Log Monitoring in UNIX

- Linux and the applications that run on it can generate all different types of messages, which are recorded in various log files.
- To create, store and recycle these log messages, linux uses a set of
  - configuration files
  - directories
  - programs
  - commands
  - daemons.
- The default location for log files in Linux is /var/log.

List of log files in Centos

- view the list of log files

#ls -l /var/log

Here are some common log files you will find under /var/log:

wtmp
utmp
dmesg
messages
maillog or mail.log
spooler
auth.log or secure

- The wtmp and utmp files keep track of users logging in and out of the system.
- You cannot directly read the contents of these files using cat
- To see who is currently logged in to the Linux server,

- [root~]# who
- root tty1 2013-12-09 10:44
- root pts/0 2013-12-09 10:29 (10.0.2.2)
- sysadmin pts/1 2013-12-09 10:31 (10.0.2.2)

Last command

- To see login history of user sysadmin
- [root@TestLinux ~]# last | grep sysadmin
- sysadmin pts/1 10.0.2.2 Mon Dec 9 10:31 still logged in
- sysadmin pts/0 10.0.2.2 Fri Nov 29 15:42 - crash (00:01)
- sysadmin pts/0 10.0.2.2 Thu Nov 28 17:06 - 17:13 (00:06)
- sysadmin pts/0 10.0.2.2 Thu Nov 28 16:17 - 17:05 (00:48)
- sysadmin pts/0 10.0.2.2 Thu Nov 28 09:29 - crash (06:04)
- sysadmin pts/0 10.0.2.2 Wed Nov 27 16:37 - down (00:29)
- sysadmin tty1 Wed Nov 27 14:05 - down (00:36)
- sysadmin tty1 Wed Nov 27 13:49 - 14:04 (00:15)

- To find out when was the system last rebooted,
- [root@TestLinux ~]# last reboot

  The result may look like this

  reboot system boot 2.6.32-358.el6.x Mon Dec 9 10:27 - 10:47 (00:19)
  reboot system boot 2.6.32-358.el6.x Fri Dec 6 16:37 - 10:47 (2+18:10)
  reboot system boot 2.6.32-358.el6.x Fri Dec 6 16:28 - 16:36 (00:08) reboot system boot 2.6.32-358.el6.x Fri Dec 6 11:06 - 16:36 (05:29)
  reboot system boot 2.6.32-358.el6.x Mon Dec 2 17:00 - 16:36 (3+23:36)
  reboot system boot 2.6.32-358.el6.x Fri Nov 29 16:01 - 16:36 (7+00:34)
  reboot system boot 2.6.32-358.el6.x Fri Nov 29 15:43 - 16:36 (7+00:53)
  ...
  ...
  wtmp begins Fri Nov 15 16:11:54 2013

- To see when did someone last log in to the system, use lastlog:

```
[root@hpc ~]# lastlog
Username         Port     From             Latest
root             tty1                      Mon Dec  9 10:44:30 +1100 2013
bin                                        **Never logged in****
sshd                                       **Never logged in**
sysadmin         pts/1    10.0.2.2         Mon Dec  9 10:31:50 +1100 2013
dbus                                       **Never logged in**
hpc              pts/2    10.0.2.2         Mon Dec  9 10:39:24 +1100 2013
```

- For other text-based log files, you can use cat, head or tail commands to read the contents.
- To display last ten lines of /var/log/messages file in a Debian box:
- user1@user1:~$ sudo tail /var/log/messages
- Output:
- Dec 16 01:21:08 debian kernel: [9.584074] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
- Dec 16 01:21:08 debian kernel: [9.584074] Bluetooth: BNEP filters: protocol multicast
- Dec 16 01:21:08 debian kernel: [9.648220] Bridge firewalling registered
- Dec 16 01:21:08 debian kernel: [9.696728] Bluetooth: SCO (Voice Link) ver 0.6
- Dec 16 01:21:08 debian kernel: [9.696728] Bluetooth: SCO socket layer initialized
- Dec 16 01:21:08 debian kernel: [9.832215] lp: driver loaded but no devices found
- Dec 16 01:21:08 debian kernel: [9.868897] ppdev: user-space parallel port driver
- Dec 16 01:21:11 debian kernel: [12.748833] [drm] Initialized drm 1.1.0 20060810
- Dec 16 01:21:11 debian kernel: [12.754412] [drm] Initialized vboxvideo 1.0.0 20090303 for 000

The rsyslog Daemon

- This service is responsible for
  - listening to log messages from different parts of a Linux system
  - routing the message to an appropriate log file in the /var/log directory.
  - It can also forward log messages to another Linux server.
- The rsyslog Configuration File
  - The rsyslog daemon gets its configuration information from the rsyslog.conf file.
  - The file is located under the /etc directory.
- The rsyslog.conf file tells the rsyslog daemon where to save its log messages.
- This instruction comes from a series of two-part lines within the file.

