

Лабораторная работа №15

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Российский университет дружбы народов, Москва, Россия

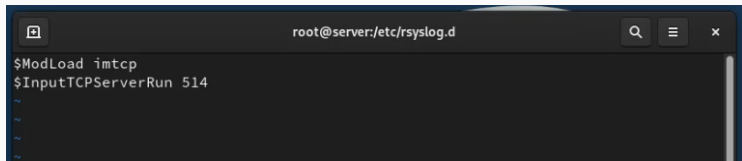
Получение навыков по работе с журналами системных событий.

Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d
```

```
touch netlog-server.conf
```

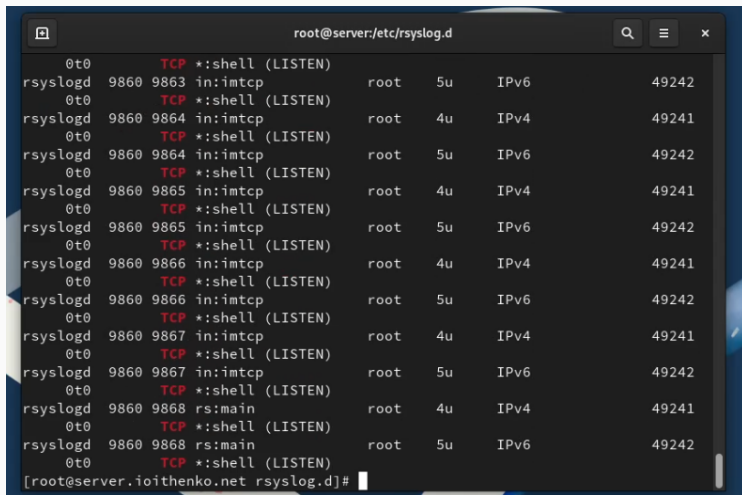


```
root@server:/etc/rsyslog.d
$ModLoad imtcp
$InputTCPServerRun 514
~
~
~
~
```

The image shows a terminal window with a dark background. The title bar at the top reads 'root@server:/etc/rsyslog.d'. Inside the terminal, the following commands have been entered: '\$ModLoad imtcp' and '\$InputTCPServerRun 514'. Below these commands, there are four tilde characters (~) on separate lines, indicating the end of the configuration file or a prompt for further input. The terminal window has standard icons for search, menu, and close on the right side of the title bar.

Рис. 1: Включение журналирования по TCP-порту 514

Настройка сервера сетевого журнала



```
root@server:/etc/rsyslog.d
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9863 in:imtcp      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9864 in:imtcp      root    4u     IPv4    49241
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9864 in:imtcp      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9865 in:imtcp      root    4u     IPv4    49241
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9865 in:imtcp      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9866 in:imtcp      root    4u     IPv4    49241
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9866 in:imtcp      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9867 in:imtcp      root    4u     IPv4    49241
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9867 in:imtcp      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9868 rs:main      root    4u     IPv4    49241
0t0      TCP *:shell (LISTEN)
rsyslogd 9860 9868 rs:main      root    5u     IPv6    49242
0t0      TCP *:shell (LISTEN)
[root@server.ioithenko.net rsyslog.d]#
```

Рис. 2: Перезапуск `rsyslog` и просмотр прослушиваемых портов

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

Рис. 3: Настройка межсетевого экрана для работы с TCP-портом 514

На клиенте создадим файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d  
touch netlog-client.conf
```

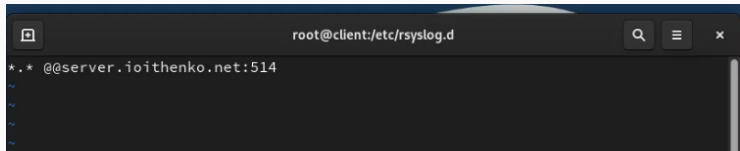
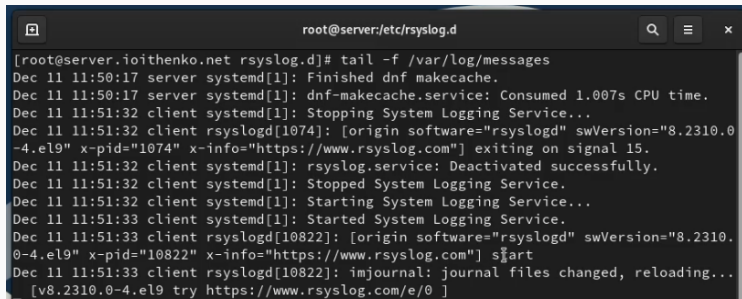



