

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

дисциплина: Администрирование сетевых подсистем

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы:

Целью данной работы является приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

Выполнение работы:

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

```
cd /var/tmp/ismakhorin/vagrant
```

Далее запустим виртуальную машину server (Рис. 1.1):

```
make server-up
```

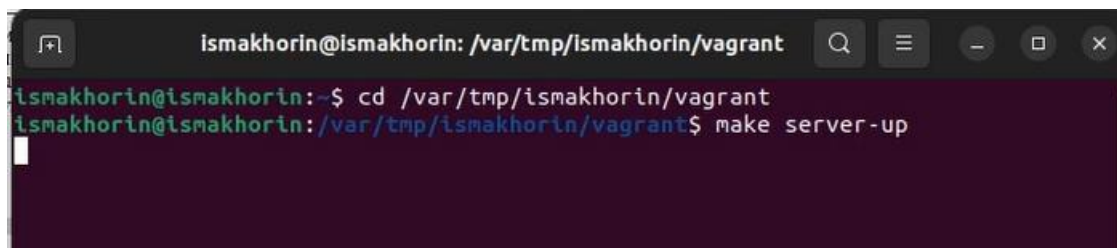


Рис. 1.1. Открытие рабочего каталога с проектом и запуск виртуальной машины server.

На виртуальной машине server войдём под созданным нами в предыдущей работе пользователем и откройте терминал. Перейдём в режим суперпользователя:

```
sudo -i
```

И установим bind и bind-utils (Рис. 1.2):

```
dnf -y install bind bind-utils
```

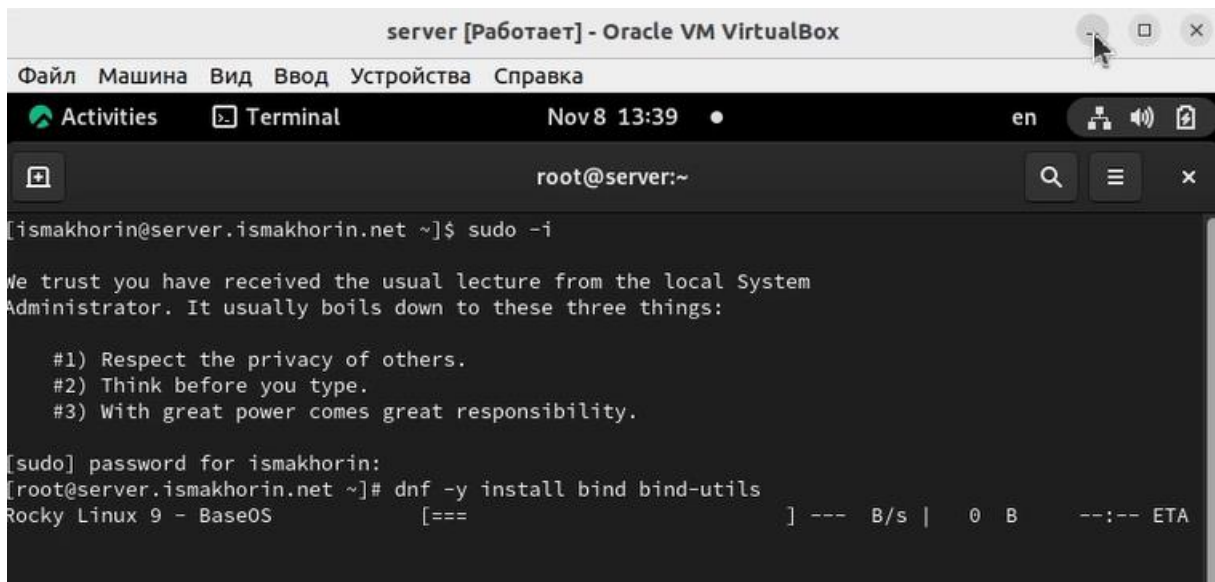


Рис. 1.2. Переход в режим суперпользователя и установка bind,bind-utils.

С помощью утилиты dig сделаем запрос к DNSАдресу www.yandex.ru (Рис. 1.3):

dig www.yandex.ru

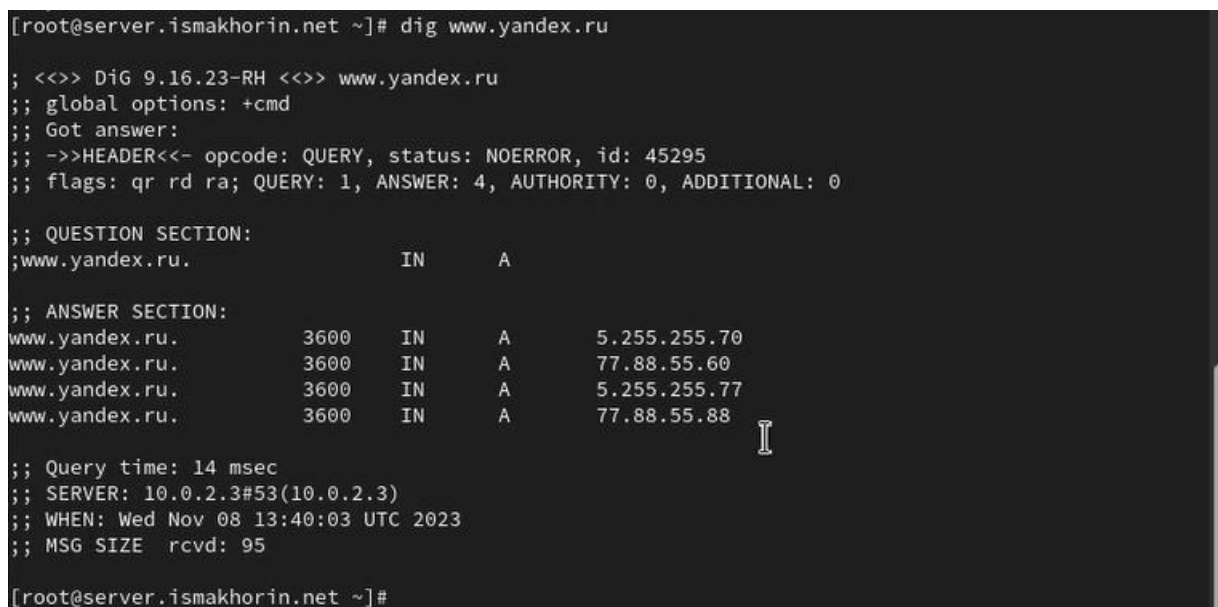


Рис. 1.3. Запрос с помощью утилиты dig.

