

Лабораторная работа №15

Настройка сетевого журналирования

Спелов Андрей Николаевич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Выводы	14
4 Ответы на контрольные вопросы:	15
Список литературы	17

Список иллюстраций

2.1	Создание на сервере файла конфигурации сетевого хранения журналов.	6
2.2	Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514.	6
2.3	Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.	7
2.4	Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.	7
2.5	Создание на клиенте файла конфигурации сетевого хранения журналов.	7
2.6	Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.	8
2.7	Перезапуск службы rsyslog.	8
2.8	Просмотр на сервере одного из файлов журнала.	8
2.9	Запуск на сервере под пользователем anspelov графической программы для просмотра журналов.	9
2.10	Установка на сервере просмотрика журналов системных сообщений.	9
2.11	Просмотр логов.	10
2.12	Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.	10
2.13	Открытие файла на редактирование и добавление в него скрипта.	11
2.14	Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.	11
2.15	Открытие файла на редактирование и добавление в него скрипта.	12
2.16	Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.	13

Список таблиц

1 Цель работы

Целью данной работы является получение навыков по работе с журналами системных событий.

2 Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов(рис. 2.1).

```
[anspelov@server.an spelov.net rsyslog.d]$ sudo -i  
[sudo] password for an spelov:  
[root@server.an spelov.net ~]# cd /etc/rsyslog.d  
[root@server.an spelov.net rsyslog.d]# touch netlog-server.conf  
[root@server.an spelov.net rsyslog.d]# █
```

Рис. 2.1: Создание на сервере файла конфигурации сетевого хранения журналов.

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514 (рис. 2.2).

```
netlog-server.conf [-M-] 22 L:[ 1+ 1 2/ 2] *(37 / 37b) <EOF>  
$ModLoad imtcp  
$InputTCPServerRun 514
```

Рис. 2.2: Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приема записей журнала по TCP-порту 514.

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются(рис. 2.3).

```
[root@server.an spelov.net rsyslog.d]# systemctl restart rsyslog
[root@server.an spelov.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.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
systemd      1      root    78u   IPv6          7589    0t0      TCP *:websm (LISTEN)
cupaud     1236      root    7u   IPv6         11076    0t0      TCP localhost:ipp (LISTEN)
cupaud     1236      root    8u   IPv4         11077    0t0      TCP localhost:ipp (LISTEN)
sshd      1237      root    7u   IPv4         11067    0t0      TCP *:ssh (LISTEN)
sshd      1237      root    8u   IPv6         11069    0t0      TCP *:ssh (LISTEN)
smbd      1317      root   27u   IPv6         12295    0t0      TCP *:microsoft-ds (LISTEN)
smbd      1317      root   28u   IPv6         12296    0t0      TCP *:netbios-ssn (LISTEN)
smbd      1317      root   29u   IPv4         12297    0t0      TCP *:microsoft-ds (LISTEN)
smbd      1317      root   30u   IPv4         12298    0t0      TCP *:netbios-ssn (LISTEN)
rsyslogd   9044      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9046 in:imjour      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9046 in:imjour      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9047 in:imtcp      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9047 in:imtcp      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9048 in:imtcp      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9048 in:imtcp      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9049 in:imtcp      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9049 in:imtcp      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9050 in:imtcp      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9050 in:imtcp      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9051 in:imtcp      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9051 in:imtcp      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9052 rs:main      root    4u   IPv4         39958    0t0      TCP *:shell (LISTEN)
rsyslogd   9044 9052 rs:main      root    5u   IPv6         39959    0t0      TCP *:shell (LISTEN)
[root@server.an spelov.net rsyslog.d]#
```

Рис. 2.3: Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514(рис. 2.4).

```
[root@server.an spelov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.an spelov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.an spelov.net rsyslog.d]#
```

Рис. 2.4: Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

На клиенте создадим файл конфигурации сетевого хранения журналов (рис. 2.5).

```
[an spelov@client.an spelov.net ~]$ sudo -i
[sudo] password for an spelov:
[root@client.an spelov.net ~]# cd /etc/rsyslog.d
[root@client.an spelov.net rsyslog.d]# touch netlog-client.conf
[root@client.an spelov.net rsyslog.d]#
```

Рис. 2.5: Создание на клиенте файла конфигурации сетевого хранения журналов.

Далее в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщений журнала на 514 TCP-порт сервера (рис. 2.6).

```
netlog-client.conf [-M--] 29 L:[ 1+ 0 1/ 1 ] *(29 / 29b) <EOF>
*.* @server.an spelov.net:514
```

Рис. 2.6: Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Перезапустим службу rsyslog (рис. 2.7).

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

Рис. 2.7: Перезапуск службы rsyslog.

