

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**  
**ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**  
**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЕТ**  
**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2**

*Дисциплина «Администрирование сетевых подсистем»*

*Тема «Настройка DNS-сервера»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

## Цель работы

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

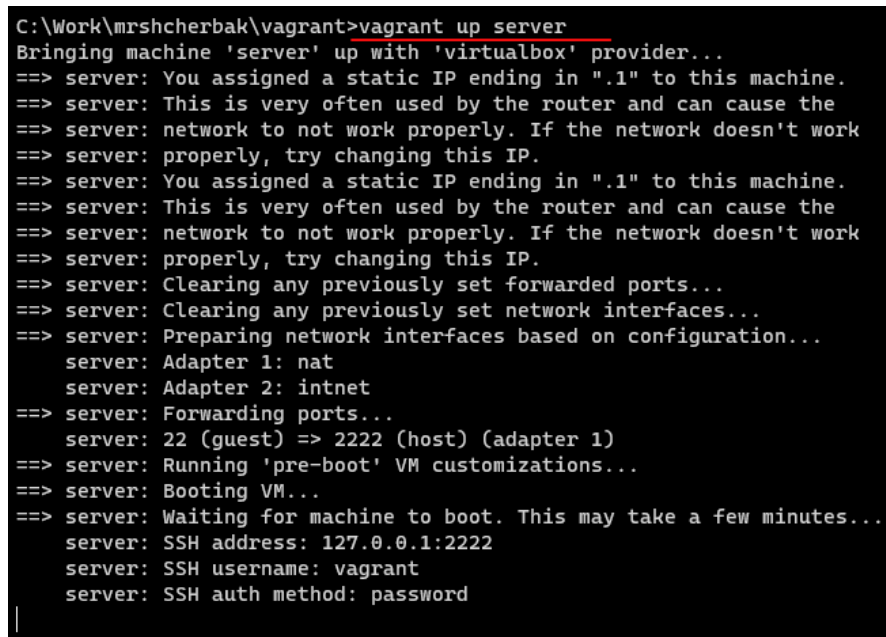
## Задание

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

### 1. Установка DNS-сервера

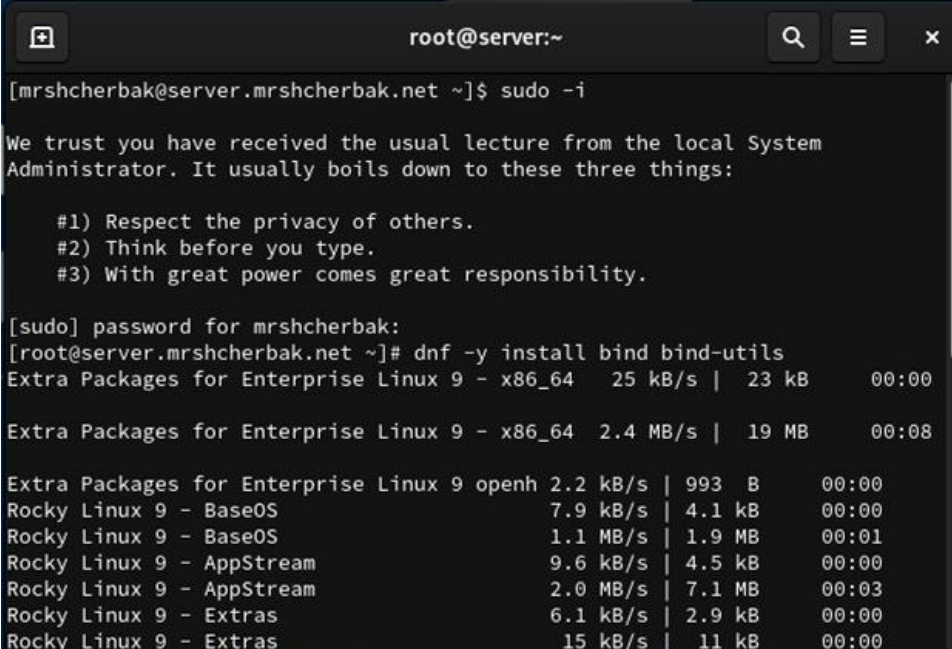
1. Я загрузила свою операционную систему и перешла в рабочий каталог с проектом: `cd /var/tmp/mrshcherbak/vagrant`.
2. Запустила виртуальную машину server (рис.1.1).



```
C:\Work\mrshcherbak\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
server: Adapter 1: nat
server: Adapter 2: intnet
==> server: Forwarding ports...
server: 22 (guest) => 2222 (host) (adapter 1)
==> server: Running 'pre-boot' VM customizations...
==> server: Booting VM...
==> server: Waiting for machine to boot. This may take a few minutes...
server: SSH address: 127.0.0.1:2222
server: SSH username: vagrant
server: SSH auth method: password
```

Рис.1.1. Запуск виртуальной машины Server

3. На виртуальной машине server вошла под созданным в предыдущей работе пользователем и открыла терминал. Перешла в режим суперпользователя: `sudo -i`. Установила bind и bind-utils: `dnf -y install bind bind-utils`. Команды представлены на рис.1.2.



```
root@server:~  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 25 kB/s | 23 kB 00:00  
Extra Packages for Enterprise Linux 9 - x86_64 2.4 MB/s | 19 MB 00:08  
Extra Packages for Enterprise Linux 9 openh 2.2 kB/s | 993 B 00:00  
Rocky Linux 9 - BaseOS 7.9 kB/s | 4.1 kB 00:00  
Rocky Linux 9 - BaseOS 1.1 MB/s | 1.9 MB 00:01  
Rocky Linux 9 - AppStream 9.6 kB/s | 4.5 kB 00:00  
Rocky Linux 9 - AppStream 2.0 MB/s | 7.1 MB 00:03  
Rocky Linux 9 - Extras 6.1 kB/s | 2.9 kB 00:00  
Rocky Linux 9 - Extras 15 kB/s | 11 kB 00:00
```

Рис.1.2. Выполнение команд

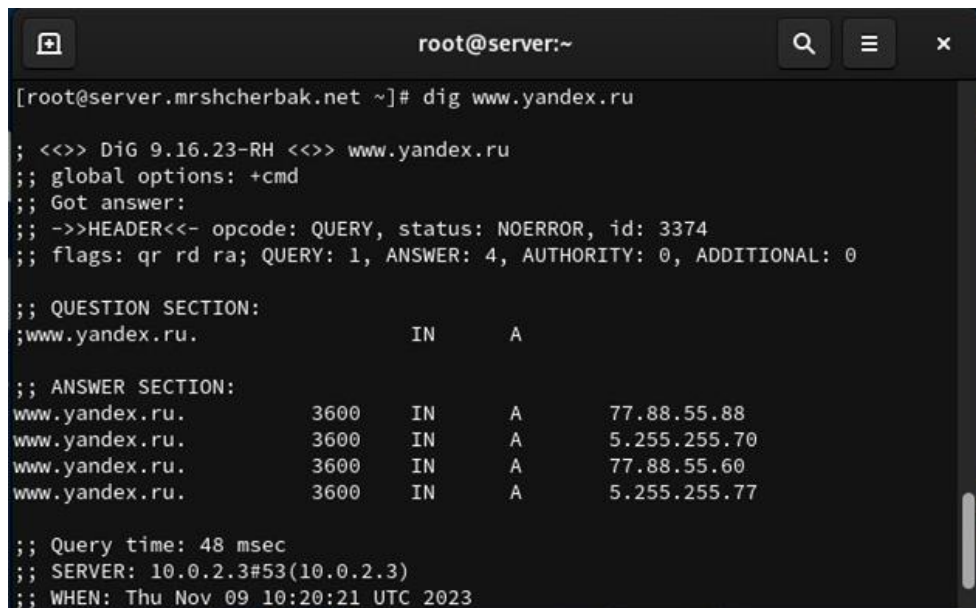
4. В качестве упражнения с помощью утилиты dig сделала запрос к DNS адресу [www.yandex.ru](http://www.yandex.ru) (рис.1.3). Мы можем увидеть A-записи домена [www.yandex.ru](http://www.yandex.ru) в разделе ANSWER SECTION.

HEADER — отображает информацию о версии утилиты, ID запроса, полученных ошибках и использованных флагах вывода. Выводится и другая важная информация о количестве запросов, обращений к DNS-серверу и т. д.;

QUESTION SECTION — секция, которая отображает текущий запрос;

ANSWER SECTION — секция, в которой отображается результат обработки созданного запроса (в данном случае это A-запись для [www.yandex.ru](http://www.yandex.ru)).

Последняя секция это статистика по запросу (служебная информация) - время выполнения запроса, имя DNS-сервера который запрашивался, когда был создан запрос. Получили информацию с сервера 10.0.2.3.



```
root@server:~  
[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: 3374  
;; 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      5.255.255.70  
www.yandex.ru.                3600    IN      A      77.88.55.60  
www.yandex.ru.                3600    IN      A      5.255.255.77  
  
;; Query time: 48 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Thu Nov 09 10:20:21 UTC 2023
```

Рис.1.3. Вывод информации о домене [www.yandex.ru](http://www.yandex.ru)

## 2. Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

1. Проанализировала содержание файлов `/etc/resolv.conf`, `/etc/named.conf`, `/var/named/named.ca`, `/var/named/named.localhost`, `/var/named/named.loopback`.

