**LOG MANAGEMENT**

What does log messages mean?

In computing, a log file is a file that records either events that occur in an operating system or other software runs, or **messages between different users of a communication software.**

**LOG MESSAGES STORS IN /VAR/LOG**

Secure = Authentication and privileges related messages, sudo messages.

Boot.log = when system starts those msg stores.

Message = normal information messages.

Cron = (cron is a command scheduling feature that related msg stores in it.)

Maillog = Mail server related msgs.

* tail /var/log/secure

**LOG MESSAGES 4 FIELDS**

DATE|TIME HOSTNAME|IP PROGRAM NAME WITH PID ACTUAL MSG

* tail -f /var/log/secure (f = follow, live log msgs.)

**HOW LOG MSGS STORES IN THESE FILES?**

**These 2 services stores log msgs.**

**(NOTE:- SYSTEMD-JOURNALD IS THE HEART OF LOGIN ARCHITECTURE)**

1. **systemd-journald(Ephemeral)** (store all row logs/msgs and no filter to save msgs and it saves msgs at **/run/log/journal** and it is a runtime data like after system shutdown these msgs get delete)
2. **rsyslog** (this service picks log msgs from /run/log/journal and filter them and save them in different specific locations at **/var/log** in human readable form.

**RSYSLOG CONF FILE = /etc/rsyslog.conf**

TO SHOW /run/log/journal log msgs run this command

* journalctl
* journalctl -f
* journalctl -n 5
* journalctl -r (IN reverse formate)
* journalctl -p err (show error msgs)
* journalctl –since today
* journalctl –since DATE – until DATE

If we stop these two services then no log msgs will store in the system.

* systemctl status systemd-journald
* systemctl status rsyslog

**IQ- HOW TO SAVE /run/log/journal THESE MSGS. PERMANENTLY**

**ANS - STEPS**

* MAKE A DIRECTORY IN /var/log
* mkdir /var/log/journal
* THEN CHANGE GROUP OWNER
* chgrp systemd-journal journal
* systemctl restart systemd-journald