Защита лабораторной работы № 15

дисциплина: администрирование сетевых подсистем

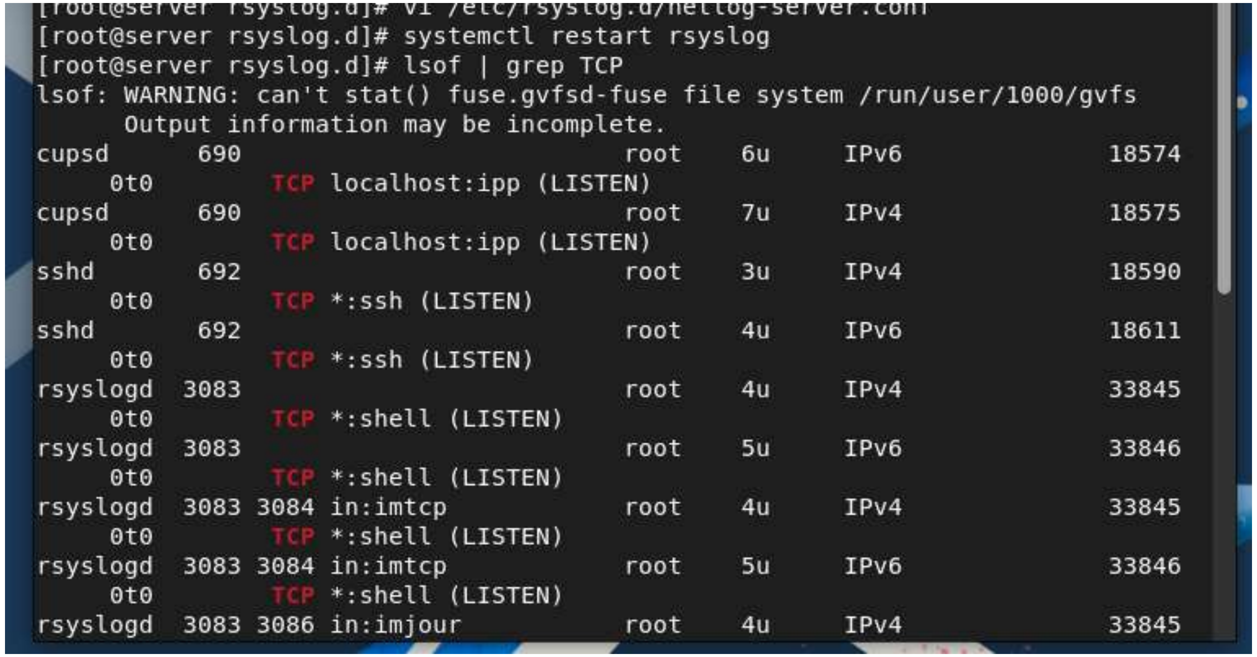
Студент:яссин оулед салем

Группа: НПИбд-02-20

Постановка задачи

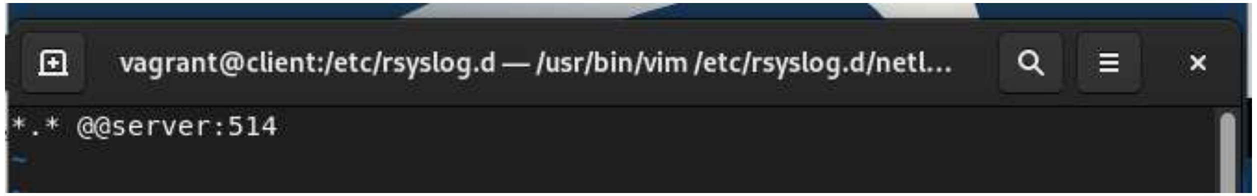
- Получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала



```
[root@server rsyslog.d]# vi /etc/rsyslog.d/netlog-server.conf
[root@server rsyslog.d]# systemctl restart rsyslog
[root@server rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
cupsd      690                          root    6u     IPv6             18574
     0t0          TCP localhost:ipp (LISTEN)
cupsd      690                          root    7u     IPv4             18575
     0t0          TCP localhost:ipp (LISTEN)
sshd       692                          root    3u     IPv4             18590
     0t0          TCP *:ssh (LISTEN)
sshd       692                          root    4u     IPv6             18611
     0t0          TCP *:ssh (LISTEN)
rsyslogd  3083                          root    4u     IPv4             33845
     0t0          TCP *:shell (LISTEN)
rsyslogd  3083                          root    5u     IPv6             33846
     0t0          TCP *:shell (LISTEN)
rsyslogd  3083 3084 in:imtcp            root    4u     IPv4             33845
     0t0          TCP *:shell (LISTEN)
rsyslogd  3083 3084 in:imtcp            root    5u     IPv6             33846
     0t0          TCP *:shell (LISTEN)
rsyslogd  3083 3086 in:imjour           root    4u     IPv4             33845
```

