

Лабораторная работа

Номер 15

Кобзев Д. К.
Российский университет дружбы народов, Москва, Россия
7 декабря 2025

Информация

Докладчик

- ▶ Кобзев Дмитрий Константинович
- ▶ Студент
- ▶ Российский университет дружбы народов
- ▶ НПИбд-01-23

Цель работы

Целью данной работы является получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала

На сервере создаем файл конфигурации сетевого хранения журналов (Рис. 12.1).

```
[dkkobzev@server.dkkobzev.net ~]$ cd /etc/rsyslog.d  
[dkkobzev@server.dkkobzev.net rsyslog.d]$ touch netlog-server.conf  
touch: cannot touch 'netlog-server.conf': Permission denied  
[dkkobzev@server.dkkobzev.net rsyslog.d]$ sudo -i  
[sudo] password for dkkobzev:  
[root@server.dkkobzev.net ~]# touch netlog-server.conf
```

Рис. 1: Создание файла конфигурации сетевого хранения журналов

Настройка сервера сетевого журнала

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включаем приём записей журнала по TCP-порту 514 (Рис. 12.2).

```
GNU nano 8.1                                     /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 2: Файл конфигурации /etc/rsyslog.d/netlog-server.conf

Настройка сервера сетевого журнала

Перезапускаем службу rsyslog и смотрим, какие порты, связанные с rsyslog, прослушиваются. На сервере настраиваем межсетевой экран для приёма сообщений по TCP-порту 514 (Рис. 12.3).

rsyslogd 13129	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13131 in:imjour	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13131 in:imjour	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13132 in:imtcp	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13132 in:imtcp	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13133 in:imtcp	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13133 in:imtcp	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13134 in:imtcp	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13134 in:imtcp	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13135 in:imtcp	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13135 in:imtcp	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13136 in:imtcp	root	4u	IPv4	44519	0t0	TCP *:shell (LISTEN)
rsyslogd 13129 13136 in:imtcp	root	5u	IPv6	44520	0t0	TCP *:shell (LISTEN)
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp success						
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp --permanent success						

Рис. 3: Настройка сервера сетевого журнала

Настройка клиента сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов (Рис. 12.4).

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

Рис. 4: Создание файла конфигурации сетевого хранения журналов

Настройка клиента сетевого журнала

На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включаем перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 12.5).

```
GNU nano 8.1                                     netlog-client.conf
*. * @@server.dkkobzev.net:514
```

Рис. 5: Файл конфигурации /etc/rsyslog.d/netlog-client.conf

Настройка клиента сетевого журнала

Перезапускаем службу rsyslog (Рис. 12.6).

```
[root@client.dkkobzev.net ~]# systemctl restart rsyslog
```

Рис. 6: Перезапуск службы rsyslog

Просмотр журнала

На сервере смотрим один из файлов журнала (Рис. 12.7).