Просмотрим содержание файлов /etc/resolv.conf (Рис. 2.1), /etc/named.conf (Рис. 2.2), /var/named/named.ca (Рис. 2.3), /var/named/named.localhost (Рис. 2.4), /var/named/named.loopback (Рис. 2.5).

```
[root@server.ismakhorin.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ismakhorin.net
nameserver 10.0.2.3
```

Рис. 2.1. Просмотр содержания файла /etc/resolv.conf.

```
[root@server.ismakhorin.net ~]# cat /etc/named.conf
//
// 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; };
    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; };

    /*
     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
     - If you are building a RECURSIVE (caching) DNS server, you need to enable
       recursion.
     - If your recursive DNS server has a public IP address, you MUST enable access
```

Рис. 2.2. Просмотр содержания файла /etc/named.conf.

```
[root@server.ismakhorin.net ~]# cat /var/named/named.ca

; <<>> DiG 9.11.3-RedHat-9.11.3-3.fc27 <<>> +bufsize=1200 +norec @a.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46900
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
; .                                IN      NS

;; ANSWER SECTION:
.      518400 IN      NS      a.root-servers.net.
.      518400 IN      NS      b.root-servers.net.
.      518400 IN      NS      c.root-servers.net.
.      518400 IN      NS      d.root-servers.net.
.      518400 IN      NS      e.root-servers.net.
.      518400 IN      NS      f.root-servers.net.
.      518400 IN      NS      g.root-servers.net.
.      518400 IN      NS      h.root-servers.net.
.      518400 IN      NS      i.root-servers.net.
.      518400 IN      NS      j.root-servers.net.
.      518400 IN      NS      k.root-servers.net.
.      518400 IN      NS      l.root-servers.net.
.      518400 IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
```

Рис. 2.3. Просмотр содержания файла /var/named/named.ca.

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

Рис. 2.4. Просмотр содержания файла /var/named/named.localhost.

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

Рис. 2.5. Просмотр содержания файла /var/named/named.loopback.

Запустим DNS-сервер:

```
systemctl start named
```

Включим запуск DNS-сервера в автозапуск при загрузке системы:

```
systemctl enable named
```

Проанализируем отличие в выведенной на экран информации при выполнении команд:

```
dig www.yandex.ru (Рис. 2.6)
```

и

```
dig @127.0.0.1 www.yandex.ru (Рис. 2.7)
```

```

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

;<<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36370
;; 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      5.255.255.70
www.yandex.ru.                3600    IN      A      5.255.255.77
www.yandex.ru.                3600    IN      A      77.88.55.60
www.yandex.ru.                3600    IN      A      77.88.55.88

;; Query time: 16 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Wed Nov 08 13:45:37 UTC 2023
;; MSG SIZE rcvd: 95

[root@server.ismakhorin.net ~]#

```

Рис. 2.6. Запуск DNS-сервера, включение запуска DNS-сервера в автозапуск при загрузке системы, анализ выведенной на экран информации при выполнении команды `dig www.yandex.ru`.

```

[root@server.ismakhorin.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: SERVFAIL, id: 29953
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0ad5c4b79d878b3901000000654b910eb2f6a5f6b2626e62 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; Query time: 398 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 08 13:45:50 UTC 2023
;; MSG SIZE rcvd: 70

[root@server.ismakhorin.net ~]#

```

Рис. 2.7. Анализ выведенной на экран информации при выполнении команды `dig @127.0.0.1 www.yandex.ru`.

Сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого изменим 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.ismakhorin.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, et
htool, 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 'eth0' (70a96a32-3852-4357-acca-ad13f910d5f8) successfully updated.
nmcli> quit
[root@server.ismakhorin.net ~]#
```

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

Сделаем тоже самое для соединения System eth0 (рис. 2.9):

```
[root@server.ismakhorin.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.

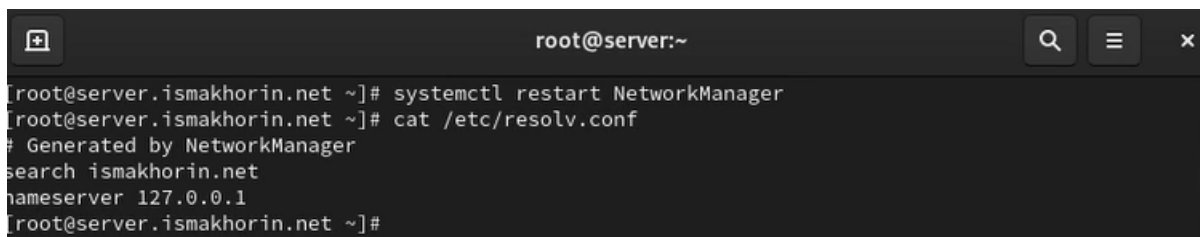
You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, et
htool, match, ipv4, ipv6, hostname, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
[root@server.ismakhorin.net ~]#
```

Рис. 2.9. Повторяем действия для соединения System eth0.

Перезапустим NetworkManager:

```
systemctl restart NetworkManager
```

Проверим наличие изменений в файле /etc/resolv.conf (рис. 2.10):



```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl restart NetworkManager  
[root@server.ismakhorin.net ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search ismakhorin.net  
nameserver 127.0.0.1  
[root@server.ismakhorin.net ~]#
```

Рис. 2.10. Перезапуск NetworkManager и проверка наличия изменений в файле /etc/resolv.conf.

Теперь нам требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server (рис. 2.11). Для этого внесём изменения в файл /etc/named.conf, заменив строку

listen-on port 53 { 127.0.0.1; }; на listen-on port 53 { 127.0.0.1; any; };

и строку

allow-query { localhost; }; на allow-query { localhost; 192.168.0.0/16; };

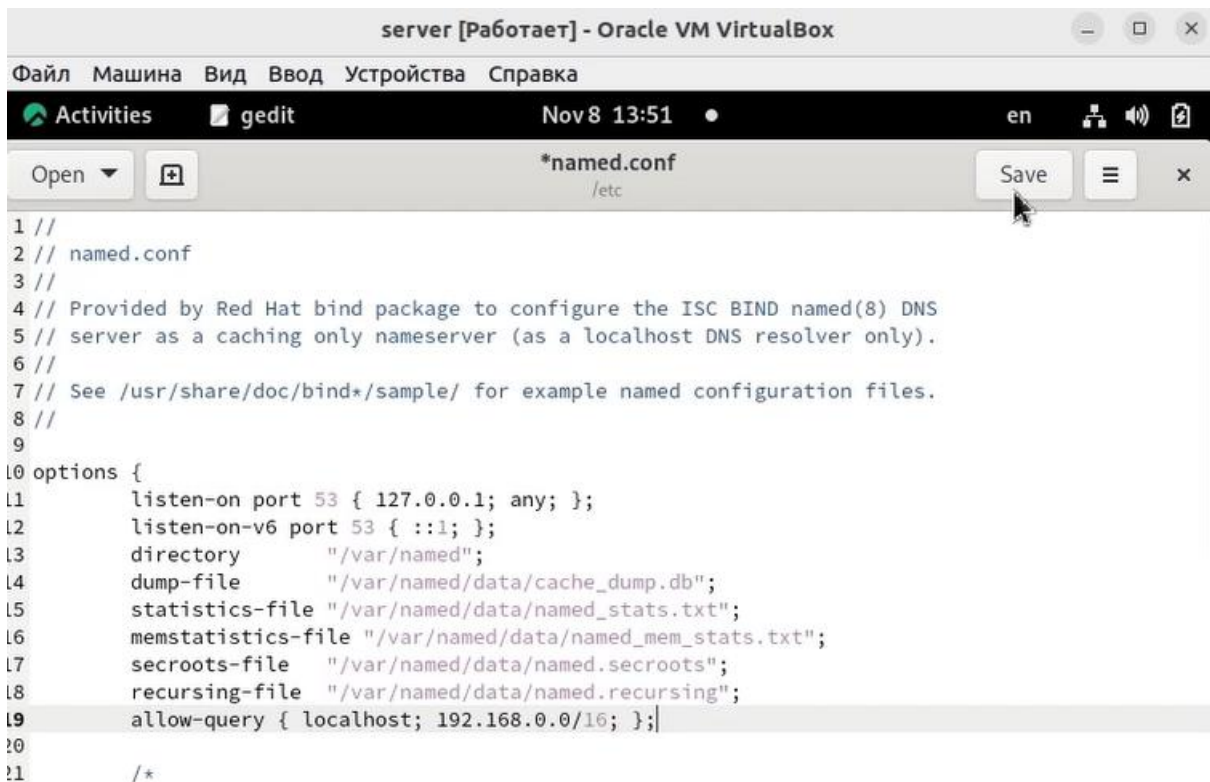


Рис. 2.11. Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server.

Внесём изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:

