# Лабораторная работа №2

## Тема «Настройка DNS-сервера»

по дисциплине «Администрирование сетевых подсистем»

Выполнил:  Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«11» ноября 2023г.

**Цель работы:**

Приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

**Задание**

1. Установить на виртуальной машине server DNS-сервер bind и bind-utils.
2. Сконфигурировать на виртуальной машине server кэширующий DNS-сервер.
3. Сконфигурировать на виртуальной машине server первичный DNS-сервер.
4. При помощи утилит dig и host проанализировать работу DNS-сервера.
5. Написать скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внести изменения в Vagrantfile.

# Выполнение работы

## Установка DNS-сервера

Вывод информации о домене www.yandex.ru



**Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами**
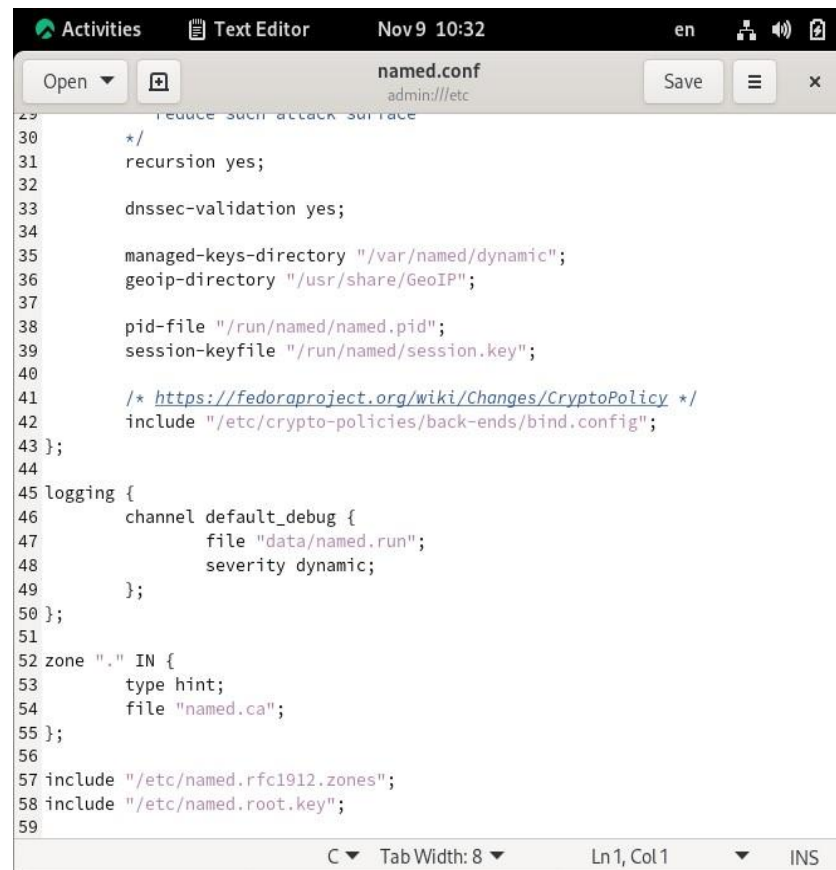
Содержимое файла /etc/named.conf



```
1  //
2  // named.conf
3  //
4  // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5  // server as a caching only nameserver (as a localhost DNS resolver only).
6  //
7  // See /usr/share/doc/bind*/sample/ for example named configuration files.
8  //
9
10 options {
11         listen-on port 53 { 127.0.0.1; };
12         listen-on-v6 port 53 { ::1; };
13         directory       "/var/named";
14         dump-file       "/var/named/data/cache_dump.db";
15         statistics-file "/var/named/data/named_stats.txt";
16         memstatistics-file "/var/named/data/named_mem_stats.txt";
17         secroots-file   "/var/named/data/named.secroots";
18         recursing-file  "/var/named/data/named.recursing";
19         allow-query     { localhost; };
20
21         /*
22            - If you are building an AUTHORITATIVE DNS server, do NOT enable
   recursion.
23            - If you are building a RECURSIVE (caching) DNS server, you need to
   enable
24              recursion.
25            - If your recursive DNS server has a public IP address, you MUST
   enable access
26              control to limit queries to your legitimate users. Failing to do so
   will
```

```
29     reduce such attack surface
30        */
31        recursion yes;
32
33        dnssec-validation yes;
34
35        managed-keys-directory "/var/named/dynamic";
36        geoip-directory "/usr/share/GeoIP";
37
38        pid-file "/run/named/named.pid";
39        session-keyfile "/run/named/session.key";
40
41        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
42        include "/etc/crypto-policies/back-ends/bind.config";
43 };
44
45 logging {
46        channel default_debug {
47                file "data/named.run";
48                severity dynamic;
49        };
50 };
51
52 zone "." IN {
53        type hint;
54        file "named.ca";
55 };
56
57 include "/etc/named.rfc1912.zones";
58 include "/etc/named.root.key";
59
```

