

Отчет по лабораторной работе № 3. Настройка DHCP-сервера

Данила Стариков
НПИбд-02-22

2024

Содержание

1	Цель работы	3
2	Выполнение работы	4
2.1	Установка DHCP-сервера	4
2.2	Конфигурирование DHCP-сервера	4
2.3	Анализ работы DHCP-сервера	8
2.4	Настройка обновления DNS-зоны	10
2.5	Внесение изменений в настройки внутреннего окружения виртуальной машины	12
3	Выводы	13

1 Цель работы

Приобретение практических навыков по установке и конфигурированию DHCP-сервера.

2 Выполнение работы

2.1 Установка DHCP-сервера

1. Запустили виртуальную машину server:

```
make server-up
```

2. На виртуальной машине server вошли под своим пользователем и открыли терминал. Перешли в режим суперпользователя:

```
sudo -i
```

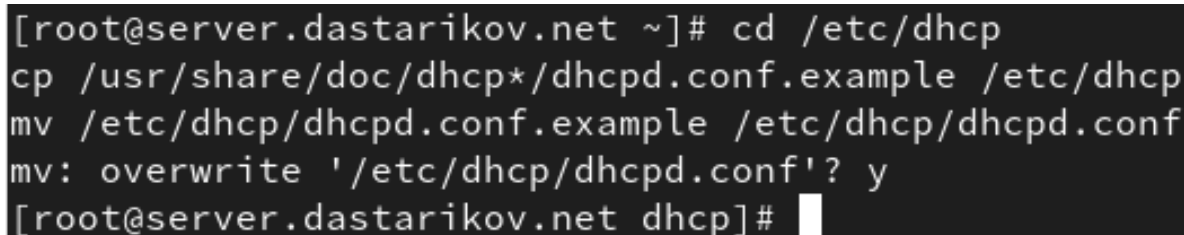
3. Установили dhcp:

```
dnf -y install dhcp-server
```

2.2 Конфигурирование DHCP-сервера

1. Скопировали файл примера конфигурации DHCP `dhcpd.conf.example` из каталога `/usr/share/doc/dhcp*` в каталог `/etc/dhcp` и переименовали его в файл с названием `dhcpd.conf` (Рис. 1):

```
cd /etc/dhcp
cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp
mv /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf
```



```
[root@server.dastarikov.net ~]# cd /etc/dhcp
cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp
mv /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf
mv: overwrite '/etc/dhcp/dhcpd.conf'? y
[root@server.dastarikov.net dhcp]#
```

Рис. 1: Подготовка файла конфигурации.

2. Открыли файл `/etc/dhcp/dhcpd.conf` на редактирование. В этом файле:

- Заменяли строку
`option domain-name "example.org";`
на строку
`option domain-name "dastarikov.net";`
- Заменяли строку
`option domain-name-servers ns1.example.org, ns2.example.org;`
на строку
`option domain-name-servers ns.dastarikov.net;`

- Раскомментировали строку authoritative;
- На базе одного из приведённых в файле примеров конфигурирования подсети задали собственную конфигурацию dhcp-сети, задав адрес подсети, диапазон адресов для распределения клиентам, адрес маршрутизатора и broadcast-адрес:


```
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.30 192.168.1.199;
option routers 192.168.1.1;
option broadcast-address 192.168.1.255;
}
```

Остальные примеры задания конфигураций подсетей удалили.

3. Настроили привязку dhcpd к интерфейсу eth1 виртуальной машины server. Для этого скопировали файл dhcpd.service из каталога /lib/systemd/system в каталог /etc/systemd/system (Рис. 2):

