**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

# ОТЧЕТ
# ПО ЛАБОРАТОРНОЙ РАБОТЕ № 15

**Настройка сетевого журналирования**

*дисциплина: Администрирование Сетевых Подсистем*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

## Цель работы:

Получение навыков по работе с журналами системных событий.

## Выполнение работы:

### 1. Настройка сервера сетевого журнала

1. На сервере создайте файл конфигурации сетевого хранения журналов:

   cd /etc/rsyslog.d

   touch netlog-server.conf

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# cd /etc/rsyslog.d
[root@server.kreachna.net rsyslog.d]# touch netlog-server.conf
```

2. В файле конфигурации /etc/rsyslog.d/netlog-server.conf включите приём записей журнала по TCP-порту 514:

   $ModLoad imtcp

   $InputTCPServerRun 514

```
[root@server.kreachna.net rsyslog.d]# vim /etc/rsyslog.d/netlog-server.conf
[root@server.kreachna.net rsyslog.d]# cat /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

3. Перезапустите службу rsyslog и посмотрите, какие порты, связанные с rsyslog, прослушиваются:

   systemctl restart rsyslog

   lsof | grep TCP

```
[root@server.kreachna.net rsyslog.d]# systemctl restart rsyslog
[root@server.kreachna.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.
systemd      1                        root   44u     IPv4              17307       0t0        TCP *:sunrpc (LISTEN)
systemd      1                        root   46u     IPv6              17323       0t0        TCP *:sunrpc (LISTEN)
rpcbind    525                         rpc    4u     IPv4              17307       0t0        TCP *:sunrpc (LISTEN)
rpcbind    525                         rpc    6u     IPv6              17323       0t0        TCP *:sunrpc (LISTEN)
cupsd      695                        root    6u     IPv6              20721       0t0        TCP localhost:ipp (LIST
EN)
cupsd      695                        root    7u     IPv4              20722       0t0        TCP localhost:ipp (LIST
EN)
sshd       724                        root    3u     IPv4              20945       0t0        TCP *:down (LISTEN)
sshd       724                        root    4u     IPv6              20956       0t0        TCP *:down (LISTEN)
sshd       724                        root    5u     IPv4              20958       0t0        TCP *:ssh (LISTEN)
sshd       724                        root    6u     IPv6              20960       0t0        TCP *:ssh (LISTEN)
named      756                       named   17u     IPv4              21138       0t0        TCP localhost:domain (L
ISTEN)
named      756                       named   21u     IPv6              21140       0t0        TCP localhost:domain (L
ISTEN)
named      756                       named   22u     IPv4              21295       0t0        TCP localhost:rndc (LIS
TEN)
named      756                       named   23u     IPv6              21296       0t0        TCP localhost:rndc (LIS
TEN)
named      756                       named   24u     IPv4              22578       0t0        TCP server.kreachna.net
:domain (LISTEN)
named      756                       named   26u     IPv4              32258       0t0        TCP mail.kreachna.net:d
omain (LISTEN)
named      756  757 isc-net-0        named   17u     IPv4              21138       0t0        TCP localhost:domain (L
ISTEN)
named      756  757 isc-net-0        named   21u     IPv6              21140       0t0        TCP localhost:domain (L
ISTEN)
named      756  757 isc-net-0        named   22u     IPv4              21295       0t0        TCP localhost:rndc (LIS
```

```
rpc.mount 1113                          root    5u     IPv4              22706       0t0        TCP *:mountd (LISTEN)
rpc.mount 1113                          root    7u     IPv6              22721       0t0        TCP *:mountd (LISTEN)
dovecot   1116                          root   21u     IPv4              23145       0t0        TCP *:pop3 (LISTEN)
dovecot   1116                          root   22u     IPv6              23146       0t0        TCP *:pop3 (LISTEN)
dovecot   1116                          root   23u     IPv4              23147       0t0        TCP *:pop3s (LISTEN)
dovecot   1116                          root   24u     IPv6              23148       0t0        TCP *:pop3s (LISTEN)
dovecot   1116                          root   40u     IPv4              23164       0t0        TCP *:imap (LISTEN)
dovecot   1116                          root   41u     IPv6              23165       0t0        TCP *:imap (LISTEN)
dovecot   1116                          root   42u     IPv4              23166       0t0        TCP *:imaps (LISTEN)
dovecot   1116                          root   43u     IPv6              23167       0t0        TCP *:imaps (LISTEN)
smbd      6650                          root   35u     IPv4              40199       0t0        TCP mail.kreachna.net:m
icrosoft-ds->client.kreachna.net:46774 (ESTABLISHED)
rsyslogd  6806                          root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806                          root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6807 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6807 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6809 in:imjour           root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6809 in:imjour           root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6810 rs:main             root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6810 rs:main             root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6811 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6811 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6812 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6812 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6813 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6813 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6814 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6814 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
```

