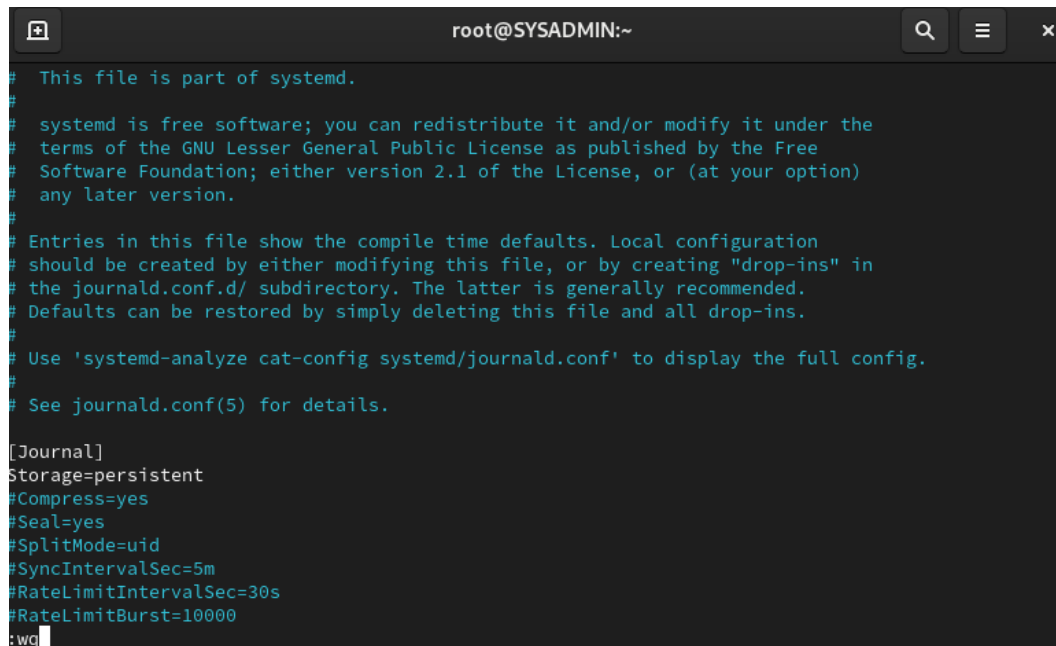Question 1:

```
[root@SYSADMIN ~]# mkdir -p /var/log/journal
[root@SYSADMIN ~]#
```

```
[root@SYSADMIN ~]# vim /etc/systemd//journald.conf
```

Changing the default to permissive mode by editing /etc/systemd/journald.conf

```
root@SYSADMIN:~

#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the journald.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config.
#
# See journald.conf(5) for details.

[Journal]
Storage=persistent
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
:wq
```

Question 2:

```
[root@SYSADMIN ~]# journalctl -u sshd -p debug
Aug 12 13:07:47 SYSADMIN systemd[1]: Starting OpenSSH server daemon...
Aug 12 13:07:49 SYSADMIN sshd[929]: Server listening on 0.0.0.0 port 22.
Aug 12 13:07:49 SYSADMIN sshd[929]: Server listening on :: port 22.
Aug 12 13:07:49 SYSADMIN systemd[1]: Started OpenSSH server daemon.
[root@SYSADMIN ~]#
```

Question 3:

```
[nadasamir@SYSADMIN ~]$ cat /var/log/boot.log
cat: /var/log/boot.log: Permission denied
[nadasamir@SYSADMIN ~]$ sudo cat /var/log/boot.log
[sudo] password for nadasamir:
------------ Sun Aug 13 09:19:37 EET 2023 ------------
[  OK  ] Started Show Plymouth Boot Screen.
[  OK  ] Started Forward Password R…s to Plymouth Directory Watch.
[  OK  ] Reached target Path Units.
         Starting D-Bus System Message Bus...
[  OK  ] Found device /dev/mapper/cs_192-root.
[  OK  ] Reached target Initrd Root Device.
[  OK  ] Started D-Bus System Message Bus.
[  OK  ] Found device /dev/mapper/cs_192-swap.
         Starting Resume from hibernation using device /dev/mapper/cs_192-swap..
.
[  OK  ] Finished Resume from hibernation using device /dev/mapper/cs_192-swap.
[  OK  ] Reached target Preparation for Local File Systems.
[  OK  ] Reached target Local File Systems.
[  OK  ] Reached target System Initialization.
[  OK  ] Reached target Basic System.
[  OK  ] Finished dracut initqueue hook.
[  OK  ] Reached target Preparation for Remote File Systems.
[  OK  ] Reached target Remote File Systems.
         Starting File System Check on /dev/mapper/cs_192-root...
```