Файл `/etc/resolv.conf` указывает на использование NetworkManager для управления сетевыми подключениями, домен поиска установлен как `mrshcherbak.net`, и DNS-сервер установлен как `10.0.2.3` (рис.2.1).



```
Activities Text Editor Nov 9 10:25 en  
Open resolv.conf [Read-Only] Save  
/etc  
1 # Generated by NetworkManager  
2 search mrshcherbak.net  
3 nameserver 10.0.2.3
```

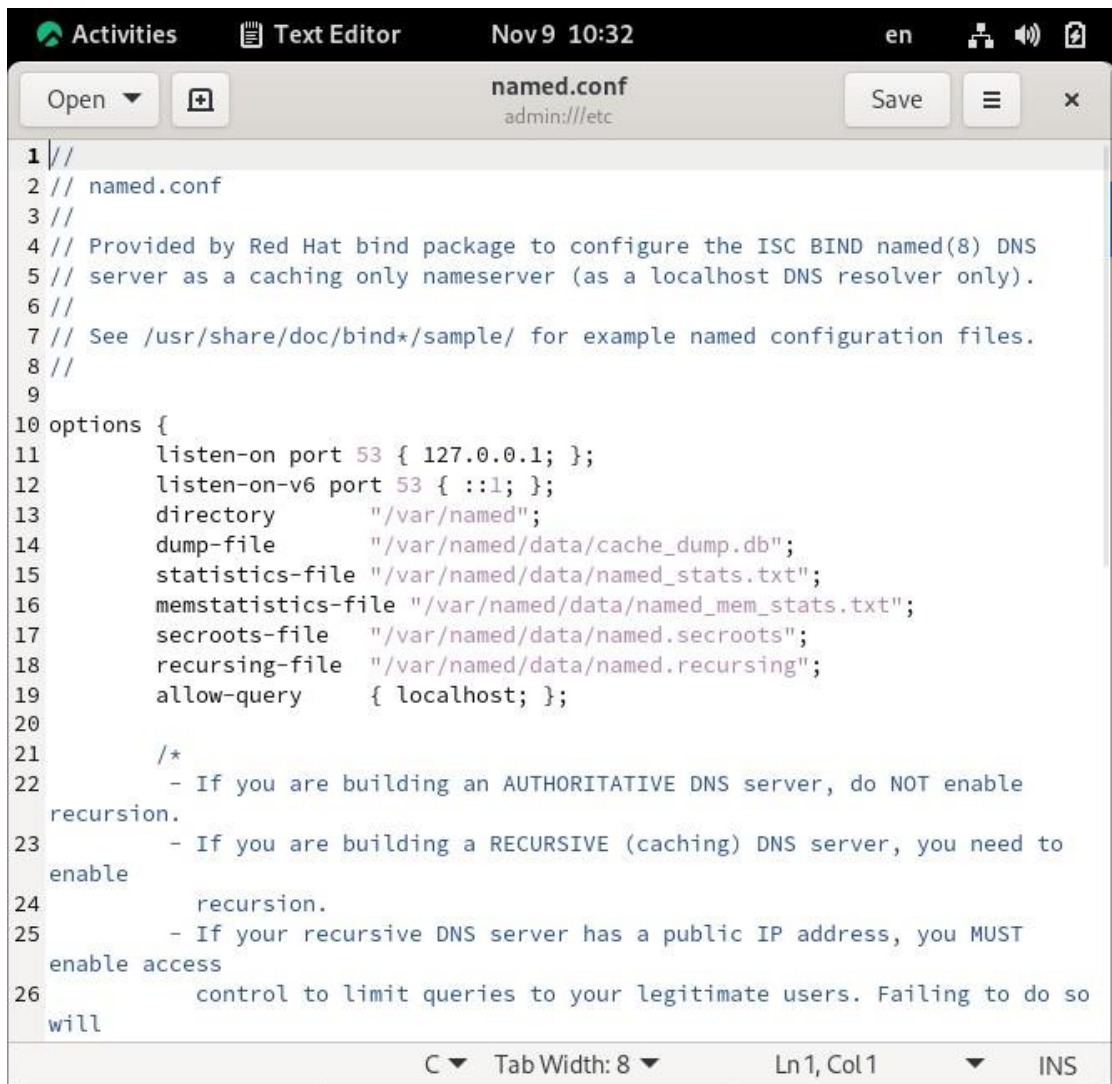
Рис.2.1. Содержимое файла `/etc/resolv.conf`

Файл `/etc/named.conf` является основным конфигурационным файлом для BIND (рис.2.2 – рис.2.3).

- `listen-on port 53 { 127.0.0.1; };` — устанавливает, на каком IP-адресе и порту будет слушать сервер DNS-запросы. В данном случае, сервер слушает на

локальном адресе 127.0.0.1 на порту 53.

- `listen-on-v6 port 53 { ::1; };` — то же самое, но для IPv6.
- `directory "/var/named";` — указывает директорию, в которой находятся файлы зон и другие данные сервера.
- `dump-file "/var/named/data/cache_dump.db";` — определяет файл, в который будут записаны дампы кеша.
- `statistics-file "/var/named/data/named_stats.txt";` — определяет файл, в который будет записана статистика сервера.
- `memstatistics-file "/var/named/data/named_mem_stats.txt";` — определяет файл, в который будет записана статистика использования памяти.
- `secroots-file "/var/named/data/named.secroots";` — определяет файл, в который будут записаны данные о корневых DNS-серверах для DNSSEC.
- `recursing-file "/var/named/data/named.recursing";` — определяет файл, в который будут записаны данные о рекурсивных запросах.
- `allow-query { localhost; any; };` — указывает, какие IP-адреса разрешены для выполнения DNS-запросов. Здесь разрешены запросы с локального хоста (localhost).



```
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.secrets";
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
23      recursion.
24      - If you are building a RECURSIVE (caching) DNS server, you need to
25      enable
26      recursion.
27      - If your recursive DNS server has a public IP address, you MUST
28      enable access
29      control to limit queries to your legitimate users. Failing to do so
30      will
```

Рис.2.2. Содержимое файла /etc/named.conf

- recursion yes; — разрешает серверу выполнять рекурсивные DNS-запросы.
- dnssec-validation yes; — включает валидацию DNSSEC.
- managed-keys-directory "/var/named/dynamic"; — указывает директорию для хранения динамически управляемых ключей.
- pid-file "/run/named/named.pid"; — указывает путь к файлу, в котором будет сохранен PID процесса сервера.
- session-keyfile "/run/named/session.key"; — указывает путь к файлу, в котором будет сохранен ключ сессии.
- logging { channel default\_debug { file "data/named.run"; severity dynamic; }; — настройки логирования, указывает файл и уровень логирования.

- `zone "." IN { type hint; file "named.ca"; };` — определяет информацию о зоне "." (корневая зона). Тип "hint" указывает на использование файла подсказок, а файл "named.ca" содержит информацию о корневых серверах.
- `include "/etc/named.rfc1912.zones";` — подключает файл с настройками зон, соответствующих рекомендациям RFC 1912.
- `include "/etc/named.root.key";` — подключает файл с корневыми ключами DNS.

```

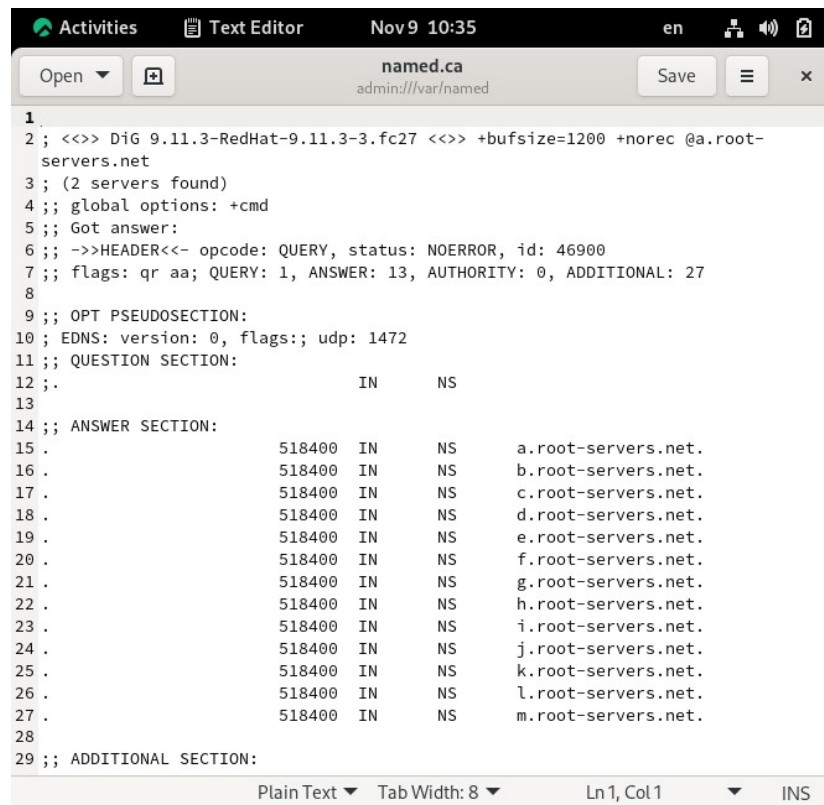
29     /* Reduce such attack surface
30     */
31     recursion yes;
32
33     dnssec-validation yes;
34
35     managed-keys-directory "/var/named/dynamic";
36     geoip-directory "/usr/share/GeoIP";
37
38     pid-file "/run/named/named.pid";
39     session-keyfile "/run/named/session.key";
40
41     /* 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

```

Рис.2.3. Продолжение файла /etc/named.conf

Файл /var/named/named.ca описывает все рутовые сервера (root) (рис.2.4).





```
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:
```

Рис.2.4. Содержимое файла /var/named/named.ca

Файлы /var/named/named.localhost и /var/named/named.loopback описывают прямую и обратную зону для локальной машины. В этих файлах DNS-имя сервера @ rname.invalid; формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-записи 127.0.0.1.



```
[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 ~]#
```

Рис.2.5. Содержимое файлов /var/named/named.localhost и /var/named/named.loopback



2. Запустила DNS-сервер: `systemctl start named`. Включила запуск DNS-сервера в автозапуск при загрузке системы: `systemctl enable named`. Выполнила команду `dig www.yandex.ru` и `dig @127.0.0.1 www.yandex.ru`. Команды представлены на рис.2.6 и рис.2.7.

```
[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
```

Рис.2.6. Выполнение команд

По команде `dig www.yandex.ru` сделали запрос с внешнего сервера, а по команде `dig @127.0.0.1 www.yandex.ru` — с локального сервера. Но этот DNS-сервер не является сервером по умолчанию для локальной машины. Для этого нужно настроить конфигурацию.

```
[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 ~]#
```

Рис.2.7. Выполнение команды dig @127.0.0.1 [www.yandex.ru](http://www.yandex.ru)

3. Сделала DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Изменила настройки сетевого соединения eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0.1 (рис.2.8).

```
[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-
lx, 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-clc35717f76d) successfully updated.
nmcli> quit
[root@server.mrshcherbak.net ~]#
```

Рис.2.8. Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети

4. Сделала то же самое для соединения System eth0 и проверила наличие изменений в файле /etc/resolv.conf, перезапустив NetworkManager с помощью команды `systemctl restart NetworkManager`. (рис.2.9 – рис.2.10).

