

Лабораторная работа №2

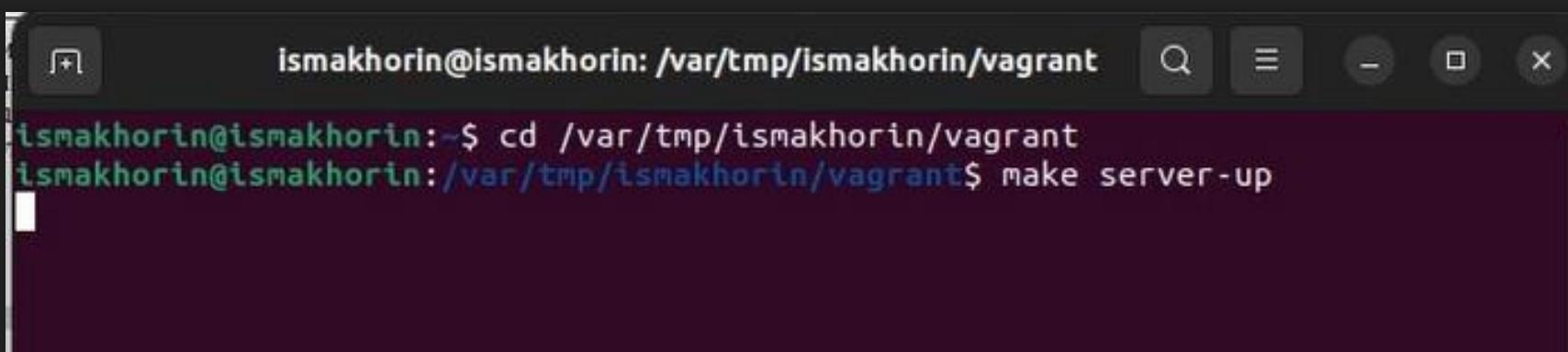
Настройка DNS-сервера

Махорин Иван Сергеевич

1032211221

НПИБд-02-21

Установка DNS-сервера



A screenshot of a terminal window with a dark background and light-colored text. The terminal title bar reads "ismakhorin@ismakhorin: /var/tmp/ismakhorin/vagrant". The main area of the terminal shows the command:

```
ismakhorin@ismakhorin:~$ cd /var/tmp/ismakhorin/vagrant  
ismakhorin@ismakhorin:/var/tmp/ismakhorin/vagrant$ make server-up
```

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

Установка DNS-сервера



server [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Activities Terminal Nov 8 13:39 ● en

root@server:~

```
[ismakhorin@server.ismakhorin.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 ismakhorin:
[root@server.ismakhorin.net ~]# dnf -y install bind bind-utils
Rocky Linux 9 - BaseOS      [===[--- B/s | 0 B --:-- ETA
```

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

Установка DNS-сервера

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

; <>> DiG 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45295
;; 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      77.88.55.60
www.yandex.ru.      3600    IN      A      5.255.255.77
www.yandex.ru.      3600    IN      A      77.88.55.88

;; Query time: 14 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Wed Nov 08 13:40:03 UTC 2023
;; MSG SIZE  rcvd: 95

[root@server.ismakhорин.net ~]#
```

Рис. 1.3. Запрос с помощью утилиты dig.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

```
[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.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

```
[root@server.ismakhori.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.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

```
[root@server.ismakhorin.net ~]# cat /var/named/named.localhost
$TTL 1D
@      IN SOA  @ rname.invalid. (
                           0      ; serial
                           10     ; 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.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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`.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

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

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

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

Рис. 2.9. Повторяем действия для соединения System eth0.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

