

Chapter 14

System Monitoring

This chapter introduces the user to how the administrator can monitor user access and applications, and especially for server installation problems.

Concepts Learned in this Chapter

- Monitoring of a System's usage
- Who has had access to a system
- Log Messages

Table of Contents

System Monitoring.....	1
14.1 System Logging.....	3
14.1.1 System Even Logs.....	3
14.1.2 Log File Specification	3
14.1.3 Log Rotate	5
14.1.4 GUI Monitoring of System Messages.....	5
14.1.5 Log Messages.....	5
14.1.5.1 Logged Security Messages.....	5
14.1.5.2 Server Configuration Error Messages.....	6
14.2 Monitoring Processes using a GUI.....	6
14.2.1 GNOME System Manager – gtop.....	6
14.2.1.1 gtop Processes.....	6
14.2.1.2 gtop Memory Usage.....	7
14.2.1.3 gtop File System	7
14.2.2 KDE Process Manager – kpm.....	9
14.2.2.1 kpm - Graphical.....	9
14.2.2.2 KPM - Numeric.....	10
14.3 Commands Used in this Chapter.....	11
14.4 Chapter Review Questions.....	11

14.1 System Logging

It is often an excellent practice to configure a system to monitor various actions, specifically those that may cause a system problem. Linux comes pre-configured to monitor and log various problems.

14.1.1 System Even Logs

System logs are normally maintained in the `/var/log` directory. Files within this directory typically include:

boot.log	A log of when the system was started and shut down.
cron	A log of cron jobs performed.
dmesg	A copy of the last bootup message.
messages	A general log of non-specific daemon actions where an error occurred, also logs remote logon username / IP address.
rpm_pkgs	A list of rpm packages installed on the system.
secure	A log of various access attempts (successful or not).
up2date	A log of Red Hat's up2date application and actions taken.
xferlog	A log of ftp transfers, does not show file, only date.

In addition, there are directories within the `/var/log` directory for specific applications, such as fax, gdm, httpd, news, sa, and samba.

When viewing the list of logs, one may note that several have a numeric suffix. There are two reasons for this. In the first case, the numeric value is set up for a specific type of log message. In the second case, the log files are “rotated”, so that no one file becomes too long.

14.1.2 Log File Specification ¹

How an event is logged and to what file is specified by the `/etc/syslog.conf` file. This file specifies the type of event or facility generating the event, its level of priority, and the file to which the event log is appended to. The format of the log designation is:

facility.priority	logfile
where	
facility	Specifies the type of event that is to be logged.
auth-priv	Authorization message
cron	Clock messages
daemon	Other system daemon messages
kern	Kernel messages
lpr	Line Printer daemon messages
mail	Mail daemon messages
news	Usenet news daemon messages
syslog	System internal messages
user	Generic user-level messages
uucp	UUCP daemon messages

¹ man 3 syslog

local0 ~ local7	Local use
priority	Specifies the level of the alert.
debug	Lowest level – used when debugging an application
info	Information messages
notice	Normal, but significant condition for warning
warning	Warning of an abnormal condition
err	Error messages
crit	Critical condition
alert	Immediate action required
emerg	Unstable system condition

A useful shortcut for specifying either a facility or priority is the “*”, which acts like a wildcard. Thus **cron.*** would log all priority levels to the specified file, and ***.emerg** would log any system failure to the designated file.

Multiple events may be combined on one line, each separated by a semicolon. Thus **mail.none; news.none** would log either event to the same file.

A typical **/etc/syslog.conf** file consists of (without the comments):

```
*.info; mail.none; news.none; authpriv.none; cron.none
    /var/log/messages
authpriv.*                /var/log/secure
mail.*                    /var/log/maillog
*.emerg                   *
uucp,news.crit            /var/log/spooler
local7.*                  /var/log/boot.log
news.=crit                /var/log/news.crit
news.=err                  /var/log/news.err
news.=notice              /ave/log/news.notice
```

From the above, one may observe the following:

All log files ending in .info, except for mail, news, authpriv, and cron are all saved to the /var/log/messages file (note the “;” separating facilities). Facilities ending in “.none” are not logged.