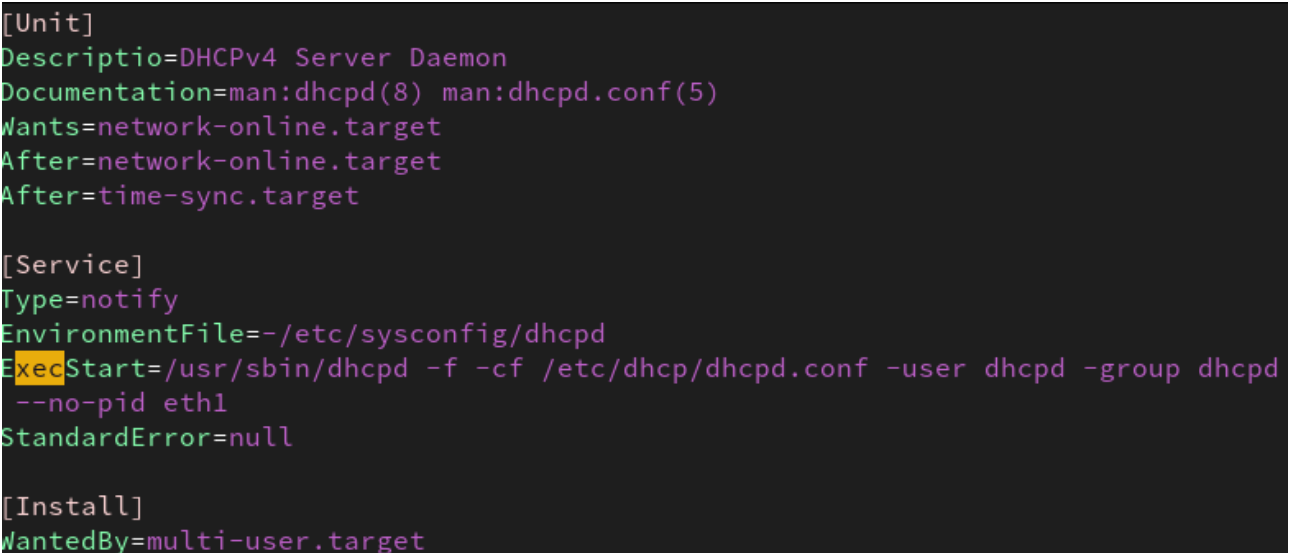
```
cp /lib/systemd/system/dhcpd.service /etc/systemd/system/
```

Открыли файл /etc/systemd/system/dhcpd.service на редактирование и заменили в нём строку

```
ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group
↪ dhcpd --no-pid
```

на строку

```
ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group
↪ dhcpd --no-pid eth1
```



```
[Unit]
Description=DHCPv4 Server Daemon
Documentation=man:dhcpd(8) man:dhcpd.conf(5)
Wants=network-online.target
After=network-online.target
After=time-sync.target

[Service]
Type=notify
EnvironmentFile=-/etc/sysconfig/dhcpd
ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd
--no-pid eth1
StandardError=null

[Install]
WantedBy=multi-user.target
```

Рис. 2: Настройка dhcpd.

Перезагрузили конфигурацию dhcpd и разрешили загрузку DHCP-сервера при запуске виртуальной машины server (Рис. 3):

```
systemctl --system daemon-reload
systemctl enable dhcpd
```

```
[root@server.dastarikov.net dhcp]# systemctl --system daemon-reload
systemctl enable dhcpd
Created symlink /etc/systemd/system/multi-user.target.wants/dhcpd.service → /etc/systemd/system/dhcpd.service.
[root@server.dastarikov.net dhcp]#
```

Рис. 3: Перезагрузка демона dhcpd.

4. Добавили запись для DHCP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/dastarikov.net (Рис. 4):

dhcp A 192.168.1.1

```
$TTL 1D
@           IN SOA  @ server.dastarikov.net (
                                2024101901 ; serial
                                1D         ; refresh
                                1H         ; retry
                                1W         ; expire
                                3H )       ; minimum
           NS      @
           A       192.168.1.1
$ORIGIN dastarikov.net.
server A 192.168.1.1
ns     A 192.168.1.1
dhcp   A 192.168.1.1
```

Рис. 4: Изменение файла прямой DNS-зоны.

и в конце файла обратной зоны /var/named/master/rz/192.168.1 (Рис. 5):

1 PTR dhcp.dastarikov.net.

```
$TTL 1D
@           IN SOA  @ server.dastarikov.net. (
                                2024101901 ; serial
                                1D         ; refresh
                                1H         ; retry
                                1W         ; expire
                                3H )       ; minimum
           NS      @
           A       192.168.1.1
           PTR     server.dastarikov.net
$ORIGIN 1.168.192.in-addr.arpa.
1       PTR     server.dastarikov.net.
1       PTR     ns.dastarikov.net.
1       PTR     dhcp.dastarikov.net.
```

Рис. 5: Изменение файла обратной DNS-зоны.

