

Лабораторная работа № 15

Настройка сетевого журналирования

Митрофанов Тимур Александрович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	13
	Список литературы	14

Список иллюстраций

3.1	Настройка сервера сетевого журнала	7
3.2	Настройка межсетевого экрана	8
3.3	настройка клиента	8
3.4	Просмотр журнала	9
3.5	Графическое окружение	9
3.6	lnav	10
3.7	Настройка запуска службы на сервере	11
3.8	Настройка запуска службы на клиенте	11
3.9	Вагрант для сервера	12
3.10	Вагрант для клиента	12

Список таблиц

1 Цель работы

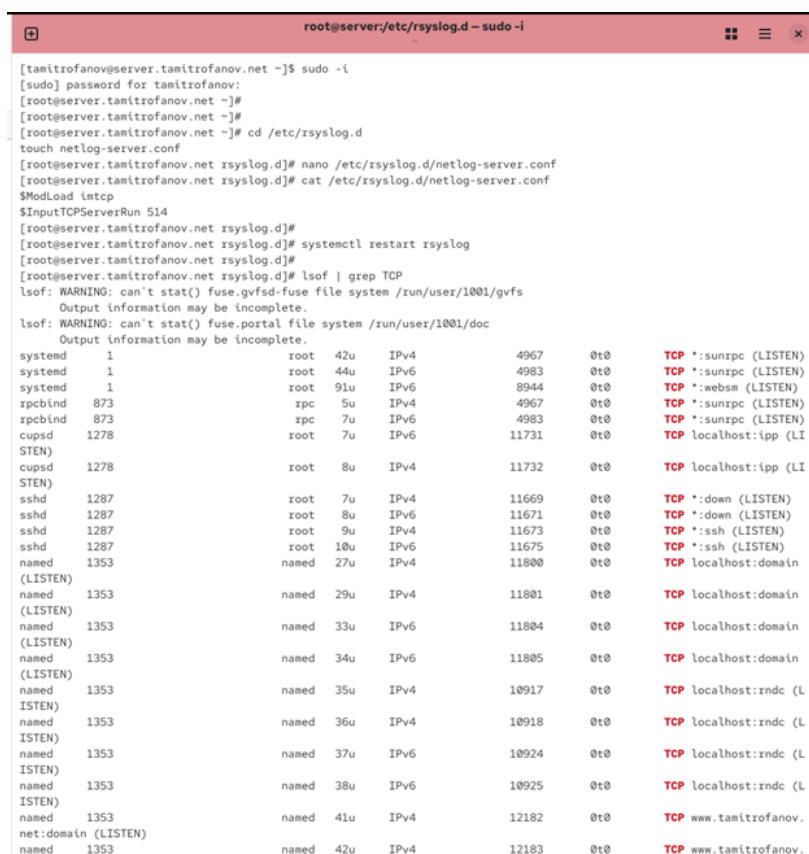
Получение навыков по работе с журналами системных событий.

2 Задание

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.
4. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования.

