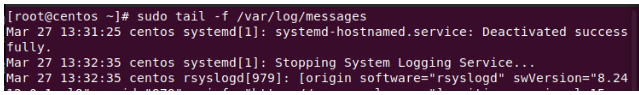
What Different Between Rsyslog and Jornald?

	rsyslog	journald
Log Format	Stores logs in Plain text (/var/log/)	Stores logs in Binary (needs journalctl to view)
Storage	Saves logs forever (if configured)	Loses logs after reboot (unless set to save)
Best For	Servers, long-term logs, remote logging	Debugging systemd services, fast searching
Commands	tail /var/log/syslog	journalctl -xe (view logs)

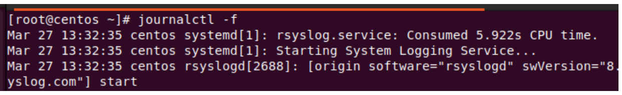
2. What are the main configuration files for Rsyslog?

/etc/rsyslog.conf	Main configuration file for Rsyslog. Defines rules for where logs are saved
/etc/rsyslog.d/50-default.conf	Default rules for common logs (like syslog, auth, kernel).
/etc/rsyslog.d/remote.conf	Used to send logs to another server
/etc/rsyslog.d/	Extra config files

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

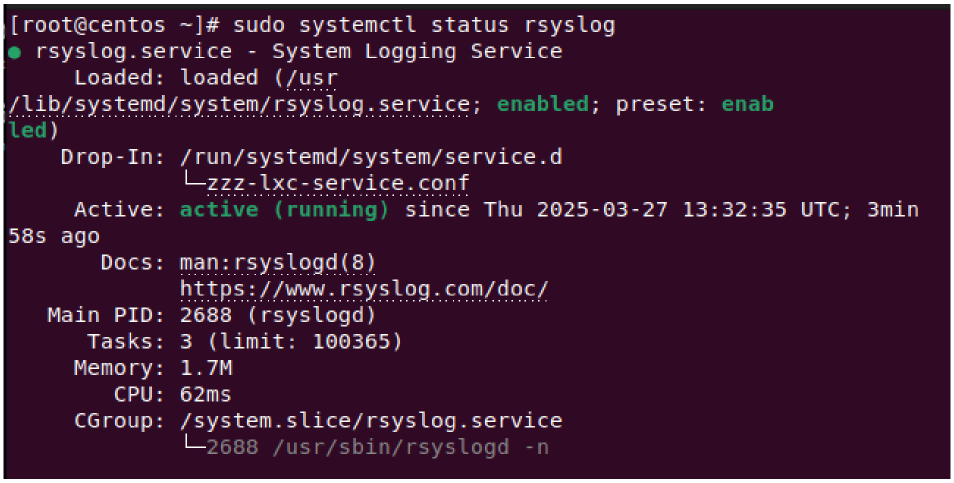


```
[root@centos ~]# sudo tail -f /var/log/messages
Mar 27 13:31:25 centos systemd[1]: systemd-hostnamed.service: Deactivated success
fully.
Mar 27 13:32:35 centos systemd[1]: Stopping System Logging Service...
Mar 27 13:32:35 centos rsyslogd[979]: [origin software="rsyslogd" swVersion="8.24
```



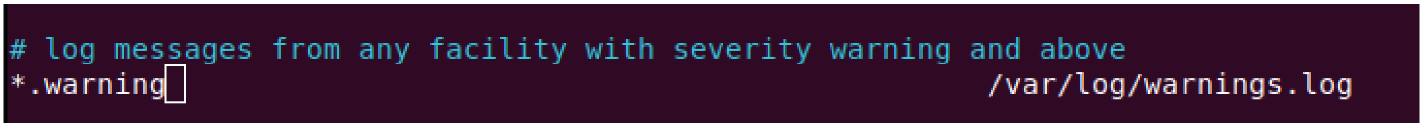
```
[root@centos ~]# journalctl -f
Mar 27 13:32:35 centos systemd[1]: rsyslog.service: Consumed 5.922s CPU time.
Mar 27 13:32:35 centos systemd[1]: Starting System Logging Service...
Mar 27 13:32:35 centos rsyslogd[2688]: [origin software="rsyslogd" swVersion="8.
yslog.com"] start
```

