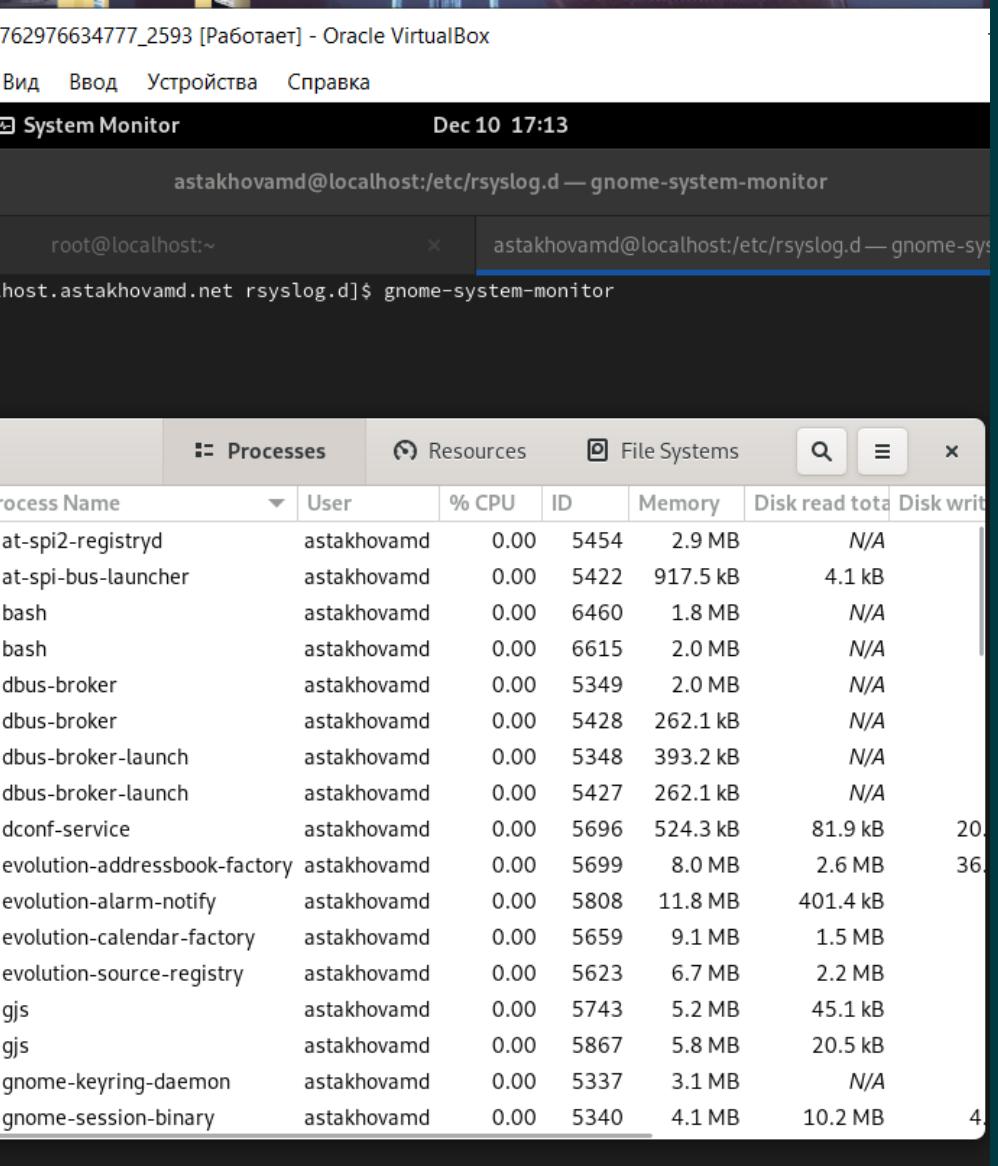


ЛАБОРАТОРНАЯ РАБОТА №15.
НАСТРОЙКА СЕТЕВОГО
ЖУРНАЛИРОВАНИЯ

Астахова Марина
Дмитриевна
НПИБД02-23

ЦЕЛЬ РАБОТЫ

Получение навыков по
работе с журналами
системных событий.