3 Выполнение лабораторной работы

На сервере создайте файл конфигурации сетевого хранения журналов. В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включите приём записей журнала по TCP-порту 514. Перезапустите службу `rsyslog` и посмотрите, какие порты, связанные с `rsyslog`, прослушиваются. (рис. 3.1)



```
root@server:/etc/rsyslog.d ~$ sudo -i
[tamitrofanov@server.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]# cd /etc/rsyslog.d
touch netlog-server.conf
[root@server.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-server.conf
[root@server.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
[root@server.tamitrofanov.net rsyslog.d]#
[root@server.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@server.tamitrofanov.net rsyslog.d]#
[root@server.tamitrofanov.net rsyslog.d]# ss -tlnp
ss: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
ss: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd 1 root 42u IPv4 4967 0t0 TCP *:sunrpc (LISTEN)
systemd 1 root 44u IPv6 4983 0t0 TCP *:sunrpc (LISTEN)
systemd 1 root 91u IPv6 8944 0t0 TCP *:websock (LISTEN)
rpcbind 873 rpc 5u IPv4 4967 0t0 TCP *:sunrpc (LISTEN)
rpcbind 873 rpc 7u IPv6 4983 0t0 TCP *:sunrpc (LISTEN)
cupsd 1278 root 7u IPv6 11731 0t0 TCP localhost:ipp (LISTEN)
cupsd 1278 root 8u IPv4 11732 0t0 TCP localhost:ipp (LISTEN)
sshd 1287 root 7u IPv4 11669 0t0 TCP *:down (LISTEN)
sshd 1287 root 8u IPv6 11671 0t0 TCP *:down (LISTEN)
sshd 1287 root 9u IPv4 11673 0t0 TCP *:ssh (LISTEN)
sshd 1287 root 10u IPv6 11675 0t0 TCP *:ssh (LISTEN)
named 1353 named 27u IPv4 11800 0t0 TCP localhost:domain (LISTEN)
named 1353 named 29u IPv4 11801 0t0 TCP localhost:domain (LISTEN)
named 1353 named 33u IPv6 11804 0t0 TCP localhost:domain (LISTEN)
named 1353 named 34u IPv6 11805 0t0 TCP localhost:domain (LISTEN)
named 1353 named 35u IPv4 10917 0t0 TCP localhost:rndc (LISTEN)
named 1353 named 36u IPv4 10918 0t0 TCP localhost:rndc (LISTEN)
named 1353 named 37u IPv6 10924 0t0 TCP localhost:rndc (LISTEN)
named 1353 named 38u IPv6 10925 0t0 TCP localhost:rndc (LISTEN)
named 1353 named 41u IPv4 12182 0t0 TCP www.tamitrofanov.net:domain (LISTEN)
named 1353 named 42u IPv4 12183 0t0 TCP www.tamitrofanov.net:domain (LISTEN)
```

Рисунок 3.1: Настройка сервера сетевого журнала

На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514

(рис. 3.2)

```
[root@server.tamitrofanov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
success
success
[root@server.tamitrofanov.net rsyslog.d]#
```

Рисунок 3.2: Настройка межсетевого экрана

На клиенте создайте файл конфигурации сетевого хранения журналов. На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включите перенаправление сообщений журнала на 514 TCP-порт сервера. Перезапустите службу `rsyslog`. (рис. 3.3)

```
root@client:/etc/rsyslog.d – sudo -i

[tamitrofanov@client.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]#
[root@client.tamitrofanov.net ~]# cd /etc/rsyslog.d
touch netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*. * @@server.user.net:514
[root@client.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@client.tamitrofanov.net rsyslog.d]#
[root@client.tamitrofanov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-client.conf
[root@client.tamitrofanov.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*. * @@server.tamitrofanov.net:514
[root@client.tamitrofanov.net rsyslog.d]# systemctl restart rsyslog
[root@client.tamitrofanov.net rsyslog.d]#
```

