

# Лабораторная работа №15

## Настройка сетевого журналирования

---

Спелов А. Н.

12 декабря 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Спелов Андрей Николаевич
- НПИбд-02-23 Студ. билет: 1132231839
- Российский университет дружбы народов
- 1132231839@pfur.ru

# **Вводная часть**

---

- Целью данной работы является получение навыков по работе с журналами системных событий.

## Основная часть

---

# Настройка сервера сетевого журнала

- Создание на сервере файла конфигурации сетевого хранения журналов.

```
[anspelov@server.anspelov.net rsyslog.d]$ sudo -i  
[sudo] password for anspelov:  
[root@server.anspelov.net ~]# cd /etc/rsyslog.d  
[root@server.anspelov.net rsyslog.d]# touch netlog-server.conf  
[root@server.anspelov.net rsyslog.d]#
```

# Настройка сервера сетевого журнала

- Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514

```
netlog-server.conf [-M--] 22 L:[ 1+ 1 2/ 2] *(37 / 37b) <EOF>  
$ModLoad imtcp  
$InputTCPServerRun 514
```



# Настройка сервера сетевого журнала

- Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

```
[root@server.anspelov.net rsyslog.d]# systemctl restart rsyslog
[root@server.anspelov.net rsyslog.d]# 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/doc
Output information may be incomplete.
```

systemd	1	root	78u	IPv6	7589	0t0	TCP *:websm (LISTEN)
cupsd	1236	root	7u	IPv6	11076	0t0	TCP localhost:ipp (LISTEN)
cupsd	1236	root	8u	IPv4	11077	0t0	TCP localhost:ipp (LISTEN)
sshd	1237	root	7u	IPv4	11067	0t0	TCP *:ssh (LISTEN)
sshd	1237	root	8u	IPv6	11069	0t0	TCP *:ssh (LISTEN)
smbd	1317	root	27u	IPv6	12295	0t0	TCP *:microsoft-ds (LISTEN)
smbd	1317	root	28u	IPv6	12296	0t0	TCP *:netbios-ssn (LISTEN)
smbd	1317	root	29u	IPv4	12297	0t0	TCP *:microsoft-ds (LISTEN)
smbd	1317	root	30u	IPv4	12298	0t0	TCP *:netbios-ssn (LISTEN)
rsyslogd	9044	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)
rsyslogd	9044	root	5u	IPv6	39959	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9046 in:imjour	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9046 in:imjour	root	5u	IPv6	39959	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9047 in:imtcp	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9047 in:imtcp	root	5u	IPv6	39959	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9048 in:imtcp	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9048 in:imtcp	root	5u	IPv6	39959	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9049 in:imtcp	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9049 in:imtcp	root	5u	IPv6	39959	0t0	TCP *:shell (LISTEN)
rsyslogd	9044 9050 in:imtcp	root	4u	IPv4	39958	0t0	TCP *:shell (LISTEN)

# Настройка сервера сетевого журнала

- Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514

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

- Создание на клиенте файла конфигурации сетевого хранения журналов.

```
[anspelov@client.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@client.anspelov.net ~]# cd /etc/rsyslog.d
[root@client.anspelov.net rsyslog.d]# touch netlog-client.conf
[root@client.anspelov.net rsyslog.d]#
```

## Настройка клиента сетевого журнала

- Включение в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` перенаправления сообщений журнала на 514 TCP-порт сервера.

```
netlog-client.conf [-M--] 29 L:[ 1+ 0 1/ 1] *(29 / 29b) <EOF>  
*. * @@server.anspelov.net:514
```

- Перезапуск службы rsyslog.