4. На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514:

   firewall-cmd --add-port=514/tcp

   firewall-cmd --add-port=514/tcp –permanent

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

## 2. Настройка клиента сетевого журнала

1. На клиенте создайте файл конфигурации сетевого хранения журналов:

   cd /etc/rsyslog.d

   touch netlog-client.conf

```
[kreachna@client.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@client.kreachna.net ~]# cd /etc/rsyslog.d
[root@client.kreachna.net rsyslog.d]# touch netlog-client.conf
```

2. На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включите перенаправление сообщений журнала на 514 TCP-порт сервера (вместо user укажите свой логин):

   *.* @@server.user.net:514

```
[root@client.kreachna.net rsyslog.d]# vim /etc/rsyslog.d/netlog-client.conf
[root@client.kreachna.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*.* @@server.kreachna.net:514
```

3. Перезапустите службу rsyslog:

   systemctl restart rsyslog

```
[root@client.kreachna.net rsyslog.d]# systemctl restart rsyslog
```

## 3. Просмотр журнала

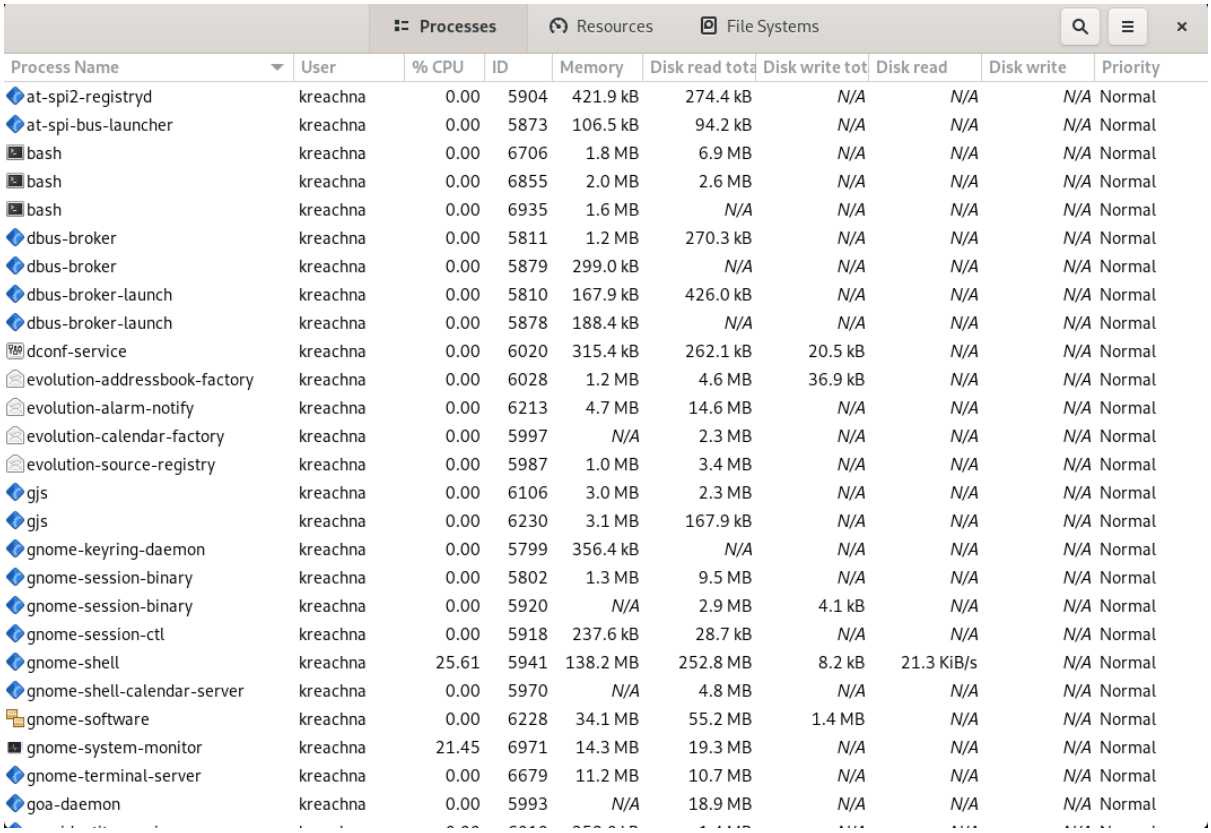
1. На сервере просмотрите один из файлов журнала

