

Отчёт о лабораторной работе

Лабораторная работа 15

Мошаров Денис Максимович

Содержание

Цель работы

Получение навыков по работе с журналами системных событий

Выполнение лабораторной работы

На сервере перейдем в каталог конфигурации rsyslog и создадим файл netlog-server.conf для настройки централизованного сбора логов (рис. [-@fig:001]).

```
[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
```

Создание файла конфигурации на сервере

В открывшемся редакторе внесем настройки для включения модуля imtcp и прослушивания порта 514 по протоколу TCP (рис. [-@fig:002]).

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

Редактирование конфигурации rsyslog на сервере

Перезапустим службу rsyslog для применения изменений и начнем проверку прослушиваемых портов с помощью утилиты lsof, отфильтровав вывод по TCP (рис. [-@fig:003]).

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ systemctl restart rsyslog
[dmmosharov@server.dmmosharov.net rsyslog.d]$ lsof | grep TCP
firefox 12674 dmmosharov 94u IPv4 276548
  0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 dmmosharov 110u IPv4 300610
  0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12694 AsyncSt-l dmmosharov 94u IPv4 276548
  0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 12694 AsyncSt-l dmmosharov 110u IPv4 304573
  0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12694 AsyncSi-l dmmosharov 112u IPv4 300610
  0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefox 12674 12695 pool-spaw dmmosharov 94u IPv4 276548
  0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 12695 pool-spaw dmmosharov 110u IPv4 304573
  0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12695 pool-spaw dmmosharov 112u IPv4 300610
  0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefox 12674 12696 gmain dmmosharov 94u IPv4 276548
  0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 12696 gmain dmmosharov 110u IPv4 304573
  0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12696 gmain dmmosharov 112u IPv4 300610
  0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefox 12674 12698 WaylandPr dmmosharov 94u IPv4 276548
  0t0      TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 12698 WaylandPr dmmosharov 110u IPv4 304573
  0t0      TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12698 WaylandPr dmmosharov 112u IPv4 300610
  0t0      TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefox 12674 12699 libuv dmmosharov 94u IPv4 276548
```

Перезапуск службы и начало проверки портов

В продолжении вывода команды lsof убедимся, что процессы rsyslogd успешно прослушивают порт 514 на всех интерфейсах (рис. [-@fig:004]).

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

Подтверждение прослушивания порта 514

Настроим межсетевой экран на сервере, разрешив прием соединений по порту 514/tcp, и сохраним правило как постоянное (рис. [-@fig:005]).

```
[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]$
```

Настройка firewall на сервере

Перейдем на клиентскую машину. В каталоге /etc/rsyslog.d создадим файл конфигурации netlog-client.conf (рис. [-@fig:006]).

```
[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]$
```

Создание файла конфигурации на клиенте

В файле конфигурации пропишем правило отправки всех журналов (.) на сервер по адресу server.nsandryushin.net через порт 514 по протоколу TCP (рис. [-@fig:007]).



Редактирование конфигурации rsyslog на клиенте

Вернемся на сервер и запустим отслеживание файла /var/log/messages в реальном времени, чтобы убедиться в поступлении логов (рис. [-@fig:008]).

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ sudo tail -f /var/log/messages  
[sudo] password for dmmosharov:  
Feb 11 12:50:28 server ptyx13783: context mismatch in svga_surface_destroy  
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.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module 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 wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 31938:#012#0 0x00000000000041db4b n/a (n/a + 0x0)#012#1 0x00000000000041dac4 n/a (n/a + 0x0)#012#2 0x00000000450a7c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x00007f086c153b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007f086c1c46bc __clone3 ((libc.so.6 + 0x1056bc)#012#012Stack trace of thread 31935:#012#0 0x00007f086c1c24bd syscallf ((libc.so.6 + 0x1034bd)#012#1 0x00000000004347a2 n/a (n/a + 0x0)#012#2 0x0000000000004506c6 n/a (n/a + 0x0)#012#3 0x000000000040405123 n/a (n/a + 0x0)#012#4 0x00007f086c0e930e __libc_start_main ((libc.so.6 + 0x2a30e)#012#5 0x00007f086c0e93c9 __libc_start_main@GLIBC_2.34 ((libc.so.6 + 0x2a3c9)#012#6 0x000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64  
Feb 11 12:50:28 server systemd[1]: systemd-coredump@1611-31939-0.service: Deactivated 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 default.target.  
Feb 11 12:50:32 server systemd[31949]: Created slice app.slice - User Application
```

Просмотр логов на сервере через tail

Запустим графическую утилиту мониторинга системы. В открывшемся окне gnome-system-monitor просмотрим список активных процессов и потребляемые ими ресурсы (рис. [-@fig:009]).

