1. **System logging**

System logging is performed to keep track of messages generated by kernel, daemons, commands, user activities and so on. There are two daemons - **klogd** and **syslogd**- responsible for logging, with the former captures kernel messages and events, and the latter all other activities. Both daemons are started when the system enters run level 2 and runs the **/etc/rc.d/rc2.d/S12syslog** script and terminated when the system changes run level to 1, 0 or 6, or shuts down, and calls the **/etc/rc.d/rc#.d/K88syslog** script. These scripts are symbolically linked to **/etc/rc.d/init.d/syslog** file, which includes "start" and "stop" functions corresponding with service startup and termination. The daemons read their configuration file **/etc/syslog.conf** when coming up.

**# service syslog status**

syslogd (pid 3465) is running...

klogd (pid 3468) is running...

**The System Log Configuration File**

The system log configuration file is located in the /etc directory and is called syslog.conf. The contents of the default file are shown below:

**# cat /etc/syslog.conf**

# Log all kernel messages to the console.

# Logging much else clutters up the screen.

#kern.\* /dev/console

# Log anything (except mail) of level info or higher.

# Don't log private authentication messages!

\*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.

authpriv.\* /var/log/secure

# Log all the mail messages in one place.

mail.\* -/var/log/maillog

# Log cron stuff

cron.\* /var/log/cron

# Everybody gets emergency messages

\*.emerg \*

# Save news errors of level crit and higher in a special file.

uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log

local7.\* /var/log/boot.log

#

# INN

#

news.=crit /var/log/news/news.crit

news.=err /var/log/news/news.err

news.notice /var/log/news/news.notice

Notice that each uncommented line entry consists of two fields. The left field is called selector and the right one is referred to as action. The selector field is further divided into two sub-fields, which are separated by the period character. The left sub-field, called facility, represents various system process categories that generate messages. Multiple facilities can be defined, with each facility separated from the other by the semicolon character. The right sub-field, called severity level or priority, represents severity associated with the message. The action field determines the destination to send the message to.

Some of the facilities are kern, authpriv, mail and cron. The asterisk character represents all of them.

In the same way, there are multiple severity levels such as emergency (emerg), alert (alert), critical (crit), error (err), warning (warning), notice (notice), informational (info), debug (debug) and none. The sequence provided is in descending order. The asterisk character represents all of them. If a lower severity level is selected, the daemons will log all messages of the service at that and higher levels.

Some example entries are listed and explained below:

1. authpriv.\* /var/log/secure
2. mail.\* /var/log/maillog
3. cron.\* /var/log/cron
4. \*.emerg \*
5. uucp,news.crit /var/log/spooler
6. local7.\* /var/log/boot.log
7. kern.err @vlad02

In the first line entry, facility is "authpriv" which is related to authentication, severity level is \* and the action field is /var/log/secure. This tells the **syslogd** daemon to log all messages generated by the authentication service to the /var/log/secure file.

Similar to the first entry, the second, third and the sixth line entries tell the daemon to capture and log all messages generated by the mail, cron and local7 facilities to the **/var/log/maillog**, **/var/log/cron** and **/var/log/boot.log** files, respectively.

The fourth line indicates that the syslogd daemon will display all emergency messages on the terminals of all logged in users.

In the fifth line entry, two facilities are defined, which tell the daemon to capture critical messages generated by uucp and news facilities and log them to /var/log/spooler file.

The last line entry tells the klogd daemon to forward all kernel error messages to the klogd daemon running on another system vlad02 to handle them. Likewise, you can have messages from any or all facilities redirected to some other system on the network. You will need to set the SYSLOGD OPTIONS directive as follows and restart syslogd to give the system the ability to receive messages from other systems, and log them.

**# grep SYSLOGD\_OPTIONS /etc/sysconfig/syslog**

SYSLOGD\_OPTIONS="-m 0"

**# grep SYSLOGD\_OPTIONS /etc/sysconfig/syslog**

SYSLOGD\_OPTIONS="-m 0 -rx"

**# service syslog restart**

Shutting down kernel logger: [ OK ]

Shutting down system logger: [ OK ]

Starting system logger: [ OK ]

Starting kernel logger: [ OK ]

The -m option changes the mark timestamp to 0 minutes, or, in other words, disables it; the -r option enables the system to receive messages from other systems; and the —x option disables DNS lookups on receiving messages.