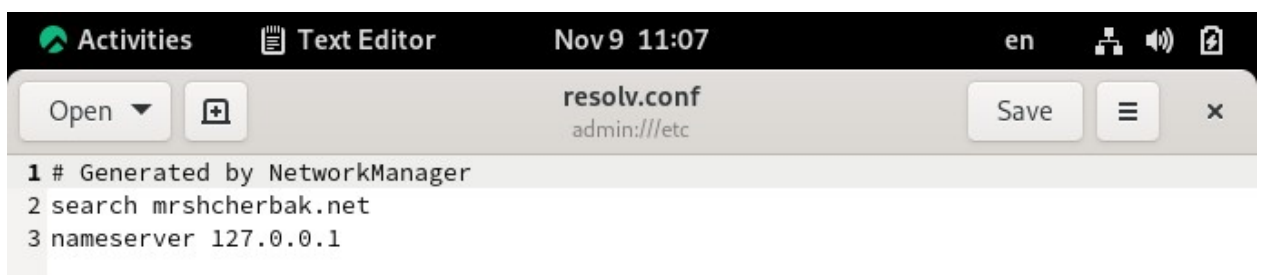
```
[root@server.mrshcherbak.net ~]# nmcli connection edit System\ eth0
===| nmcli interactive connection editor |===

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-
lx, 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 ~]#
```

Рис.2.9. Выполнение команды



The screenshot shows a text editor window titled 'Text Editor' with the file 'resolv.conf' open. The file content is as follows:

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

Рис.2.10. Проверка изменений

5. Внесла изменения в файл /etc/named.conf: «listen-on port 53 { 127.0.0.1; any; };» и «allow-query { localhost; 192.168.0.0/16; };» (рис.2.11).

```
mc [root@server.mrshcherbak.net]:/etc
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.recurring";
<----->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
```

Рис.2.11. Редактирование файла /etc/named.conf

6. Внесла изменения в настройки межсетевого экрана узла server, разрешив работу с DNS и убедилась, что DNS-запросы идут через узел server, который прослушивает порт 53, используя команду: `lsof: lsof | grep UDP` (рис.2.12 – рис.2.13).



```

root@server:~
[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-daemon 563      0t0      UDP *:mdns          avahi    12u     IPv4      18829
avahi-daemon 563      0t0      UDP *:mdns          avahi    13u     IPv6      18830
avahi-daemon 563      0t0      UDP *:40338        avahi    14u     IPv4      18831
avahi-daemon 563      0t0      UDP *:51103        avahi    15u     IPv6      18832
chronyd       588      0t0      UDP localhost:323   chrony   5u      IPv4      18707
chronyd       588      0t0      UDP localhost:323   chrony   6u      IPv6      18708
chronyd       588      0t0      195417 protocol: UDP chrony   8u      sock      0,8
named         12200    0t0      UDP localhost:domain named    16u     IPv4      208942
named         12200    0t0      UDP localhost:domain named    19u     IPv6      208944
named         12200    12201  isc-net-0         named    16u     IPv4      208942
named         12200    12201  UDP localhost:domain named    19u     IPv6      208944
named         12200    12201  isc-net-0         named    16u     IPv4      208942

```

Рис.2.12. Выполнение команд

```

root@server:~
chronyd       588      0t0      UDP localhost:323   chrony   8u      sock      0,8
named         12200    0t0      195417 protocol: UDP named    16u     IPv4      208942
named         12200    0t0      UDP localhost:domain named    19u     IPv6      208944
named         12200    0t0      UDP localhost:domain named    16u     IPv4      208942
named         12200    12201  isc-net-0         named    19u     IPv6      208944
named         12200    12201  UDP localhost:domain named    16u     IPv4      208942
named         12200    12201  isc-net-0         named    19u     IPv6      208944
named         12200    12202  isc-timer         named    16u     IPv4      208942
named         12200    12202  UDP localhost:domain named    19u     IPv6      208944
named         12200    12202  isc-timer         named    16u     IPv4      208942
named         12200    12203  isc-socket        named    19u     IPv6      208944
named         12200    12203  UDP localhost:domain named    16u     IPv4      208942
named         12200    12203  isc-socket        named    19u     IPv6      208944
named         12200    12241  isc-net-0         named    16u     IPv4      208942
named         12200    12241  UDP localhost:domain named    19u     IPv6      208944
NetworkManager 12628    0t0      UDP server.mrshcherbak.net:bootpc->_gateway:bootps root     27u     IPv4      215303
NetworkManager 12628    0t0      UDP server.mrshcherbak.net:bootpc->_gateway:bootps root     27u     IPv4      215303
NetworkManager 12628    0t0      UDP server.mrshcherbak.net:bootpc->_gateway:bootps root     27u     IPv4      215303
NetworkManager 12628    0t0      UDP server.mrshcherbak.net:bootpc->_gateway:bootps root     27u     IPv4      215303
[root@server.mrshcherbak.net ~]#

```

Рис.2.13. Вывод команды lsof: lsof | grep UDP

### 3. Конфигурирование первичного DNS-сервера

1. Скопировала шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименовала его в `mrshcherbak` (рис.3.1).

```
[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
```

Рис.3.1. Выполнение команд

2. Включила файл описания зоны `/etc/named/user.net` в конфигурационном файле DNS `/etc/named.conf`, добавив в нём в конце строку, выделенную на рис.3.2.

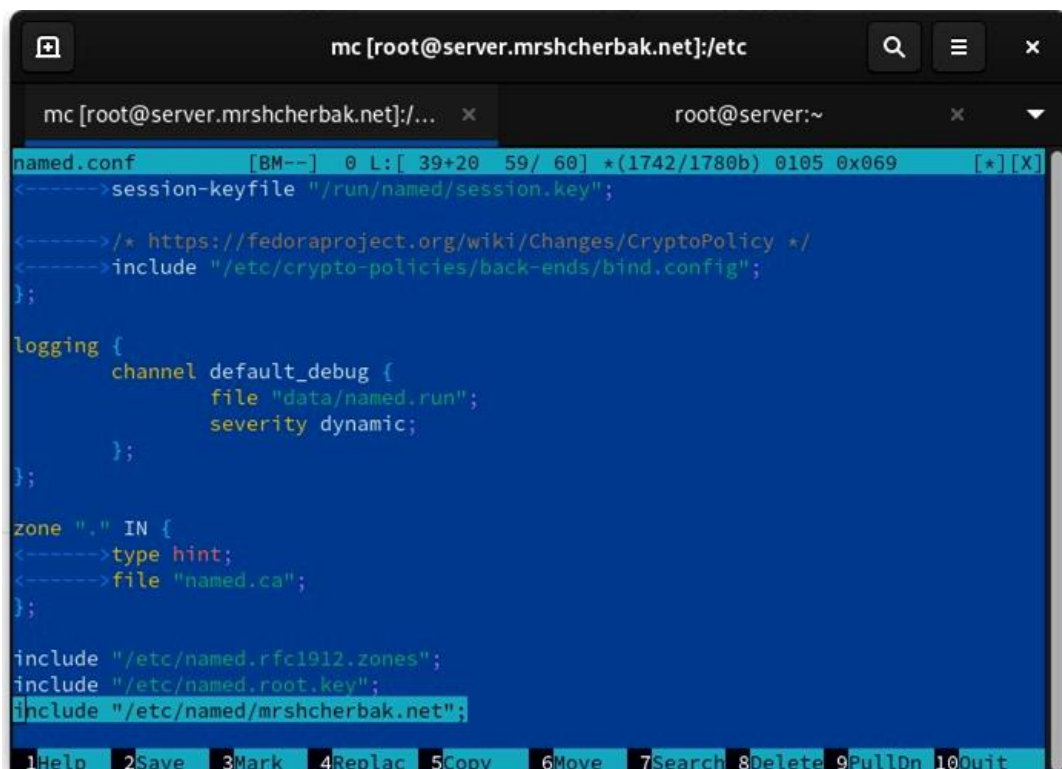
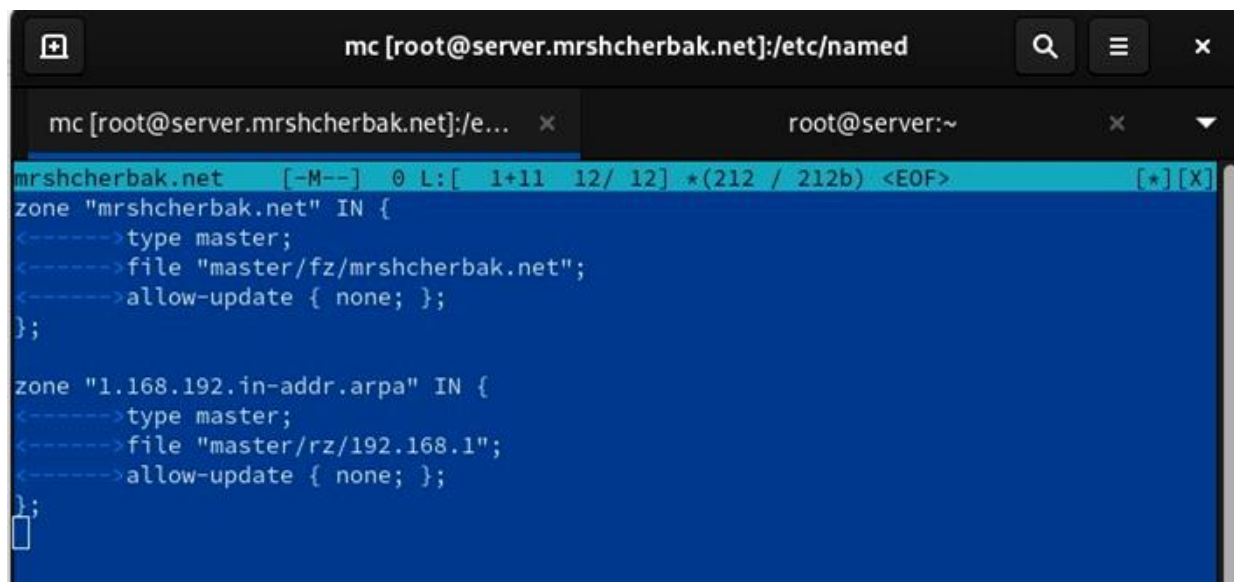