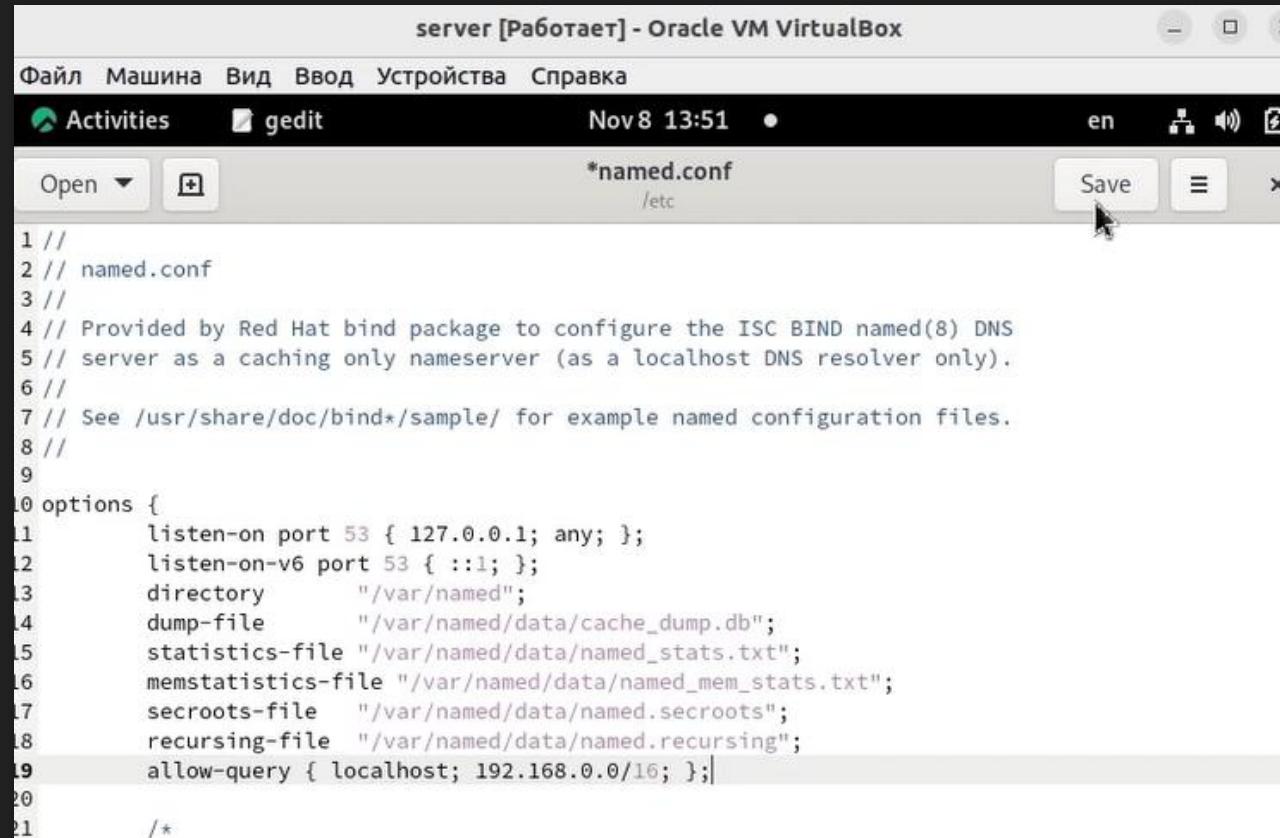


A screenshot of a terminal window titled "root@server:~". The window contains the following text:

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

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

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



The screenshot shows a Linux desktop environment with a window titled "server [Работает] - Oracle VM VirtualBox". The window contains a terminal or configuration editor showing the contents of the "/etc/named.conf" file. The file is a named configuration for an ISC BIND DNS server. The configuration includes options for listening on port 53 (IPv4 and IPv6), setting the directory to "/var/named", defining dump and statistics files, and specifying security roots and recursing files. A specific line of code is highlighted: "allow-query { localhost; 192.168.0.0/16; };". This line allows queries from the local host and from the 192.168.0.0/16 network range. The "Save" button is visible in the top right corner of the window.

```
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; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory      "/var/named";
14     dump-file      "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file  "/var/named/data/named.secroots";
18     recursing-file "/var/named/data/named.recurse";
19     allow-query { localhost; 192.168.0.0/16; };
20
21 }
```

