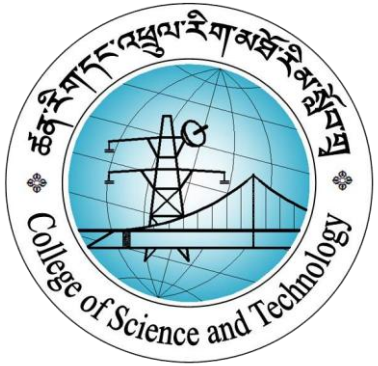

Royal University of Bhutan

LESSON – 17-4

LOGS

LEARNING OUTCOMES

- What is log?
- Importance of logs
- How to check logs

Linux Logs

- What are Linux Log Files?
  - Linux log files are records of system activities. It contains information about processes, errors, and events.
  - Whatever activity you perform on any Linux Distribution, gets recorded every time.
  - It might be any event or execution of any application, all the details are stored in the background without any interruption.
  - Even the activity of any server executing on Linux is also recorded.
  - crucial for troubleshooting issues, analyzing system performance, and ensuring system stability by identifying security threats.

Log Management

- **System Monitoring**: Logs help you keep an eye on your system's health and performance so you know if something goes wrong.
- **Security:** Logs record things like login attempts or firewall activity, helping you catch security threats early.
- **Compliance:** In many industries, logs are required to prove that you are handling data responsibly.
- **Troubleshooting:** If something breaks, logs make it easier to find out what happened and fix it.

Log Management Tools in Linux

Some of the important tools for managing logs in Linux include:

- **syslog**: A standard for logging system messages.
- **rsyslog:** An enhanced version of syslog, offering more features.
- **journald:** Part of systemd, used to manage logs in modern Linux systems.
- **logrotate:** A tool for managing log file rotation, compression, and archiving.

Log Management Tools in Linux

Some of the major log files are:

- /var/log/syslog: General system messages
- /var/log/auth.log: login and permission events
- /var/log/kern.log: Messages from the kernel
- /var/log/boot.log: What happened when the system booted up
- /var/log/dmesg: Kernel messages kept in memory

Log Files

Some of the major log files are:

- /var/log/syslog: General system messages
- /var/log/auth.log: login and permission events
- /var/log/kern.log: Messages from the kernel
- /var/log/boot.log: What happened when the system booted up
- /var/log/dmesg: Kernel messages kept in memory
- /var/log/daemon.log: messages from background processes (daemons)
- /var/log/apache2/error.log: for identifying errors related to website access, configuration issues
- /var/log/mysql/error.log: for database error problems.

Viewing Logs:

To Manage/View Linux Logs:

- using CAT Command
  cat /var/log/auth.log

- using GREP Command
  grep ”invalid” /var/log/auth.log

- using SORT Command (in ascending order.)
  sort /var/log/auth.log

Viewing Logs:

- using UNIQ Command (multiple times)
  uniq /var/log/auth.log

- using TAIL Command
  tail -f /var/log/auth.log

- using LESS Command
  less -f /var/log/auth.log

- using MORE Command
  more -f /var/log/auth.log

SUMMARY

- In this lesson, you have learnt that:

  - Log types
  - Checking logs