# Содержимое файла /var/named/named.ca

```
                              named.ca
Open ▼  ⊞                  admin:///var/named              Save   ≡   ✕

 1
 2 ; <<>> DiG 9.11.3-RedHat-9.11.3-3.fc27 <<>> +bufsize=1200 +norec @a.root-
   servers.net
 3 ; (2 servers found)
 4 ;; global options: +cmd
 5 ;; Got answer:
 6 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46900
 7 ;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
 8
 9 ;; OPT PSEUDOSECTION:
10 ; EDNS: version: 0, flags:; udp: 1472
11 ;; QUESTION SECTION:
12 ;.                         IN      NS
13
14 ;; ANSWER SECTION:
15 .                  518400  IN      NS       a.root-servers.net.
16 .                  518400  IN      NS       b.root-servers.net.
17 .                  518400  IN      NS       c.root-servers.net.
18 .                  518400  IN      NS       d.root-servers.net.
19 .                  518400  IN      NS       e.root-servers.net.
20 .                  518400  IN      NS       f.root-servers.net.
21 .                  518400  IN      NS       g.root-servers.net.
22 .                  518400  IN      NS       h.root-servers.net.
23 .                  518400  IN      NS       i.root-servers.net.
24 .                  518400  IN      NS       j.root-servers.net.
25 .                  518400  IN      NS       k.root-servers.net.
26 .                  518400  IN      NS       l.root-servers.net.
27 .                  518400  IN      NS       m.root-servers.net.
28
29 ;; ADDITIONAL SECTION:

        Plain Text ▼   Tab Width: 8 ▼        Ln 1, Col 1      ▼   INS
```

# Содержимое файлов /var/named/named.localhost и /var/named/named.loopback

```
[root@server.mrshcherbak.net ~]# cat /var/named/named.localhost
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
[root@server.mrshcherbak.net ~]# cat /var/named/named.loopback
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
        PTR     localhost.
[root@server.mrshcherbak.net ~]# 
```

```
[root@server.mrshcherbak.net ~]# systemctl start named
[root@server.mrshcherbak.net ~]# systemctl enable named
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr
/lib/systemd/system/named.service.
[root@server.mrshcherbak.net ~]# dig www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33200
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       77.88.55.88
www.yandex.ru.          3600    IN      A       77.88.55.60
www.yandex.ru.          3600    IN      A       5.255.255.70
www.yandex.ru.          3600    IN      A       5.255.255.77

;; Query time: 35 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Thu Nov 09 10:38:00 UTC 2023
;; MSG SIZE  rcvd: 95
```

```
[root@server.mrshcherbak.net ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44037
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 86c6112a12ca3da901000000654cb6a8eba814ea90ddb157 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          300     IN      A       5.255.255.70
www.yandex.ru.          300     IN      A       77.88.55.60
www.yandex.ru.          300     IN      A       5.255.255.77
www.yandex.ru.          300     IN      A       77.88.55.88

;; Query time: 1850 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 09 10:38:32 UTC 2023
;; MSG SIZE  rcvd: 134

[root@server.mrshcherbak.net ~]#
```

Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети

```
[root@server.mrshcherbak.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-
1x, dcb, sriov, ethtool, match, ipv4, ipv6, hostname, tc, proxy
nmcli> ^C
nmcli> ^C
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (50b01577-8896-4337-a2ee-c1c35717f76d) successfully updated.
nmcli> quit
[root@server.mrshcherbak.net ~]# 
```

