

# Настройка сетевого журналирования

Лабораторная работа №15

---

Элсаиед Адел

7 января 2026

Российский университет дружбы народов, Москва, Россия

## Цели и задачи работы

---

## Цель лабораторной работы

---

Получение практических навыков настройки и использования журналов системных событий, а также организации централизованного сетевого журналирования на базе rsyslog.

## Выполнение работы

---

## Конфигурация rsyslog

- Создан отдельный конфигурационный файл для сетевого журналирования
- Включен приём сообщений по TCP
- Использован стандартный порт 514



The screenshot shows a text editor window with the title bar "netlog-server.conf" and the path "/etc/rsyslog.d". The editor has three buttons: "Open", a dropdown arrow, and a "+" button. The main area contains two lines of configuration code:

```
1 $ModLoad imtcp
2 $InputTCPServerRun 514
```

Рис. 1: Настройка приёма журналов по TCP

## Настройка межсетевого экрана

- Разрешён входящий трафик на TCP-порт 514
- Правила добавлены во временную и постоянную конфигурацию
- Обеспечена доступность сервера после перезагрузки

```
smbd[192. 18952]          elsaiedadel  33u    IPv4          120104    0t0      TCP www.elsaiedadel.  
net:microsoft-ds->client.elsaiedadel.net:47188 (ESTABLISHED)  
rsyslogd 20540             root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540             root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20543 in:imjour root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20543 in:imjour root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20544 in:imtcp  root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20544 in:imtcp  root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20545 w0/imtcp root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20545 w0/imtcp root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20546 w1/imtcp root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20546 w1/imtcp root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20547 rs:main   root      4u    IPv4          146032    0t0      TCP *:shell (LISTEN)  
rsyslogd 20540 20547 rs:main   root      5u    IPv6          146033    0t0      TCP *:shell (LISTEN)  
[root@server.elsaiedadel.net rsyslog.d]# firewall-cmd --add-port=514/tcp  
success  
[root@server.elsaiedadel.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent  
success  
[root@server.elsaiedadel.net rsyslog.d]#
```

Рис. 2: Настройка firewall

## Конфигурация клиента

- Создан файл конфигурации rsyslog клиента
- Настроена пересылка всех сообщений на сервер
- Использован TCP-протокол для надёжной доставки



The screenshot shows a text editor window with the title bar "netlog-client.conf" and the path "/etc/rsyslog.d". The editor has three buttons: "Open", a dropdown arrow, and a plus sign. The main area contains the following configuration line:

```
1 *.* @@server.elsaiedadel.net:514
```

Рис. 3: Настройка клиента rsyslog

## Анализ логов на сервере

- Выполнен просмотр системных журналов
- Зафиксированы сообщения от сервера и клиента
- Подтверждена корректная идентификация хостов

```
Jan  7 08:28:12 client systemd[1]: Started systemd-coredump@480-19045-0.service - Process Core Dump (PID 19045/UID 0).
Jan  7 08:28:12 client systemd-coredump[19046]: Process 19041 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 19044:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x0000000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f5ddec15b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x000007f5ddec866bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 19041:#012#0 0x000007f5ddec844bd syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f5ddebab30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f5ddebab3c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Jan  7 08:28:12 client systemd[1]: systemd-coredump@480-19045-0.service: Deactivated successfully.
Jan  7 08:28:13 server systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Jan  7 08:28:13 server kernel: traps: VBoxClient[20839] trap int3 ip:41dd1b sp:7f6d3a635cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Jan  7 08:28:13 server systemd-coredump[20840]: Process 20836 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
```

Рис. 4: Просмотр журналов

## Мониторинг состояния системы

- Использован графический монитор ресурсов
- Проанализированы процессы и нагрузка CPU
- Оценено использование памяти и файловых систем

The screenshot shows a graphical user interface for monitoring system resources. At the top, there are tabs for 'Processes', 'Resources', and 'File Systems'. The 'Processes' tab is selected. Below the tabs is a header row with columns: Process Name, User, % CPU, ID, Memory, Disk read total, and Disk write. The main area lists various processes with their details:

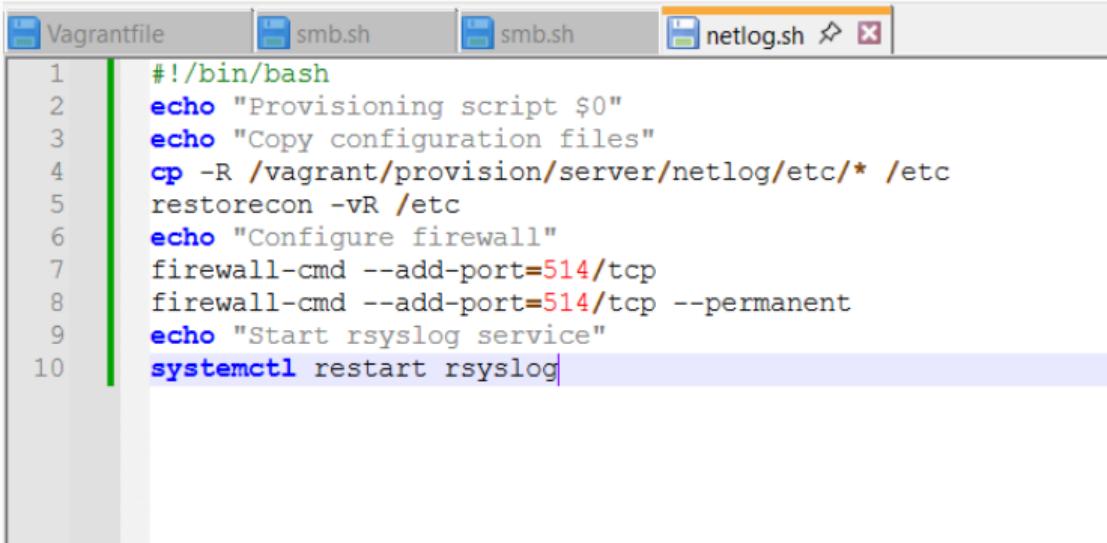
Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registryd	elsaiedadel	0.00	10977	299.0 kB	N/A	
at-spi-bus-launcher	elsaiedadel	0.00	10915	311.3 kB	N/A	
bash	elsaiedadel	0.00	15067	2.1 MB	N/A	
bash	elsaiedadel	0.00	17132	2.2 MB	N/A	
bash	elsaiedadel	0.00	17205	2.2 MB	102.4 kB	
catatonit	elsaiedadel	0.00	15026	53.2 kB	679.9 kB	
dbus-broker	elsaiedadel	0.00	10580	1.5 MB	N/A	
dbus-broker	elsaiedadel	0.00	10939	221.2 kB	N/A	
dbus-broker-launch	elsaiedadel	0.00	10559	204.8 kB	N/A	
dbus-broker-launch	elsaiedadel	0.00	10934	8.2 kB	N/A	
dconf-service	elsaiedadel	0.00	21171	544.8 kB	N/A	
evolution-addressbook-factory	elsaiedadel	0.00	11542	692.2 kB	N/A	
evolution-alarm-notify	elsaiedadel	0.00	11268	5.1 MB	N/A	
evolution-calendar-factory	elsaiedadel	0.00	11494	655.4 kB	N/A	
gnome-control-center	elsaiedadel	0.00	11207	373.0 kB	N/A	

## Подготовка server provisioning

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

Рис. 6: Provision server

## Provisioning-скрипт сервера

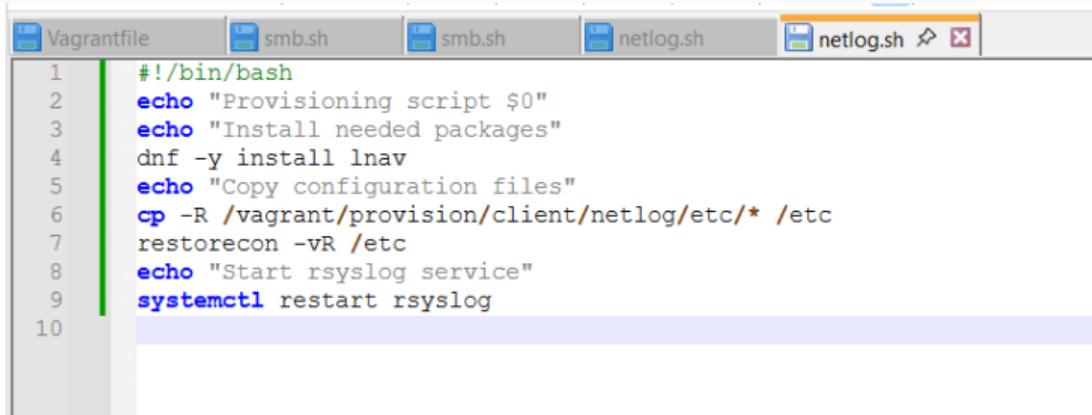


The screenshot shows a terminal window with several tabs open. The active tab is titled "netlog.sh". The code within the tab is a bash script for provisioning a server. It includes commands for copying configuration files, configuring a firewall to allow port 514/tcp, and restarting the rsyslog service.

```
#!/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. 7: netlog.sh server

## Provisioning клиента



The screenshot shows a terminal window with several tabs open. The active tab is titled "netlog.sh". The code in the editor is a bash provisioning script:

```
1 #!/bin/bash
2 echo "Provisioning script $0"
3 echo "Install needed packages"
4 dnf -y install lnav
5 echo "Copy configuration files"
6 cp -R /vagrant/provision/client/netlog/etc/* /etc
7 restorecon -vR /etc
8 echo "Start rsyslog service"
9 systemctl restart rsyslog
10
```

Рис. 8: netlog.sh client

## Выводы

---

- Настроено централизованное сетевое журналирование
- Реализована клиент-серверная модель rsyslog
- Выполнена автоматизация конфигурации с помощью Vagrant
- Обеспечена воспроизводимость и масштабируемость решения