```
firewall-cmd --add-service=dns
```

```
firewall-cmd --add-service=dns --permanent
```

Убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используем команду `lsof` (рис. 2.12):

```
lsof | grep UDP
```

The screenshot shows a terminal window titled "server [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
root@server.ismakhorin.net ~]# firewall-cmd --add-service=dns
success
root@server.ismakhorin.net ~]# firewall-cmd --add-service=dns --permanent
success
root@server.ismakhorin.net ~]# sof | grep UDP
bash: sof: command not found...
root@server.ismakhorin.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
```

Process	PID	UID	IPV	Port	Proto	State
avahi-daemon	514	avahi	IPv4	18750	TCP	UD
*:mdns						
avahi-daemon	514	avahi	IPv6	18751	TCP	UD
*:mdns						
avahi-daemon	514	avahi	IPv4	18752	TCP	UD
*:47939						
avahi-daemon	514	avahi	IPv6	18753	TCP	UD
*:41710						
chronyd	540	chrony	IPv4	18688	TCP	UD
localhost:323						
chronyd	540	chrony	IPv6	18689	TCP	UD
localhost:323						
named	6266	named	IPv4	36178	TCP	UD
localhost:domain						
named	6266	named	IPv6	36180	TCP	UD
localhost:domain						
named 6266 6267 isc-net-0		named	IPv4	36178	TCP	UD
localhost:domain						
named 6266 6267 isc-net-0		named	IPv6	36180	TCP	UD
localhost:domain						
named 6266 6268 isc-timer		named	IPv4	36178	TCP	UD

Рис. 2.12. Внос изменений в настройки межсетевого экрана узла server, разрешив работу с DNS. Проверка, что DNS-запросы идут через узел server, который прослушивает порт 53.

В случае возникновения в сети ситуации, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер. Для этого в конфигурационный файл `named.conf` в секцию `options` добавим:

```
forwarders { список DNS-серверов };  
  
forward first;
```

Кроме того, возможно вышестоящий DNS-сервер может не поддерживать технологию DNSSEC, тогда в конфигурационном файле `named.conf` укажем следующие настройки (рис. 3):

dnssec-enable no;

dnssec-validation no;

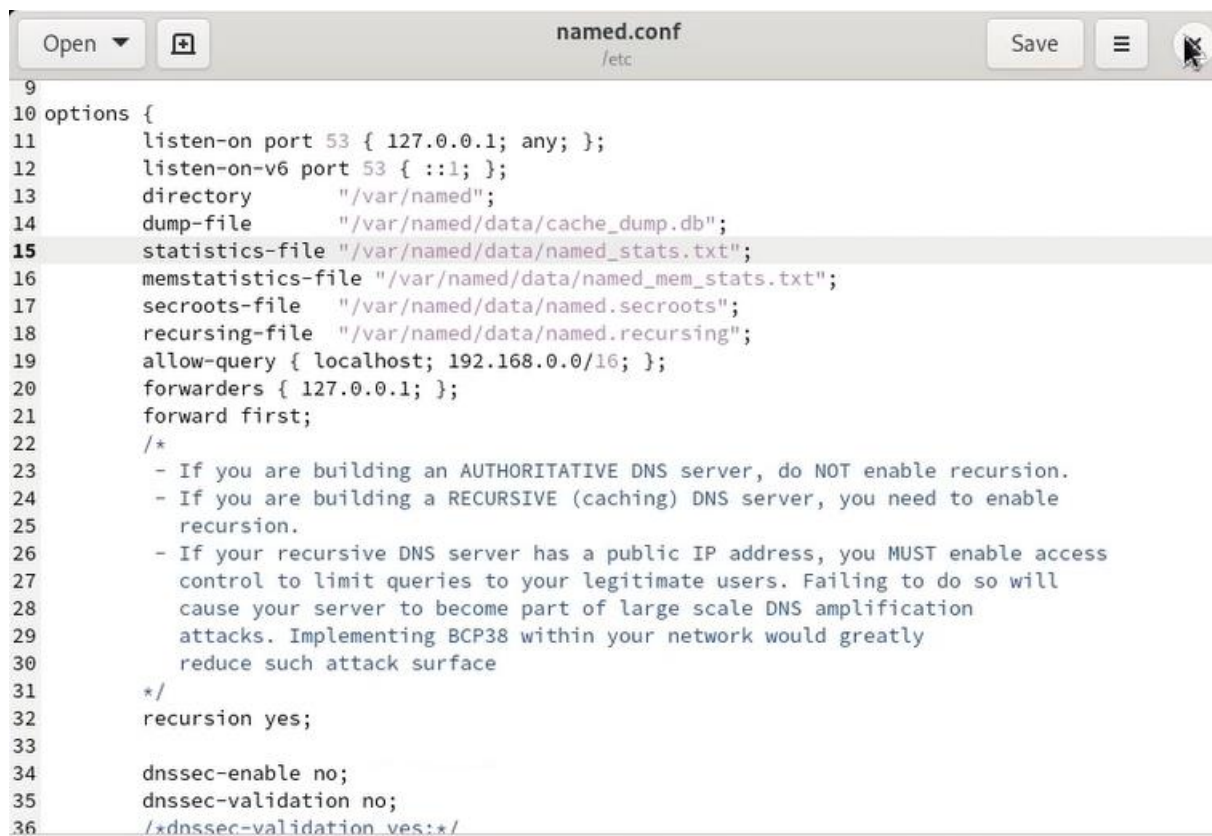


Рис. 3. Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек.

Скопируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуем его в ismakhorin.net (рис. 4.1):

```
cp /etc/named.rfc1912.zones /etc/named/
```

```
cd /etc/named
```

```
mv /etc/named/named.rfc1912.zones /etc/named/user.net
```

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

Рис. 4.1. Копирование шаблона описания DNS-зон из каталога /etc в каталог /etc/named и изменение его названия.

Включим файл описания зоны `/etc/named/ismakhorin.net` в конфигурационном файле DNS `/etc/named.conf`, добавив в нём в конце строку (рис. 4.2):

```
include "/etc/named/ismakhorin.net"
```

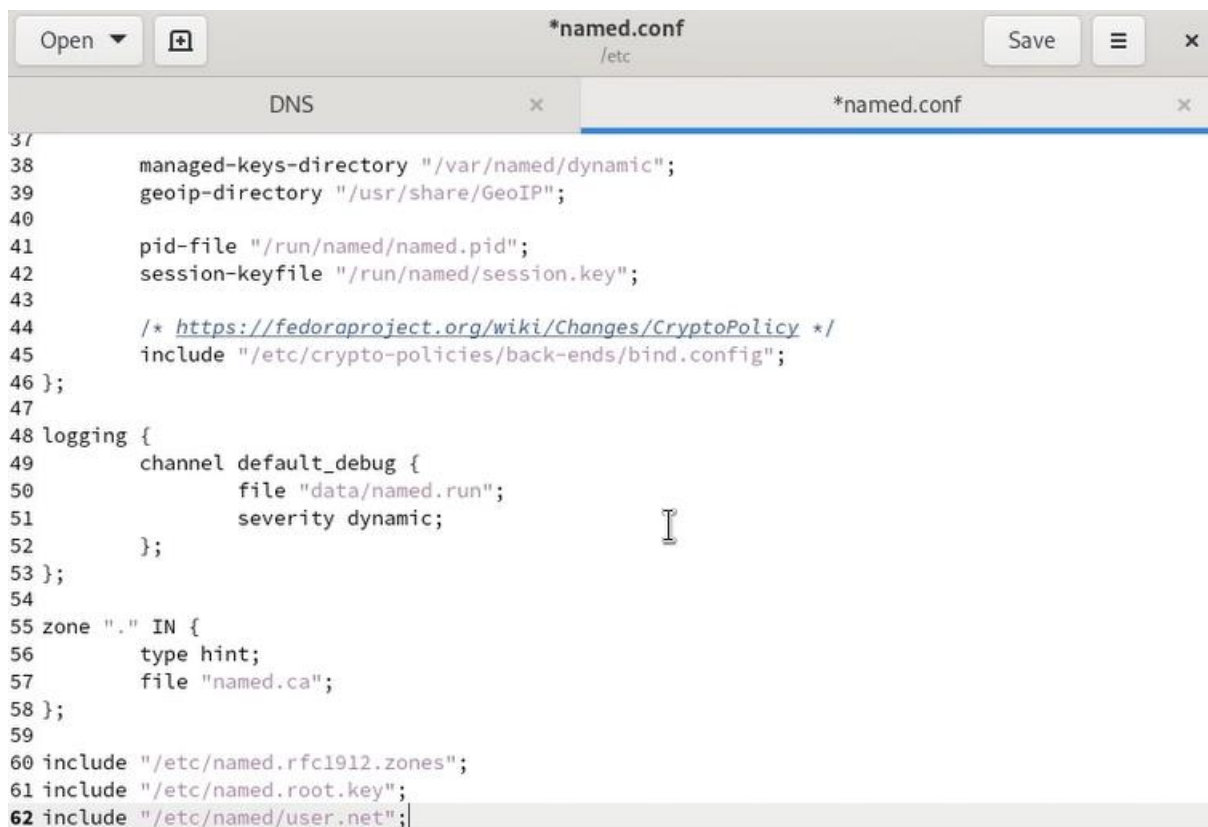
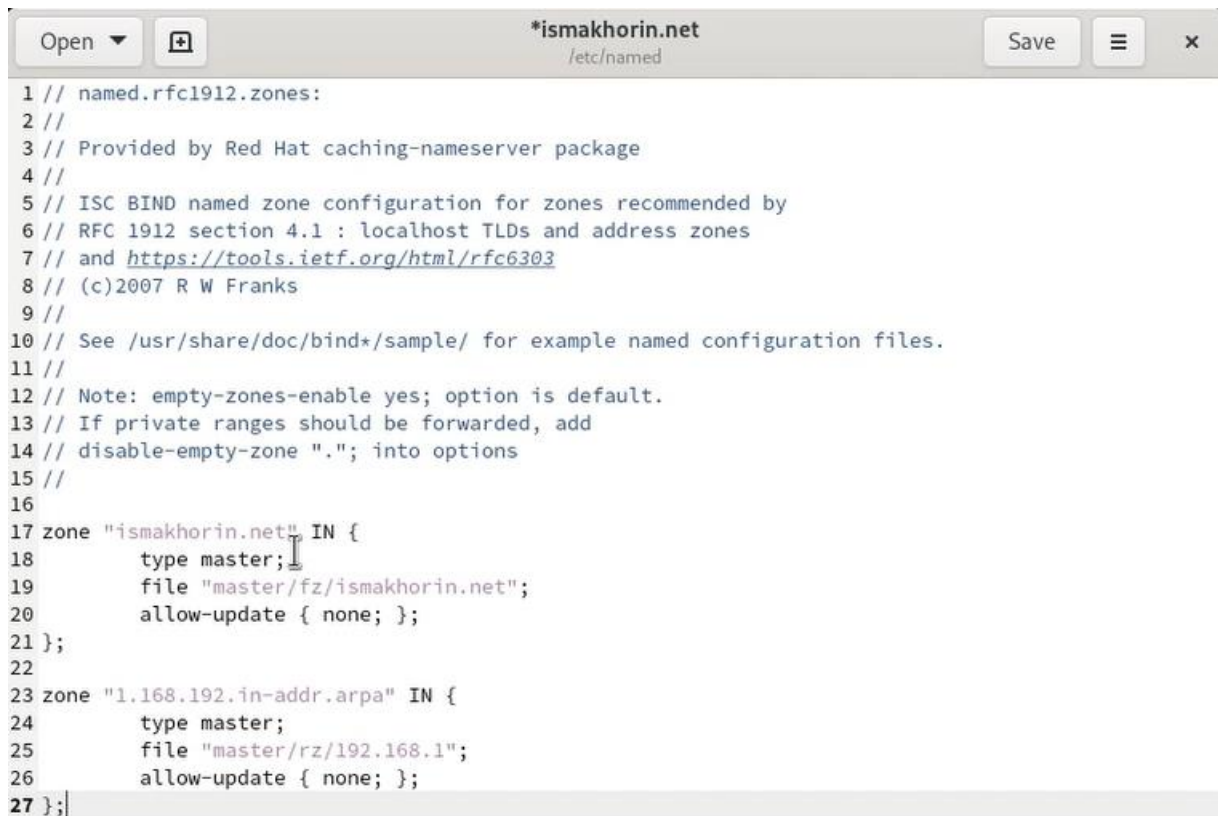


Рис. 4.2. Включение файла описания зоны `/etc/named/ismakhorin.net` в конфигурационном файле DNS `/etc/named.conf`.