5. Перезапустили named:

```
systemctl restart named
```

6. Проверили, что можно обратиться к DHCP-серверу по имени (Рис. 6):

```
ping dhcp.dastarikov.net
```

```
[root@server.dastarikov.net dhcp]# systemctl restart named
[root@server.dastarikov.net dhcp]# ping dhcp.dastarikov.net
PING dhcp.dastarikov.net (192.168.1.1) 56(84) bytes of data.
64 bytes from ns.dastarikov.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from dhcp.dastarikov.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from server.dastarikov.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.126 ms
64 bytes from server.dastarikov.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.129 ms
^C
--- dhcp.dastarikov.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3101ms
rtt min/avg/max/mdev = 0.045/0.096/0.129/0.034 ms
```

Рис. 6: Обращение к DHCP-серверу.

7. Внесли изменения в настройки межсетевого экрана узла server, разрешив работу с DHCP (Рис. 7):

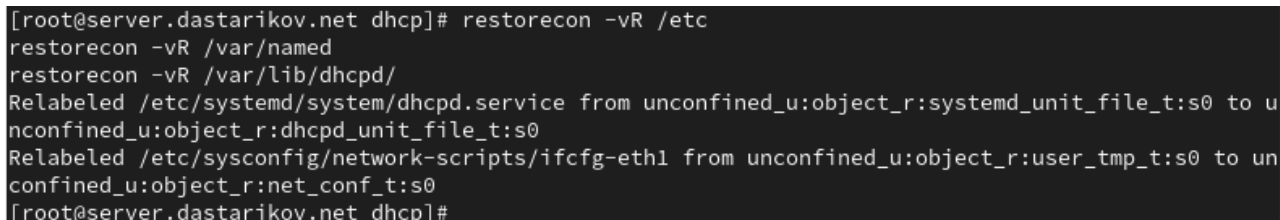
```
firewall-cmd --list-services
firewall-cmd --get-services
firewall-cmd --add-service=dhcp
firewall-cmd --add-service=dhcp --permanent
```

```
[root@server.dastarikov.net dhcp]# firewall-cmd --list-services
firewall-cmd --get-services
firewall-cmd --add-service=dhcp
firewall-cmd --add-service=dhcp --permanent
cockpit dhcpv6-client dns ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registrator docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mongodb-exporter mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap nmap-0183 ntp ntpd nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client unpn-client vds vnc-server warpinator wbem-http wbm https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
success
success
```

Рис. 7: Настройка межсетевого экрана для работы с DHCP.

8. Восстановили контекст безопасности в SELinux (Рис. 8):

```
restorecon -vR /etc
restorecon -vR /var/named
restorecon -vR /var/lib/dhcpd/
```



```
[root@server.dastarikov.net dhcp]# restorecon -vR /etc
restorecon -vR /var/named
restorecon -vR /var/lib/dhcpd/
Relabeled /etc/systemd/system/dhcpd.service from unconfined_u:object_r:systemd_unit_file_t:s0 to u
nconfined_u:object_r:dhcpd_unit_file_t:s0
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to un
confined_u:object_r:net_conf_t:s0
[root@server.dastarikov.net dhcp]#
```

Рис. 8: Восстановление контекста безопасности SELinux.

9. В дополнительном терминале запустили мониторинг происходящих в системе процессов в реальном времени:

```
tail -f /var/log/messages
```
10. В основном рабочем терминале запустили DHCP-сервер:

```
systemctl start dhcpd
```

2.3 Анализ работы DHCP-сервера

1. Перед запуском виртуальной машины client в каталоге с проектом в основной операционной системе в подкаталоге vagrant/provision/client создали файл 01- routing.sh:

```
cd /home/tmp/dastarikov/vagrant/provision/client
touch 01-routing.sh
chmod +x 01-routing.sh
```

Открыв его на редактирование, прописали в нём следующий скрипт:

```
#!/bin/bash
echo "Provisioning script $0"
nmcli connection modify "System eth1" ipv4.gateway "192.168.1.1"
nmcli connection up "System eth1"
nmcli connection modify eth0 ipv4.never-default true
nmcli connection modify eth0 ipv6.never-default true
nmcli connection down eth0
nmcli connection up eth0
# systemctl restart NetworkManager
```

