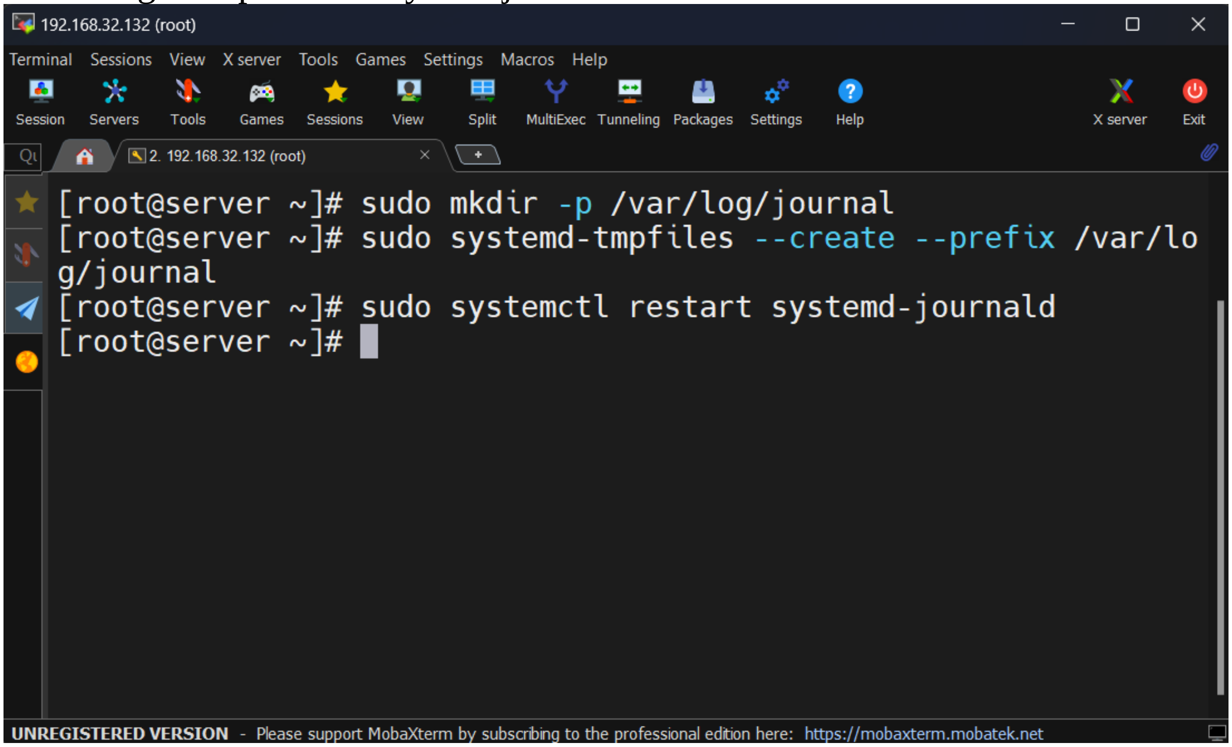
Log Server

Systemd journal

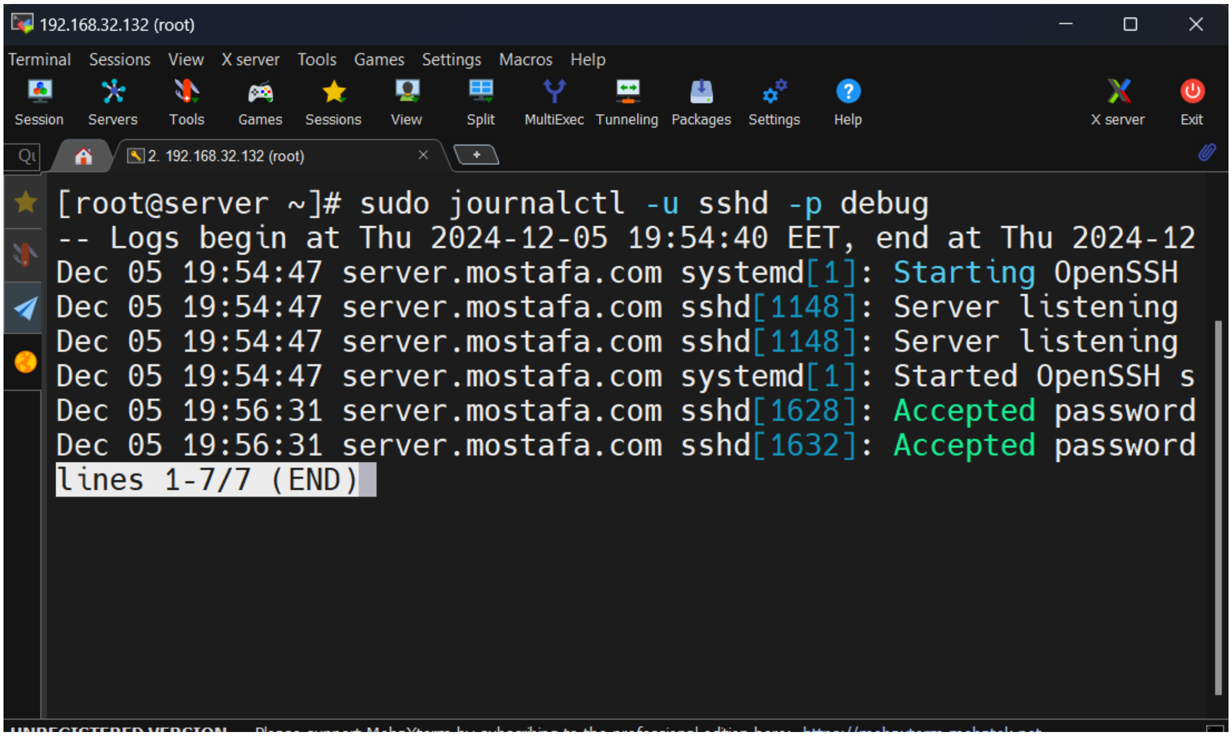
1. Configure a persistent system journal.



192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
2. 192.168.32.132 (root)
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
[root@server ~]# sudo mkdir -p /var/log/journal
[root@server ~]# sudo systemd-tmpfiles --create --prefix /var/lo
g/journal