- This file can be found at rsyslog.d/50-default.conf on ubuntu.
- The two part instruction is made up of
  - a selector
  - an action.
- The two parts are separated by white space.
  - The selector part ----- specifies what's the source and importance of the log message
  - The action part --------says what to do with the message.
- The selector is again divided into two parts separated by a dot (.).
  - The first part before the dot is called ---------*facility (the origin of the message)
  - second part after the dot is called ---------- priority (the severity of the message).
- Together, the facility/priority and the action pair tell rsyslog what to do
- when a log message matching the criteria is generated.

CentOS rsyslog.conf file:

- # rsyslog v5 configuration file
- ...
- ...
- # Include all config files in /etc/rsyslog.d/
- IncludeConfig /etc/rsyslog.d/*.conf
- #### RULES ####
- # 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;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
...
...
```

Types of facilities

- The different types of facilities recognized by Linux.
  - **auth** or **authpriv**: Messages coming from authorization and security related events
  - **kern**: Any message coming from the Linux kernel
  - **mail**: Messages generated by the mail subsystem
  - **cron**: Cron daemon related messages
  - **daemon**: Messages coming from daemons
  - **news**: Messages coming from network news subsystem
  - **lpr**: Printing related log messages
  - **user**: Log messages coming from user programs
  - **local0 to local7**: Reserved for local use

list of priorities

- list of priorities in ascending order:

  - debug: Debug information from programs
  - info: Simple informational message - no intervention is required
  - notice: Condition that may require attention
  - warn: Warning
  - err: Error
  - crit: Critical condition
  - alert: Condition that needs immediate intervention
  - emerg: Emergency condition

- consider the following line from the file:

- cron.* /var/log/cron
- This tells the rsyslog daemon to save all messages coming from the cron daemon in a file called /var/log/cron.
- The asterix (*) after the dot (.) means messages of all priorities will be logged. Similarly, if the facility was specified as an asterix, it would mean all sources.

Relation in Facilities and priorities

- Facilities and priorities can be related in a number of ways.

- In its default form, when there is only one priority specified after the dot,
- it means all events equal to or greater than that priority will be trapped.
- So the following directive causes any messages coming from the mail subsystem with a priority of warning or higher to be logged in a specific file under /var/log:

- mail.warn /var/log/mail.warn
- This will log every message equal to or greater than the warn priority, but leave everything below it. So messages with err, crit, alert or emerg will also be recorded in this file.

- Using an equal sign (=) after the dot (.) will cause only the specified priority to be logged. So if we wanted to trap only the info messages coming from the mail subsystem, the specification would be something like the following:

- mail.=info /var/log/mail.info
- Again, if we wanted to trap everything from mail subsystem except info messages, the specification would be something like the following

- mail.!info /var/log/mail.info
- or

- mail.!=info /var/log/mail.info
- In the first case, the mail.info file will contain everything with a priority lower than info. In the second case, the file will contain all messages with a priority above info.

- Multiple facilities in the same line can be separated by commas.

- Multiple sources (facility.priority) in the same line is separated by semicolon.

- When an action is marked as an asterix (*), it means all users. This entry in CentOS rsyslog.conf file is saying exactly that:

- When an action is marked as an asterix (*), it means all users. This entry in my CentOS rsyslog.conf file is saying exactly that:

- # Everybody gets emergency messages
- *.emerg *
- Try to see what's the rsyslog.conf is saying in your Linux system. Here is an excerpt from the Debian server I am running:

- # /etc/rsyslog.conf Configuration file for rsyslog.
- #
- # For more information see

- # /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
- ...
- ...
- auth,authpriv.* /var/log/auth.log
- *.*;auth,authpriv.none -/var/log/syslog
- #cron.* /var/log/cron.log
- daemon.* -/var/log/daemon.log
- kern.* -/var/log/kern.log
- lpr.* -/var/log/lpr.log
- mail.* -/var/log/mail.log
- user.* -/var/log/user.log

- #
- # Logging for the mail system. Split it up so that
- # it is easy to write scripts to parse these files.
- #
- mail.info -/var/log/mail.info
- mail.warn -/var/log/mail.warn
- mail.err /var/log/mail.err
- #
- # Logging for INN news system.
- #
- news.crit /var/log/news/news.crit
- news.err /var/log/news/news.err
- news.notice -/var/log/news/news.notice