Рис.3.2. Редактирование файла `/etc/named.conf`

3. Открыла файл `/etc/named/mrshcherbak.net` на редактирование и внесла изменения, показанные на рис.3.3.

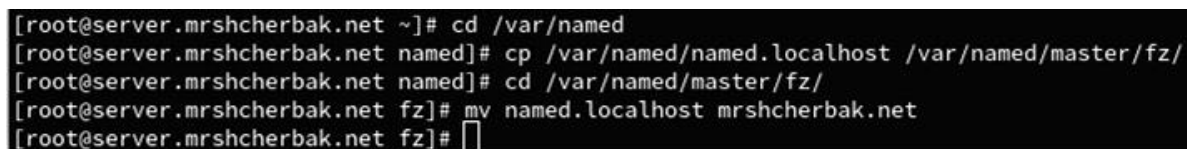


```
mc [root@server.mrshcherbak.net]:/etc/named
mrshcherbak.net  [-M--]  0 L:[ 1+11 12/ 12] *(212 / 212b) <EOF>  [*] [X]
zone "mrshcherbak.net" IN {
<----->type master;
<----->file "master/fz/mrshcherbak.net";
<----->allow-update { none; };
};

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

Рис.3.3. Редактирование файла /etc/named/mrshcherbak.net

4. В каталоге /var/named создала подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно: `cd /var/named mkdir -p /var/named/master/fz mkdir -p /var/named/master/rz` и скопировала шаблон прямой DNS-зоны `named.localhost` из каталога /var/named в каталог /var/named/master/fz и переименовала его в `mrshcherbak.net` (рис.3.4).



```
[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]#
```

Рис.3.4. Выполнение команд

5. Изменила файл /var/named/master/fz/mrshcherbak.net, указав необходимые DNS-записи для прямой зоны. В этом файле DNS-имя сервера @ name.invalid заменено на @ server.mrshcherbak.net.; формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-записи заменён с 127.0.0.1 на 192.168.1.1; в директиве \$ORIGIN задано текущее имя домена mrshcherbak.net., затем указаны имена и адреса серверов в этом домене в виде А-записей DNS (прописан сервер с именем ns и адресом 192.168.1.1. Содержимое файла представлено на рис.3.5.



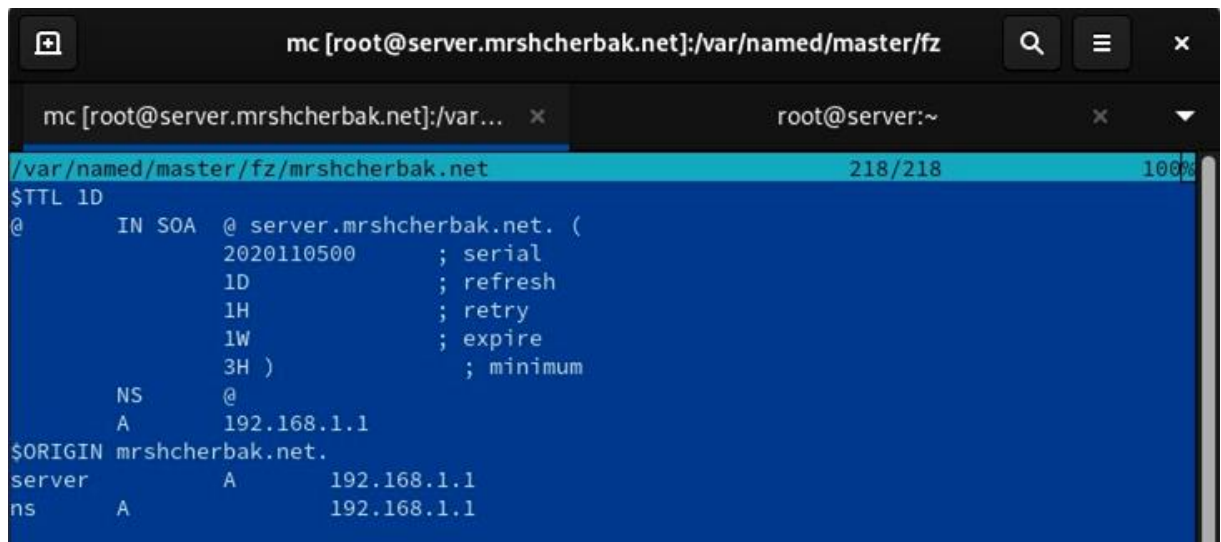


Рис.3.5. Редактирование файла /var/named/master/fz/mrshcherbak.net

6. Скопировала шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименовала его в 192.168.1 (рис.3.6).

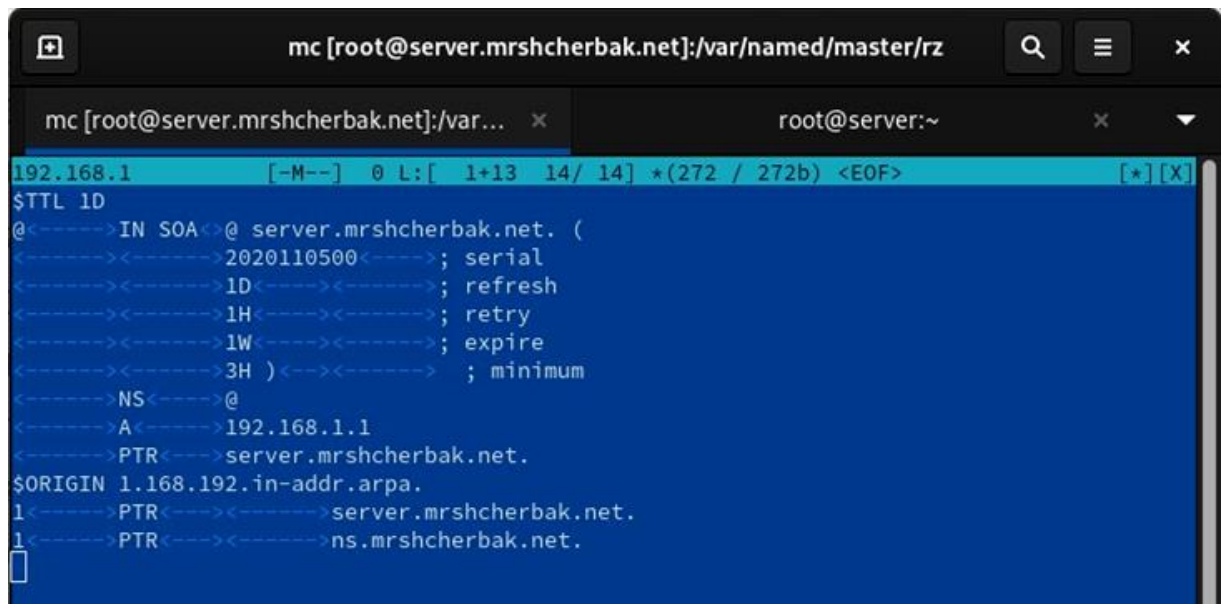
```

