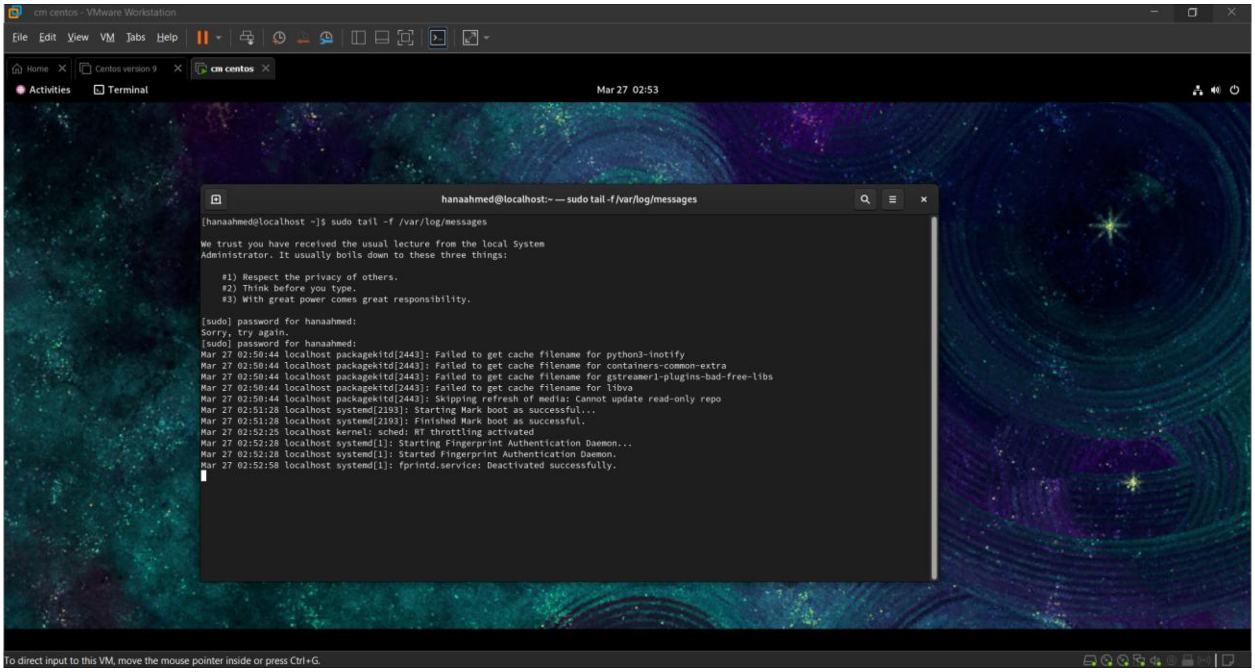
1. What Different Between Rsyslog and Jornald?
   Rsyslog: saved as txt file-saved on ram (/run)-could use UDP/TCP to connect
   Journald: saved as binary files-saved on hard disk (/var/log/)-local only