The screenshot shows the 'System Monitor' application window from Oracle VirtualBox. The title bar reads '762976634777_2593 [Работает] - Oracle VirtualBox'. The menu bar includes 'Вид', 'Ввод', 'Устройства', and 'Справка'. The top status bar shows the date and time: 'Dec 10 17:13'. The main window displays two terminal sessions: one for root at localhost (~) and another for astakhovamd at localhost (/etc/rsyslog.d). The command run in the second session is 'host.astakhovamd.net rsyslog.d]\$ gnome-system-monitor'. Below the terminals is a table titled 'Processes' with columns: process Name, User, % CPU, ID, Memory, Disk read total, and Disk write total. The table lists various system processes, all running under user 'astakhovamd' with 0.00% CPU usage. The table has 18 rows, with the last row partially visible.

process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
at-spi2-registryd	astakhovamd	0.00	5454	2.9 MB	N/A	
at-spi-bus-launcher	astakhovamd	0.00	5422	917.5 kB	4.1 kB	
bash	astakhovamd	0.00	6460	1.8 MB	N/A	
bash	astakhovamd	0.00	6615	2.0 MB	N/A	
dbus-broker	astakhovamd	0.00	5349	2.0 MB	N/A	
dbus-broker	astakhovamd	0.00	5428	262.1 kB	N/A	
dbus-broker-launch	astakhovamd	0.00	5348	393.2 kB	N/A	
dbus-broker-launch	astakhovamd	0.00	5427	262.1 kB	N/A	
dconf-service	astakhovamd	0.00	5696	524.3 kB	81.9 kB	20.1 kB
evolution-addressbook-factory	astakhovamd	0.00	5699	8.0 MB	2.6 MB	36.1 kB
evolution-alarm-notify	astakhovamd	0.00	5808	11.8 MB	401.4 kB	
evolution-calendar-factory	astakhovamd	0.00	5659	9.1 MB	1.5 MB	
evolution-source-registry	astakhovamd	0.00	5623	6.7 MB	2.2 MB	
gjs	astakhovamd	0.00	5743	5.2 MB	45.1 kB	
gjs	astakhovamd	0.00	5867	5.8 MB	20.5 kB	
gnome-keyring-daemon	astakhovamd	0.00	5337	3.1 MB	N/A	
gnome-session-binary	astakhovamd	0.00	5340	4.1 MB	10.2 MB	4.1 kB

ВЫПОЛНЕНИЕ РАБОТЫ

Настройка сервера сетевого журнала

```
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          0t0  TCP  *:sunrpc (LISTEN)
systemd    1          0t0  TCP  *:sunrpc (LISTEN)
rpcbind   617          0t0  TCP  *:sunrpc (LISTEN)
rpcbind   617          0t0  TCP  *:sunrpc (LISTEN)
cupsd     1057         0t0  TCP  localhost:ipp (LISTEN)
cupsd     1057         0t0  TCP  localhost:ipp (LISTEN)
sshd      1070         0t0  TCP  *:down (LISTEN)
sshd      1070         0t0  TCP  *:down (LISTEN)
sshd      1070         0t0  TCP  *:ssh (LISTEN)
sshd      1070         0t0  TCP  *:ssh (LISTEN)
rpc.mount 1128         0t0  TCP  *:mountd (LISTEN)
rpc.mount 1128         0t0  TCP  *:mountd (LISTEN)
named     1158         0t0  TCP  localhost:rndc (LISTEN)
named     1158         0t0  TCP  localhost:domain (LISTEN)
named     1158         0t0  TCP  localhost:domain (LISTEN)
```