Откроем файл `/etc/named/user.net` на редактирование и вместо зоны пропишем свою прямую зону. Далее, вместо зоны пропишем свою обратную зону. Остальные записи в файле `/etc/named/ismakhorin.net` удалим (рис. 4.3):



```
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ for example named configuration files.
11 //
12 // Note: empty-zones-enable yes; option is default.
13 // If private ranges should be forwarded, add
14 // disable-empty-zone "."; into options
15 //
16
17 zone "ismakhorin.net" IN {
18     type master;
19     file "master/fz/ismakhorin.net";
20     allow-update { none; };
21 };
22
23 zone "1.168.192.in-addr.arpa" IN {
24     type master;
25     file "master/rz/192.168.1";
26     allow-update { none; };
27 };
```

Рис. 4.3. Открытие файла /etc/named/user.net на редактирование.

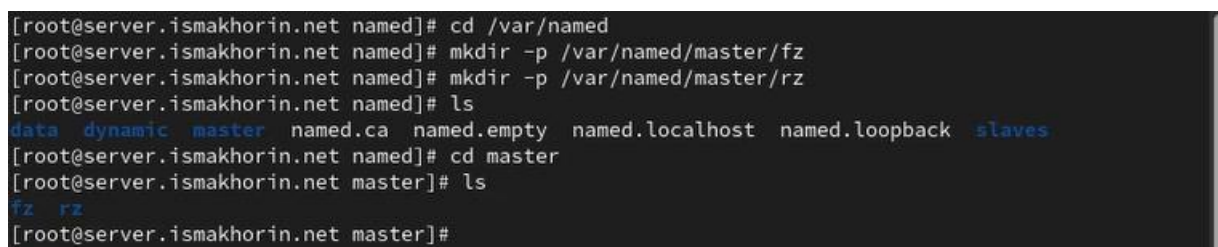
Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле.

В каталоге /var/named создадим подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно (рис. 4.4):

```
cd /var/named
```

```
mkdir -p /var/named/master/fz
```

```
mkdir -p /var/named/master/rz
```



```
[root@server.ismakhorin.net named]# cd /var/named
[root@server.ismakhorin.net named]# mkdir -p /var/named/master/fz
[root@server.ismakhorin.net named]# mkdir -p /var/named/master/rz
[root@server.ismakhorin.net named]# ls
data dynamic master named.ca named.empty named.localhost named.loopback slaves
[root@server.ismakhorin.net named]# cd master
[root@server.ismakhorin.net master]# ls
fz rz
[root@server.ismakhorin.net master]#
```

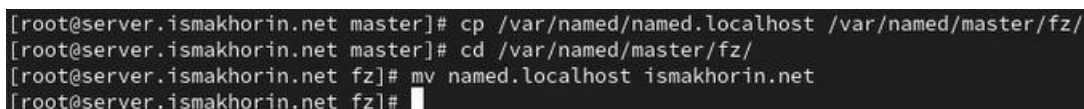
Рис. 4.4. В каталоге /var/named создание подкаталогов master/fz и master/rz.

Скопируем шаблон прямой DNS-зоны `named.localhost` из каталога `/var/named` в каталог `/var/named/master/fz` и переименуем его в `ismakhorin.net` (рис. 4.5):

```
cp /var/named/named.localhost /var/named/master/fz/
```

```
cd /var/named/master/fz/
```

```
mv named.localhost ismakhorin.net
```



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

Рис. 4.5. Копирование шаблона прямой DNS-зоны `named.localhost` из каталога `/var/named` в каталог `/var/named/master/fz` и изменение его названия.

Изменим файл `/var/named/master/fz/ismakhorin.net`, указав необходимые DNS записи для прямой зоны. В этом файле DNS-имя сервера `@ name.invalid.` заменим на `@ server.ismakhorin.net`. Формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии) [1]; адрес в А-записи заменим с `127.0.0.1` на `192.168.1.1`; в директиве `$ORIGIN` зададим текущее имя домена `ismakhorin.net`, а затем укажем имена и адреса серверов в этом домене в виде А-записей DNS (на данном этапе пропишем сервер с именем `ns` и адресом `192.168.1.1`) (рис. 4.6):



Рис. 4.6. Изменение файла /var/named/master/fz/ismakhorin.net, указав необходимые DNS записи для прямой зоны.

Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1 (рис. 4.7):

```
cp /var/named/named.loopback /var/named/master/rz/
```

```
cd /var/named/master/rz/
```

```
mv named.loopback 192.168.1
```

```

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

```

Рис. 4.7. Копирование шаблона обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и изменение его названия.

Изменим файл /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны. В этом файле DNS-имя сервера @ name.invalid заменим на @ server.ismakhorin.net. формат серийного номера ГТГТММДДВВ (ГТГТ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-записи заменим с 127.0.0.1 на 192.168.1.1; в директиве \$ORIGIN зададим название обратной зоны в виде 1.168.192.in-addr.arpa., затем зададим PTR-записи (на

данном этапе зададим PTR запись, ставящая в соответствие адресу 192.168.1.1 DNS-адрес ns.ismakhorin.net) (рис. 4.8):



Рис. 4.8. Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны.

Далее исправим права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать:

```
chown -R named:named /etc/named
```

```
chown -R named:named /var/named
```

В системах с запущенным SELinux все процессы и файлы имеют специальные метки безопасности (так называемый «контекст безопасности»), используемые системой для принятия решений по доступу к этим процессам и файлам. После изменения доступа к конфигурационным файлам named требуется корректно восстановить их метки в SELinux:

```
restorecon -vR /etc
```

```
restorecon -vR /var/named
```

Для проверки состояния переключателей SELinux, относящихся к named, введём:

```
getsebool -a | grep named
```

Теперь дадим named разрешение на запись в файлы DNS-зоны:

```
setsebool named_write_master_zones 1
```

