Лабораторная работа №2

Настройка DNS-сервера

Махорин Иван Сергеевич

1032211221

НПИбд-02-21

Установка DNS-сервера

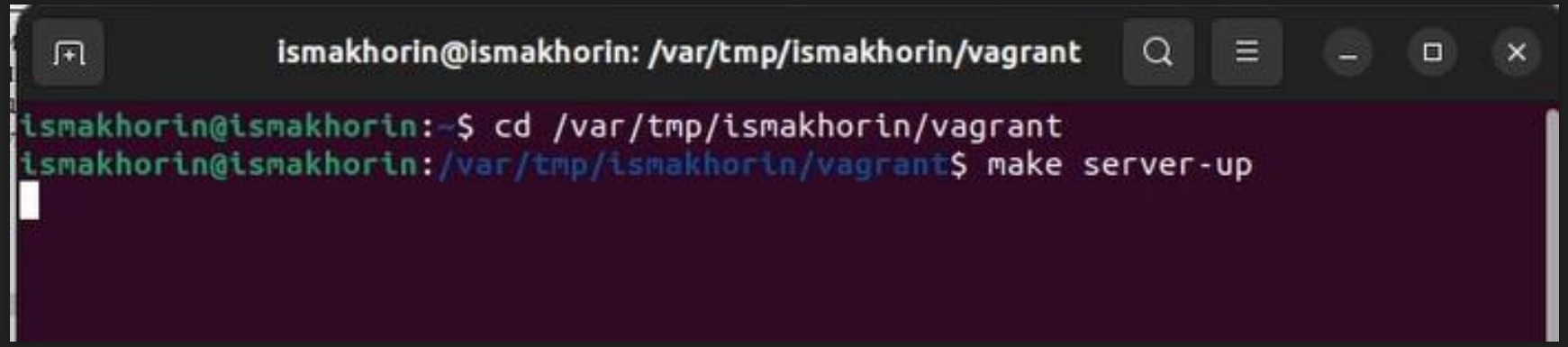


Рис. 1.1. Открытие рабочего каталога с проектом и запуск виртуальной машины server.

