

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №15

дисциплина: администрирование локальных подсистем

Студент:

Оулед салеи яссин

Группа: НПИбд-02-20

МОСКВА

2023г.

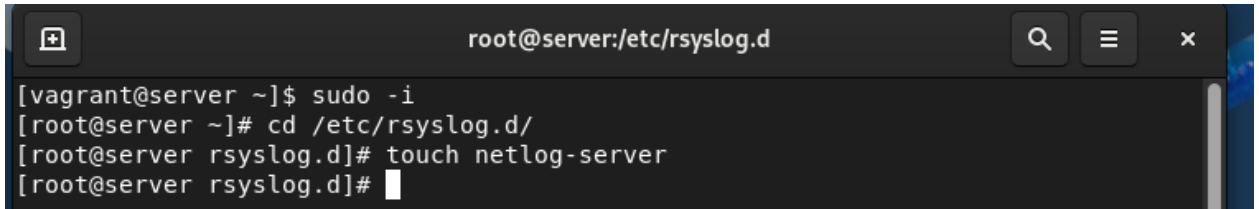
Постановка задачи

Получение навыков по работе с журналами системных событий.

Выполнение работы

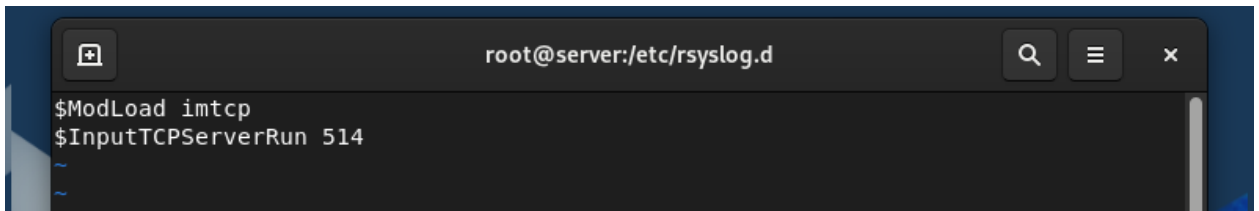
15.4.1. Настройка сервера сетевого журнала

1. На сервере создал файл конфигурации сетевого хранения журналов:



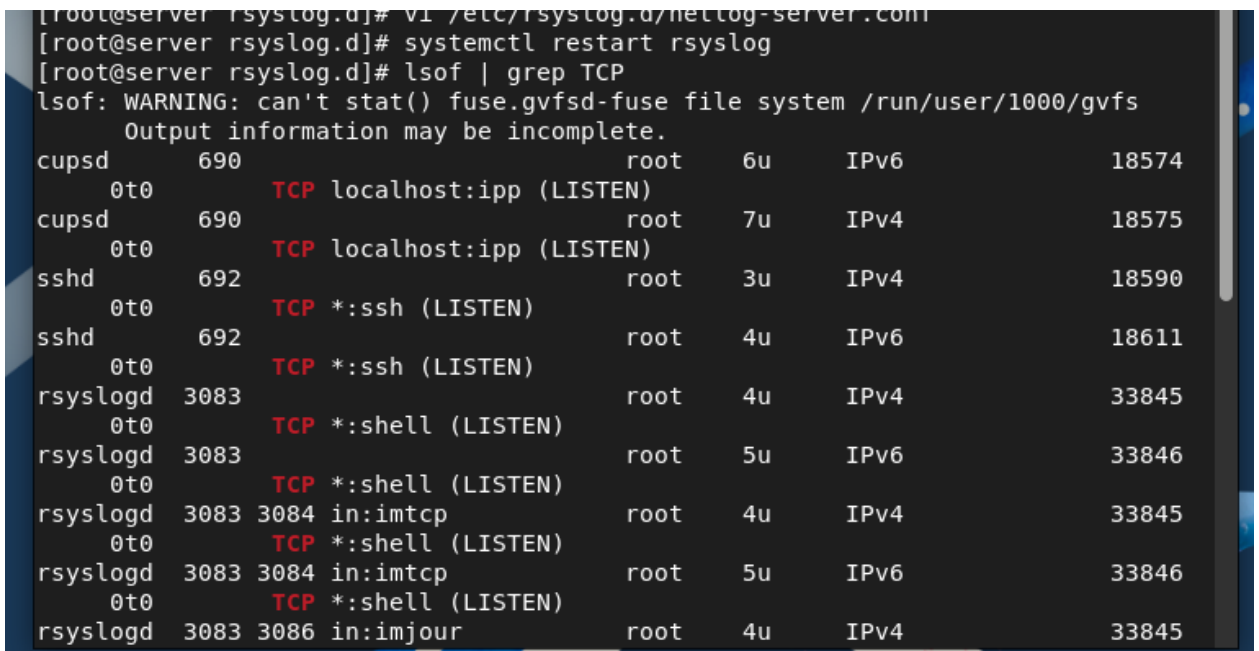
```
root@server:/etc/rsyslog.d
[vagrant@server ~]$ sudo -i
[root@server ~]# cd /etc/rsyslog.d/
[root@server rsyslog.d]# touch netlog-server
[root@server rsyslog.d]#
```

2. В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включил приём записей журнала по TCP-порту 514:



```
root@server:/etc/rsyslog.d
$ModLoad imtcp
$InputTCPServerRun 514
~
~
```