[root@server ~]# sudo systemctl restart systemd-journald
[root@server ~]# 
```

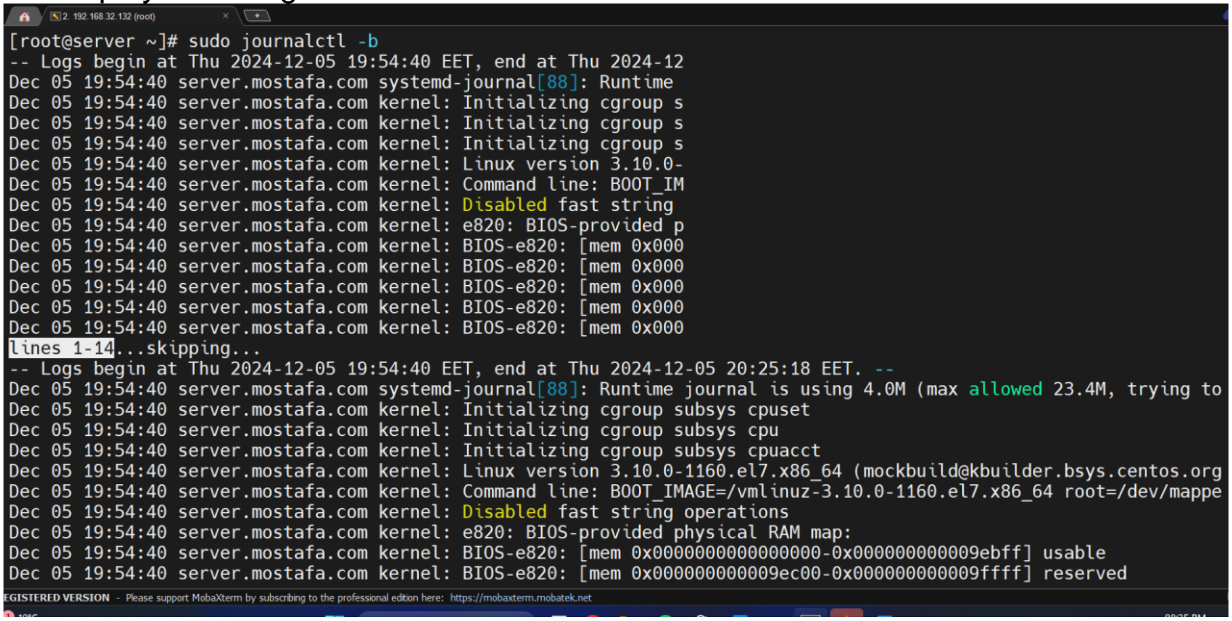
2. Display logs of sshd Service with debug Severity



192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
2. 192.168.32.132 (root)

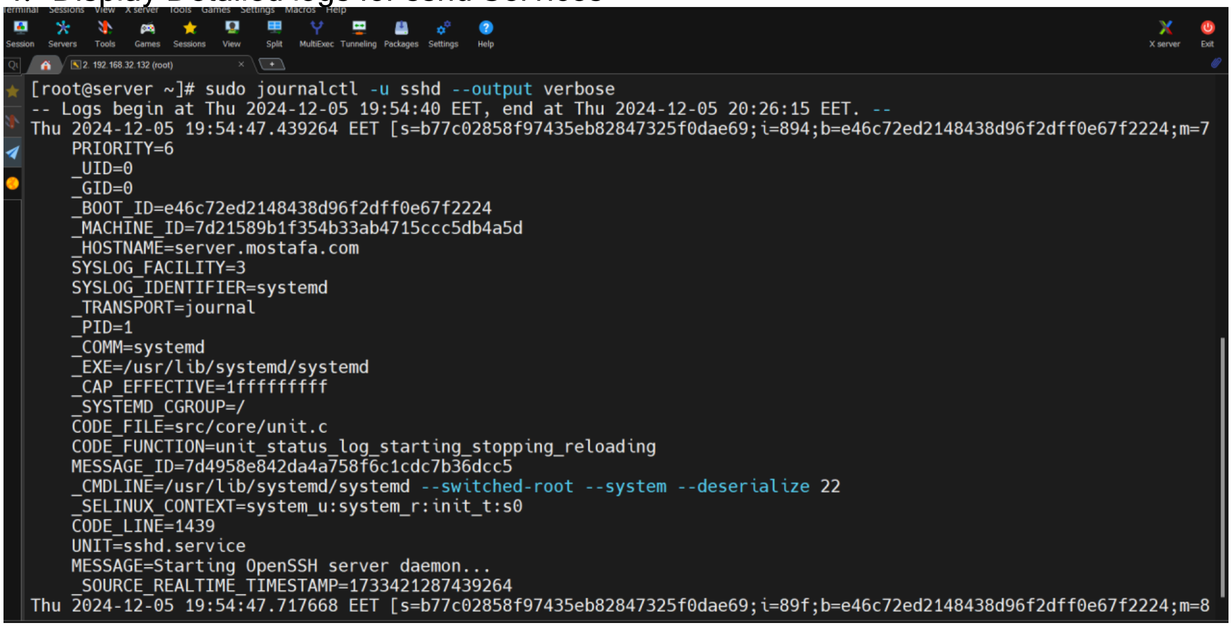
```
[root@server ~]# sudo journalctl -u sshd -p debug
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12
Dec 05 19:54:47 server.mostafa.com systemd[1]: Starting OpenSSH
Dec 05 19:54:47 server.mostafa.com sshd[1148]: Server listening
Dec 05 19:54:47 server.mostafa.com sshd[1148]: Server listening
Dec 05 19:54:47 server.mostafa.com systemd[1]: Started OpenSSH s
Dec 05 19:56:31 server.mostafa.com sshd[1628]: Accepted password
Dec 05 19:56:31 server.mostafa.com sshd[1632]: Accepted password
lines 1-7/7 (END)
```

