

Лабораторная работа № 15

Настройка сетевого журналирования

Демидова Е. А.

18 декабря 2023

Российский университет дружбы народов, Москва, Россия

Вводная часть

Получение навыков по работе с журналами системных событий.

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.
4. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d  
touch netlog-server.conf
```



The image shows a terminal window with a dark background. The title bar at the top reads "root@server:/etc/rsyslog.d". Below the title bar, the text "GNU nano 5.6.1" is on the left, "netlog-server.conf" is in the center, and "Modified" is on the right. The main content area shows two lines of configuration: "\$ModLoad imtcp" and "\$InputTCPServerRun 514". A white cursor is positioned at the end of the second line.

```
root@server:/etc/rsyslog.d
GNU nano 5.6.1 netlog-server.conf Modified
$ModLoad imtcp
$InputTCPServerRun 514

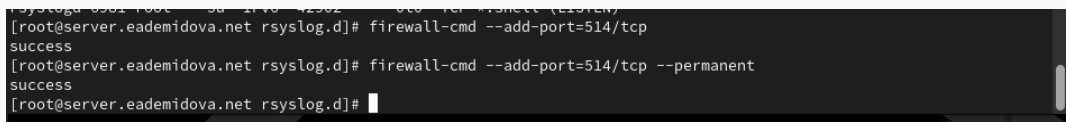
```

Рис. 1: Включение журналирования по TCP-порту 514

Настройка сервера сетевого журнала

```
packagekit 5120 4970 rx:backen root 418 IPv4 42913 0t0 TCP *:shell (LISTEN)
a.net:34614->193.174.29.5:https (ESTABLISHED)
rsyslogd 6981 root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6982 in:imtcp root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6982 in:imtcp root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6984 in:imjour root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6984 in:imjour root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6985 rs:main root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6985 rs:main root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6986 in:imtcp root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6986 in:imtcp root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6987 in:imtcp root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6987 in:imtcp root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6988 in:imtcp root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6988 in:imtcp root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6989 in:imtcp root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 6989 in:imtcp root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
[root@server.eademidova.net rsyslog.d]# systemctl restart rsyslogd
Failed to restart rsyslogd.service: Unit rsyslogd.service not found.
[root@server.eademidova.net rsyslog.d]# ss -tln -i :514
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
rsyslogd 6981 root 4u IPv4 42901 0t0 TCP *:shell (LISTEN)
rsyslogd 6981 root 5u IPv6 42902 0t0 TCP *:shell (LISTEN)
[root@server.eademidova.net rsyslog.d]#
```

Рис. 2: Просмотр прослушиваемых портов, связанных с rsyslog

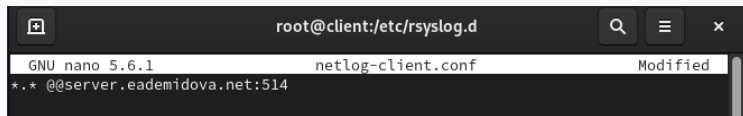
A terminal window with a dark background and light-colored text. The prompt is [root@server.eademidova.net rsyslog.d]#. The first command is firewall-cmd --add-port=514/tcp, followed by the output success. The second command is firewall-cmd --add-port=514/tcp --permanent, also followed by the output success. The prompt returns to [root@server.eademidova.net rsyslog.d]# with a cursor.

```
rsyslogd 8381 root 0 0 1178 42962 0 0 TCP #rsnet (LISTEN)  
[root@server.eademidova.net rsyslog.d]# firewall-cmd --add-port=514/tcp  
success  
[root@server.eademidova.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent  
success  
[root@server.eademidova.net rsyslog.d]#
```

Рис. 3: Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

На клиенте создадим файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d  
touch netlog-client.conf
```



The image shows a terminal window with a dark background. The title bar at the top reads 'root@client:/etc/rsyslog.d'. Below the title bar, the text 'GNU nano 5.6.1' is on the left, 'netlog-client.conf' is in the center, and 'Modified' is on the right. The main content of the terminal shows the configuration line: '*.* @@server.eademidova.net:514'.

```
root@client:/etc/rsyslog.d
GNU nano 5.6.1 netlog-client.conf Modified
*. * @@server.eademidova.net:514
```