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

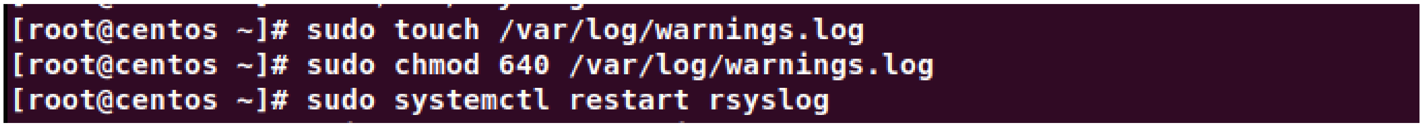


```
[root@centos ~]# sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr
/lib/systemd/system/rsyslog.service; enabled; preset: enab
led)
    Drop-In: /run/systemd/system/service.d
             └─zzz-lxc-service.conf
     Active: active (running) since Thu 2025-03-27 13:32:35 UTC; 3min
58s ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 2688 (rsyslogd)
      Tasks: 3 (limit: 100365)
     Memory: 1.7M
        CPU: 62ms
     CGroup: /system.slice/rsyslog.service
             └─2688 /usr/sbin/rsyslogd -n
```

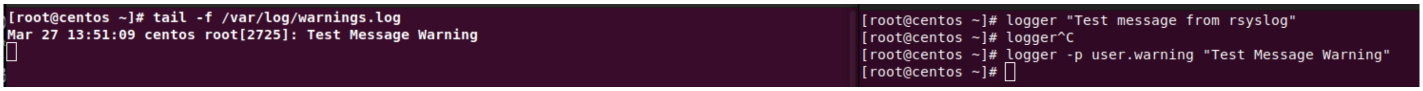
5. You need to configure Rsyslog to log messages from any facility with severity warning and above to a file located at /var/log/warnings.log.



```
# log messages from any facility with severity warning and above
*.warning                                                     /var/log/warnings.log
```



```
[root@centos ~]# sudo touch /var/log/warnings.log
[root@centos ~]# sudo chmod 640 /var/log/warnings.log
[root@centos ~]# sudo systemctl restart rsyslog
```

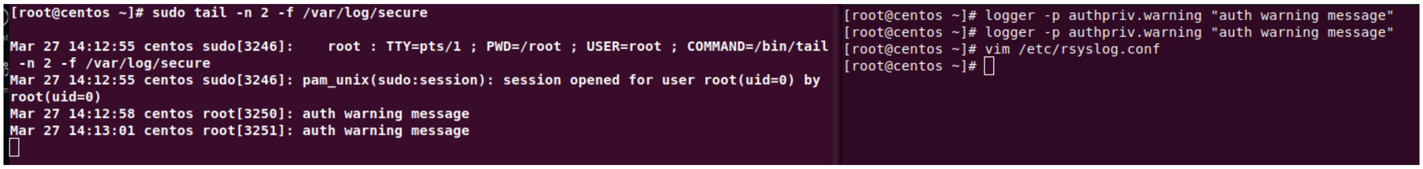


```
[root@centos ~]# tail -f /var/log/warnings.log
Mar 27 13:51:09 centos root[2725]: Test Message Warning
```

```
[root@centos ~]# logger "Test message from rsyslog"
[root@centos ~]# logger^C
[root@centos ~]# logger -p user.warning "Test Message Warning"
[root@centos ~]#
```

