Systems Software

Week 7: Sockets

Notes By: Jonathan McCarthy

Overview

- Logging
- Syslog
- Auditd

Linux System Logs

- Linux gathers a large amount of log files automatically.
- These log files can be used to see how a given process is performing and if any issues have occurred. If the process has an issue with any aspect of the tasks it performs it should place an entry in the log files.
- Where do log files reside in Linux?
  - var/log directory

Example: daemon.log

mmccarthy@debianJMC2017: /var/www/html

File Edit View Search Terminal Help

```
root@debianJMC2017:/var/log# cat daemon.log
Mar  6 09:00:47 debianJMC2017 NetworkManager[424]: <info> (eth0): link disconnec
ted (deferring action for 4 seconds)
Mar  6 09:00:51 debianJMC2017 NetworkManager[424]: <info> (eth0): link disconnec
ted (calling deferred action)
Mar  6 09:00:51 debianJMC2017 NetworkManager[424]: <info> (eth0): device state c
hange: activated -> unavailable (reason 'carrier-changed') [100 20 40]
Mar  6 09:00:51 debianJMC2017 NetworkManager[424]: <info> (eth0): deactivating d
evice (reason 'carrier-changed') [40]
Mar  6 09:00:51 debianJMC2017 NetworkManager[424]: <info> (eth0): canceled DHCP
transaction, DHCP client pid 5604
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Withdrawing address record for
fe80::a00:27ff:fe1f:f8b7 on eth0.
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Leaving mDNS multicast group on
 interface eth0.IPv6 with address fe80::a00:27ff:fe1f:f8b7.
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Interface eth0.IPv6 no longer r
elevant for mDNS.
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Withdrawing address record for
10.0.2.15 on eth0.
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Leaving mDNS multicast group on
 interface eth0.IPv4 with address 10.0.2.15.
Mar  6 09:00:51 debianJMC2017 avahi-daemon[434]: Interface eth0.IPv4 no longer r
elevant for mDNS.
Mar  6 09:00:51 debianJMC2017 NetworkManager[424]: <info> NetworkManager state i
```

Example: user.log

mmccarthy@debianJMC2017: /var/www/html

File Edit View Search Terminal Help

```
root@debianJMC2017:/var/log# cat user.log | grep mmccarthy
Mar  7 10:14:45 debianJMC2017 /etc/gdm3/Xsession[9808]: localuser:mmccarthy bein
g added to access control list
Mar  7 10:14:46 debianJMC2017 gnome-session[9808]: W: [pulseaudio] authkey.c: Fa
iled to open cookie file '/home/mmccarthy/.config/pulse/cookie': No such file or
 directory
Mar  7 10:14:46 debianJMC2017 gnome-session[9808]: W: [pulseaudio] authkey.c: Fa
iled to load authorization key '/home/mmccarthy/.config/pulse/cookie': No such f
ile or directory
Mar  7 10:14:46 debianJMC2017 gnome-session[9808]: W: [pulseaudio] authkey.c: Fa
iled to open cookie file '/home/mmccarthy/.pulse-cookie': No such file or direct
ory
Mar  7 10:14:46 debianJMC2017 gnome-session[9808]: W: [pulseaudio] authkey.c: Fa
iled to load authorization key '/home/mmccarthy/.pulse-cookie': No such file or
directory
Mar  7 10:14:47 debianJMC2017 gnome-session[9808]: Creating config directory:'/h
ome/mmccarthy/.config/tracker'
Mar  7 10:14:47 debianJMC2017 gnome-session[9808]: Creating config directory:'/h
ome/mmccarthy/.config/tracker'
root@debianJMC2017:/var/log#
```

What types of logs does Linux keep?

File Name	Description
/var/log/user.log	All user level logs
/var/log/kern.log	Info logged by the kernel. May be useful with issues in rebuilding the kernel.
/var/log/daemon.log	Holds info on processes running in the background
/var/usr/cron	When a schedule task is launched, it is logged here
/var/log/audit/	Dit that contains all log info for the auditd daemon
/var/log/boot.log	Log foles for system boot process

- Note: this list in not exhaustive, it is just a sample of the types of log files in a Linux environment!!

What is Syslog??

- The syslog daemon is used to centralise error messages for processes running on a system.
- The syslog files can be kept of the same server or centralised on a different server.

Syslog Protocol

- The syslog protocol specifies how information is propagated over a network.
- It defines a data format definition for its messages.
- This has been standardised in RFC-5424 (also called the IETF-syslog protocol), it uses port 514 for plaintext logs and 6514 for encrypted logs.

Syslog in C

```
SYSLOG(3)                    Linux Programmer's Manual                    SYSLOG(3)

NAME
       closelog, openlog, syslog, vsyslog - send messages to the system logger

SYNOPSIS
       #include <syslog.h>

       void openlog(const char *ident, int option, int facility);
       void syslog(int priority, const char *format, ...);
       void closelog(void);

       #include <stdarg.h>

       void vsyslog(int priority, const char *format, va_list ap);
```

Syslog Messages

- Events from processes will be logged to syslog via messages.
- The message is made up of a header and a number of different fields.

Openlog

- Openlog opens a connection to the system logger.
- The connection is associated to the program currently running.
- **void openlog(const char *ident, int option, int facility);**
- Ident string is added to the start of each log entry.
- If ident is null the program name will be used.

Option

option

The option argument to **openlog**() is an OR of any of these:

LOG_CONS Write directly to system console if there is an error while sending to system logger.

LOG_NDELAY Open the connection immediately (normally, the connection is opened when the first message is logged).

