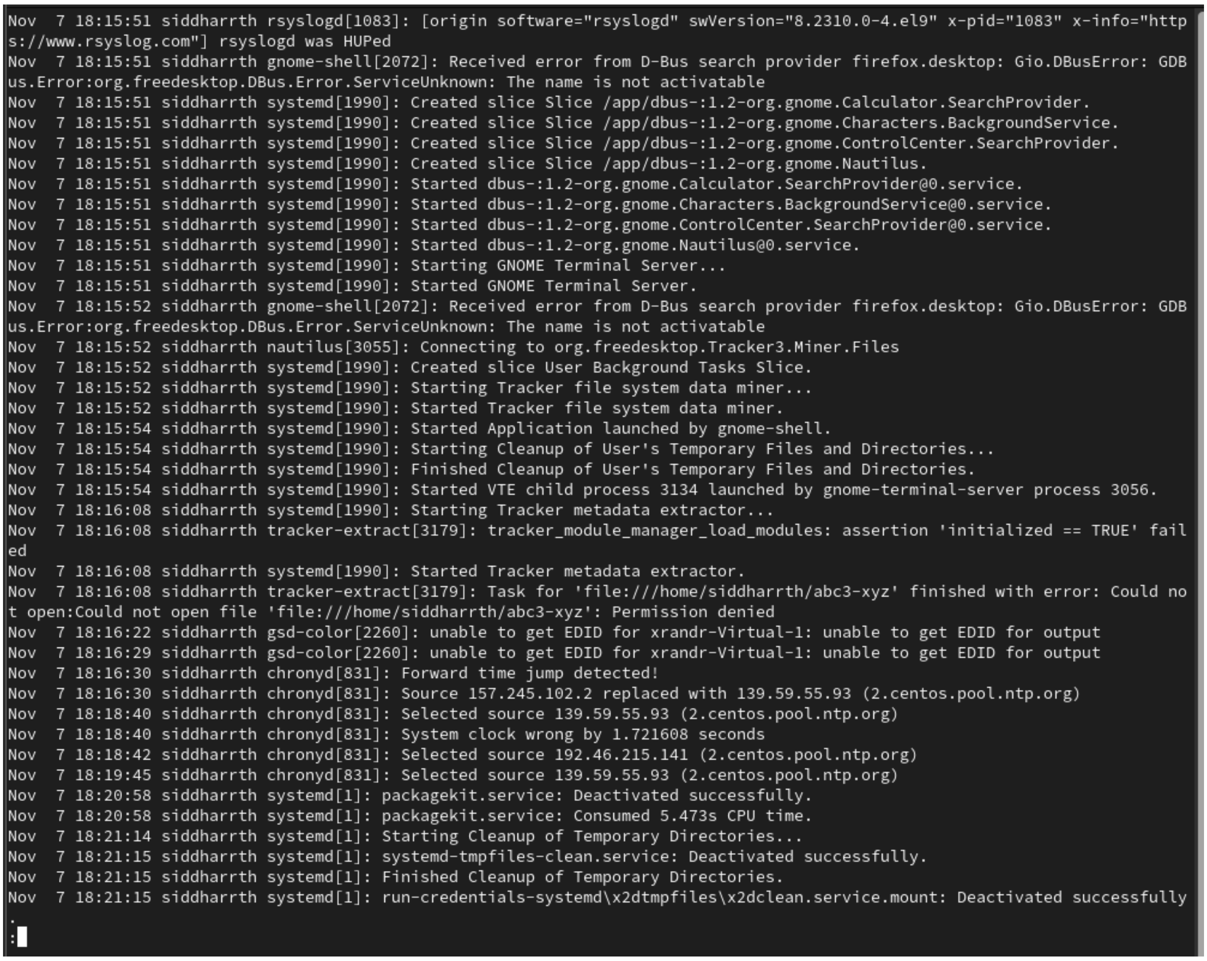
LOGS

Linux maintains various log files to help administrators track system activities and troubleshoot issues. Here are some common log files along with simple explanations:

1. */var/log/messages*

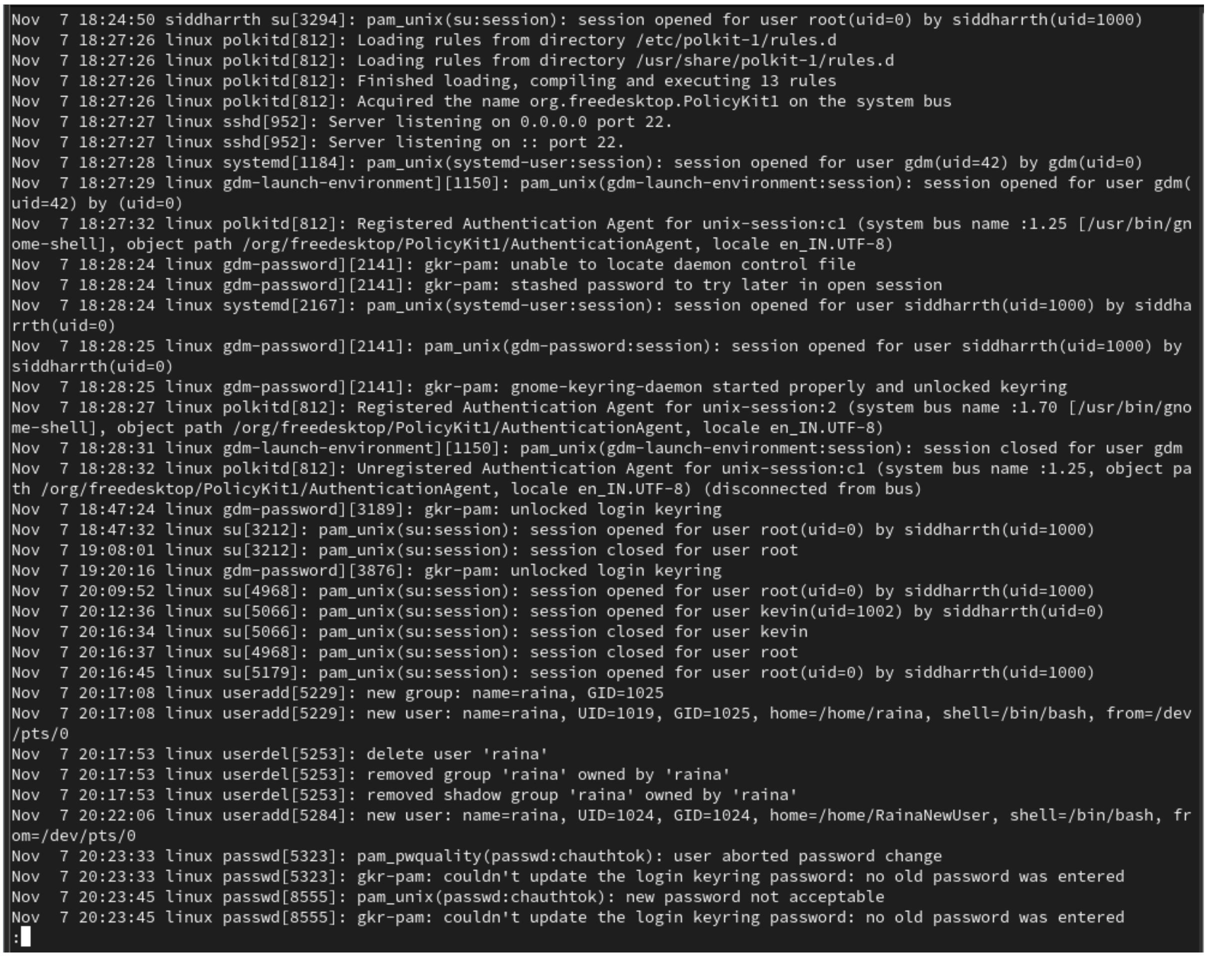
- *Explanation*: This is the primary log file that records a wide range of system events, including boot messages, service startup and shutdown, and general system errors.



```
Nov  7 18:15:51 siddharrth rsyslogd[1083]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1083" x-info="http
s://www.rsyslog.com"] rsyslogd was HUPed
Nov  7 18:15:51 siddharrth gnome-shell[2072]: Received error from D-Bus search provider firefox.desktop: Gio.DBusError: GDB
us.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name is not activatable
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Calculator.SearchProvider.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Characters.BackgroundService.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.ControlCenter.SearchProvider.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Nautilus.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Calculator.SearchProvider@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Characters.BackgroundService@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.ControlCenter.SearchProvider@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Nautilus@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Starting GNOME Terminal Server...
Nov  7 18:15:51 siddharrth systemd[1990]: Started GNOME Terminal Server.
Nov  7 18:15:52 siddharrth gnome-shell[2072]: Received error from D-Bus search provider firefox.desktop: Gio.DBusError: GDB
us.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name is not activatable
Nov  7 18:15:52 siddharrth nautilus[3055]: Connecting to org.freedesktop.Tracker3.Miner.Files
Nov  7 18:15:52 siddharrth systemd[1990]: Created slice User Background Tasks Slice.
Nov  7 18:15:52 siddharrth systemd[1990]: Starting Tracker file system data miner...
Nov  7 18:15:52 siddharrth systemd[1990]: Started Tracker file system data miner.
Nov  7 18:15:54 siddharrth systemd[1990]: Started Application launched by gnome-shell.
Nov  7 18:15:54 siddharrth systemd[1990]: Starting Cleanup of User's Temporary Files and Directories...
Nov  7 18:15:54 siddharrth systemd[1990]: Finished Cleanup of User's Temporary Files and Directories.
Nov  7 18:15:54 siddharrth systemd[1990]: Started VTE child process 3134 launched by gnome-terminal-server process 3056.
Nov  7 18:16:08 siddharrth systemd[1990]: Starting Tracker metadata extractor...
Nov  7 18:16:08 siddharrth tracker-extract[3179]: tracker_module_manager_load_modules: assertion 'initialized == TRUE' fail
ed
Nov  7 18:16:08 siddharrth systemd[1990]: Started Tracker metadata extractor.
Nov  7 18:16:08 siddharrth tracker-extract[3179]: Task for 'file:///home/siddharrth/abc3-xyz' finished with error: Could no
t open:Could not open file 'file:///home/siddharrth/abc3-xyz': Permission denied
Nov  7 18:16:22 siddharrth gsd-color[2260]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Nov  7 18:16:29 siddharrth gsd-color[2260]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Nov  7 18:16:30 siddharrth chronyd[831]: Forward time jump detected!
Nov  7 18:16:30 siddharrth chronyd[831]: Source 157.245.102.2 replaced with 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:18:40 siddharrth chronyd[831]: Selected source 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:18:40 siddharrth chronyd[831]: System clock wrong by 1.721608 seconds
Nov  7 18:18:42 siddharrth chronyd[831]: Selected source 192.46.215.141 (2.centos.pool.ntp.org)
Nov  7 18:19:45 siddharrth chronyd[831]: Selected source 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:20:58 siddharrth systemd[1]: packagekit.service: Deactivated successfully.
Nov  7 18:20:58 siddharrth systemd[1]: packagekit.service: Consumed 5.473s CPU time.
Nov  7 18:21:14 siddharrth systemd[1]: Starting Cleanup of Temporary Directories...
Nov  7 18:21:15 siddharrth systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Nov  7 18:21:15 siddharrth systemd[1]: Finished Cleanup of Temporary Directories.
Nov  7 18:21:15 siddharrth systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated successfully
.
:
```

