Лабораторная работа № 15. Настройка сетевого журналирования

Данила Стариков
НПИбд-02-22

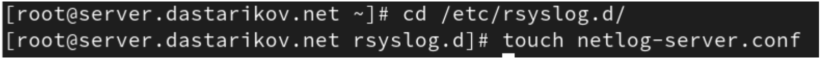
Российский университет дружбы народов имени Патриса Лумумбы

2024

Цель работы

- Получение навыков по работе с журналами системных событий.

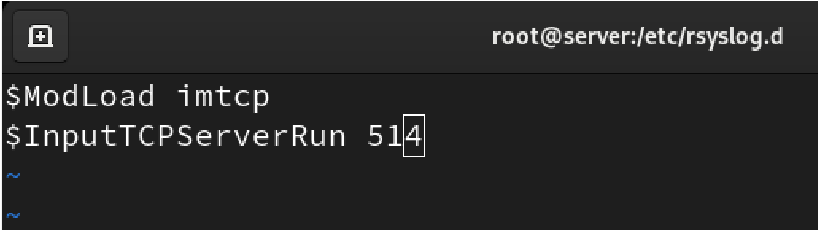
Настройка сервера сетевого журнала



```
[root@server.dastarikov.net ~]# cd /etc/rsyslog.d/
[root@server.dastarikov.net rsyslog.d]# touch netlog-server.conf
```

Рис.: Создание файла конфигурации для сетевого хранения журналов на сервере.

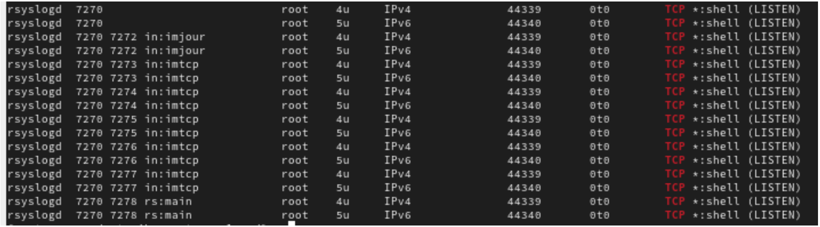
Настройка сервера сетевого журнала



```
$ModLoad imtcp
$InputTCPServerRun 514
~
~
```

Рис.: Включение приема записей журнала по TCP-порту 514.

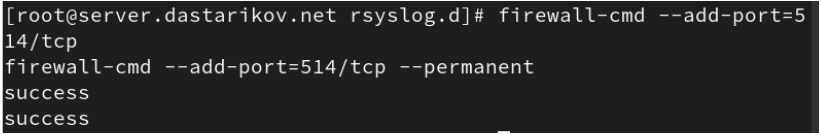
Настройка сервера сетевого журнала



```
rsyslogd  7270                          root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270                          root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7272 in:imjour           root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7272 in:imjour           root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7273 in:imtcp            root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7273 in:imtcp            root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7274 in:imtcp            root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7274 in:imtcp            root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7275 in:imtcp            root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7275 in:imtcp            root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7276 in:imtcp            root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7276 in:imtcp            root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7277 in:imtcp            root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7277 in:imtcp            root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7278 rs:main             root    4u      IPv4              44339       0t0        TCP *:shell (LISTEN)
rsyslogd  7270 7278 rs:main             root    5u      IPv6              44340       0t0        TCP *:shell (LISTEN)
```

Рис.: Проверка прослушиваемых rsyslog портов.

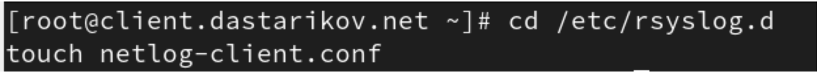
Настройка сервера сетевого журнала



```
[root@server.dastarikov.net rsyslog.d]# firewall-cmd --add-port=5
14/tcp
firewall-cmd --add-port=514/tcp --permanent
success
success
```

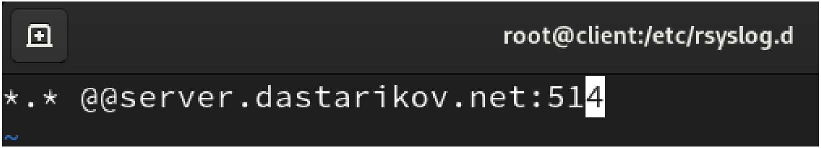
Рис.: Настройка межсетевого экрана для приема сообщений по TCP-порту 514.