Рисунок 3.3: настройка клиента

На сервере просмотрите один из файлов журнала. (рис. 3.4).

```
root@server:/etc/rsyslog.d -- sudo -i

[root@server.tamitrofanov.net rsyslog.d]# tail -f /var/log/messages
Dec 13 18:19:13 client systemd[1]: Starting faupd-refresh.service - Refresh faupd metadata and update motd...
Dec 13 18:19:13 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:13 client systemd[1]: faupd-refresh.service: Deactivated successfully.
Dec 13 18:19:13 client systemd[1]: Finished faupd-refresh.service - Refresh faupd metadata and update motd.
Dec 13 18:19:13 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 27.
Dec 13 18:19:13 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:08 server NetworkManager[1257]: <info> [1765639148.8991] agent-manager: agent[ecfd71edce40a65:.1.85/or
g.gnome.Shell.NetworkAgent/1001]: agent registered
Dec 13 18:19:23 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:23 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 28.
Dec 13 18:19:23 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:33 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:34 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 29.
Dec 13 18:19:34 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:44 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:44 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 30.
Dec 13 18:19:44 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 18:19:54 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 18:19:54 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 31.
Dec 13 18:19:54 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

Рисунок 3.4: Просмотр журнала

3На сервере под пользователем user (вместо user укажите свой логин) запустите графическую программу для просмотра журналов (рис. 3.5).

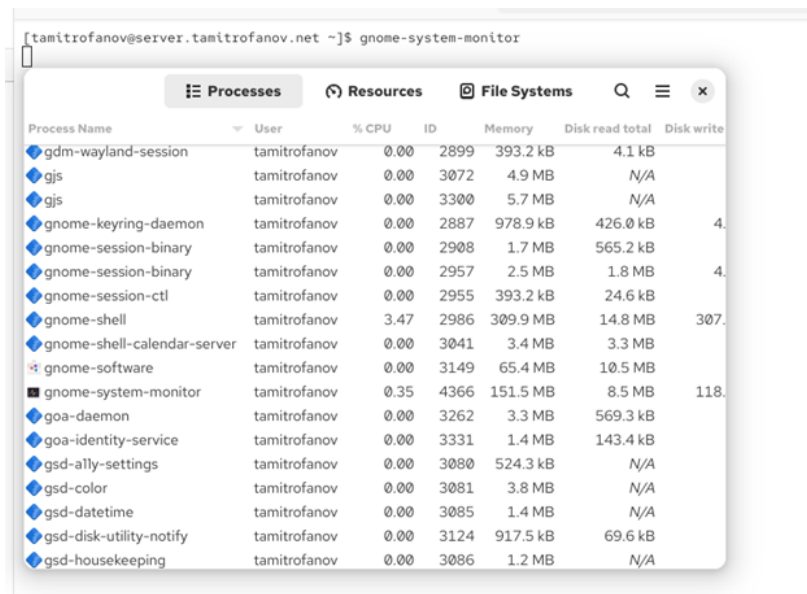
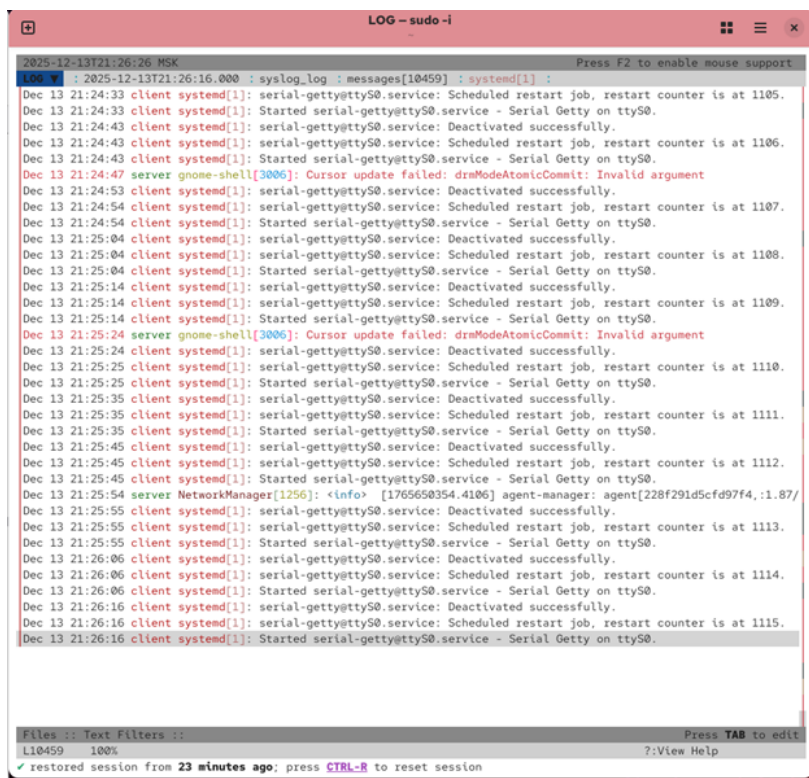


Рисунок 3.5: Графическое окружение

На сервере установите просмотрщик журналов системных сообщений lnav или его аналог. Просмотрите логи с помощью lnav или его аналога(рис. 3.6).



