

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 15

дисциплина: Администрирование сетевых подсистем

Настройка сетевого журналирования

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы

Приобретение навыков по работе с журналами системных событий.

Ход работы

1. Настройка сервера сетевого журнала

1. На сервере создайте файл конфигурации сетевого хранения журналов

```
[root@server.etanribergenov.net ~]#  
[root@server.etanribergenov.net ~]# cd /etc/rsyslog.d  
[root@server.etanribergenov.net rsyslog.d]# touch netlog-server.conf  
[root@server.etanribergenov.net rsyslog.d]#
```

Рис. 1. Создание файла конфигурации сетевого хранения журналов

2. В файле конфигурации /etc/rsyslog.d/netlog-server.conf включите приём записей журнала по TCP-порту 514

```
netlog-s~ver.conf [-M- -  
$ModLoad imtcp  
$InputTCPServerRun 514
```

Рис. 2. Включение приёма записей журнала по TCP-порту 514

3. Перезапустите службу rsyslog и посмотрите, какие порты, связанные с rsyslog, прослушиваются:
systemctl restart rsyslog

lsof | grep TCP

```
[root@server.etanribergenov.net rsyslog.d]#  
[root@server.etanribergenov.net rsyslog.d]# systemctl restart rsyslog  
[root@server.etanribergenov.net rsyslog.d]#
```

Рис. 3. Перезапуск службы rsyslog

```
[root@server.etanribergenov.net rsyslog.d]#  
[root@server.etanribergenov.net rsyslog.d]# lsof | grep TCP  
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs  
Output information may be incomplete.
```

0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6135	in:imjour	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6136	rs:main	root	4u	IPv4 39225
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6136	rs:main	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6137	in:imtcp	root	4u	IPv4 39225
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6137	in:imtcp	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6138	in:imtcp	root	4u	IPv4 39225
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6138	in:imtcp	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6139	in:imtcp	root	4u	IPv4 39225
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6139	in:imtcp	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6140	in:imtcp	root	4u	IPv4 39225
0t0	TCP	*:shell (LISTEN)				
rsyslogd	6132	6140	in:imtcp	root	5u	IPv6 39226
0t0	TCP	*:shell (LISTEN)				

```
[root@server.etanribergenov.net rsyslog.d]#
```

Рис. 4. Просмотр прослушиваемых портов, связанных с rsyslog

4. На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514

```
[root@server.etanribergenov.net rsyslog.d]#  
[root@server.etanribergenov.net rsyslog.d]# firewall-cmd --add-port=514/tcp  
success  
[root@server.etanribergenov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --pe  
rmanent  
success  
[root@server.etanribergenov.net rsyslog.d]#
```

Рис. 5. Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

2. Настройка клиента сетевого журнала

1. На клиенте создайте файл конфигурации сетевого хранения журналов

```
[root@client.etanribergenov.net ~]# cd /etc/rsyslog.d
[root@client.etanribergenov.net rsyslog.d]# touch netlog-client.conf
[root@client.etanribergenov.net rsyslog.d]#
```

Рис. 6. Создание файла конфигурации сетевого хранения журналов

2. На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включите перенаправление сообщений журнала на 514 TCP-порт сервера

```
netlog-c~ent.conf [----] 35 L:[ 1+
*.* @@server.etanribergenov.net:514
```

Рис. 7. Включение на клиенте перенаправления сообщений журнала на 514 TCP-порт сервера

3. Перезапустите службу rsyslog

```
[root@client.etanribergenov.net rsyslog.d]# systemctl restart rsyslog
[root@client.etanribergenov.net rsyslog.d]#
```

Рис. 8. Перезапуск службы rsyslog

3. Просмотр журнала

1. На сервере просмотрите один из файлов журнала

Обратите внимание на имя хоста и другие сообщения о работе сервисов. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.

```
[root@server.etanribergenov.net ~]# tail -f /var/log/messages
Apr 14 15:49:00 client rsyslogd[603]: [origin software="rsyslogd" swVersion="8.2
102.0-101.el9_0.1" x-pid="603" x-info="https://www.rsyslog.com"] exiting on sign
al 15.
Apr 14 15:49:00 client systemd[1]: rsyslog.service: Deactivated successfully.
Apr 14 15:49:00 client systemd[1]: Stopped System Logging Service.
Apr 14 15:49:00 client systemd[1]: Starting System Logging Service...
Apr 14 15:49:00 client systemd[1]: Started System Logging Service.
Apr 14 15:49:00 client rsyslogd[5859]: [origin software="rsyslogd" swVersion="8.
2102.0-101.el9_0.1" x-pid="5859" x-info="https://www.rsyslog.com"] start
Apr 14 15:49:00 client rsyslogd[5859]: imjournal: journal files changed, reloadi
ng... [v8.2102.0-101.el9_0.1 try https://www.rsyslog.com/e/0 ]
Apr 14 15:49:10 client systemd[1]: Started XFS file system (6177) loaded by
```

