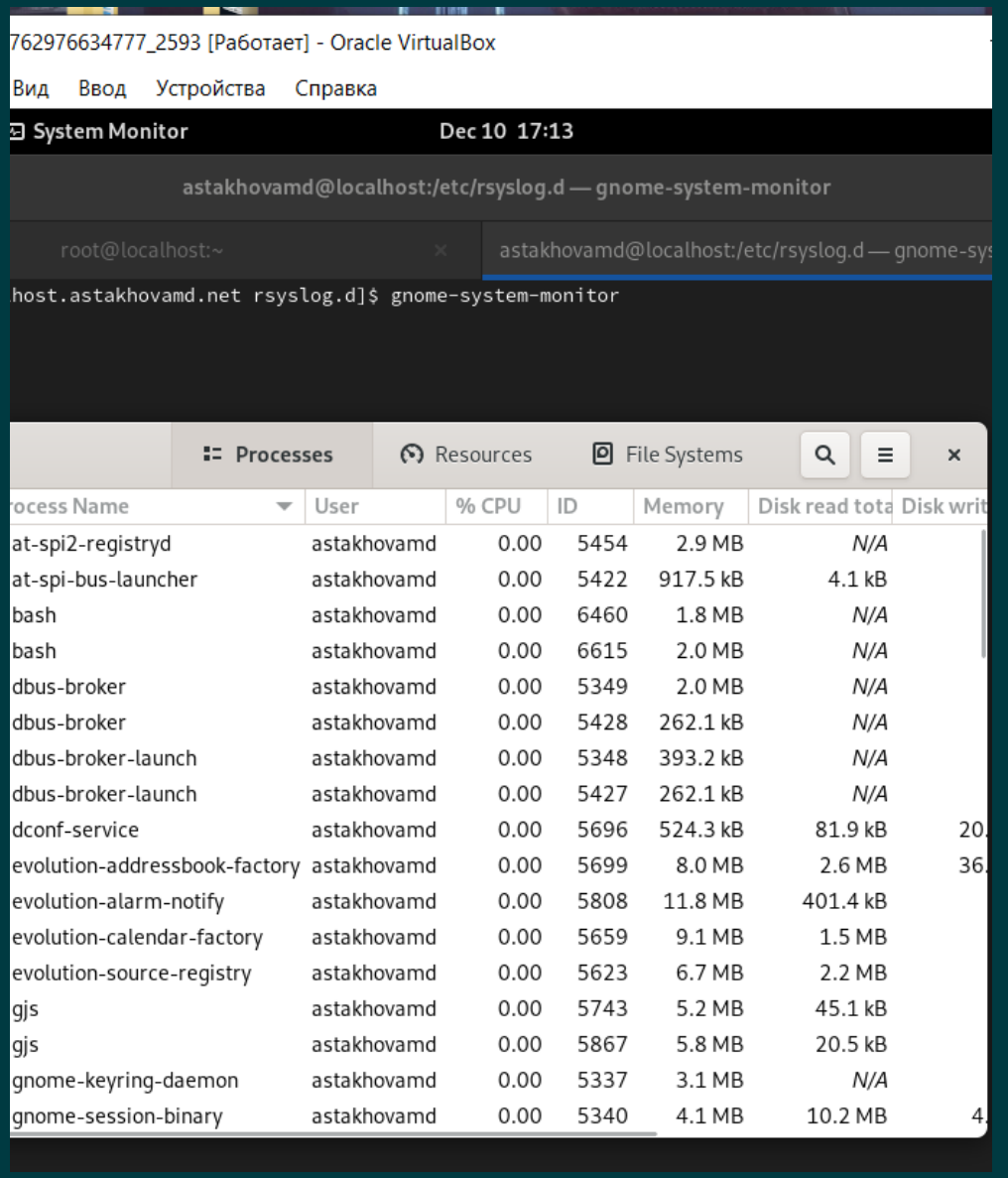
ЛАБОРАТОРНАЯ РАБОТА №15. НАСТРОЙКА СЕТЕВОГО ЖУРНАЛИРОВАНИЯ

Астахова Марина Дмитриевна
НПИБД02-23

ЦЕЛЬ РАБОТЫ

Получение навыков по работе с журналами системных событий.