3. Display boot Logs.


2. 192.168.32.132 (root)
EGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

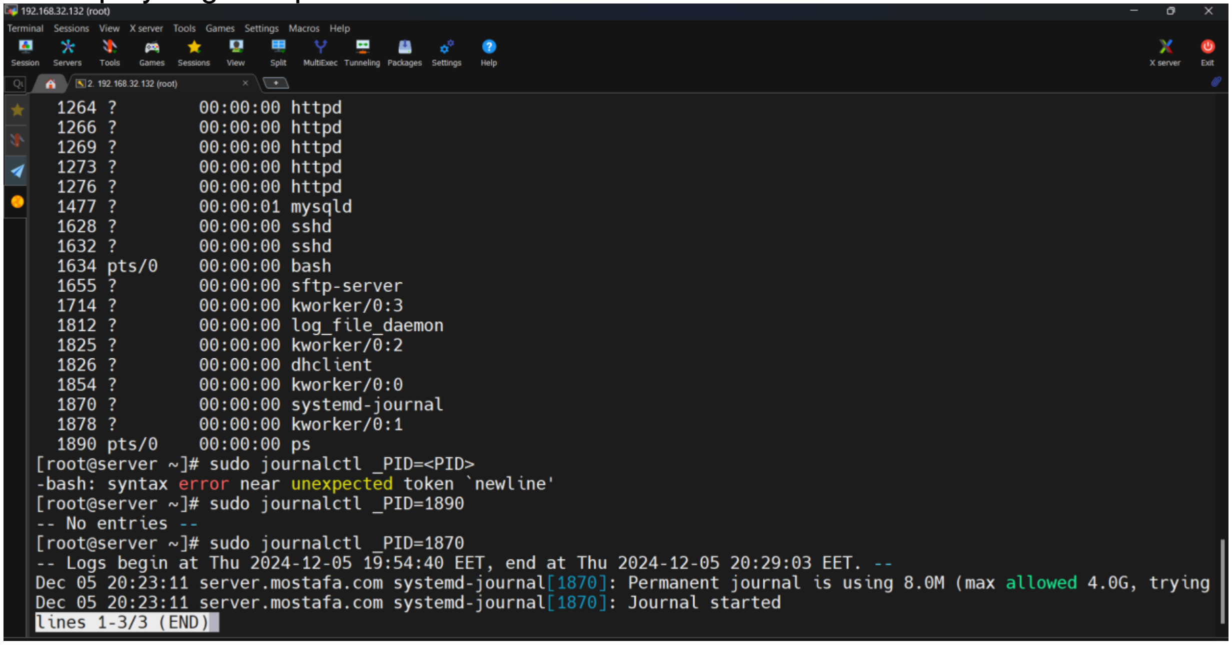
```
[root@server ~]# sudo journalctl -b
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12
Dec 05 19:54:40 server.mostafa.com systemd-journal[88]: Runtime
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup s
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup s
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup s
Dec 05 19:54:40 server.mostafa.com kernel: Linux version 3.10.0-
Dec 05 19:54:40 server.mostafa.com kernel: Command line: BOOT_IM
Dec 05 19:54:40 server.mostafa.com kernel: Disabled fast string
Dec 05 19:54:40 server.mostafa.com kernel: e820: BIOS-provided p
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000
lines 1-14...skipping...
