LPIC-1 102-400 – Lesson 11

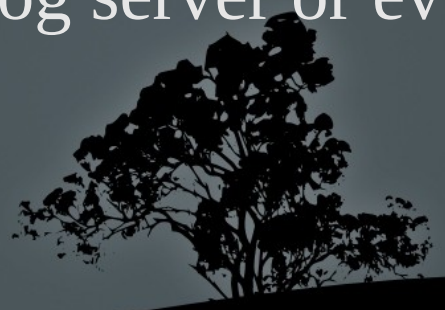
108.2 System logging

Log Files

- Log files are a very important feature of a Linux System because it facilitates looking at the past behavior of a Linux System and see how the system behaves
- The main standard for managing log file is **Syslog** which uuses the **syslogd** daemon as the backend. Syslog uses the Client – Server model, where we can have a central Syslog server and all other systems can send their logs to it.
- Most services use the central log files (/var/log/messages, /var/log/syslog) while others keep their own logs separate (/var/log/apache/*)
- Modern systems have newer implementations of Syslog with more advanced features. Such systems are **rsyslog** and **syslog-ng**. However they all share the same principles.

The */etc/syslog.conf* configuration file

- The **/etc/syslog.conf** provides the configuration for the **syslogd** daemon. The format of the file looks like this:
- **facility.priority action**
- **facility**: defines the source of log messages which can be one of: **auth**, **authpriv**, **cron**, **daemon**, **kern**, **lpr**, **mail**, **ftp**, **mark**, **news**, **syslog**, **user**, **uucp**, and **local0** to **local7**
- **priority**: gives the severity of messages and can be one of (sorted from the most severe to the mildest): **emerg**, **alert**, **crit**, **err**, **warning, notice**, **info, debug**
- **action**: here the destination of messages is set. Usually it can be some log file, a terminal, a syslog server or even a user



List of facilities

facility	Description
authpriv (auth,security)	Authentication, authorization and security messages. Using authpriv is preferable over auth and security
cron	Messages originating from the cron scheduler
daemon	Messages for daemons that do not have their own facility
ftp	Messages from ftp daemons
kern	Messages from the kernel
lpr	Messages from the printing system
mail	Messages from email daemons
mark	For internal syslog usage
news	Message from the nntp daemon (newsgroups)
syslog	Messages from syslog itself
user	Messages from user processes
uucp	Messages fron the UUCP system (Unix-to-Unix Copy)
local0,local1,...,local7	These services are intended for local use and their roles are defined by the system administrator

List of priorities

priority	Description
emerg (panic)	Ultra urgent message that concern the system stability and have the highest priority. Using ‘emerg’ is preferred versus ‘panic’
alert	Urgent messages that need immediate action. Second highest priority
crit	Critical conditions. Third higher priority
err (error)	System or services error. Using ‘err’ is preferred over ‘error’
warning (warn)	Serious warning. Using ‘warning’ is preferred over ‘warn’
notice	Important notifications
info	Informational notifications
debug	Used for debugging and problem solving

Example configurations in syslog.conf

- **mail.*** **/var/log/maillog** # send all messages (and any priority), coming from the email system, to the **/var/log/maillog** log file
- ***.emerg** * # send all messages with priority **emerg** (and any facility) to all consoles of all users
- ***.*** **@syslog.server.dom** # send (via network) all messages to the **syslog.server.dom**. Instead of the server name you can use the server IP
- **auth,authpriv.*** **/var/log/auth** # send all security related messages to **/var/log/auth**

Example configurations in syslog.conf

- **kern.crit /dev/console** # Send critical and higher priority (crit, alert, emerg) kernel message to console (usually /dev/tty1)
- **kern.=info;kern.=notice /dev/tty8** # send only information and notification kernel messages to terminal **/dev/tty8** (**Ctrl-Alt-F8**)
- **kern.info;daemon.!debug @10.0.0.10** # send all kernel related informational messages and all except debug daemon messages to the **10.0.0.10** syslog server
- ***.info;mail.none;cron.none;news.none;authpriv.none \ / var/log/messages** # all informational and higher priority system messages, will be send to **/var/log/messages** except **mail**, **cron**, **news**, and **authpriv**