Рис. 4: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

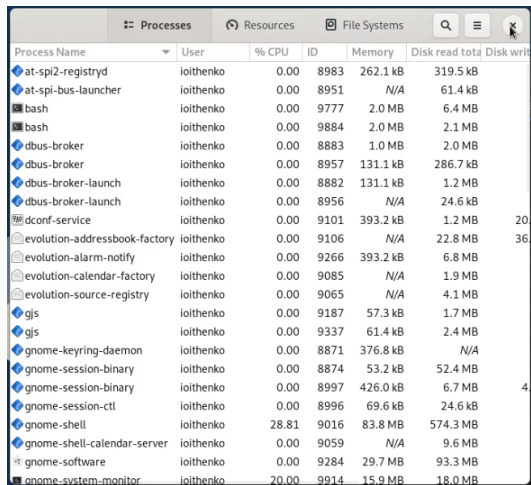
```
systemctl restart rsyslog
```



```
root@server:/etc/rsyslog.d

[root@server.ioithenko.net rsyslog.d]# tail -f /var/log/messages
Dec 11 11:50:17 server systemd[1]: Finished dnf makecache.
Dec 11 11:50:17 server systemd[1]: dnf-makecache.service: Consumed 1.007s CPU time.
Dec 11 11:51:32 client systemd[1]: Stopping System Logging Service...
Dec 11 11:51:32 client rsyslogd[1074]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1074" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 11 11:51:32 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec 11 11:51:32 client systemd[1]: Stopped System Logging Service.
Dec 11 11:51:32 client systemd[1]: Starting System Logging Service...
Dec 11 11:51:33 client systemd[1]: Started System Logging Service.
Dec 11 11:51:33 client rsyslogd[10822]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="10822" x-info="https://www.rsyslog.com"] start
Dec 11 11:51:33 client rsyslogd[10822]: imjournal: journal files changed, reloading...
[v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

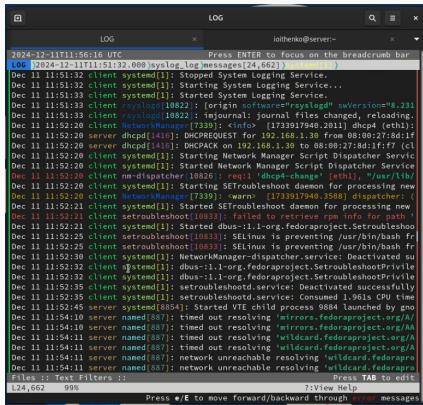
Рис. 5: Просмотр файла журнала на сервере



Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ
at-spi2-registr	ioithenko	0.00	8983	262.1 kB	319.5 kB	
at-spi-bus-launcher	ioithenko	0.00	8951	N/A	61.4 kB	
bash	ioithenko	0.00	9777	2.0 MB	6.4 MB	
bash	ioithenko	0.00	9884	2.0 MB	2.1 MB	
dbus-broker	ioithenko	0.00	8883	1.0 MB	2.0 MB	
dbus-broker	ioithenko	0.00	8957	131.1 kB	286.7 kB	
dbus-broker-launch	ioithenko	0.00	8882	131.1 kB	1.2 MB	
dbus-broker-launch	ioithenko	0.00	8956	N/A	24.6 kB	
dconf-service	ioithenko	0.00	9101	393.2 kB	1.2 MB	20
evolution-addressbook-factory	ioithenko	0.00	9106	N/A	22.8 MB	36
evolution-alarm-notify	ioithenko	0.00	9266	393.2 kB	6.8 MB	
evolution-calendar-factory	ioithenko	0.00	9085	N/A	1.9 MB	
evolution-source-registry	ioithenko	0.00	9065	N/A	4.1 MB	
gjs	ioithenko	0.00	9187	57.3 kB	1.7 MB	
gjs	ioithenko	0.00	9337	61.4 kB	2.4 MB	
gnome-keyring-daemon	ioithenko	0.00	8871	376.8 kB	N/A	
gnome-session-binary	ioithenko	0.00	8874	53.2 kB	52.4 MB	
gnome-session-binary	ioithenko	0.00	8997	426.0 kB	6.7 MB	4
gnome-session-ctl	ioithenko	0.00	8996	69.6 kB	24.6 kB	
gnome-shell	ioithenko	28.81	9016	83.8 MB	574.3 MB	
gnome-shell-calendar-server	ioithenko	0.00	9059	N/A	9.6 MB	
gnome-software	ioithenko	0.00	9284	29.7 MB	93.3 MB	
gnome-system-monitor	ioithenko	20.00	9914	15.9 MB	18.0 MB	

Рис. 6: Запуск графической программы для просмотра журналов