```
[root@server.dkkobzev.net ~]# tail -f /var/log/messages
Dec  7 16:56:08 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec  7 16:56:08 server systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
Dec  7 16:56:57 client systemd[1]: Stopping rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[1447]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="1447" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec  7 16:56:57 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec  7 16:56:57 client systemd[1]: Stopped rsyslog.service - System Logging Service.
Dec  7 16:56:57 client systemd[1]: Starting rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[9941]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="9941" x-info="https://www.rsyslog.com"] start
Dec  7 16:56:57 client systemd[1]: Started rsyslog.service - System Logging Service.
Dec  7 16:56:57 client rsyslogd[9941]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Dec  7 16:57:41 server systemd[6406]: Started run-p13552-i13852.scope - [systemd-run] /usr/bin/bash.
Dec  7 16:58:10 client systemd[8440]: Created slice background.slice - User Background Tasks Slice.
Dec  7 16:58:10 client systemd[8440]: Starting systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directories...
Dec  7 16:58:10 client systemd[8440]: Finished systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directories.
```

Рис. 7: Один из файлов журнала

Просмотр журнала

На сервере под пользователем user запускаем графическую программу для просмотра журналов (Рис. 12.8).

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total	Disk read	Disk write	Priority
at-spi2-registryd	dikobzev	0.00	5066	131.1 kB	987.1 kB	N/A	N/A	N/A	Normal
at-spi-bus-launcher	dikobzev	0.00	5017	N/A	716.8 kB	N/A	N/A	N/A	Normal
bash	dikobzev	0.00	12463	131.1 kB	25.7 MB	N/A	N/A	N/A	Normal
bash	dikobzev	0.00	13552	N/A	614.4 kB	N/A	N/A	N/A	Normal
catatonit	dikobzev	0.00	12378	N/A	725.8 kB	N/A	N/A	N/A	Normal
dbus-broker	dikobzev	0.17	8425	917.5 kB	4.2 MB	N/A	1.3 kB/s	N/A	Normal
dbus-broker	dikobzev	0.00	5049	131.1 kB	626.7 kB	N/A	N/A	N/A	Normal
dbus-broker-launch	dikobzev	0.00	8428	N/A	1.3 MB	N/A	N/A	N/A	Normal
dbus-broker-launch	dikobzev	0.00	5048	131.1 kB	8.2 kB	N/A	N/A	N/A	Normal
dconf-service	dikobzev	0.35	9246	393.2 kB	1.7 MB	278.5 kB	N/A	56.0 kB/s	Normal
evolution-addressbook-factory	dikobzev	0.00	5086	131.1 kB	2.4 MB	53.2 kB	N/A	N/A	Normal
evolution-alarm-notify	dikobzev	0.00	9376	393.2 kB	6.0 kB	N/A	N/A	N/A	Normal
evolution-calendar-factory	dikobzev	0.00	5003	131.1 kB	4.5 MB	N/A	N/A	N/A	Normal
evolution-source-registry	dikobzev	0.00	9277	131.1 kB	2.2 MB	N/A	N/A	N/A	Normal
firefox	dikobzev	0.52	11203	178.2 MB	2.3 GB	170.8 MB	94.7 kB/s	52.0 kB/s	Normal
firefox	dikobzev	0.00	22091	3.0 MB	57.7 MB	N/A	N/A	N/A	Normal
gnome-wayland-session	dikobzev	0.00	8303	N/A	12.3 kB	N/A	N/A	N/A	Normal
gjs	dikobzev	0.00	9315	41.0 kB	3.5 MB	N/A	N/A	N/A	Normal
gjs	dikobzev	0.00	9681	77.8 kB	3.4 MB	N/A	N/A	N/A	Normal
gnome-keyring-daemon	dikobzev	0.00	6561	192.5 kB	6.1 MB	4.1 kB	N/A	N/A	Normal
gnome-session-binary	dikobzev	0.00	8431	N/A	98.1 kB	N/A	N/A	N/A	Normal
gnome-session-binary	dikobzev	0.00	8584	262.1 kB	4.8 MB	4.1 kB	N/A	N/A	Normal
gnome-session-ctl	dikobzev	0.00	8579	N/A	24.6 kB	N/A	N/A	N/A	Normal
gnome-shell	dikobzev	0.51	8658	148.7 MB	956.7 MB	176.1 kB	4.0 MB/s	N/A	Normal
gnome-shell-calendar-server	dikobzev	0.00	9228	131.1 kB	8.9 MB	N/A	N/A	N/A	Normal
gnome-software	dikobzev	0.00	9408	2.6 MB	122.1 MB	N/A	N/A	N/A	Normal
gnome-system-monitor	dikobzev	23.78	13581	92.1 MB	216.4 MB	65.5 kB	1.4 MB/s	5.3 kB/s	Normal
gpa-daemon	dikobzev	0.00	5562	131.1 kB	667.6 kB	N/A	N/A	N/A	Normal
gpa-identity-service	dikobzev	0.00	9783	262.1 kB	774.1 kB	N/A	N/A	N/A	Normal
gsd-ally-settings	dikobzev	0.00	9321	N/A	8.2 kB	N/A	N/A	N/A	Normal
gsd-color	dikobzev	0.00	9325	393.2 kB	2.1 MB	N/A	N/A	N/A	Normal

Рис. 8: Графическая программа для просмотра журналов

Просмотр журнала

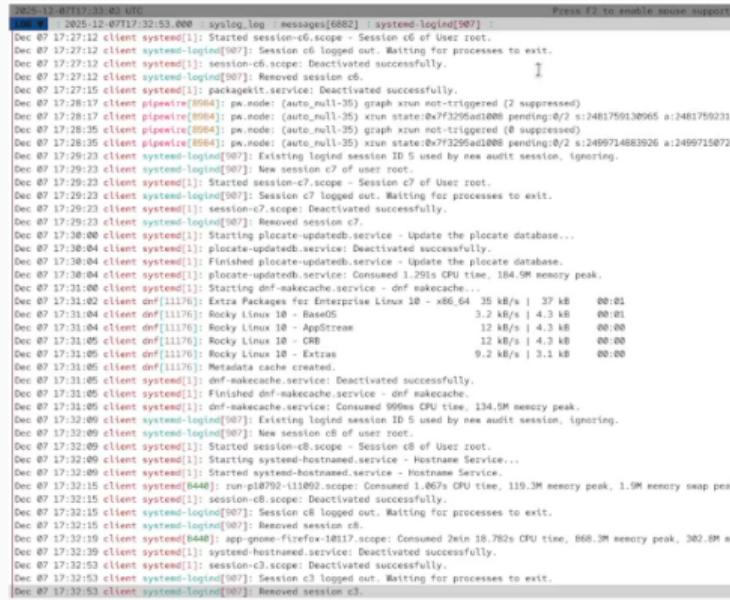
Просмотрите логи с сервера с помощью lnav (Рис. 12.9).

