Ex. No. 7 **SYSTEM SERVICES**

AIM:

To perform system service such as

a.) Daily cron jobs

b.) Logging into centralized host

PROCEDURE:

a.) Daily cron jobs

1.#tmpwatch

It deletes all files in /tmp directory that have not been accessed for 240 hours. It also deletes files in /var/tmp that have not been accessed for 720 hours.

Options:

-u, --atime

Makes the decision about deleting a file based on the file's atime (access time). This is the default.

Note that the periodic updatedb file system scans keep the atime of directories recent.

-m, --mtime

Makes the decision about deleting a file based on the file's mtime (modification time) instead of the atime.

-c, --ctime

Makes the decision about deleting a file based on the file's ctime (inode change time) instead of the atime; for directories, make the decision based on the mtime.

-M, --dirmtime

Makes the decision about deleting a directory based on the directory's mtime (modification time) instead of the atime; completely ignore atime for directories.

-a, --all

Removes all file types, not just regular files, symbolic links and directories.

-d, --nodirs

Do not attempt to remove directories, even if they are empty.

-d, --nosymlinks

Do not attempt to remove symbolic links.

-f, --force

Removes files even if root doesn't have write access (akin to rm -f).

-q, --quiet

Reports only fatal errors.

2.#logrotate

Left unchecked system logs will grow until you run out of disk space. Logrotate rotates log files from different subsystems at predefined intervals or when they reach predefined size and old logs are optionally compressed. Configuration is stored in /etc for general

settings and /etc/logrotate.d/subsystem for subsystem specific settings. Service specific rotation rules are usually installed by the services rpm.

Options:

-d Turns on debug mode and implies –v

-f Tells logrotate to force the rotation even if it doesn't think it is necessary.

-m tells logrotate which command to use when mailing ,logs.

-m <command>

-s tells logrotate to use an alternate file

-s <statefile>

--usage Prints a short usage message.

3.#logwatch

Monitoring system logs is an onerous but important task. If the system logs are not properly monitored then security,software or hardware problems may arise. Logwatch installed by default on most linux systems monitors log files reporting nightly on activity and potentially on any anomalies located. Logwatch is highly configurable.information on writing logfilters is stored in /usr/share/doc/logwatch—version.

Options:

--detail level

This is the detail level of the report. *level* can be high, med, low.

--logfile log-file-group

This will force LogWatch to process only the set of logfiles defined by *log-file-group* (i.e. messages, xferlog, ...). LogWatch will therefore process all services that use those logfiles. This option can be specified more than once to specify multiple logfile-groups.

--service service-name

This will force LogWatch to process only the service specified in *service-name* (i.e. login, pam, identd, ...). LogWatch will therefore also process any log-file-groups necessary to process these services. This option can be specified more than once to specify multiple services to process. A useful *service-name* is *All* which will process all services (and logfile-groups) for which you have filters installed.

--print

Print the results to stdout (i.e. the screen).

--mailto address

Mail the results to the email address or user specified in *address.*

--archives

Each log-file-group has basic logfiles (i.e. /var/log/messages) as well as archives (i.e. /var/log/messages.? or /var/log/messages.?.gz). This option will make LogWatch search through the archives in addition to the regular logfiles. The entries must still be in the proper date range (see below) to be processed, however.

--range range

You can specify a date-range to process. This option is currently limited to only *Yesterday,* Today and *All.*

--debug level

For debugging purposes. *level* can range from 0 to 100. This will *really* clutter up your output. You probably don't want to use this.

--save file-name

Save the output to *file-name* instead of displaying or mailing it.

--logdir directory

Look in *directory* for log files instead of the default directory.

--hostname hostname

Use *hostname* for the reports instead of this system's hostname. In addition, if HostLimit is set in */etc/log.d/logwatch.conf,* then only logs from this hostname will be processed (where appropriate).

--usage

Displays usage information

b.) Logging to a centralized host.

1.) First on the logserver setup syslog to accept remote message.

2.) On the log, client setup syslogd to several message from the facility to log server.

3.) Test the new setup by using logger to generate a syslog message.

Check the messages in /var/log/messages.

a.) Edit

Etc/syslog.config/syslog:

Syslog-options = “-r-m-o”

b.)restart syslog.

4.) append in /etc/rsyslog.conf

User: k@192.168.0.x

Then restart syslog

5.) In the command prompt, give the command logger

Logger -r –t –a “nature of god”

6.) It is appended to /var/log/messages

7.) Thus we have centralized log server.