[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]#

```

Рис.3.6. Выполнение команд

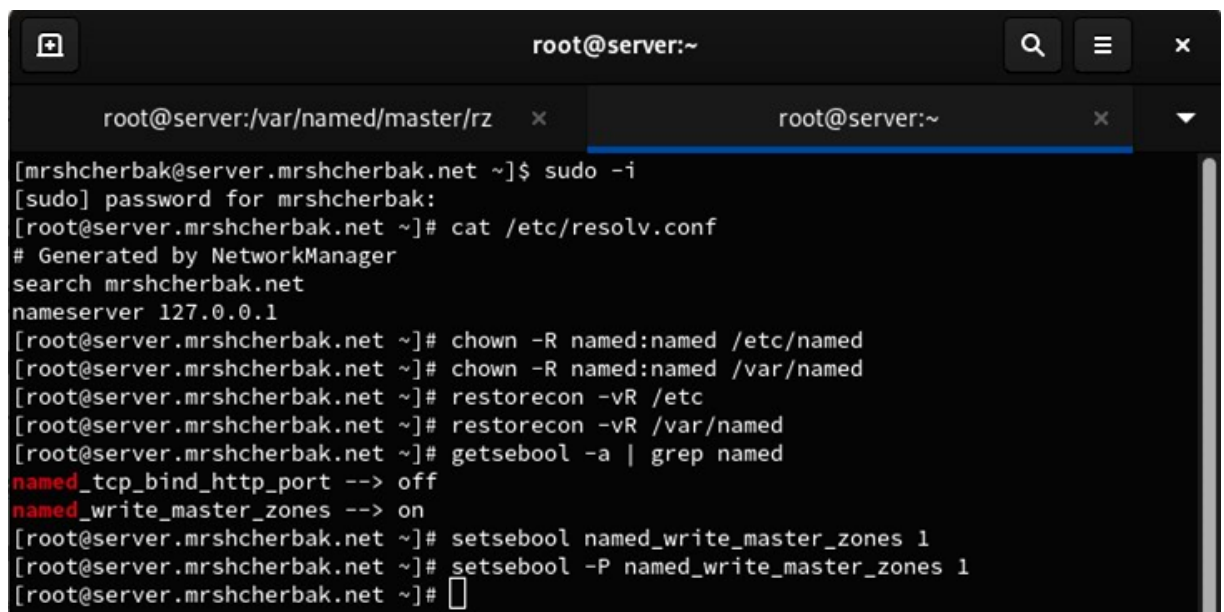
7. Изменила файл /var/named/master/rz/192.168.1, указав необходимые DNS-записи для обратной зоны. В этом файле DNS-имя сервера @ name.invalid. заменено на @ server.mrshcherbak.net.; формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в A-записи заменён с 127.0.0.1 на 192.168.1.1; в директиве \$ORIGIN задано название обратной зоны в виде 1.168.192.in-addr.arpa., затем заданы PTR-записи (задана PTR запись, ставящая в соответствие адресу 192.168.1.1 DNS-адрес ns.mrshcherbak.net). Содержимое файла представлено на рис.3.7.



```
mc [root@server.mrshcherbak.net]:/var/named/master/rz/192.168.1
$TTL 1D
@<----->IN SOA<----->@ server.mrshcherbak.net. (
<-----><----->2020110500<----->; serial
<-----><----->1D<-----><----->; refresh
<-----><----->1H<-----><----->; retry
<-----><----->1W<-----><----->; expire
<-----><----->3H )<-----><----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
<----->PTR<----->server.mrshcherbak.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<----->PTR<-----><----->server.mrshcherbak.net.
1<----->PTR<-----><----->ns.mrshcherbak.net.
```

Рис.3.7. Редактирование файла /var/named/master/rz/192.168.1

8. Исправила права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать: `chown -R named:named /etc/named` и `chown -R named:named /var/named`. Корректно восстановила метки в SELinux: `restorecon -vR /etc` и `restorecon -vR /var/named`. Для проверки состояния переключателей SELinux, относящихся к named, ввела: `getsebool -a | grep named`. Дала named разрешение на запись в файлы DNS-зоны: `setsebool named_write_master_zones 1` и `setsebool -P named_write_master_zones 1`. Команды представлены на рис.3.8.

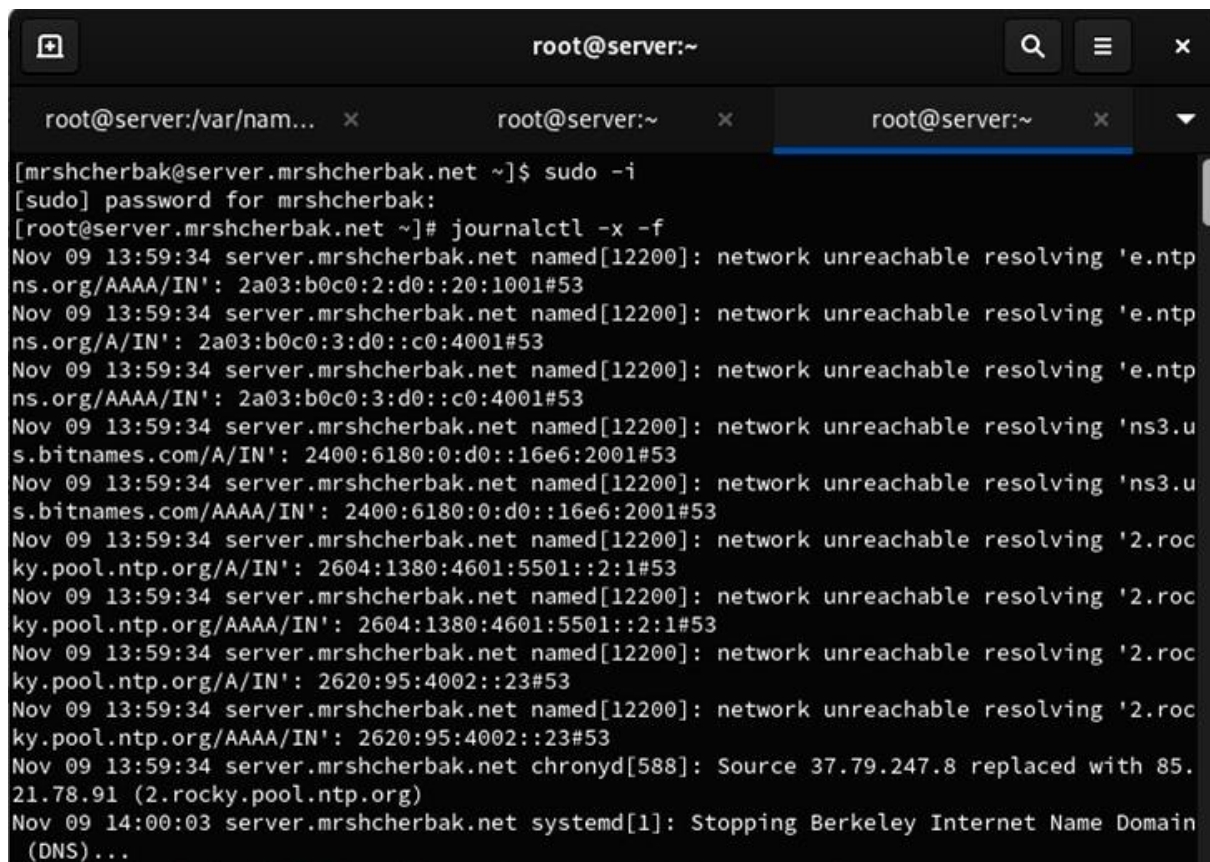


```
root@server:~
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search mrshcherbak.net
nameserver 127.0.0.1
[root@server.mrshcherbak.net ~]# chown -R named:named /etc/named
[root@server.mrshcherbak.net ~]# chown -R named:named /var/named
[root@server.mrshcherbak.net ~]# restorecon -vR /etc
[root@server.mrshcherbak.net ~]# restorecon -vR /var/named
[root@server.mrshcherbak.net ~]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.mrshcherbak.net ~]# setsebool named_write_master_zones 1
[root@server.mrshcherbak.net ~]# setsebool -P named_write_master_zones 1
[root@server.mrshcherbak.net ~]#
```

Рис.3.8. Выполнение команд

9. В дополнительном терминале запустила в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы

системы: `journalctl -x -f` (рис.3.9) и в первом терминале перезапустила DNS-сервер: `systemctl restart named`.



```
root@server:~  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# journalctl -x -f  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/AAAA/IN': 2a03:b0c0:2:d0::20:1001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/A/IN': 2a03:b0c0:3:d0::c0:4001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/AAAA/IN': 2a03:b0c0:3:d0::c0:4001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'ns3.u  
s.bitnames.com/A/IN': 2400:6180:0:d0::16e6:2001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'ns3.u  
s.bitnames.com/AAAA/IN': 2400:6180:0:d0::16e6:2001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/A/IN': 2604:1380:4601:5501::2:1#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/AAAA/IN': 2604:1380:4601:5501::2:1#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/A/IN': 2620:95:4002::23#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/AAAA/IN': 2620:95:4002::23#53  
Nov 09 13:59:34 server.mrshcherbak.net chronyd[588]: Source 37.79.247.8 replaced with 85.  
21.78.91 (2.rocky.pool.ntp.org)  
Nov 09 14:00:03 server.mrshcherbak.net systemd[1]: Stopping Berkeley Internet Name Domain  
(DNS)...
```

Рис.3.9. Выполнение команды `journalctl -x -f`

#### 4. Анализ работы DNS-сервера

1. При помощи утилиты `dig` получила описание DNS-зоны с сервера `ns.mrshcherbak.net` (рис.4.1). Команда `dig ns.mrshcherbak.net` показывает, что DNS-запрос для домена `ns.mrshcherbak.net` успешно выполнен и получен ответ с IPv4-адресом 192.168.1.1.

Вопрос (QUESTION SECTION): `ns.mrshcherbak.net. IN A` — запрос о типе записи A (IPv4) для домена `ns.mrshcherbak.net`.

Ответ (ANSWER SECTION): `ns.mrshcherbak.net. 86400 IN A 192.168.1.1` — ответ на запрос - `ns.mrshcherbak.net` имеет IPv4-адрес 192.168.1.1, с TTL (временем жизни записи) 86400 секунд.

```

[root@server.mrshcherbak.net ~]# dig ns.mrshcherbak.net

; <<> DiG 9.16.23-RH <<> ns.mrshcherbak.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56656
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3a3f8e6962a97a3301000000654ce729a9300a5599d5ee20 (good)
;; QUESTION SECTION:
;ns.mrshcherbak.net.          IN      A

;; ANSWER SECTION:
ns.mrshcherbak.net.          86400   IN      A      192.168.1.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 09 14:05:29 UTC 2023
;; MSG SIZE rcvd: 91

[root@server.mrshcherbak.net ~]#

```

Рис.4.1. Описание DNS-зоны с сервера ns.mrshcherbak.net

2. При помощи утилиты host проанализировала корректность работы DNS-сервера (рис.4.2 –рис.4.3).

- `host -l mrshcherbak.net` — команда запрашивает полный список записей для домена mrshcherbak.net и может использоваться для получения полной копии DNS-зоны.
- `host -a mrshcherbak.net` — команда выполняет запрос типа ANY. Это означает запрос всех доступных записей для домена mrshcherbak.net. Она возвращает разнообразную информацию, включая записи A (IPv4), AAAA (IPv6), NS (Name Server), MX (Mail Exchange), и другие, если они присутствуют в зоне.
- `host -t A mrshcherbak.net` — команда запрашивает только записи типа A (IPv4) для домена mrshcherbak.net. Она возвращает только IPv4-адреса, связанные с указанным доменом.
- `host -t PTR 192.168.1.1` — команда запрашивает записи типа PTR (Pointer) для IPv4-адреса 192.168.1.1. Такие записи обычно используются для выполнения обратного DNS-поиска и возвращают доменное имя, связанное с указанным IP-адресом.

Результаты этих команд свидетельствуют о том, что DNS-сервер для домена mrshcherbak.net корректно обрабатывает запросы и возвращает ожидаемые записи для данного домена.

