

Лабораторная работа №15

Администрирование сетевых подсистем

Иванов Сергей Владимирович, НПИбд-01-23

03 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получение навыков по работе с журналами системных событий.

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

Выполнение лабораторной работы

Настройка сервера сетевого журнала

Запускаю виртуальную машину Server. (рис. 1)

```
C:\work_asp\svivanov\vagrant>vagrant halt server

C:\work_asp\svivanov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
```

Рис. 1: Запуск Server

На сервере создадим файл конфигурации сетевого хранения журналов:

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

Рис. 2: Создание конф. файла

Настройка сервера сетевого журнала

В файле конфигурации включим приём записей журнала по TCP-порту 514:

```
$ModLoad imtcp  
$InputTCPServerRun 514
```

~

Рис. 3: Редактирование конф. файла

Настройка сервера сетевого журнала

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются:

```
rsyslogd 13438 root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13440 in:imjour root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13440 in:imjour root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13441 in:imtcp root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13441 in:imtcp root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13442 in:imtcp root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13442 in:imtcp root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13443 in:imtcp root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13443 in:imtcp root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13444 rs:main root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13444 rs:main root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13445 in:imtcp root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13445 in:imtcp root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13446 in:imtcp root 4u IPv4 45592 0t0 TCP *:shell (LISTEN)
rsyslogd 13438 13446 in:imtcp root 5u IPv6 45593 0t0 TCP *:shell (LISTEN)
[root@server.svivanov.net rsyslog.d]#
```

Рис. 4: Просмотр портов связанных с rsyslog

Настройка сервера сетевого журнала

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

Рис. 5: Настройка firewall

Запускаю виртуальную машину Client. (рис. 6)

```
C:\work_asp\svivanov\vagrant>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
        client: Adapter 1: nat
        client: Adapter 2: intnet
==> client: Forwarding ports...
```

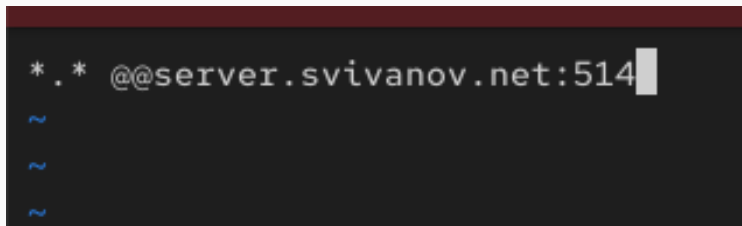
Рис. 6: Запуск Client

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

Рис. 7: Создание конф.файла

Настройка клиента сетевого журнала

На клиенте в файле конфигурации включим перенаправление сообщений на 514 сервера:

A screenshot of a terminal window with a dark background and a maroon title bar. The terminal shows a configuration file being edited. The first line is `*.* @@server.svivanov.net:514` with a white cursor at the end. The next three lines each start with a blue tilde `~`.

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

Рис. 8: Редактирование конф. файла

```
[root@client.svivanov.net rsyslog.d]# systemctl restart rsyslog  
[root@client.svivanov.net rsyslog.d]# █
```

Рис. 9: Перезапуск службы

На сервере посмотрим один из файлов журнала

```
[root@server.svivanov.net rsyslog.d]# tail -f /var/log/messages
Dec 3 09:41:08 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 53.
Dec 3 09:41:08 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:18 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:18 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 54.
Dec 3 09:41:18 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:28 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:29 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 55.
Dec 3 09:41:29 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 09:41:34 server named[1334]: timed out resolving 'mirrors.fedoraproject.org/A/IN': 127.0.0.1#53
Dec 3 09:41:34 server named[1334]: timed out resolving 'mirrors.fedoraproject.org/AAAA/IN': 127.0.0.1#53
Dec 3 09:41:39 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 09:41:39 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 56.
Dec 3 09:41:39 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
```

Рис. 10: Просмотр файла журнала

На сервере под запуским графическую программу для просмотра журналов

Процессы									
Имя процесса	Пользователь	% ЦП	ID	Память	Суммарное чте	Суммарная зап	Чтение диска	Запись диска	Приоритет
gnome-system-monitor	svivanov	7,37	14369	197,4 MB	10,7 MB	172,0 kB	16,0 KiB/c	Н/Д	Обычный
gnome-shell	svivanov	3,81	11367	278,0 MB	12,8 MB	155,6 kB	Н/Д	Н/Д	Обычный
ptysis	svivanov	0,51	13176	249,7 MB	9,5 MB	815,1 kB	Н/Д	Н/Д	Обычный
firefox	svivanov	0,00	12328	257,4 MB	230,1 MB	86,4 MB	Н/Д	Н/Д	Обычный
Web Content	svivanov	0,00	12705	13,6 MB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
Web Content	svivanov	0,00	12641	13,5 MB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
dbus-broker	svivanov	0,00	11286	2,0 MB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
at-spi2-registrd	svivanov	0,00	11421	655,4 kB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
at-spi-bus-launcher	svivanov	0,00	11413	524,3 kB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
bash	svivanov	0,00	13252	2,0 MB	761,9 kB	Н/Д	Н/Д	Н/Д	Обычный
catatonit	svivanov	0,00	13204	Н/Д	663,6 kB	Н/Д	Н/Д	Н/Д	Обычный
dbus-broker	svivanov	0,00	11420	262,1 kB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
dbus-broker-launch	svivanov	0,00	11280	393,2 kB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
dbus-broker-launch	svivanov	0,00	11419	262,1 kB	Н/Д	Н/Д	Н/Д	Н/Д	Обычный
evolution-addressbook-factory	svivanov	0,00	11756	3,8 MB	2,3 MB	53,2 kB	Н/Д	Н/Д	Обычный

```
root@server.svivanov.net rsyslog.d]#  
root@server.svivanov.net rsyslog.d]#  
root@server.svivanov.net rsyslog.d]# logout  
svivanov@server.svivanov.net ~]$ gnome-system-monitor
```

