

# Лабораторная работа 15

---

Генералов Даниил, НПИбд-01-21, 1032202280

2023

<sup>1</sup>RUDN University, Moscow, Russian Federation

## Задача

---

1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).

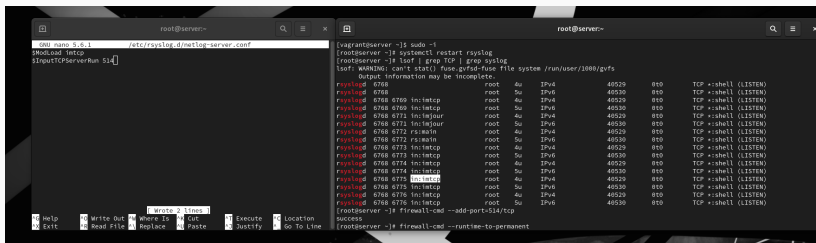
1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере (см. раздел 15.4.2).

1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере (см. раздел 15.4.2).
3. Просмотрите журналы системных событий с помощью нескольких программ (см. раздел 15.4.3). При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.

1. Настройте сервер сетевого журналирования событий (см. раздел 15.4.1).
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере (см. раздел 15.4.2).
3. Просмотрите журналы системных событий с помощью нескольких программ (см. раздел 15.4.3). 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 (см. раздел 15.4.4).

## Выполнение

---



```
root@server:~# nano 5.6.1 /etc/rsyslog.d/metlog-server.conf
IMODLoad Intcp
InputTCPServerRun 514

[variant@server ~]$ sudo -i
[root@server ~]# systemctl restart rsyslog
[root@server ~]# lsotf | grep TCP | grep syslog
lsotf: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
rsyslogd 6768 root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6769 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6769 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6771 in:imjour root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6771 in:imjour root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6772 rs:main root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6772 rs:main root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6773 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6773 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6774 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6774 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6775 in:imtcp root 4u IPv4 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6775 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6776 in:imtcp root 4u IPv4 40529 0t0 TCP *:shell (LISTEN)
rsyslogd 6768 6776 in:imtcp root 5u IPv6 40530 0t0 TCP *:shell (LISTEN)
[root@server ~]# firewall-cmd --add-port=514/tcp
success
[root@server ~]# firewall-cmd --runtime-to-permanent
```

Рис. 1: syslog



The image shows two terminal windows side-by-side, illustrating the configuration and management of the syslog service.

**Left Terminal (root@server):**

```

root@server:~#
Dec 29 22:10:20 server NetworkManager[4317]: <info> [1793887828.3550] audit: op='connection-update' uid='9c92fad9-6ecb-3efc-8a47c9f58c84' name='System eth0' args='connection.timestamp,connection.zone' pid=641 uid=0 result='success'
Dec 29 22:10:24 server systemd[1626]: Starting Mark boot as successful...
Dec 29 22:10:24 server systemd[1626]: Finished Mark boot as successful.
Dec 29 22:12:53 server dhcpcd[1224]: DHCPREQUEST for 192.168.1.30 from 08:00:27:15:c3:a7 (client) via eth1
Dec 29 22:12:53 server dhcpcd[1224]: DHCPACK on 192.168.1.30 to 08:00:27:15:c3:a7 (client) via eth1
Dec 29 22:13:24 server systemd[1626]: Created slice User Background Tasks Slice.
Dec 29 22:13:24 server systemd[1626]: Starting Cleanup of User's Temporary Files and Directories...
Dec 29 22:13:24 server systemd[1626]: Finished Cleanup of User's Temporary Files and Directories.

Dec 29 22:15:07 client systemd[1]: Stopping System Logging Service...
Dec 29 22:15:07 client rsyslogd[582]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="582" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 29 22:15:07 client systemd[2]: rsyslog.service: Deactivated successfully.
Dec 29 22:15:07 client systemd[1]: Stopped System Logging Service.
Dec 29 22:15:07 client systemd[2]: Starting System Logging Service...
Dec 29 22:15:07 client systemd[1]: Started System Logging Service.
Dec 29 22:15:07 client rsyslogd[6749]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="6749" x-info="https://www.rsyslog.com"] start
Dec 29 22:15:07 client rsyslogd[6749]: imjournal: journal files changed, reloading... [v8.2102.0-113.el9_2.1 try https://www.rsyslog.com/en/v8/]

```

**Right Terminal (vagrant@client):**

```

vagrant@client:~$ sudo nano /etc/rsyslog.d/netlog-client.conf
GNU nano 2.9.6 /etc/rsyslog.d/netlog-client.conf
** @server.dnsgeneralov.net:514

vagrant@client:~$
[vagrant@client ~]$ sudo systemctl restart rsyslog
[vagrant@client ~]$

```

Рис. 2: syslog

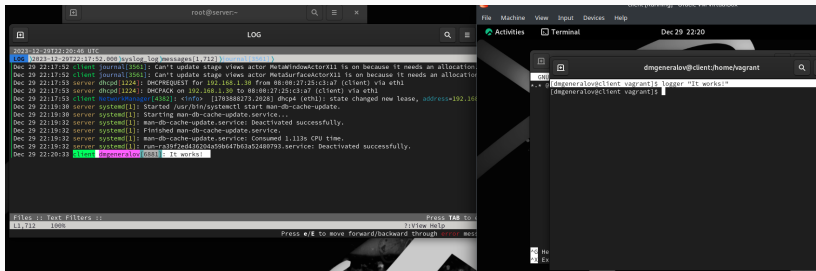


Рис. 3: syslog

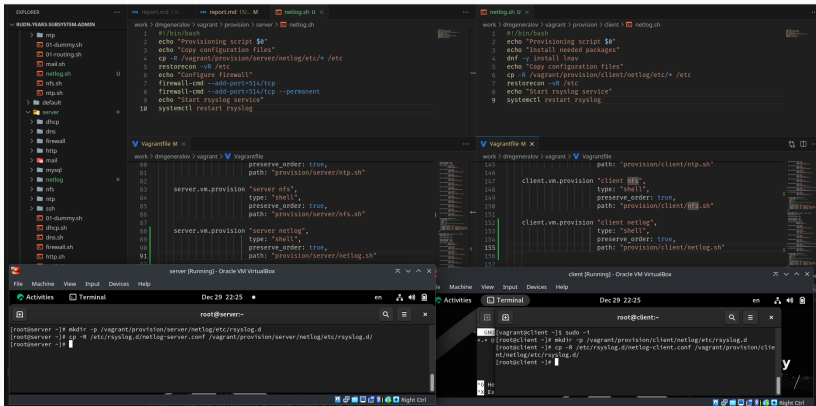


Рис. 4: vagrant

*Я получил опыт настройки службы сетевых логов rsyslog.*