---

2. What are the main configuration files for Rsyslog?
   /etc/rsyslog.conf

---

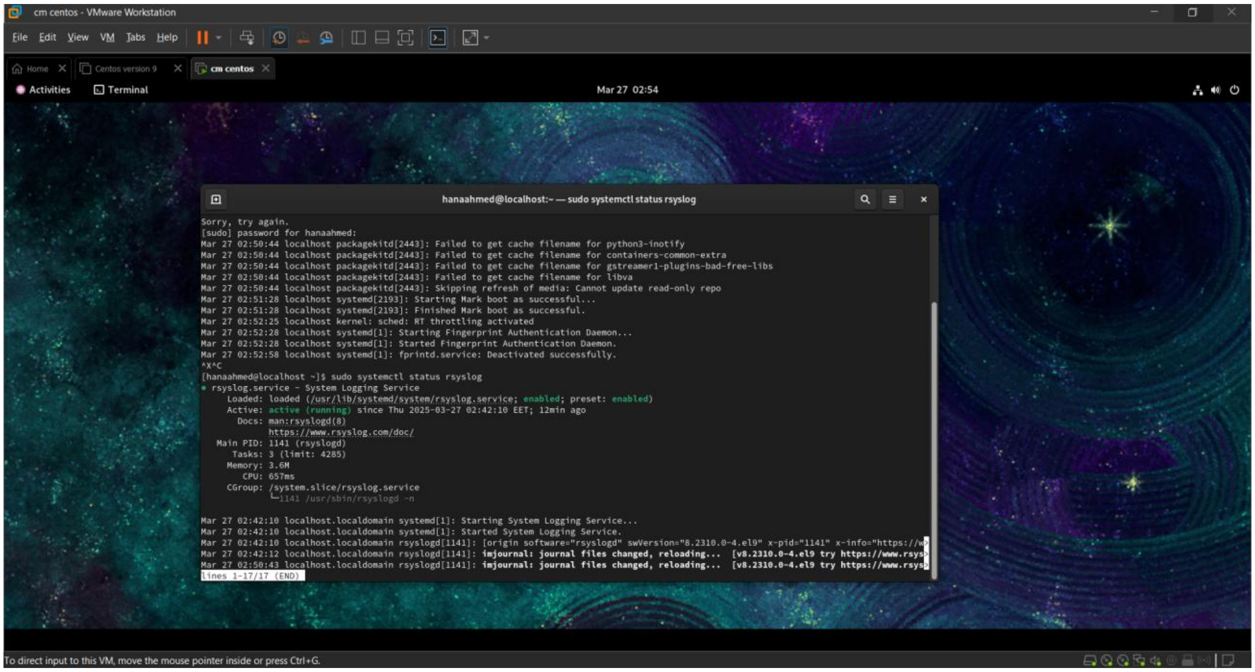
3. How do you view system logs in real time?


cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 02:53
hanaahmed@localhost:~ — sudo tail -f /var/log/messages
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
[hanaahmed@localhost ~]$ sudo tail -f /var/log/messages