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

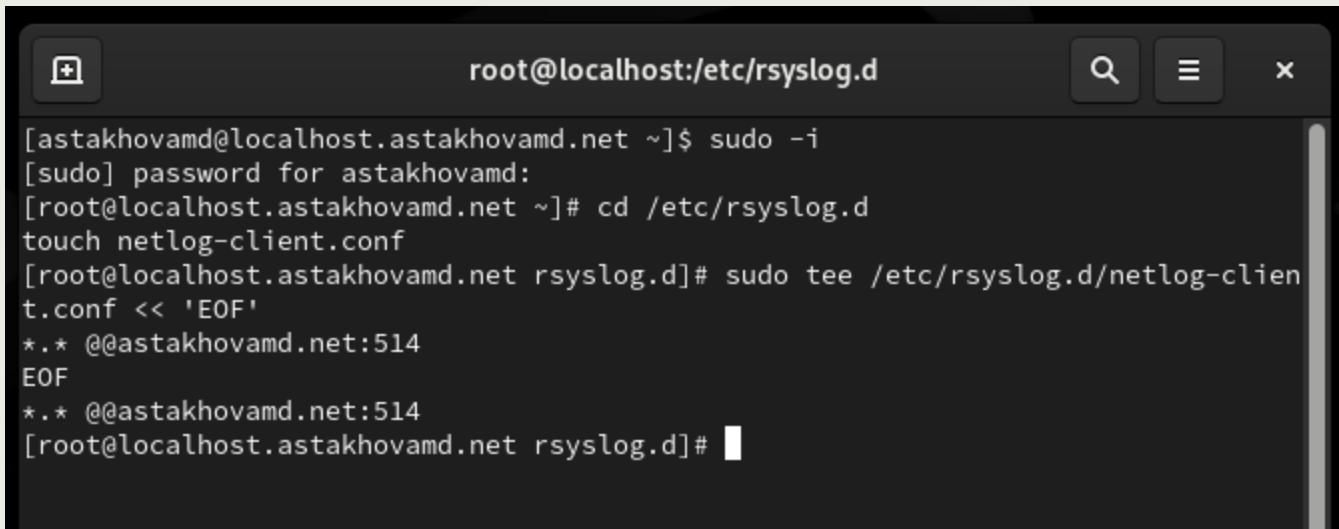
```
[root@localhost.astakhovamd.net rsyslog.d]# touch netlog-server.conf
[root@localhost.astakhovamd.net rsyslog.d]# sudo tee /etc/rsyslog.d/netlog-server.conf << 'EOF'
$ModLoad imtcp

$InputTCPServerRun 514
EOF
$ModLoad imtcp

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

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

Настройка клиента сетевого журнала



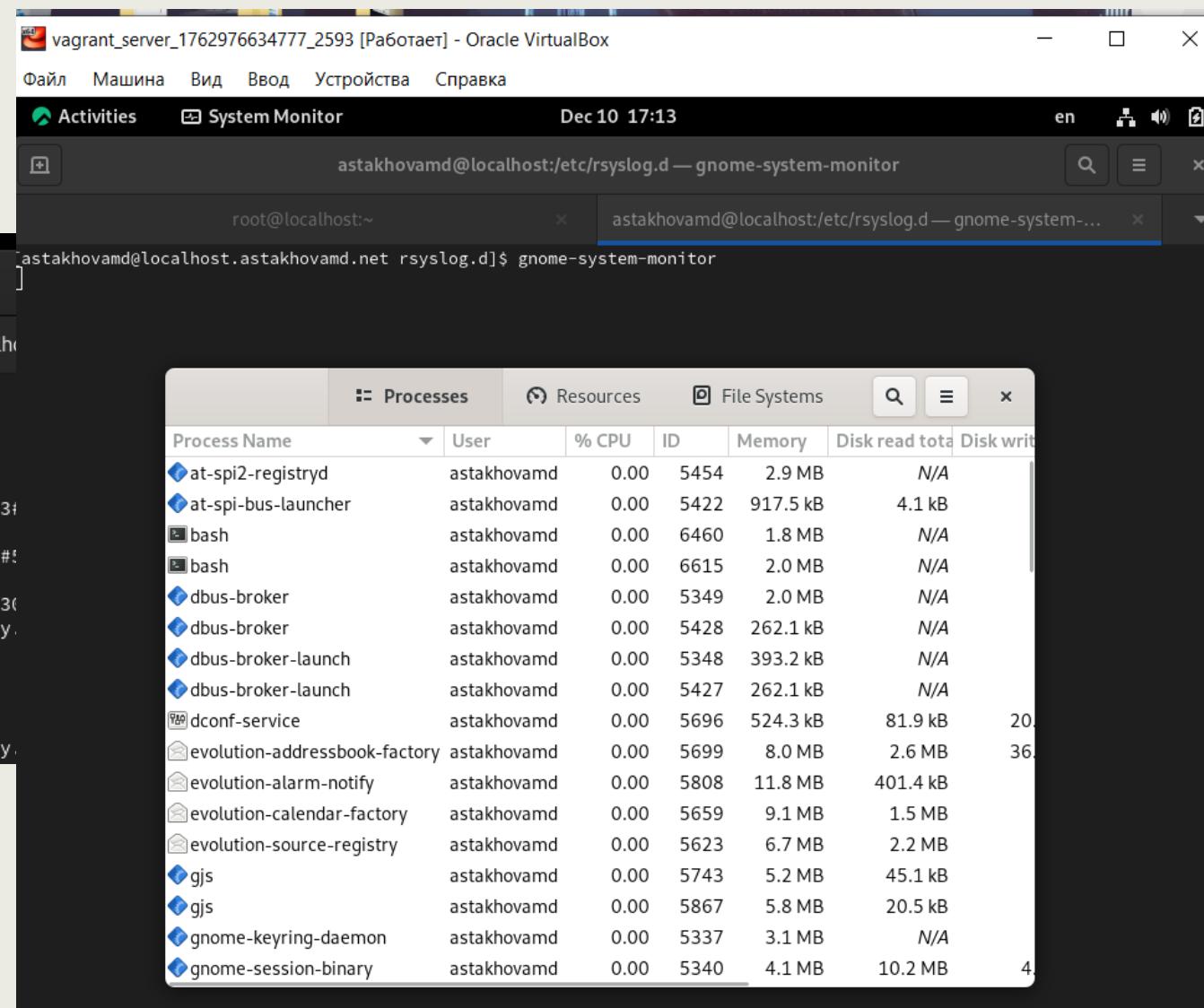
A screenshot of a terminal window titled "root@localhost:/etc/rsyslog.d". The terminal shows the following command sequence:

```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i  
[sudo] password for astakhovamd:  
[root@localhost.astakhovamd.net ~]# cd /etc/rsyslog.d  
touch netlog-client.conf  
[root@localhost.astakhovamd.net rsyslog.d]# sudo tee /etc/rsyslog.d/netlog-client.conf << 'EOF'  
.* @@astakhovamd.net:514  
EOF  
.* @@astakhovamd.net:514  
[root@localhost.astakhovamd.net rsyslog.d]#
```

```
[root@localhost.astakhovamd.net rsyslog.d]# systemctl restart rsyslog  
[root@localhost.astakhovamd.net rsyslog.d]#
```

Просмотр журнала

```
[astakhovamd@localhost.astakhovamd.net rsyslog.d]$ sudo -  
[sudo] password for astakhovamd:  
[root@localhost.astakhovamd.net ~]# tail -f /var/log/messages  
bash: tail-f: command not found...  
[root@localhost.astakhovamd.net ~]# tail -f /var/log/messages  
Dec 10 17:07:44 localhost named[1158]: no valid RRSIG resolving 'org/DS/IN': 202.12.27.33#  
Dec 10 17:07:47 localhost named[1158]: validating org/DS: no valid signature found  
Dec 10 17:07:47 localhost named[1158]: no valid RRSIG resolving 'org/DS/IN': 192.5.5.241#!  
Dec 10 17:07:47 localhost named[1158]: validating org/DS: no valid signature found  
Dec 10 17:07:47 localhost named[1158]: no valid RRSIG resolving 'org/DS/IN': 192.58.128.30#  
Dec 10 17:07:52 localhost systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Dec 10 17:12:53 localhost systemd[1]: Starting Hostname Service...  
Dec 10 17:12:53 localhost systemd[1]: Started Hostname Service.  
Dec 10 17:13:15 localhost systemd[1]: Starting PackageKit Daemon...  
Dec 10 17:13:15 localhost systemd[1]: Started PackageKit Daemon.  
Dec 10 17:13:23 localhost systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```



ПРОСМОТР ЖУРНАЛА

2025-12-10T18:11:09 UTC

LOG | 2025-12-10T17:33:00.000 | syslog_log | messages[792] | chrony[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 (From Cisco) - x86_64 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 Lease file cleanup
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 lease file cleanup
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/lib/kea/dhcp4.leases.3
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILELEASE_FILE_LOAD loading leases from file /var/lib/kea/dhcp4.leases.2
Dec 10 17:59:49 localhost DhcpLFC[46236]: INFO [DhcpLFC.dhcpsrv.140461865995584] DHCPSRV_MEMFILELEASE_FILE_LOAD loading leases from file /var/lib/kea/dhcp4.leases.3
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.astakhovam.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.astakhovam.net ~]#
```

ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ ВНУТРЕННЕГО ОКРУЖЕНИЯ ВИРТУАЛЬНЫХ МАШИН

rsyslog.d				
я	Поделиться	Вид		
Этот компьютер > Локальный диск (C:) > Users > Marine > Admitnet > vagrant > provision > client > netlog > etc > rsyslog.d				
ы Ру	Имя	Дата изменения	Тип	Размер
	netlog	10.12.2025 21:21	Shell Script	1 КБ

rsyslog.d				
я	Поделиться	Вид		
Этот компьютер > Локальный диск (C:) > Users > Marine > Admitnet > vagrant > provision > server > netlog > etc > rsyslog.d				
ы Ру	Имя	Дата изменения	Тип	Размер
	netlog-server	10.12.2025 21:19	Файл "CONF"	1 КБ

```
#!/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
```

ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ ВНУТРЕННЕГО ОКРУЖЕНИЯ ВИРТУАЛЬНЫХ МАШИН

```
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!