

Лабораторная работа

Номер 15

Мошаров Д.М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

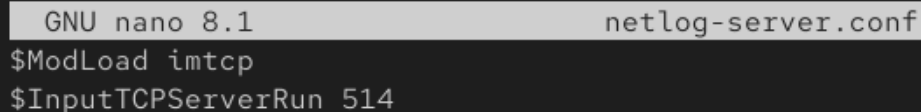
Получение навыков по работе с журналами системных событий

Создание файла конфигурации на сервере

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

Рис. 1: Создание файла конфигурации на сервере

Редактирование конфигурации rsyslog на сервере



```
GNU nano 8.1 netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 2: Редактирование конфигурации rsyslog на сервере

Перезапуск службы и начало проверки портов

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ systemctl restart rsyslog
[dmmosharov@server.dmmosharov.net rsyslog.d]$ ss -t | grep TCP
firefo 12674      dmmosharov  94u        IPv4        276548
0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefo 12674      dmmosharov  110u       IPv4        304573
0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefo 12674      dmmosharov  112u       IPv4        300610
0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefo 12674 12694 AsyncSi~l dmmosharov  94u        IPv4        276548
0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefo 12674 12694 AsyncSi~l dmmosharov  110u       IPv4        304573
0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefo 12674 12694 AsyncSi~l dmmosharov  112u       IPv4        300610
0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefo 12674 12695 pool-spaw dmmosharov  94u        IPv4        276548
0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefo 12674 12695 pool-spaw dmmosharov  110u       IPv4        304573
0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefo 12674 12695 pool-spaw dmmosharov  112u       IPv4        300610
0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefo 12674 12696 gmain dmmosharov  94u        IPv4        276548
0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefo 12674 12696 gmain dmmosharov  110u       IPv4        304573
0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefo 12674 12696 gmain dmmosharov  112u       IPv4        300610
0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefo 12674 12698 WaylandPr dmmosharov  94u        IPv4        276548
0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefo 12674 12698 WaylandPr dmmosharov  110u       IPv4        304573
0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefo 12674 12698 WaylandPr dmmosharov  112u       IPv4        300610
0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
```

Рис. 3: Перезапуск службы и начало проверки портов

Подтверждение прослушивания порта 514

```
rsyslogd 30458 TCP *:shell (LISTEN) root 4u IPv4 304981
0t0
rsyslogd 30458 TCP *:shell (LISTEN) root 5u IPv6 304982
0t0
rsyslogd 30458 30460 in:imjour root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30460 in:imjour root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30461 in:imtcp root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30461 in:imtcp root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30462 in:imtcp root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30462 in:imtcp root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30463 in:imtcp root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30463 in:imtcp root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30464 in:imtcp root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30464 in:imtcp root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30465 in:imtcp root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30465 in:imtcp root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30466 rs:main root 4u IPv4 304981
0t0 TCP *:shell (LISTEN)
rsyslogd 30458 30466 rs:main root 5u IPv6 304982
0t0 TCP *:shell (LISTEN)
[dmosharov@server.dmosharov.net rsyslog.d]$
```

Рис. 4: Подтверждение прослушивания порта 514

Настройка firewall на сервере

```
982      0t0      TCP *:shell (LISTEN)
[dmmosharov@server.dmmosharov.net rsyslog.d]$ firewall-cmd --add-port=514/tcp
success
[dmmosharov@server.dmmosharov.net rsyslog.d]$ firewall-cmd --add-port=514/tcp
--permanent
success
[dmmosharov@server.dmmosharov.net rsyslog.d]$ █
```

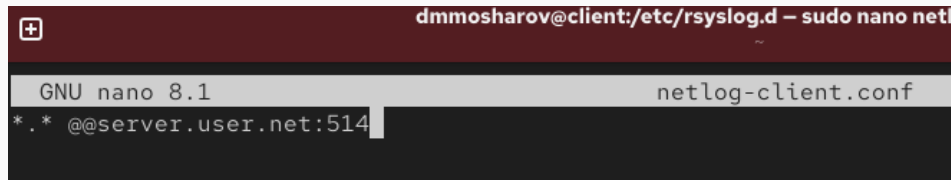
Рис. 5: Настройка firewall на сервере

Создание файла конфигурации на клиенте

```
[dmmosharov@client.dmmosharov.net ~]$ cd /etc/rsyslog.d
[dmmosharov@client.dmmosharov.net rsyslog.d]$ touch netlog-client.conf
touch: cannot touch 'netlog-client.conf': Permission denied
[dmmosharov@client.dmmosharov.net rsyslog.d]$ sudo touch netlog-client.conf
[sudo] password for dmmosharov:
[dmmosharov@client.dmmosharov.net rsyslog.d]$ sudo nano netlog-client.conf
[dmmosharov@client.dmmosharov.net rsyslog.d]$
```