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for hanaahmed:
Sorry, try again.
[sudo] password for hanaahmed:
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for python3-inotify
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for containers-common-extra
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for gstreamer1-plugins-bad-free-libs
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for libva
Mar 27 02:50:44 localhost packagekitd[2443]: Skipping refresh of media: Cannot update read-only repo
Mar 27 02:51:28 localhost systemd[2193]: Starting Mark boot as successful...
Mar 27 02:51:28 localhost systemd[2193]: Finished Mark boot as successful.
Mar 27 02:52:25 localhost kernel: sched: RT throttling activated
Mar 27 02:52:28 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Mar 27 02:52:28 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Mar 27 02:52:58 localhost systemd[1]: fprintd.service: Deactivated successfully.
```

---

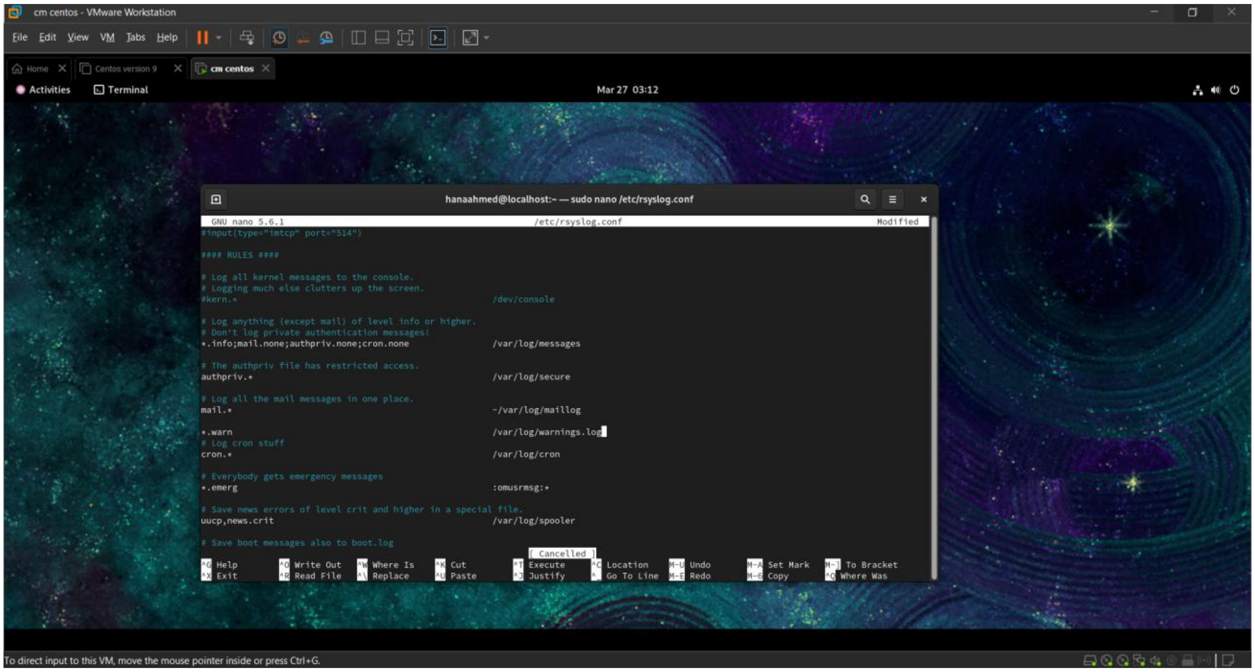
4. How do you test if Rsyslog is working properly after making changes?


cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 02:54
hanaahmed@localhost:~ — sudo systemctl status rsyslog
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Sorry, try again.
[sudo] password for hanaahmed:
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for python3-inotify
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for containers-common-extra
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for gstreamer1-plugins-bad-free-libs
Mar 27 02:50:44 localhost packagekitd[2443]: Failed to get cache filename for libva
Mar 27 02:50:44 localhost packagekitd[2443]: Skipping refresh of media: Cannot update read-only repo
Mar 27 02:51:28 localhost systemd[2193]: Starting Mark boot as successful...
Mar 27 02:51:28 localhost systemd[2193]: Finished Mark boot as successful.
Mar 27 02:52:25 localhost kernel: sched: RT throttling activated
Mar 27 02:52:28 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Mar 27 02:52:28 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Mar 27 02:52:58 localhost systemd[1]: fprintd.service: Deactivated successfully.
^X^C
[hanaahmed@localhost ~]$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-27 02:42:10 EET; 12min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 1141 (rsyslogd)
      Tasks: 3 (limit: 4285)
     Memory: 3.6M
        CPU: 657ms
     CGroup: /system.slice/rsyslog.service
             └─1141 /usr/sbin/rsyslogd -n

Mar 27 02:42:10 localhost.localdomain systemd[1]: Starting System Logging Service...
Mar 27 02:42:10 localhost.localdomain systemd[1]: Started System Logging Service.
Mar 27 02:42:10 localhost.localdomain rsyslogd[1141]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1141" x-info="https://w>
Mar 27 02:42:12 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try https://www.rsys>
Mar 27 02:50:43 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try https://www.rsys>
lines 1-17/17 (END)
```