```
[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
```

Рис.4.2. Выполнение команд

```
[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 ~]#
```

Рис.4.3. Выполнение команд

## 5. Внесение изменений в настройки внутреннего окружения виртуальной машины

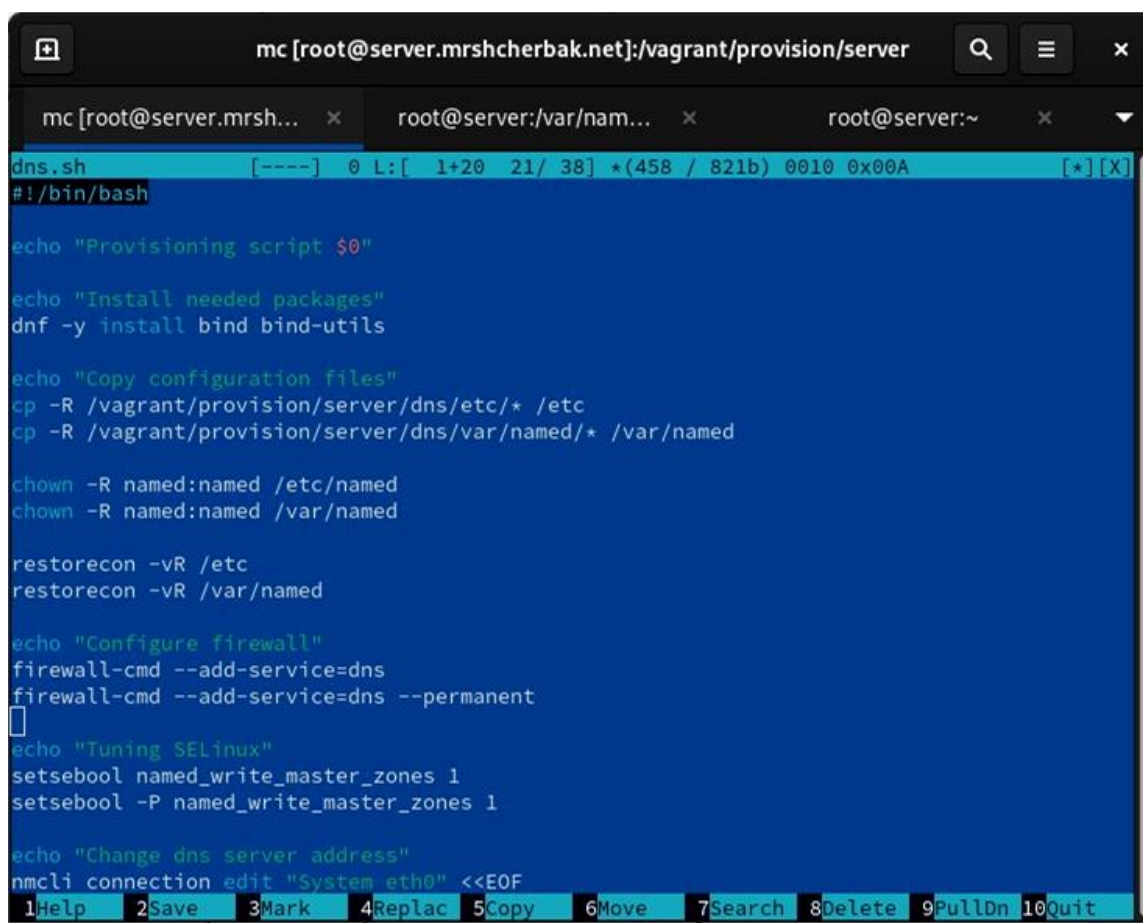
1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создала в нём каталог dns, в который поместила в соответствующие каталоги конфигурационные файлы DNS (рис.5.1).

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

Рис.5.1. Выполнение команд



2. В каталоге `/vagrant/provision/server` создала исполняемый файл `dns.sh`: `touch dns.sh`, `chmod +x dns.sh`. Открыв его на редактирование, прописала в нём скрипт (рис.5.2 – рис.5.3). Этот скрипт повторяет произведённые вами действия по установке и настройке DNS-сервера: подставляет в нужные каталоги подготовленные конфигурационные файлы; меняет соответствующим образом права доступа, метки безопасности SELinux и правила межсетевого экрана; настраивает сетевое соединение так, чтобы сервер выступал DNS-сервером по умолчанию для узлов внутренней виртуальной сети; запускает DNS-сервер.



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

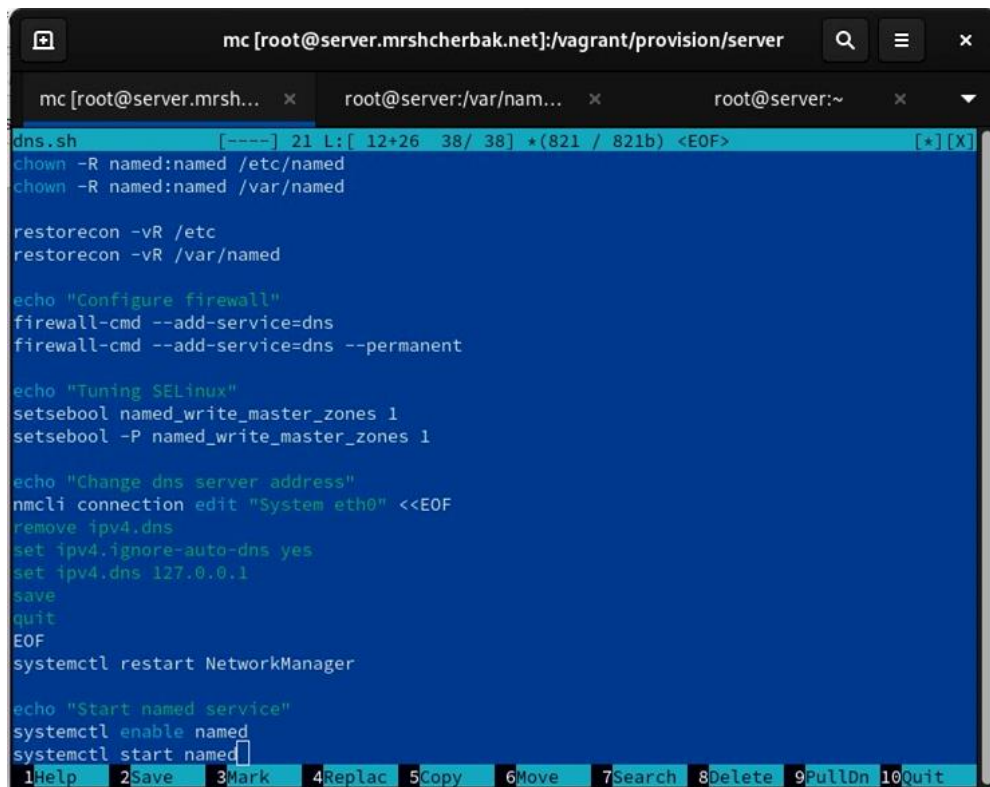
chown -R named:named /etc/named
chown -R named:named /var/named

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
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис.5.2. Содержимое файла `dns.sh`



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

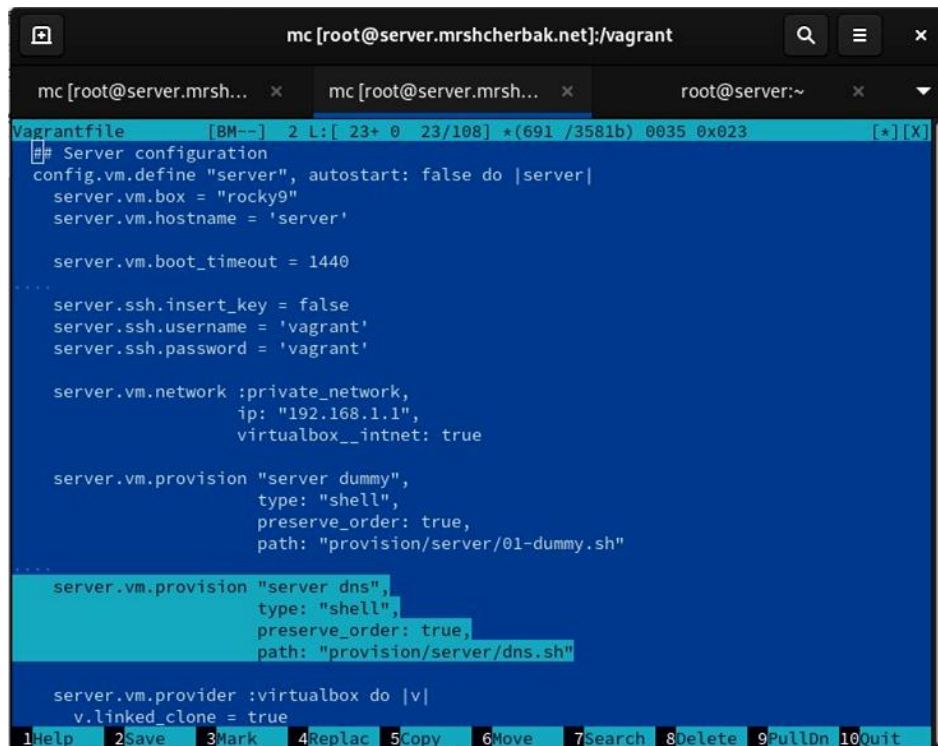
echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1

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
```

Рис.5.3. Продолжение содержимого файла dns.sh

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавила в разделе конфигурации для сервера блок, выделенный на рис.5.4.



```
mc [root@server.mrshcherbak.net]:/vagrant
Vagrantfile
# Server configuration
config.vm.define "server", autostart: false do |server|
  server.vm.box = "rocky9"
  server.vm.hostname = 'server'

  server.vm.boot_timeout = 1440
  ....
  server.ssh.insert_key = false
  server.ssh.username = 'vagrant'
  server.ssh.password = 'vagrant'

  server.vm.network :private_network,
    ip: "192.168.1.1",
    virtualbox____intnet: true

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

  server.vm.provider :virtualbox do |v|
    v.linked_clone = true
```

Рис.5.4. 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.