На сервере просмотрим один из файлов журнала(рис. 2.8).

```
[root@server.an spelov.net rsyslog.d]# tail -f /var/log/messages
Dec 8 09:39:21 server kernel: traps: VBoxClient[10180] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,4000000+bb000]
Dec 8 09:39:21 server systemd-coredump[10181]: Process 10177 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 09:39:21 server systemd[1]: Started systemd-coredump@152-10181-0.service - Process Core Dump (PID 10181/UID 0)

Dec 8 09:39:21 server systemd-coredump[10182]: Process 10177 (VBoxClient) of user 1001 dumped core.#012#012Module libKau.so.6 from rpm libKau-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 10180:#012#0 0x0000000000041db4b n/a (n/a + 0x0)#012#1 0x0000000000041dac4 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x000007f20c4b4db68 start_thread (libc.so.6 + 0x94b68)#012#5 0x000007f20c4bbe6bc __clone3 (libc.so.6 + 0x1056bc)#012#6 0x000007f20c4bbe4bd syscall (libc.so.6 + 0x1034bd)#012#1 0x000000000004347e2 n/a (n/a + 0x0)#012#2 0x0000000000450d6d n/a (n/a + 0x0)#012#3 0x00000000000416449 n/a (n/a + 0x0)#012#4 0x000000000004181c1 n/a (n/a + 0x0)#012#5 0x00000000000417c5a n/a (n/a + 0x0)#012#6 0x00000000000404860 n/a (n/a + 0x0)#012#7 0x0000000000450a8c n/a (n/a + 0x0)#012#8 0x00000000000435890 n/a (n/a + 0x0)#012#9 0x00007f20c4b4db68 start_thread (libc.so.6 + 0x94b68)#012#10 0x000007f20c4bbe6bc __clone3 (libc.so.6 + 0x1056bc)#012#11 0x000007f20c4bbe4bd syscall (libc.so.6 + 0x1034bd)#012#12 0x000000000004506d6 n/a (n/a + 0x0)#012#13 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x000007f20c4ae330e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x000007f20c4ae33c9 __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
Dec 8 09:39:21 server systemd[1]: system-coredump@152-10181-0.service: Deactivated successfully.
Dec 8 09:39:26 server kernel: traps: VBoxClient[10190] trap int3 ip:41db4b sp:7f20b6435cd0 error:0 in VBoxClient[1db4b,4000000+bb000]
Dec 8 09:39:26 server systemd-coredump[10191]: Process 10187 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 8 09:39:26 server systemd[1]: Started systemd-coredump@153-10191-0.service - Process Core Dump (PID 10191/UID 0)

Dec 8 09:39:26 server systemd-coredump[10192]: Process 10187 (VBoxClient) of user 1001 dumped core.#012#012Module libKau.so.6 from rpm libKau-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 10190:#012#0 0x0000000000041db4b n/a (n/a + 0x0)#012#1 0x0000000000041dac4 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x000007f20c4b4db68 start_thread (libc.so.6 + 0x94b68)#012#5 0x000007f20c4bbe6bc __clone3 (libc.so.6 + 0x1056bc)#012#6 0x000007f20c4bbe4bd syscall (libc.so.6 + 0x1034bd)#012#7 0x00000000000434fe0 n/a (n/a + 0x0)#012#8 0x00000000000435890 n/a (n/a + 0x0)#012#9 0x000007f20c4b4db68 start_thread (libc.so.6 + 0x94b68)#012#10 0x000007f20c4bbe6bc __clone3 (libc.so.6 + 0x1056bc)#012#11 0x000007f20c4bbe4bd syscall (libc.so.6 + 0x1034bd)#012#12 0x000000000004506d6 n/a (n/a + 0x0)#012#13 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x000007f20c4ae330e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x000007f20c4ae33c9 __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
Dec 8 09:39:26 server systemd[1]: system-coredump@153-10191-0.service: Deactivated successfully.
```

Рис. 2.8: Просмотр на сервере одного из файлов журнала.

На сервере под пользователем an spelov запустим графическую программу для просмотра журналов (рис. 2.9).

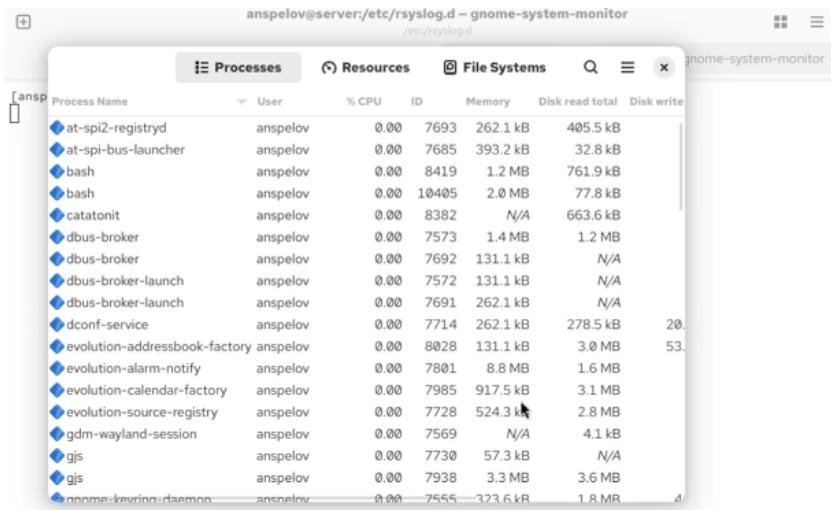


Рис. 2.9: Запуск на сервере под пользователем anspelov графической программы для просмотра журналов.