Рис. 9. Просмотр одного из файлов журнала на сервере

2. На сервере под пользователем etanribergenov запустите графическую программу для просмотра журналов
gnome-system-monitor

Processes							
Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ	
at-spi2-registryd	etanribergenov	0.00	5143	446.5 kB	573.4 kB		
at-spi-bus-launcher	etanribergenov	0.00	5112	143.4 kB	16.4 kB		
bash	etanribergenov	0.00	5919	938.0 kB	5.9 MB		
bash	etanribergenov	0.00	6039	2.0 MB	409.6 kB		
bash	etanribergenov	0.00	6177	2.0 MB	782.3 kB		
bash	etanribergenov	0.00	6233	2.0 MB	376.8 kB		
dbus-broker	etanribergenov	0.00	5053	1.4 MB	N/A		
dbus-broker	etanribergenov	0.00	5118	303.1 kB	N/A		
dbus-broker-launch	etanribergenov	0.00	5052	200.7 kB	98.3 kB		
dbus-broker-launch	etanribergenov	0.00	5117	344.1 kB	N/A		
dconf-service	etanribergenov	0.00	5281	450.6 kB	176.1 kB	20.	
evolution-addressbook-factory	etanribergenov	0.00	5284	938.0 kB	4.2 MB	36.	
evolution-alarm-notify	etanribergenov	0.00	5442	8.0 MB	22.4 MB		
evolution-calendar-factory	etanribergenov	0.00	5240	3.3 MB	3.5 MB		
evolution-source-registry	etanribergenov	0.00	5229	3.1 MB	3.5 MB		
gjs	etanribergenov	0.00	5341	3.0 MB	1.2 MB		
gjs	etanribergenov	0.00	5433	3.7 MB	20.5 kB		

Рис. 10. Запуск графической программы для просмотра журналов на сервере под пользователем etanribergenov

3. На сервере установите просмотрщик журналов системных сообщений lnav или его аналог.

```
[root@server.etanribergenov.net ~]# dnf -y install lnav
```

Рис. 11. Установка просмотрщика журналов сист. сообщений lnav

4. Просмотрите логи с помощью lnav или его аналога

```
2023-04-14T16:01:25 UTC Press ENTER to focus on the breadcrumb bar
LOG >2023-04-14T15:55:06.000>syslog log>messages[32,595]>named[898]>
Apr 14 15:55:06 server named[898]: network unreachable resolving 'ns-iad02.fed
Apr 14 15:55:07 server named[898]: network unreachable resolving 'ns-iad01.fed
Apr 14 15:57:27 server systemd[1]: Started /usr/bin/systemctl start man-db-cac
Apr 14 15:57:28 server systemd[1]: Starting man-db-cache-update.service...
Apr 14 15:57:44 server systemd[1]: man-db-cache-update.service: Deactivated su
Apr 14 15:57:44 server systemd[1]: Finished man-db-cache-update.service.
Apr 14 15:57:44 server systemd[1]: man-db-cache-update.service: Consumed 3.040
Apr 14 15:57:44 server systemd[1]: run-racf7233437564f278d4eb246c470b360.servi
Apr 14 15:58:41 client NetworkManager[4678]: <info> [1681487921.1993] dhcp4 (
Apr 14 15:58:41 server dhcpcd[1140]: DHCPREQUEST for 192.168.1.125 from 08:00:2
Apr 14 15:58:41 server dhcpcd[1140]: DHCPACK on 192.168.1.125 to 08:00:27:3c:83
```

