

Cloud Platform Development

Moaaz Sobhy Mahmoud Ismail Briek

[WhatsApp](#) | [Email](#) | [LinkedIn](#) | [GitHub](#)

1. What Different Between Rsyslog and Journald?

Rsyslog is a traditional system logging daemon that writes logs to text files in /var/log

Journald is a newer systemd-based logging system that stores logs in a binary format

Rsyslog supports multiple log storage formats and network logging

Journald provides more structured logging with metadata and faster log retrieval

Rsyslog can work with Journald and forward its logs to traditional text files

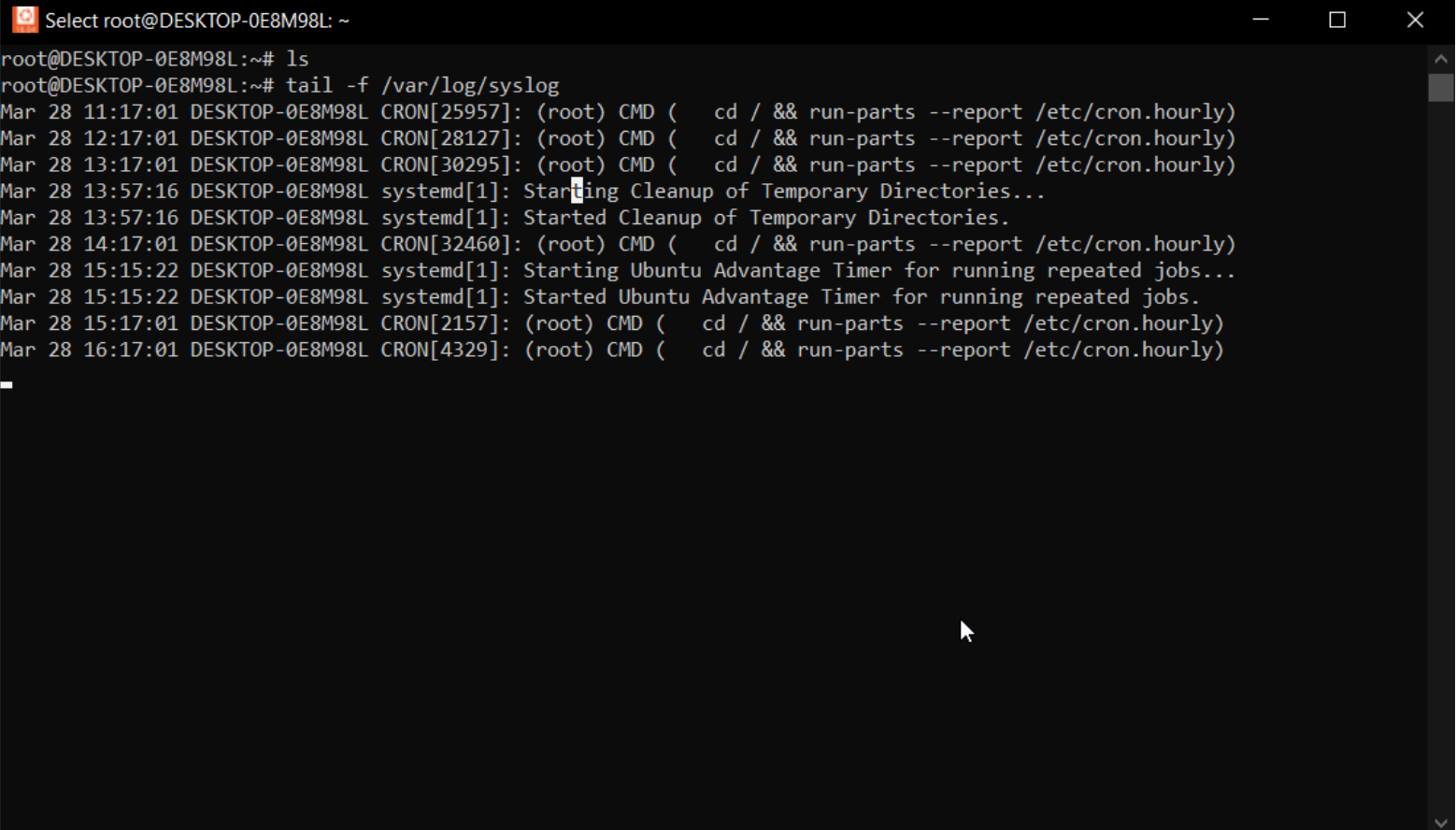
2. What are the main configuration files for Rsyslog?