## Контрольные вопросы

### 1. Что такое DNS?

Система доменных имён (Domain Name System, DNS) — распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес, и наоборот.

### 2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.

### 3. Чем отличается прямая DNS-зона от обратной?

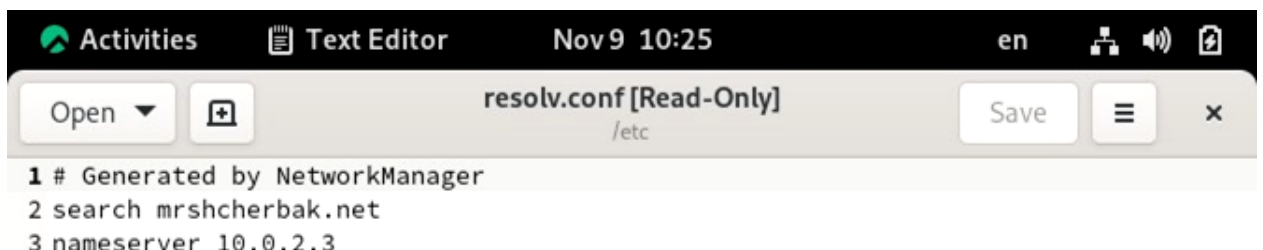
Прямая DNS-зона связана с преобразованием доменных имен в IP-адреса, а обратная — с обратным преобразованием IP-адресов в доменные имена.

### 4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.

Основные настройки DNS-сервера могут располагаться в файлах `/etc/named.conf` и в директории `/var/named/`. `named.conf` содержит глобальные настройки, а файлы в `/var/named/` - данные о DNS-зонах и кэше.

### 5. Что указывается в файле `resolv.conf`?

Файл `/etc/resolv.conf` указывает на использование NetworkManager для управления сетевыми подключениями, домен поиска установлен как `mrshcherbak.net`, и DNS-сервер установлен как `10.0.2.3`.

A screenshot of a Linux desktop environment. The top panel shows the 'Activities' button, 'Text Editor' window title, the date and time 'Nov 9 10:25', the language 'en', and system icons for network, volume, and battery. Below the panel is a window titled 'resolv.conf [Read-Only]' with a path indicator '/etc'. The window contains a text editor with the following content:

```
1 # Generated by NetworkManager
2 search mrshcherbak.net
3 nameserver 10.0.2.3
```

### 6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?

Типы записи описания ресурсов:

- SOA-запись — указывает на авторитативность для зоны;
- NS-запись — перечисляет DNS-серверы зоны;
- A — задаёт отображение имени узла в IP-адрес;
- PTR — задаёт отображение IP-адреса в имя узла;
- CNAME — задаёт каноническое имя (для псевдонимов);
- MX — задаёт имена почтовым серверам.

7. Для чего используется домен in-addr.arpa?

Этот домен используется для поиска соответствия между известным IP-адресом и (искомым) доменным именем. Реальный IP-адрес преобразуется в доменное имя в домене in-addr.arpa посредством переименования: так, компьютер с адресом 127.0.0.1 представляется в домене in-addr.arpa как 1.0.0.127.in-addr.arpa.

8. Для чего нужен демон named?

Named - это демон, входящий в состав пакета bind9 и являющийся сервером доменных имен. Демон named может реализовывать функции серверов любого типа: master, slave, cache. Он отвечает за обработку запросов, разрешение имен и обслуживание DNS-зон.

9. В чём заключаются основные функции slave-сервера и master-сервера?

Чтобы организовать DNS-хостинг, провайдеры используют несколько DNS-серверов. Один главный и хотя бы один ведомый:

- главный (master) хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых;
- ведомый (slave) получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.

10. Какие параметры отвечают за время обновления зоны?

Временные параметры в записи SOA отвечают за время обновления зоны:

- Refresh — интервал времени, после которого slave-сервер обязан обратиться к master-серверу с запросом на верификацию своего описания зоны;
- Retry — интервал времени, после которого slave-сервер должен повторить попытку синхронизировать описание зоны с master сервером;
- Expire — интервал времени, после которого slave-сервер должен прекратить обслуживание запросов к зоне, если он не смог в течение этого времени верифицировать описание зоны, используя информацию с master-сервера;

#### 11. Как обеспечить защиту зоны от скачивания и просмотра?

Защита зоны от скачивания и просмотра может быть обеспечена ограничением доступа к файлам зоны и конфигурационным файлам DNS-сервера. Например, ограничение прав доступа к файлам с помощью утилиты `chmod` или использование ACL (Access Control List).

#### 12. Какая запись RR применяется при создании почтовых серверов?

Для создания почтовых серверов используется запись RR (Resource Record) типа MX (Mail Exchange). Она указывает на почтовый сервер, который обслуживает почтовые ящики для данного домена.

#### 13. Как протестировать работу сервера доменных имён?

Для тестирования работы сервера доменных имён можно использовать утилиту `dig`. Например:

`dig @dns_server_ip example.com` - выполнить базовый DNS-запрос.

`dig +trace example.com` - отслеживание маршрута запроса от корневых серверов до конечного ответа.

```
[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 ~]#
```

14. Как запустить, перезапустить или остановить какую-либо службу в системе?

Для управления службами в Linux используется утилита `systemctl`. Например:

- Запустить службу: `sudo systemctl start service_name`.
- Перезапустить службу: `sudo systemctl restart service_name`.
- Остановить службу: `sudo systemctl stop service_name`.

15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?

Для просмотра отладочной информации при запуске службы можно использовать команду `journalctl`. Например:

`journalctl -u service_name` - просмотр логов для конкретной службы.

Так, в ходе выполнения работы я запускала в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы: `journalctl -x -f`.

```
root@server:~  
root@server:/var/nam... x root@server:~ x root@server:~ x  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# journalctl -x -f  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/AAAA/IN': 2a03:b0c0:2:d0::20:1001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/A/IN': 2a03:b0c0:3:d0::c0:4001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'e.ntp  
ns.org/AAAA/IN': 2a03:b0c0:3:d0::c0:4001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'ns3.u  
s.bitnames.com/A/IN': 2400:6180:0:d0::16e6:2001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving 'ns3.u  
s.bitnames.com/AAAA/IN': 2400:6180:0:d0::16e6:2001#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/A/IN': 2604:1380:4601:5501::2:1#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/AAAA/IN': 2604:1380:4601:5501::2:1#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/A/IN': 2620:95:4002::23#53  
Nov 09 13:59:34 server.mrshcherbak.net named[12200]: network unreachable resolving '2.roc  
ky.pool.ntp.org/AAAA/IN': 2620:95:4002::23#53  
Nov 09 13:59:34 server.mrshcherbak.net chronyd[588]: Source 37.79.247.8 replaced with 85.  
21.78.91 (2.rocky.pool.ntp.org)  
Nov 09 14:00:03 server.mrshcherbak.net systemd[1]: Stopping Berkeley Internet Name Domain  
(DNS)...
```

16. Где хранится отладочная информация по работе системы и служб? Как её посмотреть?

Отладочная информация хранится в системных журналах. Просмотреть журнал можно с использованием journalctl. Например:

journalctl - просмотр всех системных журналов.

```
Nov 09 21:47:09 server.mrshcherbak.net kernel: Linux version 5.14.0-284.30.1.el9_2.x86_64 (mockbuild@id1-prod-build001  
Nov 09 21:47:09 server.mrshcherbak.net kernel: The list of certified hardware and cloud instances for Enterprise Linux  
Nov 09 21:47:09 server.mrshcherbak.net kernel: Command line: BOOT_IMAGE=(hdd,msdos1)/boot/vmlinuz-5.14.0-284.30.1.el9_2  
Nov 09 21:47:09 server.mrshcherbak.net kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'  
Nov 09 21:47:09 server.mrshcherbak.net kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'  
Nov 09 21:47:09 server.mrshcherbak.net kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'  
Nov 09 21:47:09 server.mrshcherbak.net kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256  
Nov 09 21:47:09 server.mrshcherbak.net kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using  
Nov 09 21:47:09 server.mrshcherbak.net kernel: signal: max sigframe size: 1776  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-provided physical RAM map:  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000000000009ffff] reserved  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffff] reserved  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x0000000000010000-0x000000000003ffff] usable  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x000000000003ff0000-0x000000000003ffffff] ACPI data  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved  
Nov 09 21:47:09 server.mrshcherbak.net kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] reserved  
Nov 09 21:47:09 server.mrshcherbak.net kernel: NX (Execute Disable) protection: active  
Nov 09 21:47:09 server.mrshcherbak.net kernel: SMBIOS 2.5 present.  
Nov 09 21:47:09 server.mrshcherbak.net kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006  
Nov 09 21:47:09 server.mrshcherbak.net kernel: Hypervisor detected: KVM  
Nov 09 21:47:09 server.mrshcherbak.net kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Nov 09 21:47:09 server.mrshcherbak.net kernel: kvm-clock: using sched offset of 5792102700 cycles  
lines 1-24
```

17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс?