2. */var/log/secure*

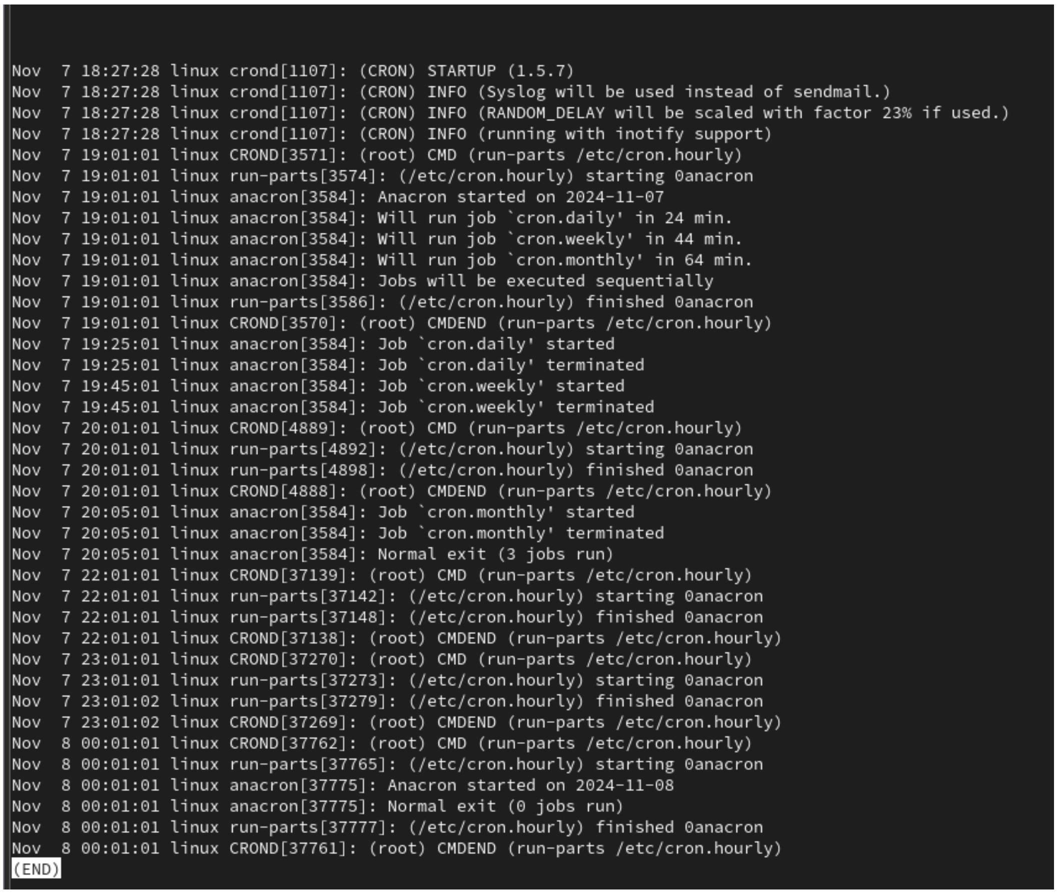
- *Explanation*: This log file keeps track of security-related events, such as authentication attempts (successful and failed), sudo usage, and other securityrelated messages.



```
Nov  7 18:24:50 siddharrth su[3294]: pam_unix(su:session): session opened for user root(uid=0) by siddharrth(uid=1000)
Nov  7 18:27:26 linux polkitd[812]: Loading rules from directory /etc/polkit-1/rules.d
Nov  7 18:27:26 linux polkitd[812]: Loading rules from directory /usr/share/polkit-1/rules.d
Nov  7 18:27:26 linux polkitd[812]: Finished loading, compiling and executing 13 rules
Nov  7 18:27:26 linux polkitd[812]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Nov  7 18:27:27 linux sshd[952]: Server listening on 0.0.0.0 port 22.
Nov  7 18:27:27 linux sshd[952]: Server listening on :: port 22.
Nov  7 18:27:28 linux systemd[1184]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Nov  7 18:27:29 linux gdm-launch-environment][1150]: pam_unix(gdm-launch-environment:session): session opened for user gdm(
uid=42) by (uid=0)
Nov  7 18:27:32 linux polkitd[812]: Registered Authentication Agent for unix-session:c1 (system bus name :1.25 [/usr/bin/gn
ome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_IN.UTF-8)
Nov  7 18:28:24 linux gdm-password][2141]: gkr-pam: unable to locate daemon control file
Nov  7 18:28:24 linux gdm-password][2141]: gkr-pam: stashed password to try later in open session
Nov  7 18:28:24 linux systemd[2167]: pam_unix(systemd-user:session): session opened for user siddharrth(uid=1000) by siddha
rrth(uid=0)
Nov  7 18:28:25 linux gdm-password][2141]: pam_unix(gdm-password:session): session opened for user siddharrth(uid=1000) by
siddharrth(uid=0)
Nov  7 18:28:25 linux gdm-password][2141]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Nov  7 18:28:27 linux polkitd[812]: Registered Authentication Agent for unix-session:2 (system bus name :1.70 [/usr/bin/gno
me-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_IN.UTF-8)
Nov  7 18:28:31 linux gdm-launch-environment][1150]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Nov  7 18:28:32 linux polkitd[812]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.25, object pa
th /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_IN.UTF-8) (disconnected from bus)
Nov  7 18:47:24 linux gdm-password][3189]: gkr-pam: unlocked login keyring
Nov  7 18:47:32 linux su[3212]: pam_unix(su:session): session opened for user root(uid=0) by siddharrth(uid=1000)
Nov  7 19:08:01 linux su[3212]: pam_unix(su:session): session closed for user root
Nov  7 19:20:16 linux gdm-password][3876]: gkr-pam: unlocked login keyring
Nov  7 20:09:52 linux su[4968]: pam_unix(su:session): session opened for user root(uid=0) by siddharrth(uid=1000)
Nov  7 20:12:36 linux su[5066]: pam_unix(su:session): session opened for user kevin(uid=1002) by siddharrth(uid=0)
Nov  7 20:16:34 linux su[5066]: pam_unix(su:session): session closed for user kevin
Nov  7 20:16:37 linux su[4968]: pam_unix(su:session): session closed for user root
Nov  7 20:16:45 linux su[5179]: pam_unix(su:session): session opened for user root(uid=0) by siddharrth(uid=1000)
Nov  7 20:17:08 linux useradd[5229]: new group: name=raina, GID=1025
Nov  7 20:17:08 linux useradd[5229]: new user: name=raina, UID=1019, GID=1025, home=/home/raina, shell=/bin/bash, from=/dev
/pts/0
Nov  7 20:17:53 linux userdel[5253]: delete user 'raina'
Nov  7 20:17:53 linux userdel[5253]: removed group 'raina' owned by 'raina'
Nov  7 20:17:53 linux userdel[5253]: removed shadow group 'raina' owned by 'raina'
Nov  7 20:22:06 linux useradd[5284]: new user: name=raina, UID=1024, GID=1024, home=/home/RainaNewUser, shell=/bin/bash, fr
om=/dev/pts/0
Nov  7 20:23:33 linux passwd[5323]: pam_pwquality(passwd:chauthtok): user aborted password change
Nov  7 20:23:33 linux passwd[5323]: gkr-pam: couldn't update the login keyring password: no old password was entered
Nov  7 20:23:45 linux passwd[8555]: pam_unix(passwd:chauthtok): new password not acceptable
Nov  7 20:23:45 linux passwd[8555]: gkr-pam: couldn't update the login keyring password: no old password was entered
:
```