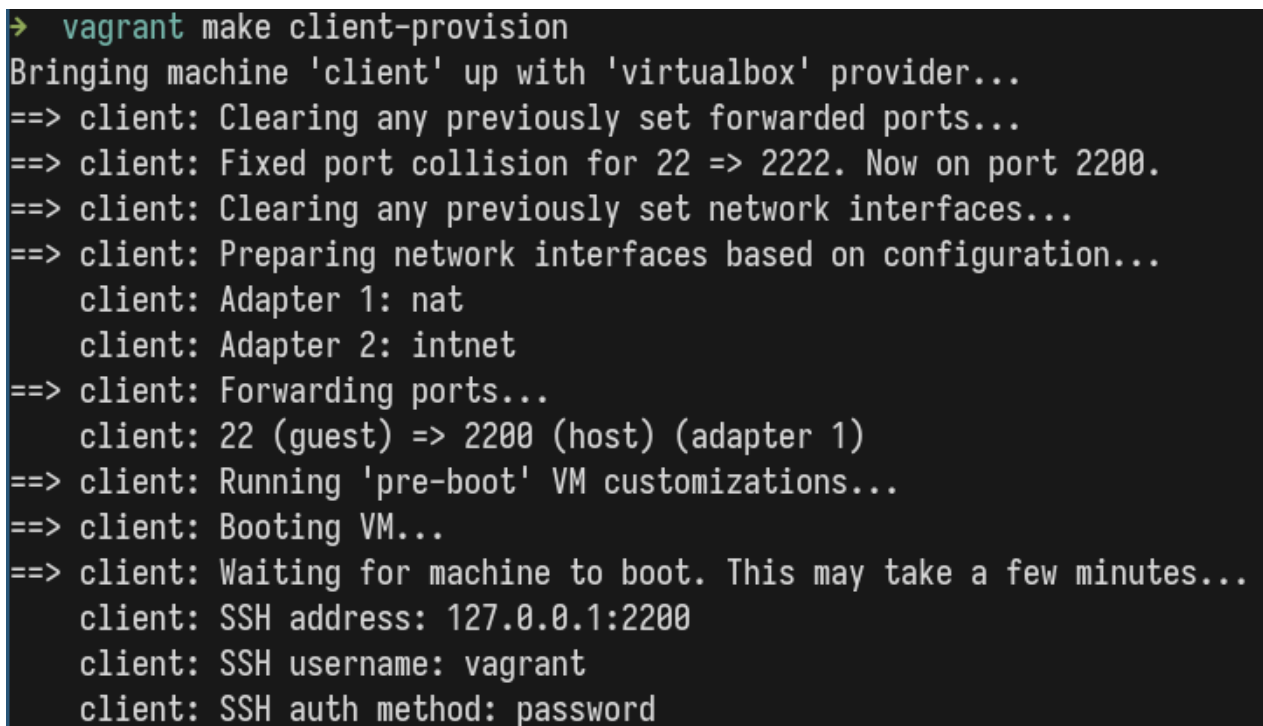
Этот скрипт изменяет настройки NetworkManager так, чтобы весь трафик на виртуальной машине client шёл по умолчанию через интерфейс eth1.

2. В Vagrantfile подключили этот скрипт в разделе конфигурации для клиента:


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

3. Зафиксировали внесённые изменения для внутренних настроек виртуальной машины client и запустите её, введя в терминале (Рис. 9):

```
make client-provision
```



```
> vagrant make client-provision  
Bringing machine 'client' up with 'virtualbox' provider...  
==> client: Clearing any previously set forwarded ports...  
==> client: Fixed port collision for 22 => 2222. Now on port 2200.  
==> client: Clearing any previously set network interfaces...  
==> client: Preparing network interfaces based on configuration...  
      client: Adapter 1: nat  
      client: Adapter 2: intnet  
==> client: Forwarding ports...  
      client: 22 (guest) => 2200 (host) (adapter 1)  
==> client: Running 'pre-boot' VM customizations...  
==> client: Booting VM...  
==> client: Waiting for machine to boot. This may take a few minutes...  
      client: SSH address: 127.0.0.1:2200  
      client: SSH username: vagrant  
      client: SSH auth method: password
```

Рис. 9: Фиксирование внесенных изменений и запуск виртуальной машины client.