ВЫПОЛНЕНИЕ РАБОТЫ

Настройка сервера сетевого журнала

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

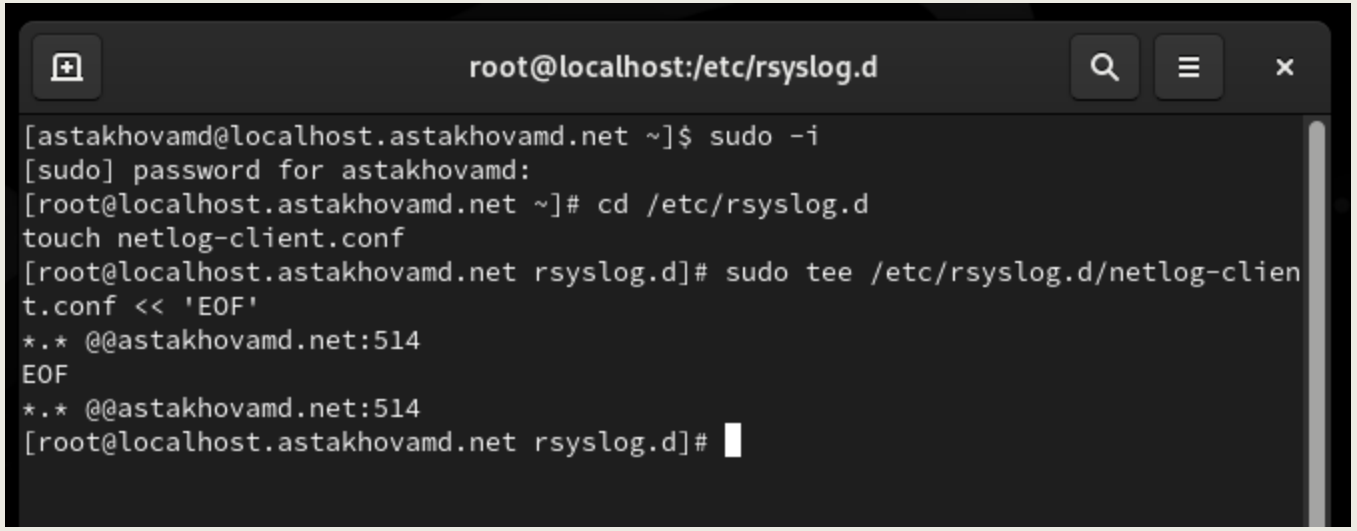
```
[root@localhost.astakhovamd.net rsyslog.d]# sudo tee /etc/rsyslog.d/netlog-serve
r.conf << 'EOF'
$ModLoad imtcp

$InputTCPServerRun 514
EOF
$ModLoad imtcp

$InputTCPServerRun 514
[root@localhost.astakhovamd.net rsyslog.d]#
```

```
[root@localhost.astakhovamd.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@localhost.astakhovamd.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@localhost.astakhovamd.net rsyslog.d]#
```