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
firefox	dmmosharov	0.08	12674	403.7 MB	340.6 MB	381.6 kB
gnome-software	dmmosharov	0.00	11975	100.1 MB	15.3 MB	2.5 kB
ptyxis	dmmosharov	0.59	13783	96.1 MB	58.5 MB	1.8 kB
Isolated Web Co	dmmosharov	0.00	13009	88.4 MB	659.5 kB	0 kB
gnome-shell	dmmosharov	4.83	11775	79.8 MB	23.8 MB	49.0 kB
gnome-system-monitor	dmmosharov	1.95	32061	72.0 MB	9.5 MB	8.5 kB
Privileged Cont	dmmosharov	0.00	12774	59.2 MB	9.6 MB	x0 kB
WebExtensions	dmmosharov	0.00	12832	23.3 MB	708.6 kB	n/a kB
Xwayland	dmmosharov	0.00	12151	15.9 MB	1.9 MB	0 kB
Web Content	dmmosharov	0.00	13058	15.2 MB	N/A	x0 kB
Web Content	dmmosharov	0.00	26898	14.9 MB	3.7 MB	12 kB
Web Content	dmmosharov	0.00	26968	14.9 MB	N/A	rtt kB
mutter-x11-frames	dmmosharov	0.00	12319	12.7 MB	897.0 kB	n@0 kB
Socket Process	dmmosharov	0.00	12745	10.1 MB	3.5 MB	#0 kB
RDD Process	dmmosharov	0.00	12779	9.8 MB	2.5 MB	ce kB
Utility Process	dmmosharov	0.00	12888	9.7 MB	N/A	ce kB
ibus-extension-gtk3	dmmosharov	0.00	12000	9.4 MB	1.3 MB	ce kB
xdg-desktop-portal-gnome	dmmosharov	0.00	12283	6.2 MB	254.0 kB	ce kB

Интерфейс Gnome System Monitor

Установим продвинутый просмотрщик логов lnav на сервере, скопировав исполняемый файл в системную директорию /usr/bin (рис. [-@fig:010]).

```
[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
✖ error: default syslog file is not readable -- /var/log/messages
[dmmosharov@server.dmmosharov.net Downloads]$ sudo lnav
[dmmosharov@server.dmmosharov.net Downloads]$
```

Ручная установка lnav на сервере

Запустим lnav на сервере и просмотрим журналы в удобном структурированном виде с подсветкой синтаксиса (рис. [-@fig:011]).

```

LOG - sudo inav
Press F2 to enable mouse support
~/Downloads

2026-02-11T12:59:26 UTC          Press F2 to enable mouse support
LOG : 2026-02-11T12:59:23.000 : syslog_log : messages[3112] : systemd[1]
Feb 11 12:59:07 server kernel: traps: VBoxClient[33915] trap int3 ip:41db4b
Feb 11 12:59:07 server systemd-coredump[33916]: Process 33912 (VBoxClient)
Feb 11 12:59:07 server systemd[1]: Started systemd-coredump@1710-33916-0.service
Feb 11 12:59:07 server systemd-coredump[33917]: Process 33912 (VBoxClient)
Feb 11 12:59:07 server systemd[1]: systemd-coredump@1710-33916-0.service: D
Feb 11 12:59:12 server kernel: traps: VBoxClient[33925] trap int3 ip:41db4b
Feb 11 12:59:12 server systemd-coredump[33926]: Process 33922 (VBoxClient)
Feb 11 12:59:12 server systemd[1]: Started systemd-coredump@1711-33926-0.service
Feb 11 12:59:12 server systemd-coredump[33927]: Process 33922 (VBoxClient)
Feb 11 12:59:12 server systemd[1]: systemd-coredump@1711-33926-0.service: D
Feb 11 12:59:17 server kernel: traps: VBoxClient[33936] trap int3 ip:41db4b
Feb 11 12:59:17 server systemd-coredump[33937]: Process 33933 (VBoxClient)
Feb 11 12:59:17 server systemd[1]: Started systemd-coredump@1712-33937-0.service
Feb 11 12:59:18 server systemd-coredump[33938]: Process 33933 (VBoxClient)
Feb 11 12:59:18 server systemd[1]: systemd-coredump@1712-33937-0.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 c18 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 kernel: traps: VBoxClient[33954] trap int3 ip:41db4b
Feb 11 12:59:23 server systemd-coredump[33955]: Process 33951 (VBoxClient)
Feb 11 12:59:23 server systemd[1]: Started systemd-coredump@1713-33955-0.service
Feb 11 12:59:23 server systemd[33948]: Queued start job for default target
Feb 11 12:59:23 server systemd[33948]: Created slice app.slice - User Appli
Feb 11 12:59:23 server systemd[33948]: grub-boot-success.timer - Mark boot
Feb 11 12:59:23 server systemd[33948]: Started systemd-tmpfiles-clean.timer
Feb 11 12:59:23 server systemd[33948]: Reached target paths.target - Paths.
Feb 11 12:59:23 server systemd[33948]: Reached target timers.target - Timer
Feb 11 12:59:23 server systemd[33948]: Starting dbus.socket - D-Bus User Me
Feb 11 12:59:23 server systemd[33948]: pipewire-pulse.socket - PipeWire Pul
Feb 11 12:59:23 server systemd[33948]: Listening on pipewire.socket - PipeW
Feb 11 12:59:23 server systemd[33948]: Starting systemd-tmpfiles-setup.serv
Feb 11 12:59:23 server systemd[33948]: Listening on dbus.socket - D-Bus Use
Feb 11 12:59:23 server systemd[33948]: Finished systemd-tmpfiles-setup.serv
Feb 11 12:59:23 server systemd[33948]: Reached target sockets.target - Sock
Feb 11 12:59:23 server systemd[33948]: Reached target basic.target - Basic
Feb 11 12:59:23 server systemd[33948]: Reached target default.target - Main
Feb 11 12:59:23 server systemd[33948]: Startup finished in 200ms.
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-c18.scope - Session c18
Feb 11 12:59:23 server systemd-coredump[33956]: Process 33951 (VBoxClient)
Feb 11 12:59:23 server systemd[1]: systemd-coredump@1713-33955-0.service: D

