

# **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 (LISTEN)
cupsd       695        root     7u    IPv4        20722      0t0      TCP localhost:ipp (LISTEN)
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 (LISTEN)
named       756        named    21u    IPv6        21140      0t0      TCP localhost:domain (LISTEN)
named       756        named    22u    IPv4        21295      0t0      TCP localhost:rndc (LISTEN)
named       756        named    23u    IPv6        21296      0t0      TCP localhost:rndc (LISTEN)
named       756        named    24u    IPv4        22578      0t0      TCP server.kreachna.net:domain (LISTEN)
named       756        named    26u    IPv4        32258      0t0      TCP mail.kreachna.net:domain (LISTEN)
named       756 757 isc-net-0 17u    IPv4        21138      0t0      TCP localhost:domain (LISTEN)
named       756 757 isc-net-0 21u    IPv6        21140      0t0      TCP localhost:domain (LISTEN)
named       756 757 isc-net-0 22u    IPv4        21295      0t0      TCP localhost:rndc (LISTEN)
```

```

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

		Processes		Resources		File Systems			
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@dall-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 0x0000000000000000-0x0000000000009fbfff] usable
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x0000000000009fc000-0x0000000000009fffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x000000000000f00000-0x000000000000ffffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x000000000001000000-0x0000000000003fffff] usable
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x000000000003fff00000-0x000000000003ffffffffff] ACPI data
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fec0000000-0x00000000fec00fffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fee0000000-0x00000000fee00fffff] reserved
Dec 30 17:08:28 server.kreachna.net kernel: BIOS-e820: [mem 0x00000000fffc000000-0x00000000ffffffffffff] 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 0x00000000-0x00000fffff] usable ==> reserved
Dec 30 17:08:28 server.kreachna.net kernel: e820: remove [mem 0x000a00000-0x000fffff] 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 0x0009fff0-0x0009fffff]
Dec 30 17:08:28 server.kreachna.net kernel: RAMDISK: [mem 0x31acf000-0x34d5fffff]
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 regist>
Dec 30 17:12:47 client.kreachna.net kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX regist>
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 0x0000000000100000-0x00000000003ffeffff>
Dec 30 17:12:47 client.kreachna.net kernel: BIOS-e820: [mem 0x00000000003fff0000-0x000000003ffffff>
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 0x00000000fffc0000-0x00000000ffffff>
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 = 0x40000000
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 x netlog.sh x netlog.sh x Vagrantfile x
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/netlog/etc/* /etc
7  restorecon -vR /etc
8
9  echo "Configure firewall"
10 firewall-cmd --add-port=514/tcp
11 firewall-cmd --add-port=514/tcp --permanent
12
13 echo "Start rsyslog service"
14 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 netlog, 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 x netlog.sh x netlog.sh x Vagrantfile x
#!/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:

```
9
10     server.vm.provision "server netlog",
11         type: "shell",
12         preserve_order: true,
13         path: "provision/server/netlog.sh"
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

## 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. Во-вторых 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.