Seif Hendawy
RHCSA II Day 2

1. What Different Between Rsyslog and Jornald?

Rsyslog:

A traditional syslog daemon designed for efficient log processing, filtering, and forwarding to remote servers
Stores logs in plain text files
More efficient for high-volume logging; supports multi-threading and can offload logs to external storage or remote servers
Supports remote logging

Journald:

A modern logging system introduced with systemd, designed for structured logging, log rotation, and better integration with systemd services
Saves data in structured format uses a binary journal format stored in /var/log/journal
Optimized for local logging
orwarding via TCP, UDP, or RELP, making it ideal for centralized logging.
Does not support remote logging

---

2. What are the main configuration files for Rsyslog?

/etc/rsyslog.conf
/etc/rsyslog.d/*.conf

---

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

```
seif@172:~$ journalctl -f
Mar 27 14:51:44 172.16.224.128 systemd[1]: Started systemd-timedated.service - Time & Date Service.
Mar 27 14:51:44 172.16.224.128 rtkit-daemon[891]: Successfully made thread 6916 of process 6785 (/usr/lib64/firefox/f
irefox) owned by '1000' RT at priority 10.
Mar 27 14:52:14 172.16.224.128 systemd[1]: systemd-timedated.service: Deactivated successfully.
Mar 27 14:54:15 172.16.224.128 systemd[5645]: Created slice background.slice - User Background Tasks Slice.
Mar 27 14:54:15 172.16.224.128 systemd[5645]: Starting systemd-tmpfiles-clean.service - Cleanup of User's Temporary F
iles and Directories...
Mar 27 14:54:15 172.16.224.128 systemd[5645]: Finished systemd-tmpfiles-clean.service - Cleanup of User's Temporary F
iles and Directories.
Mar 27 14:54:34 172.16.224.128 PackageKit[1861]: daemon quit
Mar 27 14:54:34 172.16.224.128 systemd[1]: packagekit.service: Deactivated successfully.
Mar 27 14:54:34 172.16.224.128 systemd[1]: packagekit.service: Consumed 4.050s CPU time, 258.8M memory peak.
Mar 27 14:56:02 172.16.224.128 chronyd[898]: Selected source 160.119.248.252 (2.centos.pool.ntp.org)
^C
seif@172:~$
```

---

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

```
*.*                                                     /var/log/syslog
```

```
seif@172:~$ sudo nano /etc/rsyslog.conf
seif@172:~$ sudo systemctl restart rsyslog
seif@172:~$ logger "Seif Hendawy DevOps Engineer lab 2"
seif@172:~$ cat /var/log/syslog
cat: /var/log/syslog: Permission denied
seif@172:~$ sudo cat /var/log/syslog
Mar 27 15:04:19 172 sudo[8170]:    seif : TTY=pts/0 ; PWD=/home/seif ; USER=root ;
slog
Mar 27 15:04:19 172 systemd-logind[896]: Existing logind session ID 3 used by new
Mar 27 15:04:19 172 systemd-logind[896]: New session c6 of user root.
Mar 27 15:04:19 172 systemd[1]: Started session-c6.scope - Session c6 of User root
Mar 27 15:04:19 172 sudo[8170]: pam_unix(sudo:session): session opened for user ro
```

```
seif@172:~$ cat /var/log/syslog | grep DevOps
cat: /var/log/syslog: Permission denied
seif@172:~$ sudo cat /var/log/syslog | grep DevOps
Mar 27 15:04:29 172 seif[8182]: Seif Hendawy DevOps Engineer lab 2
seif@172:~$
```

---

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.

```
*.*                                                     /var/log/syslog

*.warning                                               /var/log/warnings.log
```

---

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

```
auth.* ~
```

---

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

if $programname == x' then /var/log/x.log

---

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

```
seif@172:~$ echo "Seif Hendawy DevOps Enginer" >> tmrw.txt | at 17:30 tomorrow
warning: commands will be executed using /bin/sh
job 1 at Fri Mar 28 17:30:00 2025
```

---

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

```
seif@172:~$ echo "Seif Hendawy DevOps Enginer" >> tmrw.txt | at midnight
warning: commands will be executed using /bin/sh
job 2 at Fri Mar 28 00:00:00 2025
seif@172:~$
```

---

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

```
seif@172:~$ echo "Seif Hendawy DevOps Enginer" >> tmrw.txt | at now + 10 minutes
warning: commands will be executed using /bin/sh
job 3 at Thu Mar 27 15:28:00 2025
seif@172:~$
```

---

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

```
seif@172:~$ atq
1       Fri Mar 28 17:30:00 2025 a seif
2       Fri Mar 28 00:00:00 2025 a seif
3       Thu Mar 27 15:28:00 2025 a seif
seif@172:~$
```

---

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

```
seif@172:~$ atq
1       Fri Mar 28 17:30:00 2025 a seif
2       Fri Mar 28 00:00:00 2025 a seif
3       Thu Mar 27 15:28:00 2025 a seif
seif@172:~$ atrm 2
seif@172:~$ atq
1       Fri Mar 28 17:30:00 2025 a seif
3       Thu Mar 27 15:28:00 2025 a seif
seif@172:~$
```

---

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