

Logging - Chapter 10

Log messages

- Virtually everything and anything in the system gets logged.
- Useful for troubleshooting system, if you know where to look.
- What is log entry?
 - line of text with attached properties: timestamp, type and severity of the event, PID and process name written to a file.
 - example: a note of a process starting up, or a critical error or stack trace.
- Sources of logged data:
 - system daemons,
 - kernel
 - custom applications.
- Log data resides on your *finite* size disks.
- Has limited useful life.
- Needs to be retained as long as useful, or legally required, but not indefinitely.
- May need to be summarized, analyzed, searched, filtered, compressed, archives, and finally discarded.

Who is responsible for researching and making sense of logs and records?

System administrator!

System Logs

- Deal with system functioning:
 - authorization mechanisms,
 - system daemons, system messages,
 - and the all-encompassing system log itself, *syslog*.
- Authorization log
 - Lives in `/var/log/auth.log`.
 - Useful for learning about user logins and usage of the `sudo` command.
 - Tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords:
 - Pluggable Authentication Module (PAM) system,
 - the `sudo` command,
 - remote logins to `sshd`.
 - Use `grep` to see specific info:

```
grep sshd /var/log/auth.log | less
```

- Daemon Log
 - Program that runs in the background, usually without human intervention.
 - Performs some operation important to the proper system functioning.
 - Lives in `/var/log/daemon.log` in some systems

- Contains info about running system and application daemons, gdm, mysqld, etc.
- Debug Log
 - Lives in /var/log/debug in some systems
 - Provides detailed debug messages from the Ubuntu system and applications which log to syslogd at the DEBUG level.
- Kernel Log
 - Lives in /var/log/kern.log
 - Provides detailed log of messages from the Ubuntu Linux kernel.
 - Useful for trouble-shooting a new or custom-built kernel, for example.
- Kernel Ring Buffer
 - Not a log per se.
 - An area in the running kernel you can query for kernel bootup messages via the dmesg utility.

`dmesg | less`
- System Log
 - typically contains a lot of information by default about Ubuntu system.
 - Located at /var/log/syslog, and
 - May contain information other logs do not.
 - Contains everything that used to be in /var/log/messages.

Application logs

- Apache server logs
- Samba logs
- Common Unix Printing System (CUPS)

Non-Human readable logs

- Designed to be read by apps, not humans.
- Last logins log.
- Failed logins log.

lastlog and *faillog*

- Login Records log
 - Lives in /var/log/wtmp
 - Not used to show a list of logins.

- Used by who to list all currently logged in users.

Log rotation

- Logs are rotated after a certain timeframe or after reaching a certain size.
- After certain timeframe they are compressed/zipped:
- Archive and compress so they take less space, but still available.
- in /var/log:

```
syslog
syslog1
syslog.2.gz
syslog.3gz
syslog.4.gz
syslog.5.gz
```

- Who rotates logs?
- *logrotate* command
- configurations are in /etc/logrotate.conf file called by /etc/cron.daily/logrotate ...

Log Management

- Collecting logs from many files.
- Providing an interface for querying, analyzing, filtering, and monitoring messages.
- Managing retention and expiration of messages.

Unix syslog

- An integrated system writing messages to plain text files
- Used to collect messages
- Had a number of shortcomings
- Shortcomings resulted in apps, daemons, and scripts writing to their own ad hoc files.
- Result -> a variety of logs that varies among Unix and Linux distros.
- /etc/syslog.conf
- Can you write a message to the log? YES!

```
logger HELLO WORLD!!!!!!!
```

Now check /var/log/syslog

Linux's systemd journal

- Collects messages, indexes and stores them in compressed binary format
- Provides command line interface for viewing and filtering them.
- Can be a standalone or integrated with syslog daemon

Third party tools

- Some open source, some proprietary
- Feature GUI, query languages, data visualization, alerting, automatic anomaly detection.
- Capable of processing terabytes of data.
- Can be hosted on private servers, or can subscribe as cloud services

