

Linux Admin 2 - Lab 2

Name: Muhamad Mamoun Elsaid Hassan

1-

journald	rsyslog
Binary format logs	Plain text logs (Human Readable)
Stored in RAM (/run/logs/journald)	Stored in FileSystem (/var/logs/)
Limited configurations	Highly configurable than journald and allows you to access remote machines

2-

```
mamoun@mamoun-laptop: ~  
[mamoun@mamoun-laptop]-[~]  
$ ls /etc/rsyslog.conf  
/etc/rsyslog.conf  
[mamoun@mamoun-laptop]-[~]  
$ _
```

3-

```
mamoun@mamoun-laptop: ~  
[mamoun@mamoun-laptop]-[~]  
$ tail -f /var/log/syslog  
2025-03-28T06:31:24.792729+02:00 mamoun-laptop gnome-shell[34947]:  
Can't update stage views actor bms-dash-blurred-widget [StWidget]  
is on because it needs an allocation.  
2025-03-28T06:31:24.808504+02:00 mamoun-laptop gnome-shell[34947]:  
Can't update stage views actor unnamed [Gjs_dash-to-dock_micxgx_g  
mail_com_docking_DashSlideContainer] is on because it needs an all
```

4-

```
mamoun@mamoun-laptop: ~  
(mamoun@mamoun-laptop)-[~]  
$ systemctl status rsyslog.service  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled;  
   Active: active (running) since Wed 2025-03-26 17:10:07 EET; 1min  
TriggeredBy: ● syslog.socket  
   Docs: man:rsyslogd(8)  
         man:rsyslog.conf(5)  
         https://www.rsyslog.com/doc/  
 Main PID: 1164 (rsyslogd)  
   Tasks: 4 (limit: 13951)  
  Memory: 5.9M (peak: 6.5M)  
    CPU: 1.429s  
   CGroup: /system.slice/rsyslog.service  
           └─1164 /usr/sbin/rsyslogd -n -iNONE
```

5-

```
#### RULES ####  
*.warn                                /var/log/warnings.log_  
  
mamoun@redhat:~ — systemctl status rsyslog.service  
(mamoun@redhat)-[~]  
$ systemctl restart rsyslog.service  
(mamoun@redhat)-[~]  
$ systemctl status rsyslog.service  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)  
   Active: active (running) since Fri 2025-03-28 06:49:22 EET; 8s ago  
   Docs: man:rsyslogd(8)  
         https://www.rsyslog.com/doc/  
  
mamoun@redhat:~ — sudo tail -f /var/log/warnings.log  
(mamoun@redhat)-[~]  
$ sudo tail -f /var/log/warnings.log  
[sudo] password for mamoun:  
Mar 28 06:49:37 redhat gnome-shell[1937]: Timelines with detached actors are not supported  
Mar 28 06:49:37 redhat gnome-shell[1937]: Timelines with detached actors are not supported  
Mar 28 06:49:37 redhat gnome-shell[1937]: Timelines with detached actors are not supported  
Mar 28 06:49:37 redhat gnome-shell[1937]: Timelines with detached actors are not supported  
Mar 28 06:50:25 redhat sudo[3185]: pam_unix(sudo:auth): conversation failed  
Mar 28 06:50:25 redhat sudo[3185]: pam_unix(sudo:auth): auth could not identify password for [mamoun]  
Mar 28 06:50:27 redhat sudo[3185]: mamoun : 1 incorrect password attempt ; TTY=pts/0 ; PWD=/home/mamoun  
; USER=root ; COMMAND=/bin/tail -f /var/log/warnings.log
```

6-

```
auth.*
```

7-

The screenshot shows a terminal window titled "mamoun@redhat:~ — sudo visudo /etc/rsyslog.d/my-app.conf" at 07:02. The content of the file is:

```
if $programname == 'my-app' then /var/log/my-app.logs
& stop_
```

Below this, another terminal window is shown at 07:09, split into two panes. The left pane shows the user configuring rsyslog:

```
(mamoun@redhat)-[~]
$ sudo touch /etc/rsyslog.d/my-app.conf
(mamoun@redhat)-[~]
$ sudo vim /etc/rsyslog.d/my-app.conf
(mamoun@redhat)-[~]
$ systemctl restart rsyslog.service
(mamoun@redhat)-[~]
$ logger -t my-app "Hello, World!"
(mamoun@redhat)-[~]
$ logger -t my-app "Hello, World!"
(mamoun@redhat)-[~]
$
```

The right pane shows the output of `sudo tail -F /var/log/my-app.logs`:

```
(mamoun@redhat)-[~]
$ sudo tail -F /var/log/my-app.logs
Mar 28 07:06:37 redhat my-app[3713]: Hello, World!
Mar 28 07:09:19 redhat my-app[3883]: Hello, World!
Mar 28 07:09:23 redhat my-app[3888]: Hello, World!
_
```

8-

The screenshot shows a terminal window at 07:19. The user sets up an at job:

```
(mamoun@redhat)-[~]
$ echo "touch ~/text.at" | at 5:30 PM tomorrow
warning: commands will be executed using /bin/sh
job 2 at Sat Mar 29 17:30:00 2025
(mamoun@redhat)-[~]
$ at -l
2      Sat Mar 29 17:30:00 2025 a mamoun
(mamoun@redhat)-[~]
$
```

