1. What Different Between Rsyslog and Jornald?

- **Rsyslog:** A traditional syslog daemon with high-performance logging, advanced filtering, and remote logging capabilities.
- **Journald:** Part of systemd, it provides structured logging, binary logs, and integrates with systemctl for viewing logs.

2. What are the main configuration files for Rsyslog?

/etc/rsyslog.conf

```
[moe404@localhost ~]$ ls /etc/rsyslog.conf
/etc/rsyslog.conf
[moe404@localhost ~]$
```

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

```
[moe404@localhost ~]$ journalctl -f
Mar 28 15:05:14 localhost.localdomain systemd[1]: Started Fingerprint Authentication Daemon.
Mar 28 15:05:27 localhost.localdomain sudo[3371]: pam_unix(sudo:session): session closed for user root
Mar 28 15:05:31 localhost.localdomain sudo[3428]:   moe404 : TTY=pts/0 ; PWD=/home/moe404 ; USER=root ;
COMMAND=/bin/tail -F /var/log/messages
Mar 28 15:05:31 localhost.localdomain sudo[3428]: pam_unix(sudo:session): session opened for user root(u
id=0) by moe404(uid=1000)
Mar 28 15:05:31 localhost.localdomain rsyslogd[1144]: imjournal: journal files changed, reloading...  [v
8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Mar 28 15:05:37 localhost.localdomain unix_chkpwd[3432]: password check failed for user (moe404)
Mar 28 15:05:44 localhost.localdomain systemd[1]: fprintd.service: Deactivated successfully.
Mar 28 15:06:00 localhost.localdomain sudo[3428]: pam_unix(sudo:session): session closed for user root
Mar 28 15:06:18 localhost.localdomain unix_chkpwd[3442]: password check failed for user (moe404)
Mar 28 15:06:21 localhost.localdomain sudo[3412]:   moe404 : 3 incorrect password attempts ; TTY=pts/1 ;
 PWD=/home/moe404 ; USER=root ; COMMAND=/bin/su root
```

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

```
[moe404@localhost ~]$ sudo systemctl restart rsyslog
[moe404@localhost ~]$ logger "Test message"
[moe404@localhost ~]$ sudo tail -n 5 /var/log/messages
Mar 28 15:12:33 localhost systemd[1]: Starting System Logging Service...
Mar 28 15:12:33 localhost systemd[1]: Started System Logging Service.
Mar 28 15:12:33 localhost rsyslogd[3525]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="
3525" x-info="https://www.rsyslog.com"] start
Mar 28 15:12:33 localhost rsyslogd[3525]: imjournal: journal files changed, reloading...  [v8.2412.0-1.e
l9 try https://www.rsyslog.com/e/0 ]
Mar 28 15:12:47 localhost moe404[3533]: Test message
[moe404@localhost ~]$
```

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.

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

*.warn                                                  /var/log/warnings.log
```

```
[moe404@localhost ~]$ sudo nano /etc/rsyslog.conf
[moe404@localhost ~]$ sudo systemctl restart rsyslog
[moe404@localhost ~]$
```

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

```
mail.*                                                  -/va

auth.*                                                  ~
```

```
[moe404@localhost ~]$ sudo nano /etc/rsyslog.conf
[moe404@localhost ~]$ sudo systemctl restart rsyslog
[moe404@localhost ~]$
```

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

```
if $programname == 'myapp' then /var/log/myapp.log
```

```
[moe404@localhost ~]$ sudo nano /etc/rsyslog.conf
[moe404@localhost ~]$ sudo systemctl restart rsyslog
[moe404@localhost ~]$
```

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

```
[moe404@localhost ~]$ echo "script.sh" | at 17:30 tomorrow
warning: commands will be executed using /bin/sh
job 4 at Sat Mar 29 17:30:00 2025
```

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

```
[moe404@localhost ~]$ echo "script.sh" | at midnight
warning: commands will be executed using /bin/sh
job 5 at Sat Mar 29 00:00:00 2025
```

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

```
[moe404@localhost ~]$ echo "script.sh" | at now + 10 minutes
warning: commands will be executed using /bin/sh
job 6 at Fri Mar 28 15:40:00 2025
```

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

```
[moe404@localhost ~]$ atq
4       Sat Mar 29 17:30:00 2025 a moe404
5       Sat Mar 29 00:00:00 2025 a moe404
6       Fri Mar 28 15:40:00 2025 a moe404
```

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

```
[moe404@localhost ~]$ atrm 4 5
[moe404@localhost ~]$ atq
6       Fri Mar 28 15:40:00 2025 a moe404
[moe404@localhost ~]$
```

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

```
[moe404@localhost ~]$ at -c 6
#!/bin/sh
# atrun uid=1000 gid=1000
# mail moe404 0
umask 22
SHELL=/bin/bash; export SHELL
```