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



# Просмотр журнала

- Запуск на сервере под пользователем anspelov графической программы для просмотра журналов.

anspelov@server:/etc/rsyslog.d - gnome-system-monitor

/etc/rsyslog.d

gnome-system-monitor

Processes Resources File Systems

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registr	anspelov	0.00	7693	262.1 kB	405.5 kB	
at-spi-bus-launcher	anspelov	0.00	7685	393.2 kB	32.8 kB	
bash	anspelov	0.00	8419	1.2 MB	761.9 kB	
bash	anspelov	0.00	10405	2.0 MB	77.8 kB	
catatonit	anspelov	0.00	8382	N/A	663.6 kB	
dbus-broker	anspelov	0.00	7573	1.4 MB	1.2 MB	
dbus-broker	anspelov	0.00	7692	131.1 kB	N/A	
dbus-broker-launch	anspelov	0.00	7572	131.1 kB	N/A	
dbus-broker-launch	anspelov	0.00	7691	262.1 kB	N/A	
dconf-service	anspelov	0.00	7714	262.1 kB	278.5 kB	20.
evolution-addressbook-factory	anspelov	0.00	8028	131.1 kB	3.0 MB	53.
evolution-alarm-notify	anspelov	0.00	7801	8.8 MB	1.6 MB	
evolution-calendar-factory	anspelov	0.00	7985	917.5 kB	3.1 MB	
evolution-source-registry	anspelov	0.00	7728	524.3 kB	2.8 MB	
qdm-wayland-session	anspelov	0.00	7569	N/A	4.1 kB	

- Установка на сервере просмотрщика журналов системных сообщений.

```
[root@server.anspelov.net rsyslog.d]# sudo dnf install -y multitail
Last metadata expiration check: 0:29:50 ago on Mon 08 Dec 2025 09:53:25 AM UTC.
Dependencies resolved.
```

Package	Architecture	Version
Installing: <b>multitail</b>	x86_64	7.1.3-2.el10_0

#### Transaction Summary

Install 1 Package

Total download size: 148 k

Installed size: 326 k

Downloading Packages:

multitail-7.1.3-2.el10\_0.x86\_64.rpm

#### Total

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction

Preparing :

Installing : multitail-7.1.3-2.el10\_0.x86\_64

Running scriptlet: multitail-7.1.3-2.el10\_0.x86\_64



## • Просмотр логов

```
Dec 8 10:24:46 server systemd-coredump[125906]: Process 125902 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:24:46 server systemd[1]: Started systemd-coredump[636-125906-0.service - Process Core Dump (PID 125906/UID 0)].
Dec 8 10:24:47 server systemd-coredump[125907]: Process 125902 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Mo
bX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Stack trace of thread 125905:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x00000000041dac4 n/a (n/a + 0x0)#012#2
n/a + 0x0)#012#4 0x00007f20c4b4db68 n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 8 10:24:47 server systemd[1]: systemd-coredump[636-125906-0.service: Deactivated successfully.
Dec 8 10:24:52 server kernel: traps: VBoxClient[125950] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 8 10:24:52 server systemd-coredump[125951]: Process 125947 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:24:52 server systemd[1]: Started systemd-coredump[637-125951-0.service - Process Core Dump (PID 125951/UID 0)].
Dec 8 10:24:52 server systemd-coredump[125952]: Process 125947 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Mo
bX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Stack trace of thread 125950:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x00000000041dac4 n/a (n/a + 0x0)#012#2
n/a + 0x0)#012#4 0x00007f20c4b4db68 n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 8 10:24:52 server systemd[1]: systemd-coredump[637-125951-0.service: Deactivated successfully.
Dec 8 10:24:57 server kernel: traps: VBoxClient[125995] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 8 10:24:57 server systemd-coredump[125996]: Process 125992 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:24:57 server systemd[1]: Started systemd-coredump[638-125996-0.service - Process Core Dump (PID 125996/UID 0)].
Dec 8 10:24:57 server systemd-coredump[125997]: Process 125992 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Mo
bX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Stack trace of thread 125995:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x00000000041dac4 n/a (n/a + 0x0)#012#2
n/a + 0x0)#012#4 0x00007f20c4b4db68 n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 8 10:24:57 server systemd[1]: systemd-coredump[638-125996-0.service: Deactivated successfully.
Dec 8 10:25:02 server kernel: traps: VBoxClient[126040] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 8 10:25:02 server systemd-coredump[126041]: Process 126037 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:25:02 server systemd[1]: Started systemd-coredump[639-126041-0.service - Process Core Dump (PID 126041/UID 0)].
Dec 8 10:25:03 server systemd-coredump[126042]: Process 126037 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Mo
bX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Stack trace of thread 126040:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x00000000041dac4 n/a (n/a + 0x0)#012#2
n/a + 0x0)#012#4 0x00007f20c4b4db68 n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 8 10:25:03 server systemd[1]: systemd-coredump[639-126041-0.service: Deactivated successfully.
Dec 8 10:25:08 server kernel: traps: VBoxClient[126088] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 8 10:25:08 server systemd-coredump[126089]: Process 126085 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:25:08 server systemd[1]: Started systemd-coredump[640-126089-0.service - Process Core Dump (PID 126089/UID 0)].
Dec 8 10:25:08 server systemd-coredump[126090]: Process 126085 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Mo
bX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Stack trace of thread 126088:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x00000000041dac4 n/a (n/a + 0x0)#012#2
n/a + 0x0)#012#4 0x00007f20c4b4db68 n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 8 10:25:08 server systemd[1]: systemd-coredump[640-126089-0.service: Deactivated successfully.
Dec 8 10:25:09 server ptyxis[8348]: context mismatch in svga_surface_destroy
Dec 8 10:25:13 server kernel: traps: VBoxClient[126133] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 8 10:25:13 server systemd-coredump[126134]: Process 126130 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 10:25:13 server systemd[1]: Started systemd-coredump[641-126134-0.service - Process Core Dump (PID 126134/UID 0)].
```