```
Dec 07 17:18:58 server tracker-miner-fs-3.service[1100]: Could not create store. Database version is too old: got version 8, but 29 is a
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:18:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service: Unit tracker-miner-fs-3.service failed to start.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 1.
Dec 07 17:18:59 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner...
Dec 07 17:18:59 server tracker-miner-fs-3.service[1101]: Could not create store. Database version is too old: got version 8, but 29 is a
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:18:59 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 2.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Failed to start tracker-miner-fs-3.service: Unit tracker-miner-fs-3.service failed to start.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 3.
Dec 07 17:18:59 server systemd[6400]: tracker-miner-fs-3.service: Failed to start tracker-miner-fs-3.service: Unit tracker-miner-fs-3.service failed to start.
Dec 07 17:11:00 server tracker-miner-fs-3.service[1102]: Could not create store. Database version is too old: got version 8, but 29 is a
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:11:00 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 4.
Dec 07 17:11:00 server systemd[6400]: Starting tracker-miner-fs-3.service - Tracker file system data miner...
Dec 07 17:11:00 server tracker-miner-fs-3.service[1103]: Could not create store. Database version is too old: got version 8, but 29 is a
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Main process exited, code=exited, status=1/FAILURE
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:11:00 server systemd[6400]: Failed to start tracker-miner-fs-3.service: Unit tracker-miner-fs-3.service failed to start.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Scheduled restart job, restart counter is at 5.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Failed to start tracker-miner-fs-3.service: Unit tracker-miner-fs-3.service failed to start.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Start request repeated too quickly.
Dec 07 17:11:00 server systemd[6400]: tracker-miner-fs-3.service: Failed with result 'exit-code'.
Dec 07 17:11:00 server systemd[6400]: Failed to start tracker-miner-fs-3.service - Tracker file system data miner.
Dec 07 17:11:01 server tracker-miner-fs-3.service[1104]: Failed to create connection for session-user:Tracker Indexer: Could not activate result
Dec 07 17:11:02 server systemd[1]: Started system-hostname.service - Hostname Service...
Dec 07 17:11:03 server gdm[1105]: Warning: X server configuration: last_fov_size (1075000) is greater than configuration timeout (4000). This will cause the X server to freeze in this state. Please reduce the last_fov_size or increase the configuration timeout.
Dec 07 17:11:13 server firejail.desktop[12001]: Critical Annotation GraphicsCriticalError: [[04][0932-1]] Managed to allocate after
Dec 07 17:11:23 server systemd[1]: packagekit.service: Deactivated successfully.
Dec 07 17:11:23 server systemd[1]: packagekit.service: Consumed 38.423s CPU time, 580.18 memory peak, 232.08 memory swap peak.
Dec 07 17:11:37 server systemd[1]: Starting system-hostname.service - Hostname Service...
Dec 07 17:11:37 server systemd[1]: Started system-hostname.service - Hostname Service.
Dec 07 17:12:07 server systemd[1]: system-hostname.service: Deactivated successfully.
Dec 07 17:12:25 server systemd[6400]: Started org-freedesktopUPnP@ scope [upnpd-run] /usr/bin/bash.
Dec 07 17:12:25 server systemd[6400]: Started org-freedesktopUPnP@ scope [upnpd-run] /usr/bin/bash.
Dec 07 17:13:56 server systemd[1]: Starting packagekit.service - PackageKit Daemon...
Dec 07 17:13:57 server systemd[1]: Started packagekit.service - PackageKit Daemon.
Dec 07 17:13:57 server systemd[6400]: dmes:1:2 eng generic Noutflus0d:service Consumed 3.864ms CPU time, 277.07 memory peak, 16
Dec 07 17:14:15 server systemd[1]: Starting plciate-updated.service - Update the plciate database...
Dec 07 17:14:15 server systemd[1]: plciate-updated.service: Deactivated successfully.
    Press TAB to scroll
L205 69% 7/View Help
```

Рис. 9: Логи с сервера

Просмотр журнала

Просмотрите логи с клиента с помощью lnav (Рис. 12.10).