Настройка клиента сетевого журнала



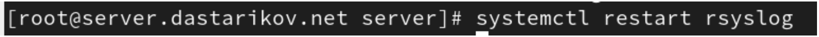
```
[root@client.dastarikov.net ~]# cd /etc/rsyslog.d
touch netlog-client.conf
```

Рис.: Создание файла конфигурации сетевого хранения журналов на клиенте.



```
*.* @@server.dastarikov.net:514
~
```

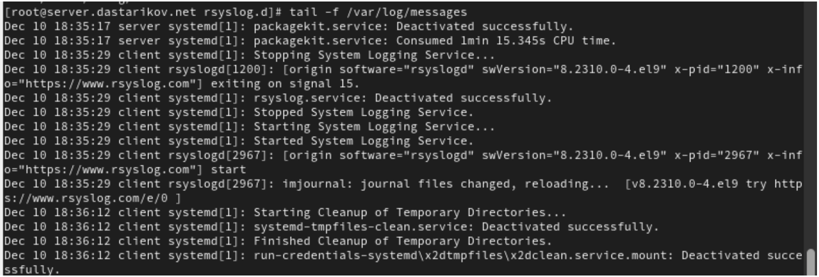
Рис.: Включение перенаправления сообщений журнала на сервер через TCP-порт 514.



```
[root@server.dastarikov.net server]# systemctl restart rsyslog
```

Рис.: Перезапуск службы rsyslog.

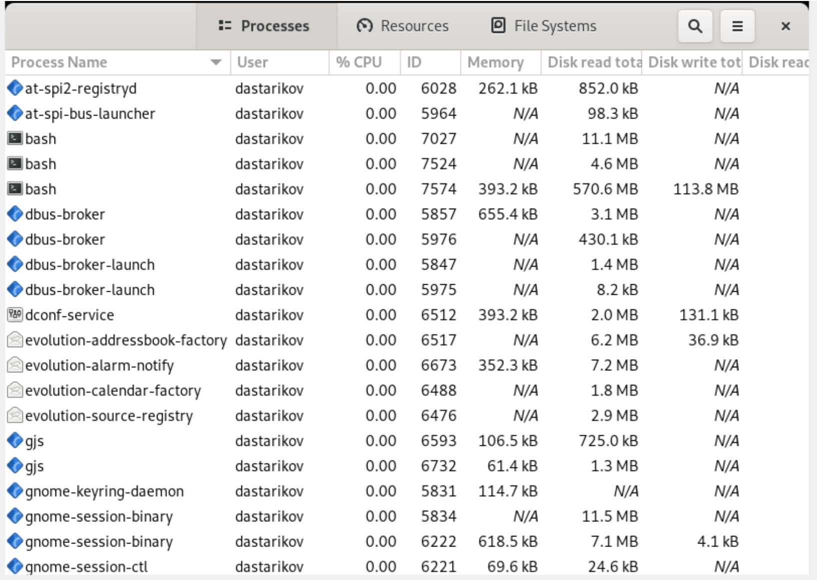
Просмотр журнала



```
[root@server.dastarikov.net rsyslog.d]# tail -f /var/log/messages
Dec 10 18:35:17 server systemd[1]: packagekit.service: Deactivated successfully.
Dec 10 18:35:17 server systemd[1]: packagekit.service: Consumed 1min 15.345s CPU time.
Dec 10 18:35:29 client systemd[1]: Stopping System Logging Service...
Dec 10 18:35:29 client rsyslogd[1200]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1200" x-inf
o="https://www.rsyslog.com"] exiting on signal 15.
Dec 10 18:35:29 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec 10 18:35:29 client systemd[1]: Stopped System Logging Service.
Dec 10 18:35:29 client systemd[1]: Starting System Logging Service...
Dec 10 18:35:29 client systemd[1]: Started System Logging Service.
Dec 10 18:35:29 client rsyslogd[2967]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="2967" x-inf
o="https://www.rsyslog.com"] start
Dec 10 18:35:29 client rsyslogd[2967]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try http
s://www.rsyslog.com/e/0 ]
Dec 10 18:36:12 client systemd[1]: Starting Cleanup of Temporary Directories...
Dec 10 18:36:12 client systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec 10 18:36:12 client systemd[1]: Finished Cleanup of Temporary Directories.
Dec 10 18:36:12 client systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated succe
ssfully.
```

