

# Презентация по лабораторной работе №15

Администрирование сетевых подсистем

true

2025-12-02

## Вводная часть

### Цель работы

Целью данной работы получить навыки по работе с журналами системных событий.

### Задание

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

## Выполнение лабораторной работы

### Настройка сервера сетевого журнала

Загрузили нашу операционную систему и перешли в рабочий каталог с проектом: `cd /var/tmp/tbmanturov/vagrant`

### Настройка сервера сетевого журнала

Запустили виртуальную машину server: `make server-up`

### Настройка сервера сетевого журнала

Далее на виртуальной машине server вошли под созданным нами пользователем и открыли терминал. Перешли в режим суперпользователя: `sudo -i`

### Настройка сервера сетевого журнала

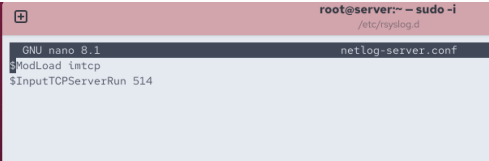
На сервере создали файл конфигурации сетевого хранения журналов ([рис. @fig-004]):

```
[tbmanturov@server.tbmanturov.net ~]$ cd /etc/rsyslog.d
[tbmanturov@server.tbmanturov.net rsyslog.d]$ touch netlog-server.conf
touch: cannot touch 'netlog-server.conf': Permission denied
[tbmanturov@server.tbmanturov.net rsyslog.d]$ sudo -i
[sudo] password for tbmanturov:
[root@server.tbmanturov.net ~]# touch netlog-server.conf
```

Создание файла /etc/rsyslog.d/netlog-server.conf на server

## Настройка сервера сетевого журнала

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включили приём записей журнала по TCP-порту 514 (рис. @fig-005):



```
root@server:~ -- sudo -i
/etc/rsyslog.d
GNU nano 8.1 netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Редактирование файла /etc/rsyslog.d/netlog-server.conf на server

## Настройка сервера сетевого журнала

Перезапустили службу rsyslog на сервере: systemctl restart rsyslog (рис. @fig-006)

```
[root@server.tbmanturov.net ~]# systemctl restart rsyslog
[root@server.tbmanturov.net ~]# ^C
[root@server.tbmanturov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/door
Output information may be incomplete.
systemd 1 root 42u IPv4 0003 0t0 TCP *sunrpc (LISTEN)
systemd 1 root 44u IPv6 5389 0t0 TCP *sunrpc (LISTEN)
systemd 1 root 93u IPv6 6906 0t0 TCP *websockets (LISTEN)
rpcbind 911 rpc 5u IPv4 5003 0t0 TCP *sunrpc (LISTEN)
rpcbind 911 rpc 7u IPv6 5389 0t0 TCP *sunrpc (LISTEN)
cupsd 1376 root 7u IPv6 12638 0t0 TCP localhost:ipp (LISTEN)
cupsd 1376 root 8u IPv4 12639 0t0 TCP localhost:ipp (LISTEN)
sshd 1391 root 7u IPv4 18779 0t0 TCP *down (LISTEN)
sshd 1391 root 8u IPv6 18781 0t0 TCP *down (LISTEN)
sshd 1391 root 9u IPv4 18783 0t0 TCP *ssh (LISTEN)
sshd 1391 root 10u IPv6 18785 0t0 TCP *ssh (LISTEN)
named 1588 named 45u IPv4 13431 0t0 TCP localhost:domain (LISTEN)
named 1588 named 46u IPv4 13431 0t0 TCP localhost:domain (LISTEN)
```

Перезапуск службы rsyslog на server

## Настройка сервера сетевого журнала

Посмотрели, какие порты, связанные с rsyslog, прослушиваются: lsof | grep TCP (рис. @fig-007)