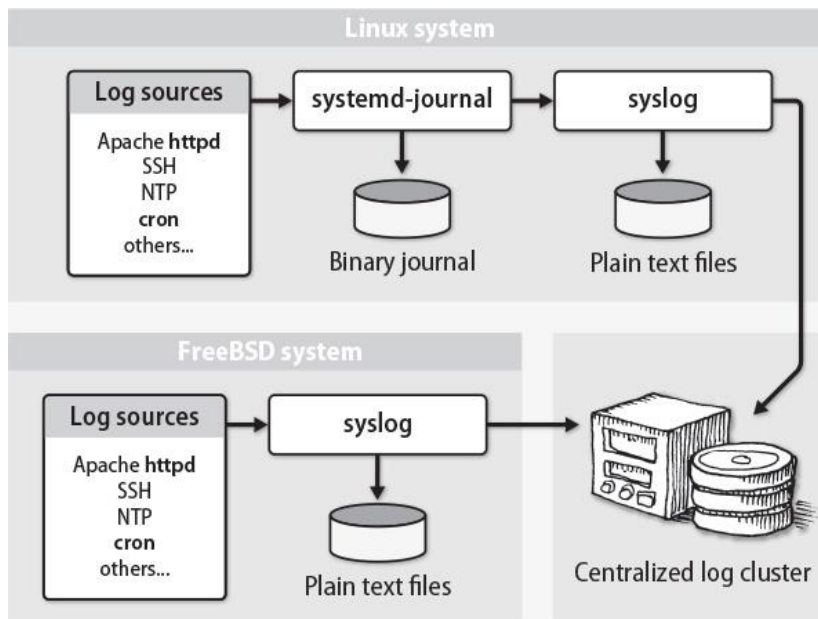


Exhibit A Logging architecture for a site with centralized logging. Img src: course textbook.

Formal IT standards

- PCI DSS (Payment Card Industry Data Security Standard).
 - A set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.
 - Collect logs daily.
 - Centralize logs.
 - Retain logs for 1 year, 3 months shd be easily accessible
 - Protect logs from changes and unauthorized views.
 - Log access to logs.
 - Review logs daily.
 - Backup logs!
 - Log all admin accesses.
 - User logs should have their names.

- COBIT (Control Objectives for Information and Related Technologies)
 - A good-practice framework created by international professional association ISACA for IT management and IT governance.
- ISO 27001 (International Standardization Organization)
 - Provide requirements for information security management system (ISMS)
- Individual industries set their own standards as well.

Log Locations

- Most are in /var/log directory, but some are scattered across the system.
- Unix (and Linux) are not very consistent...

File	Program	Where ^a	Freq ^a	Systems ^a	Contents
apache2/*	httpd	F	D	D	Apache HTTP server logs (v2)
apt*	APT	F	M	D	Aptitude package installations
auth.log	sudo, etc. ^b	S	M	DF	Authorizations
boot.log	rc scripts	F	M	R	Output from system startup scripts
cloud-init.log	cloud-init	F	–	–	Output from cloud init scripts
cron, cron/log	cron	S	W	RF	cron executions and errors
daemon.log	various	S	W	D*	All daemon facility messages
debug*	various	S	D	F,D*	Debugging output
dmesg	kernel	H	–	all	Dump of kernel message buffer
dpkg.log	dpkg	F	M	D	Package management log
faillog ^c	login	H	W	D*	Failed login attempts
httpd/*	httpd	F	D	R	Apache HTTP server logs
kern.log	kernel	S	W	D	All kern facility messages
lastlog	login	H	–	R	Last login time per user (binary)
mail*	mail-related	S	W	RF	All mail facility messages
messages	various	S	W	R	The main system log file
samba/*	smbd, etc.	F	W	–	Samba (Windows/SMB file sharing)
secure	sshd, etc. ^b	S	M	R	Private authorization messages
syslog*	various	S	W	D	The main system log file
wtmp	login	H	M	RD	Login records (binary)
xen/*	Xen	F	1m	RD	Xen virtual machine information
Xorg.n.log	Xorg	F	W	R	X Windows server errors
yum.log	yum	F	M	R	Package management log

a. Where: F = Configuration file, H = Hardwired, S = Syslog
 Frequency: D = Daily, M = Monthly, NNm = Size-based (in MB, e.g., 1m), W = Weekly
 Systems: D = Debian and Ubuntu (D* = Debian only), R = Red Hat and CentOS, F = FreeBSD
 b. passwd, sshd, login, and shutdown also write to the authorization log.
 c. Binary file that must be read with the faillog utility

Image src: course textbook

- Log files are owned by root.
- Some low level processes may have permission to write to logs (httpd)
- May need to use sudo to view some logs.
- /var/log shd be a separate partition on the disk because some logs can be very large.