3. */var/log/cron*

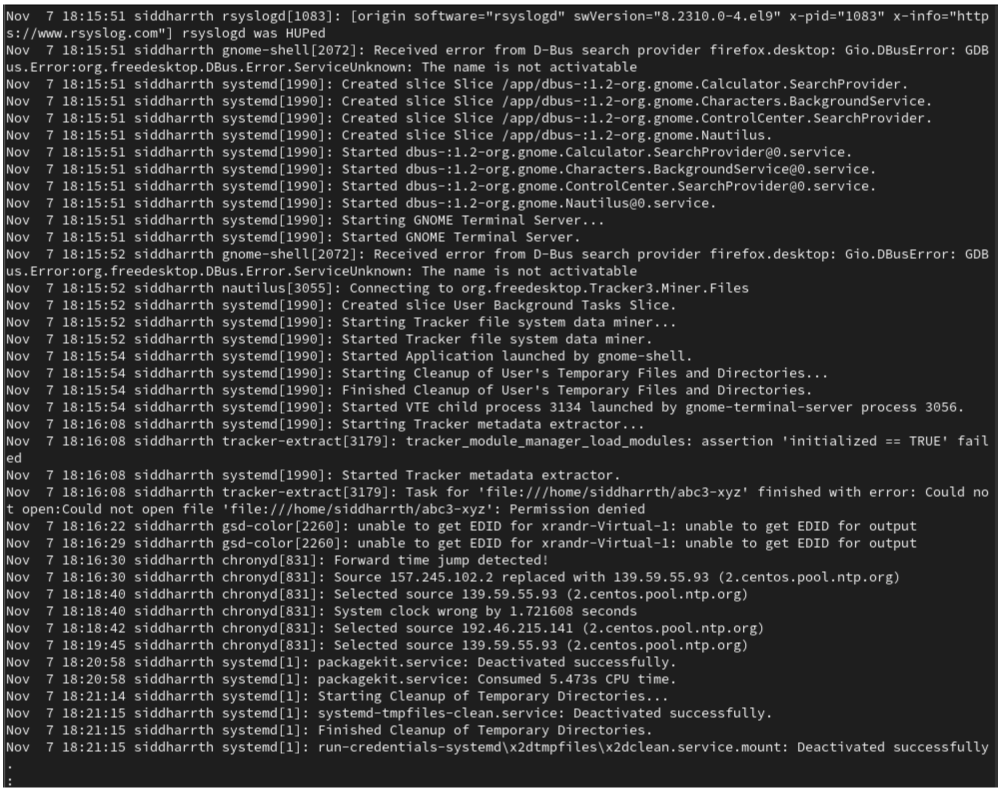
   - *Explanation*: Logs generated by the cron daemon, which schedules and executes periodic tasks, are recorded here.



```
Nov  7 18:27:28 linux crond[1107]: (CRON) STARTUP (1.5.7)
Nov  7 18:27:28 linux crond[1107]: (CRON) INFO (Syslog will be used instead of sendmail.)
Nov  7 18:27:28 linux crond[1107]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 23% if used.)
Nov  7 18:27:28 linux crond[1107]: (CRON) INFO (running with inotify support)
Nov  7 19:01:01 linux CROND[3571]: (root) CMD (run-parts /etc/cron.hourly)
Nov  7 19:01:01 linux run-parts[3574]: (/etc/cron.hourly) starting 0anacron
Nov  7 19:01:01 linux anacron[3584]: Anacron started on 2024-11-07
Nov  7 19:01:01 linux anacron[3584]: Will run job `cron.daily' in 24 min.
Nov  7 19:01:01 linux anacron[3584]: Will run job `cron.weekly' in 44 min.
Nov  7 19:01:01 linux anacron[3584]: Will run job `cron.monthly' in 64 min.
Nov  7 19:01:01 linux anacron[3584]: Jobs will be executed sequentially
Nov  7 19:01:01 linux run-parts[3586]: (/etc/cron.hourly) finished 0anacron
Nov  7 19:01:01 linux CROND[3570]: (root) CMDEND (run-parts /etc/cron.hourly)
Nov  7 19:25:01 linux anacron[3584]: Job `cron.daily' started
Nov  7 19:25:01 linux anacron[3584]: Job `cron.daily' terminated
Nov  7 19:45:01 linux anacron[3584]: Job `cron.weekly' started
Nov  7 19:45:01 linux anacron[3584]: Job `cron.weekly' terminated
Nov  7 20:01:01 linux CROND[4889]: (root) CMD (run-parts /etc/cron.hourly)
Nov  7 20:01:01 linux run-parts[4892]: (/etc/cron.hourly) starting 0anacron
Nov  7 20:01:01 linux run-parts[4898]: (/etc/cron.hourly) finished 0anacron
Nov  7 20:01:01 linux CROND[4888]: (root) CMDEND (run-parts /etc/cron.hourly)
Nov  7 20:05:01 linux anacron[3584]: Job `cron.monthly' started
Nov  7 20:05:01 linux anacron[3584]: Job `cron.monthly' terminated
Nov  7 20:05:01 linux anacron[3584]: Normal exit (3 jobs run)
Nov  7 22:01:01 linux CROND[37139]: (root) CMD (run-parts /etc/cron.hourly)
Nov  7 22:01:01 linux run-parts[37142]: (/etc/cron.hourly) starting 0anacron
Nov  7 22:01:01 linux run-parts[37148]: (/etc/cron.hourly) finished 0anacron
Nov  7 22:01:01 linux CROND[37138]: (root) CMDEND (run-parts /etc/cron.hourly)
Nov  7 23:01:01 linux CROND[37270]: (root) CMD (run-parts /etc/cron.hourly)
Nov  7 23:01:01 linux run-parts[37273]: (/etc/cron.hourly) starting 0anacron
Nov  7 23:01:02 linux run-parts[37279]: (/etc/cron.hourly) finished 0anacron
Nov  7 23:01:02 linux CROND[37269]: (root) CMDEND (run-parts /etc/cron.hourly)
Nov  8 00:01:01 linux CROND[37762]: (root) CMD (run-parts /etc/cron.hourly)
Nov  8 00:01:01 linux run-parts[37765]: (/etc/cron.hourly) starting 0anacron
Nov  8 00:01:01 linux anacron[37775]: Anacron started on 2024-11-08
Nov  8 00:01:01 linux anacron[37775]: Normal exit (0 jobs run)
Nov  8 00:01:01 linux run-parts[37777]: (/etc/cron.hourly) finished 0anacron
Nov  8 00:01:01 linux CROND[37761]: (root) CMDEND (run-parts /etc/cron.hourly)
(END)
```