4. После загрузки виртуальной машины client увидели на виртуальной машине server на терминале с мониторингом происходящих в системе процессов записи о подключении к виртуальной внутренней сети узла client и выдачи ему IP-адреса из соответствующего диапазона адресов. Также информацию о работе DHCP-сервера можно наблюдать в файле `/var/lib/dhcpd/dhcpd.leases`. В отчёте прокомментируйте построчно информацию из этого файла.
5. Вошли в систему виртуальной машины client под своим пользователем и открыли терминал. В терминале ввели (Рис. 10)

```
ifconfig
```

```
[dastarikov@client.dastarikov.net ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe4c:cc9c  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:4c:cc:9c  txqueuelen 1000  (Ethernet)
    RX packets 1592  bytes 178414 (174.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 1474  bytes 226540 (221.2 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.30  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe16:c3e7  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:16:c3:e7  txqueuelen 1000  (Ethernet)
    RX packets 17  bytes 2944 (2.8 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 166  bytes 21528 (21.0 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 19  bytes 2146 (2.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 19  bytes 2146 (2.0 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 10: Вывод информации об имеющихся интерфейсах.

2.4 Настройка обновления DNS-зоны

Требуется настроить обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов.

1. На виртуальной машине server под пользователем с правами суперпользователя отредактировали файл `/etc/named/dastarikov.net`, разрешив обновление зоны с локального адреса, т.е. заменив в этом файле в строке `allow-update` слово `none` на `127.0.0.1` (Рис. 11):

```
zone "dastarikov.net" IN {
    type master;
    file "master/fz/dastarikov.net";
    allow-update { 127.0.0.1; };
};
zone "1.168.192.in-addr.arpa" IN {
    type master;
```

```
file "master/rz/192.168.1";  
allow-update { 127.0.0.1; };  
};
```

```
zone "dastarikov.net" IN {  
    type master;  
    file "master/fz/dastarikov.net";  
    allow-update { 127.0.0.1; };  
};  
  
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "master/rz/192.168.1";  
    allow-update { 127.0.0.1; };  
};
```

Рис. 11: Обновление файла DNS-зоны на виртуальной машине server.

2. Перезапустили DNS-сервер:

```
systemctl restart named
```

3. Внесли изменения в конфигурационный файл `/etc/dhcp/dhcpd.conf`, добавив в него разрешение на динамическое обновление DNS-записей с локального узла прямой и обратной зон:

```
# Use this to enable / disable dynamic dns updates globally.  
ddns-updates on;  
ddns-update-style interim;  
ddns-domainname "dastarikov.net";  
ddns-rev-domainname "in-addr.arpa";  
zone dastarikov.net. {  
    primary 127.0.0.1;  
}  
zone 1.168.192.in-addr.arpa. {  
    primary 127.0.0.1;  
}
```

4. Перезапустили DHCP-сервер:

```
systemctl restart dhcpd
```

5. Если перезапуск DHCP-сервера прошёл успешно, то в каталоге прямой DNS-зоны /var/named/master/fz должен появиться файл dastarikov.net.jnl, в котором в бинарном файле автоматически вносятся изменения записей зоны (Рис. 12).



```
[root@server.dastarikov.net fz]# ls
dastarikov.net  dastarikov.net.jnl
```

Рис. 12: Проверка создания файла.

2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перешли в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создали в нём каталог dhcp, в который поместите в соответствующие подкаталоги конфигурационные файлы DHCP:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/dhcp/etc/dhcp
mkdir -p /vagrant/provision/server/dhcp/etc/systemd/system
cp -R /etc/dhcp/dhcpd.conf /vagrant/provision/server/dhcp/etc/dhcp/
cp -R /etc/systemd/system/dhcpd.service
↪ /vagrant/provision/server/dhcp/etc/systemd/system/
```

2. Заменяли конфигурационные файлы DNS-сервера:

```
cd /vagrant/provision/server/dns/
cp -R /var/named/* /vagrant/provision/server/dns/var/named/
cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
```

3. В каталоге /vagrant/provision/server создали исполняемый файл dhcp.sh:

```
cd /vagrant/provision/server
touch dhcp.sh
chmod +x dhcp.sh
```

Открыв его на редактирование, прописали в нём следующий скрипт:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install dhcp-server
echo "Copy configuration files"
cp -R /vagrant/provision/server/dhcp/etc/* /etc
chown -R dhcpd:dhcpd /etc/dhcp
restorecon -vR /etc
restorecon -vR /var/lib/dhcpd
```

```
echo "Configure firewall"
firewall-cmd --add-service=dhcp
firewall-cmd --add-service=dhcp --permanent
echo "Start dhcpd service"
systemctl --system daemon-reload
systemctl enable dhcpd
systemctl start dhcpd
```

4. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавили в разделе конфигурации для сервера:

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

5. После этого виртуальные машины client и server можно выключить.

3 Выводы

В результате выполнения лабораторной работы приобрели практические навыки по установке и конфигурированию DHCP-сервера.