tail -f /var/log/messages

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# tail -f /var/log/messages
Dec 30 17:22:26 client rsyslogd[559]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="559" x-info="http
s://www.rsyslog.com"] exiting on signal 15.
Dec 30 17:22:26 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec 30 17:22:26 client systemd[1]: Stopped System Logging Service.
Dec 30 17:22:26 client systemd[1]: Starting System Logging Service...
Dec 30 17:22:26 client systemd[1]: Started System Logging Service.
Dec 30 17:22:26 client rsyslogd[5534]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="5534" x-info="ht
tps://www.rsyslog.com"] start
Dec 30 17:22:26 client rsyslogd[5534]: imjournal: journal files changed, reloading...  [v8.2102.0-105.el9 try https://w
ww.rsyslog.com/e/0 ]
Dec 30 17:22:46 server systemd[5787]: Started VTE child process 6855 launched by gnome-terminal-server process 6679.
Dec 30 17:22:52 server systemd[1]: Starting Hostname Service...
Dec 30 17:22:52 server systemd[1]: Started Hostname Service.
Dec 30 17:23:04 client NetworkManager[4441]: <info>  [1672410184.5317] dhcp4 (eth1): state changed new lease, address=1
92.168.1.30
Dec 30 17:23:04 server dhcpd[1092]: DHCPREQUEST for 192.168.1.30 from 08:00:27:83:06:b8 (client) via eth1
Dec 30 17:23:04 server dhcpd[1092]: DHCPACK on 192.168.1.30 to 08:00:27:83:06:b8 (client) via eth1
Dec 30 17:23:22 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 30 17:23:29 server systemd[1]: Starting Cleanup of Temporary Directories...
Dec 30 17:23:29 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec 30 17:23:29 server systemd[1]: Finished Cleanup of Temporary Directories.
Dec 30 17:24:31 server systemd[5787]: Started VTE child process 6935 launched by gnome-terminal-server process 6679.
```

2. На сервере под пользователем user (вместо user укажите свой логин) запустите графическую программу для просмотра журналов:

   gnome-system-monitor




| Process Name | User | % CPU | ID | Memory | Disk read tota | Disk write tot | Disk read | Disk write | Priority |
|---|---|---|---|---|---|---|---|---|---|
| at-spi2-registryd | kreachna | 0.00 | 5904 | 421.9 kB | 274.4 kB | N/A | N/A | N/A | Normal |
| at-spi-bus-launcher | kreachna | 0.00 | 5873 | 106.5 kB | 94.2 kB | N/A | N/A | N/A | Normal |
| bash | kreachna | 0.00 | 6706 | 1.8 MB | 6.9 MB | N/A | N/A | N/A | Normal |
| bash | kreachna | 0.00 | 6855 | 2.0 MB | 2.6 MB | N/A | N/A | N/A | Normal |
| bash | kreachna | 0.00 | 6935 | 1.6 MB | N/A | N/A | N/A | N/A | Normal |
| dbus-broker | kreachna | 0.00 | 5811 | 1.2 MB | 270.3 kB | N/A | N/A | N/A | Normal |
| dbus-broker | kreachna | 0.00 | 5879 | 299.0 kB | N/A | N/A | N/A | N/A | Normal |
| dbus-broker-launch | kreachna | 0.00 | 5810 | 167.9 kB | 426.0 kB | N/A | N/A | N/A | Normal |
| dbus-broker-launch | kreachna | 0.00 | 5878 | 188.4 kB | N/A | N/A | N/A | N/A | Normal |
| dconf-service | kreachna | 0.00 | 6020 | 315.4 kB | 262.1 kB | 20.5 kB | N/A | N/A | Normal |
| evolution-addressbook-factory | kreachna | 0.00 | 6028 | 1.2 MB | 4.6 MB | 36.9 kB | N/A | N/A | Normal |
| evolution-alarm-notify | kreachna | 0.00 | 6213 | 4.7 MB | 14.6 MB | N/A | N/A | N/A | Normal |
| evolution-calendar-factory | kreachna | 0.00 | 5997 | N/A | 2.3 MB | N/A | N/A | N/A | Normal |
| evolution-source-registry | kreachna | 0.00 | 5987 | 1.0 MB | 3.4 MB | N/A | N/A | N/A | Normal |
| gjs | kreachna | 0.00 | 6106 | 3.0 MB | 2.3 MB | N/A | N/A | N/A | Normal |
| gjs | kreachna | 0.00 | 6230 | 3.1 MB | 167.9 kB | N/A | N/A | N/A | Normal |
| gnome-keyring-daemon | kreachna | 0.00 | 5799 | 356.4 kB | N/A | N/A | N/A | N/A | Normal |
| gnome-session-binary | kreachna | 0.00 | 5802 | 1.3 MB | 9.5 MB | N/A | N/A | N/A | Normal |
| gnome-session-binary | kreachna | 0.00 | 5920 | N/A | 2.9 MB | 4.1 kB | N/A | N/A | Normal |
| gnome-session-ctl | kreachna | 0.00 | 5918 | 237.6 kB | 28.7 kB | N/A | N/A | N/A | Normal |
| gnome-shell | kreachna | 25.61 | 5941 | 138.2 MB | 252.8 MB | 8.2 kB | 21.3 KiB/s | N/A | Normal |
| gnome-shell-calendar-server | kreachna | 0.00 | 5970 | N/A | 4.8 MB | N/A | N/A | N/A | Normal |
| gnome-software | kreachna | 0.00 | 6228 | 34.1 MB | 55.2 MB | 1.4 MB | N/A | N/A | Normal |
| gnome-system-monitor | kreachna | 21.45 | 6971 | 14.3 MB | 19.3 MB | N/A | N/A | N/A | Normal |
| gnome-terminal-server | kreachna | 0.00 | 6679 | 11.2 MB | 10.7 MB | N/A | N/A | N/A | Normal |
| goa-daemon | kreachna | 0.00 | 5993 | N/A | 18.9 MB | N/A | N/A | N/A | Normal |

3. На сервере установите просмотрщик журналов системных сообщений lnav:

   dnf -y install lnav