Question 4:

```
[nadasamir@SYSADMIN ~]$ journalctl -u sshd
Aug 13 09:19:45 SYSADMIN systemd[1]: Starting OpenSSH server daemon...
Aug 13 09:19:45 SYSADMIN sshd[920]: Server listening on 0.0.0.0 port 22.
Aug 13 09:19:45 SYSADMIN sshd[920]: Server listening on :: port 22.
Aug 13 09:19:45 SYSADMIN systemd[1]: Started OpenSSH server daemon.
[nadasamir@SYSADMIN ~]$
```

Question 5

```
[nadasamir@SYSADMIN ~]$ journalctl _PID=1
Aug 13 09:19:15 localhost systemd[1]: Starting Create Volatile Files and Direct▷
Aug 13 09:19:15 localhost systemd[1]: Finished Load Kernel Modules.
Aug 13 09:19:15 localhost systemd[1]: Starting Apply Kernel Variables...
Aug 13 09:19:15 localhost systemd[1]: Finished Apply Kernel Variables.
Aug 13 09:19:15 localhost systemd[1]: Finished Create Volatile Files and Direct▷
Aug 13 09:19:15 localhost systemd[1]: Finished dracut cmdline hook.
Aug 13 09:19:15 localhost systemd[1]: Starting dracut pre-udev hook...
Aug 13 09:19:15 localhost systemd[1]: Finished dracut pre-udev hook.
Aug 13 09:19:15 localhost systemd[1]: Starting Rule-based Manager for Device Ev▷
Aug 13 09:19:15 localhost systemd[1]: Started Rule-based Manager for Device Eve▷
Aug 13 09:19:15 localhost systemd[1]: dracut pre-trigger hook was skipped becau▷
Aug 13 09:19:15 localhost systemd[1]: Starting Coldplug All udev Devices...
Aug 13 09:19:17 localhost systemd[1]: Finished Coldplug All udev Devices.
Aug 13 09:19:17 localhost systemd[1]: nm-initrd.service was skipped because of ▷
Aug 13 09:19:17 localhost systemd[1]: Reached target Network.
Aug 13 09:19:17 localhost systemd[1]: nm-wait-online-initrd.service was skipped▷
Aug 13 09:19:17 localhost systemd[1]: Starting dracut initqueue hook...
Aug 13 09:19:17 localhost systemd[1]: Starting Show Plymouth Boot Screen
```