```
[root@server.tbmanturov.net ~]# systemctl restart rsyslog
[root@server.tbmanturov.net ~]# ^C
[root@server.tbmanturov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/door
Output information may be incomplete.
systemd 1 root 42u IPv4 0003 0t0 TCP *sunrpc (LISTEN)
systemd 1 root 44u IPv6 5389 0t0 TCP *sunrpc (LISTEN)
systemd 1 root 93u IPv6 6906 0t0 TCP *websockets (LISTEN)
rpcbind 911 rpc 5u IPv4 5003 0t0 TCP *sunrpc (LISTEN)
rpcbind 911 rpc 7u IPv6 5389 0t0 TCP *sunrpc (LISTEN)
cupsd 1376 root 7u IPv6 12638 0t0 TCP localhost:ipp (LISTEN)
cupsd 1376 root 8u IPv4 12639 0t0 TCP localhost:ipp (LISTEN)
sshd 1391 root 7u IPv4 18779 0t0 TCP *down (LISTEN)
sshd 1391 root 8u IPv6 18781 0t0 TCP *down (LISTEN)
sshd 1391 root 9u IPv4 18783 0t0 TCP *ssh (LISTEN)
sshd 1391 root 10u IPv6 18785 0t0 TCP *ssh (LISTEN)
named 1588 named 45u IPv4 13431 0t0 TCP localhost:domain (LISTEN)
named 1588 named 46u IPv4 13431 0t0 TCP localhost:domain (LISTEN)
```

Просмотр прослушиваемых портов связанных с rsyslog

## Настройка сервера сетевого журнала

На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514 (рис. @fig-008):

```
[root@server.tbmanturov.net ~]# firewall-cmd --add-port=514/tcp
Warning: ALREADY_ENABLED: 514:tcp already in 'public'
success
[root@server.tbmanturov.net ~]# firewall-cmd --add-port=514/tcp --permanent
Warning: ALREADY_ENABLED: 514:tcp
success
[root@server.tbmanturov.net ~]#
```

Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

# Настройка клиента сетевого журнала

Запустили виртуальную машину client: make client-up ([рис. @fig-009])

# Настройка клиента сетевого журнала

Далее на виртуальной машине client вошли под созданным нами пользователем и открыли терминал. Перешли в режим суперпользователя: sudo -i ([рис. @fig-010])

# Настройка клиента сетевого журнала

На клиенте создали файл конфигурации сетевого хранения журналов ([рис. @fig-011]):

```
[root@client.tbmanturov.net ~]# cd /etc/rsyslog.d
[root@client.tbmanturov.net rsyslog.d]# touch netlog-client.conf
[root@client.tbmanturov.net rsyslog.d]#
```

Создание файла /etc/rsyslog.d/netlog-client.conf на client

# Настройка клиента сетевого журнала

На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включили перенаправление сообщений журнала на 514 TCP-порт сервера: \*.\* @server.tbmanturov.net:514 ([рис. @fig-012])

```
### netlog-client.conf
#
# @server.tbmanturov.net:514
```

Редактирование файла /etc/rsyslog.d/netlog-client.conf на client

# Просмотр журнала

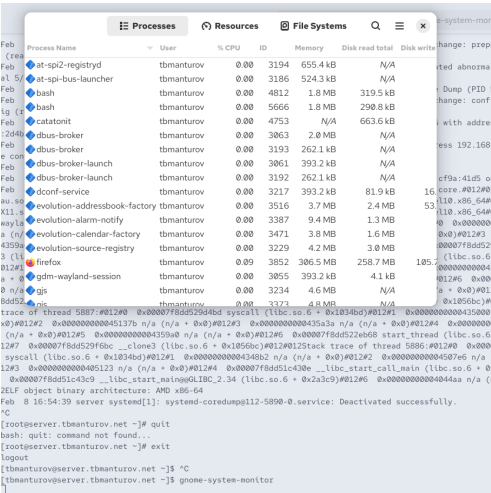
На сервере посмотрели один из файлов журнала: tail -f /var/log/messages ([рис. @fig-014])

