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

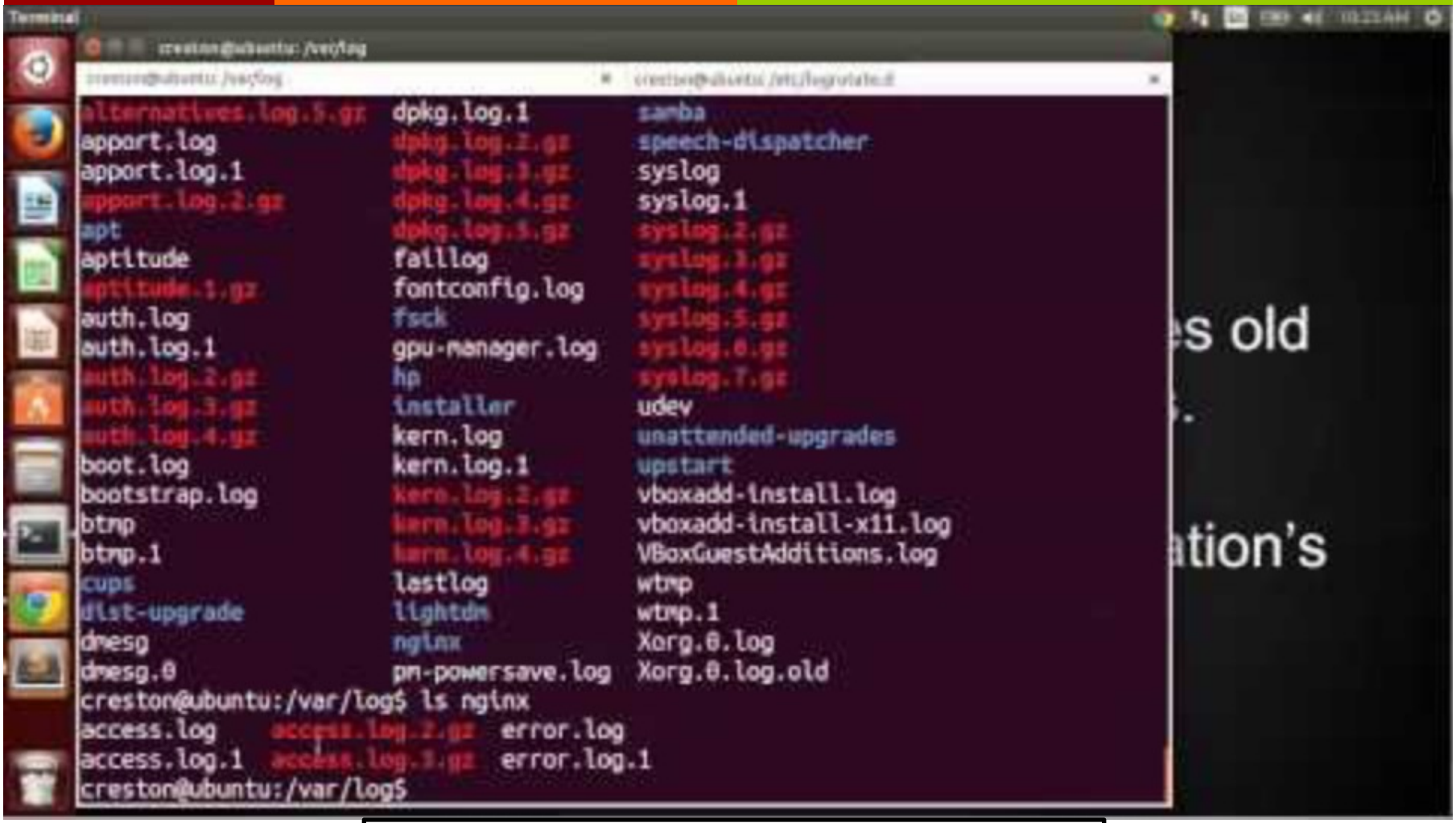
```
Sep 24 06:45:33 cyberlab systemd-networkd[646]: ens5: DHCPv6
address 2600:1f14:536:b01:9cda:64e:15a9:da0/128 timeout preferred
150 valid 450
```

- 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



https://www.youtube.com/watch?v=0U2RMbzKUCY

Wrap-Up

- Questions?
- Concerns?

- **This Week**
  - **Lab 7** – VPN
  - **Lab 8** – Scripting (with DNS and Logs)