Рис. 6: Создание файла конфигурации на клиенте

Редактирование конфигурации rsyslog на клиенте



The screenshot shows a terminal window with a dark red title bar. The title bar text is "dmmosharov@client:/etc/rsyslog.d – sudo nano netl". On the left of the title bar is a square icon with a white plus sign. The main area of the terminal has a light gray header bar with "GNU nano 8.1" on the left and "netlog-client.conf" on the right. Below the header bar, the text "*. * @@server.user.net:514" is visible in a dark background, with a white cursor at the end of the line.

```
dmmosharov@client:/etc/rsyslog.d – sudo nano netl
GNU nano 8.1 netlog-client.conf
*. * @@server.user.net:514
```

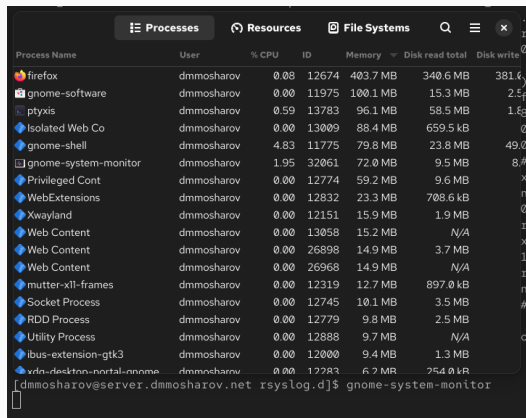
Рис. 7: Редактирование конфигурации rsyslog на клиенте

Просмотр логов на сервере через tail

```
[dmnosharov@server.dmnosharov.net rsyslog.d]$ sudo tail -f /var/log/messages
[sudo] password for dmnosharov:
Feb 11 12:50:28 server ptxis[13783]: context mismatch in svga_surface_destro
y
Feb 11 12:50:28 server systemd-coredump[31940]: Process 31935 (VBoxClient) of
user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el
10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Modul
e libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from
rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm way
land-1.23.0-2.el10.x86_64#012Stack trace of thread 31938:#012#0 0x0000000000
41db4b n/a (n/a + 0x0)#012#1 0x000000000041dac4 n/a (n/a + 0x0)#012#2 0x000
0000000450a7c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4
0x000007f086c153b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x000007f086c1c
46bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 31935:#012#
0 0x000007f086c1c24bd syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000004347a
2 n/a (n/a + 0x0)#012#2 0x00000000004506c6 n/a (n/a + 0x0)#012#3 0x00000000
00405123 n/a (n/a + 0x0)#012#4 0x000007f086c0e930e __libc_start_call_main (li
bc.so.6 + 0x2a30e)#012#5 0x000007f086c0e93c9 __libc_start_main@@GLIBC_2.34 (l
ibc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object b
inary architecture: AMD x86-64
Feb 11 12:50:28 server systemd[1]: systemd-coredump[31940].service: Dea
ctivated successfully.
Feb 11 12:50:32 server systemd-logind[991]: Existing logind session ID 5 used
by new audit session, ignoring.
Feb 11 12:50:32 server systemd[1]: Created slice user-0.slice - User Slice of
UID 0.
Feb 11 12:50:32 server systemd[1]: Starting user-runtime-dir@0.service - User
Runtime Directory /run/user/0...
Feb 11 12:50:32 server systemd-logind[991]: New session c11 of user root.
Feb 11 12:50:32 server systemd[1]: Finished user-runtime-dir@0.service - User
Runtime Directory /run/user/0.
Feb 11 12:50:32 server systemd[1]: Starting user@0.service - User Manager for
UID 0...
Feb 11 12:50:32 server systemd-logind[991]: New session 14 of user root.
Feb 11 12:50:32 server systemd[31949]: Queued start job for default target de
fault.target.
Feb 11 12:50:32 server systemd[31949]: Created slice app.slice - User Applicat
```