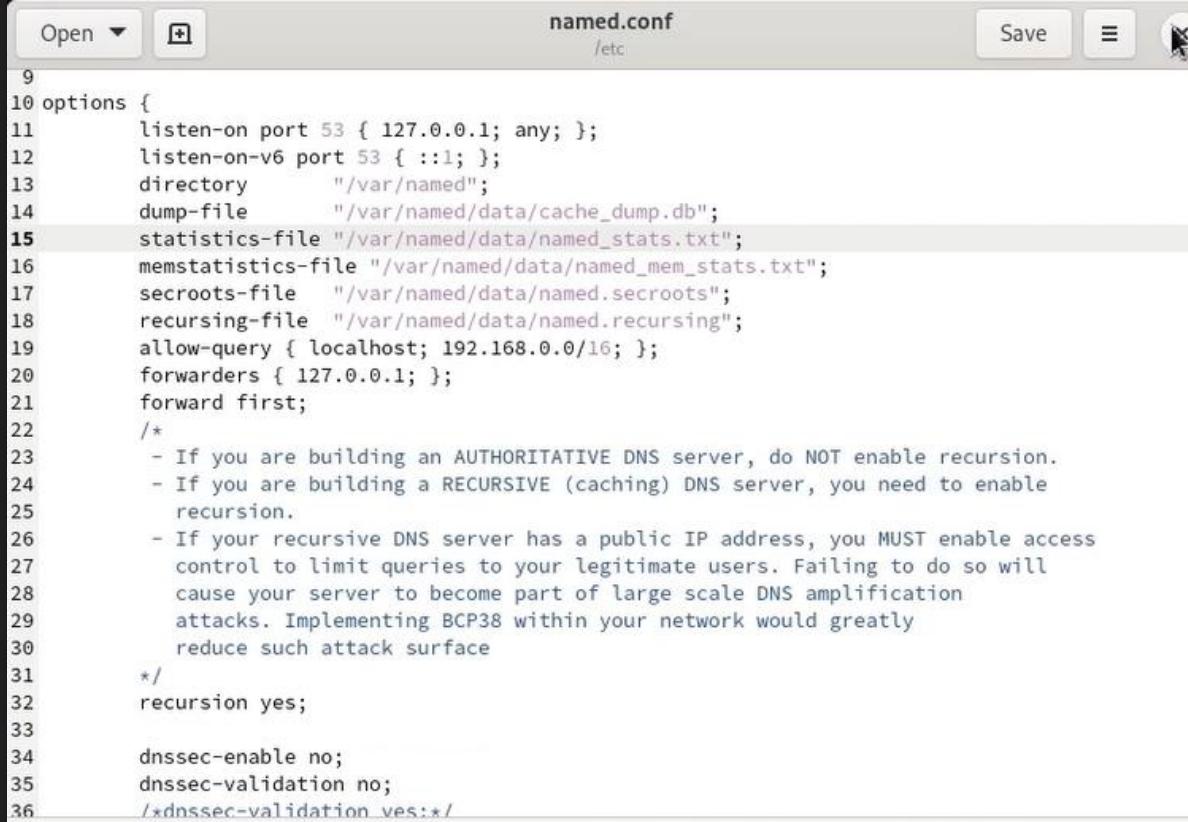
Рис. 2.11. Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server.

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

```
[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.
avahi-dae 514 avahi 12u IPv4 18750 0t0 UD
> *:mdns
avahi-dae 514 avahi 13u IPv6 18751 0t0 UD
> *:mdns
avahi-dae 514 avahi 14u IPv4 18752 0t0 UD
> *:47939
avahi-dae 514 avahi 15u IPv6 18753 0t0 UD
> *:41710
chronyd 540 chrony 5u IPv4 18688 0t0 UD
> localhost:323
chronyd 540 chrony 6u IPv6 18689 0t0 UD
named 6266 named 16u IPv4 36178 0t0 UD
> localhost:domain
named 6266 named 19u IPv6 36180 0t0 UD
> localhost:domain
named 6266 6267 isc-net-0 named 16u IPv4 36178 0t0 UD
> localhost:domain
named 6266 6267 isc-net-0 named 19u IPv6 36180 0t0 UD
> localhost:domain
named 6266 6268 isc-timer named 16u IPv4 36178 0t0 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.

Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



The screenshot shows a text editor window with the title bar "named.conf /etc". The file content is a configuration for a DNS server, specifically a caching server. The configuration includes options for listening on port 53, setting a directory for data, defining a dump file, and specifying statistics files. It also includes sections for recursion and forwarders, and a note about recursion. The file ends with a dnssec-enable and dnssec-validation directive.