The *syslogd* and *klogd* daemons

- The Syslog systems is separated into the **syslogd** and the **klogd** daemons
- The **syslogd** deamon is about all logs except those related to kernel. For kernel related logs the **klogd** daemon is used
- They have a common configuration file, **/etc/syslog.conf**
- In **sysvinit** systems they have a common startup script: **/etc/rc.d/init.d/syslog start|stop|restart|reload** # in legacy systems
- In modern systems there is only one improved syslog daemon, **rsyslog**

Logging with `logger`

- The **logger** command is used to manually log messages from some user, or via a script
- **`$ logger -p user.info "Strange behavior on console"`**
  `# send the message in quotes to facility` **`user`** `with priority` **`info`**
- **`$ logger -t bug -p user.info "Strange behavior on \ console"`** `# replace the username, at the beginning of the message, with '`**`bug:`**`'`
- The destination of the message depends on the **/etc/syslog.conf** configuration

Rotate/archive old logs with`logrotate`

- The **logrotate** utility is used to prevent the uncontrolled growth of log files which can fill up the disk and cause problems on a running system
- It can archive old, compress and delete old log files after they pass their lifetime. It can also send some log files as email. In the place of old files, new empty files are creating and ready to accept log messages
- Its behavior is controlled from the **/etc/logrotate.conf** configuration file and the individual configuration files under **/etc/logrotate.d/***
- Old log files are renamed numerically and compressed with gzip, e.g. **logfile**, **logfile.1**, **logfile.2.gz**, **logfile.3.gz**

A */etc/logrotate.conf* example

weekly # weekly rotation by default
rotate 4 # hold log files up to 4 weeks by default
create # create new file after archiving
include /etc/logrotate.d # include configuration **/etc/logrotate.d**
/var/log/wtmp { # custom settings for **wtmp**
    missingok # if file is missing no error message is created
    monthly # monthly arciving
    create 0664 root utmp # create a new file with 0664 permissions and root:utmp user and group ownership
    rotate 1 # hold files up to a month
}
/var/log/btmp { # custom settings for **btmp**
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

Viewing log files

- Any text reader/editor can show log files in text form. For binary files there are custom tools depending on the case e.g **last** for **wtmp**
- **# less /var/log/messages** # basic text viewer
- **# view /var/log/syslog** # read only version of vi (also supports compressed files)
- **# zless /var/log/user.2.gz** # for compressed files
- **# grep <string> -r /var/log** # recursively look into log files
- **# zgrep <string> /var/log/auth.log.*.gz** # look into compress files
- **# tail -f -n30 /var/log/secure** # show the last 30 lines of a log file and "follow" as it grows
- **# multitail /var/log/syslog /var/log/mail.log** # **tail** on steroids. View multiple logs simultaneously, colorized messages, mark the position of a log file ...

The *journald* daemon

- Syslog is unstructured and finding what you are looking for in massive text file can be a hard task
- The **journald** daemon aims to be a more efficient log facility on **systemd** systems
- It provides an efficient, structured binary file format
- It uses the **journalctl** command to query its database
- It can cooperate with existing syslog systems
- Unlike syslog, it does not work over the network
- Its configuration file is **/etc/systemd/journald.conf**
- There is a **/var/log/journald** log store of persistent storage. If it does not exist, syslog is used instead

The `journalctl` command

- For querying the **journald** database, the **journalctl** command is used
- **$ journalctl** # show all logs
- **$ journalctl –since "2 hours ago"** # logs for last two hours
- **$ journalctl -u ssh.service** # show ssh logs
- **$ journal -p crit** # show logs with critical priority
- **$ journal _PID=7654** # query by process id
- **$ journal _UID=999** # query by user id
- **$ journal -n 30** # show the 30 most recent entries\
- **$ journal -xe** # show more informational message (x) and jump to the end of pager (e)

License