```
lnav - 2025-12-07T17:33:03 UTC
Dec 07 17:27:12 client syslogd[32:53.000]: syslogd.log : messages[6882] : systemd-logind[907] :
Dec 07 17:27:12 client systemd[1]: Started session-c6.scope - Session c6 of User root.
Dec 07 17:27:12 client systemd-logind[907]: Session c6 logged out. Waiting for processes to exit.
Dec 07 17:27:12 client systemd[1]: session-c6.scope: Deactivated successfully.
Dec 07 17:27:12 client systemd-logind[907]: Removed session c6.
Dec 07 17:27:15 client systemd[1]: packagekit.service: Deactivated successfully.
Dec 07 17:28:17 client pipewire[8984]: pa-node: (auto_null-35) graph xrun not-triggered (2 suppressed)
Dec 07 17:28:17 client pipewire[8984]: pa-node: (auto_null-35) xrun state:0x7732956d0000 pending:0/7 s:2461759138965 n:24617592331
Dec 07 17:28:39 client pipewire[8984]: pa-node: (auto_null-35) graph xrun not-triggered (0 suppressed)
Dec 07 17:28:40 client pipewire[8984]: pa-node: (auto_null-35) xrun state:0x7732956d0000 pending:0/2 s:2409714883926 a:2409714883926
Dec 07 17:28:40 client pipewire[8984]: pa-node: (auto_null-35) xrun state:0x7732956d0000 pending:0/2 s:2409714883926 a:2409714883926
Dec 07 17:29:23 client systemd-logind[907]: Existing logind session ID 5 used by new audit session, ignoring.
Dec 07 17:29:23 client systemd-logind[907]: New session c7 of user root.
Dec 07 17:29:23 client systemd[1]: Started session-c7.scope - Session c7 of User root.
Dec 07 17:29:23 client systemd-logind[907]: Session c7 logged out. Waiting for processes to exit.
Dec 07 17:29:23 client systemd[1]: session-c7.scope: Deactivated successfully.
Dec 07 17:29:23 client systemd-logind[907]: Removed session c7.
Dec 07 17:30:00 client systemd[1]: Starting pllocate-updatedb.service - Update the pllocate database...
Dec 07 17:30:04 client systemd[1]: pllocate-updatedb.service: Deactivated successfully.
Dec 07 17:30:04 client systemd[1]: Finished pllocate-updatedb.service - Update the pllocate database.
Dec 07 17:30:04 client systemd[1]: pllocate-updatedb.service: Consumed 1.291s CPU time, 184.9M memory peak.
Dec 07 17:31:00 client systemd[1]: Starting dnf-makecache.service - dnf makecache...
Dec 07 17:31:02 client dnf[11176]: Extra Packages for Enterprise Linux 10 - x86_64 35 kB/s | 37 kB 00:01
Dec 07 17:31:04 client dnf[11176]: Rocky Linux 10 - BaseOS 3.2 kB/s | 4.3 kB 00:01
Dec 07 17:31:04 client dnf[11176]: Rocky Linux 10 - AppStream 12 kB/s | 4.3 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Rocky Linux 10 - CRB 12 kB/s | 4.3 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Rocky Linux 10 - Extras 9.2 kB/s | 3.1 kB 00:00
Dec 07 17:31:05 client dnf[11176]: Metadata cache created.
Dec 07 17:31:05 client systemd[1]: dnf-makecache.service: Deactivated successfully.
Dec 07 17:31:05 client systemd[1]: Finished dnf-makecache.service - dnf makecache.
Dec 07 17:31:05 client systemd[1]: dnf-makecache.service: Consumed 999ms CPU time, 134.5M memory peak.
Dec 07 17:32:00 client systemd[1]: Existing logind session ID 5 used by new audit session, ignoring.
Dec 07 17:32:00 client systemd-logind[907]: New session cb of user root.
Dec 07 17:32:00 client systemd[1]: Started session-cb.scope - Session c6 of User root.
Dec 07 17:32:00 client systemd[1]: Started systemd-hostnamed.service - Hostname Service...
Dec 07 17:32:00 client systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 07 17:32:15 client systemd[8449]: runpl0792-111002.scope: Consumed 1.067s CPU time, 119.3M memory peak, 1.9M memory swap peak
Dec 07 17:32:15 client systemd[8449]: session-c8.scope: Deactivated successfully.
Dec 07 17:32:15 client systemd-logind[907]: Session c8 logged out. Waiting for processes to exit.
Dec 07 17:32:15 client systemd-logind[907]: Removed session c8.
Dec 07 17:32:19 client systemd[8449]: app-gnome-Firefox-10117.scope: Consumed 2min 18.792s CPU time, 868.3M memory peak, 382.6M memory swap peak
Dec 07 17:32:39 client systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 07 17:32:53 client systemd-logind[907]: Session c3 logged out. Waiting for processes to exit.
Dec 07 17:32:53 client systemd-logind[907]: Removed session c3.
```

Рис. 10: Логи с клиента

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине server переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаем в нём каталог netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создаем файл netlog.sh (Рис. 12.11).