4. */var/log/dmesg*

   - *Explanation*: Contains kernel ring buffer messages, which are low-level system messages useful for diagnosing hardware and driver issues.



```
Nov  7 18:15:51 siddharrth rsyslogd[1083]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1083" x-info="http
s://www.rsyslog.com"] rsyslogd was HUPed
Nov  7 18:15:51 siddharrth gnome-shell[2072]: Received error from D-Bus search provider firefox.desktop: Gio.DBusError: GDB
us.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name is not activatable
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Calculator.SearchProvider.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Characters.BackgroundService.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.ControlCenter.SearchProvider.
Nov  7 18:15:51 siddharrth systemd[1990]: Created slice Slice /app/dbus-:1.2-org.gnome.Nautilus.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Calculator.SearchProvider@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Characters.BackgroundService@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.ControlCenter.SearchProvider@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Started dbus-:1.2-org.gnome.Nautilus@0.service.
Nov  7 18:15:51 siddharrth systemd[1990]: Starting GNOME Terminal Server...
Nov  7 18:15:51 siddharrth systemd[1990]: Started GNOME Terminal Server.
Nov  7 18:15:52 siddharrth gnome-shell[2072]: Received error from D-Bus search provider firefox.desktop: Gio.DBusError: GDB
us.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name is not activatable
Nov  7 18:15:52 siddharrth nautilus[3055]: Connecting to org.freedesktop.Tracker3.Miner.Files
Nov  7 18:15:52 siddharrth systemd[1990]: Created slice User Background Tasks Slice.
Nov  7 18:15:52 siddharrth systemd[1990]: Starting Tracker file system data miner...
Nov  7 18:15:52 siddharrth systemd[1990]: Started Tracker file system data miner.
Nov  7 18:15:54 siddharrth systemd[1990]: Started Application launched by gnome-shell.
Nov  7 18:15:54 siddharrth systemd[1990]: Starting Cleanup of User's Temporary Files and Directories...
Nov  7 18:15:54 siddharrth systemd[1990]: Finished Cleanup of User's Temporary Files and Directories.