Установка DNS-сервера

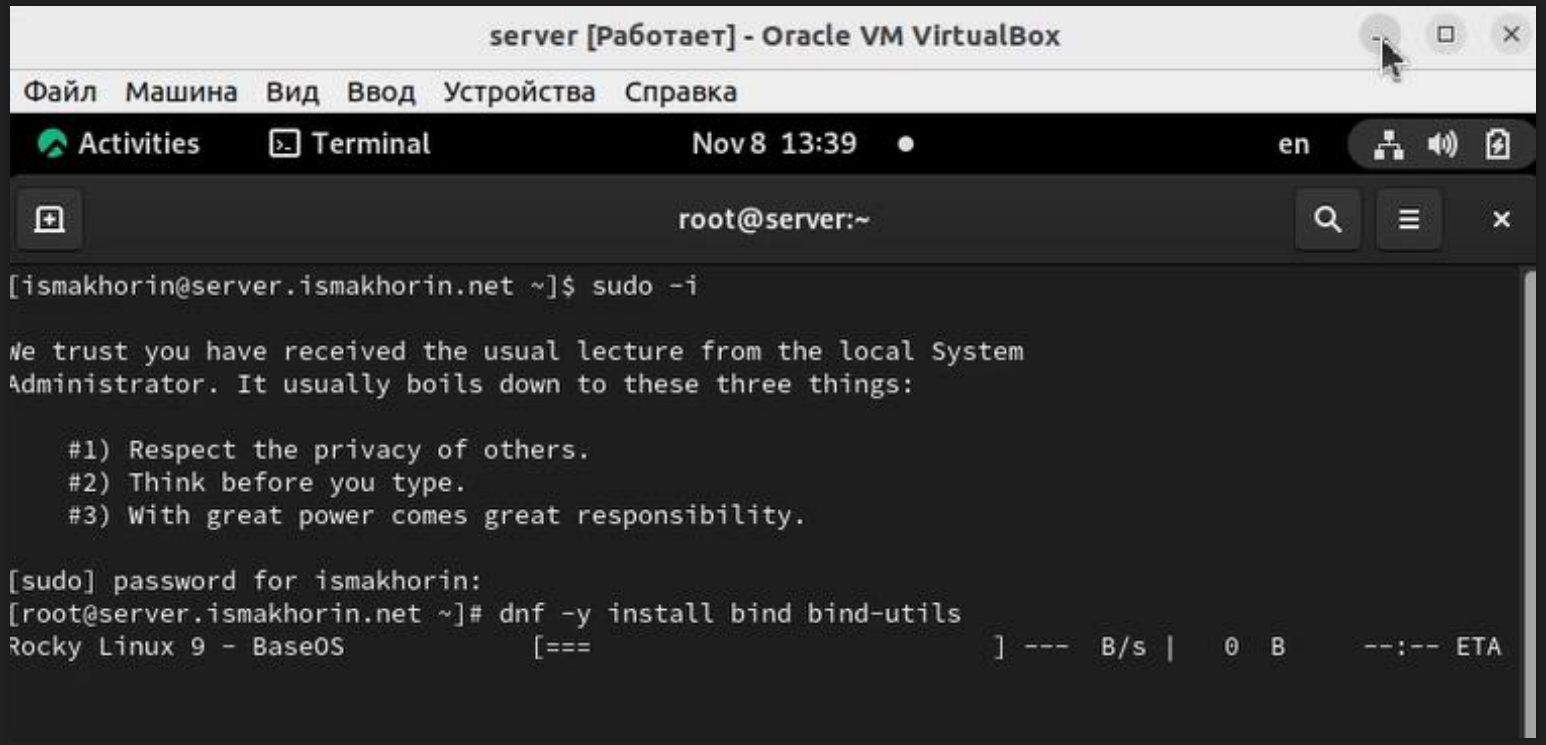


Рис. 1.2. Переход в режим суперпользователя и установка bind,bind-utils.

Установка DNS-сервера

```
[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: 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.ismakhorin.net ~]#
```

Рис. 1.3. Запрос с помощью утилиты dig.

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

```
[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.

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.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.

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
                                        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.

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

```
[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.

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

```
[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/syste
m/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.

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

```
[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.

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

```
[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.

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

```
[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.