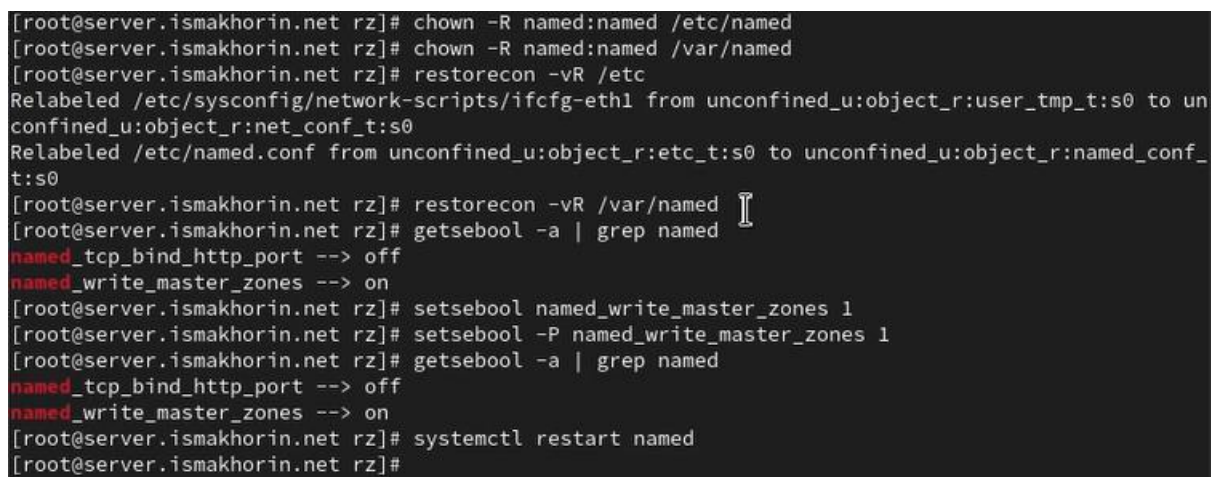
```
setsebool -P named_write_master_zones 1
```

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы (рис. 4.10):

```
journalctl -x -f
```

и в первом терминале перезапустим DNS-сервер (рис. 4.9):

```
systemctl restart named
```



```
[root@server.ismakhorin.net rz]# chown -R named:named /etc/named
[root@server.ismakhorin.net rz]# chown -R named:named /var/named
[root@server.ismakhorin.net rz]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
Relabeled /etc/named.conf from unconfined_u:object_r:etc_t:s0 to unconfined_u:object_r:named_conf_t:s0
[root@server.ismakhorin.net rz]# restorecon -vR /var/named
[root@server.ismakhorin.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ismakhorin.net rz]# setsebool named_write_master_zones 1
[root@server.ismakhorin.net rz]# setsebool -P named_write_master_zones 1
[root@server.ismakhorin.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ismakhorin.net rz]# systemctl restart named
[root@server.ismakhorin.net rz]#
```

Рис. 4.9. Исправление прав доступа к файлам в каталогах /etc/named и /var/named, корректное восстановление их меток в SELinux, проверка состояния переключателей SELinux и перезапуск DNS-сервера.

```
root@server:/var/named/master/rz x ismakhorin@server:~ — journalctl -x -f x
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 199.9.14.201#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 192.58.128.30#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 202.12.27.33#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 192.33.4.12#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 192.36.148.17#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 193.0.14.129#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 199.7.83.42#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 198.97.190.53#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 198.41.0.4#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 199.7.91.13#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:500:200::b#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: REFUSED unexpected RCODE resolving './NS/IN': 192.203.230.10#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Nov 08 15:20:19 server.ismakhorin.net named[7202]: resolver priming query complete
```

Рис. 4.10. Проверка корректности работы системы.

При помощи утилиты `dig` получим описание DNS-зоны с сервера `ns.ismakhorin.net` (рис. 5.1):

`dig ns.user.net`

```
[root@server.ismakhorin.net rz]# dig ns.ismakhorin.net
; <<>> DiG 9.16.23-RH <<>> ns.ismakhorin.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57595
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a2b29eac6c8ec79001000000654ba77d8cda777e2436d8e4 (good)
;; QUESTION SECTION:
;ns.ismakhorin.net.          IN      A
;; ANSWER SECTION:
ns.ismakhorin.net.          86400   IN      A      192.168.1.1
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 08 15:21:33 UTC 2023
;; MSG SIZE rcvd: 90
[root@server.ismakhorin.net rz]#
```

Рис. 5.1. Получение описания DNS-зоны с сервера `ns.ismakhorin.net`.

При помощи утилиты `host` проанализируем корректность работы DNS-сервера (рис. 5.2):

```
host -l ismakhorin.net
```

```
host -a ismakhorin.net
```

```
host -t A ismakhorin.net
```

```
host -t PTR 192.168.1.1
```

```
[root@server.ismakhorin.net rz]# host -l ismakhorin.net
ismakhorin.net name server ismakhorin.net.
ismakhorin.net has address 192.168.1.1
ns.ismakhorin.net has address 192.168.1.1
server.ismakhorin.net has address 192.168.1.1
[root@server.ismakhorin.net rz]# host -a ismakhorin.net
Trying "ismakhorin.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16164
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

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

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

Received 121 bytes from 127.0.0.1#53 in 2 ms
[root@server.ismakhorin.net rz]# host -t A ismakhorin.net
ismakhorin.net has address 192.168.1.1
[root@server.ismakhorin.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ismakhorin.net.
1.1.168.192.in-addr.arpa domain name pointer server.ismakhorin.net.
[root@server.ismakhorin.net rz]# clear
```

Рис. 5.2. Анализ корректности работы DNS-сервера.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS (рис. 6.1):

```
cd /vagrant
```

```
mkdir -p /vagrant/provision/server/dns/etc/named
```

```
mkdir -p /vagrant/provision/server/dns/var/named/master/
```

```
cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
```

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

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



```
[root@server.ismakhorin.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
cp: overwrite '/vagrant/provision/server/dns/etc/named.conf'? yes
[root@server.ismakhorin.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
cp: overwrite '/vagrant/provision/server/dns/etc/named/ismakhorin.net'? yes
[root@server.ismakhorin.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
cp: missing destination file operand after '/var/named/master/* /vagrant/provision/server/dns/var/named/master/'
Try 'cp --help' for more information.
[root@server.ismakhorin.net vagrant]# cp -R /var/named/master/ /vagrant/provision/server/dns/var/named/master/
[root@server.ismakhorin.net vagrant]#
```

Рис. 6.1. Переход в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `dns`, в который помещаем в соответствующие каталоги конфигурационные файлы DNS.