```
[root@server.tbmanturov.net ~]# tail -f /var/log/messages
Feb  8 16:53:58 server systemd-logind[588]: Existing logind session ID 3 used by new audit session, ignoring.
Feb  8 16:53:58 server systemd-logind[588]: New session c3 of user root.
Feb  8 16:53:58 server systemd[1]: Started session-c3.scope - Session c3 of user root.
Feb  8 16:53:58 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Feb  8 16:53:58 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Feb  8 16:53:52 server kernel: traps: VBoxClient[5781] trap int3 ip:41dc5b sp:7f8dc6880a0b error:0 in VBoxClient[1dc5
b,400000-1dc600]
Feb  8 16:53:52 server systemd-coredump[5782]: Process 5778 (VBoxClient) of user 1001 terminated abnormally with signa
l 5/7TRAP, processing...
Feb  8 16:53:52 server systemd[1]: Started systemd-coredump[5782-0.service - Process Core Dump (PID 5782/UID 0)].
Feb  8 16:53:53 server systemd-coredump[5783]: Process 5778 (VBoxClient) of user 1001 dumped core:#0129012Module libX
au.so.6 from rpe libXau-1.0.11-8.el10.x86_64012Module libxcb.so.1 from rpe libxcb-1.17.0-3.el10.x86_64012Module lib
X11.so.6 from rpe libX11-1.8.10-1.el10.x86_64012Module libffi.so.8 from rpe libffi-3.4.4-9.el10.x86_64012Module lib
wayland-client.so.0 from rpe wayland-1.23.0-2.el10.x86_64012Stack trace of thread 5781.#012900 @0000000000000000 n/a
(n/a) * 0x0#01291 @000000000041d0d4 n/a (n/a) * 0x0#01292 @000000000045805c n/a (n/a) * 0x0#01293 @00000000000
4550b n/a (n/a) * 0x0#01294 @000007f8dc51c58e start_thread (libc.so.6 * 0x0#02)0#01295 @000007f8dc519f0c _clone
3 (libc.so.6 * 0x1856dc)0#0129612Stack trace of thread 5778.#01290 @000007f8dc519f0c syscall (libc.so.6 * 0x1856dc)0#
01291 @0000000000434032 n/a (n/a) * 0x0#01292 @00000000004507a6 n/a (n/a) * 0x0#01293 @0000000000405123 n/a (n/
a) * 0x0#01294 @000007f8dc51c58e _libc_start_call_main (libc.so.6 * 0x0a30)0#01295 @000007f8dc51c5c9 _libc_star
t_main@GLIBC_2.34 (libc.so.6 * 0x2a3c9)0#01296 @00000000004044aa n/a (n/a) * 0x0#01297 @0000000000000000 object binary architecture:
AMD x86_64
Feb  8 16:53:53 server systemd[1]: systemd-coredump[5782-0.service: Deactivated successfully.
Feb  8 16:53:58 server kernel: traps: VBoxClient[5883] trap int3 ip:41dc5b sp:7f8dc6880a0b error:0 in VBoxClient[1dc5
b,400000-1dc600]
Feb  8 16:53:58 server systemd-coredump[5884]: Process 5880 (VBoxClient) of user 1001 terminated abnormally with signa
l 5/7TRAP, processing...
Feb  8 16:53:58 server systemd[1]: Started systemd-coredump[5884-0.service - Process Core Dump (PID 5884/UID 0)].
Feb  8 16:53:58 server systemd-coredump[5885]: Process 5880 (VBoxClient) of user 1001 dumped core:#0129012Module libX
au.so.6 from rpe libXau-1.0.11-8.el10.x86_64012Module libxcb.so.1 from rpe libxcb-1.17.0-3.el10.x86_64012Module lib
X11.so.6 from rpe libX11-1.8.10-1.el10.x86_64012Module libffi.so.8 from rpe libffi-3.4.4-9.el10.x86_64012Module lib
wayland-client.so.0 from rpe wayland-1.23.0-2.el10.x86_64012Stack trace of thread 5883.#012900 @0000000000000000 n/a
(n/a) * 0x0#01291 @000000000041d0d4 n/a (n/a) * 0x0#01292 @000000000045805c n/a (n/a) * 0x0#01293 @00000000000
4550b n/a (n/a) * 0x0#01294 @000007f8dc51c58e start_thread (libc.so.6 * 0x0#02)0#01295 @000007f8dc519f0c _clone
3 (libc.so.6 * 0x1856dc)0#0129612Stack trace of thread 5778.#01290 @000007f8dc519f0c syscall (libc.so.6 * 0x1856dc)0#
01291 @0000000000434032 n/a (n/a) * 0x0#01292 @00000000004507a6 n/a (n/a) * 0x0#01293 @0000000000405123 n/a (n/
a) * 0x0#01294 @000007f8dc51c58e _libc_start_call_main (libc.so.6 * 0x0a30)0#01295 @000007f8dc51c5c9 _libc_star
t_main@GLIBC_2.34 (libc.so.6 * 0x2a3c9)0#01296 @00000000004044aa n/a (n/a) * 0x0#01297 @0000000000000000 object binary architecture:
AMD x86_64
```

Просмотр одного из файлов журнала на server

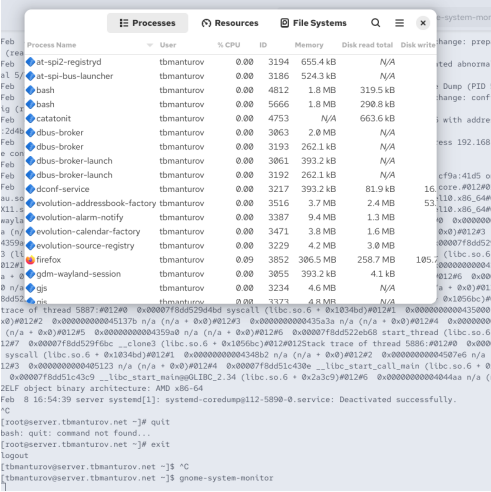
# Просмотр журнала

На сервере под пользователем tbmanturov запустили графическую программу для просмотра журналов: gnome-system-monitor ([рис. @fig-015]), ([рис. @fig-016])



Запуск графической программы для просмотра журналов

# Просмотр журнала



Просмотра журналов в графической программе gnome-system-monitor

# Просмотр журнала

На сервере установили просмотрщик журналов системных сообщений lnav.