```
9
10 options {
11     listen-on port 53 { 127.0.0.1; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory      "/var/named";
14     dump-file      "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file   "/var/named/data/named.secroots";
18     recursing-file  "/var/named/data/named.recursing";
19     allow-query { localhost; 192.168.0.0/16; };
20     forwarders { 127.0.0.1; };
21     forward first;
22     /*
23      - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
24      - If you are building a RECURSIVE (caching) DNS server, you need to enable
25        recursion.
26      - If your recursive DNS server has a public IP address, you MUST enable access
27        control to limit queries to your legitimate users. Failing to do so will
28        cause your server to become part of large scale DNS amplification
29        attacks. Implementing BCP38 within your network would greatly
30        reduce such attack surface
31     */
32     recursion yes;
33
34     dnssec-enable no;
35     dnssec-validation no;
36     /*dnssec-validation yes;*/
```

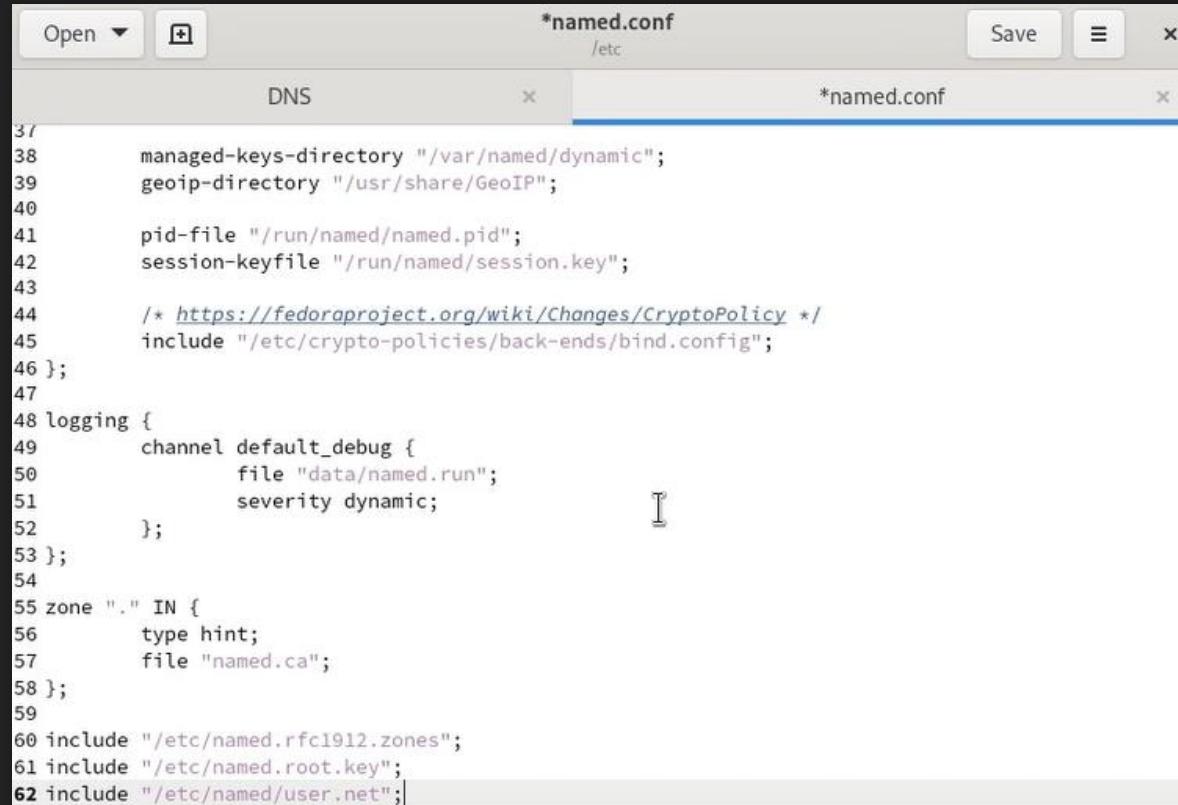
Рис. 3. Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек.

Конфигурирование первичного DNS-сервера

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

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

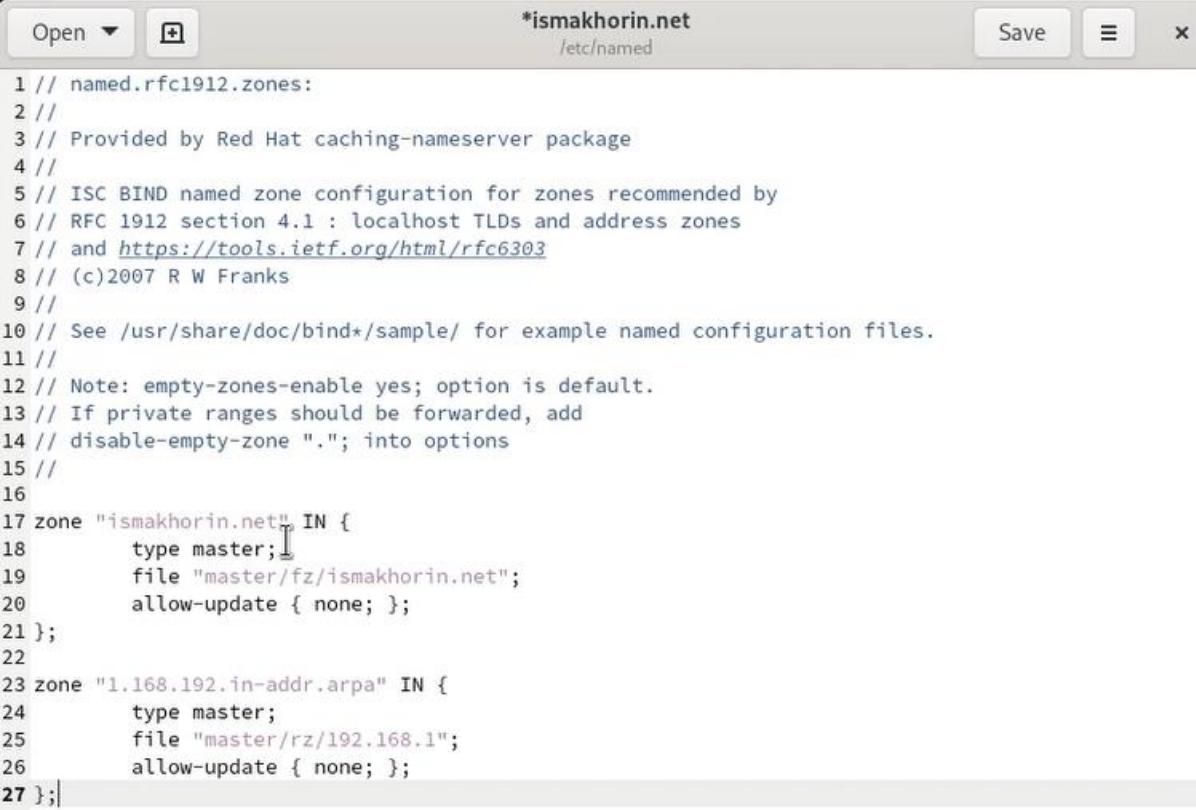
Конфигурирование первичного DNS-сервера