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12-05 20:25:18 EET. --
Dec 05 19:54:40 server.mostafa.com systemd-journal[88]: Runtime journal is using 4.0M (max allowed 23.4M, trying to
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup subsys cpuset
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup subsys cpu
Dec 05 19:54:40 server.mostafa.com kernel: Initializing cgroup subsys cpuacct
Dec 05 19:54:40 server.mostafa.com kernel: Linux version 3.10.0-1160.el7.x86_64 (mockbuild@kbuilder.bsys.centos.org
Dec 05 19:54:40 server.mostafa.com kernel: Command line: BOOT_IMAGE=/vmlinuz-3.10.0-1160.el7.x86_64 root=/dev/mappe
Dec 05 19:54:40 server.mostafa.com kernel: Disabled fast string operations
Dec 05 19:54:40 server.mostafa.com kernel: e820: BIOS-provided physical RAM map:
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009ebff] usable
Dec 05 19:54:40 server.mostafa.com kernel: BIOS-e820: [mem 0x000000000009ec00-0x000000000009ffff] reserved
```

4. Display Detailed logs for sshd Services



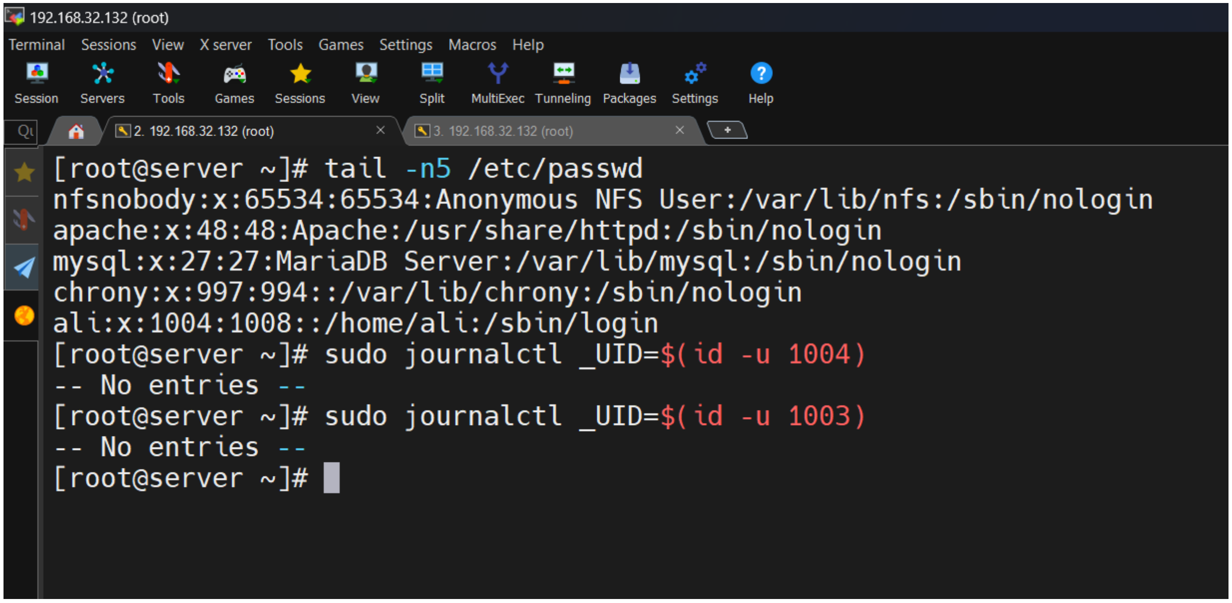
```
[root@server ~]# sudo journalctl -u sshd --output verbose
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12-05 20:26:15 EET. --
Thu 2024-12-05 19:54:47.439264 EET [s=b77c02858f97435eb82847325f0dae69;i=894;b=e46c72ed2148438d96f2dff0e67f2224;m=7
    PRIORITY=6
    _UID=0
    _GID=0
    _BOOT_ID=e46c72ed2148438d96f2dff0e67f2224
    _MACHINE_ID=7d21589b1f354b33ab4715ccc5db4a5d
    _HOSTNAME=server.mostafa.com
    SYSLOG_FACILITY=3
    SYSLOG_IDENTIFIER=systemd
    _TRANSPORT=journal
    _PID=1
    _COMM=systemd
    _EXE=/usr/lib/systemd/systemd
    _CAP_EFFECTIVE=1ffffffff
    _SYSTEMD_CGROUP=/
    CODE_FILE=src/core/unit.c
    CODE_FUNCTION=unit_status_log_starting_stopping_reloading
    MESSAGE_ID=7d4958e842da4a758f6c1cdc7b36dcc5
    _CMDLINE=/usr/lib/systemd/systemd --switched-root --system --deserialize 22
    _SELINUX_CONTEXT=system_u:system_r:init_t:s0
    CODE_LINE=1439
    UNIT=sshd.service
    MESSAGE=Starting OpenSSH server daemon...