Информацию о файлах, используемых процессом, можно получить с помощью

команды lsof. Например:

`lsof -p PID` - список открытых файлов для процесса с определенным идентификатором.

Например, в работе я вносила изменения в настройки межсетевого экрана узла server, разрешив работу с DNS, после чего мне нужно было убедиться, что DNS-запросы идут через узел server, который прослушивает порт 53. Поэтому я использовала команду `lsof: lsof | grep UDP`.

```
root@server:~
[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-daemon 563      0t0      UDP *:mdns          avahi  12u    IPv4  18829
avahi-daemon 563      0t0      UDP *:mdns          avahi  13u    IPv6  18830
avahi-daemon 563      0t0      UDP *:40338        avahi  14u    IPv4  18831
avahi-daemon 563      0t0      UDP *:51103        avahi  15u    IPv6  18832
chronyd       588      0t0      UDP localhost:323   chrony  5u     IPv4  18707
chronyd       588      0t0      UDP localhost:323   chrony  6u     IPv6  18708
chronyd       588      0t0      UDP 195417 protocol: UDP chrony  8u     sock  0,8
named         12200    0t0      UDP localhost:domain named  16u    IPv4  208942
named         12200    0t0      UDP localhost:domain named  19u    IPv6  208944
named         12200    12201   UDP isc-net-0       named  16u    IPv4  208942
named         12200    12201   UDP localhost:domain named  19u    IPv6  208944
named         12200    12202   UDP isc-timer       named  16u    IPv4  208942
```



```
root@server:~  
0t0      UDP localhost:323  
chronyd  588      195417 protocol: UDP      chrony    8u      sock      0,8  
named    12200      UDP localhost:domain      named     16u     IPv4      208942  
named    12200      UDP localhost:domain      named     19u     IPv6      208944  
named    12200 12201 isc-net-0      named     16u     IPv4      208942  
named    12200 12201 isc-net-0      named     19u     IPv6      208944  
named    12200 12202 isc-timer      named     16u     IPv4      208942  
named    12200 12202 isc-timer      named     19u     IPv6      208944  
named    12200 12203 isc-socket     named     16u     IPv4      208942  
named    12200 12203 isc-socket     named     19u     IPv6      208944  
named    12200 12241 isc-net-0      named     16u     IPv4      208942  
named    12200 12241 isc-net-0      named     19u     IPv6      208944  
NetworkMa 12628      UDP localhost:domain      root      27u     IPv4      215303  
NetworkMa 12628 12637 gmain          root      27u     IPv4      215303  
NetworkMa 12628 12638 gdbus         root      27u     IPv4      215303  
[root@server.mrshcherbak.net ~]#
```

18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli.

Для изменения сетевого соединения с использованием nmcli:

- nmcli connection up connection\_name - включить соединение.
- nmcli connection down connection\_name - отключить соединение.
- nmcli connection mod connection\_name ipv4.method manual - изменить метод настройки IPv4 на ручной.
- nmcli connection edit connection\_name - редактировать параметры соединения.

Например, в ходе выполнения л/р №2 я сделала DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Изменила настройки сетевого соединения eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0.1.



```
[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-
lx, 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 ~]#
```

И сделала то же самое для соединения System eth0 и проверила наличие изменений в файле /etc/resolv.conf.

```
[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-
lx, 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 ~]#
```

19. Что такое SELinux?

SELinux — система контроля доступа. Данная система разрабатывалась как защита ОС от несанкционированного доступа к ней. В настоящее время SELinux включена во многие Linux-дистрибутивы. Реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.

20. Что такое контекст (метка) SELinux?

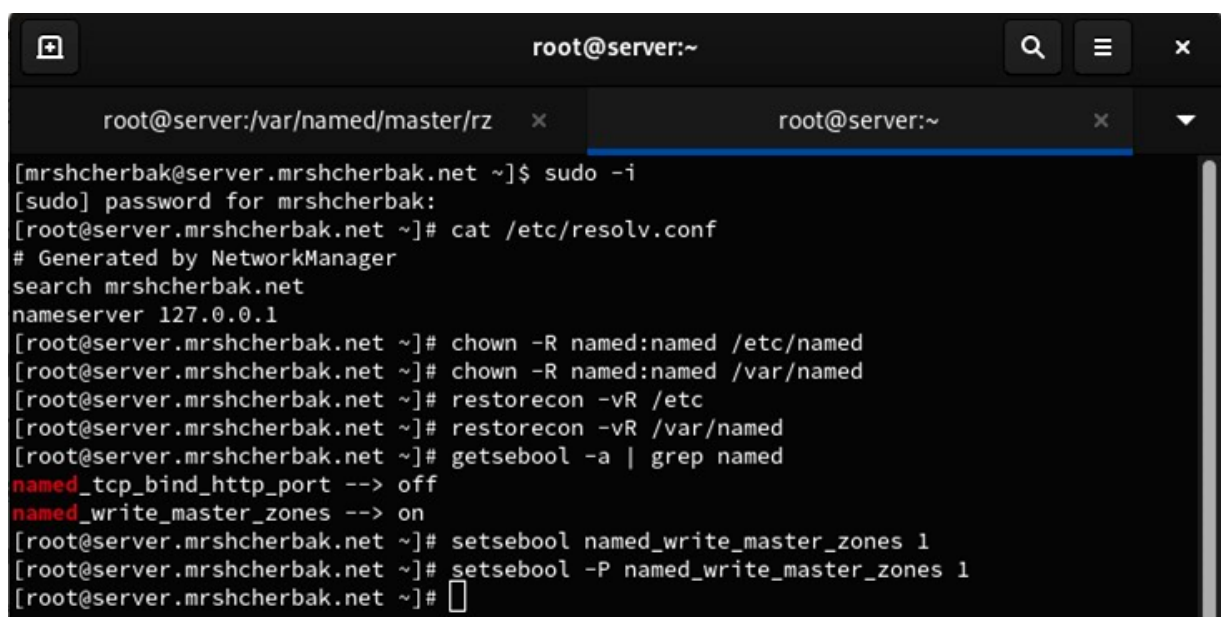
Контекст SELinux (Security Context) - это метка, которая присваивается файлам, процессам и другим ресурсам в системе. Контекст используется для определения политики безопасности SELinux, определяющей, какие операции разрешены или запрещены для каждого ресурса. Контекст безопасности записывается в атрибуты файла (в файловой системе) и создается при установке SELinux (операция labeling).

21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?

Для восстановления контекста SELinux после изменений в конфигурационных файлах можно использовать команду `restorecon`. Например:

`restorecon -Rv /path/to/directory` - рекурсивно восстановить контекст для указанного каталога.

В работе я корректно восстанавливала метки в SELinux: `restorecon -vR /etc` и `restorecon -vR /var/named`.



```
root@server:~  
root@server:/var/named/master/rz x root@server:~ x  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search mrshcherbak.net  
nameserver 127.0.0.1  
[root@server.mrshcherbak.net ~]# chown -R named:named /etc/named  
[root@server.mrshcherbak.net ~]# chown -R named:named /var/named  
[root@server.mrshcherbak.net ~]# restorecon -vR /etc  
[root@server.mrshcherbak.net ~]# restorecon -vR /var/named  
[root@server.mrshcherbak.net ~]# getsebool -a | grep named  
named_tcp_bind_http_port --> off  
named_write_master_zones --> on  
[root@server.mrshcherbak.net ~]# setsebool named_write_master_zones 1  
[root@server.mrshcherbak.net ~]# setsebool -P named_write_master_zones 1  
[root@server.mrshcherbak.net ~]#
```

22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?

Для создания разрешающих правил SELinux из файлов журналов можно использовать утилиту `audit2allow`. Пример:

`audit2allow -a -M mypolicy` - создать модуль политики SELinux на основе журналов.

23. Что такое булевый переключатель в SELinux?

Булевый переключатель (Boolean) в SELinux - это параметр, который изменяет поведение политики безопасности. Он позволяет включать или выключать определенные функции без изменения контекстов SELinux.

#### 24. Как посмотреть список переключателей SELinux и их состояние?

Список булевых переключателей и их состояние можно посмотреть с помощью команды `semanage boolean -l` или `getsebool -a`.

В работе я проверяла состояние переключателей SELinux, относящихся к `named`. Вводила: `getsebool -a | grep named`.

```
[root@server.mrshcherbak.net ~]# chown -R named:named /etc/named
[root@server.mrshcherbak.net ~]# chown -R named:named /var/named
[root@server.mrshcherbak.net ~]# restorecon -vR /etc
[root@server.mrshcherbak.net ~]# restorecon -vR /var/named
[root@server.mrshcherbak.net ~]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.mrshcherbak.net ~]# setsebool named_write_master_zones 1
[root@server.mrshcherbak.net ~]# setsebool -P named_write_master_zones 1
[root@server.mrshcherbak.net ~]#
```

#### 25. Как изменить значение переключателя SELinux?

Значение булевого переключателя SELinux можно изменить с использованием команды `setsebool`. Например:

`setsebool -P httpd_enable_homedirs 1` - установить значение булевого переключателя в 1 (включено) и сохранить изменения.

В работе я дала `named` разрешение на запись в файлы DNS-зоны: `setsebool named_write_master_zones 1` и `setsebool -P named_write_master_zones 1`.

```
[root@server.mrshcherbak.net ~]# setsebool named_write_master_zones 1
[root@server.mrshcherbak.net ~]# setsebool -P named_write_master_zones 1
[root@server.mrshcherbak.net ~]#
```