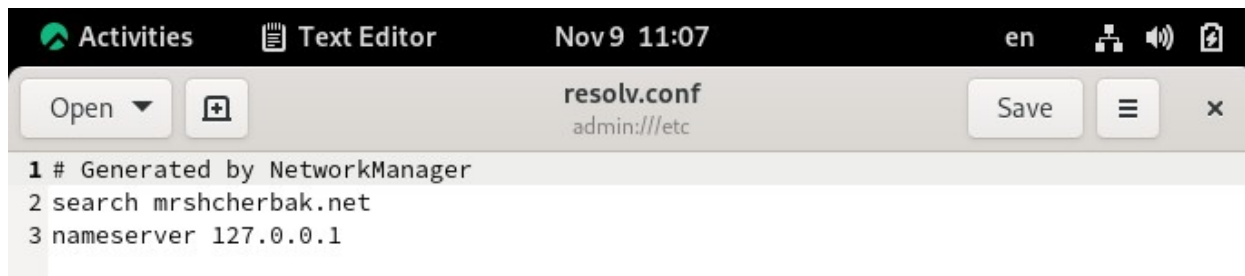то же самое для соединения System eth0

```
[root@server.mrshcherbak.net ~]# nmcli connection edit System\ eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'System eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-
1x, dcb, sriov, ethtool, match, ipv4, ipv6, hostname, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully upd
ated.
nmcli> quit
[root@server.mrshcherbak.net ~]# 
```
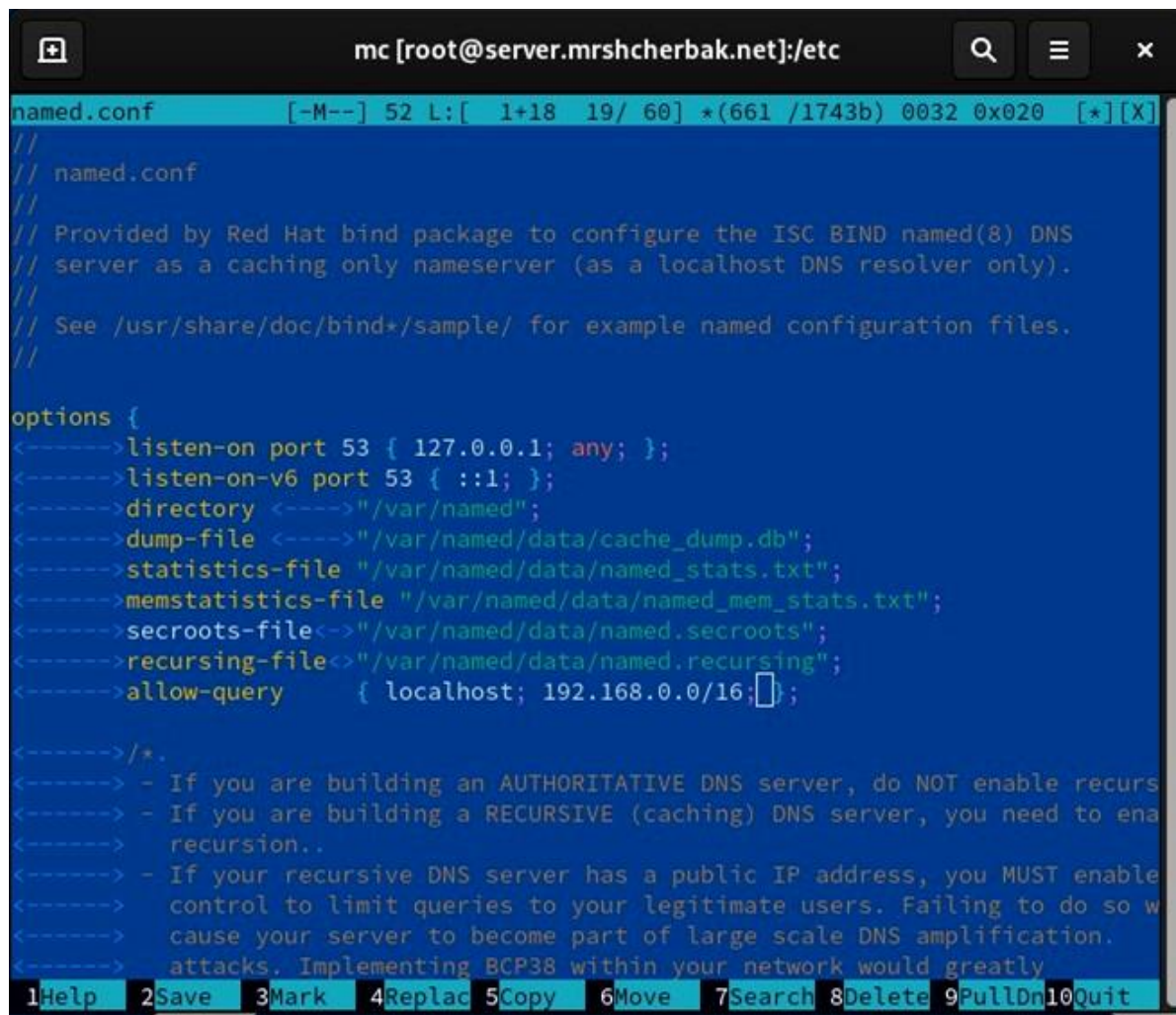
Open ▼    ⊞        **resolv.conf**         Save    ≡    ×
                   admin:///etc

```
1 # Generated by NetworkManager
2 search mrshcherbak.net
3 nameserver 127.0.0.1
```