3. Перезапустил службу rsyslog и посмотрел, какие порты, связанные с rsyslog, прослушиваются:



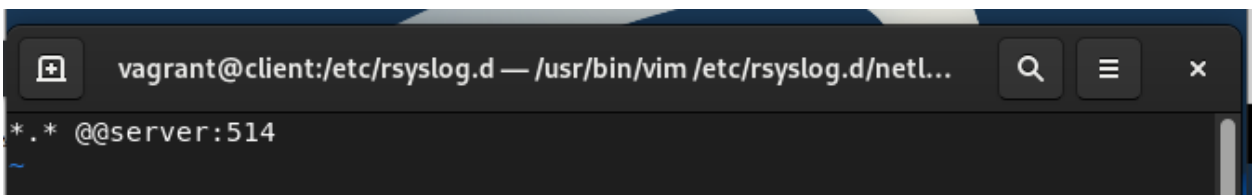
```
[root@server rsyslog.d]# vi /etc/rsyslog.d/netlog-server.conf
[root@server rsyslog.d]# systemctl restart rsyslog
[root@server rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
cupsd        690          root        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
```

4. На сервере настроил межсетевой экран для приёма сообщений по TCP-порту 514:

```
0t0 TCP *:shell (LISTEN)
[root@server rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server rsyslog.d]#
```

15.4.2. Настройка клиента сетевого журнала

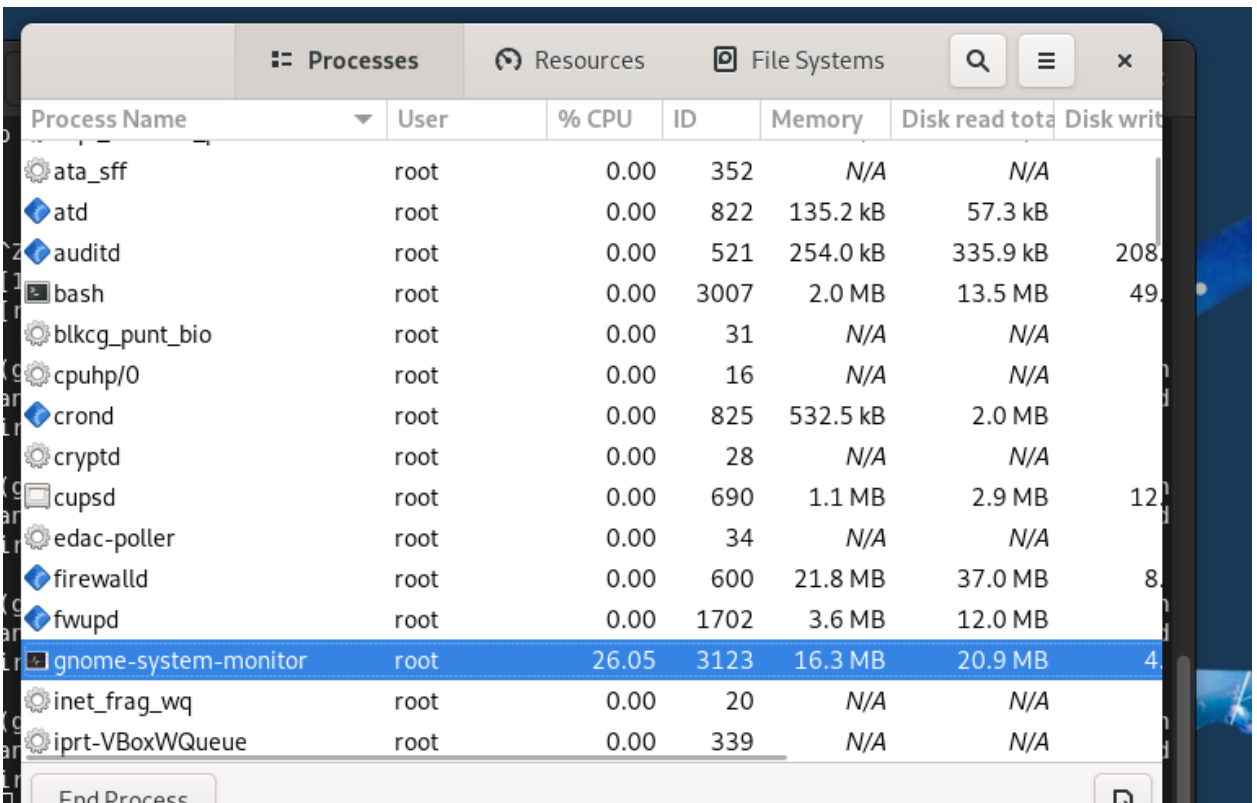
1. На клиенте создал файл конфигурации сетевого хранения журналов:
2. На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включил перенаправление сообщений журнала на 514 TCP-порт



3. Перезапустил службу rsyslog:

15.4.3. Просмотр журнала

1. На сервере просмотрел один из файлов журнала
2. На сервере под пользователем запустил графическую программу для просмотра журналов:



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
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	

3. На сервере установил просмотрщик журналов системных сообщений `lnav`:

4. Просмотрел логи с помощью lnav:

```
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 dhcpcd[1297]: DHCPREQUEST for 192.168.1.30 fr
Dec 23 14:19:57 server dhcpcd[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 dhcpcd[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.