Logging

Linux System Administration
Spring 2023

Importance of Logging

- History of events
  - Kernel events
  - System reboots
  - System errors
  - Service start/stop
    - Startup warnings
  - cron jobs
- Audit trail
  - logins
    - refused logins
  - sudo commands
  - files accessed
    - invalid or refused
  - mail messages
  - DHCP requests

Logging types

- **syslog**
  - IETF standard
  - includes remote logging
  - facility.severity
- **systemd-journal**
  - logging by systemd
  - binary format
- Custom logging
  - Apache
    - access
    - error
  - sendmail
  - sudo

syslog

- `rsyslog` newer version
  - IETF standard
  - Systematic logging
    `time host[PID] message`
- Configured by `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf`
  - selectors `facility.level action`

syslog selectors

- facilities (`*`=all except `mark`)
  - `auth` authorization
  - `authpriv` sensitive auth
  - `cron` cron daemon
  - `daemon` system daemons
  - `kern` kernel
  - `localX` local messages
    - `X` = 0-7
  - `mark` regular time
  - `mail` mail
  - `syslog` internal
  - `user` default
- level (minimum) `*`=all
  - `emerg` system panic
  - `alert` action required
  - `crit` critical error
  - `err` error condition
  - `warning` could be a problem
  - `notice` pay attention
  - `info` informational
  - `debug` testing
  - `none` nothing

syslog actions

- `filename` Append to filename (- means no sync)
- `@hostname` Send to remote host
- `@ipaddress` Forward to IP port UDP 514
- `@@ipaddress` Forward to IP port TCP 514
- `|fifo` Write to named pipe
- `user1,user,...` Write message to use consoles
- `*` Write to all user consoles
- `^prog;template` Send to program
- `~` Discard

syslog example (Machine C)

```
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
user.*                          -/var/log/user.log
# Split mail
mail.*                          -/var/log/mail.log
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err
#  Catchall
*.=info;*.=notice;*.=warn;auth,authpriv.none;\
  cron,daemon.none;mail.none   -/var/log/messages
```

systemd-journal

- systemd attempt to take over logging
- Binary journal for quick retrieval
  - More difficult to manage than text files
- Access with `journalctl`
  - See output in `systemctl status`
- Works in tandem with syslog
  - Log messages also forwarded to syslog

journalctl examples

- Show all boots
  - `journalctl --list-boots`
- Show logs as the arrive (follow)
  - `journalctl -f`
- Show entries for a service (`sshd`)
  - `journalctl -u sshd` (RedHat)
  - `journalctl -u ssh` (Debian)

Other logging

- Apache
  - Configured in `<VirtualHost>`
  - `TransferLog` - standard log format
  - `CustomLog` - custom fields and order
  - Strored in `/var/log/httpd` or `/var/log/apache2`
- sudo
  - Configured in `/etc/sudo_logsrvd.conf`
  - Stored in `/var/log/secure` or `/var/log/auth.log`

logger

- Program to add syslog entries (from scripts)
- `logger -p facility.level message`
  - `logger -p daemon.info "Start foo"`
  - `logger -n log.dm.com "Machine C boot"`
- Also useful for testing syslog configs
- systemd-journal has to be different
  - `echo 'Start foo' | systemd-cat -t myapp -p info`

Managing logs

- Logs are stored in `/var/log` or `/var/log/*`
- Log aging set by site policy
- logrotate
  - `/etc/logrotate.conf` and `/etc/logrotate.d/*`
  - Starts new log file daily, weekly, monthly, etc.
  - Keeps older logs as `.1`, `.2.gz`, `.3.gz`, ...
- By default systemd journal grow without limit
  - Limit in `/etc/systemd/journald.conf` with `SystemMaxUse`

Central Logging

- It doesn't take much to drown in logs
  - Roll you own with syslog and scripts
  - ELK : Elasticsearch, Logstash,Kibana
  - Network Management Software (e.g. Observium)
- Make sure all your systems agree on time
  - NTP to synchronize close
  - Consistent time zone