```
dnf -y install lnav
```



The screenshot shows a terminal window titled 'LOG' with a search bar and navigation icons. The terminal displays system logs from 2024-12-11T11:56:16 UTC. The logs include messages from 'systemd', 'NetworkManager', 'nm-dispatcher', 'setroubleshoot', and 'named'. The user has entered the command 'less /var/log/messages' to view the logs. The terminal shows the first few lines of the log file, which include messages about stopping and starting the System Logging Service, reloading rsyslogd, and DHCP requests. The terminal also shows the 'less' command being used to navigate through the log file, with the cursor positioned at line 124,662.

```
LOG
2024-12-11T11:56:16 UTC Press ENTER to focus on the breadcrumb bar
[06] 2024-12-11T11:51:32.000 syslog_log[messages[24,662]]
Dec 11 11:51:32 client systemd[1]: Stopped System Logging Service.
Dec 11 11:51:32 client systemd[1]: Starting System Logging Service...
Dec 11 11:51:33 client systemd[1]: Started System Logging Service.
Dec 11 11:51:33 client rsyslogd[10822]: [origin software="rsyslogd" swVersion="8.231
Dec 11 11:51:33 client rsyslogd[10822]: injournal: journal files changed, reloading.
Dec 11 11:52:20 client NetworkManager[7339]: <info> [1733917940.2011] dhcp4 (eth1):
Dec 11 11:52:20 server dhcpd[1416]: DHCPREQUEST for 192.168.1.30 from 08:00:27:8d:1f
Dec 11 11:52:20 server dhcpd[1416]: DHCPACK on 192.168.1.30 to 08:00:27:8d:1f:f7 (cl
Dec 11 11:52:20 client systemd[1]: Starting Network Manager Script Dispatcher Servic
Dec 11 11:52:20 client systemd[1]: Started Network Manager Script Dispatcher Service
Dec 11 11:52:20 client nm-dispatcher[10826]: req:1 'dhcp4-change' [eth1], "/usr/lib/
Dec 11 11:52:20 client systemd[1]: Starting SETroubleshoot daemon for processing new
Dec 11 11:52:20 client NetworkManager[7339]: <warn> [1733917940.3508] dispatcher: (
Dec 11 11:52:21 client systemd[1]: Started SETroubleshoot daemon for processing new
Dec 11 11:52:21 client setroubleshoot[10833]: failed to retrieve rpm info for path '
Dec 11 11:52:21 client systemd[1]: Started dbus-1.1-org.fedoraproject.Setroubleshoo
Dec 11 11:52:25 client setroubleshoot[10833]: SELinux is preventing /usr/bin/bash fr
Dec 11 11:52:25 client setroubleshoot[10833]: SELinux is preventing /usr/bin/bash fr
Dec 11 11:52:30 client systemd[1]: NetworkManager-dpdispatcher.service: Deactivated su
Dec 11 11:52:32 client systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivile
Dec 11 11:52:32 client systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivile
Dec 11 11:52:35 client systemd[1]: setroubleshootd.service: Deactivated successfully
Dec 11 11:52:35 client systemd[1]: setroubleshootd.service: Consumed 1.961s CPU time
Dec 11 11:52:45 server systemd[6054]: Started VTE child process 9884 launched by gno
Dec 11 11:54:10 server named[887]: timed out resolving 'mirrors.fedoraproject.org/A
Dec 11 11:54:10 server named[887]: timed out resolving 'mirrors.fedoraproject.org/AA
Dec 11 11:54:11 server named[887]: timed out resolving 'wildcard.fedoraproject.org/A
Dec 11 11:54:11 server named[887]: timed out resolving 'wildcard.fedoraproject.org/A
Dec 11 11:54:11 server named[887]: network unreachable resolving 'wildcard.fedorapro
Dec 11 11:54:11 server named[887]: network unreachable resolving 'wildcard.fedorapro
Files :: Text Filters :: Press TAB to edit
L24,662 99% ?!View Help
Press ?/E to move forward/backward through error messages
```

Рис. 7: Использование `lnav` для просмотра логов

В ходе выполнения лабораторной работы я приобрела практические навыки по работе с журналами системных событий.