---

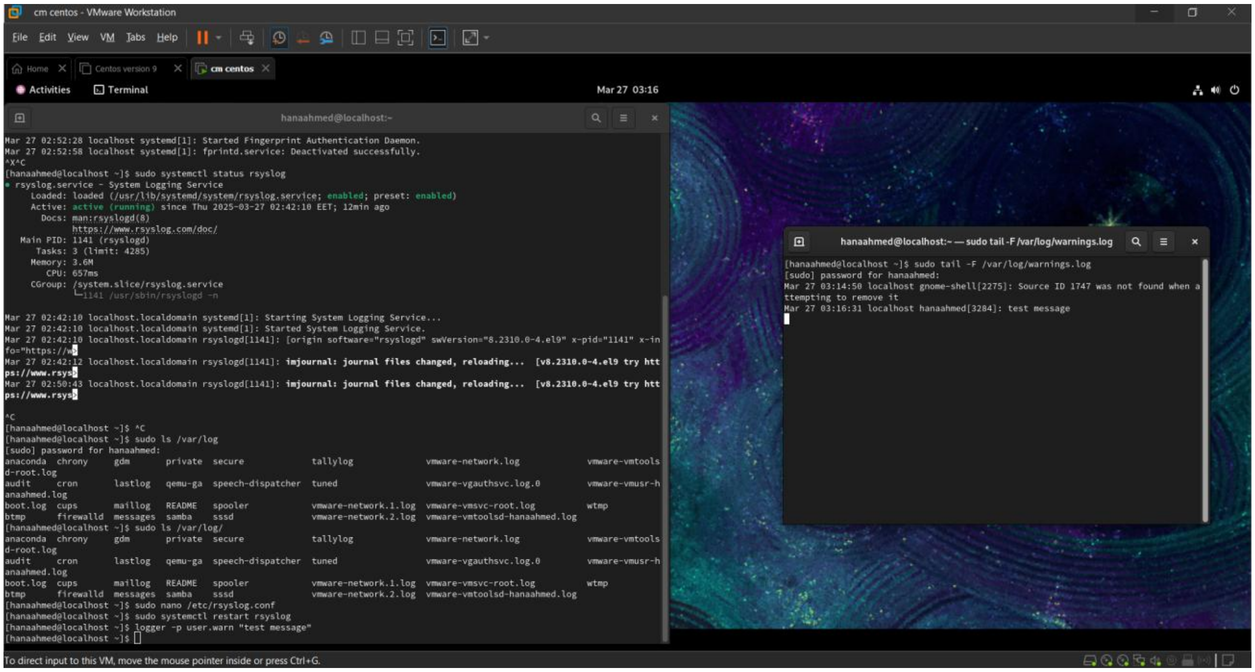
5. You need to configure Rsyslog to log messages from any facility with severity warning and above to a file located at /var/log/warnings.log.


cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 03:12
hanaahmed@localhost:~ — sudo nano /etc/rsyslog.conf
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
  GNU nano 5.6.1                      /etc/rsyslog.conf                                Modified
#input(type="imtcp" port="514")

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog

*.warn                                                  /var/log/warnings.log
# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
                                                     [ Cancelled ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^_ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