Рис.: Просмотр файла журнала на сервере.

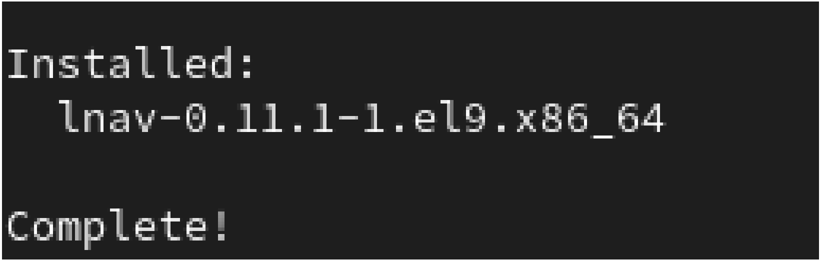
Просмотр журнала



Process Name	User	% CPU	ID	Memory	Disk read tota	Disk write tot	Disk reac
at-spi2-registryd	dastarikov	0.00	6028	262.1 kB	852.0 kB	N/A	
at-spi-bus-launcher	dastarikov	0.00	5964	N/A	98.3 kB	N/A	
bash	dastarikov	0.00	7027	N/A	11.1 MB	N/A	
bash	dastarikov	0.00	7524	N/A	4.6 MB	N/A	
bash	dastarikov	0.00	7574	393.2 kB	570.6 MB	113.8 MB	
dbus-broker	dastarikov	0.00	5857	655.4 kB	3.1 MB	N/A	
dbus-broker	dastarikov	0.00	5976	N/A	430.1 kB	N/A	
dbus-broker-launch	dastarikov	0.00	5847	N/A	1.4 MB	N/A	
dbus-broker-launch	dastarikov	0.00	5975	N/A	8.2 kB	N/A	
dconf-service	dastarikov	0.00	6512	393.2 kB	2.0 MB	131.1 kB	
evolution-addressbook-factory	dastarikov	0.00	6517	N/A	6.2 MB	36.9 kB	
evolution-alarm-notify	dastarikov	0.00	6673	352.3 kB	7.2 MB	N/A	
evolution-calendar-factory	dastarikov	0.00	6488	N/A	1.8 MB	N/A	
evolution-source-registry	dastarikov	0.00	6476	N/A	2.9 MB	N/A	
gjs	dastarikov	0.00	6593	106.5 kB	725.0 kB	N/A	
gjs	dastarikov	0.00	6732	61.4 kB	1.3 MB	N/A	
gnome-keyring-daemon	dastarikov	0.00	5831	114.7 kB	N/A	N/A	
gnome-session-binary	dastarikov	0.00	5834	N/A	11.5 MB	N/A	
gnome-session-binary	dastarikov	0.00	6222	618.5 kB	7.1 MB	4.1 kB	
gnome-session-ctl	dastarikov	0.00	6221	69.6 kB	24.6 kB	N/A	

Рис.: Просмотр журнала на клиенте через графическую программу.