Question 6:

```
[nadasamir@SYSADMIN ~]$ journalctl _UID=$(id -u nadasamir)
Aug 13 09:20:35 SYSADMIN systemd[2109]: Queued start job for default target Main User T▷
Aug 13 09:20:35 SYSADMIN systemd[2109]: Created slice User Application Slice.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Started Mark boot as successful after the user ▷
Aug 13 09:20:35 SYSADMIN systemd[2109]: Started Daily Cleanup of User's Temporary Direc▷
Aug 13 09:20:35 SYSADMIN systemd[2109]: Reached target Paths.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Reached target Timers.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Starting D-Bus User Message Bus Socket...
Aug 13 09:20:35 SYSADMIN systemd[2109]: Listening on PipeWire PulseAudio.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Listening on PipeWire Multimedia System Socket.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Starting Create User's Volatile Files and Direc▷
Aug 13 09:20:35 SYSADMIN systemd[2109]: Listening on D-Bus User Message Bus Socket.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Reached target Sockets.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Finished Create User's Volatile Files and Direc▷
Aug 13 09:20:35 SYSADMIN systemd[2109]: Reached target Basic System.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Reached target Main User Target.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Startup finished in 374ms.
Aug 13 09:20:35 SYSADMIN systemd[2109]: Starting D-Bus User Message Bus...
Aug 13 09:20:35 SYSADMIN systemd[2109]: Started D-Bus User Message Bus.
Aug 13 09:20:35 SYSADMIN dbus-broker-launch[2148]: Policy to allow eavesdropping in /us▷
Aug 13 09:20:35 SYSADMIN dbus-broker-launch[2148]: Policy to allow eavesdropping in /us▷
Aug 13 09:20:35 SYSADMIN dbus-broker-lau[2148]: Ready
```
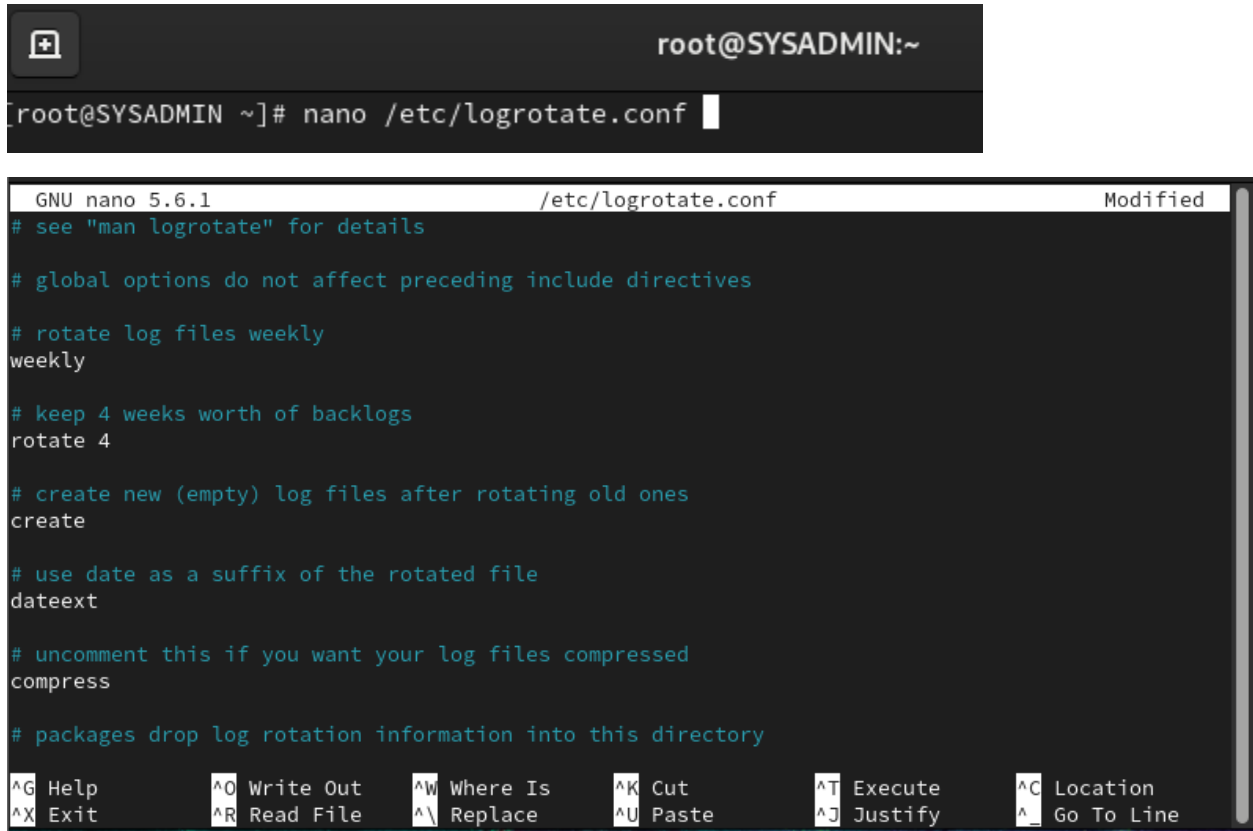
Question 7:

Error logs

```
[root@SYSADMIN ~]# grep -i error /var/log/messages
Aug 13 07:32:20 SYSADMIN dnf[3316]: Errors during downloading metadata for repository 'baseos':
Aug 13 07:32:20 SYSADMIN dnf[3316]:  - Curl error (6): Couldn't resolve host name for https://mi
rrors.centos.org/metalink?repo=centos-baseos-9-stream&arch=x86_64&protocol=https,http [Could not
 resolve host: mirrors.centos.org]
Aug 13 07:32:22 SYSADMIN dnf[3316]: Error: Failed to download metadata for repo 'baseos': Cannot
 prepare internal mirrorlist: Curl error (6): Couldn't resolve host name for https://mirrors.cen
tos.org/metalink?repo=centos-baseos-9-stream&arch=x86_64&protocol=https,http [Could not resolve
host: mirrors.centos.org]
Aug 13 08:10:24 SYSADMIN gnome-shell[2023]: libinput error: event2  - VirtualPS/2 VMware VMMouse
: client bug: event processing lagging behind by 126ms, your system is too slow
Aug 13 08:14:35 SYSADMIN cupsd[928]: REQUEST localhost - - "POST / HTTP/1.1" 200 188 Renew-Subsc
ription client-error-not-found
Aug 13 08:38:58 SYSADMIN gnome-shell[2023]: libinput error: event1  - AT Translated Set 2 keyboa
rd: client bug: event processing lagging behind by 22ms, your system is too slow
Aug 13 08:44:41 SYSADMIN gnome-shell[2023]: libinput error: event2  - VirtualPS/2 VMware VMMouse
: client bug: event processing lagging behind by 12ms, your system is too slow
Aug 13 09:12:56 SYSADMIN cupsd[928]: REQUEST localhost - - "POST / HTTP/1.1" 200 188 Renew-Subsc
ription client-error-not-found
Aug 13 09:19:39 SYSADMIN alsactl[822]: alsa-lib main.c:1541:(snd_use_case_mgr_open) error: faile
d to import hw:0 use case configuration -2
Aug 13 09:19:41 SYSADMIN journal[800]: Error probing device: Error sending ATA command IDENTIFY
```

logs with error severity

```
[nadasamir@SYSADMIN ~]$ journalctl -p err
Aug 13 09:19:17 localhost kernel: Warning: Unmaintained hardware is detected:  e1000:100F:8086 >
Aug 13 09:19:30 SYSADMIN kernel: piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
Aug 13 09:19:34 SYSADMIN kernel: Bluetooth: hci0: unexpected cc 0x0c12 length: 2 < 3
Aug 13 09:19:34 SYSADMIN kernel: Bluetooth: hci0: Opcode 0x c12 failed: -38
Aug 13 09:19:39 SYSADMIN alsactl[822]: alsa-lib main.c:1541:(snd_use_case_mgr_open) error: fail>
Aug 13 09:20:34 SYSADMIN gdm-password][2095]: gkr-pam: unable to locate daemon control file
Aug 13 09:20:46 SYSADMIN systemd[2109]: Failed to start Application launched by gnome-session-b>
Aug 13 09:20:46 SYSADMIN systemd[2109]: Failed to start Application launched by gnome-session-b>
Aug 13 09:20:47 SYSADMIN systemd[2109]: Failed to start Application launched by gnome-session-b>
Aug 13 09:20:47 SYSADMIN gdm-wayland-session[1486]: GLib: Source ID 2 was not found when attemp>
Aug 13 09:20:47 SYSADMIN systemd[2109]: Failed to start Application launched by gnome-session-b>
Aug 13 09:20:48 SYSADMIN gdm-launch-environment][1153]: GLib-GObject: g_object_unref: assertion>
Aug 13 09:20:50 SYSADMIN systemd[2109]: Failed to start GNOME subscription management service.
Aug 13 09:20:55 SYSADMIN systemd[2109]: Failed to start GNOME subscription management service.
Aug 13 09:20:58 SYSADMIN systemd[2109]: Failed to start GNOME subscription management service.
```

Question 8:

Editing in the file /etc/logrotate.conf uncommenting compress


```
[root@SYSADMIN ~]# nano /etc/logrotate.conf
```

```
  GNU nano 5.6.1                        /etc/logrotate.conf                        Modified
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
compress

# packages drop log rotation information into this directory

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^_ Go To Line
```