Рис. 8: Просмотр логов на сервере через tail

Интерфейс Gnome System Monitor



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
firefox	dmmosharov	0.08	12674	403.7 MB	340.6 MB	381.4
gnome-software	dmmosharov	0.00	11975	100.1 MB	15.3 MB	2.5
ptexis	dmmosharov	0.59	13783	96.1 MB	58.5 MB	1.63
Isolated Web Co	dmmosharov	0.00	13009	88.4 MB	659.5 kB	0.0
gnome-shell	dmmosharov	4.83	11775	79.8 MB	23.8 MB	49.00
gnome-system-monitor	dmmosharov	1.95	32061	72.0 MB	9.5 MB	8.5
Privileged Cont	dmmosharov	0.00	12774	59.2 MB	9.6 MB	x0
WebExtensions	dmmosharov	0.00	12832	23.3 MB	708.6 kB	n/
Xwayland	dmmosharov	0.00	12151	15.9 MB	1.9 MB	0
Web Content	dmmosharov	0.00	13058	15.2 MB	N/A	re
Web Content	dmmosharov	0.00	26898	14.9 MB	3.7 MB	x0
Web Content	dmmosharov	0.00	26968	14.9 MB	N/A	12
mutter-x11-frames	dmmosharov	0.00	12319	12.7 MB	897.0 kB	rt
Socket Process	dmmosharov	0.00	12745	10.1 MB	3.5 MB	ne
RDD Process	dmmosharov	0.00	12779	9.8 MB	2.5 MB	#0
Utility Process	dmmosharov	0.00	12888	9.7 MB	N/A	ce
ibus-extension-gtk3	dmmosharov	0.00	12000	9.4 MB	1.3 MB	
vdo-desktop-portal-gnome	dmmosharov	0.00	12283	6.2 MB	254.0 kB	

[dmmosharov@server.dmmosharov.net rsyslog.d]\$ gnome-system-monitor

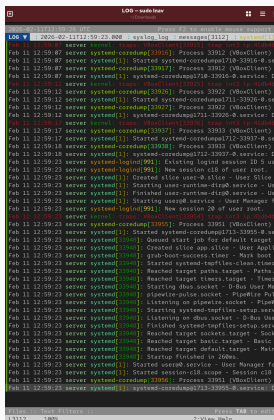
Рис. 9: Интерфейс Gnome System Monitor

Ручная установка lnav на сервере

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ cd ~/Downloads/  
[dmmosharov@server.dmmosharov.net Downloads]$ sudo cp lnav /usr/bin  
cp: cannot stat 'lnav': No such file or directory  
[dmmosharov@server.dmmosharov.net Downloads]$ sudo cp lnav /usr/bin  
[dmmosharov@server.dmmosharov.net Downloads]$ lnav  
X error: default syslog file is not readable -- /var/log/messages  
[dmmosharov@server.dmmosharov.net Downloads]$ sudo lnav  
[dmmosharov@server.dmmosharov.net Downloads]$
```

Рис. 10: Ручная установка lnav на сервере

Просмотр логов через lnav на сервере