```
[root@server.kreachna.net rsyslog.d]# dnf -y install lnav
Extra Packages for Enterprise Linux 9 - x86_64                  27 kB/s |  29 kB     00:01
Extra Packages for Enterprise Linux 9 - x86_64                 6.1 MB/s |  12 MB     00:01
Rocky Linux 9 - BaseOS                                         3.1 kB/s | 3.6 kB     00:01
Rocky Linux 9 - AppStream                                      6.8 kB/s | 4.1 kB     00:00
Rocky Linux 9 - Extras                                         5.4 kB/s | 2.9 kB     00:00
No match for argument: lnav
Error: Unable to find a match: lnav
```

4. Просмотрите логи с помощью lnav:

   lnav

```
[root@server.kreachna.net rsyslog.d]# lnav
bash: lnav: command not found...
```

```
[root@server.kreachna.net rsyslog.d]# journalctl
Dec 30 17:08:28 server.kreachna.net kernel: Linux version 5.14.0-162.6.1.el9_1.0.1.x86_64 (mockbuild@dal1-prod-bui>
Dec 30 17:08:28 server.kreachna.net kernel: The list of certified hardware and cloud instances for Enterprise Linu>
Dec 30 17:08:28 server.kreachna.net kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/boot/vmlinuz-5.14.0-162.6.1.el9_>
Dec 30 17:08:28 server.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Dec 30 17:08:28 server.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Dec 30 17:08:28 server.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Dec 30 17:08:28 server.kreachna.net kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Dec 30 17:08:28 server.kreachna.net kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using>
Dec 30 17:08:28 server.kreachna.net kernel: signal: max sigframe size: 1776
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-provided physical RAM map:
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: NX (Execute Disable) protection: active
Dec 30 17:08:28 server.kreachna.net kernel: SMBIOS 2.5 present.
Dec 30 17:08:28 server.kreachna.net kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Dec 30 17:08:28 server.kreachna.net kernel: Hypervisor detected: KVM
Dec 30 17:08:28 server.kreachna.net kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Dec 30 17:08:28 server.kreachna.net kernel: kvm-clock: using sched offset of 5496750239 cycles
Dec 30 17:08:28 server.kreachna.net kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4>
Dec 30 17:08:28 server.kreachna.net kernel: tsc: Detected 2207.998 MHz processor
Dec 30 17:08:28 server.kreachna.net kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Dec 30 17:08:28 server.kreachna.net kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Dec 30 17:08:28 server.kreachna.net kernel: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
Dec 30 17:08:28 server.kreachna.net kernel: Disabled
Dec 30 17:08:28 server.kreachna.net kernel: x86/PAT: MTRRs disabled, skipping PAT initialization too.
Dec 30 17:08:28 server.kreachna.net kernel: CPU MTRRs all blank - virtualized system.
Dec 30 17:08:28 server.kreachna.net kernel: x86/PAT: Configuration [0-7]: WB  WT  UC- UC  WB  WT  UC- UC
Dec 30 17:08:28 server.kreachna.net kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
Dec 30 17:08:28 server.kreachna.net kernel: RAMDISK: [mem 0x31acf000-0x34d5ffff]
Dec 30 17:08:28 server.kreachna.net kernel: ACPI: Early table checksum verification disabled
```