/etc/rsyslog.conf: Primary configuration file

Files in /etc/rsyslog.d/: Additional configuration snippets

/etc/logrotate.d/rsyslog: Log rotation configuration

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

A terminal window titled "Select root@DESKTOP-0E8M98L: ~" with standard window controls. The user enters the command `tail -f /var/log/syslog`. The terminal displays a stream of log messages from the system log. The messages include timestamps, hostnames, and log entries from cron jobs and systemd. A mouse cursor is visible at the bottom right of the terminal window.

```
root@DESKTOP-0E8M98L:~# ls
root@DESKTOP-0E8M98L:~# tail -f /var/log/syslog
Mar 28 11:17:01 DESKTOP-0E8M98L CRON[25957]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 12:17:01 DESKTOP-0E8M98L CRON[28127]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 13:17:01 DESKTOP-0E8M98L CRON[30295]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 13:57:16 DESKTOP-0E8M98L systemd[1]: Starting Cleanup of Temporary Directories...
Mar 28 13:57:16 DESKTOP-0E8M98L systemd[1]: Started Cleanup of Temporary Directories.
Mar 28 14:17:01 DESKTOP-0E8M98L CRON[32460]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 15:15:22 DESKTOP-0E8M98L systemd[1]: Starting Ubuntu Advantage Timer for running repeated jobs...
Mar 28 15:15:22 DESKTOP-0E8M98L systemd[1]: Started Ubuntu Advantage Timer for running repeated jobs.
Mar 28 15:17:01 DESKTOP-0E8M98L CRON[2157]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 16:17:01 DESKTOP-0E8M98L CRON[4329]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
```

root@DESKTOP-0E8M98L: ~

root@DESKTOP-0E8M98L:~# journalctl -f

-- Logs begin at Tue 2025-02-18 09:36:54 EET. --

Mar 28 14:17:01 DESKTOP-0E8M98L CRON[32460]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

Mar 28 14:17:01 DESKTOP-0E8M98L CRON[32459]: pam_unix(cron:session): session closed for user root

Mar 28 15:15:22 DESKTOP-0E8M98L systemd[1]: Starting Ubuntu Advantage Timer for running repeated jobs...

Mar 28 15:15:22 DESKTOP-0E8M98L systemd[1]: Started Ubuntu Advantage Timer for running repeated jobs.

Mar 28 15:17:01 DESKTOP-0E8M98L CRON[2156]: pam_unix(cron:session): session opened for user root by (uid=0)

Mar 28 15:17:01 DESKTOP-0E8M98L CRON[2157]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

Mar 28 15:17:01 DESKTOP-0E8M98L CRON[2156]: pam_unix(cron:session): session closed for user root

Mar 28 16:17:01 DESKTOP-0E8M98L CRON[4328]: pam_unix(cron:session): session opened for user root by (uid=0)

Mar 28 16:17:01 DESKTOP-0E8M98L CRON[4329]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