Рис. 11: Запуск программы для просмотра журналов

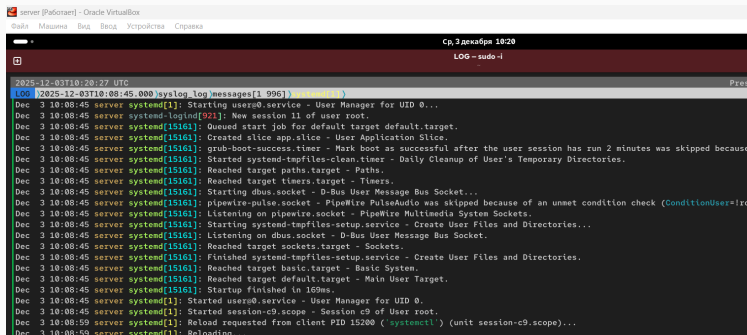
На сервере установим просмотрщик журналов системных сообщений lnav:

```
[svivanov@server.svivanov.net ~]$ sudo dnf -y install lnav
Last metadata expiration check: 0:00:06 ago on Cp 03 дек 2025 10:09:10.
Dependencies resolved.
=====
Package                Architecture          Version               Repository            Size
=====
Installing:
lnav                   x86_64                0.11.1-1.el9         epel                  2.4 M
Transaction Summary
=====
Install 1 Package

Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
lnav-0.11.1-1.el9.x86_64.rpm                                5.7 MB/s | 2.4 MB    00:00
-----
Total                                                         2.4 MB/s | 2.4 MB    00:00
Extra Packages for Enterprise Linux 9 - x86_64              1.6 MB/s | 1.6 kB    00:00
Importing GPG key 0x3228467C:
Usrid      : "Fedora (epel9) (epel@fedoraproject.org)"
```

Рис. 12: Установка lnav

Просмотр логов с помощью lnav на сервере:



```
server [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Вклад  Устройства  Справка
[ ]
Ср, 3 декабря 10:20
LOG ~ sudo -i
2025-12-03T10:20:27 UTC
[00] 2025-12-03T10:08:45.000 syslog log messages[1 996] systemd[1]
Dec 3 10:08:45 server systemd[1]: Starting user@0.service - User Manager for UID 0...
Dec 3 10:08:45 server systemd-logind[921]: New session 11 of user root.
Dec 3 10:08:45 server systemd[15161]: Queued start job for default target default.target.
Dec 3 10:08:45 server systemd[15161]: Created slice app.slice - User Application Slice.
Dec 3 10:08:45 server systemd[15161]: grub-boot-success.timer - Mark boot as successful after the user session has run 2 minutes was skipped because
Dec 3 10:08:45 server systemd[15161]: Started systemd-tmpfiles-clean.timer - Daily Cleanup of User's Temporary Directories.
Dec 3 10:08:45 server systemd[15161]: Reached target paths.target - Paths.
Dec 3 10:08:45 server systemd[15161]: Reached target timers.target - Timers.
Dec 3 10:08:45 server systemd[15161]: Starting dbus.socket - D-Bus User Message Bus Socket...
Dec 3 10:08:45 server systemd[15161]: pipewire-pulse.socket - PipeWire PulseAudio was skipped because of an unmet condition check (ConditionUser=ro
Dec 3 10:08:45 server systemd[15161]: Listening on pipewire.socket - PipeWire Multimedia System Sockets.
Dec 3 10:08:45 server systemd[15161]: Starting systemd-tmpfiles-setup.service - Create User Files and Directories...
Dec 3 10:08:45 server systemd[15161]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Dec 3 10:08:45 server systemd[15161]: Reached target sockets.target - Sockets.
Dec 3 10:08:45 server systemd[15161]: Finished systemd-tmpfiles-setup.service - Create User Files and Directories.
Dec 3 10:08:45 server systemd[15161]: Reached target basic.target - Basic System.
Dec 3 10:08:45 server systemd[15161]: Reached target default.target - Main User Target.
Dec 3 10:08:45 server systemd[15161]: Startup finished in 169ms.
Dec 3 10:08:45 server systemd[1]: Started user@0.service - User Manager for UID 0.
Dec 3 10:08:45 server systemd[1]: Started session-c9.scope - Session c9 of user root.
Dec 3 10:08:59 server systemd[1]: Reload requested from client PID 15200 ('systemctl') (unit session-c9.scope)...
Dec 3 10:08:59 server systemd[1]: Reloading...
```

