

# Лабораторная работа 15

---

Ярметов Камран

17 февраля, 2023., Москва, Россия

Российский Университет Дружбы Народов

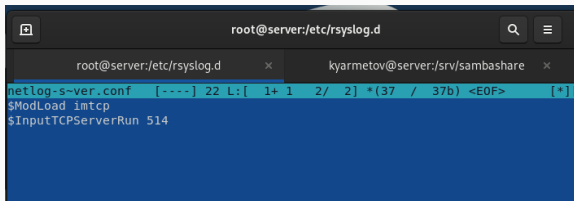
## Цель лабораторной работы

Получение навыков по работе с журналами системных событий.

# **Выполнение лабораторной работы**

---

# Настройка сервера сетевого журнала



The image shows a terminal window with a dark background. The title bar at the top reads "root@server:/etc/rsyslog.d". Below the title bar, there are two tabs: "root@server:/etc/rsyslog.d" and "kyarmetov@server:/srv/sambashare". The active tab is "root@server:/etc/rsyslog.d". The terminal content shows the following lines:

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

**Figure 1:** файл /etc/rsyslog.d/netlog-server.conf

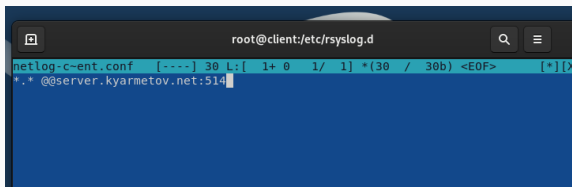
# Настройка сервера сетевого журнала

```
[root@server.kyarmetov.net srv]# cd /etc/rsyslog.d/
[root@server.kyarmetov.net rsyslog.d]# touch netlog-server.conf
[root@server.kyarmetov.net rsyslog.d]# mcedit netlog-server.conf

[root@server.kyarmetov.net rsyslog.d]#
[root@server.kyarmetov.net rsyslog.d]# systemctl restart rsyslog.service
[root@server.kyarmetov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.kyarmetov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --perman
nt
success
[root@server.kyarmetov.net rsyslog.d]#
[root@server.kyarmetov.net rsyslog.d]#
```

Figure 2: Настройка файрвола

# Настройка клиента сетевого журнала

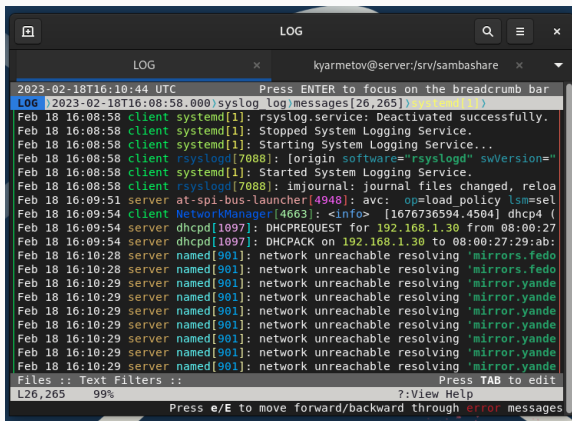


The image shows a terminal window with a dark blue background. The title bar at the top reads "root@client:/etc/rsyslog.d". The terminal content shows the configuration file "netlog-c-ent.conf" being edited. The first line is "[----] 30 L:[ 1+ 0 1/ 1] \*(30 / 30b) <E0F> [\*][X". The second line is " \*.\* @@server.kyarmetov.net:514". The cursor is at the end of the second line.

```
root@client:/etc/rsyslog.d
netlog-c-ent.conf [----] 30 L:[ 1+ 0 1/ 1] *(30 / 30b) <E0F> [*][X
 *.* @@server.kyarmetov.net:514
```

**Figure 3:** файл /etc/rsyslog.d/netlog-client.conf

# Просмотр журнала



The screenshot shows a terminal window titled "LOG" with a search icon, a menu icon, and a close icon in the top right corner. The window has two tabs: "LOG" and "kyarmetov@server:/srv/sambashare". The main content area displays a log stream with timestamps and messages. The first line is "2023-02-18T16:10:44 UTC Press ENTER to focus on the breadcrumb bar". The second line is "LOG 2023-02-18T16:08:58.000 syslog log.messages[26,265]". The log messages include: "Feb 18 16:08:58 client systemd[1]: rsyslog.service: Deactivated successfully.", "Feb 18 16:08:58 client systemd[1]: Stopped System Logging Service.", "Feb 18 16:08:58 client systemd[1]: Starting System Logging Service...", "Feb 18 16:08:58 client rsyslogd[7088]: [origin software="rsyslogd" swVersion=", "Feb 18 16:08:58 client systemd[1]: Started System Logging Service.", "Feb 18 16:08:58 client rsyslogd[7088]: imjournal: journal files changed, reloa", "Feb 18 16:09:51 server at-spi-bus-launcher[4948]: avc: op=load policy lsm=sel", "Feb 18 16:09:54 client NetworkManager[4663]: <info> [1676736594.4504] dhcp4 (", "Feb 18 16:09:54 server dhcpd[1097]: DHCPREQUEST for 192.168.1.30 from 08:00:27", "Feb 18 16:09:54 server dhcpd[1097]: DHCPACK on 192.168.1.30 to 08:00:27:29:ab:", "Feb 18 16:10:28 server named[901]: network unreachable resolving 'mirrors.fedo", "Feb 18 16:10:28 server named[901]: network unreachable resolving 'mirrors.fedo", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande", "Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande". The bottom status bar shows "Files :: Text Filters :: Press TAB to edit", "L26,265 99%", "? : View Help", and "Press e/E to move forward/backward through error messages".

```
LOG
2023-02-18T16:10:44 UTC Press ENTER to focus on the breadcrumb bar
LOG 2023-02-18T16:08:58.000 syslog log.messages[26,265]
Feb 18 16:08:58 client systemd[1]: rsyslog.service: Deactivated successfully.
Feb 18 16:08:58 client systemd[1]: Stopped System Logging Service.
Feb 18 16:08:58 client systemd[1]: Starting System Logging Service...
Feb 18 16:08:58 client rsyslogd[7088]: [origin software="rsyslogd" swVersion="
Feb 18 16:08:58 client systemd[1]: Started System Logging Service.
Feb 18 16:08:58 client rsyslogd[7088]: imjournal: journal files changed, reloa
Feb 18 16:09:51 server at-spi-bus-launcher[4948]: avc: op=load policy lsm=sel
Feb 18 16:09:54 client NetworkManager[4663]: <info> [1676736594.4504] dhcp4 (
Feb 18 16:09:54 server dhcpd[1097]: DHCPREQUEST for 192.168.1.30 from 08:00:27
Feb 18 16:09:54 server dhcpd[1097]: DHCPACK on 192.168.1.30 to 08:00:27:29:ab:
Feb 18 16:10:28 server named[901]: network unreachable resolving 'mirrors.fedo
Feb 18 16:10:28 server named[901]: network unreachable resolving 'mirrors.fedo
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Feb 18 16:10:29 server named[901]: network unreachable resolving 'mirror.yande
Files :: Text Filters :: Press TAB to edit
L26,265 99% ? : View Help
Press e/E to move forward/backward through error messages
```

Figure 4: Просмотр системных сообщений

Приобретены практические навыки по работе с журналами системных событий.