    _SOURCE_REALTIME_TIMESTAMP=1733421287439264
Thu 2024-12-05 19:54:47.717668 EET [s=b77c02858f97435eb82847325f0dae69;i=89f;b=e46c72ed2148438d96f2dff0e67f2224;m=8
```

5. Display Logs of specific PID


192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
2. 192.168.32.132 (root)

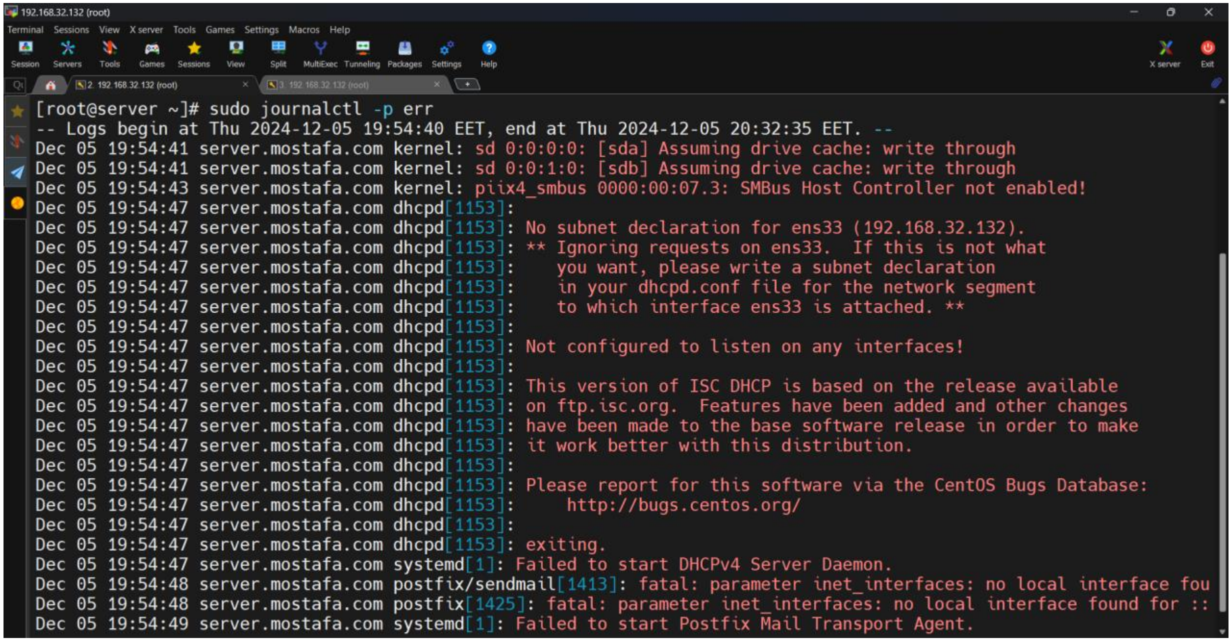
```
  1264 ?        00:00:00 httpd
  1266 ?        00:00:00 httpd
  1269 ?        00:00:00 httpd
  1273 ?        00:00:00 httpd
  1276 ?        00:00:00 httpd
  1477 ?        00:00:01 mysqld
  1628 ?        00:00:00 sshd
  1632 ?        00:00:00 sshd
  1634 pts/0    00:00:00 bash
  1655 ?        00:00:00 sftp-server
  1714 ?        00:00:00 kworker/0:3
  1812 ?        00:00:00 log_file_daemon
  1825 ?        00:00:00 kworker/0:2
  1826 ?        00:00:00 dhclient
  1854 ?        00:00:00 kworker/0:0
  1870 ?        00:00:00 systemd-journal
  1878 ?        00:00:00 kworker/0:1
  1890 pts/0    00:00:00 ps
[root@server ~]# sudo journalctl _PID=<PID>
-bash: syntax error near unexpected token `newline'
[root@server ~]# sudo journalctl _PID=1890
-- No entries --
[root@server ~]# sudo journalctl _PID=1870
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12-05 20:29:03 EET. --
Dec 05 20:23:11 server.mostafa.com systemd-journal[1870]: Permanent journal is using 8.0M (max allowed 4.0G, trying
Dec 05 20:23:11 server.mostafa.com systemd-journal[1870]: Journal started
lines 1-3/3 (END)
```

6. Display Logs of specific User


192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
2. 192.168.32.132 (root)
3. 192.168.32.132 (root)

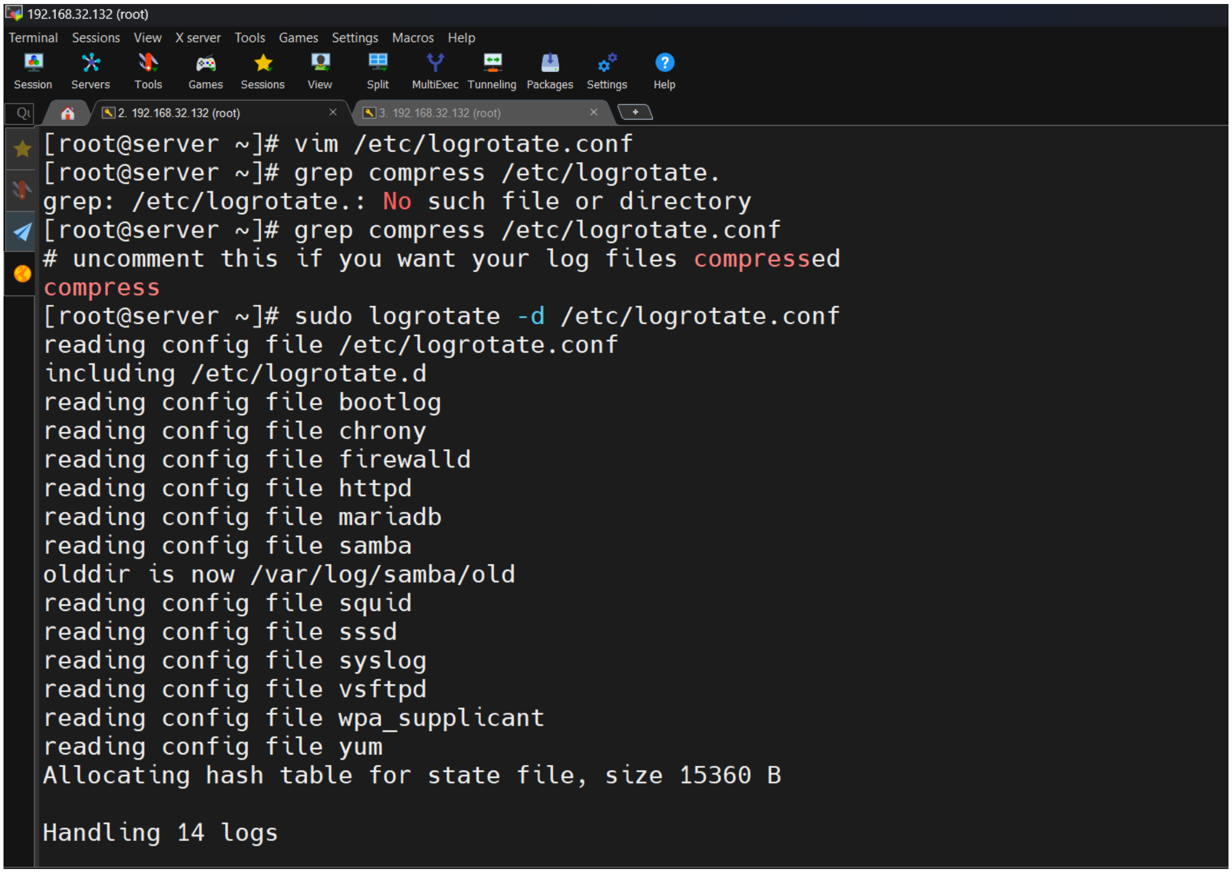
```
[root@server ~]# tail -n5 /etc/passwd
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
chrony:x:997:994::/var/lib/chrony:/sbin/nologin