Редактирование файла
/etc/named.conf



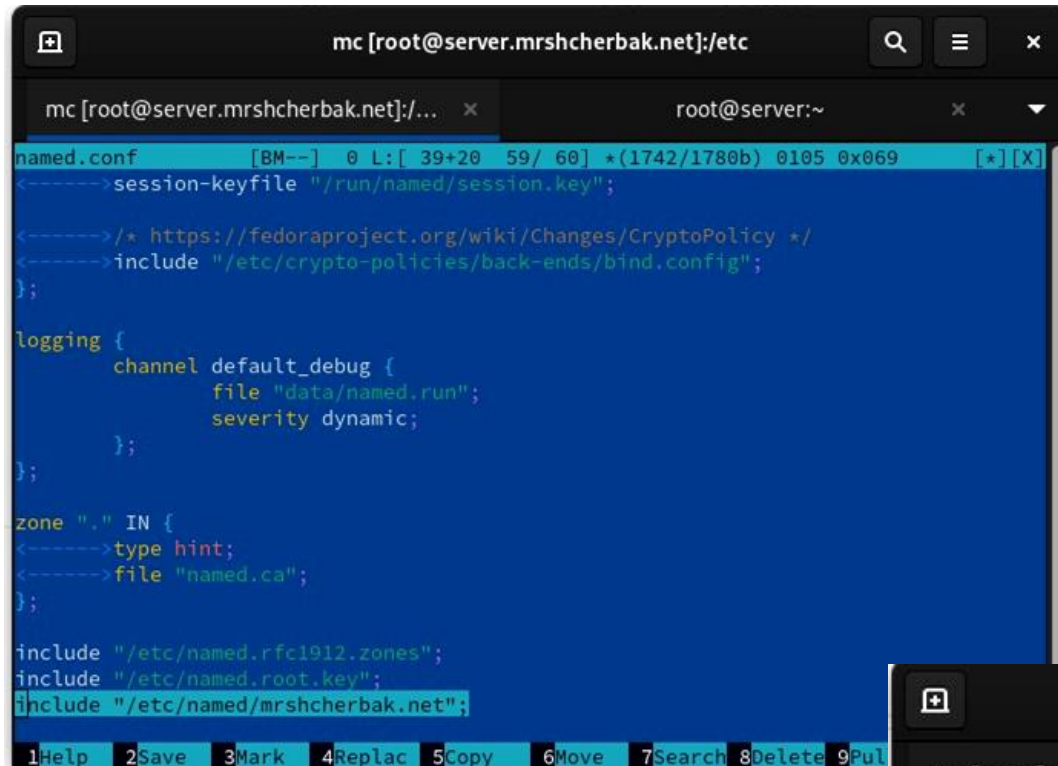mc [root@server.mrshcherbak.net]:/etc                Q    ≡    ×

```
named.conf          [-M--] 52 L:[  1+18   19/ 60] *(661 /1743b) 0032 0x020    [*][X]
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
<------->listen-on port 53 { 127.0.0.1; any; };
<------->listen-on-v6 port 53 { ::1; };
<------->directory <---->"/var/named";
<------->dump-file <---->"/var/named/data/cache_dump.db";
<------->statistics-file "/var/named/data/named_stats.txt";
<------->memstatistics-file "/var/named/data/named_mem_stats.txt";
<------->secroots-file<->"/var/named/data/named.secroots";
<------->recursing-file<>"/var/named/data/named.recursing";
<------->allow-query       { localhost; 192.168.0.0/16;□};

<------>/*.
<------> - If you are building an AUTHORITATIVE DNS server, do NOT enable recurs
<------> - If you are building a RECURSIVE (caching) DNS server, you need to ena
<------>   recursion..
<------> - If your recursive DNS server has a public IP address, you MUST enable
<------>   control to limit queries to your legitimate users. Failing to do so w
<------>   cause your server to become part of large scale DNS amplification.
<------>   attacks. Implementing BCP38 within your network would greatly
1Help    2Save    3Mark    4Replac 5Copy    6Move    7Search 8Delete 9PullDn10Quit
```

```
[root@server.mrshcherbak.net ~]# firewall-cmd --add-service=dns
success
[root@server.mrshcherbak.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.mrshcherbak.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
avahi-dae   563                             avahi   12u    IPv4              18829
      0t0          UDP *:mdns
avahi-dae   563                             avahi   13u    IPv6              18830
      0t0          UDP *:mdns
avahi-dae   563                             avahi   14u    IPv4              18831
      0t0          UDP *:40338
avahi-dae   563                             avahi   15u    IPv6              18832
      0t0          UDP *:51103
chronyd     588                             chrony   5u    IPv4              18707
      0t0          UDP localhost:323
chronyd     588                             chrony   6u    IPv6              18708
      0t0          UDP localhost:323
chronyd     588                             chrony   8u    sock               0,8
      0t0      195417 protocol: UDP
named     12200                             named   16u    IPv4             208942
      0t0          UDP localhost:domain
named     12200                             named   19u    IPv6             208944
      0t0          UDP localhost:domain
named     12200 12201 isc-net-0            named   16u    IPv4             208942
      0t0          UDP localhost:domain
named     12200 12201 isc-net-0            named   19u    IPv6             208944
      0t0          UDP localhost:domain
named     12200 12202 isc-timer            named   16u    IPv4             208942
```

**Конфигурирование первичного DNS-сервера**



```
[root@server.mrshcherbak.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.mrshcherbak.net ~]# cd /etc/named
[root@server.mrshcherbak.net named]# mv /etc/named/named.rfc1912.zones /etc/named/mrshcherbak.net
```