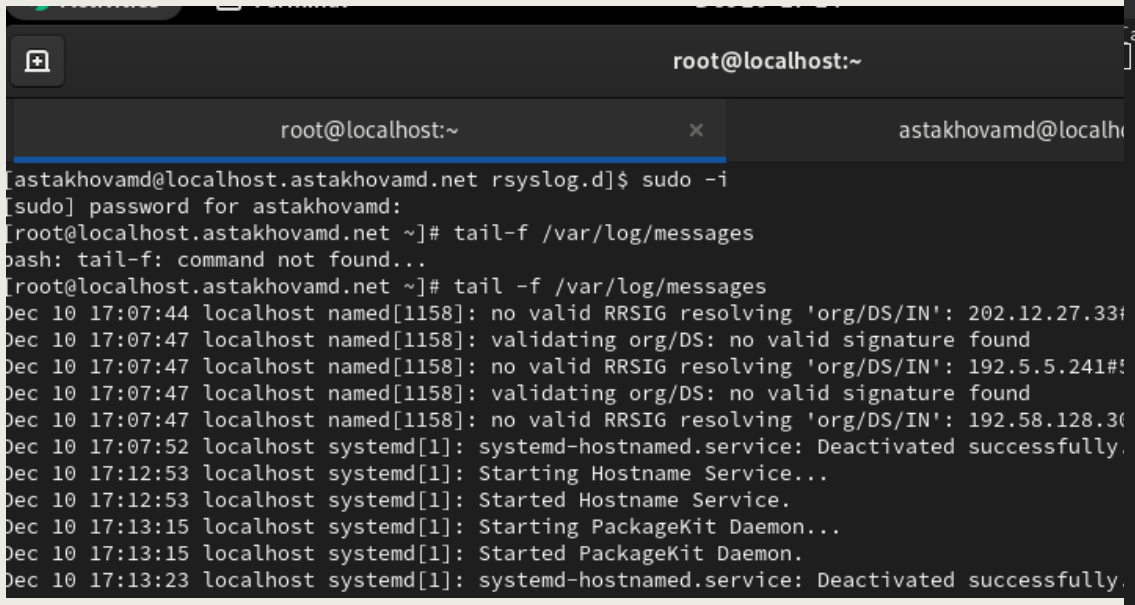
root@localhost:/etc/rsyslog.d

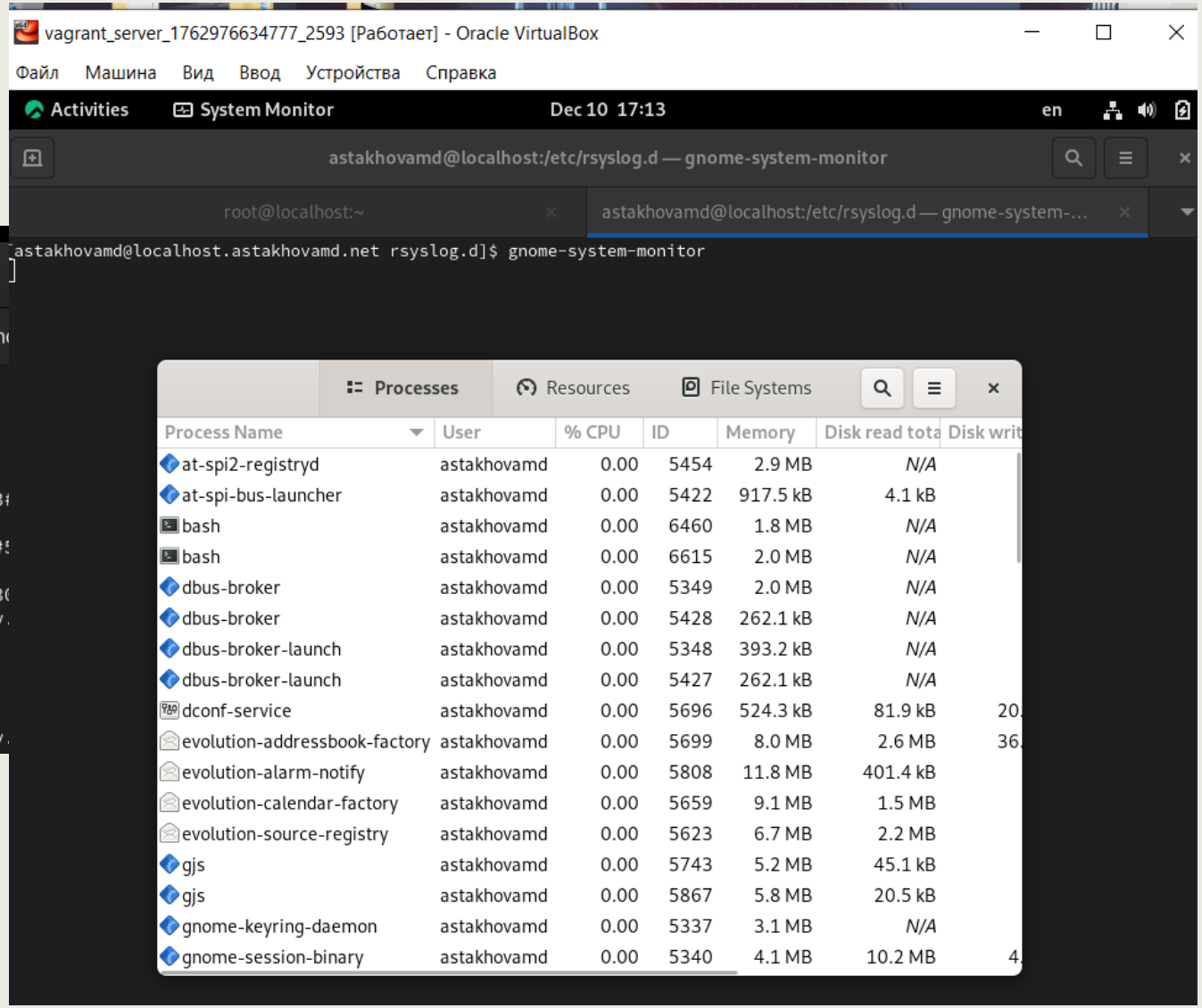
```
[root@localhost.astakhovamd.net rsyslog.d]# systemctl restart rsyslog
[root@localhost.astakhovamd.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
systemd      1                          root   34u     IPv4              19758
     0t0        TCP *:sunrpc (LISTEN)
systemd      1                          root   36u     IPv6              19770
     0t0        TCP *:sunrpc (LISTEN)
rpcbind    617                           rpc    4u     IPv4              19758
     0t0        TCP *:sunrpc (LISTEN)
rpcbind    617                           rpc    6u     IPv6              19770
     0t0        TCP *:sunrpc (LISTEN)
cupsd     1057                          root    7u     IPv6              24411
     0t0        TCP localhost:ipp (LISTEN)
cupsd     1057                          root    8u     IPv4              24412
     0t0        TCP localhost:ipp (LISTEN)
sshd      1070                          root    3u     IPv4              25256
     0t0        TCP *:down (LISTEN)
sshd      1070                          root    4u     IPv6              25258
     0t0        TCP *:down (LISTEN)
sshd      1070                          root    5u     IPv4              25260
     0t0        TCP *:ssh (LISTEN)
sshd      1070                          root    6u     IPv6              25262
     0t0        TCP *:ssh (LISTEN)
rpc.mount 1128                          root    5u     IPv4              25328
     0t0        TCP *:mountd (LISTEN)
rpc.mount 1128                          root    7u     IPv6              25334
     0t0        TCP *:mountd (LISTEN)
named     1158                         named   31u     IPv4              27333
     0t0        TCP localhost:rndc (LISTEN)
named     1158                         named   34u     IPv4              25587
     0t0        TCP localhost:domain (LISTEN)
named     1158                         named   35u     IPv4              25588
     0t0        TCP localhost:domain (LISTEN)
```