```
[root@server.tbmanturov.net ~]# dnf -y install lnav
```

Установка lnav на server (1)

# Просмотр журнала

Далее посмотрели логи с помощью lnav: lnav ([рис. @fig-022])



```
[root@server.tbmanturov.net server]# touch netlog.sh
[root@server.tbmanturov.net server]# chmod +x netlog.sh
[root@server.tbmanturov.net server]# nano netlog.sh
[root@server.tbmanturov.net server]#
```

Создание исполняемого файла netlog.sh на сервере

## Внесение изменений в настройки внутреннего окружения виртуальной машины

Открыв его на редактирование, прописали в нём следующий скрипт ([рис. @fig-027]):

```
GNU nano 8.1 netlog.sh
#!/bin/bash
echo "Provisioning script 50"
echo "Copy configuration files"
cp -R /vagrant/provision/servez/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
```

Редактирование файла netlog.sh на сервере

## Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине client перешли в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/ и создали в нём каталог netlog, в который поместили в соответствующие подкаталоги конфигурационные файлы ([рис. @fig-028]):

```
[root@client.tbmanturov.net ~]# cd /vagrant/provision/client
[root@client.tbmanturov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.tbmanturov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.tbmanturov.net client]#
```

Копирование конфигурационных файлов в каталог netlog на клиенте

## Внесение изменений в настройки внутреннего окружения виртуальной машины

В каталоге /vagrant/provision/client/ создали исполняемый файл netlog.sh ([рис. @fig-029]):

```
[root@client.tbmanturov.net client]# touch netlog.sh
[root@client.tbmanturov.net client]# chmod +x netlog.sh
[root@client.tbmanturov.net client]#
```

Создание исполняемого файла netlog.sh на клиенте

## Внесение изменений в настройки внутреннего окружения виртуальной машины

Открыв его на редактирование, прописали в нём следующий скрипт ([рис. @fig-030]):

```
GNU nano 8.1 netlog.sh
#!/bin/bash
echo "Provisioning script 50"
echo "Install needed packages"
dnf -y install lnav
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog
```

Редактирование файла netlog.sh на клиенте

## Внесение изменений в настройки внутреннего окружения виртуальной машины

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента ([рис. @fig-031]), ([рис. @fig-032]):

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

Редактирование файла Vagrantfile (1)

## Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Редактирование файла Vagrantfile (2)

## Внесение изменений в настройки внутреннего окружения виртуальной машины

После этого можно выключать виртуальные машины server и client: make server-halt и make client-halt ([рис. @fig-033])

## Подведение итогов

### Выводы

В ходе выполнения лабораторной работы №15 мы получили навыки по работе с журналами системных событий.

### Список литературы

1. Лабораторная работа №15