Nov  7 18:15:54 siddharrth systemd[1990]: Started VTE child process 3134 launched by gnome-terminal-server process 3056.
Nov  7 18:16:08 siddharrth systemd[1990]: Starting Tracker metadata extractor...
Nov  7 18:16:08 siddharrth tracker-extract[3179]: tracker_module_manager_load_modules: assertion 'initialized == TRUE' fail
ed
Nov  7 18:16:08 siddharrth systemd[1990]: Started Tracker metadata extractor.
Nov  7 18:16:08 siddharrth tracker-extract[3179]: Task for 'file:///home/siddharrth/abc3-xyz' finished with error: Could no
t open:Could not open file 'file:///home/siddharrth/abc3-xyz': Permission denied
Nov  7 18:16:22 siddharrth gsd-color[2260]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Nov  7 18:16:29 siddharrth gsd-color[2260]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output
Nov  7 18:16:30 siddharrth chronyd[831]: Forward time jump detected!
Nov  7 18:16:30 siddharrth chronyd[831]: Source 157.245.102.2 replaced with 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:18:40 siddharrth chronyd[831]: Selected source 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:18:40 siddharrth chronyd[831]: System clock wrong by 1.721608 seconds
Nov  7 18:18:42 siddharrth chronyd[831]: Selected source 192.46.215.141 (2.centos.pool.ntp.org)
Nov  7 18:19:45 siddharrth chronyd[831]: Selected source 139.59.55.93 (2.centos.pool.ntp.org)
Nov  7 18:20:58 siddharrth systemd[1]: packagekit.service: Deactivated successfully.
Nov  7 18:20:58 siddharrth systemd[1]: packagekit.service: Consumed 5.473s CPU time.
Nov  7 18:21:14 siddharrth systemd[1]: Starting Cleanup of Temporary Directories...
Nov  7 18:21:15 siddharrth systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Nov  7 18:21:15 siddharrth systemd[1]: Finished Cleanup of Temporary Directories.
Nov  7 18:21:15 siddharrth systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated successfully
.
:
```

5. */var/log/boot.log*

  - *Explanation*: Captures messages related to system boot processes, including the startup of various services.

```
(END)
```

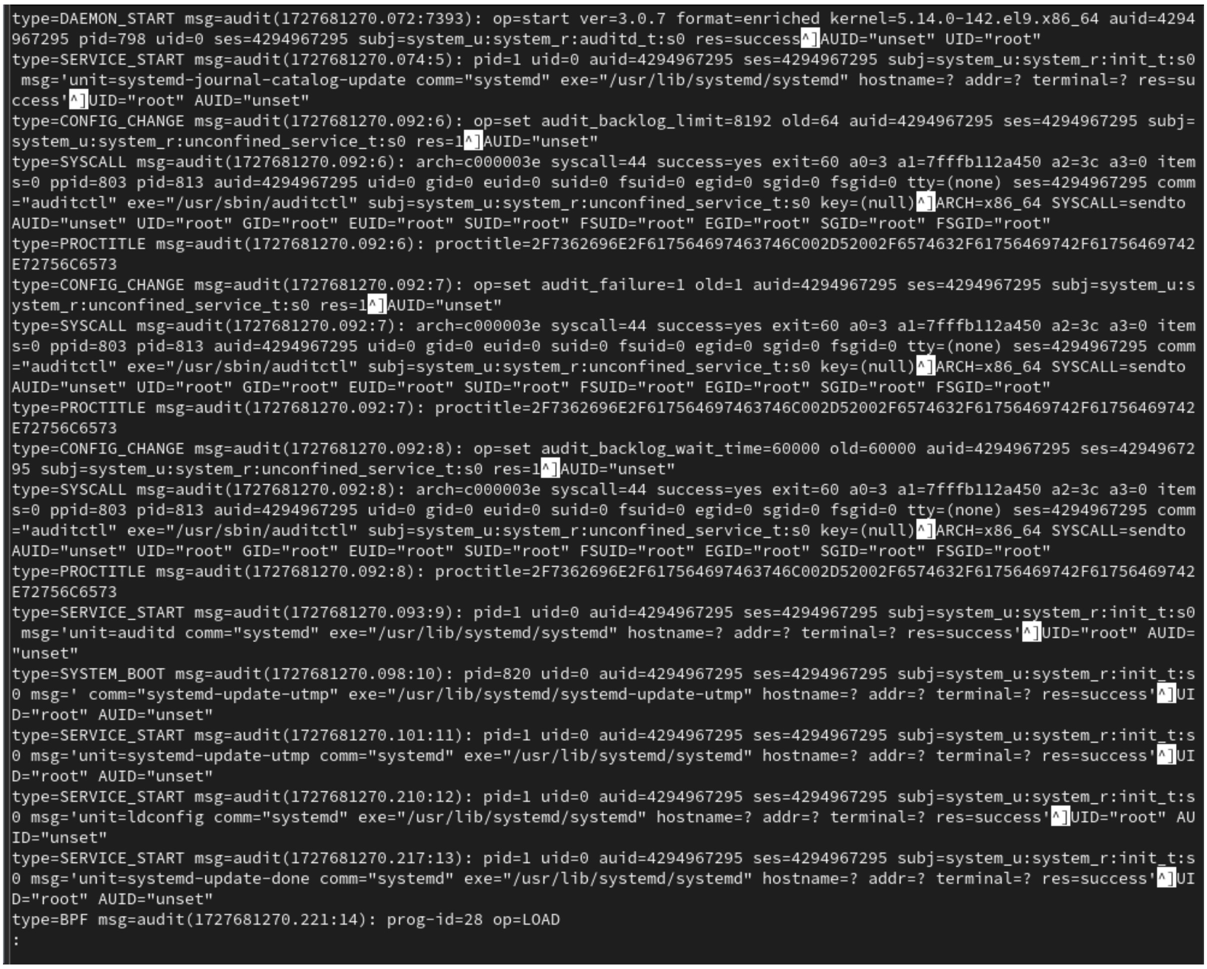
6. */var/log/yum.log*

  - *Explanation*: Tracks package installation, updates, and removal activities performed using the YUM package manager.