All other priority messages are saved to the respective log file for authpriv, mail and local7.

Uucp and news.crit are logged to the spooler file (note that the two facilities are separated by a “,”).

All emergency messages are saved to all log files.

News.crit, news.err, and news.notice messages are saved to their respective log files.

Note that whenever a remote user logs onto the system, via either telnet, ssh, or ftp, that a log message will be written to the secure log file. This is because an authorization message (auth-priv) message is generated.

If an application is installed on a system that is capable of generating log messages, then the **syslog.conf** file may be modified to support the logs and to send them to its own log file if desired.

14.1.3 Log Rotate ²

An application included with the system for the system logs is **logrotate**. This monitors the system log files and rotates them, based either on size or date. When the active log file full (max size limit) or on a periodic basis (typically one week), then it renames the file from (for example) cronlog to cronlog.1. As specified in the global section of the **/etc/logrotate.conf** file, files are typically maintained for four weeks, then the oldest one is discarded. Individual logs may over-ride the global setting, for example the **/var/log/messages** file might be set to rotate for 9 weeks before deleting the oldest file.

It is designed to ease administration of systems that generate large numbers of log files, and thus minimize the amount of hard drive capacity used. Rotated log files may be compressed for further size reduction.

The application is **/usr/sbin/logrotate**, and its configuration file is **/etc/logrotate.conf**. The logrotate.conf file specifies what files are to be rotated, specifying that they are rotated once a week (as specified in the **/etc/cron.weekly** directory), retaining the last four weeks of logs. By default, the logs are not compressed, but may be so configured in the global section of the **/etc/logrotate.conf** file. It is set to run on a daily basis in accordance to the **/etc/cron.daily** configuration file.

14.1.4 GUI Monitoring of System Messages

Newer versions of Red Hat (8 and 9) support a GUI interface for monitoring the log files, rather than having to manually display them using **less**. This is the **redhat-logviewer**. It is typically accessible from the Menu-System Tools-System Logs tab. The benefit of using the logviewer is the inclusion of a filter to limit what is viewed.

14.1.5 Log Messages

There are two categories of log messages that an administrator may focus on in a normal operating environment. They are system security and server configuration error messages.

14.1.5.1 Logged Security Messages

When every a user logs onto a system, their authentication is logged to both the **/var/log/messages** and **/var/log/secure** files. This provides a means to track users that have access to a specific system. Remote users are also logged to the **/var/log/wtmp** file, but this is encrypted and may not be directly read.

Two log files, messages and secure, are displayed for review.
/var/log/messages file (highly abbreviated):

```
# less messages
[root@friedrice log]# less messages
May 10 16:34:13 friedrice ucd-snmp[3540]: Received SNMP packet(s) from 10.7.11.204
May 12 18:09:10 friedrice sshd(pam_unix)[632]: session opened for user root by (uid=0)
May 12 18:36:50 friedrice ftpd[735]: FTP LOGIN FROM ricent [10.7.9.148], dennis
May 12 18:40:06 friedrice ftpd[735]: FTP session closed
```

² man logrotate

From this short example, we can observe that the system logged an snmp request, received on May 10th at 4:34:13 PM from the system at 10.7.11.204. On May 12th at 6:09:10 PM an ssh session was opened for the user root. At 6:36:50 PM an FTP from recent (10.7.9.148) was opened. Finally, the FTP session was closed at 6:40:06 PM.

/var/log/secure file:

```
# less secure
May 11 11:03:08 friedrice xinetd[862]: START: sgi_fam pid=31596 from=0.0.0.0
May 12 18:09:10 friedrice sshd[632]: Accepted password for root from 10.7.9.148 port 1626 ssh2
May 12 18:36:33 friedrice xinetd[862]: START: ftp pid=735 from=10.7.9.148
May 12 18:40:06 friedrice xinetd[862]: EXIT: ftp pid=735 duration=213(sec)
```

From the secure file we can see that xinetd was run at 11:03:08 AM and that on May 12th at 6:09:10 PM (same as above) that the ssh session was started and that the password for root was accepted, and that the originating system was at 10.7.9.148. We also observe that an FTP session was started at 6:36:33 from 10.7.9.148 and was closed at 6:40:06 PM, lasting for 213 seconds.