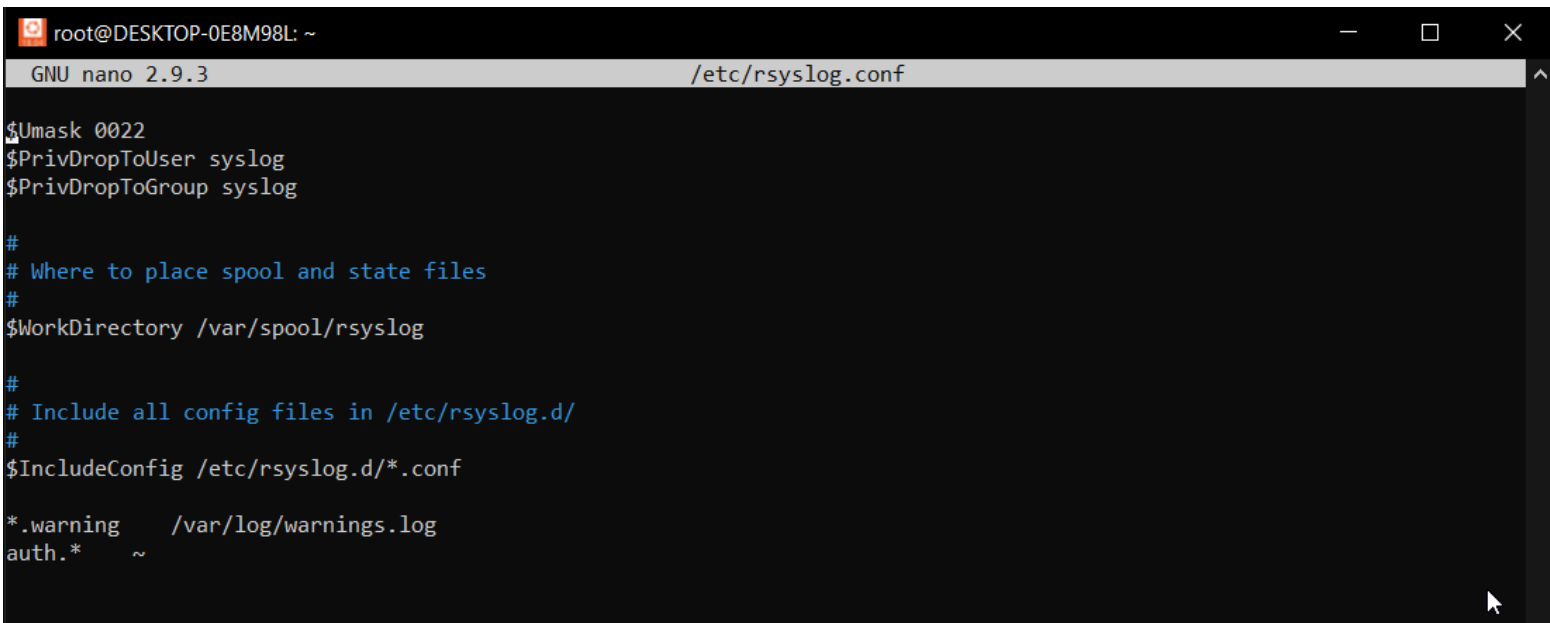
Mar 28 16:17:01 DESKTOP-0E8M98L CRON[4328]: pam_unix(cron:session): session closed for user root