ali:x:1004:1008::/home/ali:/sbin/login
[root@server ~]# sudo journalctl _UID=$(id -u 1004)
-- No entries --
[root@server ~]# sudo journalctl _UID=$(id -u 1003)
-- No entries --
[root@server ~]# 
```

7. Display error logs


192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
2. 192.168.32.132 (root)
3. 192.168.32.132 (root)

```
[root@server ~]# sudo journalctl -p err
-- Logs begin at Thu 2024-12-05 19:54:40 EET, end at Thu 2024-12-05 20:32:35 EET. --
Dec 05 19:54:41 server.mostafa.com kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Dec 05 19:54:41 server.mostafa.com kernel: sd 0:0:1:0: [sdb] Assuming drive cache: write through
Dec 05 19:54:43 server.mostafa.com kernel: piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: No subnet declaration for ens33 (192.168.32.132).
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: ** Ignoring requests on ens33.  If this is not what
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:    you want, please write a subnet declaration
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:    in your dhcpd.conf file for the network segment
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:    to which interface ens33 is attached. **
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: Not configured to listen on any interfaces!
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: This version of ISC DHCP is based on the release available
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: on ftp.isc.org.  Features have been added and other changes
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: have been made to the base software release in order to make
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: it work better with this distribution.
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: Please report for this software via the CentOS Bugs Database:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:     http://bugs.centos.org/
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]:
Dec 05 19:54:47 server.mostafa.com dhcpd[1153]: exiting.
Dec 05 19:54:47 server.mostafa.com systemd[1]: Failed to start DHCPv4 Server Daemon.
Dec 05 19:54:48 server.mostafa.com postfix/sendmail[1413]: fatal: parameter inet_interfaces: no local interface fou
Dec 05 19:54:48 server.mostafa.com postfix[1425]: fatal: parameter inet_interfaces: no local interface found for ::
Dec 05 19:54:49 server.mostafa.com systemd[1]: Failed to start Postfix Mail Transport Agent.
```

8. Configure logrotate default setting to compress log files when they are rotated


192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
2. 192.168.32.132 (root)
3. 192.168.32.132 (root)

```
[root@server ~]# vim /etc/logrotate.conf
[root@server ~]# grep compress /etc/logrotate.
grep: /etc/logrotate.: No such file or directory
[root@server ~]# grep compress /etc/logrotate.conf
# uncomment this if you want your log files compressed
compress
[root@server ~]# sudo logrotate -d /etc/logrotate.conf
reading config file /etc/logrotate.conf
including /etc/logrotate.d
reading config file bootlog
reading config file chrony
reading config file firewalld
reading config file httpd
reading config file mariadb
reading config file samba
olddir is now /var/log/samba/old
reading config file squid
reading config file sssd
reading config file syslog
reading config file vsftpd
reading config file wpa_supplicant
reading config file yum
Allocating hash table for state file, size 15360 B

Handling 14 logs
```