14.1.5.2 Server Configuration Error Messages

When configuring a server and an error in the configuration occurs, quite often (well, most of the time), an error message is generated and written to the **/var/log/messages** file. One of the most common examples of configuration errors occurs when setting up a DNS server. Although the information is not specific, by reading closely one may often determine what the problem is and fix it. Most specifically, the line number typically follows the filename of the file in error, thus providing a clue as to where to look for the problem.

14.2 Monitoring Processes using a GUI

Previously we discussed the CLI commands of vmstat, free, top, iostat, and sar. In addition to these, we have two X Window applications that provide similar information in a graphical format.

14.2.1 GNOME System Manager – gtop

The GNOME System Manager, or **gtop**, provides a very nice graphical presentation of the system processes. Three screens are available to show how the system is performing.

14.2.1.1 gtop Processes

The Processes screen displays all active processes that are running on the system. This is equivalent to the **ps aux** command. See Figure 14.1.

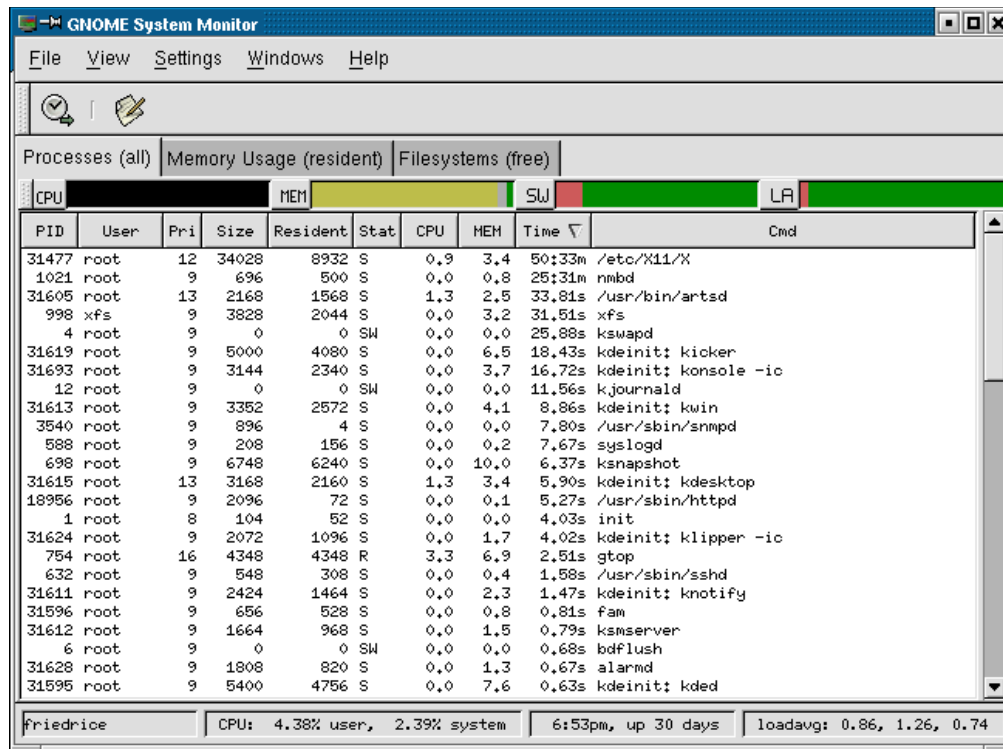


Figure 14.1: gtop Processes

14.2.1.2 gtop Memory Usage

The Memory Usage screen displays how memory is being allocated. See Figure 14.2.

14.2.1.3 gtop File System

The gtop Filesystems displays the usage of the hard drive(s). This is similar to the **du** command. See Figure 14.3.