Редактирование файла /etc/named.conf



```
named.conf          [BM--]  0 L:[ 39+20  59/ 60] *(1742/1780b) 0105 0x069      [*][X]
------->session-keyfile "/run/named/session.key";

------->/* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
------->include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
------->type hint;
------->file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/mrshcherbak.net";
```
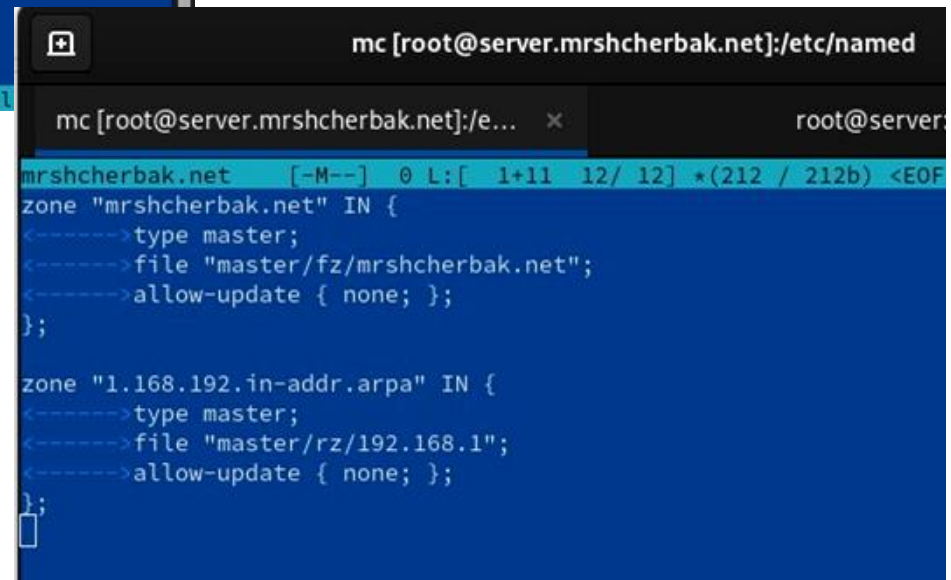
1Help  2Save  3Mark  4Replac  5Copy  6Move  7Search 8Delete 9Pul

Редактирование файла /etc/named/mrshcherbak.net
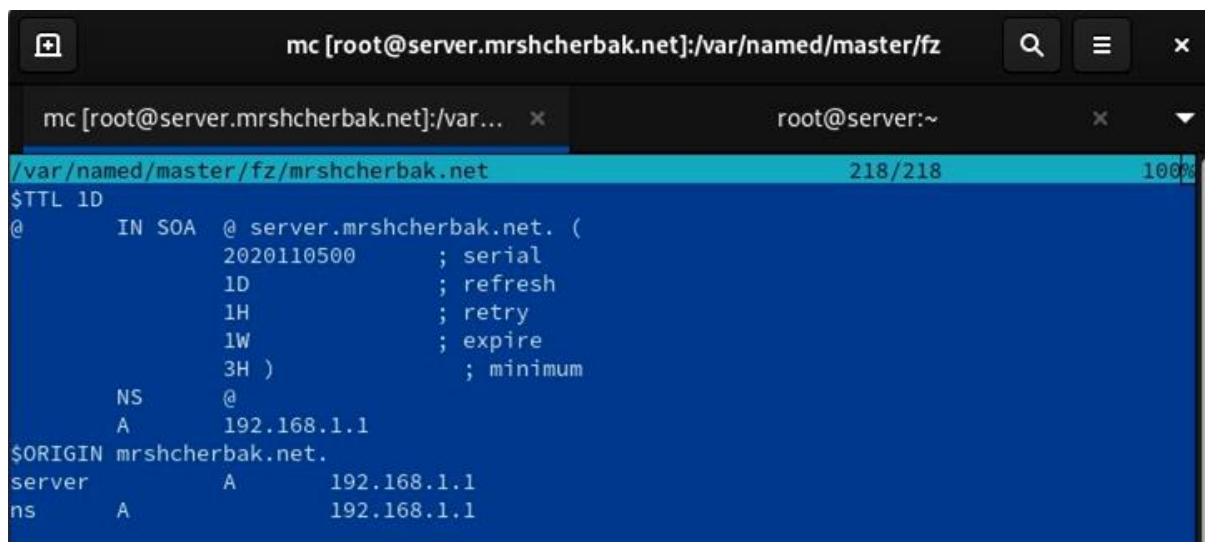


```
mrshcherbak.net     [-M--]  0 L:[  1+11  12/ 12] *(212 / 212b) <EOF
zone "mrshcherbak.net" IN {
------->type master;
------->file "master/fz/mrshcherbak.net";
------->allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
------->type master;
------->file "master/rz/192.168.1";
------->allow-update { none; };
};
```

```
[root@server.mrshcherbak.net ~]# cd /var/named
[root@server.mrshcherbak.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.mrshcherbak.net named]# cd /var/named/master/fz/
[root@server.mrshcherbak.net fz]# mv named.localhost mrshcherbak.net
[root@server.mrshcherbak.net fz]# ▯
```