Просмотр журнала

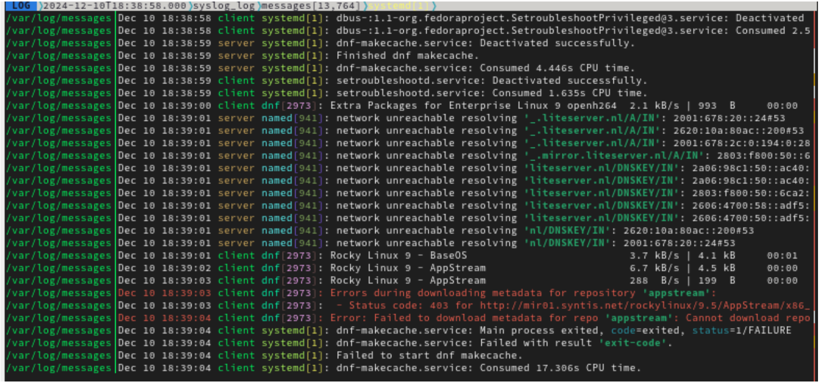


```
Installed:
  lnav-0.11.1-1.el9.x86_64

Complete!
```

Рис.: Установка просмотрщика журналов системных сообщений на сервер.

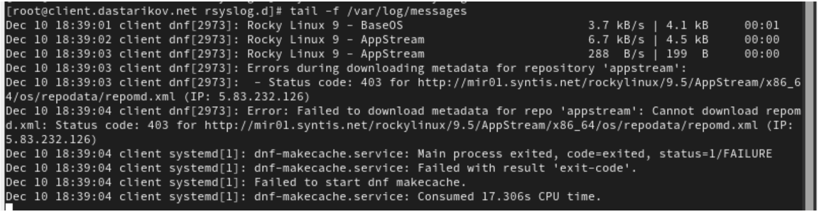
Просмотр журнала



```
 LOG ⟩2024-12-10T18:38:58.000⟩syslog_log⟩messages[13,764]⟩systemd[1]⟩
/var/log/messages│Dec 10 18:38:58 client systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@3.service: Deactivated
/var/log/messages│Dec 10 18:38:58 client systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@3.service: Consumed 2.5
/var/log/messages│Dec 10 18:38:59 server systemd[1]: dnf-makecache.service: Deactivated successfully.
/var/log/messages│Dec 10 18:38:59 server systemd[1]: Finished dnf makecache.
/var/log/messages│Dec 10 18:38:59 server systemd[1]: dnf-makecache.service: Consumed 4.446s CPU time.
/var/log/messages│Dec 10 18:38:59 client systemd[1]: setroubleshootd.service: Deactivated successfully.
/var/log/messages│Dec 10 18:38:59 client systemd[1]: setroubleshootd.service: Consumed 1.635s CPU time.
/var/log/messages│Dec 10 18:39:00 client dnf[2973]: Extra Packages for Enterprise Linux 9 openh264  2.1 kB/s | 993  B     00:00
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving '_.liteserver.nl/A/IN': 2001:678:20::24#53
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving '_.liteserver.nl/A/IN': 2620:10a:80ac::200#53
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving '_.liteserver.nl/A/IN': 2001:678:2c:0:194:0:28
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving '_.mirror.liteserver.nl/A/IN': 2803:f800:50::6
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'liteserver.nl/DNSKEY/IN': 2a06:98c1:50::ac40:
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'liteserver.nl/DNSKEY/IN': 2a06:98c1:50::ac40:
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'liteserver.nl/DNSKEY/IN': 2803:f800:50::6ca2:
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'liteserver.nl/DNSKEY/IN': 2606:4700:58::adf5:
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'liteserver.nl/DNSKEY/IN': 2606:4700:50::adf5:
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'nl/DNSKEY/IN': 2620:10a:80ac::200#53
/var/log/messages│Dec 10 18:39:01 server named[941]: network unreachable resolving 'nl/DNSKEY/IN': 2001:678:20::24#53
/var/log/messages│Dec 10 18:39:01 client dnf[2973]: Rocky Linux 9 - BaseOS                          3.7 kB/s | 4.1 kB     00:01
/var/log/messages│Dec 10 18:39:02 client dnf[2973]: Rocky Linux 9 - AppStream                       6.7 kB/s | 4.5 kB     00:00
/var/log/messages│Dec 10 18:39:03 client dnf[2973]: Rocky Linux 9 - AppStream                       288  B/s | 199  B     00:00
/var/log/messages│Dec 10 18:39:03 client dnf[2973]: Errors during downloading metadata for repository 'appstream':
/var/log/messages│Dec 10 18:39:03 client dnf[2973]:  - Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_
/var/log/messages│Dec 10 18:39:04 client dnf[2973]: Error: Failed to download metadata for repo 'appstream': Cannot download repo
/var/log/messages│Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Main process exited, code=exited, status=1/FAILURE
/var/log/messages│Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
/var/log/messages│Dec 10 18:39:04 client systemd[1]: Failed to start dnf makecache.
/var/log/messages│Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Consumed 17.306s CPU time.
```