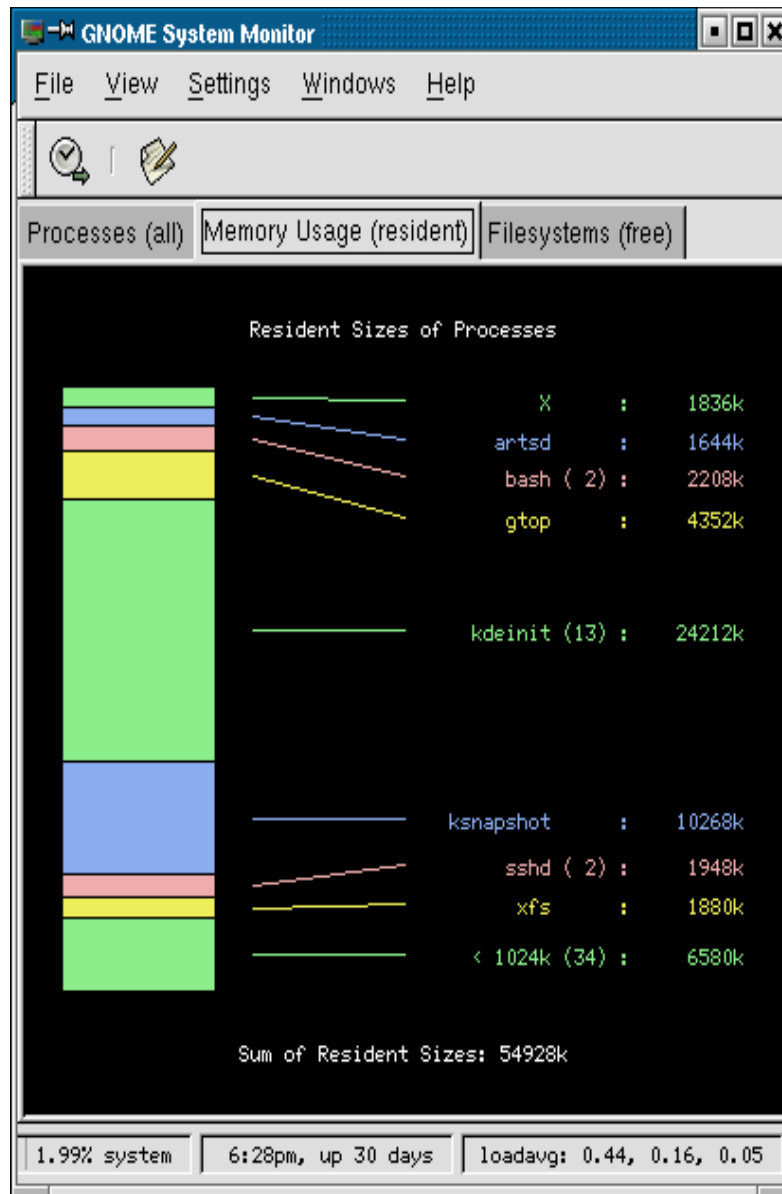
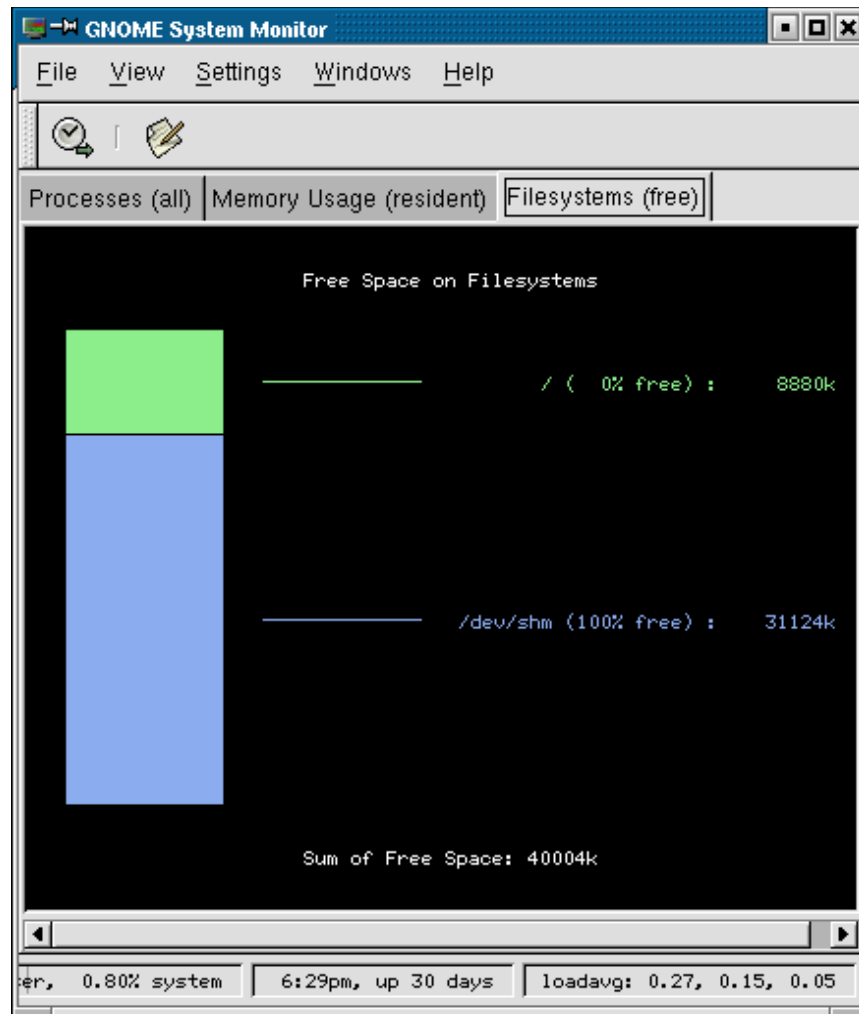