В каталоге `/vagrant/provision/server` создадим исполняемый файл `dns.sh` (рис. 6.2):

```
touch dns.sh
```

```
chmod +x dns.sh
```

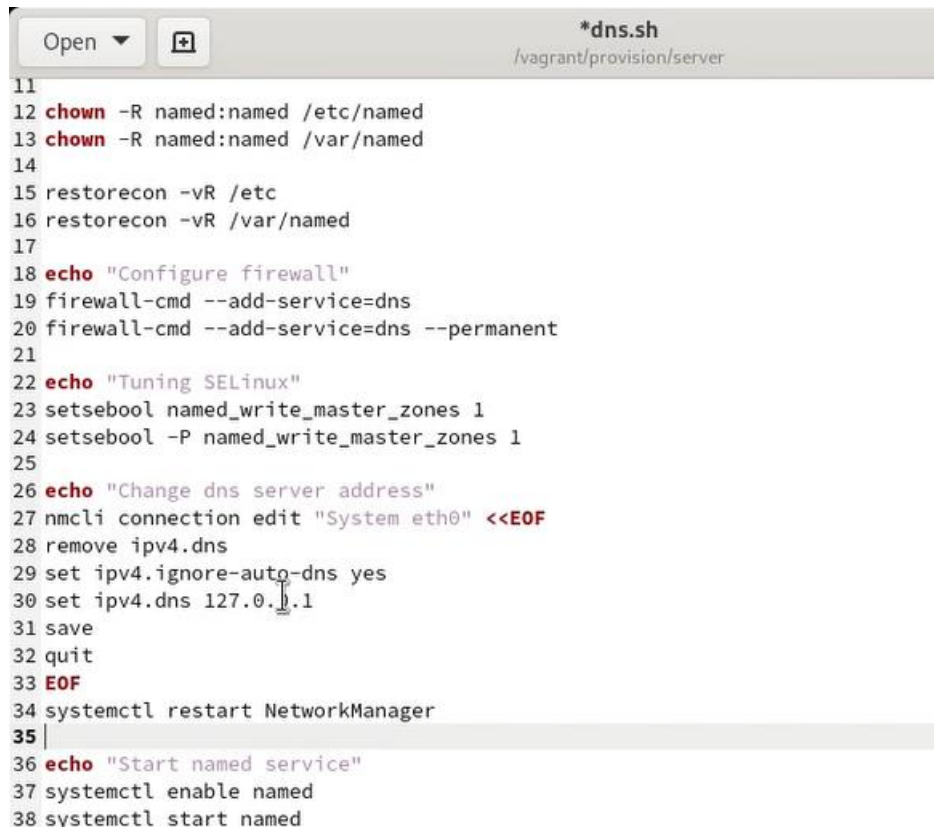
```
[root@server.ismakhorin.net server]# touch dns.sh
[root@server.ismakhorin.net server]# ls
@1-dummy.sh dns dns.sh
[root@server.ismakhorin.net server]# chmod +x dns.sh
[root@server.ismakhorin.net server]#
```

Рис. 6.2. Создание в каталоге `/vagrant/provision/server` исполняемого файла `dns.sh`.

Откроем его на редактирование и пропишем в нём следующий скрипт (приведён в лабораторной работе). Этот скрипт, по сути, повторяет произведённые нами действия по установке и настройке DNS-сервера (рис. 6.3):

1. подставляет в нужные каталоги подготовленные вами конфигурационные файлы;
2. меняет соответствующим образом права доступа, метки безопасности SELinux и правила межсетевого экрана;

3. настраивает сетевое соединение так, чтобы сервер выступал DNS-сервером по умолчанию для узлов внутренней виртуальной сети;
4. запускает DNS-сервер;

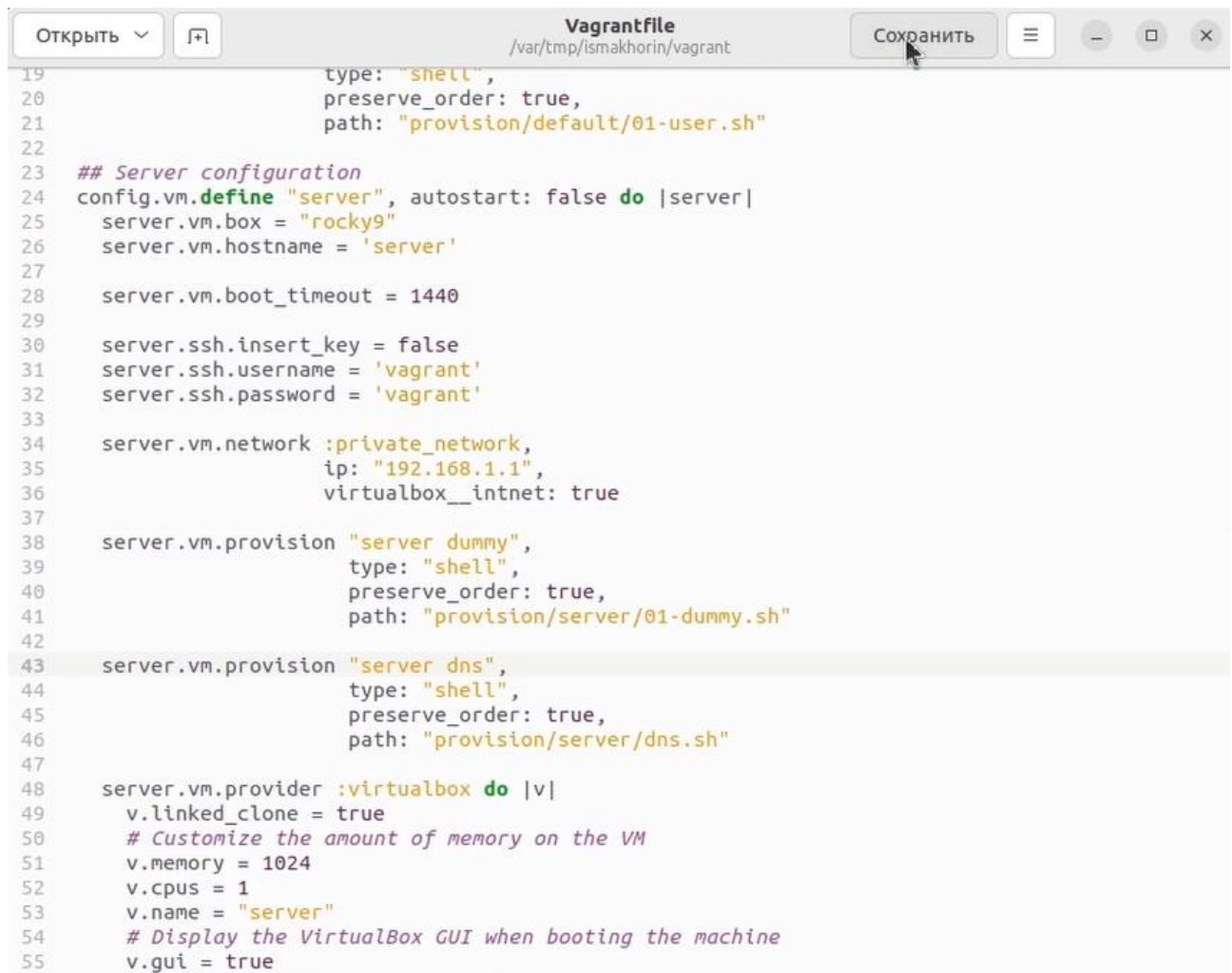


```
*dns.sh
/vagrant/provision/server

11
12 chown -R named:named /etc/named
13 chown -R named:named /var/named
14
15 restorecon -vR /etc
16 restorecon -vR /var/named
17
18 echo "Configure firewall"
19 firewall-cmd --add-service=dns
20 firewall-cmd --add-service=dns --permanent
21
22 echo "Tuning SELinux"
23 setsebool named_write_master_zones 1
24 setsebool -P named_write_master_zones 1
25
26 echo "Change dns server address"
27 nmcli connection edit "System eth0" <<EOF
28 remove ipv4.dns
29 set ipv4.ignore-auto-dns yes
30 set ipv4.dns 127.0.0.1
31 save
32 quit
33 EOF
34 systemctl restart NetworkManager
35
36 echo "Start named service"
37 systemctl enable named
38 systemctl start named
```