[hanaahmed@localhost ~]$ sudo nano /etc/rsyslog.conf

[hanaahmed@localhost ~]$ sudo systemctl restart rsyslog

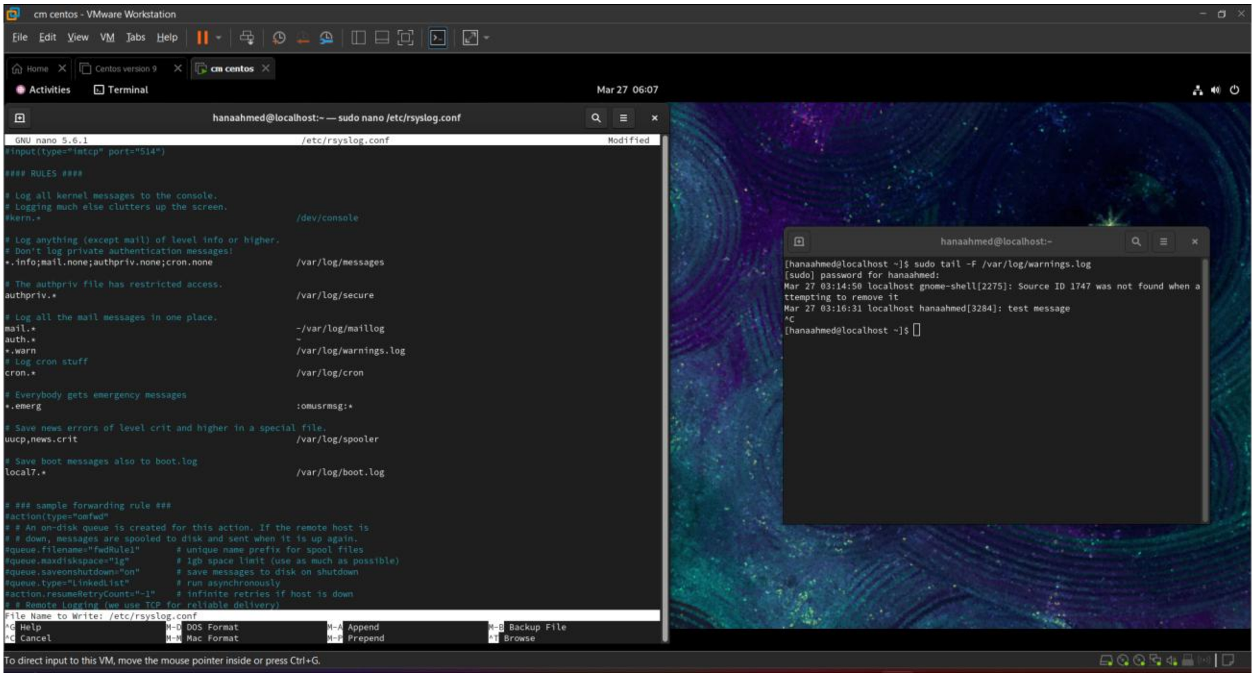

cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 03:16
hanaahmed@localhost:~
hanaahmed@localhost:~ — sudo tail -F /var/log/warnings.log
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Mar 27 02:52:28 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Mar 27 02:52:58 localhost systemd[1]: fprintd.service: Deactivated successfully.
^X^C
[hanaahmed@localhost ~]$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-27 02:42:10 EET; 12min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 1141 (rsyslogd)
      Tasks: 3 (limit: 4285)
     Memory: 3.6M
        CPU: 657ms
     CGroup: /system.slice/rsyslog.service
             └─1141 /usr/sbin/rsyslogd -n

Mar 27 02:42:10 localhost.localdomain systemd[1]: Starting System Logging Service...
Mar 27 02:42:10 localhost.localdomain systemd[1]: Started System Logging Service.
Mar 27 02:42:10 localhost.localdomain rsyslogd[1141]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1141" x-in
fo="https://w>
Mar 27 02:42:12 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try htt
ps://www.rsys>
Mar 27 02:50:43 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try htt
ps://www.rsys>

^C
[hanaahmed@localhost ~]$ ^C
[hanaahmed@localhost ~]$ sudo ls /var/log
[sudo] password for hanaahmed:
anaconda  chrony     gdm       private  secure            tallylog              vmware-network.log          vmware-vmtools
d-root.log
audit     cron       lastlog   qemu-ga  speech-dispatcher  tuned                vmware-vgauthsvc.log.0      vmware-vmusr-h
anaahmed.log
boot.log  cups       maillog   README   spooler           vmware-network.1.log  vmware-vmsvc-root.log       wtmp
btmp      firewalld  messages  samba    sssd              vmware-network.2.log  vmware-vmtoolsd-hanaahmed.log
[hanaahmed@localhost ~]$ sudo ls /var/log/
anaconda  chrony     gdm       private  secure            tallylog              vmware-network.log          vmware-vmtools
d-root.log
audit     cron       lastlog   qemu-ga  speech-dispatcher  tuned                vmware-vgauthsvc.log.0      vmware-vmusr-h
anaahmed.log
boot.log  cups       maillog   README   spooler           vmware-network.1.log  vmware-vmsvc-root.log       wtmp
btmp      firewalld  messages  samba    sssd              vmware-network.2.log  vmware-vmtoolsd-hanaahmed.log
[hanaahmed@localhost ~]$ sudo nano /etc/rsyslog.conf
[hanaahmed@localhost ~]$ sudo systemctl restart rsyslog
[hanaahmed@localhost ~]$ logger -p user.warn "test message"
[hanaahmed@localhost ~]$ 
```