Do not manage:

- wtmp (wtmpx) – record of all logins and logouts, reboots and shutdowns
 - Very routine info
 - Binary format, use *last* command to read
- lastlog
 - records time of each user's login
 - indexed by UID
 - in binary form
- Database binary transaction logs

Viewing systemd journal

`journalctl -u [some daemon]` – view messages from some daemon

`journalctl -f` – print real time messages as they arrive

Systemd journal

- Systemd has logging daemon `systemd-journald`.
- Can run along `syslog` or independently.
- Saves messages to indexed binary format for easy searches.
- Messages come from:
 - `/dev/log` socket from software that submits messages according to `syslog` conventions (it is a soft link to `/run/systemd/journal/dev-log`).
 - `/dev/kmsg` from Linux kernel
 - Unix `/run/systemd/journal/stdout`
 - Unix `/run/systemd/journal/socket`
 - Audit messages from *auditd* daemon
- Can use utilities to stream journal messages to remote journals:
 - `systemd-journal-remote`
 - `systemd-journal-gateway`
 - `systemd-journal-upload`

Configuring systemd journal

- Configuration file is in `/etc/systemd/journald.conf`
 - Default Storage is set *auto*: saves to `/var/log/journal`, does not create a directory.
 - Other options are *none*, *volatile*, *persistent*.

- Journal is not saved between reboots (BAD?)
- Do not edit directly!
- Create a dir `/etc/systemd/journald.conf.d` and place your configs into a file with `.conf` extension. They get incorporated into the configuration automatically.

Adding options to journalctl

- To enable users to use journalctl to filter messages: add to `systemd-journal` group in `/etc/group`
- Check journal size on disk:

```
$journalctl --disk-usage
Archived and active journals take up 248.0M in the file
system.
```

- Show list of system boots with numerical identifiers:

```
$journalctl --list-boots
```

- To view logs of specific boot session generated by some application:

```
$journalctl -b 0 -u ssh
```

- Restrict by time:

```
$journalctl--since=yesterday--until=now
```

- Show most recent 100 entries from a specific binary:

```
$journalctl -n 100 /usr/sbin/sshd
```

- To find arguments to the command:

```
$journalctl --help
```

Coexisting with syslog

- Both *syslog* and *systemd* are active by default on Linux.
- Both needed to achieve full functionality.
- Both collect and store messages.
- *journald* is missing features that *syslog* has:
 - *syslog* receiving messages from input plug-ins and forwarding to different sets of outputs according to rules and filters.
- Certain files are more convenient in text format.
- *systemd-journald* controls message collection from `/dev/log` socket
- *Syslog* accesses message stream through *systemd*
- *Syslog* retrieves messages in 2 ways:
 - Forwarded by *systemd* to an accessible socket. (Linux)
 - Get messages from journal API, same as `journalctl` command.

Syslog

- Written originally by Eric Allman.
- Comprehensive logging system and IETF standard logging protocol.
- Allows to sort messages by source (facility) and importance (severity levels).
- Allows to route messages to log files, terminals, and remote machines.
- Can receive messages from various sources.
- Can examine message attributes.
- Can modify contents.
- Centralizes the logging.
- Original Linux *syslogd* daemon is replaced by *rsyslogd* (open source project with backward API compatibility).

Reading syslog messages

- Contains messages from different daemons and systems
- Plaintext is read with `pico`, `vi`, `grep`, `less`, etc.

```
vi /var/log/syslog
```

Rsyslogd architecture

- Can be configured in */etc/rsyslog.conf*.
- If edit, restart *rsyslogd* to take effect.
- Starts at boot and runs continuously.
- TERM signal makes daemon exit
- HUP signal makes daemon close all open log files.
- *rsyslog*'s PID is written to */var/run/rsyslogd.pid*. There is just one PID in the file, nth else.

```
kill -HUP `/bin/cat /var/run/rsyslodg.pid`
```