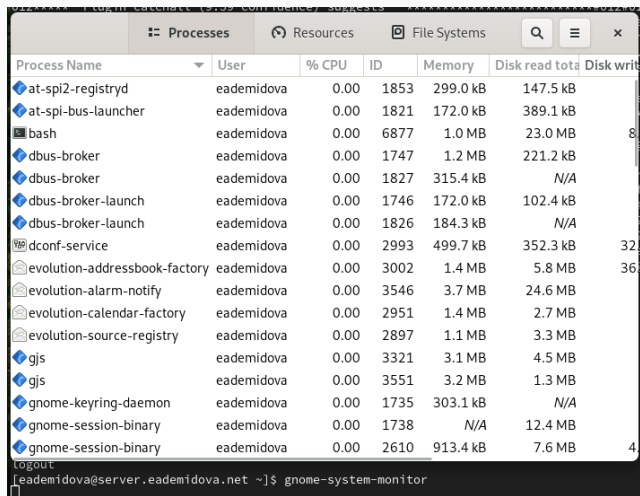
Рис. 4: Включение перенаправления сообщений журнала на 514 TCP-порт сервера

```
systemctl restart rsyslog
```

Просмотр журнала

```
success
[root@server.eademidova.net rsyslog.d]# tail -f /var/log/messages
Dec 24 14:34:10 client systemd[1]: Started Network Manager Script Dispatcher Service.
Dec 24 14:34:10 client systemd[1]: Starting SETroubleshoot daemon for processing new SELinux denial logs...
Dec 24 14:34:10 client nm-dispatcher[7547]: req:1 'dhcp4-change' [eth1], "/usr/lib/NetworkManager/dispatcher.d/20-chr
rony-dhcp": complete: failed with Script '/usr/lib/NetworkManager/dispatcher.d/20-chroney-dhcp' exited with status 1.
Dec 24 14:34:10 client NetworkManager[4777]: <warn> [1703428450.6610] dispatcher: (25) /usr/lib/NetworkManager/disp
atcher.d/20-chroney-dhcp failed (failed): Script '/usr/lib/NetworkManager/dispatcher.d/20-chroney-dhcp' exited with st
atus 1.
Dec 24 14:34:10 client systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
Dec 24 14:34:11 client systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@4.service.
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using the dac_read_search capa
bility. For complete SELinux messages run: sealert -l 20ba8c39-db5e-4379-a931-d3a564f623dd
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using the dac_read_search capa
bility.#012#012***** Plugin dac_override (91.4 confidence) suggests *****#012#012If you want to
help identify if domain needs this access or you have a file with the wrong permissions on your system#012Then turn
on full auditing to get path information about the offending file and generate the error again.#012Do#012#012Turn on
full auditing#012# auditctl -w /etc/shadow -p w#012Try to recreate AVC. Then execute#012# ausearch -m avc -ts recen
t#012If you see PATH record check ownership/permissions on file, and fix it,#012otherwise report as a bugzilla.#012#
012***** Plugin catchall (9.59 confidence) suggests *****#012#012If you believe that bash sh
ould have the dac_read_search capability by default.#012Then you should report this as a bug.#012You can generate a
local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c '20-chro
ny-dhcp' --raw | audit2allow -M my-20chroneydhcp#012# semodule -X 300 -i my-20chroneydhcp.pp#012
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using the dac_override capabil
ity. For complete SELinux messages run: sealert -l 0af3bb6b-28d3-4a13-9594-864c2e688b4b
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using the dac_override capabil
ity.#012#012***** Plugin dac_override (91.4 confidence) suggests *****#012#012If you want to hel
p identify if domain needs this access or you have a file with the wrong permissions on your system#012Then turn on
full auditing to get path information about the offending file and generate the error again.#012Do#012#012Turn on fu
ll auditing#012# auditctl -w /etc/shadow -p w#012Try to recreate AVC. Then execute#012# ausearch -m avc -ts recent#0
12If you see PATH record check ownership/permissions on file, and fix it,#012otherwise report as a bugzilla.#012#012
***** Plugin catchall (9.59 confidence) suggests *****#012#012If you believe that bash shoul
d have the dac_override capability by default.#012Then you should report this as a bug.#012You can generate a local
policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c '20-chroney-dhc
p' --raw | audit2allow -M my-20chroneydhcp#012# semodule -X 300 -i my-20chroneydhcp.pp#012
Dec 24 14:34:20 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Dec 24 14:34:22 client systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@4.service: Deactivated succe
ssfully.
Dec 24 14:34:22 client systemd[1]: setroubleshootd.service: Deactivated successfully.
```