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

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

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

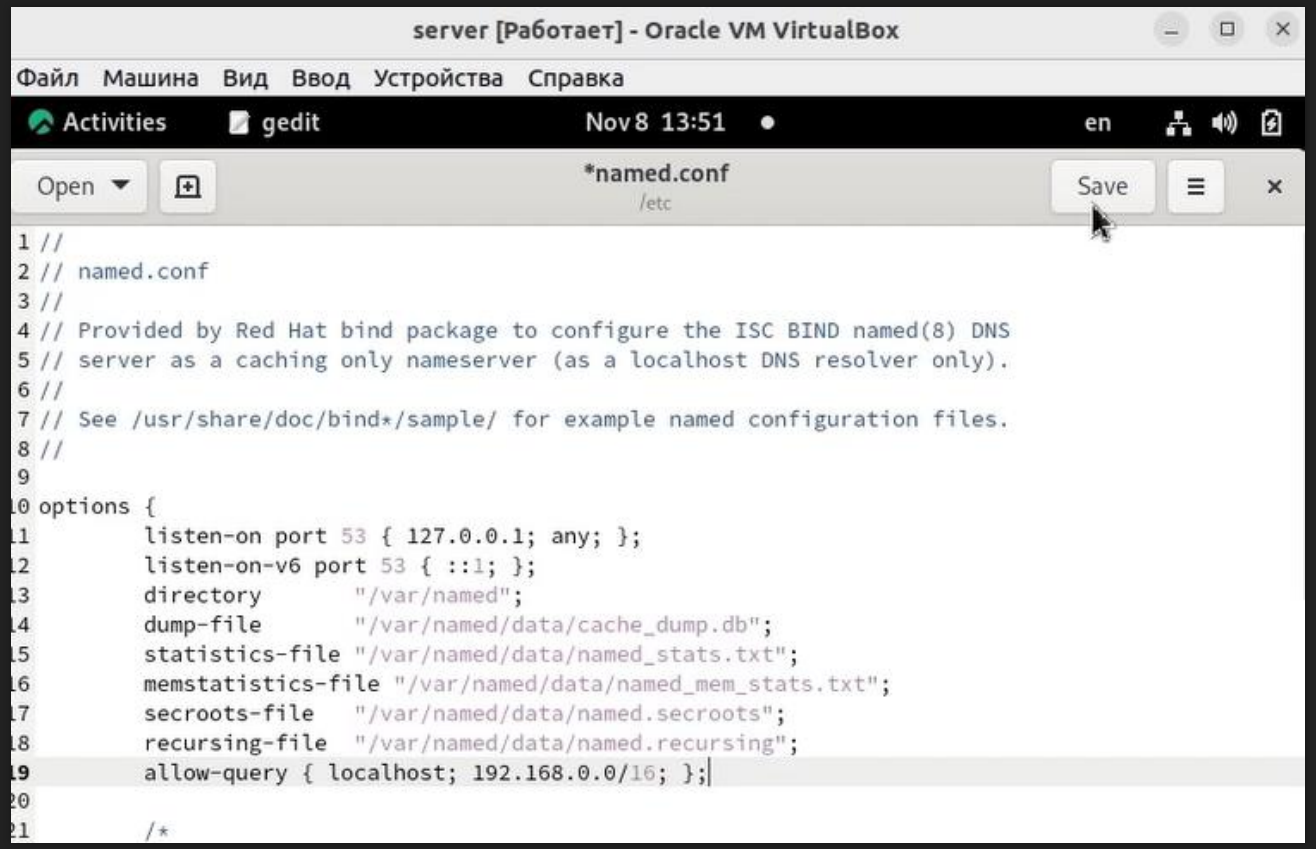


Рис. 2.11. Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server.

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

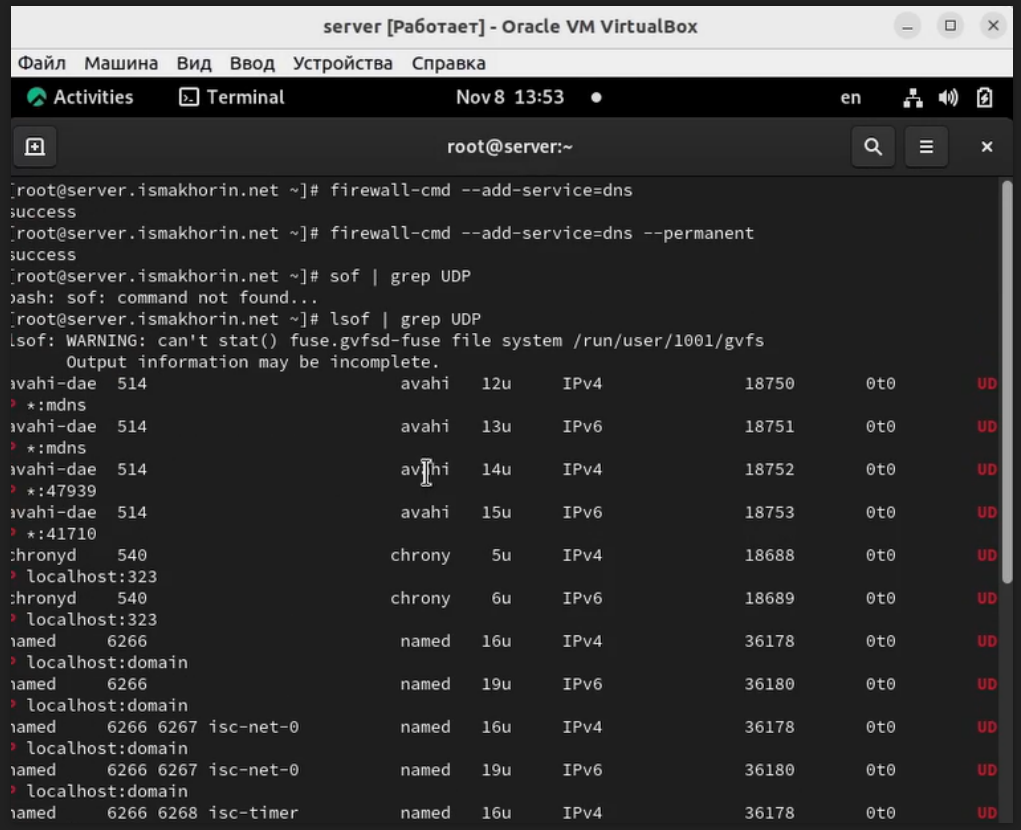


Рис. 2.12. Внос изменений в настройки межсетевого экрана узла server, разрешив работу с DNS. Проверка, что DNS-запросы идут через узел server, который прослушивает порт 53.