LOGS

7. */var/log/audit/audit.log*

  - *Explanation*: Stores audit logs generated by the Linux Auditing System, which is used for security auditing and monitoring.



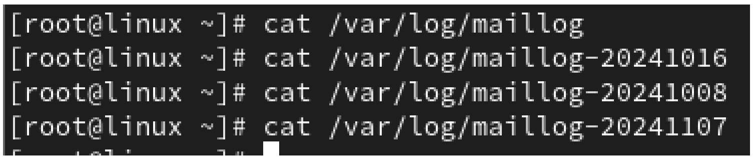
```
type=DAEMON_START msg=audit(1727681270.072:7393): op=start ver=3.0.7 format=enriched kernel=5.14.0-142.el9.x86_64 auid=4294
967295 pid=798 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=success^]AUID="unset" UID="root"
type=SERVICE_START msg=audit(1727681270.074:5): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
 msg='unit=systemd-journal-catalog-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=su
ccess'^]UID="root" AUID="unset"
type=CONFIG_CHANGE msg=audit(1727681270.092:6): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=
system_u:system_r:unconfined_service_t:s0 res=1^]AUID="unset"
type=SYSCALL msg=audit(1727681270.092:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fffb112a450 a2=3c a3=0 item
s=0 ppid=803 pid=813 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm
="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)^]ARCH=x86_64 SYSCALL=sendto
AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1727681270.092:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742
E72756C6573
type=CONFIG_CHANGE msg=audit(1727681270.092:7): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=system_u:s
ystem_r:unconfined_service_t:s0 res=1^]AUID="unset"
type=SYSCALL msg=audit(1727681270.092:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fffb112a450 a2=3c a3=0 item
s=0 ppid=803 pid=813 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm
="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)^]ARCH=x86_64 SYSCALL=sendto
AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1727681270.092:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742
E72756C6573
type=CONFIG_CHANGE msg=audit(1727681270.092:8): op=set audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=42949672
95 subj=system_u:system_r:unconfined_service_t:s0 res=1^]AUID="unset"
type=SYSCALL msg=audit(1727681270.092:8): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fffb112a450 a2=3c a3=0 item
s=0 ppid=803 pid=813 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm
="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)^]ARCH=x86_64 SYSCALL=sendto
AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1727681270.092:8): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742
E72756C6573
type=SERVICE_START msg=audit(1727681270.093:9): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'^]UID="root" AUID=
"unset"
type=SYSTEM_BOOT msg=audit(1727681270.098:10): pid=820 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg=' comm="systemd-update-utmp" exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success'^]UI
D="root" AUID="unset"
type=SERVICE_START msg=audit(1727681270.101:11): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=systemd-update-utmp comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'^]UI
D="root" AUID="unset"
type=SERVICE_START msg=audit(1727681270.210:12): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=ldconfig comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'^]UID="root" AU
ID="unset"
type=SERVICE_START msg=audit(1727681270.217:13): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=systemd-update-done comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'^]UI
D="root" AUID="unset"
type=BPF msg=audit(1727681270.221:14): prog-id=28 op=LOAD
:
```

8. */var/log/httpd/*

   - *Explanation*: Directory containing log files for the Apache web server, including access logs and error logs.

9. */var/log/maillog*

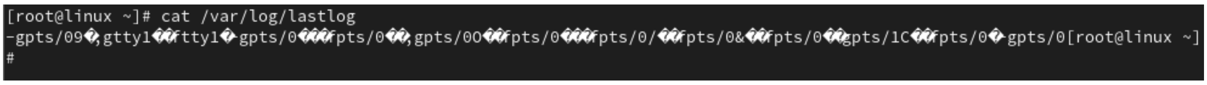
   - *Explanation*: Logs related to the mail server, including messages sent and received, errors, and other mail server activities.



```
[root@linux ~]# cat /var/log/maillog
[root@linux ~]# cat /var/log/maillog-20241016
[root@linux ~]# cat /var/log/maillog-20241008
[root@linux ~]# cat /var/log/maillog-20241107
```

10. */var/log/lastlog*

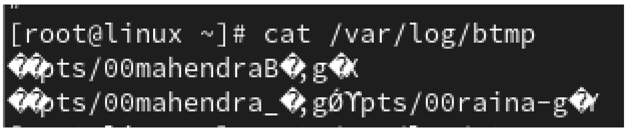
- *Explanation*: Records the last login time of each user. It is not a regular text file but can be viewed using the lastlog command.



```
[root@linux ~]# cat /var/log/lastlog
-gpts/09�,gtty1��ftty1�-gpts/0���fpts/0��,gpts/0O��fpts/0���fpts/0/��fpts/0&��fpts/0��gpts/1C��fpts/0�-gpts/0[root@linux ~]
#
```

