CS 447/647

Logging

Overview

- General
- Log Locations
- systemd Journal
- syslog
- Kernel and Boot-time logging
- Logging at scale

What is logging?

- Line of text with properties
  - Timestamp
  - Type
  - Severity
  - Process Name
  - PID
- Used to glean useful, actionable information
  - AKA Log Management

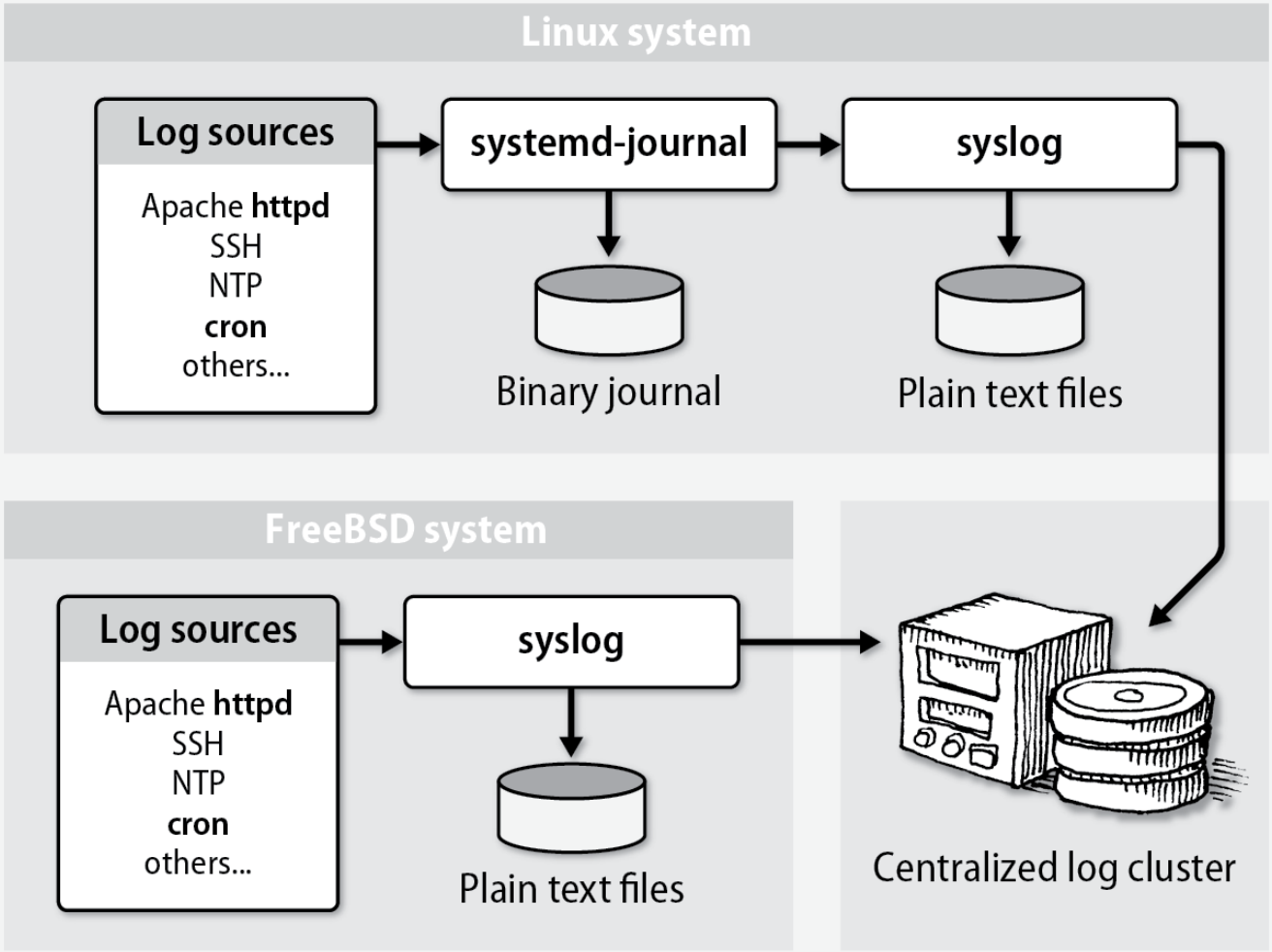
```
tail -n 2 /var/log/syslog


Feb 16 09:36:53 banyan dnsmasq[21819]: using nameserver
134.197.5.1#53

Feb 16 09:36:53 banyan systemd[1]: Started dnsmasq - A
lightweight DHCP and caching DNS server.
```