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

```
root@DESKTOP-0E8M98L: ~  
root@DESKTOP-0E8M98L:~# rsyslogd -N1  
rsyslogd: version 8.32.0, config validation run (level 1), master config /etc/rsyslog.conf  
rsyslogd: End of config validation run. Bye.  
root@DESKTOP-0E8M98L:~# sudo systemctl restart rsyslog  
root@DESKTOP-0E8M98L:~# sudo systemctl status rsyslog  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2025-03-28 16:30:51 EET; 4s ago  
     Docs: man:rsyslogd(8)  
           http://www.rsyslog.com/doc/  
 Main PID: 4839 (rsyslogd)  
    Tasks: 4 (limit: 4915)  
   CGroup: /system.slice/rsyslog.service  
           └─4839 /usr/sbin/rsyslogd -n  
  
Mar 28 16:30:51 DESKTOP-0E8M98L systemd[1]: Starting System Logging Service...  
Mar 28 16:30:51 DESKTOP-0E8M98L rsyslogd[4839]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from  
Mar 28 16:30:51 DESKTOP-0E8M98L rsyslogd[4839]: rsyslogd's groupid changed to 106  
Mar 28 16:30:51 DESKTOP-0E8M98L systemd[1]: Started System Logging Service.  
Mar 28 16:30:51 DESKTOP-0E8M98L rsyslogd[4839]: rsyslogd's userid changed to 102  
Mar 28 16:30:51 DESKTOP-0E8M98L rsyslogd[4839]: [origin software="rsyslogd" swVersion="8.32.0" x-pid="4839" x-info="htt  
lines 1-16/16 (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.

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

A screenshot of a terminal window titled 'root@DESKTOP-0E8M98L: ~'. The terminal shows the GNU nano 2.9.3 editor editing the file /etc/rsyslog.conf. The configuration includes settings for umask, privilege dropping to syslog, work directory, and including config files from /etc/rsyslog.d/. At the bottom, there are two log rules: one for *.warning to log to /var/log/warnings.log, and another for auth.* to log to ~.

```
root@DESKTOP-0E8M98L: ~  
GNU nano 2.9.3 /etc/rsyslog.conf  
$Umask 0022  
$PrivDropToUser syslog  
$PrivDropToGroup syslog  
  
#  
# Where to place spool and state files  
#  
$WorkDirectory /var/spool/rsyslog  
  
#  
# Include all config files in /etc/rsyslog.d/  
#  
$IncludeConfig /etc/rsyslog.d/*.conf  
  
*.warning    /var/log/warnings.log  
auth.*      ~
```

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

```
root@DESKTOP-0E8M98L: ~  
GNU nano 2.9.3  
  
$Umask 0022  
$PrivDropToUser syslog  
$PrivDropToGroup syslog  
  
#  
# Where to place spool and state files  
#  
$WorkDirectory /var/spool/rsyslog  
  
#  
# Include all config files in /etc/rsyslog.d/  
#  
$IncludeConfig /etc/rsyslog.d/*.conf  
  
*.warning    /var/log/warnings.log  
auth.*      ~  
  
if $programname == 'apache2' then /var/log/apache_custom.log  
& stop_
```

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

```
root@DESKTOP-0E8M98L: ~  
root@DESKTOP-0E8M98L:~# ls -l  
total 4  
-rw-r--r-- 1 root root 37 Apr  1 03:11 scheduler.sh  
root@DESKTOP-0E8M98L:~# chmod 645 scheduler.sh  
root@DESKTOP-0E8M98L:~# ls -l  
total 4  
-rw-r--r-x 1 root root 37 Apr  1 03:11 scheduler.sh  
root@DESKTOP-0E8M98L:~# ./scheduler.sh  
Hello scheduler  
root@DESKTOP-0E8M98L:~# echo scheduler.sh | at 5:30 PM tomorrow  
warning: commands will be executed using /bin/sh  
job 1 at Wed Apr  2 17:30:00 2025  
root@DESKTOP-0E8M98L:~#
```

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

```
root@DESKTOP-0E8M98L:~# echo scheduler.sh | at midnight  
warning: commands will be executed using /bin/sh  
job 2 at Wed Apr  2 00:00:00 2025  
root@DESKTOP-0E8M98L:~#
```

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