```
[root@server.dkkobzev.net ~]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf
cp: missing destination file operand after '/etc/rsyslog.d/netlog-server.conf'
Try 'cp --help' for more information.
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# touch netlog.sh
[root@server.dkkobzev.net server]# chmod +x netlog.sh
```

Рис. 11: Внесение изменений в настройки внутреннего окружения виртуальной машины

Внесение изменений в настройки внутреннего окружения виртуальных машин

Прописываем скрипт в netlog.sh (Рис. 12.12).

```
GNU nano 8.1                                         netlog.sh
#!/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
```

Рис. 12: Файл netlog.sh

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине client переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создаем в нём каталог netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создаем файл netlog.sh (Рис. 12.13).

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

Рис. 13: Внесение изменений в настройки внутреннего окружения виртуальной машины

Внесение изменений в настройки внутреннего окружения виртуальных машин

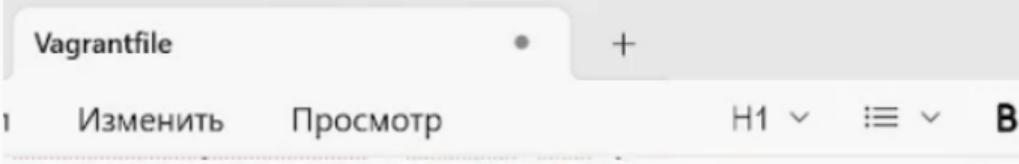
Прописываем скрипт в netlog.sh (Рис. 12.14).

```
GNU nano 8.1                                     netlog.sh
#!/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
```

Рис. 14: Файл netlog.sh

Внесение изменений в настройки внутреннего окружения виртуальных машин

Для отработки созданного скрипта во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервера и клиент (Рис. 12.15), (Рис. 12.16).

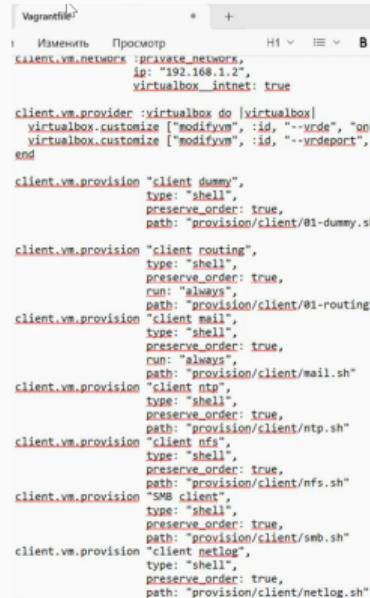


The screenshot shows a code editor window titled "Vagrantfile". The file contains configuration for two virtual machines: "server" and "client". The "server" machine has three provisions: "nfs.sh", "smb.sh", and "netlog.sh". The "client" machine has one provision: "netlog.sh". The configuration uses the "shell" type and preserves the order of the scripts.

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

Рис. 15: Vagrantfile

Внесение изменений в настройки внутреннего окружения виртуальных машин



```
Vagrantfile
+
+ Использовать Просмотр H1 ≡ ⌂ ⌂
client.vm.network :private_network,
  ip: "192.168.1.2",
  virtualbox_intnet: true

client.vm.provider :virtualbox do |virtualbox|
  virtualbox.customize ["modifyvm", :id, "--vrdp", "on"]
  virtualbox.customize ["modifyvm", :id, "--vrdeport", "1522"]
end

client.vm.provision "client dummy",
  type: "shell",
  preserve_order: true,
  path: "provision/client/01-dummy.sh"

client.vm.provision "client routing",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/01-routing.sh"

client.vm.provision "client mail",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/mail.sh"

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

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

client.vm.provision "SMB client",
  type: "shell",
  preserve_order: true,
  path: "provision/client/smb.sh"

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

Рис. 16: Vagrantfile

Выводы

В результате выполнения лабораторной работы мною были получены навыки по работе с журналами системных событий.