```
*named.conf
/etc
Save ×
DNS × *named.conf ×
37     managed-keys-directory "/var/named/dynamic";
38     geoip-directory "/usr/share/GeoIP";
39
40     pid-file "/run/named/named.pid";
41     session-keyfile "/run/named/session.key";
42
43     /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
44     include "/etc/crypto-policies/back-ends/bind.config";
45   };
46
47   logging {
48     channel default_debug {
49       file "data/named.run";
50       severity dynamic;
51     };
52   };
53
54
55 zone "." IN {
56   type hint;
57   file "named.ca";
58 };
59
60 include "/etc/named.rfc1912.zones";
61 include "/etc/named.root.key";
62 include "/etc/named/user.net";
```

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

Конфигурирование первичного DNS-сервера



The screenshot shows a text editor window titled '*ismakhorin.net /etc/named'. The file contains a BIND named configuration for a local zone. The configuration includes comments about RFC 1912 zones and a copyright notice. It defines two zones: 'ismakhorin.net' (IN) and '1.168.192.in-addr.arpa' (IN). Both zones are set to type 'master' and have their respective files and update permissions defined.

```
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.

Конфигурирование первичного DNS-сервера

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

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

Конфигурирование первичного DNS-сервера

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

Конфигурирование первичного DNS-сервера



The screenshot shows a text editor window with the title bar "*ismakhorin.net /var/named/master/fz". The window contains the following DNS zone configuration:

```
1 $TTL 1D
2 @      IN SOA  @ server.ismakhorin.net. (
3                               2020110500      ; serial
4                               1D              ; refresh
5                               1H              ; retry
6                               1W              ; expire
7                               3H )            ; minimum
8       NS    @
9       A     192.168.1.1
10 $ORIGIN ismakhorin.net.
11 server A     192.168.1.1
12 ns    A     192.168.1.1|
```

The configuration includes a SOA record for the zone, an NS record pointing to the server, and two A records for the server and a secondary name 'ns'.

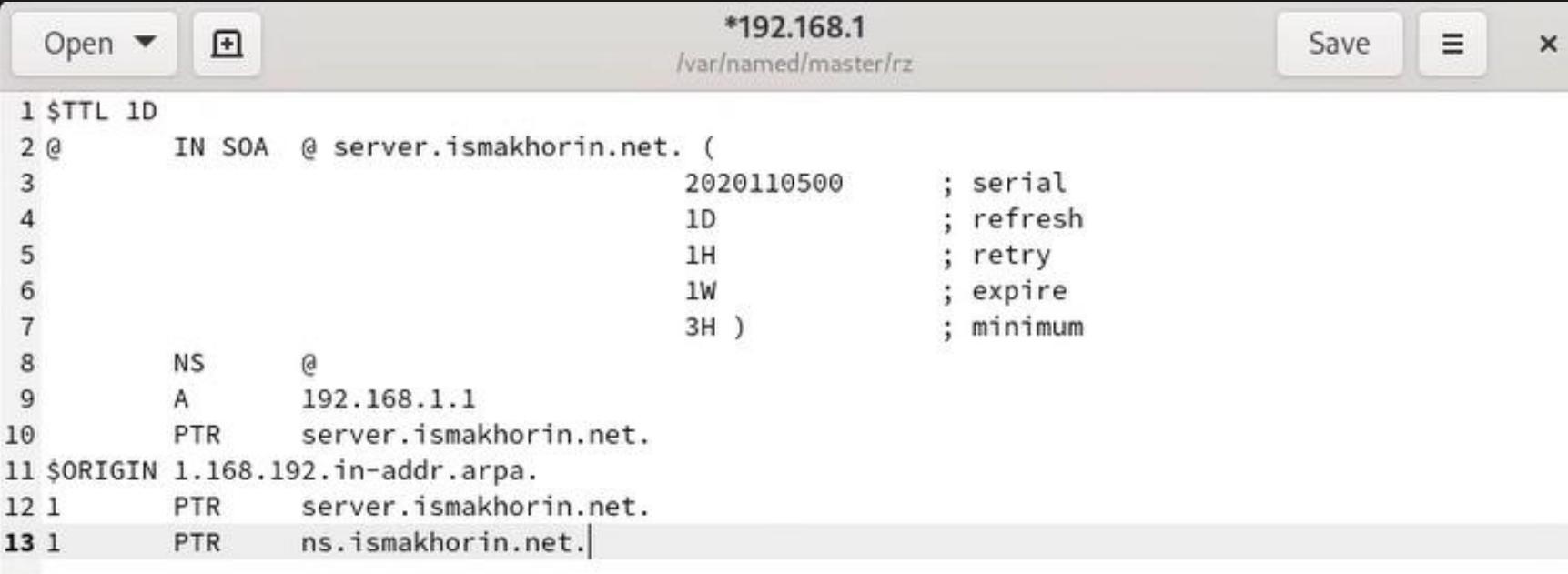
Рис. 4.6. Изменение файла /var/named/master/fz/ismakhorin.net, указав необходимые DNS записи для прямой зоны.