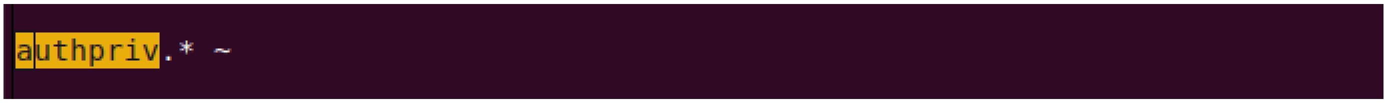
----

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

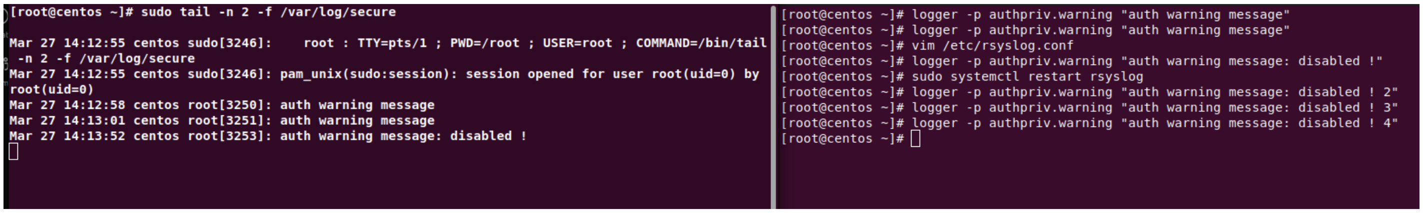


```
[root@centos ~]# sudo tail -n 2 -f /var/log/secure

Mar 27 14:12:55 centos sudo[3246]:    root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/bin/tail
 -n 2 -f /var/log/secure
Mar 27 14:12:55 centos sudo[3246]: pam_unix(sudo:session): session opened for user root(uid=0) by
root(uid=0)
Mar 27 14:12:58 centos root[3250]: auth warning message
Mar 27 14:13:01 centos root[3251]: auth warning message
```

```
[root@centos ~]# logger -p authpriv.warning "auth warning message"
[root@centos ~]# logger -p authpriv.warning "auth warning message"
[root@centos ~]# vim /etc/rsyslog.conf
[root@centos ~]#
```



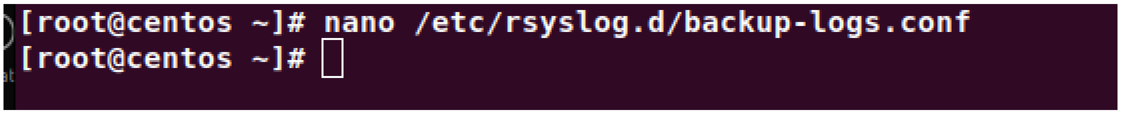
```
authpriv.* ~
```



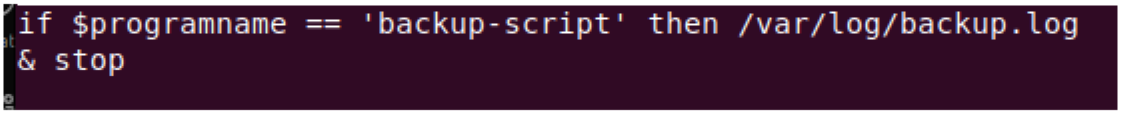
```
[root@centos ~]# sudo tail -n 2 -f /var/log/secure

Mar 27 14:12:55 centos sudo[3246]:    root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/bin/tail
 -n 2 -f /var/log/secure
Mar 27 14:12:55 centos sudo[3246]: pam_unix(sudo:session): session opened for user root(uid=0) by
root(uid=0)
Mar 27 14:12:58 centos root[3250]: auth warning message
Mar 27 14:13:01 centos root[3251]: auth warning message
Mar 27 14:13:52 centos root[3253]: auth warning message: disabled !
```

```
[root@centos ~]# logger -p authpriv.warning "auth warning message"
[root@centos ~]# logger -p authpriv.warning "auth warning message"
[root@centos ~]# vim /etc/rsyslog.conf
[root@centos ~]# logger -p authpriv.warning "auth warning message: disabled !"
[root@centos ~]# sudo systemctl restart rsyslog
[root@centos ~]# logger -p authpriv.warning "auth warning message: disabled ! 2"
[root@centos ~]# logger -p authpriv.warning "auth warning message: disabled ! 3"
[root@centos ~]# logger -p authpriv.warning "auth warning message: disabled ! 4"
[root@centos ~]#
```

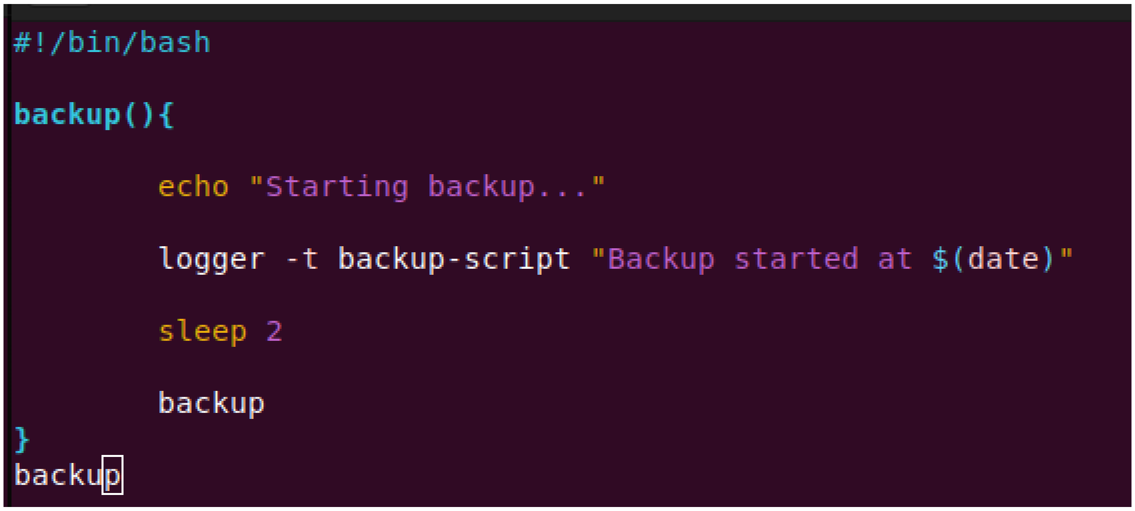
7. How do you configure Rsyslog to log messages from a specific application to a customlog file?