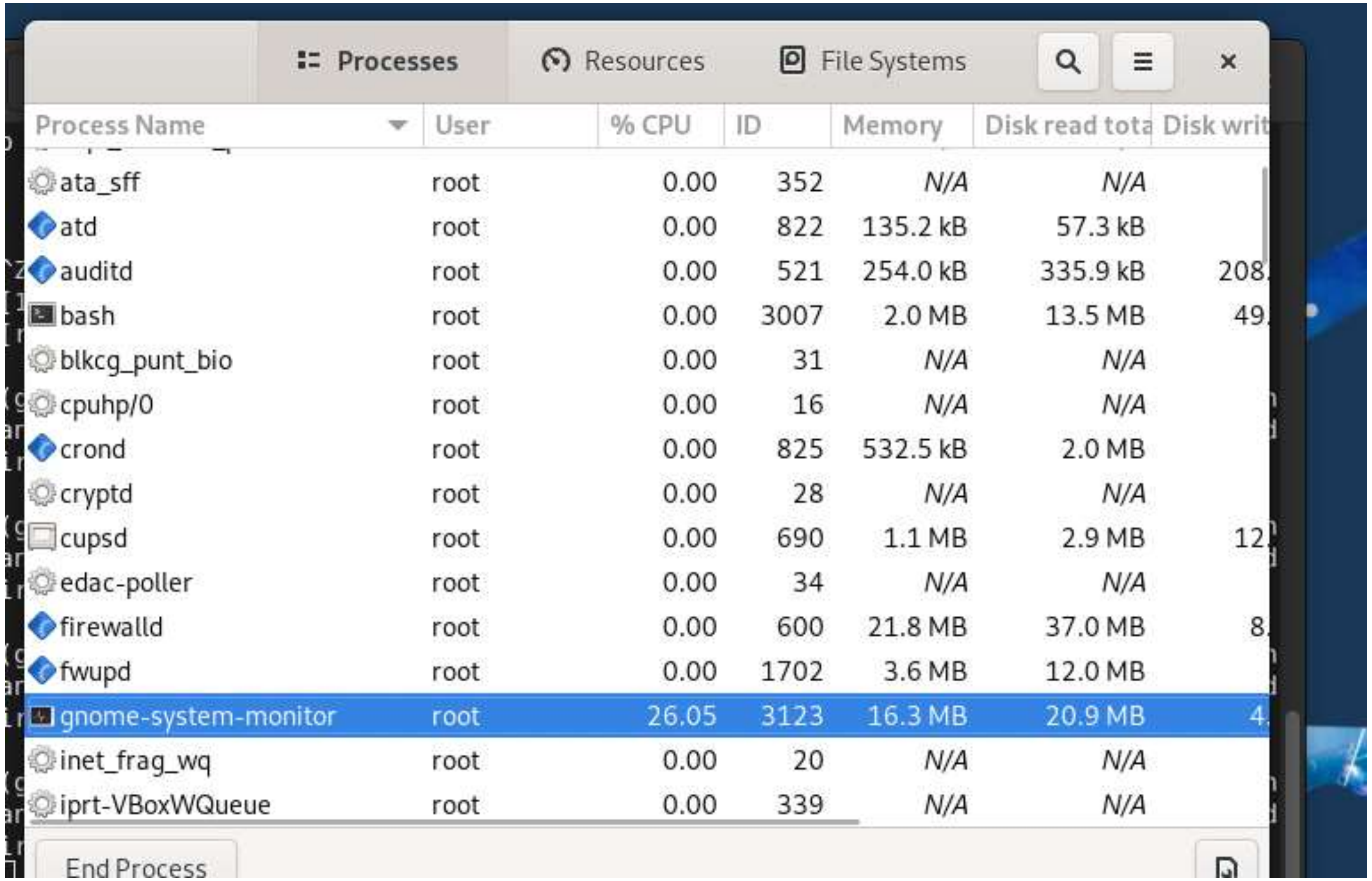
Настройка клиента сетевого журнала



vagrant@client:/etc/rsyslog.d — /usr/bin/vim /etc/rsyslog.d/netl...