Рис. 12. Просмотр записей с сервера с помощью lnav

```
2023-04-14T16:05:42 UTC
LOG >2023-04-14T15:48:18.000>syslog log>messages[31,901]>systemd[1]>
Apr 14 15:48:18 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated
Apr 14 15:48:18 server systemd[1]: Finished Cleanup of Temporary Directories.
Apr 14 15:48:41 server dhcpcd[1140]: DHCPREQUEST for 192.168.1.125 from 08:00:2
Apr 14 15:48:41 server dhcpcd[1140]: DHCPACK on 192.168.1.125 to 08:00:27:3c:83
Apr 14 15:48:59 client systemd[1]: Stopping System Logging Service...
Apr 14 15:49:00 client rsyslogd[603]: [origin software="rsyslogd" swVersion="8
Apr 14 15:49:00 client systemd[1]: rsyslog.service: Deactivated successfully.
Apr 14 15:49:00 client systemd[1]: Stopped System Logging Service.
Apr 14 15:49:00 client systemd[1]: Starting System Logging Service...
Apr 14 15:49:00 client systemd[1]: Started System Logging Service.
Apr 14 15:49:00 client rsyslogd[5859]: [origin software="rsyslogd" swVersion="
Apr 14 15:49:00 client rsyslogd[5859]: imjournal: journal files changed, reloa
Apr 14 15:49:12 server systemd[5029]: Started VTE child process 6177 launched
Apr 14 15:49:18 server systemd[1]: Starting Hostname Service...
Apr 14 15:49:19 server systemd[1]: Started Hostname Service.
Apr 14 15:49:41 server systemd[5029]: Started VTE child process 6233 launched
Apr 14 15:49:49 server systemd[1]: systemd-hostnamed.service: Deactivated succ
Apr 14 15:51:07 client PackageKit[5163]: uid 1001 is trying to obtain org.free
Apr 14 15:51:08 client PackageKit[5163]: uid 1001 obtained auth for org.freede
Files :: Text Filters :: Press TAB to edit
```

