

System Administration & Security



COMP 175 | Fall 2021 | University of the Pacific | Jeff Shafer

Linux Fundamental Skills: Logs and Log Rotation

Why Logging?

- Provides answers to the questions “**what happened?**” and “**when?**”
- Troubleshooting systems / troubleshooting programs
- Hardware errors?
 - I/O errors for storage, parity errors for memory, ...
- Application failures?
 - Failed logins, crashing services, ...
- Network failures?

Log Files: /var/log/

- **auth.log**
 - User logins (successful and failed)
 - Authentication type used

- **dpkg.log**
 - Packages (*applications*) installed and removed with package manager

- **kern.log**
 - OS kernel log messages
 - Boot messages + OS-level error messages

- **syslog**
 - Application information, warning, and error messages

- *Note: specific file names and contents may vary between Linux distributions*

Syslog Format

- Confusing point: “syslog” is both the name of the log file, and also the name of the system logger process that manages these log files
- Allows for monitoring of network devices and **aggregation** of log messages at a **centralized** collector

Syslog *File* Format

```
Sep 24 06:45:33 cyberlab systemd-networkd[646]: ens5: DHCPv6  
address 2600:1f14:536:b01:9cda:64e:15a9:da0/128 timeout preferred  
150 valid 450
```

- Format
 - Timestamp
 - Hostname where log entry originated
 - Application/process name
 - Process ID
 - Message

NGINX Log Files: `/var/log/nginx`

- `access.log`
 - All requests to the web server, and the response code (either success or failure)

- `error.log`
 - Errors encountered by the web server

Log Rotation

The image shows a terminal window with two panes. The left pane shows the output of a command listing files in the /var/log directory, including various system logs and their rotated versions (e.g., alternatives.log.5.gz, dpkg.log.1, samba). The right pane shows the output of a command listing files in the /etc/logrotate.d directory, including configuration files for various services like speech-dispatcher, syslog, faillog, fontconfig, fsck, gpu-manager, hp, installer, udev, unattended-upgrades, upstart, vboxadd, and wtmp.

```

Terminal
creston@ubuntu: /var/log
creston@ubuntu: /etc/logrotate.d

alternatives.log.5.gz  dpkg.log.1          samba
appart.log             dpkg.log.2.gz      speech-dispatcher
appart.log.1          dpkg.log.3.gz      syslog
appart.log.2.gz       dpkg.log.4.gz      syslog.1
apt                   dpkg.log.5.gz      syslog.2.gz
aptitude              faillog             syslog.3.gz
aptitude.1.gz         fontconfig.log      syslog.4.gz
auth.log              fsck                syslog.5.gz
auth.log.1            gpu-manager.log     syslog.6.gz
auth.log.2.gz         hp                  syslog.7.gz
auth.log.3.gz         installer           udev
auth.log.4.gz         kern.log            unattended-upgrades
boot.log              kern.log.1          upstart
bootstrap.log         kern.log.2.gz      vboxadd-install.log
btmp                  kern.log.3.gz      vboxadd-install-x11.log
btmp.1                kern.log.4.gz      VBoxGuestAdditions.log
cups                  lastlog             wtmp
dist-upgrade          lightdm             wtmp.1
dmesg                 nginx               Xorg.0.log
dmesg.0               pn-powersave.log  Xorg.0.log.old
creston@ubuntu:/var/log$ ls nginx
access.log  access.log.2.gz  error.log
access.log.1  access.log.3.gz  error.log.1
creston@ubuntu:/var/log$
  
```

Wrap-Up

➤ Questions?

➤ Concerns?

➤ **This Week**

➤ **Lab 7** – VPN

➤ **Lab 8** – Scripting (with DNS and Logs)