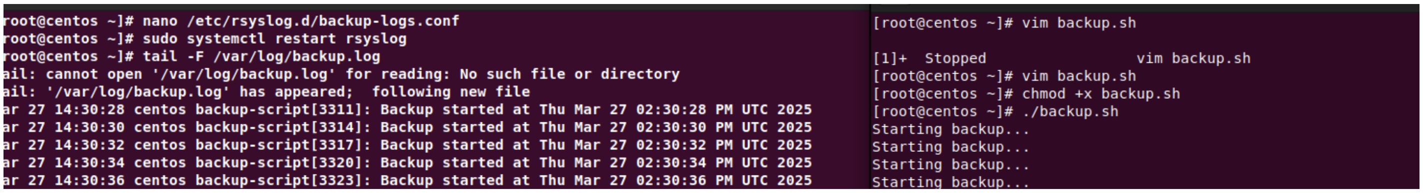
```
[root@centos ~]# nano /etc/rsyslog.d/backup-logs.conf
[root@centos ~]#
```



```
if $programname == 'backup-script' then /var/log/backup.log
& stop
```



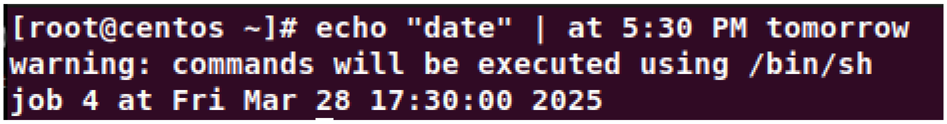
```
#!/bin/bash

backup(){

        echo "Starting backup..."

        logger -t backup-script "Backup started at $(date)"

        sleep 2

        backup
}
backup
```



```
root@centos ~]# nano /etc/rsyslog.d/backup-logs.conf
root@centos ~]# sudo systemctl restart rsyslog
root@centos ~]# tail -F /var/log/backup.log
ail: cannot open '/var/log/backup.log' for reading: No such file or directory
ail: '/var/log/backup.log' has appeared;  following new file
ar 27 14:30:28 centos backup-script[3311]: Backup started at Thu Mar 27 02:30:28 PM UTC 2025
ar 27 14:30:30 centos backup-script[3314]: Backup started at Thu Mar 27 02:30:30 PM UTC 2025
ar 27 14:30:32 centos backup-script[3317]: Backup started at Thu Mar 27 02:30:32 PM UTC 2025
ar 27 14:30:34 centos backup-script[3320]: Backup started at Thu Mar 27 02:30:34 PM UTC 2025
ar 27 14:30:36 centos backup-script[3323]: Backup started at Thu Mar 27 02:30:36 PM UTC 2025
```

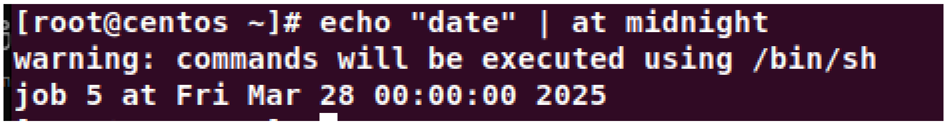
```
[root@centos ~]# vim backup.sh

[1]+  Stopped                 vim backup.sh
[root@centos ~]# vim backup.sh
[root@centos ~]# chmod +x backup.sh
[root@centos ~]# ./backup.sh
Starting backup...
Starting backup...
Starting backup...
Starting backup...
```