```
[root@client.kreachna.net rsyslog.d]# journalctl
Dec 30 17:12:47 client.kreachna.net kernel: Linux version 5.14.0-162.6.1.el9_1.0.1.x86_64 (mockbu>
Dec 30 17:12:47 client.kreachna.net kernel: The list of certified hardware and cloud instances fo>
Dec 30 17:12:47 client.kreachna.net kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/boot/vmlinuz-5.>
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floatin>
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registe>
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registe>
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: Enabled xstate features 0x7, context size is>
Dec 30 17:12:47 client.kreachna.net kernel: signal: max sigframe size: 1776
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-provided physical RAM map:
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff>
Dec 30 17:12:47 client.kreachna.net kernel: NX (Execute Disable) protection: active
Dec 30 17:12:47 client.kreachna.net kernel: SMBIOS 2.5 present.
Dec 30 17:12:47 client.kreachna.net kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Virtual>
Dec 30 17:12:47 client.kreachna.net kernel: Hypervisor detected: KVM
Dec 30 17:12:47 client.kreachna.net kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Dec 30 17:12:47 client.kreachna.net kernel: kvm-clock: using sched offset of 5779140117 cycles
Dec 30 17:12:47 client.kreachna.net kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_>
Dec 30 17:12:47 client.kreachna.net kernel: tsc: Detected 2207.998 MHz processor
Dec 30 17:12:47 client.kreachna.net kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> r>
Dec 30 17:12:47 client.kreachna.net kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Dec 30 17:12:47 client.kreachna.net kernel: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
lines 1-29
```

Просмотрите записи с сервера и клиента.

## 4. Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
[root@server.kreachna.net ~]# cd /vagrant/provision/server
[root@server.kreachna.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.kreachna.net server]# cp -R /etc/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
cp: cannot stat '/etc/netlog-server.conf': No such file or directory
[root@server.kreachna.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog
.d
```

2. В каталоге /vagrant/provision/server создайте исполняемый файл netlog.sh:

   cd /vagrant/provision/server

   touch netlog.sh

   chmod +x netlog.sh

```
[root@server.kreachna.net server]# cd /vagrant/provision/server
[root@server.kreachna.net server]# touch netlog.sh
[root@server.kreachna.net server]# chmod +x netlog.sh
[root@server.kreachna.net server]#
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

nfs.sh | netlog.sh | netlog.sh | Vagrantfile

```
#!/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
```

3. На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создайте в нём каталог nentlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
[root@client.kreachna.net ~]# cd /vagrant/provision/client
[root@client.kreachna.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.kreachna.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc
/rsyslog.d/
```

4. В каталоге /vagrant/provision/client создайте исполняемый файл netlog.sh:

   cd /vagrant/provision/client

   touch netlog.sh

   chmod +x netlog.sh

```
[root@client.kreachna.net client]# cd /vagrant/provision/client
[root@client.kreachna.net client]# touch netlog.sh
[root@client.kreachna.net client]# chmod +x netlog.sh
[root@client.kreachna.net client]#
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

s.sh | netlog.sh | netlog.sh | Vagrantfile

```
#!/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
```

5. Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента:



## Ответы на контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?

   imjournal

2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?

   imuxsock

3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?

   $OmitLocalLogging on – данная строка отключает прием логов через модуль imuxsock.

4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?

   Все настройки rsyslog находятся в файле /etc/rsyslog.conf.

5. Каким параметром управляется пересылка сообщений из journald в rsyslog?

   Journald отправляет сообщения в rsyslog по умолчанию. Об этом заботятся две части конфигурации. Во-первых, файл /etc/systemd/journald.conf содержит строку ForwardToSyslog, которая по умолчанию имеет значение yes. Вовторых rsyslog.conf содержит модуль imjournal, необходимый для получения сообщений из journald.

6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

   imfile - модуль ввода текстовых файлов

7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?

   ommysql

8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?

$ModLoad imtcp и $InputTCPServerRun 514

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

   firewall-cmd --add-port=514/tcp

   firewall-cmd --add-port=514/tcp --permanent

## Вывод:

Получила навыков по работе с журналами системных событий.