Figure 14.2: gtop Memory Usage



14.3: gtop File System

14.2.2 KDE Process Manager – kpm

KDE also has a X Windows GUI display for monitoring the system operation. It provides the same information as **gtop**, but in a different format. The three boxes at the top of the window may be switched between a graphical display or a text display by a click of the mouse. A nice feature of **kpm** is that by clicking on the desired column header, one can modify the sort order of the display. Thus the administrator may quickly determine which application is using the most memory or CPU time by clicking on the respective tabs.

14.2.2.1 kpm - Graphical

The **kpm** graphical mode displays the system usage through displays at the top of the window. This is shown in Figure 14.4.

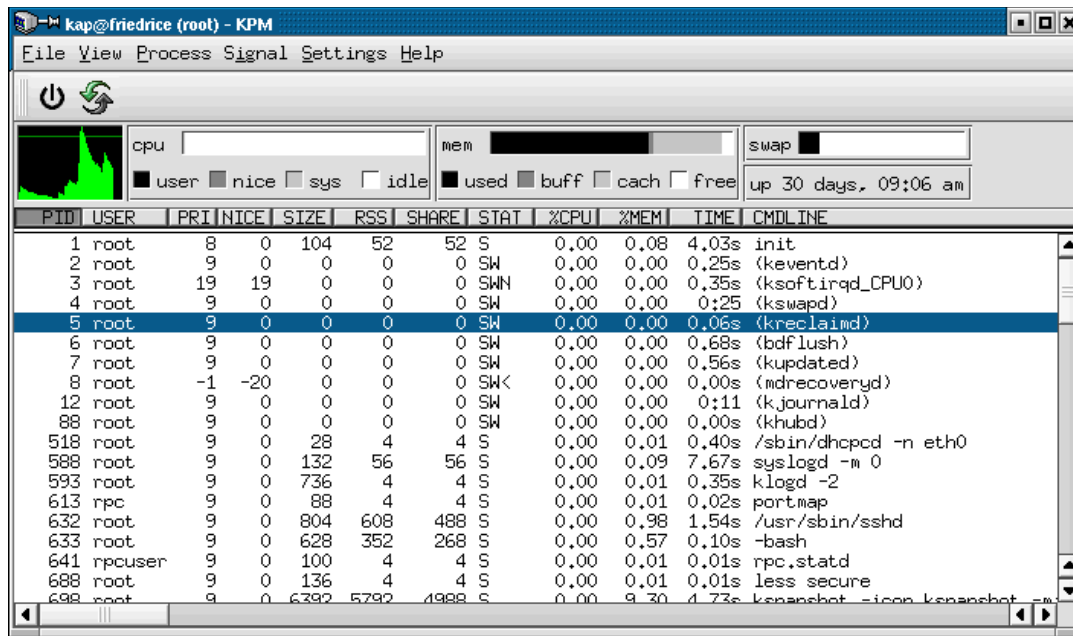


Figure 14.4: KPM Processes

14.2.2.2 KPM - Numeric