Рис. 5: Просмотр файла /var/log/messages журнала

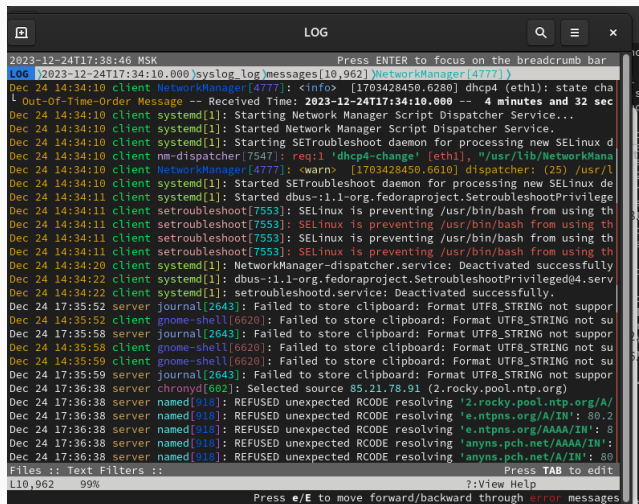


Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
at-spi2-registryd	eademidova	0.00	1853	299.0 kB	147.5 kB	
at-spi-bus-launcher	eademidova	0.00	1821	172.0 kB	389.1 kB	
bash	eademidova	0.00	6877	1.0 MB	23.0 MB	8
dbus-broker	eademidova	0.00	1747	1.2 MB	221.2 kB	
dbus-broker	eademidova	0.00	1827	315.4 kB	N/A	
dbus-broker-launch	eademidova	0.00	1746	172.0 kB	102.4 kB	
dbus-broker-launch	eademidova	0.00	1826	184.3 kB	N/A	
dconf-service	eademidova	0.00	2993	499.7 kB	352.3 kB	32
evolution-addressbook-factory	eademidova	0.00	3002	1.4 MB	5.8 MB	36
evolution-alarm-notify	eademidova	0.00	3546	3.7 MB	24.6 MB	
evolution-calendar-factory	eademidova	0.00	2951	1.4 MB	2.7 MB	
evolution-source-registry	eademidova	0.00	2897	1.1 MB	3.3 MB	
gjs	eademidova	0.00	3321	3.1 MB	4.5 MB	
gjs	eademidova	0.00	3551	3.2 MB	1.3 MB	
gnome-keyring-daemon	eademidova	0.00	1735	303.1 kB	N/A	
gnome-session-binary	eademidova	0.00	1738	N/A	12.4 MB	
gnome-session-binary	eademidova	0.00	2610	913.4 kB	7.6 MB	4
logout						

```
logout  
[eademidova@server.eademidova.net ~]$ gnome-system-monitor
```

Рис. 6: Запуск графической программы для просмотра журналов

```
dnf -y install lnav
```