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



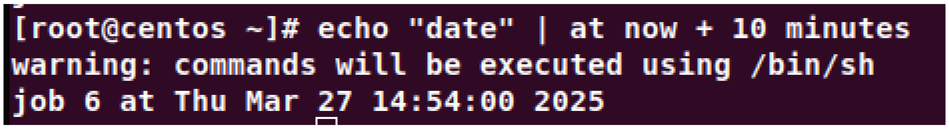
```
[root@centos ~]# echo "date" | at 5:30 PM tomorrow
warning: commands will be executed using /bin/sh
job 4 at Fri Mar 28 17:30:00 2025
```

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



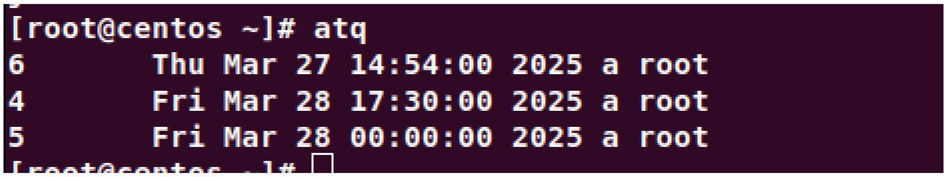
```
[root@centos ~]# echo "date" | at midnight
warning: commands will be executed using /bin/sh
job 5 at Fri Mar 28 00:00:00 2025
```

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



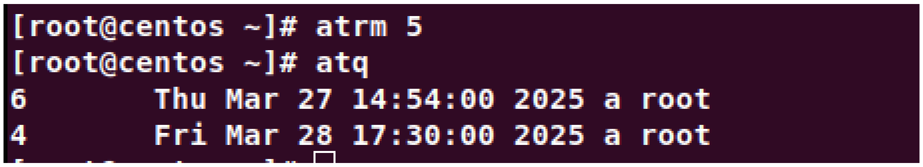
```
[root@centos ~]# echo "date" | at now + 10 minutes
warning: commands will be executed using /bin/sh
job 6 at Thu Mar 27 14:54:00 2025
```

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



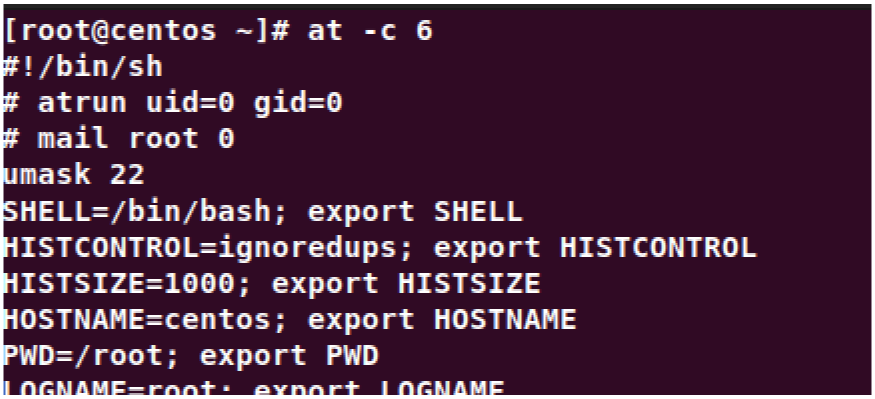
```
[root@centos ~]# atq
6       Thu Mar 27 14:54:00 2025 a root
4       Fri Mar 28 17:30:00 2025 a root
5       Fri Mar 28 00:00:00 2025 a root
[root@centos ~]#
```

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

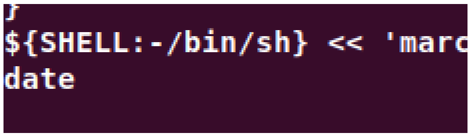


```
[root@centos ~]# atrm 5
[root@centos ~]# atq
6       Thu Mar 27 14:54:00 2025 a root
4       Fri Mar 28 17:30:00 2025 a root
```

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



```
[root@centos ~]# at -c 6
#!/bin/sh
# atrun uid=0 gid=0
# mail root 0
umask 22
SHELL=/bin/bash; export SHELL
HISTCONTROL=ignoredups; export HISTCONTROL
HISTSIZE=1000; export HISTSIZE
HOSTNAME=centos; export HOSTNAME
PWD=/root; export PWD
LOGNAME=root; export LOGNAME
```



```
}
${SHELL:-/bin/sh} << 'marc
date
```