

Лабораторная работа

Номер 15

Мошаров Д.М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

Цель работы

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
```

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]$ 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 304573
  0t0  TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 dmmosharov 112u IPv4 300610
  0t0  TCP server.dmmosharov.net:51334->146.75.121.91:https (ESTABLISHED)
firefox 12674 12694 AsyncSsl-l dmmosharov 94u IPv4 276548
  0t0  TCP server.dmmosharov.net:59234->34.107.243.93:https (ESTABLISHED)
firefox 12674 12694 AsyncSsl-l dmmosharov 110u IPv4 304573
  0t0  TCP server.dmmosharov.net:60936->146.75.121.91:https (ESTABLISHED)
firefox 12674 12694 AsyncSsl-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)
```

Рис. 3: Перезапуск службы и начало проверки портов

Подтверждение прослушивания порта 514

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ tail -f /var/log/rsyslog.log
rsyslogd 30458                                     root    4u      IPv4          304981
          0t0      TCP *:shell (LISTEN)
rsyslogd 30458                                     root    5u      IPv6          304982
          0t0      TCP *:shell (LISTEN)
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)
[dmmosharov@server.dmmosharov.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]$ █
```

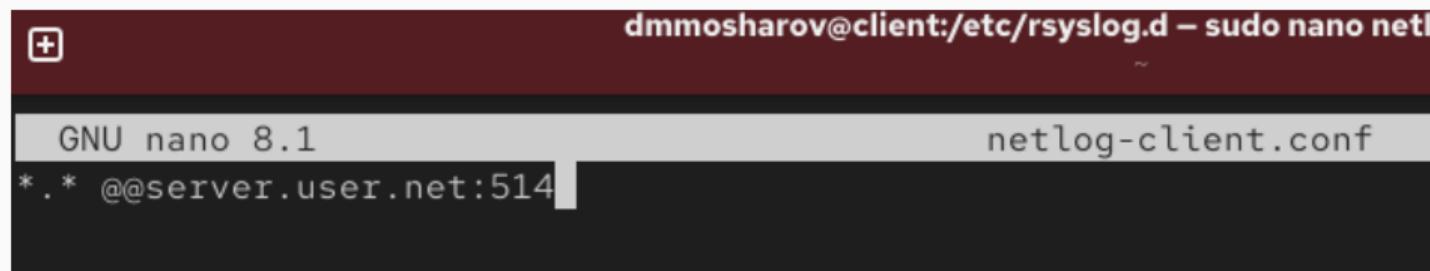
Рис. 5: Настройка firewall на сервере

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 the following details:

- Terminal title: dmmosharov@client:/etc/rsyslog.d – sudo nano netl
- File name: netlog-client.conf
- Content of the file:

```
GNU nano 8.1
*. * @@server.user.net:514
```

Рис. 7: Редактирование конфигурации rsyslog на клиенте

Просмотр логов на сервере через tail

```
[dmmosharov@server.dmmosharov.net rsyslog.d]$ sudo tail -f /var/log/messages
[sudo] password for dmmosharov:
Feb 11 12:50:28 server ptyxis[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 libKau.so.6 from rpm libKau-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 libffii.so.8 from
rpm libffii-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 0x00000000000
41db4b n/a (n/a + 0x0)#012#1 0x0000000000041dac4 n/a (n/a + 0x0)#012#2 0x00
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#6 0x000007f086c1c24bd syscall (libc.so.6 + 0x1034bd)#012#7 0x00000000004347a
2 n/a (n/a + 0x0)#012#8 0x00000000004506c6 n/a (n/a + 0x0)#012#9 0x00000000
00405123 n/a (n/a + 0x0)#012#10 0x000007f086c0e93c9 __libc_start_main (li
bc.so.6 + 0x2a30e)#012#5 0x000007f086c0e93c9 __libc_start_main@GLIBC_2.34 (l
(bc.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]: Activated 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 Applica
```

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 kB
gnome-software	dmmosharov	0.00	11975	100.1 MB	15.3 MB	2.5 kB
ptyxix	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	n/a
WebExtensions	dmmosharov	0.00	12832	23.3 MB	708.6 kB	0 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	re
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	rt
mutter-x11-frames	dmmosharov	0.00	12319	12.7 MB	897.0 kB	n/a
Socket Process	dmmosharov	0.00	12745	10.1 MB	3.5 MB	#0
RDD Process	dmmosharov	0.00	12779	9.8 MB	2.5 MB	
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	
xbla-desktop-portal-gnome	dmmosharov	0.00	12283	6.2 MR	254.0 kB	

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

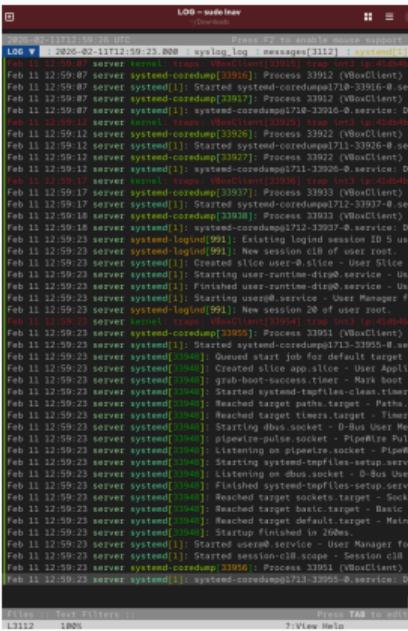


Рис. 11: Просмотр логов через lnav на сервере

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