```
root@DESKTOP-0E8M98L:~# echo scheduler.sh | at now + 10 minutes  
warning: commands will be executed using /bin/sh  
job 3 at Tue Apr  1 03:25:00 2025  
root@DESKTOP-0E8M98L:~#
```

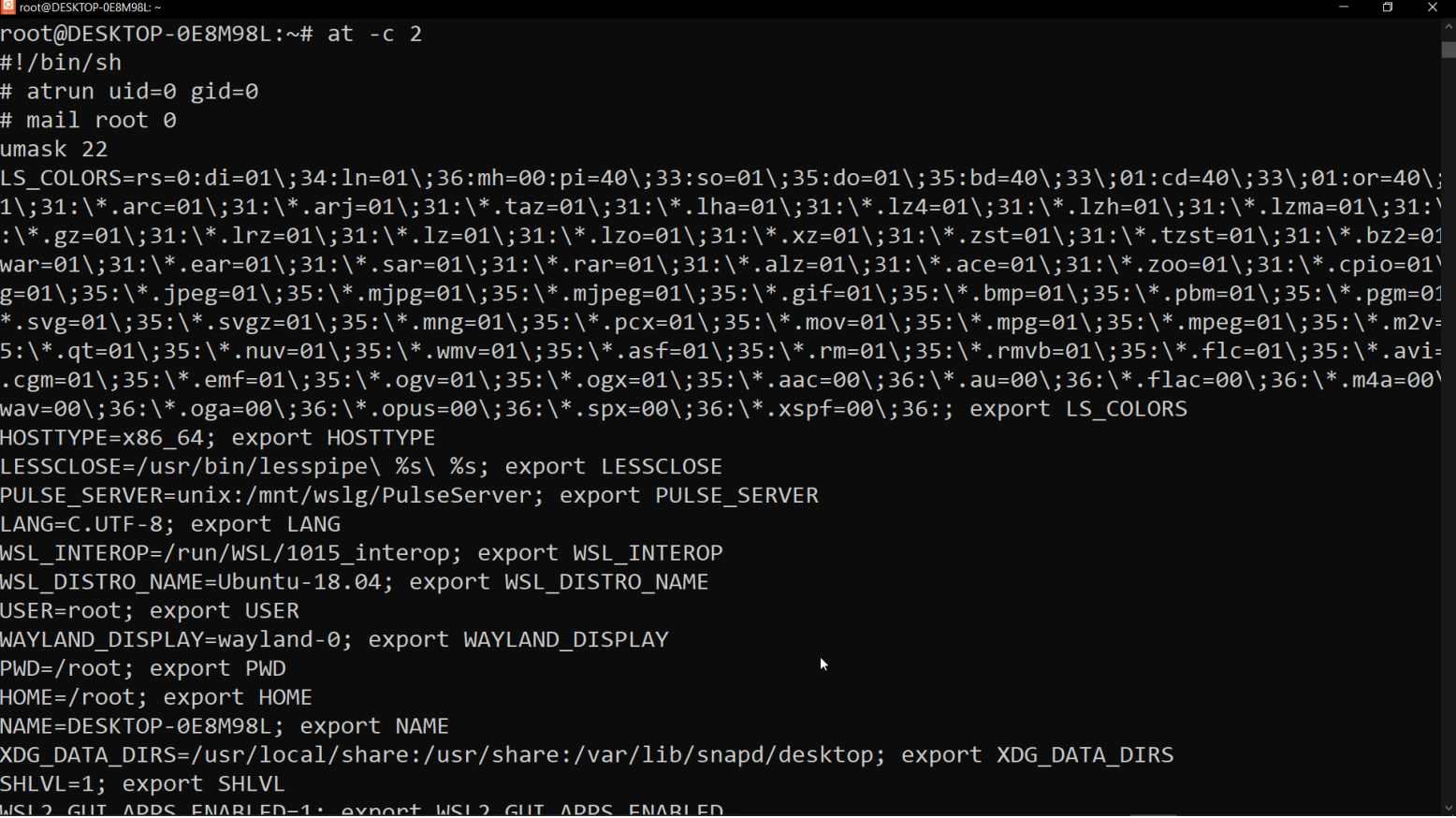
11. How do you list all scheduled tasks using the AT command?