Рис. 6.3. Открытие файла на редактирование и прописывание в нём скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле Vagrantfile добавим определённые параметры в разделе конфигурации для сервера (рис. 6.4):

The image shows a text editor window titled 'Vagrantfile' with the path '/var/tmp/ismakhorin/vagrant'. The editor contains a Vagrant configuration file. Line 19-22 shows a shell provisioner configuration. Line 23 is a comment '## Server configuration'. Line 24 starts a 'config.vm.define' block for 'server'. Lines 25-26 set 'server.vm.box' to 'rocky9' and 'server.vm.hostname' to 'server'. Line 27 sets 'server.vm.boot_timeout' to 1440. Line 30 sets 'server.ssh.insert_key' to false. Lines 31-32 set 'server.ssh.username' and 'server.ssh.password' to 'vagrant'. Line 33 is a comment. Line 34 sets 'server.vm.network' to 'private_network'. Lines 35-36 set 'ip' to '192.168.1.1' and 'virtualbox__intnet' to true. Line 37 is a comment. Line 38 sets 'server.vm.provision' to 'server dummy'. Lines 39-42 set 'type' to 'shell', 'preserve_order' to true, and 'path' to 'provision/server/01-dummy.sh'. Line 43 sets 'server.vm.provision' to 'server dns'. Lines 44-46 set 'type' to 'shell', 'preserve_order' to true, and 'path' to 'provision/server/dns.sh'. Line 47 is a comment. Line 48 sets 'server.vm.provider' to 'virtualbox'. Lines 49-55 set 'v.linked_clone' to true, add a comment '# Customize the amount of memory on the VM', set 'v.memory' to 1024, 'v.cpus' to 1, 'v.name' to 'server', add a comment '# Display the VirtualBox GUI when booting the machine', and set 'v.gui' to true.

```
19         type: "shell",
20         preserve_order: true,
21         path: "provision/default/01-user.sh"
22
23     ## Server configuration
24     config.vm.define "server", autostart: false do |server|
25       server.vm.box = "rocky9"
26       server.vm.hostname = 'server'
27
28       server.vm.boot_timeout = 1440
29
30       server.ssh.insert_key = false
31       server.ssh.username = 'vagrant'
32       server.ssh.password = 'vagrant'
33
34       server.vm.network :private_network,
35         ip: "192.168.1.1",
36         virtualbox__intnet: true
37
38       server.vm.provision "server dummy",
39         type: "shell",
40         preserve_order: true,
41         path: "provision/server/01-dummy.sh"
42
43       server.vm.provision "server dns",
44         type: "shell",
45         preserve_order: true,
46         path: "provision/server/dns.sh"
47
48       server.vm.provider :virtualbox do |v|
49         v.linked_clone = true
50         # Customize the amount of memory on the VM
51         v.memory = 1024
52         v.cpus = 1
53         v.name = "server"
54         # Display the VirtualBox GUI when booting the machine
55         v.gui = true
```

Рис. 6.4. Добавление параметров в конфигурационном файле Vagrantfile в разделе конфигурации для сервера.

Вывод:

В ходе выполнения лабораторной работы были приобретены практические навыки по установке и конфигурированию DNS-сервера, а также усвоили принципы работы системы доменных имён.

Ответы на контрольные вопросы:

1. Что такое DNS? - Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса, используемые компьютерами для идентификации друг друга в сети.

2. Каково назначение кэширующего DNS-сервера? - Его задача - хранить результаты предыдущих DNS-запросов в памяти. Когда клиент делает запрос, кэширующий DNS проверяет свой кэш, и если он содержит соответствующую информацию, сервер возвращает ее без необходимости обращаться к другим DNS-серверам. Это ускоряет процесс запроса.
3. Чем отличается прямая DNS-зона от обратной? - Прямая зона преобразует доменные имена в IP-адреса, обратная зона выполняет обратное: преобразует IP-адреса в доменные имена.
4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают. - В Linux-системах обычно используется файл `/etc/named.conf` для общих настроек. Зоны хранятся в файлах в каталоге `/var/named/`, например, `/var/named/example.com.zone`.
5. Что указывается в файле `resolv.conf`? - Содержит информацию о DNS-серверах, используемых системой, а также о параметрах конфигурации.
6. Какие типы записи описания ресурсов есть в DNS и для чего они используются? - A (IPv4-адрес), AAAA (IPv6-адрес), CNAME (каноническое имя), MX (почтовый сервер), NS (имя сервера), PTR (обратная запись), SOA (начальная запись зоны), TXT (текстовая информация).
7. Для чего используется домен `in-addr.arpa`? - Используется для обратного маппинга IP-адресов в доменные имена.
8. Для чего нужен демон `named`? - Это DNS-сервер, реализация BIND (Berkeley Internet Name Domain).
9. В чём заключаются основные функции slave-сервера и master-сервера? - Master-сервер хранит оригинальные записи зоны, slave-серверы получают копии данных от master-сервера.
10. Какие параметры отвечают за время обновления зоны? - `refresh`, `retry`, `expire`, и `minimum`.

11. Как обеспечить защиту зоны от скачивания и просмотра? - Это может включать в себя использование TSIG (Transaction SIGnatures) для аутентификации между серверами.
12. Какая запись RR применяется при создании почтовых серверов? - MX (Mail Exchange).
13. Как протестировать работу сервера доменных имён? - Используйте команды nslookup, dig, или host.
14. Как запустить, перезапустить или остановить какую-либо службу в системе? - `systemctl start|stop|restart <service>`.
15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы? - Используйте опции, такие как `-d` или `-v` при запуске службы.
16. Где храниться отладочная информация по работе системы и служб? Как её посмотреть? - В системных журналах, доступных через `journalctl`.
17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров. - `lsuf -p <pid>` или `fuser -v <file>`.
18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса `nmcli`. - Примеры включают `nmcli connection up|down <connection_name>`.
19. Что такое SELinux? - Это мандатный контроль доступа для ядра Linux.
20. Что такое контекст (метка) SELinux? - Метка, определяющая, какие ресурсы могут быть доступны процессу или объекту.
21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы? - `restorecon -Rv <directory>`.
22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций? - Используйте `audit2allow`.

- 23.Что такое булевый переключатель в SELinux? - Это параметр, который включает или отключает определенные аспекты защиты SELinux.
- 24.Как посмотреть список переключателей SELinux и их состояние? -
getsebool -a.
- 25.Как изменить значение переключателя SELinux? - setsebool -P
<boolean_name> <on|off>.