Конфигурирование первичного DNS-сервера

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

Конфигурирование первичного DNS-сервера



The screenshot shows a terminal window with the following details:

- WindowTitle: *192.168.1
- WorkingDir: /var/named/master/rz
- Buttons: Open, Save, and Close.

The content of the terminal window is a DNS zone file:

```
1 $TTL 1D
2 @      IN SOA  @ server.ismakhordin.net. (
3                               2020110500      ; serial
4                               1D              ; refresh
5                               1H              ; retry
6                               1W              ; expire
7                               3H )            ; minimum
8       NS    @
9       A     192.168.1.1
10      PTR   server.ismakhordin.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1      PTR   server.ismakhordin.net.
13 1      PTR   ns.ismakhordin.net.|
```

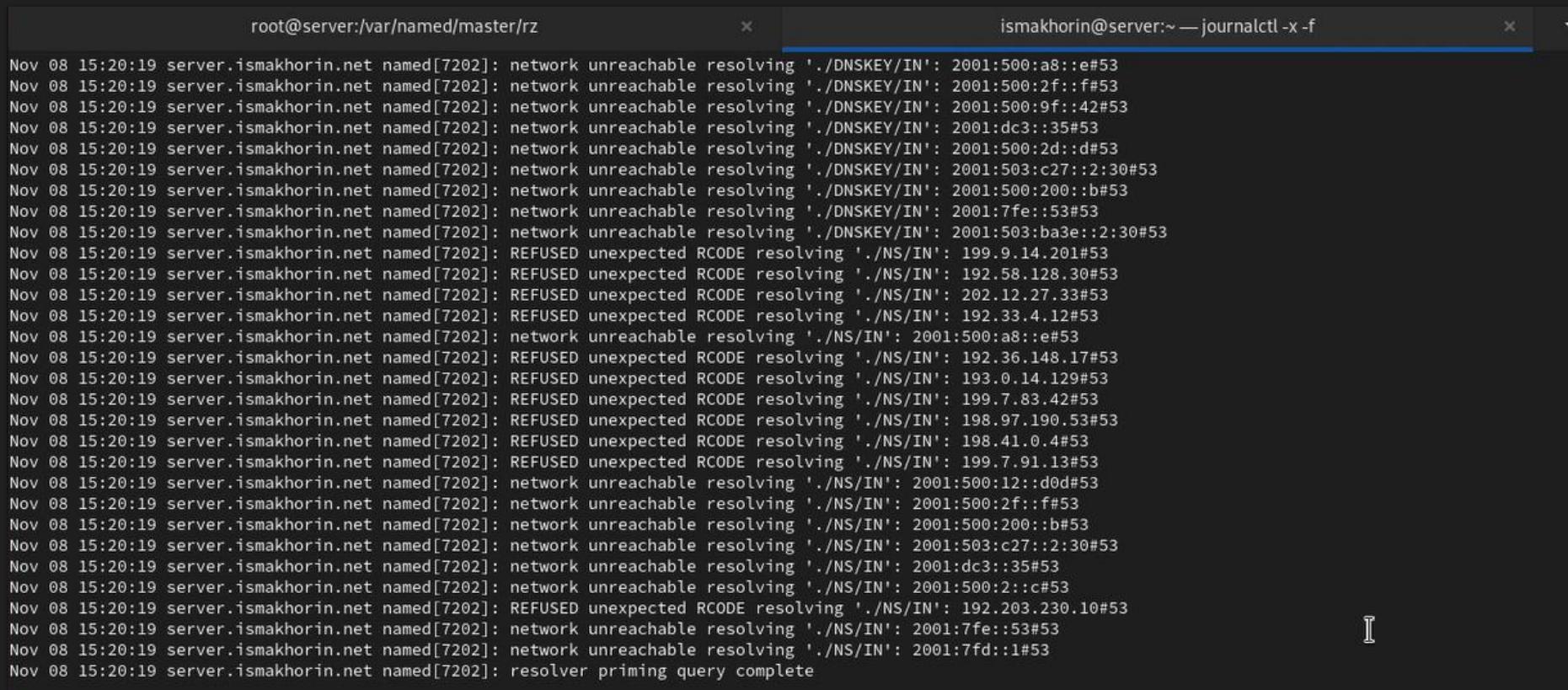
Рис. 4.8. Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны.