```
root@DESKTOP-0E8M98L: ~  
root@DESKTOP-0E8M98L:~# atq  
2      Wed Apr  2 00:00:00 2025 a root  
1      Wed Apr  2 17:30:00 2025 a root  
3      Tue Apr  1 03:25:00 2025 a root  
root@DESKTOP-0E8M98L:~#
```

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

```
root@DESKTOP-0E8M98L: ~  
root@DESKTOP-0E8M98L:~# atq  
2      Wed Apr  2 00:00:00 2025 a root  
1      Wed Apr  2 17:30:00 2025 a root  
3      Tue Apr  1 03:25:00 2025 a root  
root@DESKTOP-0E8M98L:~# atrm 1  
root@DESKTOP-0E8M98L:~# atq  
2      Wed Apr  2 00:00:00 2025 a root  
3      Tue Apr  1 03:25:00 2025 a root  
root@DESKTOP-0E8M98L:~#
```

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



```
root@DESKTOP-0E8M98L: ~# at -c 2
#!/bin/sh
# atrun uid=0 gid=0
# mail root 0
umask 22
LS_COLORS=rs=0:di=01\;34:ln=01\;36:mh=00:pi=40\;33:so=01\;35:do=01\;35:bd=40\;33\;01:cd=40\;33\;01:or=40\;
1\;31\;*\*.arc=01\;31\;*\*.arj=01\;31\;*\*.taz=01\;31\;*\*.lha=01\;31\;*\*.lz4=01\;31\;*\*.lzh=01\;31\;*\*.lzma=01\;31\;
*\*.gz=01\;31\;*\*.lrz=01\;31\;*\*.lz=01\;31\;*\*.lzo=01\;31\;*\*.xz=01\;31\;*\*.zst=01\;31\;*\*.tazst=01\;31\;*\*.bz2=01\;
war=01\;31\;*\*.ear=01\;31\;*\*.sar=01\;31\;*\*.rar=01\;31\;*\*.alz=01\;31\;*\*.ace=01\;31\;*\*.zoo=01\;31\;*\*.cpio=01\;
g=01\;35\;*\*.jpeg=01\;35\;*\*.mjpg=01\;35\;*\*.mjpeg=01\;35\;*\*.gif=01\;35\;*\*.bmp=01\;35\;*\*.pbm=01\;35\;*\*.pgm=01\;
*\*.svg=01\;35\;*\*.svgz=01\;35\;*\*.mng=01\;35\;*\*.pcx=01\;35\;*\*.mov=01\;35\;*\*.mpg=01\;35\;*\*.mpeg=01\;35\;*\*.m2v=
5\;*\*.qt=01\;35\;*\*.nuv=01\;35\;*\*.wmv=01\;35\;*\*.asf=01\;35\;*\*.rm=01\;35\;*\*.rmvb=01\;35\;*\*.flc=01\;35\;*\*.avi=
.cgm=01\;35\;*\*.emf=01\;35\;*\*.ogv=01\;35\;*\*.ogx=01\;35\;*\*.aac=00\;36\;*\*.au=00\;36\;*\*.flac=00\;36\;*\*.m4a=00\;
wav=00\;36\;*\*.oga=00\;36\;*\*.opus=00\;36\;*\*.spx=00\;36\;*\*.xspf=00\;36\;; export LS_COLORS
HOSTTYPE=x86_64; export HOSTTYPE
LESSCLOSE=/usr/bin/lesspipe\ %s\ %s; export LESSCLOSE
PULSE_SERVER=unix:/mnt/wslg/PulseServer; export PULSE_SERVER
LANG=C.UTF-8; export LANG
WSL_INTEROP=/run/WSL/1015_interop; export WSL_INTEROP
WSL_DISTRO_NAME=Ubuntu-18.04; export WSL_DISTRO_NAME
USER=root; export USER
WAYLAND_DISPLAY=wayland-0; export WAYLAND_DISPLAY
PWD=/root; export PWD
HOME=/root; export HOME
NAME=DESKTOP-0E8M98L; export NAME
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop; export XDG_DATA_DIRS
SHLVL=1; export SHLVL
WSL_2_GIT_APPS_ENABLED=1; export WSL_2_GIT_APPS_ENABLED
```