```
[hanaahmed@localhost ~]$ sudo tail -F /var/log/warnings.log
[sudo] password for hanaahmed:
Mar 27 03:14:50 localhost gnome-shell[2275]: Source ID 1747 was not found when a
ttempting to remove it
Mar 27 03:16:31 localhost hanaahmed[3284]: test message
```

----

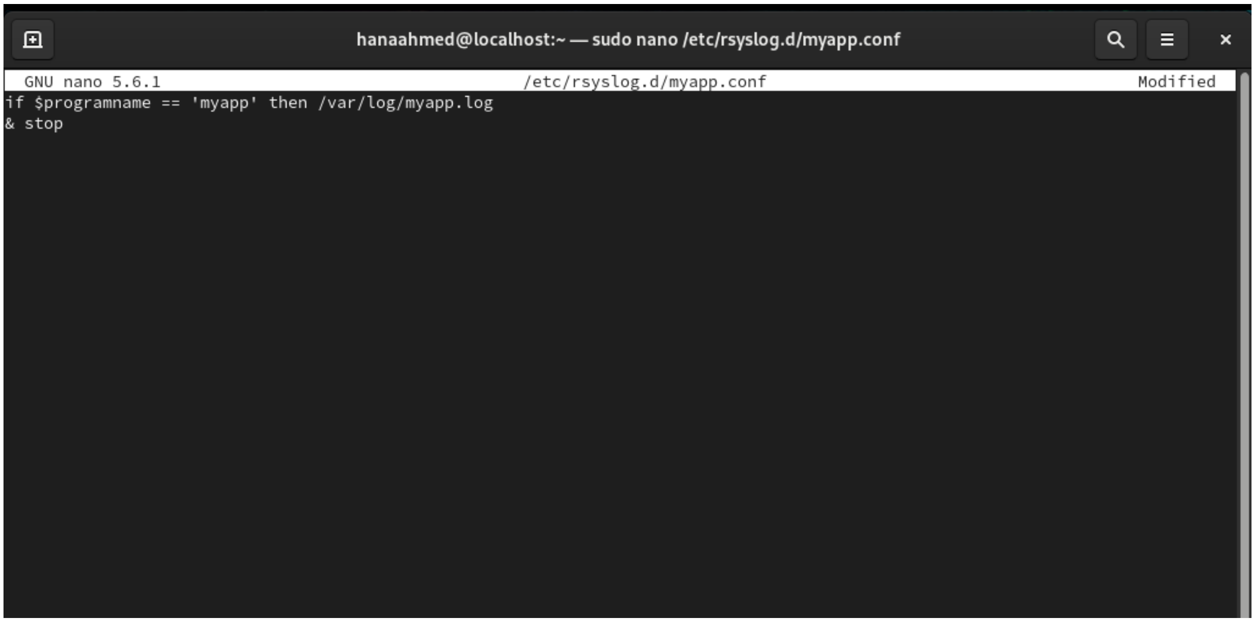
6. How can you configure Rsyslog to discard log messages discard logs from a specific facility (e.g., auth)


cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 06:07
hanaahmed@localhost:~ — sudo nano /etc/rsyslog.conf
hanaahmed@localhost:~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

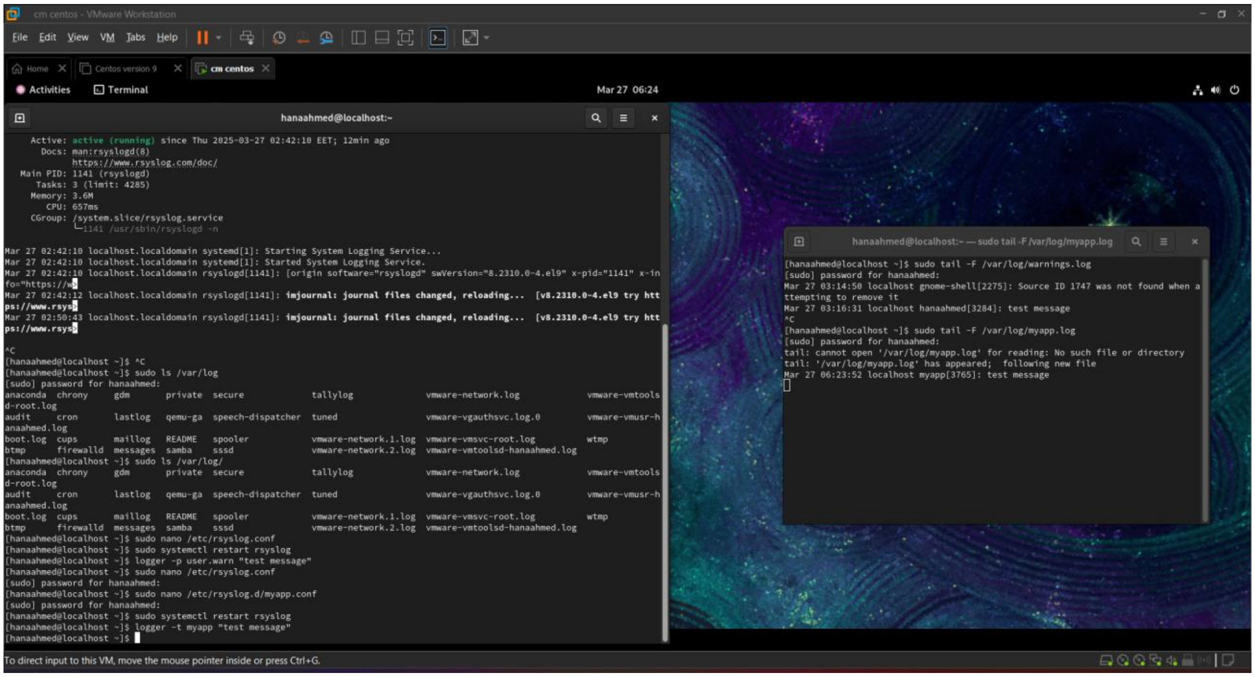
```
  GNU nano 5.6.1                              /etc/rsyslog.conf                              Modified
#input(type="imtcp" port="514")