Рис. 12. Просмотр записей с клиента с помощью lnav

4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы

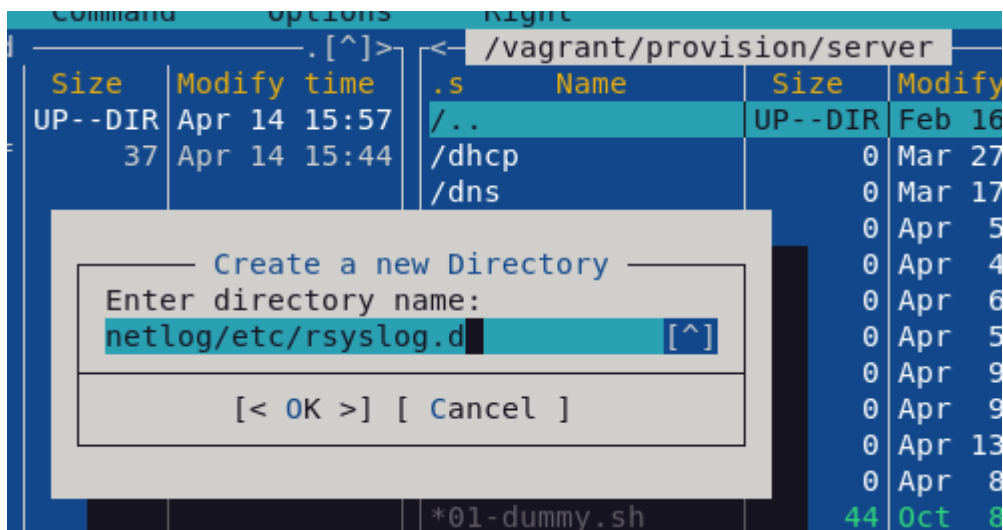


Рис. 13. Создание подкаталогов для конф. файла сервера

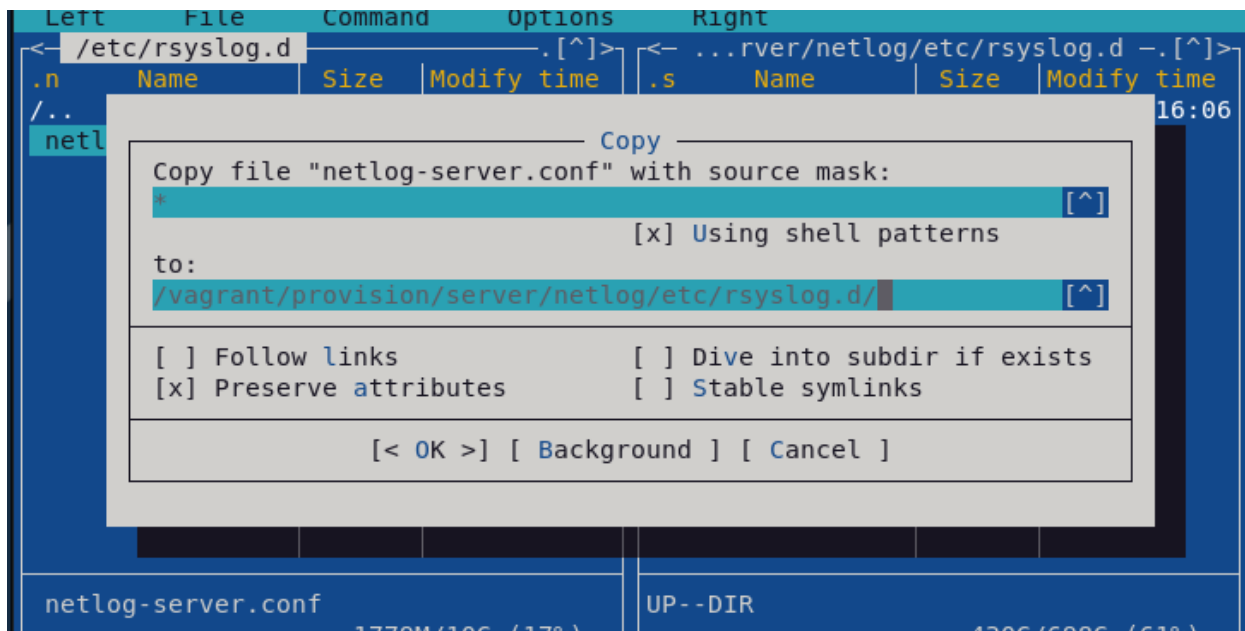


Рис. 14. Копирование конфигурационного файла на сервере

2. В каталоге `/vagrant/provision/server` создайте исполняемый файл `netlog.sh`, в котором пропишите скрипт, повторяющий произведённые в лаб. работе действия.

```
[root@server.etanribergenov.net server]# touch netlog.sh
[root@server.etanribergenov.net server]# chmod +x netlog.sh
[root@server.etanribergenov.net server]#
```