```

Files :: Text Filters :: Press TAB to edit
L3112 100% ?:View Help

Просмотр логов через `inav` на сервере

Приступим к автоматизации настроек. На сервере в каталоге `/vagrant/provision` создадим структуру папок для хранения конфигов и скопируем туда текущий файл настроек. Также создадим скрипт `netlog.sh` (рис. [-@fig:014]).

```
[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]$
```

Подготовка файлов для автоматизации сервера

Напишем скрипт `netlog.sh`, который будет копировать конфигурационные файлы, восстанавливать контекст безопасности SELinux, настраивать фаервол и перезапускать службу `rsyslog` (рис. [-@fig:015]).

```

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

```

Скрипт provisioning для сервера

На клиенте выполним аналогичные действия: создадим структуру каталогов в /vagrant/provision, скопируем конфиг клиента и создадим установочный скрипт (рис. [-@fig:016]).

```

[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

```

Подготовка файлов для автоматизации клиента

В скрипте netlog.sh для клиента пропишем установку пакета lnav, копирование конфигурации rsyslog, восстановление контекста SELinux и перезапуск службы (рис. [-@fig:017]).

```

dmmosharov@client:/vagrant/provision/client - nano netlog.sh
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

```

Скрипт provisioning для клиента

Наконец, откроем Vagrantfile и добавим в конфигурации сервера и клиента блоки vm.provision типа shell, указывающие на созданные нами скрипты netlog.sh (рис. [-@fig:018]).

```
132      server.vm.provision "server netlog",
133          type: "shell",
134          preserve_order: true,
135          path: "provision/server/netlog.sh"
136      end
137
138
139  ## Client configuration
140 config.vm.define "client", autostart: false do |client|
141     client.vm.box = "rockylinux10"
142     client.vm.hostname = 'client'
143
144     client.vm.boot_timeout = 1440
145
146     client.ssh.insert_key = false
147     client.ssh.username = 'vagrant'
148     client.ssh.password = 'vagrant'
149
150     client.vm.network :private_network,
151         type: "dhcp",
152         virtualbox_intnet: true
153
154
155     client.vm.provider :virtualbox do |virtualbox|
156         virtualbox.customize ["modifyvm", :id, "--vrde", "on"]
157         virtualbox.customize ["modifyvm", :id, "--vrdeport", "3392"]
158     end
159
160
161     client.vm.provision "client dummy",
162         type: "shell",
163         preserve_order: true,
164         path: "provision/client/01-dummy.sh"
165
166
167     client.vm.provision "client routing",
168         type: "shell",
169         preserve_order: true,
170         run: "always",
171         path: "provision/client/01-routing.sh"
172
173     client.vm.provision "client mail",
174         type: "shell",
175         preserve_order: true,
176         path: "provision/client/mail.sh"
177
178     client.vm.provision "client ntp",
179         type: "shell",
180         preserve_order: true,
181         path: "provision/client/ntp.sh"
182
183
184     client.vm.provision "SMB client",
185         type: "shell",
186         preserve_order: true,
187         path: "provision/client/smb.sh"
188
189
190     server.vm.provision "client netlog",
191         type: "shell",
192         preserve_order: true,
193         path: "provision/client/netlog.sh"
```

Настройка Vagrantfile

Выводы

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