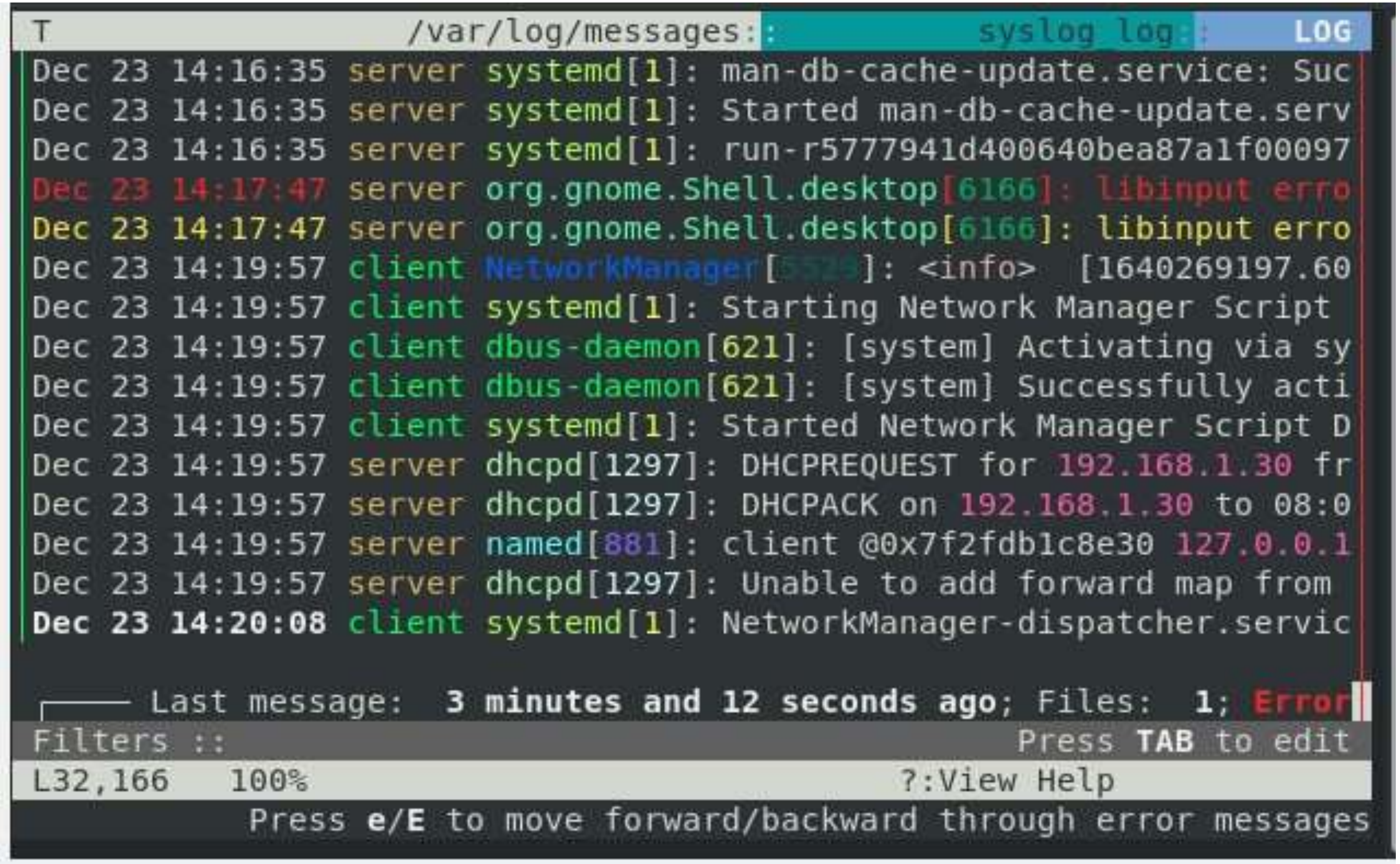
```
*.* @@server:514
~
```

Просмотр журнала



Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ
ata_sff	root	0.00	352	N/A	N/A	
atd	root	0.00	822	135.2 kB	57.3 kB	
auditd	root	0.00	521	254.0 kB	335.9 kB	208.
bash	root	0.00	3007	2.0 MB	13.5 MB	49.
blkcg_punt_bio	root	0.00	31	N/A	N/A	
cpuhp/0	root	0.00	16	N/A	N/A	
crond	root	0.00	825	532.5 kB	2.0 MB	
cryptd	root	0.00	28	N/A	N/A	
cupsd	root	0.00	690	1.1 MB	2.9 MB	12.
edac-poller	root	0.00	34	N/A	N/A	
firewalld	root	0.00	600	21.8 MB	37.0 MB	8.
fwupd	root	0.00	1702	3.6 MB	12.0 MB	
gnome-system-monitor	root	26.05	3123	16.3 MB	20.9 MB	4.
inet_frag_wq	root	0.00	20	N/A	N/A	
iprt-VBoxWQueue	root	0.00	339	N/A	N/A	

Просмотр журнала



```
 T                  /var/log/messages: :           syslog_log : :        LOG
 Dec 23 14:16:35 server systemd[1]: man-db-cache-update.service: Suc
 Dec 23 14:16:35 server systemd[1]: Started man-db-cache-update.serv
 Dec 23 14:16:35 server systemd[1]: run-r5777941d400640bea87a1f00097
 Dec 23 14:17:47 server org.gnome.Shell.desktop[6166]: libinput erro