LOG_NOWAIT Don't wait for child processes that may have been created while logging the message. (The GNU C library does not create a child process, so this option has no effect on Linux.)

LOG_ODELAY The converse of **LOG_NDELAY**; opening of the connection is delayed until **syslog**() is called. (This is the default, and need not be specified.)

LOG_PERROR (Not in POSIX.1-2001 or POSIX.1-2008.) Print to stderr as well.

LOG_PID Include PID with each message.

- **void openlog(const char *ident, int option, int facility);**

Facility

facility

The facility argument is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently.

LOG_AUTH security/authorization messages

LOG_AUTHPRIV security/authorization messages (private)

LOG_CRON clock daemon (**cron** and **at**)

LOG_DAEMON system daemons without separate facility value

LOG_FTP ftp daemon

LOG_KERN kernel messages (these can't be generated from user processes)

LOG_LOCAL0 through **LOG_LOCAL7**
reserved for local use

LOG_LPR line printer subsystem

LOG_MAIL mail subsystem

LOG_NEWS USENET news subsystem

LOG_SYSLOG messages generated internally by **syslogd**(8)

LOG_USER (default)
generic user-level messages

LOG_UUCP UUCP subsystem

- **void openlog(const char *ident, int option, int facility);**

Level

level

This determines the importance of the message. The levels are, in order of decreasing importance:

LOG_EMERG	system is unusable
LOG_ALERT	action must be taken immediately
LOG_CRIT	critical conditions
LOG_ERR	error conditions
LOG_WARNING	warning conditions
LOG_NOTICE	normal, but significant, condition
LOG_INFO	informational message
LOG_DEBUG	debug-level message

The function **setlogmask**(3) can be used to restrict logging to specified levels only.

- void syslog(int priority, const char *format, ...);

Simple Example

Open

syslog1.c
~/Documents/Apps/week7/syslog

```c
#include <stdio.h>
#include <unistd.h>
#include <syslog.h>

int main(void) {

    openlog("DT228Yr4", LOG_PID|LOG_CONS, LOG_USER);
    syslog(LOG_INFO, "DT228 rule Linux!!!");
    closelog();

    return 0;
}
```

View the Log

jmccarthy@debianJMC2017: ~/Documents/Apps/week7/syslog

File Edit View Search Terminal Help

```
Mar  9 11:39:03 debianJMC2017 gnome-session[12170]: (tracker-miner-fs:12390): Tr
acker-CRITICAL **:   (Sparql buffer) Error in task 42 of the array-update: UNIQU
E constraint failed: nie:DataObject.nie:url (strerror of errno (not necessarily
related): No such file or directory)
Mar  9 11:39:03 debianJMC2017 gnome-session[12170]: (tracker-miner-fs:12390): Tr
acker-CRITICAL **: Could not execute sparql: UNIQUE constraint failed: nie:DataO
bject.nie:url (strerror of errno (not necessarily related): No such file or dire
ctory)
Mar  9 11:39:03 debianJMC2017 gnome-session[12170]: (tracker-miner-fs:12390): Tr
acker-CRITICAL **:   (Sparql buffer) Error in task 43 of the array-update: UNIQU
E constraint failed: nie:DataObject.nie:url (strerror of errno (not necessarily
related): No such file or directory)
Mar  9 11:39:03 debianJMC2017 gnome-session[12170]: (tracker-miner-fs:12390): Tr
acker-CRITICAL **: Could not execute sparql: UNIQUE constraint failed: nie:DataO
bject.nie:url (strerror of errno (not necessarily related): No such file or dire
ctory)
Mar  9 11:40:07 debianJMC2017 gnome-session[12170]: (gnome-settings-daemon:12271
): color-plugin-WARNING **: unable to get EDID for xrandr-VGA-0: unable to get E
DID for output
Mar  9 11:41:20 debianJMC2017 DT228[12776]: DT228 rule Linux!!!
Mar  9 11:45:18 debianJMC2017 DT228Yr4[12819]: DT228 rule Linux!!!
Mar  9 11:45:30 debianJMC2017 DT228Yr4[12821]: DT228 rule Linux!!!
Mar  9 11:45:40 debianJMC2017 DT228Yr4[12823]: DT228 rule Linux!!!
>>
```

- cd /var/log
- cat user.log

Auditing user actions

Who is doing what? Who modified that file??

Auditd

AUDITD(8) System Administration Utilities AUDITD(8)

NAME

auditd - The Linux Audit daemon

SYNOPSIS

auditd [**-f**] [**-l**] [**-n**] [**-s disable|enable|nochange**]

DESCRIPTION

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk. Viewing the logs is done with the **ausearch** or **aureport** utilities. Configuring the audit rules is done with the **auditctl** utility. During startup, the rules in /etc/audit/audit.rules are read by **auditctl** and loaded into the kernel. Alterately, there is also an **augenrules** program that reads rules located in /etc/audit/rules.d/ and compiles them into an audit.rules file. The audit daemon itself has some configuration options that the admin may wish to customize. They are found in the **auditd.conf** file.

Auditd

- Auditd - Tool for Security Auditing on Linux Server
- Auditd or audit daemon, is a userspace component to the Linux Auditing System.
- It’s responsible for writing audit records to the disk.
- Install: apt-get install auditd
- To add a watch to a file or directory:
  - auditctl -w /var/www/html -p rwxa
- Search logs:
  - ausearch -f /var/www/html/ > accesslog.txt

In Class Demo

- Show how Auditd works and how it can track how it can track file modifications by different system users.

Assignment and General Questions