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog
auth.*                                                  ~
*.warn                                                  /var/log/warnings.log
# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### sample forwarding rule ###
#action(type="omfwd"
# # An on-disk queue is created for this action. If the remote host is
# # down, messages are spooled to disk and sent when it is up again.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# # Remote Logging (we use TCP for reliable delivery)
File Name to Write: /etc/rsyslog.conf
^G Help              M-D DOS Format         M-A Append            M-B Backup File
^C Cancel            M-M Mac Format         M-P Prepend           ^T Browse
```

```
[hanaahmed@localhost ~]$ sudo tail -F /var/log/warnings.log
[sudo] password for hanaahmed:
Mar 27 03:14:50 localhost gnome-shell[2275]: Source ID 1747 was not found when a
ttempting to remove it
Mar 27 03:16:31 localhost hanaahmed[3284]: test message
^C
[hanaahmed@localhost ~]$ 
```

7. How do you configure Rsyslog to log messages from a specific application to a custom log file?



```
  GNU nano 5.6.1                          /etc/rsyslog.d/myapp.conf                                    Modified
if $programname == 'myapp' then /var/log/myapp.log
& stop
```



cm centos - VMware Workstation
File Edit View VM Tabs Help
Home
Centos version 9
cm centos
Activities
Terminal
Mar 27 06:24
hanaahmed@localhost:~
hanaahmed@localhost:~ — sudo tail -F /var/log/myapp.log
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
     Active: active (running) since Thu 2025-03-27 02:42:10 EET; 12min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 1141 (rsyslogd)
      Tasks: 3 (limit: 4285)
     Memory: 3.6M
        CPU: 657ms
     CGroup: /system.slice/rsyslog.service
             └─1141 /usr/sbin/rsyslogd -n

Mar 27 02:42:10 localhost.localdomain systemd[1]: Starting System Logging Service...
Mar 27 02:42:10 localhost.localdomain systemd[1]: Started System Logging Service.
Mar 27 02:42:10 localhost.localdomain rsyslogd[1141]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1141" x-in
fo="https://w>
Mar 27 02:42:12 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try htt
ps://www.rsys>
Mar 27 02:50:43 localhost.localdomain rsyslogd[1141]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try htt
ps://www.rsys>

^C
[hanaahmed@localhost ~]$ ^C
[hanaahmed@localhost ~]$ sudo ls /var/log
[sudo] password for hanaahmed:
anaconda  chrony     gdm       private  secure            tallylog            vmware-network.log          vmware-vmtools
d-root.log
audit     cron       lastlog   qemu-ga  speech-dispatcher  tuned               vmware-vgauthsvc.log.0      vmware-vmusr-h
anaahmed.log
boot.log  cups       maillog   README   spooler           vmware-network.1.log  vmware-vmsvc-root.log     wtmp
btmp      firewalld  messages  samba    sssd              vmware-network.2.log  vmware-vmtoolsd-hanaahmed.log
[hanaahmed@localhost ~]$ sudo ls /var/log/
anaconda  chrony     gdm       private  secure            tallylog            vmware-network.log          vmware-vmtools
d-root.log
audit     cron       lastlog   qemu-ga  speech-dispatcher  tuned               vmware-vgauthsvc.log.0      vmware-vmusr-h
anaahmed.log
boot.log  cups       maillog   README   spooler           vmware-network.1.log  vmware-vmsvc-root.log     wtmp
btmp      firewalld  messages  samba    sssd              vmware-network.2.log  vmware-vmtoolsd-hanaahmed.log
[hanaahmed@localhost ~]$ sudo nano /etc/rsyslog.conf
[hanaahmed@localhost ~]$ sudo systemctl restart rsyslog
[hanaahmed@localhost ~]$ logger -p user.warn "test message"
[hanaahmed@localhost ~]$ sudo nano /etc/rsyslog.conf
[sudo] password for hanaahmed:
[hanaahmed@localhost ~]$ sudo nano /etc/rsyslog.d/myapp.conf
[sudo] password for hanaahmed:
[hanaahmed@localhost ~]$ sudo systemctl restart rsyslog
[hanaahmed@localhost ~]$ logger -t myapp "test message"
[hanaahmed@localhost ~]$ 
```

```
[hanaahmed@localhost ~]$ sudo tail -F /var/log/warnings.log
[sudo] password for hanaahmed:
Mar 27 03:14:50 localhost gnome-shell[2275]: Source ID 1747 was not found when a
ttempting to remove it
Mar 27 03:16:31 localhost hanaahmed[3284]: test message
^C
[hanaahmed@localhost ~]$ sudo tail -F /var/log/myapp.log
[sudo] password for hanaahmed:
tail: cannot open '/var/log/myapp.log' for reading: No such file or directory
tail: '/var/log/myapp.log' has appeared;  following new file
Mar 27 06:23:52 localhost myapp[3765]: test message
```

----

8. How do you schedule a task to run a script at 5:30 PM tomorrow using the AT command?

echo "echo "Task 0"" | at 17:30 tomorrow

----

9. How do you schedule a task to run at midnight tonight?

```
echo "echo "Task 1"" | at midnight
```

----

10. How do you schedule a task to run 10 minutes from now?

```
echo "echo "Task 2"" | at now + 10 minutes
```

----

11. How do you list all scheduled tasks using the AT command?

```
atq
```

----

12. How do you cancel a scheduled task using the AT command?

```
atrm 1
```

```
at -r 1
```

----

13. How would you view the contents of a scheduled at job?

```
At -c 3
```