Конфигурирование первичного DNS-сервера

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

Конфигурирование первичного DNS-сервера



The screenshot shows two terminal windows side-by-side. The left window is titled 'root@server:/var/named/master/rz' and displays a log of DNS queries from the 'named' process. The right window is titled 'ismakhorin@server:~ — journalctl -x -f' and shows the system's journal logs. Both logs are timestamped 'Nov 08 15:20:19'.

```
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: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.

Анализ работы DNS-сервера

```
[root@server.ismakhori.net rz]# dig ns.ismakhori.net

; <>> DiG 9.16.23-RH <>> ns.ismakhori.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.ismakhori.net.          IN      A

;; ANSWER SECTION:
ns.ismakhori.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.ismakhori.net rz]#
```

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

Анализ работы DNS-сервера

```
[root@server.ismakhорин.net rz]# host -l ismakhорин.net
ismakhорин.net name server ismakhорин.net.
ismakhорин.net has address 192.168.1.1
ns.ismakhорин.net has address 192.168.1.1
server.ismakhорин.net has address 192.168.1.1
[root@server.ismakhорин.net rz]# host -a ismakhорин.net
Trying "ismakhорин.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16164
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;ismakhорин.net.          IN      ANY
;; ANSWER SECTION:
ismakhорин.net.    86400   IN      SOA     ismakhорин.net. server.ismakhорин.net. 2020110500 86400 3600 604800 10800
ismakhорин.net.    86400   IN      NS      ismakhорин.net.
ismakhорин.net.    86400   IN      A       192.168.1.1
;; ADDITIONAL SECTION:
ismakhорин.net.    86400   IN      A       192.168.1.1