 Dec 23 14:17:47 server org.gnome.Shell.desktop[6166]: libinput erro
 Dec 23 14:19:57 client NetworkManager[5529]: <info>  [1640269197.60
 Dec 23 14:19:57 client systemd[1]: Starting Network Manager Script
 Dec 23 14:19:57 client dbus-daemon[621]: [system] Activating via sy
 Dec 23 14:19:57 client dbus-daemon[621]: [system] Successfully acti
 Dec 23 14:19:57 client systemd[1]: Started Network Manager Script D
 Dec 23 14:19:57 server dhcpd[1297]: DHCPREQUEST for 192.168.1.30 fr
 Dec 23 14:19:57 server dhcpd[1297]: DHCPACK on 192.168.1.30 to 08:0
 Dec 23 14:19:57 server named[881]: client @0x7f2fdb1c8e30 127.0.0.1
 Dec 23 14:19:57 server dhcpd[1297]: Unable to add forward map from
 Dec 23 14:20:08 client systemd[1]: NetworkManager-dispatcher.servic

  ┌──── Last message:  3 minutes and 12 seconds ago; Files:  1; Error
 Filters ::                                            Press TAB to edit
 L32,166   100%                             ?:View Help
           Press e/E to move forward/backward through error messages
```

Вывод

- Получил навыки по работе с журналами системных событий.