11. */var/log/btmp*

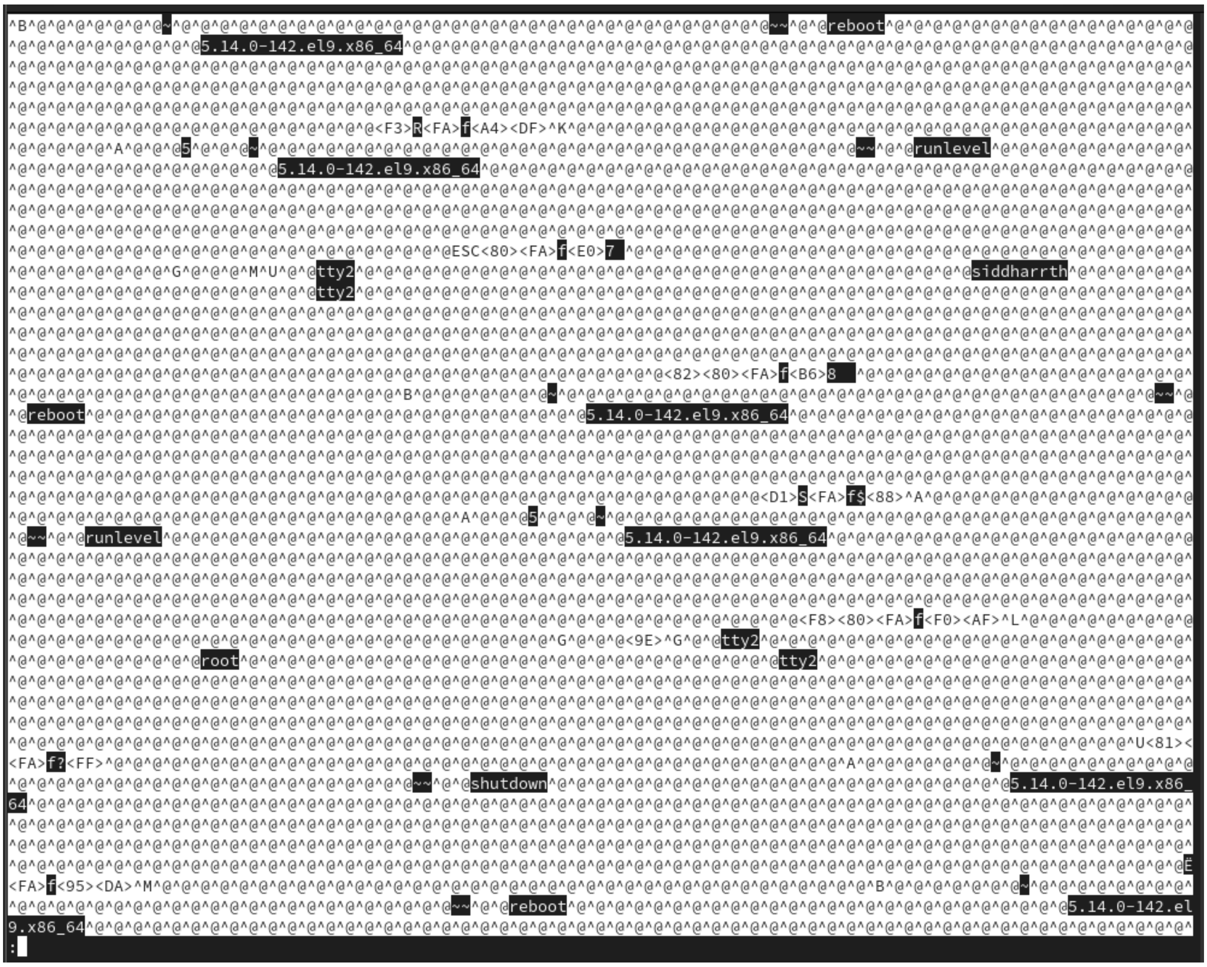
- *Explanation*: Records failed login attempts. Like lastlog, this is a binary file and can be viewed using the lastb command.



```
[root@linux ~]# cat /var/log/btmp
��pts/00mahendraB�,g�X
��pts/00mahendra_�,g0Ypts/00raina-g�Y
```

12. */var/log/wtmp*

- *Explanation*: Records login and logout events. This binary file can be viewed using the last command.



```
^B^@^@^@^@^@^@^@~^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@~~^@^@reboot^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@5.14.0-142.el9.x86_64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<F3>R<FA>f<A4><DF>^K^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^A^@^@^@5^@^@^@~^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@~~^@^@runlevel^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@5.14.0-142.el9.x86_64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@ESC<80><FA>f<E0>7 ^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^G^@^@^@^M^U^@^@tty2^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@siddharrth^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@tty2^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<82><80><FA>f<B6>8  ^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^B^@^@^@^@^@^@^@~^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@~~^@
^@reboot^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@5.14.0-142.el9.x86_64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<D1>S<FA>f$<88>^A^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^A^@^@^@5^@^@^@~^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@~~^@^@runlevel^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@5.14.0-142.el9.x86_64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<F8><80><FA>f<F0><AF>^L^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^G^@^@^@<9E>^G^@^@tty2^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@root^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@tty2^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^U<81><
<FA>f?<FF>^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^A^@^@^@^@^@^@^@~^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@~~^@^@shutdown^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@5.14.0-142.el9.x86_
64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@Ë
<FA>f<95><DA>^M^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^B^@^@^@^@^@^@^@~^@^@^@^@^@^@^@^@^
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@~~^@^@reboot^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@5.14.0-142.el
9.x86_64^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
:
```

These logs provide valuable information for monitoring system performance, identifying issues, and ensuring security. Regularly reviewing these logs can help maintain the health and security of a CentOS Linux system.