```
LOG - syslog.log
2026-02-11T12:59:23.000 - syslog.log messages[3112] - system[1]
Feb 11 12:59:07 server user@server: ~$ sshd[3101]: Process 3101 (VBoxClient)
Feb 11 12:59:07 server systemd-coredump[31016]: Process 31012 (VBoxClient)
Feb 11 12:59:07 server systemd[1]: Started systemd-coredump[718-31016-0.service: D
Feb 11 12:59:07 server systemd-coredump[31017]: Process 31012 (VBoxClient)
Feb 11 12:59:07 server systemd[1]: systemd-coredump[718-31016-0.service: D
Feb 11 12:59:12 server systemd-coredump[31016]: Process 31022 (VBoxClient)
Feb 11 12:59:12 server systemd[1]: Started systemd-coredump[711-31026-0.se
Feb 11 12:59:12 server systemd-coredump[31027]: Process 31022 (VBoxClient)
Feb 11 12:59:12 server systemd[1]: systemd-coredump[711-31026-0.service: D
Feb 11 12:59:17 server user@server: ~$ sshd[3106]: sshd: user@server:
Feb 11 12:59:17 server systemd-coredump[31027]: Process 31033 (VBoxClient)
Feb 11 12:59:17 server systemd[1]: Started systemd-coredump[712-31037-0.se
Feb 11 12:59:18 server systemd-coredump[31038]: Process 31033 (VBoxClient)
Feb 11 12:59:18 server systemd[1]: systemd-coredump[712-31037-0.service: D
Feb 11 12:59:23 server systemd-logind[991]: Existing logind session ID 5 us
Feb 11 12:59:23 server systemd-logind[991]: New session c1b of user root.
Feb 11 12:59:23 server systemd[1]: Created slice user-0.slice - User Slice
Feb 11 12:59:23 server systemd[1]: Starting user-runtime-dir@0.service - Us
Feb 11 12:59:23 server systemd[1]: Finished user-runtime-dir@0.service - Us
Feb 11 12:59:23 server systemd[1]: Starting user@0.service - User Manager f
Feb 11 12:59:23 server systemd-logind[991]: New session 20 of user root.
Feb 11 12:59:23 server user@server: ~$ sshd[3106]: sshd: user@server:
Feb 11 12:59:23 server systemd-coredump[31062]: Process 31061 (VBoxClient)
Feb 11 12:59:23 server systemd[1]: Started systemd-coredump[713-31065-0.se
Feb 11 12:59:23 server systemd[1000]: Queued start job for default target.
Feb 11 12:59:23 server systemd[1000]: Created slice app.slice - User Appli
Feb 11 12:59:23 server systemd[1000]: grab-hoat-access.timer - Max boot
Feb 11 12:59:23 server systemd[1000]: Started systemd-tapfiles-clean.timer
Feb 11 12:59:23 server systemd[1000]: Reached target paths.target - Patha
Feb 11 12:59:23 server systemd[1000]: Reached target timers.target - Timer
Feb 11 12:59:23 server systemd[1000]: Starting dbus.socket - D-Bus User Me
Feb 11 12:59:23 server systemd[1000]: pipeline-pulse.socket - Pipeline Pul
Feb 11 12:59:23 server systemd[1000]: Listening on pipeline.socket - Pipe@
Feb 11 12:59:23 server systemd[1000]: Starting systemd-tapfiles-setup.serv
Feb 11 12:59:23 server systemd[1000]: Listening on dbus.socket - D-Bus Use
Feb 11 12:59:23 server systemd[1000]: Finished systemd-tapfiles-setup.serv
Feb 11 12:59:23 server systemd[1000]: Reached target sockets.target - Sock
Feb 11 12:59:23 server systemd[1000]: Reached target basic.target - Basic
Feb 11 12:59:23 server systemd[1000]: Reached target default.target - Main
Feb 11 12:59:23 server systemd[1000]: Startup finished in 260ms.
Feb 11 12:59:23 server systemd[1]: Started user@0.service - User Manager fo
Feb 11 12:59:23 server systemd[1]: Started session-c1b.scope - Session C1b
Feb 11 12:59:23 server systemd-coredump[31066]: Process 31061 (VBoxClient)
Feb 11 12:59:23 server systemd[1]: systemd-coredump[713-31065-0.service: D
```

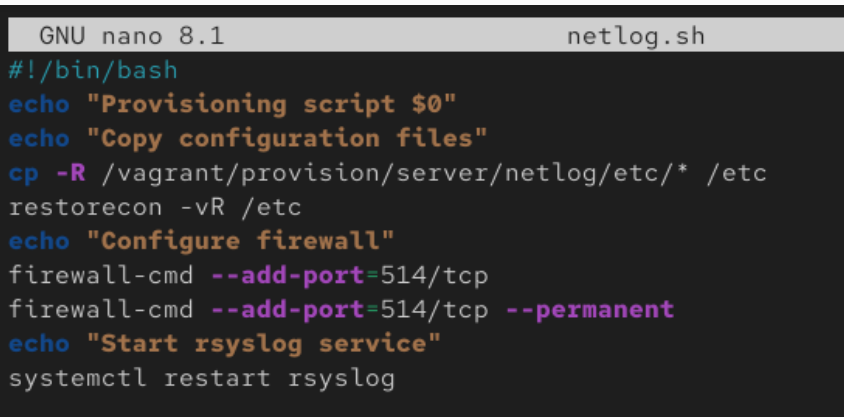
Рис. 11: Просмотр логов через lnav на сервере

Подготовка файлов для автоматизации сервера

```
[dmmosharov@server.dmmosharov.net Downloads]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ mkdir -p /vagrant/provision/server
/netlog/etc/rsyslog.d
[dmmosharov@server.dmmosharov.net server]$ cp -R /etc/rsyslog.d/netlog-server
.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[dmmosharov@server.dmmosharov.net server]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ touch netlog.sh
[dmmosharov@server.dmmosharov.net server]$ chmod +x netlog.sh
[dmmosharov@server.dmmosharov.net server]$ nano netlog.sh
[dmmosharov@server.dmmosharov.net server]$
```

Рис. 14: Подготовка файлов для автоматизации сервера

Скрипт provisioning для сервера



The image shows a terminal window with a dark background. At the top, there is a light gray header bar containing the text "GNU nano 8.1" on the left and "netlog.sh" on the right. Below the header, the script content is displayed in a monospaced font with syntax highlighting. The script starts with a shebang line, followed by two echo statements for logging. It then uses 'cp' to copy files from a vagrant provision directory to /etc, and 'restorecon' to set permissions. Next, it echoes a message and uses 'firewall-cmd' to add a port to the firewall. Finally, it echoes another message and uses 'systemctl' to restart the rsyslog service.

