Logging

CSC 510

Log Management

- Many processes emit operational data, called log messages which typically are a line of text that contain associated process information.
- Log management subtasks
  - Collecting logs from a variety of sources
  - Providing a structured interface for querying, analyzing, filtering, and monitoring messages.
  - Managing the retention and expiration of log messages so that information is kept as long as it is potentially useful or legally required, but not indefinitely.

Logging Methods

- Processes write log files in the `/var/log` directory.
- Syslog is a comprehensive logging system that: (1) allows programmers to not need to consider the details of writing log files and (2) gives system administrators control of logging.
- The `systemd` journal, called `systemd-journald`, which is an implementation that duplicates most of syslog's functions.
- Note: most modern Linux distributions run both syslog and journald.

Syslog

- Syslog messages are stored in plain text at `/var/log/syslog` and can be processed with tools such as grep, less, cat, etc.
- The default configuration file is at `/etc/rsyslog.conf` (rsyslog is the common implementation of syslog)
- By default, syslog listens on a Unix domain socket at `/dev/log`
- See the `rsyslog.conf` man page for configuration details.

The systemd Journal

- The systemd journal stores logs in a binary format where all attributes are indexed automatically.
- The journalctl command queries the journal.
- The journal collects logs from various sources:
  - The /dev/log socket
  - The device file /dev/kmsg
  - The /run/systemd/journal/stdout socket
  - The /run/systemd/journal/socket socket
  - Audit messages from the auditd daemon
- The default configuration file is at /etc/systemd/journald.conf; custom configurations are at /etc/systemd/journald.conf.d