9-

The screenshot shows a terminal window at 07:20. The user sets up an at job for midnight:

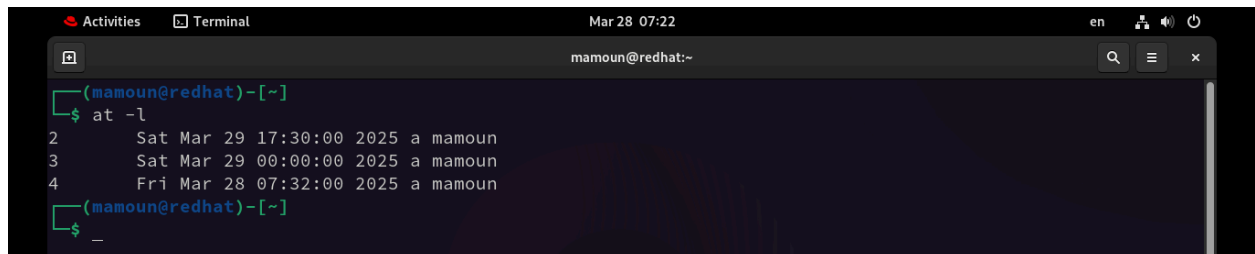
```
(mamoun@redhat)-[~]
$ echo "touch ~/text.at" | at midnight
warning: commands will be executed using /bin/sh
job 3 at Sat Mar 29 00:00:00 2025
(mamoun@redhat)-[~]
$
```

10-

The screenshot shows a terminal window at 07:22. The user sets up an at job for 10 minutes from now:

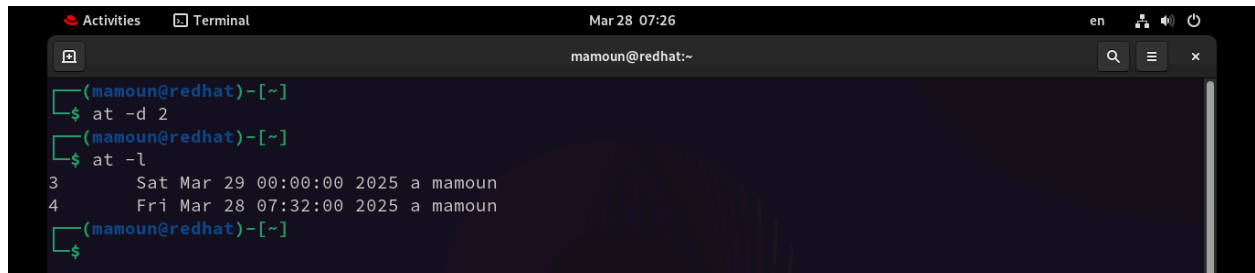
```
(mamoun@redhat)-[~]
$ echo "touch ~/text.at" | at now+10min
warning: commands will be executed using /bin/sh
job 4 at Fri Mar 28 07:32:00 2025
(mamoun@redhat)-[~]
$
```

11-



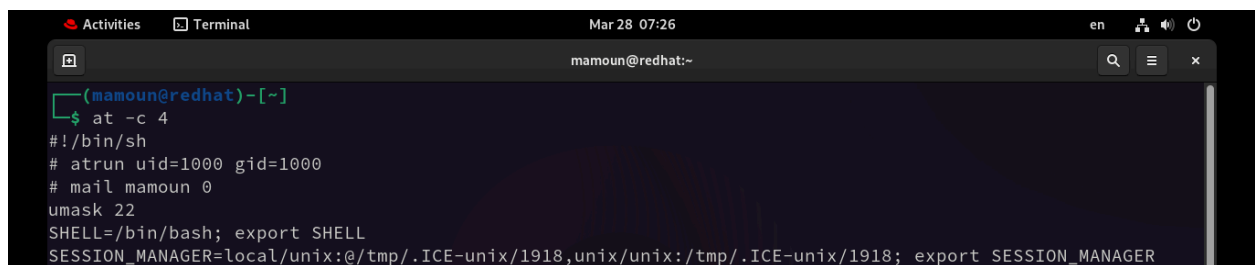
```
Activities Terminal Mar 28 07:22 en mamoun@redhat:~
(mamoun@redhat)-[~]
$ at -l
2      Sat Mar 29 17:30:00 2025 a mamoun
3      Sat Mar 29 00:00:00 2025 a mamoun
4      Fri Mar 28 07:32:00 2025 a mamoun
(mamoun@redhat)-[~]
$ _
```

12-



```
Activities Terminal Mar 28 07:26 en mamoun@redhat:~
(mamoun@redhat)-[~]
$ at -d 2
(mamoun@redhat)-[~]
$ at -l
3      Sat Mar 29 00:00:00 2025 a mamoun
4      Fri Mar 28 07:32:00 2025 a mamoun
(mamoun@redhat)-[~]
$
```

13-



```
Activities Terminal Mar 28 07:26 en mamoun@redhat:~
(mamoun@redhat)-[~]
$ at -c 4
#!/bin/sh
# atrun uid=1000 gid=1000
# mail mamoun 0
umask 22
SHELL=/bin/bash; export SHELL
SESSION_MANAGER=local/unix:@/tmp/.ICE-unix/1918,unix/unix:/tmp/.ICE-unix/1918; export SESSION_MANAGER
```