```
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
```

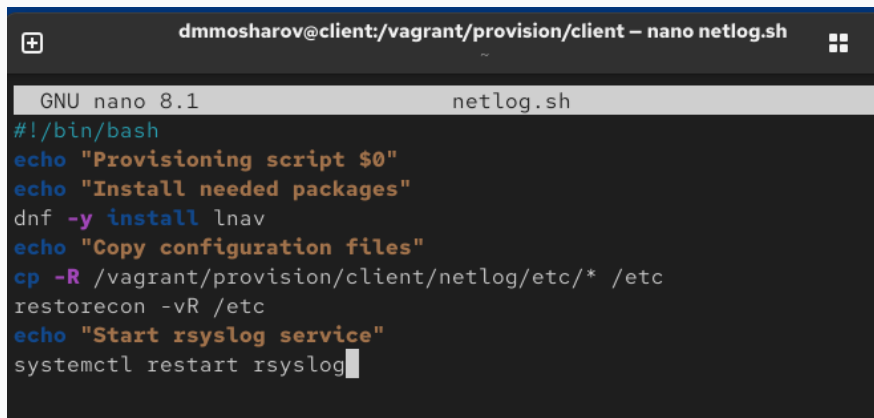
Рис. 15: Скрипт provisioning для сервера

Подготовка файлов для автоматизации клиента

```
[dmmosharov@client.dmmosharov.net rsyslog.d]$ cd /vagrant/provision/client
[dmmosharov@client.dmmosharov.net client]$ mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[dmmosharov@client.dmmosharov.net client]$ cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[dmmosharov@client.dmmosharov.net client]$ cd /vagrant/provision/client
[dmmosharov@client.dmmosharov.net client]$ touch netlog.sh
[dmmosharov@client.dmmosharov.net client]$ chmod +x netlog.sh
[dmmosharov@client.dmmosharov.net client]$ nano netlog.sh
```

Рис. 16: Подготовка файлов для автоматизации клиента

Скрипт provisioning для клиента



The screenshot shows a terminal window with the title bar "dmmosharov@client:/vagrant/provision/client – nano netlog.sh". The editor is GNU nano 8.1, editing the file netlog.sh. The script content is as follows:

```
#!/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. 17: Скрипт provisioning для клиента

Настройка Vagrantfile

```
131 server.vm.provision "server setup",
132     type: "shell",
133     preserve_order: true,
134     path: "provision/server/setup.sh"
135 end
136
137 # client configuration
138 config.vm.define "client", autostart: false do |client|
139     client.vm.box = "rocklinux"
140     client.vm.hostname = "client"
141
142     client.vm.boot_timeout = 1000
143
144     client.ssh.fragment_key = false
145     client.ssh.username = "vagrant"
146     client.ssh.password = "vagrant"
147
148     client.vm.network :private_network,
149         type: "dhcp",
150         virtualbox____device__id__1__true
151
152     client.vm.provisioner virtualbox__do__virtualbox__do__
153         virtualbox__customize__["modify__", "id__", "-__v__", "id__"]
154         virtualbox__customize__["modify__", "id__", "-__v__", "id__"]
155     end
156
157     client.vm.provision "client dummy",
158         type: "shell",
159         preserve_order: true,
160         path: "provision/client/01-dummy.sh"
161
162     client.vm.provision "client routing",
163         type: "shell",
164         preserve_order: true,
165         run: "sleep",
166         path: "provision/client/01-routing.sh"
167
168     client.vm.provision "client mail",
169         type: "shell",
170         preserve_order: true,
171         path: "provision/client/mail.sh"
172
173     client.vm.provision "client dns",
174         type: "shell",
175         preserve_order: true,
176         path: "provision/client/dns.sh"
177
178     client.vm.provision "client nfs",
179         type: "shell",
180         preserve_order: true,
181         path: "provision/client/nfs.sh"
182
183     client.vm.provision "SSH client",
184         type: "shell",
185         preserve_order: true,
186         path: "provision/client/ssh.sh"
187
188     server.vm.provision "client setup",
189         type: "shell",
190         preserve_order: true,
191         path: "provision/client/setup.sh"
192 end
```

Рис. 18: Настройка Vagrantfile

В результате выполнения лабораторной работы были получены навыки использования журналов системных событий