Рис. 13: Просмотр логов

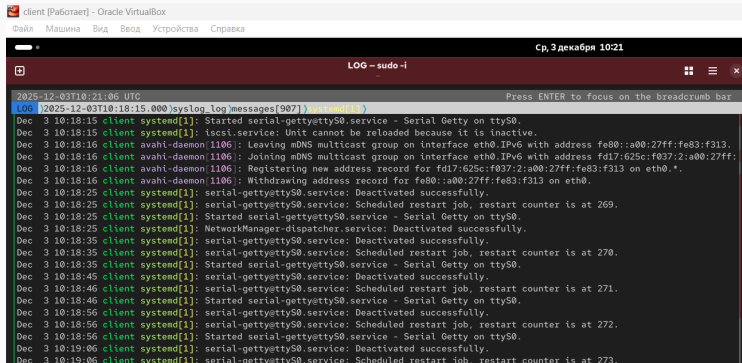
На клиенте установим просмотрщик журналов системных сообщений lnav:

```
[root@client.svivanov.net rsyslog.d]# dnf install -y lnav
Extra Packages for Enterprise Linux 9 - x86_64                2.4 MB/s | 5.9 MB    00:02
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64 878 B/s | 1.7 kB    00:01
Зависимости разрешены.
=====
Пакет                Архитектура          Версия                Репозиторий           Размер
=====
Установка:
lnav                 x86_64               0.11.1-1.el9         epel                   2.4 М
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 2.4 М
Объем изменений: 6.1 М
Загрузка пакетов:
lnav-0.11.1-1.el9.x86_64.rpm                    5.5 MB/s | 2.4 MB    00:00
```

Рис. 14: Установка lnav

Просмотр логов с помощью lnav на клиенте: (рис. 15)



The screenshot shows a terminal window titled "client [Работает] - Oracle VirtualBox" with a menu bar (Файл, Машина, Вид, Ввод, Устройства, Справка). The terminal displays the output of the command "LOG - sudo -i". The output shows a list of log messages from the system journal, including messages about the serial-getty@ttyS0.service, avahi-daemon, and NetworkManager-dispatcher.service. The messages are color-coded: "client" is green, "systemd[1]" is blue, and the log level "Dec 3" is red. The terminal window has a title bar "LOG - sudo -i" and a status bar "Ср, 3 декабря 10:21".

```
2025-12-03T10:21:06 UTC
LOG | 2025-12-03T10:18:15.000|syslog_log|messages[907]| | |
Dec 3 10:18:15 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 10:18:15 client systemd[1]: iscsi.service: Unit cannot be reloaded because it is inactive.
Dec 3 10:18:16 client avahi-daemon[1106]: Leaving mDNS multicast group on interface eth0.IPv6 with address fe80::a00:27ff:fe83:f313.
Dec 3 10:18:16 client avahi-daemon[1106]: Joining mDNS multicast group on interface eth0.IPv6 with address fd17:625c:f037:2:a00:27ff:fe83:f313 on eth0.*.
Dec 3 10:18:16 client avahi-daemon[1106]: Registering new address record for fd17:625c:f037:2:a00:27ff:fe83:f313 on eth0.*.
Dec 3 10:18:16 client avahi-daemon[1106]: Withdrawing address record for fe80::a00:27ff:fe83:f313 on eth0.
Dec 3 10:18:25 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 10:18:25 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 269.
Dec 3 10:18:25 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 10:18:25 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Dec 3 10:18:35 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 10:18:35 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 270.
Dec 3 10:18:35 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 10:18:45 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 10:18:46 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 271.
Dec 3 10:18:46 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 10:18:56 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 10:18:56 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 272.
Dec 3 10:18:56 client systemd[1]: Started serial-getty@ttyS0.service - Serial Getty on ttyS0.
Dec 3 10:19:06 client systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 3 10:19:06 client systemd[1]: serial-getty@ttyS0.service: Scheduled restart job, restart counter is at 273.
```

Рис. 15: Просмотр логов

Внесение изменений в настройки внутреннего окружения виртуальных машин

На машине `server` перейдем в каталог для внесения изменений, в который поместим конфигурационные файлы:

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

Рис. 16: Создание каталогов и копирование конф.файлов

Внесение изменений в настройки внутреннего окружения виртуальных машин

Создадим скрипт

```
#!/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
~
~
~
```

Рис. 17: Создание скрипта

Внесение изменений в настройки внутреннего окружения виртуальных машин

На машине client перейдем в каталог для внесения изменений, в который поместим конфигурационные файлы:

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

Рис. 18: Создание каталогов и копирование конф.файлов

Внесение изменений в настройки внутреннего окружения виртуальных машин

Создадим скрипт

```
#!/bin/bash
echo "Provisioning script $0"
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
```

Рис. 19: Создание скрипта

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

Рис. 20: Редактирование Vagrantfile

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

Рис. 21: Редактирование Vagrantfile

В ходе выполнения лабораторной работы мы получили навыки по работе с журналами системных событий.