Настройка клиента сетевого журнала



Просмотр журнала



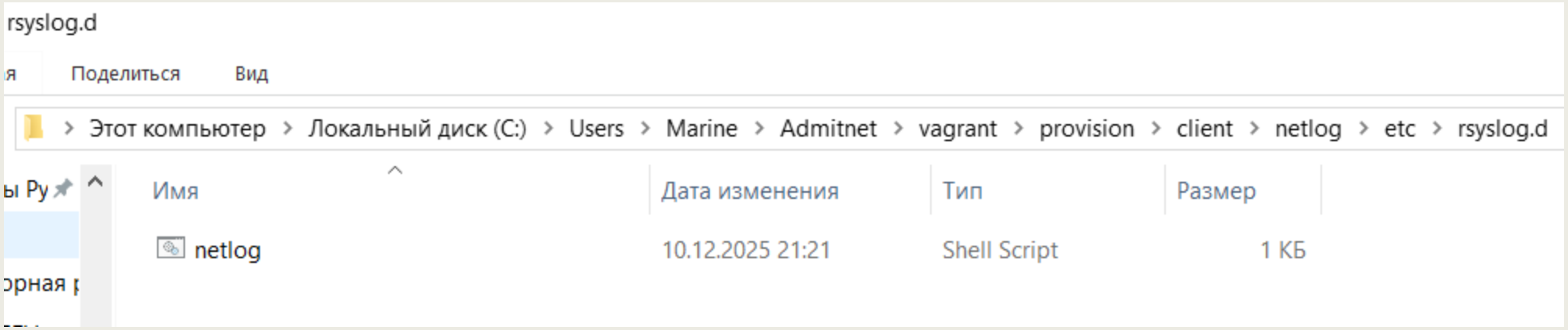


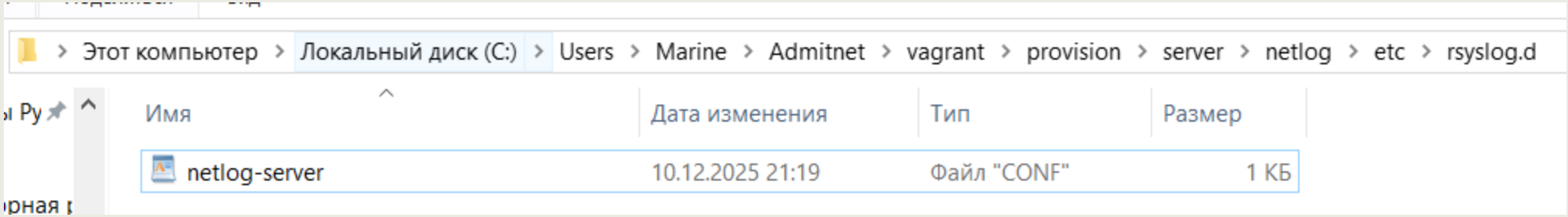
ПРОСМОТР ЖУРНАЛА

```
2025-12-10T18:11:09 UTC                                                      Press ENTER to focus on the breadcrumb bar
LOG 〉2025-12-10T17:33:00.000〉syslog_log〉messages[792]〉chronyd[679]〉
Dec 10 17:33:00 localhost chronyd[679]: Source 2a00:b700:3::288 replaced with 2a02:6bf:f000:1:4::21 (2.rocky.pool.ntp.org)
Dec 10 17:33:55 localhost chronyd[679]: Selected source 82.146.53.58 (2.rocky.pool.ntp.org)
Dec 10 17:36:11 localhost dnf[6801]: Extra Packages for Enterprise Linux 9 - x86_64    12 kB/s |  36 kB     00:02
Dec 10 17:36:12 localhost dnf[6801]: Extra Packages for Enterprise Linux 9 openh264  1.0 kB/s | 993  B     00:00
Dec 10 17:36:42 localhost dnf[6801]: Rocky Linux 9 - BaseOS                          152  B/s | 4.3 kB     00:29
Dec 10 17:36:43 localhost dnf[6801]: Rocky Linux 9 - AppStream                       2.6 kB/s | 4.8 kB     00:01
Dec 10 17:36:48 localhost dnf[6801]: Rocky Linux 9 - Extras                          676  B/s | 3.1 kB     00:04
Dec 10 17:36:48 localhost dnf[6801]: Metadata cache created.
Dec 10 17:36:48 localhost systemd[1]: dnf-makecache.service: Deactivated successfully.
Dec 10 17:36:48 localhost systemd[1]: Finished dnf makecache.
Dec 10 17:38:31 localhost systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 10 17:38:31 localhost systemd[1]: Starting man-db-cache-update.service...
Dec 10 17:38:31 localhost systemd[1]: Starting PackageKit Daemon...
Dec 10 17:38:31 localhost systemd[1]: Started PackageKit Daemon.
Dec 10 17:38:47 localhost systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 10 17:38:47 localhost systemd[1]: Finished man-db-cache-update.service.
Dec 10 17:38:47 localhost systemd[1]: man-db-cache-update.service: Consumed 15.879s CPU time.
Dec 10 17:38:47 localhost systemd[1]: run-re051f5604ae54958bd1b1205cf242ff8.service: Deactivated successfully.
Dec 10 17:43:37 localhost systemd[1]: packagekit.service: Deactivated successfully.
Dec 10 17:58:25 localhost cupsd[1057]: REQUEST localhost - - "POST / HTTP/1.1" 200 190 Renew-Subscription successful-ok
Dec 10 17:59:49 localhost kea-dhcp4[1098]: 2025-12-10 17:59:49.740 INFO  [kea-dhcp4.dhcpsrv/1098.140540041559360] DHCPSRV_MEMFILE_LFC_START starting Le
Dec 10 17:59:49 localhost kea-dhcp4[1098]: 2025-12-10 17:59:49.741 INFO  [kea-dhcp4.dhcpsrv/1098.140540041559360] DHCPSRV_MEMFILE_LFC_EXECUTE executing
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_START Starting lease file cleanup
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_PROCESSING Previous file: /var/lib/kea/dhcp4.leases.2, copy file: /var/li
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILE_LEASE_FILE_LOAD loading leases from file /var/lib/kea
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILE_LEASE_FILE_LOAD loading leases from file /var/lib/kea
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_READ_STATS Leases: 0, attempts: 2, errors: 0.
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_WRITE_STATS Leases: 0, attempts: 0, errors: 0.
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_ROTATING LFC rotating files
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO  [DhcpLFC.140461865995584] LFC_TERMINATE LFC finished processing
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:40 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Dec 10 18:09:41 localhost gsd-color[5754]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