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

Рис. 5.2. Анализ корректности работы DNS-сервера.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[root@server.ismakhорин.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
cp: overwrite '/vagrant/provision/server/dns/etc/named.conf'? yes
[root@server.ismakhорин.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
cp: overwrite '/vagrant/provision/server/dns/etc/named/ismakhорин.net'? yes
[root@server.ismakhорин.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.ismakhорин.net vagrant]# cp -R /var/named/master/ /vagrant/provision/server/dns/var/named/master/
[root@server.ismakhорин.net vagrant]# █
```

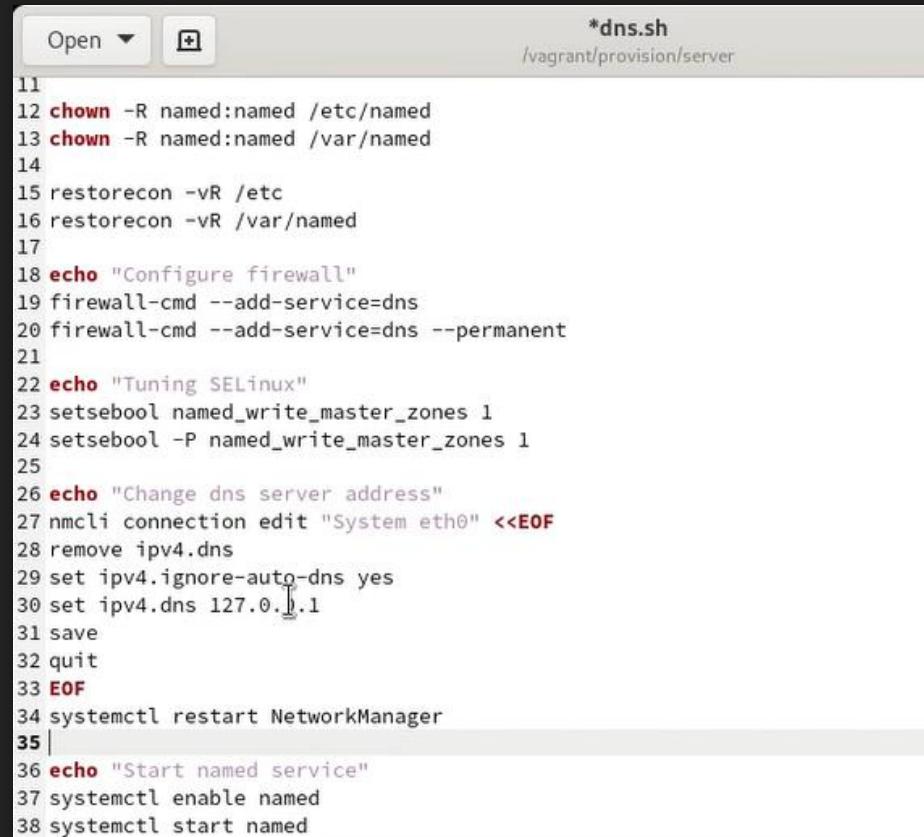
Рис. 6.1. Переход в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога dns, в который помещаем в соответствующие каталоги конфигурационные файлы DNS.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[root@server.ismakhorin.net server]# touch dns.sh
[root@server.ismakhorin.net server]# ls
01-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.

Внесение изменений в настройки внутреннего окружения виртуальной машины

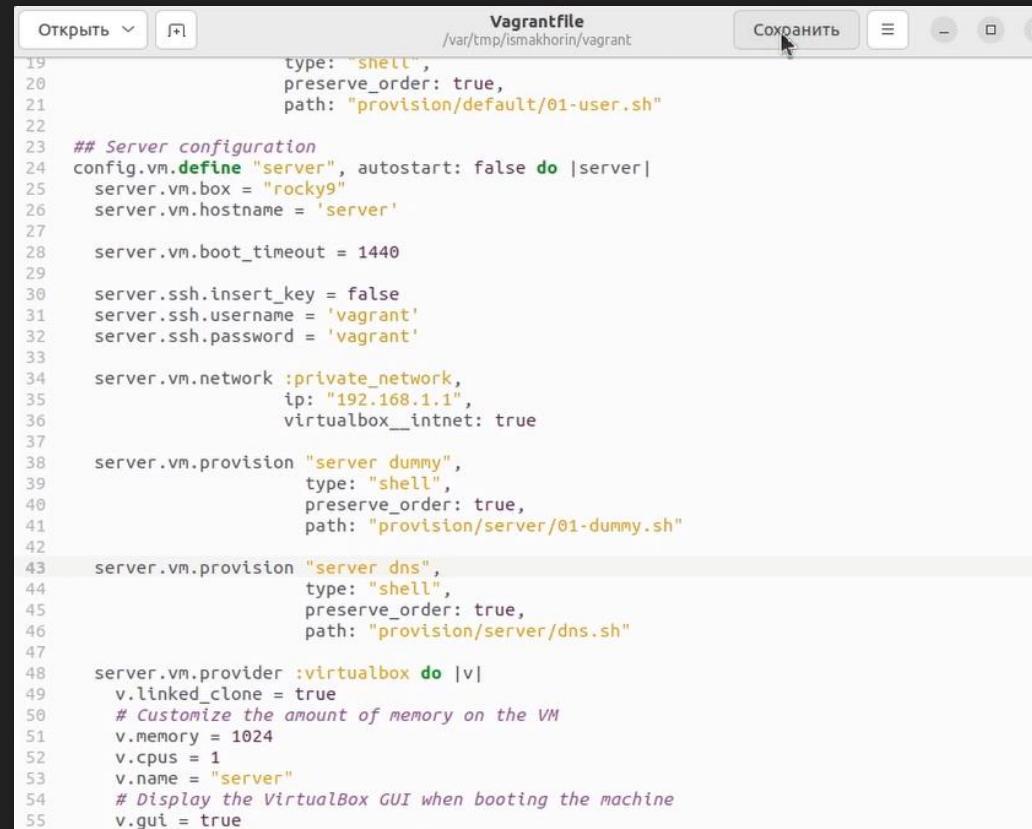


The screenshot shows a terminal window with the title bar "dns.sh" and the path "/vagrant/provision/server". The window contains a script with numbered lines from 11 to 38. Lines 11 through 14 show standard Linux file permissions. Lines 15 and 16 involve the "restorecon" command. Lines 17 through 21 involve configuring a firewall. Lines 22 and 23 involve setting SELinux boolean values. Lines 24 and 25 involve changing network connection settings. Lines 26 through 30 involve modifying IPv4 settings. Line 31 involves saving changes. Lines 32 and 33 involve exiting the configuration tool. Line 34 restarts NetworkManager. Line 35 is a blank line. Lines 36 through 38 start the named service.

```
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 127.0.1.1
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.

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
Открыть  Vagrantfile /var/tmp/ismakhorin/vagrant Сохранить
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.



Спасибо за внимание!