The **kpm** numeric mode displays the system usage through displays at the top of the window. Figure 14.5 shows this tool.

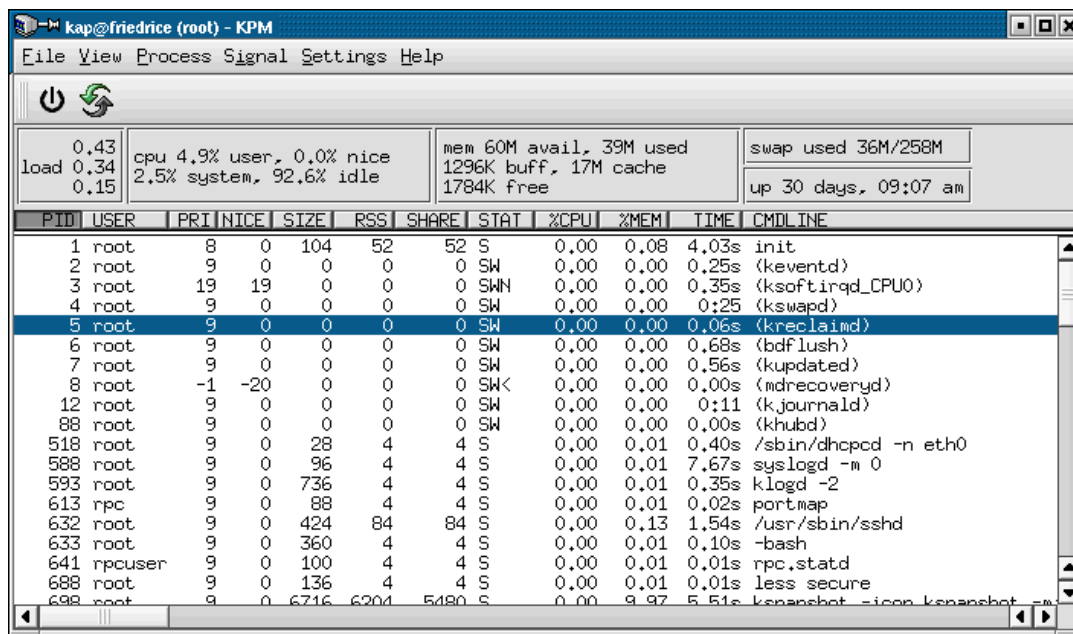


Figure 14.5: KPM Numeric

14.3 Commands Used in this Chapter

gtop	GNOME GUI process monitor
kpm	KDE GUI process monitor
less	Display of a file application

14.4 Chapter Review Questions

Chapter Index

A		Processes	6
Application		K	
GNOME System Manager - gtop	6	kpm	
KDE Process Manager - kpm	9	Graphical Display	9
logrotate	5	Numeric Display	10
redhat-logviewer	5	L	
D		Logging	
Directory		facility	3
/etc/cron.weekly	5	File Specification	3
F		Log Rotate	5
File		Server Configuration Errors	6
/etc/cron.daily	5	System Security	5
/etc/logrotate.conf	5	S	
/etc/syslog.conf example	4	System	
/var/log/messages	5	Event Logs	3
/var/log/wtmp	5	Logging	3
G		U	
gtop		Utility	
Filesystems	7	kpm	9
Memory Usage	7	less	5