What’s in these Linux Logs?

/var/log/syslog or /var/log/messages:

Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system. Know that everything that happens on Redhat-based systems, like CentOS or Rhel, will go in messages. Whereas for Ubuntu and other Debian systems, they go in Syslog.

/var/log/auth.log or /var/log/secure:

Keep authentication logs for both successful or failed logins, and authentication processes. Storage depends on system type. For Debian/Ubuntu, look in /var/log/auth.log. For Redhat/CentrOS, go to /var/log/secure.

/var/log/boot.log: start-up messages and boot info.

/var/log/maillog or var/log/mail.log: is for mail server logs, handy for postfix, smtpd, or email-related services info running on your server.

/var/log/kern: keeps in Kernel logs and warning info. Also useful to fix problems with custom kernels.

/var/log/dmesg: a repository for device driver messages. Use dmesg to see messages in this file.

/var/log/faillog: records info on failed logins. Hence, handy for examining potential security breaches like login credential hacks and brute-force attacks.

/var/log/cron: keeps a record of Crond-related messages (cron jobs). Like when the cron daemon started a job.

/var/log/daemon.log: keeps track of running background services but doesn’t represent them graphically.

/var/log/btmp: keeps a note of all failed login attempts. lastb or last -f /var/log/btmp to read

/var/log/utmp: current login state by user.

/var/log/wtmp: record of each login/logout. last or last -f /var/log/btmp to read

/var/log/lastlog: holds every user’s last login. A binary file you can read via lastlog command.

/var/log/yum.log: holds data on any package installations that used the yum command. So you can check if all went well.

/var/log/httpd/: a directory containing error\_log and access\_log files of the Apache httpd daemon. Every error that httpd comes across is kept in the error\_log file. Think of memory problems and other system-related errors. access\_log logs all requests which come in via HTTP.

/var/log/mysqld.log or /var/log/mysql.log : MySQL log file that records every debug, failure and success message, including starting, stopping and restarting of MySQL daemon mysqld. The system decides on the directory. RedHat, CentOS, Fedora, and other RedHat-based systems use /var/log/mariadb/mariadb.log. However, Debian/Ubuntu use /var/log/mysql/error.log directory.

/var/log/pureftp.log: monitors for FTP connections using the pureftp process. Find data on every connection, FTP login, and authentication failure here.

/var/log/spooler: Usually contains nothing, except rare messages from USENET.

/var/log/xferlog: keeps FTP file transfer sessions. Includes info like file names and user-initiated FTP transfers.

last 查看用户最近的login记录：

last username