```
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
```

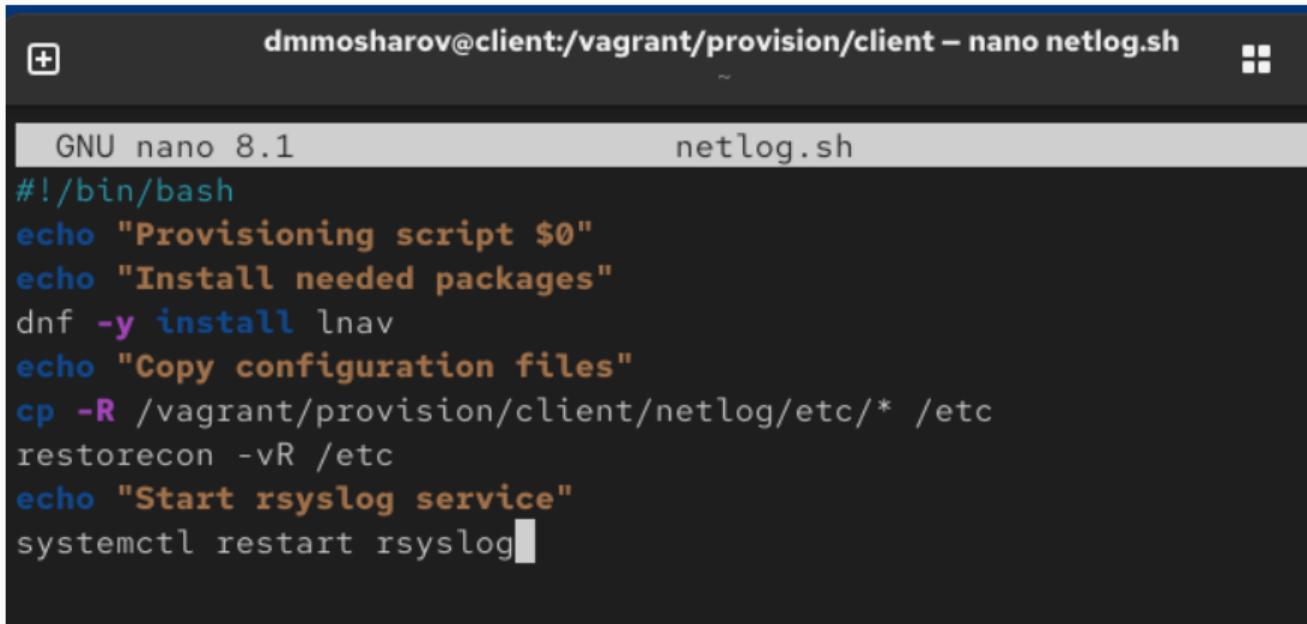
Рис. 15: Скрипт provisioning для сервера

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 terminal content is a shell script named "netlog.sh" with the following code:

```
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. 17: Скрипт provisioning для клиента

Настройка Vagrantfile

```
111      server.vm.provider "vmware_desktop"
112      type: "vmware_desktop"
113      preserve_order: true,
114      path: "precision/server/netlog.vmx"
115    end
116
117  # client configuration
118 config.vm.define "client", autostart: false do |client|
119  client.vm.box = "rockylinux8"
120  client.vm.hostname = "client"
121
122  client.vm.boot_timeout = 3400
123
124  client.ssh.insert_key = false
125  client.ssh.username = "vagrant"
126  client.ssh.password = "vagrant"
127
128  client.vm.network "private_network",
129    type: "dhcp",
130    virtualbox_guestip: true
131
132  client.vm.provider :virtualbox do |vb|
133    virtualbox.customize ["modifyvm", :id, "-vram", "1024"]
134    virtualbox.customize ["modifyvm", :id, "--vcpuset", "2000"]
135  end
136
137  client.vm.provider "client_desktop",
138    type: "shell",
139    preserve_order: true,
140    path: "precision/client/01-dummy.sh"
141
142  client.vm.provider "client_routing",
143    type: "shell",
144    preserve_order: true,
145    run: "always",
146    path: "precision/client/01-routing.sh"
147  client.vm.provider "client_mail",
148    type: "shell",
149    preserve_order: true,
150    path: "precision/client/mail.sh"
151
152  client.vm.provider "client_nfs",
153    type: "shell",
154    preserve_order: true,
155    path: "precision/client/nfs.sh"
156
157  client.vm.provider "client_rsync",
158    type: "shell",
159    preserve_order: true,
160    path: "precision/client/rsync.sh"
161
162  client.vm.provider "client_vnc",
163    type: "shell",
164    preserve_order: true,
165    path: "precision/client/vnc.sh"
166
167  client.vm.provider "client_vnc",
168    type: "shell",
169    preserve_order: true,
170    path: "precision/client/vnc.sh"
171
172  server.vm.provider "client_routing",
173    type: "shell",
174    preserve_order: true,
175    path: "precision/client/routing.sh"
```

Рис. 18: Настройка Vagrantfile

Выводы

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