**Maintaining and managing log files**

In Linux, all system log files are stored in the **/var/log** directory. Do an **ll** on the directory to list the contents:

**# ll /var/log**

total 2104

-rw-r----- 1 root root 4287 Mar 28 10:19 acpid

-rw------- 1 root root 629539 Feb 23 16:37 anaconda.log

-rw------- 1 root root 26234 Feb 23 16:37 anaconda.syslog

-rw------- 1 root root 47530 Feb 23 16:37 anaconda.xlog

drwxr-x--- 2 root root 4096 Feb 23 16:39 audit

-rw------- 1 root root 0 Mar 28 11:24 boot.log

-rw------- 1 root root 0 Mar 23 09:29 boot.log.1

-rw------- 1 root root 0 Mar 15 20:13 boot.log.2

-rw------- 1 root utmp 1152 Mar 22 10:18 btmp

drwxr-xr-x 2 root root 4096 Nov 11 2007 conman

drwxr-xr-x 2 root root 4096 Nov 11 2007 conman.old

-rw------- 1 root root 1010 Mar 28 13:01 cron

-rw------- 1 root root 917 Mar 28 11:24 cron.1

-rw------- 1 root root 2152 Mar 23 09:29 cron.2

drwxr-xr-x 2 lp sys 4096 Mar 28 11:24 cups

-rw-r--r-- 1 root root 22995 Mar 28 10:17 dmesg

-rw------- 1 root root 16128 Mar 23 10:45 faillog

drwxr-xr-x 2 root root 4096 Mar 28 10:19 gdm

drwx------ 2 root root 4096 Mar 23 10:05 httpd

-rw-r--r-- 1 root root 147168 Mar 28 10:22 lastlog

drwxr-xr-x 2 root root 4096 Feb 23 16:26 mail

-rw------- 1 root root 0 Mar 28 11:24 maillog

-rw------- 1 root root 1196 Mar 28 11:24 maillog.1

-rw------- 1 root root 2592 Mar 23 09:29 maillog.2

-rw------- 1 root root 4435 Mar 15 20:13 maillog.3

-rw------- 1 root root 4788 Mar 1 10:40 maillog.4

-rw-r--r-- 1 root root 0 Feb 23 17:01 mcelog

-rw------- 1 root root 536 Mar 28 13:51 messages

-rw------- 1 root root 43702 Mar 28 11:19 messages.1

The output indicates that there are different log files for different services. Depending on the number of messages generated and captured, log files may fill up the file system where the directory is located very quickly. Also, if a log file grows to a very large size, it becomes troublesome to load and read it.

In RHEL 5, a script **/etc/cron.daily/logrotate** runs the **logrotate** command once a day to rotate log files by sourcing the **/etc/logrotate.conf** file and configuration files from the **/etc/logrotate.d** directory. These files may be modified to perform additional tasks such as removing, compressing and emailing identified log files.

Here is what the **/etc/cron.daily/logrotate** file contains:

**# cat /etc/cron.daily/logrotate**

#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf

EXITVALUE=$?

if [ $EXITVALUE != 0 ]; then

/usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"

fi

exit 0

The /etc/logrotate.conf file contains the following information:

**# cat /etc/logrotate.conf**

# see "man logrotate" for details

# rotate log files weekly

weekly

# keep 4 weeks worth of backlogs

rotate 4

# create new (empty) log files after rotating old ones

create

# uncomment this if you want your log files compressed

#compress

# RPM packages drop log rotation information into this directory

include /etc/logrotate.d

# no packages own wtmp -- we'll rotate them here

/var/log/wtmp {

monthly

minsize 1M

create 0664 root utmp

rotate 1

}

# system-specific logs may be also be configured here.

A log watch command called **tmpwatch** can be scheduled to run periodically, such as on a daily basis via /etc/cron.daily to remove old temporary files from /tmp and /var/tmp directories, as well as any other specified directories. This action prevents the file systems from filling up quickly.

**The system log file**

The default system log file is **/var/log/messages**. This is a plain text file and can be viewed with any file display utility such as cat, more, less, head or tail. This file may be viewed in real time using the tail command with -f switch. The messages file captures time stamp, hostname, daemon or command executed PID of the process and a short description of what is being logged.

The following shows some sample entries from the file:

**# tail -f /var/log/messages**

Mar 28 11:24:01 vlad syslogd 1.4.1: restart.

Mar 28 12:19:10 vlad : error getting update info: Cannot find a valid baseurl for repo: addons

Mar 28 13:19:10 vlad : error getting update info: Cannot find a valid baseurl for repo: addons

Mar 28 13:51:25 vlad kernel: Kernel logging (proc) stopped.

Mar 28 13:51:25 vlad kernel: Kernel log daemon terminating.

Mar 28 13:51:26 vlad exiting on signal 15

Mar 28 13:51:26 vlad syslogd 1.4.1: restart (remote reception).

Mar 28 13:51:26 vlad kernel: klogd 1.4.1, log source = /proc/kmsg started.