Рис.: Просмотр общих логов на сервере.

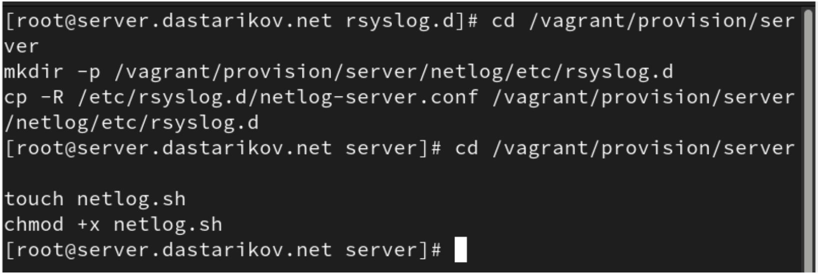
Просмотр журнала



```
[root@client.dastarikov.net rsyslog.d]# tail -f /var/log/messages
Dec 10 18:39:01 client dnf[2973]: Rocky Linux 9 - BaseOS                        3.7 kB/s | 4.1 kB     00:01
Dec 10 18:39:02 client dnf[2973]: Rocky Linux 9 - AppStream                     6.7 kB/s | 4.5 kB     00:00
Dec 10 18:39:03 client dnf[2973]: Rocky Linux 9 - AppStream                     288  B/s | 199  B     00:00
Dec 10 18:39:03 client dnf[2973]: Errors during downloading metadata for repository 'appstream':
Dec 10 18:39:03 client dnf[2973]:  - Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_6
4/os/repodata/repomd.xml (IP: 5.83.232.126)
Dec 10 18:39:04 client dnf[2973]: Error: Failed to download metadata for repo 'appstream': Cannot download repom
d.xml: Status code: 403 for http://mir01.syntis.net/rockylinux/9.5/AppStream/x86_64/os/repodata/repomd.xml (IP:
5.83.232.126)
Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Main process exited, code=exited, status=1/FAILURE
Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
Dec 10 18:39:04 client systemd[1]: Failed to start dnf makecache.
Dec 10 18:39:04 client systemd[1]: dnf-makecache.service: Consumed 17.306s CPU time.
```

Рис.: Логи на клиенте.

Внесение изменений в настройки внутреннего окружения виртуальных машин

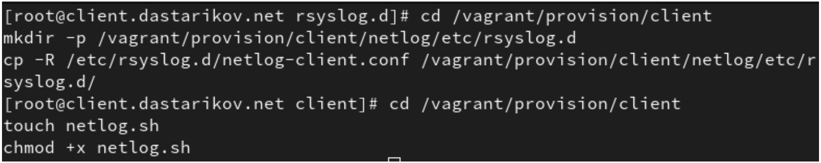


```
[root@server.dastarikov.net rsyslog.d]# cd /vagrant/provision/ser
ver
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server
/netlog/etc/rsyslog.d
[root@server.dastarikov.net server]# cd /vagrant/provision/server

touch netlog.sh
chmod +x netlog.sh
[root@server.dastarikov.net server]# 
```

Рис.: Создание каталога для настройки внутреннего окружения на сервере.

Внесение изменений в настройки внутреннего окружения виртуальных машин



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

Рис.: Создание каталога для настройки внутреннего окружения на клиенте.

Выводы

- В результате выполнений лабораторной работы получили навыки настройки сетевого хранения журналов системных событий.