Редактирование файла /var/named/master/fz/mrshcherbak.net
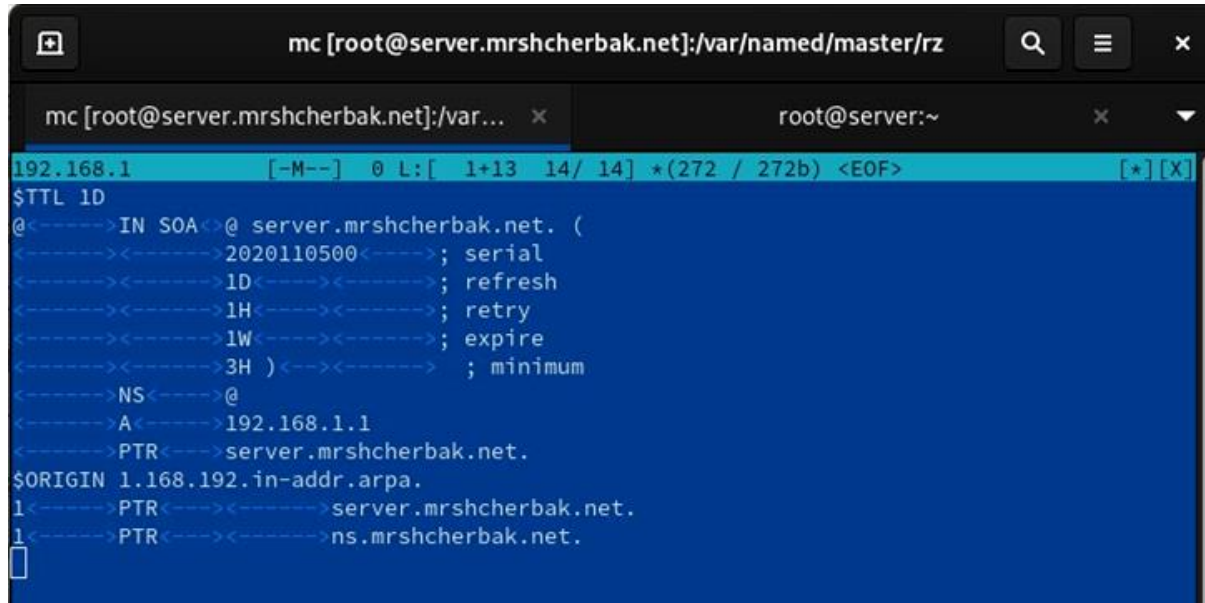
```
┌┴┐            mc [root@server.mrshcherbak.net]:/var/named/master/fz     🔍  ≡   ✕

  mc [root@server.mrshcherbak.net]:/var...  ✕              root@server:~            ✕    ▼
/var/named/master/fz/mrshcherbak.net                          218/218              100%
$TTL 1D
@       IN SOA  @ server.mrshcherbak.net. (
                2020110500      ; serial
                1D              ; refresh
                1H              ; retry
                1W              ; expire
                3H )            ; minimum
        NS      @
        A       192.168.1.1
$ORIGIN mrshcherbak.net.
server          A       192.168.1.1
ns      A               192.168.1.1
```
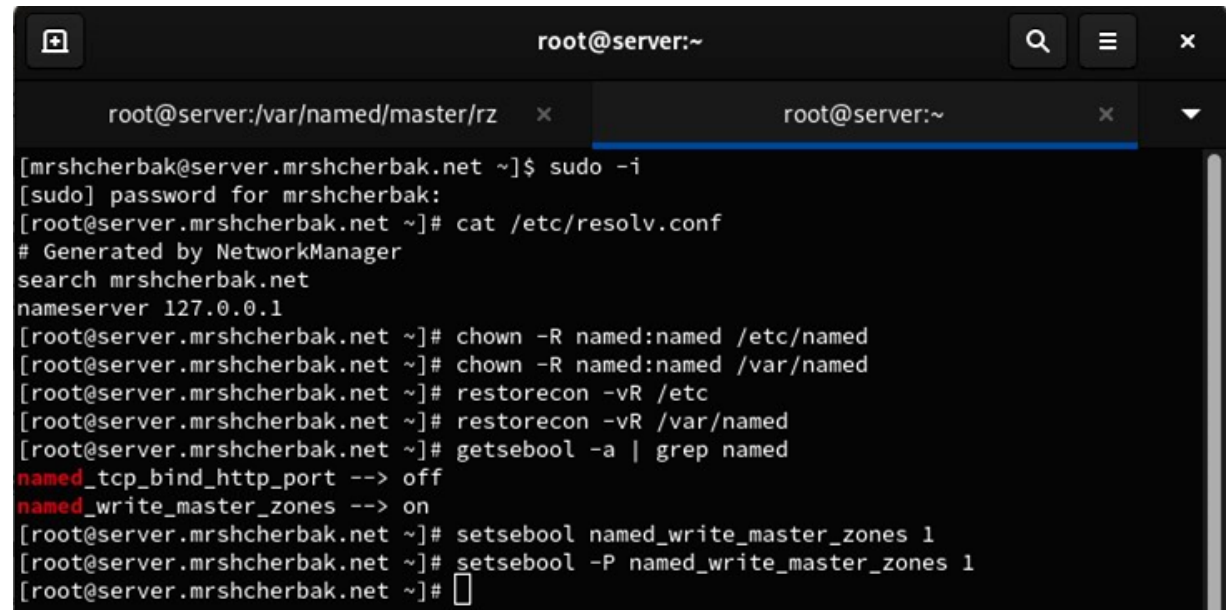
Скопировала шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог
/var/named/master/rz и переименовала его в 192.168.1

```
[root@server.mrshcherbak.net fz]# cp /var/named/named.loopback /var/named/master/rz/
[root@server.mrshcherbak.net fz]# cd /var/named/master/rz/
[root@server.mrshcherbak.net rz]# mv named.loopback 192.168.1
[root@server.mrshcherbak.net rz]# ▯
```