```

```
[root@localhost.astakhovamd.net ~]# dnf -y install lnav
Extra Packages for Enterprise Linux 9 - x86_64                                   2.4 kB/s |  36 kB     00:14
Extra Packages for Enterprise Linux 9 - x86_64                                    32 kB/s |  20 MB     10:41
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64             854  B/s | 993  B     00:01
Rocky Linux 9 - BaseOS                                                           216  B/s | 4.3 kB     00:20
Rocky Linux 9 - BaseOS                                                           206 kB/s | 5.1 MB     00:25
Rocky Linux 9 - AppStream                                                        576  B/s | 4.8 kB     00:08
Rocky Linux 9 - AppStream                                                         37 kB/s |  10 MB     04:44
Rocky Linux 9 - Extras                                                           397  B/s | 3.1 kB     00:07
Rocky Linux 9 - Extras                                                           1.8 kB/s |  16 kB     00:08
Dependencies resolved.
=======================================================================================================================
 Package                  Architecture             Version                             Repository                Size
=======================================================================================================================
Installing:
 lnav                     x86_64                   0.11.1-1.el9                        epel                     2.4 M

Transaction Summary
=======================================================================================================================
Install  1 Package

Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
lnav-0.11.1-1.el9.x86_64.rpm                                                      20 kB/s | 2.4 MB     02:02
-----------------------------------------------------------------------------------------------------------------------
Total                                                                             17 kB/s | 2.4 MB     02:21
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                             1/1
  Installing       : lnav-0.11.1-1.el9.x86_64                                                                    1/1
  Running scriptlet: lnav-0.11.1-1.el9.x86_64                                                                    1/1
  Verifying        : lnav-0.11.1-1.el9.x86_64                                                                    1/1

Installed:
  lnav-0.11.1-1.el9.x86_64

Complete!
[root@localhost.astakhovamd.net ~]#
```

ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ ВНУТРЕННЕГО ОКРУЖЕНИЯ ВИРТУАЛЬНЫХ МАШИН





ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ ВНУТРЕННЕГО ОКРУЖЕНИЯ ВИРТУАЛЬНЫХ МАШИН

```
#!/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
```

```
#!/bin/bash

echo "Provisioning script $0"
echo "Install needed packages"

dnf-y install lnav

echo "Copy configuration files"

cp-R /vagrant/provision/client/netlog/etc/* /etc
restorecon-vR /etc

echo "Start rsyslog service"

systemctl restart rsyslog
```

```
  server.vm.provision "server netlog",
                      type: "shell",
                      preserve_order: true,
                      path: "provision/server/netlog.sh"

end
```

```
client.vm.provision "client netlog",
      type: "shell",
      preserve_order: true,
      path: "provision/client/netlog.sh"

nd
```

СПАСИБО ЗА ВНИМАНИЕ!