```
LOG - sudo -i
2025-12-13T21:26:26 MSK
2025-12-13T21:26:16.000 syslog_log : messages[10459] : systemd[1] :
Dec 13 21:24:33 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1105.
Dec 13 21:24:33 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:24:43 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:24:43 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1106.
Dec 13 21:24:43 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:24:47 server gnome-shell[3006]: Cursor update failed: drmModeAtomicCommit: Invalid argument
Dec 13 21:24:53 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:24:54 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1107.
Dec 13 21:24:54 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:04 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:04 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1108.
Dec 13 21:25:04 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:14 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:14 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1109.
Dec 13 21:25:14 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:24 server gnome-shell[3006]: Cursor update failed: drmModeAtomicCommit: Invalid argument
Dec 13 21:25:24 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:25 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1110.
Dec 13 21:25:25 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:35 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:35 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1111.
Dec 13 21:25:35 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:45 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:45 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1112.
Dec 13 21:25:45 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:25:54 server NetworkManager[1256]: <info> [1765658354.4106] agent-manager: agent[228f291d5cfd97f4,1.87/
Dec 13 21:25:55 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:25:55 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1113.
Dec 13 21:25:55 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:26:06 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:26:06 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1114.
Dec 13 21:26:06 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 13 21:26:16 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 13 21:26:16 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 1115.
Dec 13 21:26:16 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.

Files :: Text Filters ::
L10459 100%
restored session from 23 minutes ago; press CTRL-R to reset session
Press TAB to edit
?:View Help
```

Рисунок 3.6: lnava

На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы

В каталоге `/vagrant/provision/server` создайте исполняемый файл `netlog.sh`

Открыв его на редактирование, пропишите в нём следующий скрипт (рис. 3.7).

```
[root@server.tamitrofanov.net lnnav-0.13.2]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.tamitrofanov.net server]# cd /vagrant/provision/server
touch netlog.sh
chmod +x netlog.sh
[root@server.tamitrofanov.net server]# nano netlog.sh
[root@server.tamitrofanov.net server]# cat netlog.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent

echo "Start rsyslog service"
systemctl restart rsyslog
[root@server.tamitrofanov.net server]#
```

Рисунок 3.7: Настройка запуска службы на сервере

На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создайте в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы

В каталоге /vagrant/provision/client создайте исполняемый файл netlog.sh

Открыв его на редактирование, пропишите в нём следующий скрипт(рис. 3.8).

```
root@client:/vagrant/provision/client -- sudo -i

[root@client.tamitrofanov.net rsyslog.d]# cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.tamitrofanov.net client]# cd /vagrant/provision/client
touch netlog.sh
chmod +x netlog.sh
[root@client.tamitrofanov.net client]# nano netlog.sh
[root@client.tamitrofanov.net client]# cat netlog.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install lnnav

echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc

echo "Start rsyslog service"
systemctl restart rsyslog
[root@client.tamitrofanov.net client]#
```

Рисунок 3.8: Настройка запуска службы на клиенте

Для отработки созданных скриптов во время загрузки виртуальных машин server

(рис. 3.9) и client (рис. 3.10) в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента

```
132     server.vm.provision "server netlog",  
133         type: "shell",  
134         preserve_order: true,  
135         path: "provision/server/netlog.sh"  
136
```

Рисунок 3.9: Вагрант для сервера

```
client.vm.provision "client netlog",  
    type: "shell",  
    preserve_order: true,  
    path: "provision/client/netlog.sh"
```

Рисунок 3.10: Вагрант для клиента

4 Выводы

Сегодня я получил навыки по работе с журналами системных событий.

Список литературы