На сервере установим просмотрщик журналов системных сообщений(рис. 2.10).

```
[root@server.an spelov.net rsyslog.d]# sudo dnf install -y multtail
Last metadata expiration check: 0:29:58 ago on Mon 08 Dec 2025 09:53:25 AM UTC.
Dependencies resolved.
=====
Package                                Architecture      Version
=====
Installing:
multtail                               x86_64          7.1.3-2.el10_0
=====
Transaction Summary
Install 1 Package
Total download size: 148 k
Installed size: 326 k
Downloading Packages:
multtail-7.1.3-2.el10_0.x86_64.rpm
=====
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing
  Installing : multtail-7.1.3-2.el10_0.x86_64
  Running scriptlet: multtail-7.1.3-2.el10_0.x86_64
```

Рис. 2.10: Установка на сервере просмотрщика журналов системных сообщений.

Просмотрим логи(рис. 2.11).

Рис. 2.11: Просмотр логов.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh(рис. 2.12).

```
[root@server anspelov.net rsyslog.d]# cd /vagrant/provision/server
[root@server anspelov.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server anspelov.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server anspelov.net server]# cd /vagrant/provision/server
[root@server anspelov.net server]# touch netlog.sh
[root@server anspelov.net server]# chmod +x netlog.sh
[root@server anspelov.net server]#
```

Рис. 2.12: Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.13).

```

netlog.sh      [-M--] 25 L:[ 1+ 9 10/ 10] *(300 / 300b) <EOF>
#!/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. 2.13: Открытие файла на редактирование и добавление в него скрипта.

На виртуальной машине client перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём каталог nentlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh(рис. 2.14).

```

[root@client.an spelov.net rsyslog.d]# cd /vagrant/provision/client
[root@client.an spelov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.an spelov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.an spelov.net client]# mcedit netlog.sh
[root@client.an spelov.net client]# cd /vagrant/provision/client
[root@client.an spelov.net client]# touch netlog.sh
[root@client.an spelov.net client]# chmod +x netlog.sh
[root@client.an spelov.net client]#

```

Рис. 2.14: Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.15).

```
netlog.sh      [-M--] 25 L:[ 1+ 8  9/  9] *(249 / 249b) <EOF>
#!/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. 2.15: Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавим в соответствующих разделах конфигураций для сервера и клиента (рис. 2.16).

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

end

## Client configuration
config.vm.define "client", autostart: false do |client|
  client.vm.box = "rockylinux10"
  client.vm.hostname = 'client'

  client.vm.boot_timeout = 1440

  client.ssh.insert_key = false
  client.ssh.username = 'vagrant'
  client.ssh.password = 'vagrant'

  client.vm.network :private_network,
    ip: "192.168.1.2",
    virtualbox__intnet: true

  client.vm.provider :virtualbox do |virtualbox|
    virtualbox.customize ["modifyvm", :id, "--vrde", "on"]
    virtualbox.customize ["modifyvm", :id, "--vrdeport", "3392"]
  end

  client.vm.provision "client dummy",
    type: "shell",
    preserve_order: true,
    path: "provision/client/01-dummy.sh"

  client.vm.provision "client routing",
    type: "shell",
    preserve_order: true,
    run: "always",
    path: "provision/client/01-routing.sh"

  client.vm.provision "client routing",
    type: "shell",
    preserve_order: true,
    run: "always",
    path: "provision/client/01-routing.sh"

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

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

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

  client.vm.provision "SMB client",
    type: "shell",
    preserve_order: true,
    path: "provision/client/smb.sh"

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

Рис. 2.16: Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.

3 Выводы

В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.

4 Ответы на контрольные вопросы:

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald? - Для приёма сообщений от journald в rsyslog используется модуль imjournal.
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog? - Устаревший модуль для приема сообщений журнала в rsyslog - imuxsock (или imuxsock_legacy).
3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать? - Для предотвращения использования устаревшего метода можно использовать параметр SystemMaxUseForward=no в файле /etc/systemd/journald.conf.
4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала? - Настройки, позволяющие настроить работу журнала, содержатся в файле /etc/systemd/journald.conf.
5. Каким параметром управляет пересылка сообщений из journald в rsyslog? - Для управления пересылкой сообщений из journald в rsyslog используется параметр ForwardToSyslog=yes в файле /etc/systemd/journald.conf.
6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog? - Для включения сообщений из файла журнала, не созданного rsyslog, используется модуль imfile.

7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB? - Для пересылки сообщений в базу данных MariaDB используется модуль ommysql или ommysqlps.
8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP? - Добавьте следующие строки в rsyslog.conf: \$ModLoad imtcp \$InputTCPServerRun 514
9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514? – Используйте команды для открытия порта: sudo firewall-cmd –permanent –add-port=514/tcp sudo firewall-cmd –reload Или: sudo iptables -A INPUT -p tcp –dport 514 -j ACCEPT sudo service iptables save sudo service iptables restart

Список литературы