Log Management

- Collecting logs from a variety of sources
- Providing a structured interface for analysis
  - Filtering
  - Monitoring
- Managing the retention
  - Legal - eDiscovery
    - UNR has a 90 day policy
- syslog - The traditional system for Unix logging
  - Handles storing and forwarding logs
  - Does not provide filtering or monitoring
  - Bypassed by certain applications


Linux system
Log sources
Apache httpd
SSH
NTP
cron
others...
systemd-journal
syslog
Binary journal
Plain text files
FreeBSD system
Log sources
Apache httpd
SSH
NTP
cron
others...
syslog
Plain text files
Centralized log cluster

Why?

- Regulatory Compliance
  - PCI DSS - Payment, Visa, MasterCard...
  - COBIT - IT Governance
  - ISO 27001
- Debugging
- Configuration errors
- Security

Log Locations

- Most logs are in `/var/log`
- Important ones:
  - auth.log - Authentication & Authorizations
    - sudo, ssh, PAM
  - mail - All mail facilities
  - messages - Main system log
  - syslog - System log file
- Mostly owned by root
  - httpd - www-data
  - uwsgi - user-defined
- `/var/log` is often on a separate partition.

Viewing log files

```
$ journalctl -u ssh
-- Logs begin at Sat 2016-08-27 23:18:17 UTC, end at Sat 2016-08-27
    23:33:20 UTC. --
Aug 27 23:18:24 uxenial sshd[2230]: Server listening on 0.0.0.0 port 22.
Aug 27 23:18:24 uxenial sshd[2230]: Server listening on :: port 22.
Aug 27 23:18:24 uxenial systemd[1]: Starting Secure Shell server...
Aug 27 23:18:24 uxenial systemd[1]: Started OpenBSD Secure Shell server.
Aug 27 23:18:28 uxenial sshd[2326]: Accepted publickey for bwhaley from
    10.0.2.2 port 60341 ssh2: RSA SHA256:aaRfGdl0untn758+UCpxL7gkSwcs
    zkAYe/wukrdBATc
Aug 27 23:18:28 uxenial sshd[2326]: pam_unix(sshd:session): session
    opened for user bwhaley by (uid=0)
Aug 27 23:18:34 uxenial sshd[2480]: Did not receive identification string
    from 10.0.2.2
```

systemd Journal

- System service that collects and stores logging data
- Stores log entries in a binary format
  - Indexed
- Collects entries from
  - /dev/log - socket
  - /dev/kmsg - kernel
  - /run/systemd/journal/stdout - collects stdout from services
  - /run/systemd/journal/socket - API

Configuring journald

```
/etc/systemd/journald.conf
/etc/systemd/journald.conf.d

[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
….
```

