7	reserved for local use
lpr	line printer subsystem
mail	messages from mail daemons
news	USENET news subsystem

syslog	messages generated internally by system log daemon
user	generic user-level messages
uucp	UUCP subsystem

Priority

The **priority** of a message signifies the importance of that message. Table below lists the standard priorities and their meanings:

Priority	Description
emerg	system is unusable
alert	action must be taken immediately
crit	critical conditions
err	error conditions

warning	warning conditions
notice	normal but significant importance
info	informational messages
debug	debugging messages

Understanding rsyslog Filter Options

Log Rotation

Log files grow regularly overtime and thus they need to be trimmed regularly. Linux provides a utility to provide this functionality without user intervention. The **logrotate** program can be used to automate the log file rotation. The basic logrotate configuration is done in the configuration file **/etc/logrotate.conf**. In the configuration file we can set options such as – how frequently logs should be rotated and how many old logs to be kept.

```
# cat /etc/logrotate.conf
weekly
rotate 4
create
include /etc/logrotate.d
/var/log/wtmp {
   monthly
   minsize 1M
   create 0664 root utmp
   rotate 1
}
```

As per the above logrotate configuration file the logs are rotated every week (renaming the existing log to filename.number order):
minsize 1M – logrotate runs and trims the messages files if the file size is equal to or greater than 1 MB.
rotate 4 – keep the most recent 4 files while rotating.
create – create new file while rotating with specified permission and ownership.
include – include the files mentioned here for the daemon specific log rotation settings.

```
# ls -l /var/log/messages*
-rw------- 1 root root   1973 Jun 10 15:07 /var/log/messages
-rw------- 1 root root  10866 Jun  6 04:02 /var/log/messages.1
-rw------- 1 root root  19931 May 30 04:02 /var/log/messages.2
-rw------- 1 root root 238772 May 23 04:02 /var/log/messages.3
-rw------- 1 root root 171450 May 14 18:29 /var/log/messages.4
```

– The logrotate daemon mainly reads all the configuration from file /etc/logrotate.conf and then includes daemon specific configuration files from **/etc/logrotate.d/** directory.
– The logrotate daemon along with rotation and removal of old logs, allows compression of log files.
– The daemon runs daily from /etc/cron.daily/logrotate.

Logwatch

– RHEL systems are also shipped with logwatch packages.
– Logwatch is used to analyze the logs to identify any interesting messages.
– Logwatch can configured to analyze logfiles from popular services and email administrator the results.
– It can be configured on hourly or nightly basis for any suspicious activity. By default, in a RHEL system, it is run on nightly basis and report is mailed to root user.