# Внесение изменений в настройки внутреннего окружения виртуальных машин

- Переход на виртуальной машине `server` в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `netlog`, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге `/vagrant/provision/server` исполняемого файла `netlog.sh`.

```
[root@server.anspelov.net rsyslog.d]# cd /vagrant/provision/server
[root@server.anspelov.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.anspelov.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.anspelov.net server]# cd /vagrant/provision/server
[root@server.anspelov.net server]# touch netlog.sh
[root@server.anspelov.net server]# chmod +x netlog.sh
[root@server.anspelov.net server]#
```

# Настройка сервера NFSv4

- Открытие файла на редактирование и добавление в него скрипта.

```
netlog.sh      [-M--] 25 L:[ 1+ 9 10/ 10] *(300 / 300b) <EOF>
#!/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
```

## Монтирование NFS на клиенте

- Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

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

[root@client.anspelov.net client]# cd /vagrant/provision/client
[root@client.anspelov.net client]# touch netlog.sh
[root@client.anspelov.net client]# chmod +x netlog.sh
[root@client.anspelov.net client]# █
```

# Монтирование NFS на клиенте

- Открытие файла на редактирование и добавление в него скрипта.

```
netlog.sh      [-M--] 25 L:[ 1+ 8  9/  9] *(249 / 249b) <EOF>
#!/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
```

# Монтирование NFS на клиенте

- Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.

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

## Client configuration
config.vm.define "client", autostart: false do |client|
  client.vm.box = "rockylinux8"
  client.vm.hostname = "client"

  client.vm.boot_timeout = 1440

  client.ssh.insert_key = false
  client.ssh.username = 'vagrant'
  client.ssh.password = 'vagrant'

  client.vm.network :private_network,
    ip: "192.168.1.2",
    virtualbox____intnet: true

  client.vm.provider :virtualbox do |virtualbox|
    virtualbox.customize ["modifyvm", :id, "--vrdm", "on"]
    virtualbox.customize ["modifyvm", :id, "--vrdmport", "3352"]
  end

  client.vm.provision "client dummy",
    type: "shell",
    preserve_order: true,
    path: "provision/client/01-dummy.sh"

  client.vm.provision "client routing",
    type: "shell",
    preserve_order: true,
    run: "always",
    path: "provision/client/01-routing.sh"

  client.vm.provision "client routing",
    type: "shell",
    preserve_order: true,
    run: "always",
    path: "provision/client/01-routing.sh"

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

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

  client.vm.provision "client nfs",
```

## Вывод

---

- В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.