journalctl filters

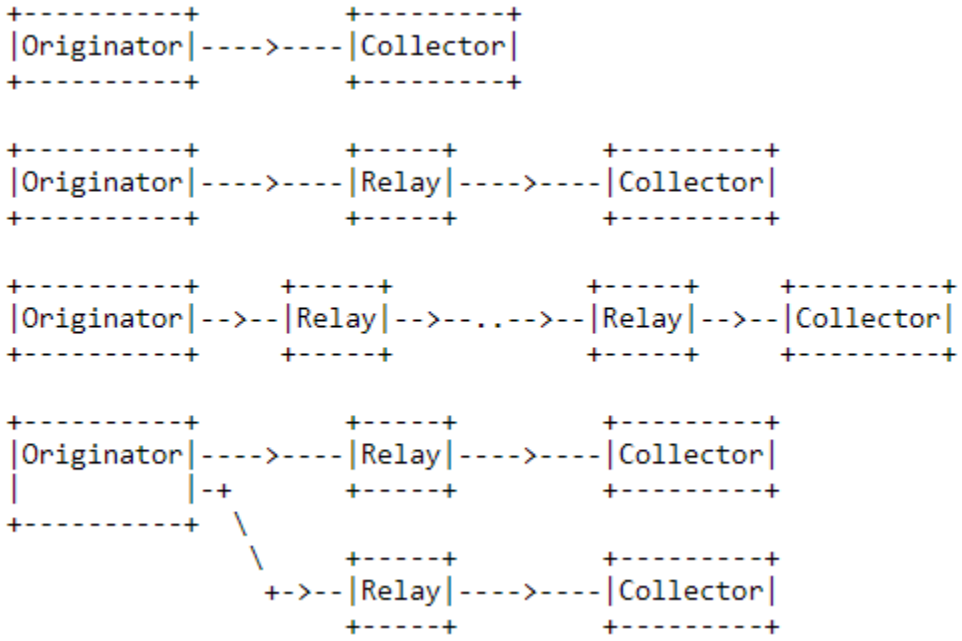
journalctl -b 0 -u ssh

journalctl --since=yesterday --until=now

journalctl -n 100 /usr/sbin/sshd

syslog

- Logging system and IETF protocol
  - RFC5424



syslog

- Two functions
  - Elevate developers from having to write logging systems
  - Administrative control over logging
- Logs can be sorted by
  - Source - Facility
  - Importance - Severity Level
- Centralized logging
- Modern version is rsyslog
  - reliable and extended syslogd

Reading syslog messages

tail -n 20 /var/log/syslog

- Fields
  - Timestamp
  - Hostname
  - Process name and PID
  - Message

```
newell2@banyan:~$ sudo tail -n 10 /var/log/syslog
Feb 16 10:00:53 banyan dhclient[1807]: DHCPACK of 192.168.2.3 from 192.168.2.1
Feb 16 10:00:53 banyan systemd[1]: Reloading Samba SMB Daemon.
Feb 16 10:00:53 banyan systemd[1]: Reloaded Samba SMB Daemon.
Feb 16 10:00:53 banyan dhclient[1807]: bound to 192.168.2.3 -- renewal in 3067 seconds.
Feb 16 10:05:01 banyan CRON[22773]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 16 10:15:01 banyan CRON[22990]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 16 10:17:01 banyan CRON[23080]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Feb 16 10:17:41 banyan smartd[1312]: Device: /dev/sda [SAT], SMART Usage Attribute: 190 Airflow_Tempe
 72 to 71
Feb 16 10:17:41 banyan smartd[1312]: Device: /dev/sdd [SAT], SMART Usage Attribute: 190 Airflow_Tempe
 73 to 72
```

rsyslog

- Configuration in /etc/rsyslogd.conf
- Starts at boot
- Uses /dev/log (Unix Domain Socket)
- Supports
  - Files
  - MySQL
  - Kafka

Facility	Programs that use it
*	All facilities except "mark"
auth	Security- and authorization-related commands
authpriv	Sensitive/private authorization messages
cron	The **cron** daemon
daemon	System daemons
ftp	The FTP daemon, **ftpd** (obsolete)
kern	The kernel
local0-7	Eight flavors of local message
lpr	The line printer spooling system
mail	**sendmail, postfix**, and other mail-related software
mark	Time stamps generated at regular intervals
news	The Usenet news system (obsolete)
syslog	**syslogd** internal messages
user	User processes (the default if not specified)

Level	Approximate meaning
emerg	Panic situations; system is unusable
alert	Urgent situations; immediate action required
crit	Critical conditions
err	Other error conditions
warning	Warning messages
notice	Things that might merit investigation
info	Informational messages
debug	For debugging only

Action	Meaning
filename	Appends the message to a file on the local machine
@*hostname*	Forwards the message to the **rsyslogd** on *hostname*
@*ipaddress*	Forwards the message to *ipaddress* on UDP port 514
@@*ipaddress*	Forwards the message to *ipaddress* on TCP port 514
| *fifoname*	Writes the message to the named pipe *fifoname* [a]
user1,user2,…	Writes the message to the screens of *users* if they are logged in
*	Writes the message to all users who are currently logged in
~	Discards the message
^*program;template*	Formats the message according to the *template* specification and sends it to *program* as the first argument [b]

a. See **man mkfifo** for more information.
b. See **man 5 rsyslog.conf** for further details on templates.

```
local5.* -/var/log/dovecot.log
local5.info -/var/log/dovecot.info
local5.warn -/var/log/dovecot.warn
local5.err -/var/log/dovecot.err
:msg,contains,"stored mail into mailbox"\
                                    -/var/log/dovecot.lmtp
dovecot.conf (END)
```

Log rotation

```
# Global options
errors errors@book.admin.com
rotate 5
weekly

# Logfile rotation definitions and options
/var/log/messages {
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid`
    endscript
}

/var/log/samba/*.log {
    notifempty
    copytruncate
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/lock/samba/*.pid`
    endscript
}
```

Logging at scale

- Elasticsearch, Logstash, Kibana - ELK
  - Open-source leader