Рис. 15. Создание исполняемого файла для сервера

```
netlog.sh [-M--] 28 L:[ 1+12 13/ 14] *(27
#!/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. 16. Скрипт в исполняемом файле для сервера

3. На виртуальной машине `client` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/client/`, создайте в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы

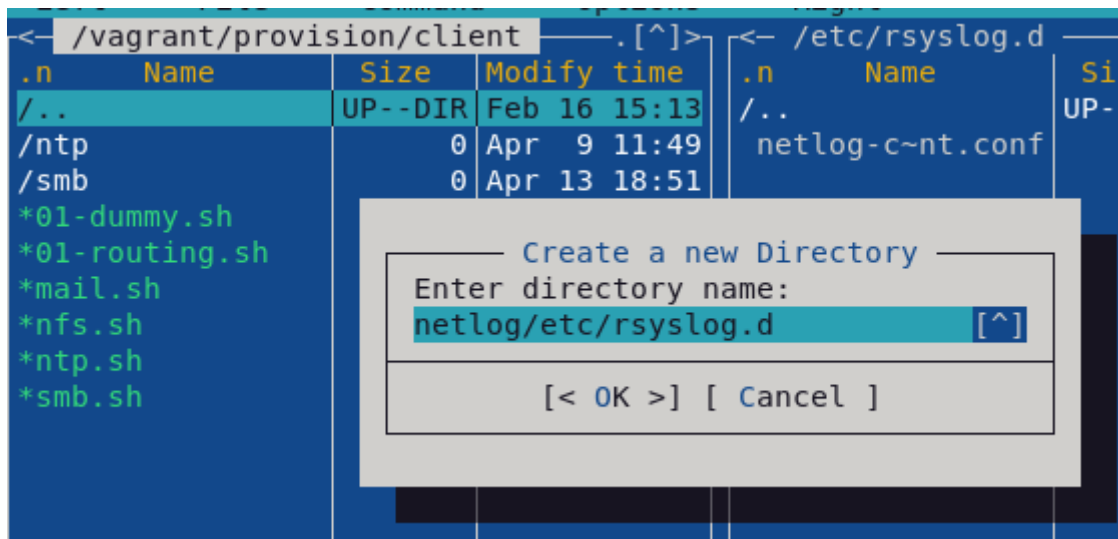


Рис. 17. Создание подкаталогов для конф. файла клиента

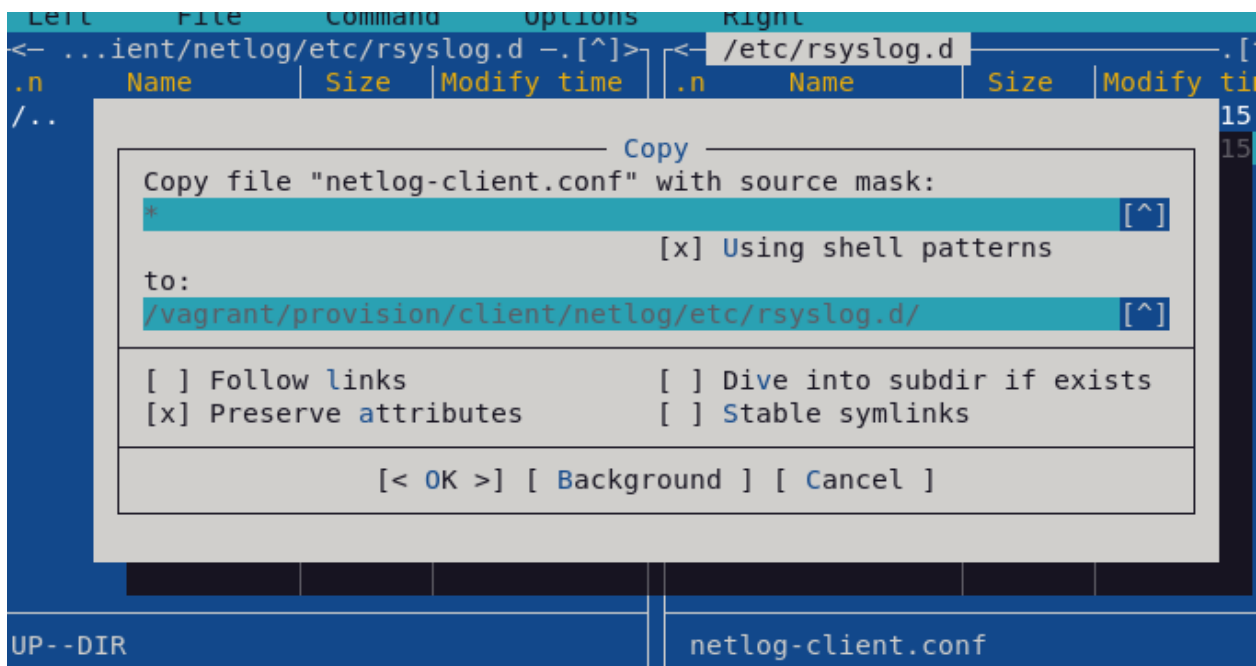


Рис. 18. Копирование конф. файла на клиенте

4. В каталоге `/vagrant/provision/client` создайте исполняемый файл `netlog.sh`

```
[root@client.etanribergenov.net client]# touch netlog.sh
[root@client.etanribergenov.net client]# chmod +x netlog.sh
[root@client.etanribergenov.net client]# d
```

Рис. 19. Создание исполняемого файла для клиента

```
netlog.sh [-M--] 25 L:[ 1+12 13/ 13] *(2
#!/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. 20. Скрипт в исполняемом файле для клиента

5. Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile необходимо добавить в разделах конфигурации сервера и клиента соответствующие записи.

```
Vagrantfile [-M--] 16 L:[ 89+12 101
server.vm.provision "server netlog",
  type: "shell",
  preserve_order: true,
  path: "provision/server/netlog.sh"
```

Рис. 21. Запись в Vagrantfile для работы скрипта сервера

```
Vagrantfile [----] 0 L:[156+21 177
  preserve_order: true,
  path: "provision/client/smb.sh"

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

Рис. 22. Запись в Vagrantfile для работы скрипта клиента

Вывод

В результате выполнения лабораторной работы я приобрёл навыки по работе с журналами системных событий.

Ответы на контрольные вопросы

1. Модуль imtcp.
2. Модуль imjournal.
3. Параметр InputTCPServerRun 514
4. Файл /etc/rsyslog.conf
5. Перенаправление: *.* @@server.user.net:514
6. Модуль imjournal
7. Модуль onmysql
8. Строки: \$ModLoad imtcp, \$InputTCPServerRun 514
9. Команда firewall-cmd --add-port=514/tcp