Редактирование файла /var/named/master/rz/192.168.1

Выполнение команды journalctl -x –f



**Анализ работы DNS-сервера**

Описание DNS-зоны с сервера ns.mrshcherbak.net

При помощи утилиты host проанализировала корректность работы DNS-сервера

```
[root@server.mrshcherbak.net ~]# host -l mrshcherbak.net
mrshcherbak.net name server mrshcherbak.net.
mrshcherbak.net has address 192.168.1.1
ns.mrshcherbak.net has address 192.168.1.1
server.mrshcherbak.net has address 192.168.1.1
[root@server.mrshcherbak.net ~]# host -a mrshcherbak.net
Trying "mrshcherbak.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58296
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;mrshcherbak.net.                 IN      ANY

;; ANSWER SECTION:
mrshcherbak.net.         86400    IN      SOA     mrshcherbak.net. server.mrshcherbak.net.
2020110500 86400 3600 604800 10800
mrshcherbak.net.         86400    IN      NS      mrshcherbak.net.
mrshcherbak.net.         86400    IN      A       192.168.1.1

;; ADDITIONAL SECTION:
mrshcherbak.net.         86400    IN      A       192.168.1.1

Received 122 bytes from 127.0.0.1#53 in 25 ms
```
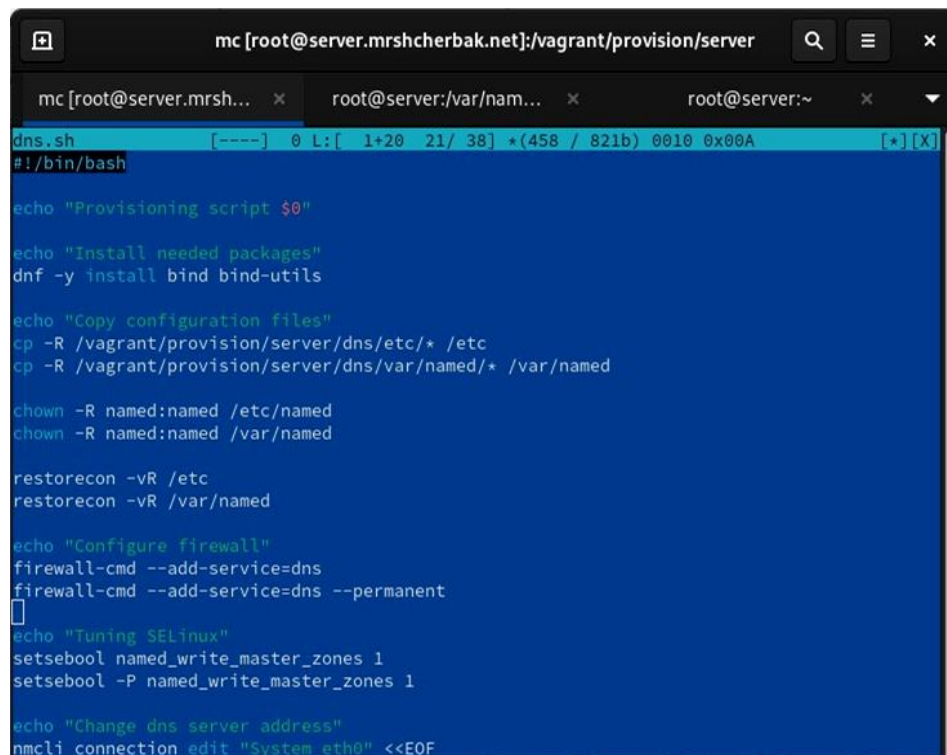
```
[root@server.mrshcherbak.net ~]# host -t A mrshcherbak.net
mrshcherbak.net has address 192.168.1.1
[root@server.mrshcherbak.net ~]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.mrshcherbak.net.
1.1.168.192.in-addr.arpa domain name pointer ns.mrshcherbak.net.
[root@server.mrshcherbak.net ~]# 
```

# Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[root@server.mrshcherbak.net ~]# cd /vagrant
[root@server.mrshcherbak.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.mrshcherbak.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
[root@server.mrshcherbak.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.mrshcherbak.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.mrshcherbak.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.mrshcherbak.net vagrant]#
```

Содержимое файла dns.sh



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server

mc [root@server.mrsh...        root@server:/var/nam...        root@server:~

dns.sh            [----]  0 L:[  1+20  21/ 38] *(458 / 821b) 0010 0x00A        [*][X]
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install bind bind-utils

echo "Copy configuration files"
cp -R /vagrant/provision/server/dns/etc/* /etc
cp -R /vagrant/provision/server/dns/var/named/* /var/named

chown -R named:named /etc/named
chown -R named:named /var/named

restorecon -vR /etc
restorecon -vR /var/named

echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1

echo "Change dns server address"
nmcli connection edit "System eth0" <<EOF
```
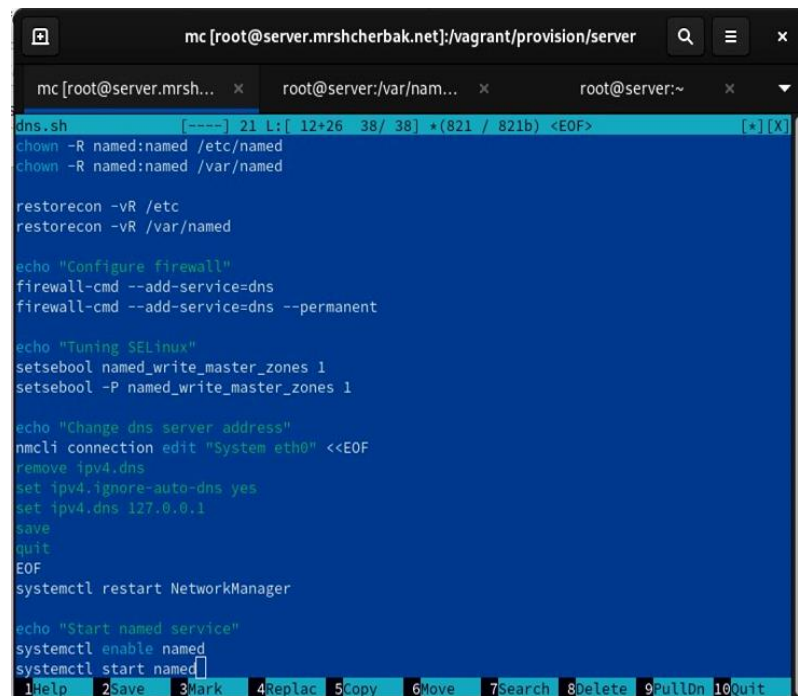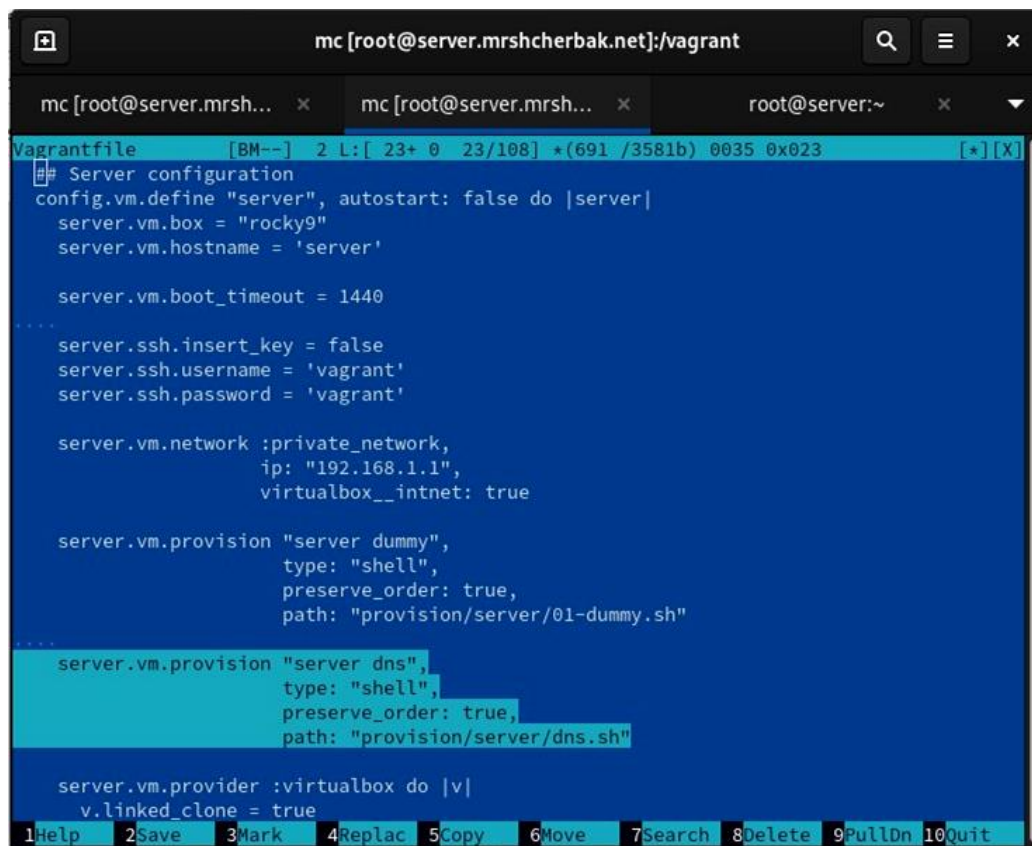
```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server

mc [root@server.mrsh...        root@server:/var/nam...        root@server:~

dns.sh            [----] 21 L:[ 12+26  38/ 38] *(821 / 821b) <EOF>        [*][X]
chown -R named:named /etc/named
chown -R named:named /var/named

restorecon -vR /etc
restorecon -vR /var/named

echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1

echo "Change dns server address"
nmcli connection edit "System eth0" <<EOF
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
EOF
systemctl restart NetworkManager

echo "Start named service"
systemctl enable named
systemctl start named
1Help   2Save   3Mark   4Replac  5Copy   6Move   7Search  8Delete  9PullDn 10Quit
```

Редактирование файла Vagrantfile



**Вывод:** таким образом, в ходе выполнения л/р №2, я приобрела практические навыки по установке и конфигурированию DNS-сервера, усвоила принципы работы системы доменных имён.