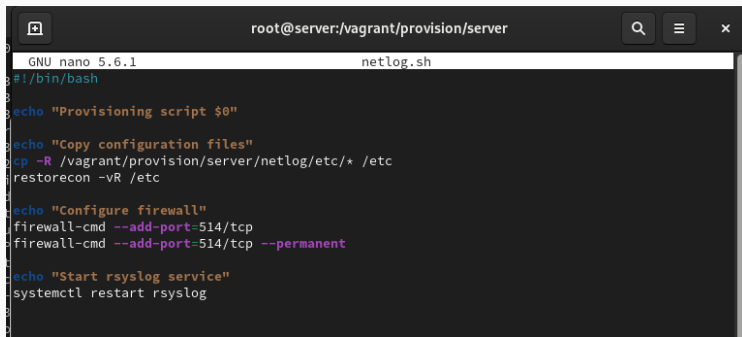
```
LOG
2023-12-24T17:38:46 MSK Press ENTER to focus on the breadcrumb bar
LOG 2023-12-24T17:34:10.000 syslog_log messages[10,962] NetworkManager[4777]
Dec 24 14:34:10 client NetworkManager[4777]: <info> [1703428450.6280] dhcp4 (eth1): state cha
l Out-Of-Time-Order Message -- Received Time: 2023-12-24T17:34:10.000 -- 4 minutes and 32 sec
Dec 24 14:34:10 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Dec 24 14:34:10 client systemd[1]: Started Network Manager Script Dispatcher Service.
Dec 24 14:34:10 client systemd[1]: Starting SETroubleshoot daemon for processing new SELinux d
Dec 24 14:34:10 client nm-dispatcher[7547]: req:1 'dhcp4-change' [eth1], "/usr/lib/NetworkMana
Dec 24 14:34:10 client NetworkManager[4777]: <warn> [1703428450.6610] dispatcher: (25) /usr/l
Dec 24 14:34:10 client systemd[1]: Started SETroubleshoot daemon for processing new SELinux de
Dec 24 14:34:11 client systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using th
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using th
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using th
Dec 24 14:34:11 client setroubleshoot[7553]: SELinux is preventing /usr/bin/bash from using th
Dec 24 14:34:20 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully
Dec 24 14:34:22 client systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@4.serv
Dec 24 14:34:22 client systemd[1]: setroubleshootd.service: Deactivated successfully.
Dec 24 17:35:52 server journal[2643]: Failed to store clipboard: Format UTF8_STRING not suppor
Dec 24 14:35:52 client gnome-shell[6620]: Failed to store clipboard: Format UTF8_STRING not su
Dec 24 17:35:58 server journal[2643]: Failed to store clipboard: Format UTF8_STRING not suppor
Dec 24 14:35:58 client gnome-shell[6620]: Failed to store clipboard: Format UTF8_STRING not su
Dec 24 14:35:59 client gnome-shell[6620]: Failed to store clipboard: Format UTF8_STRING not su
Dec 24 17:35:59 server journal[2643]: Failed to store clipboard: Format UTF8_STRING not suppor
Dec 24 17:36:38 server chronyd[602]: Selected source 85.21.78.91 (2.rocky.pool.ntp.org)
Dec 24 17:36:38 server named[918]: REFUSED unexpected RCODE resolving '2.rocky.pool.ntp.org/A/
Dec 24 17:36:38 server named[918]: REFUSED unexpected RCODE resolving 'e.ntpns.org/A/IN': 80.2
Dec 24 17:36:38 server named[918]: REFUSED unexpected RCODE resolving 'e.ntpns.org/AAAA/IN': 8
Dec 24 17:36:38 server named[918]: REFUSED unexpected RCODE resolving 'anyns.pch.net/AAAA/IN': 8
Dec 24 17:36:38 server named[918]: REFUSED unexpected RCODE resolving 'anyns.pch.net/A/IN': 80
Files :: Text Filters :: Press TAB to edit
L10,962 99% ?::View Help
Press e/E to move forward/backward through error messages
```

Рис. 7: Просмотр логов с клиента и сервера


```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/

touch netlog.sh
chmod +x netlog.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
root@server:/vagrant/provision/server
GNU nano 5.6.1 netlog.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

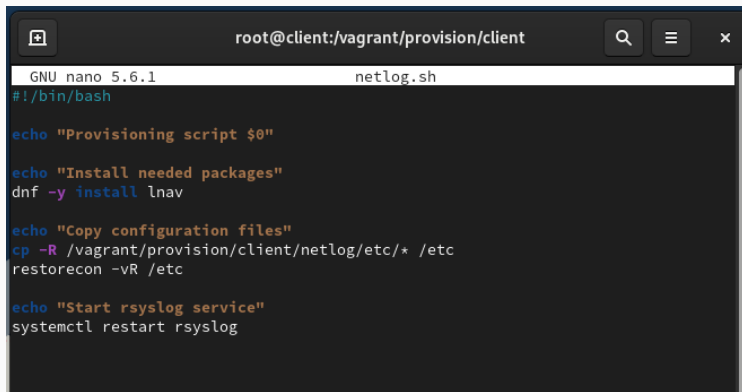
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent

echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 8: Скрипта файла /vagrant/provision/server/netlog.sh

```
cd /vagrant/provision//client
mkdir -p /vagrant/provision//client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-/client.conf /vagrant/provision//client/netlog/etc

touch netlog.sh
chmod +x netlog.sh
```



The image shows a terminal window with a dark background. The title bar at the top reads "root@client:/vagrant/provision/client". The terminal content shows the GNU nano 5.6.1 editor editing the file "netlog.sh". The script contains several lines of shell commands, each preceded by an "echo" statement for logging. The commands are: setting the shell to bash, installing lnav, copying configuration files from the netlog/etc directory to the system etc directory, and restarting the rsyslog service.

```
GNU nano 5.6.1 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. 9: Скрипта файла /vagrant/provision/client/ netlog.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"
```

Заключение

В результате выполнения данной работы были приобретены практические навыки по работе с журналами системных событий.