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

Open named.conf /etc Save

```
 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.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.

Конфигурирование первичного DNS-сервера

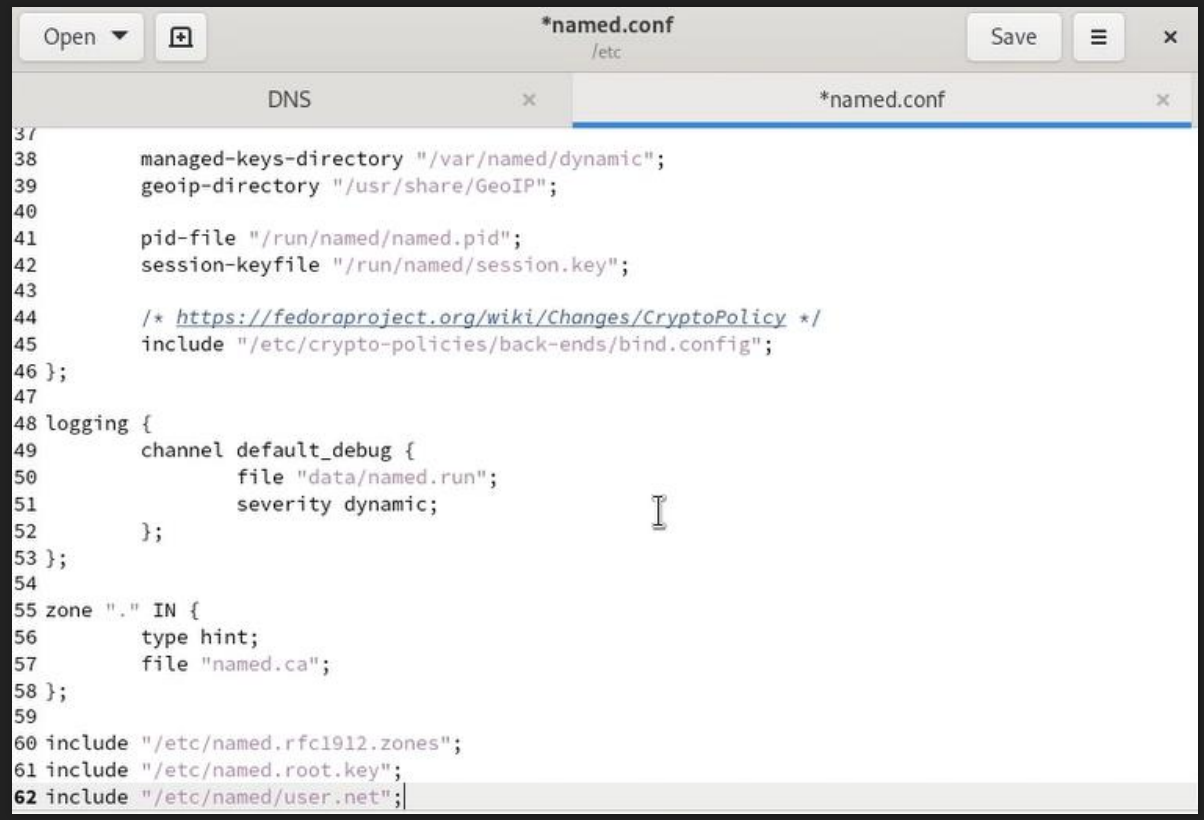


Рис. 4.2. Включение файла описания зоны /etc/named/ismakhorin.net в конфигурационном файле DNS /etc/named.conf.

Конфигурирование первичного DNS-сервера

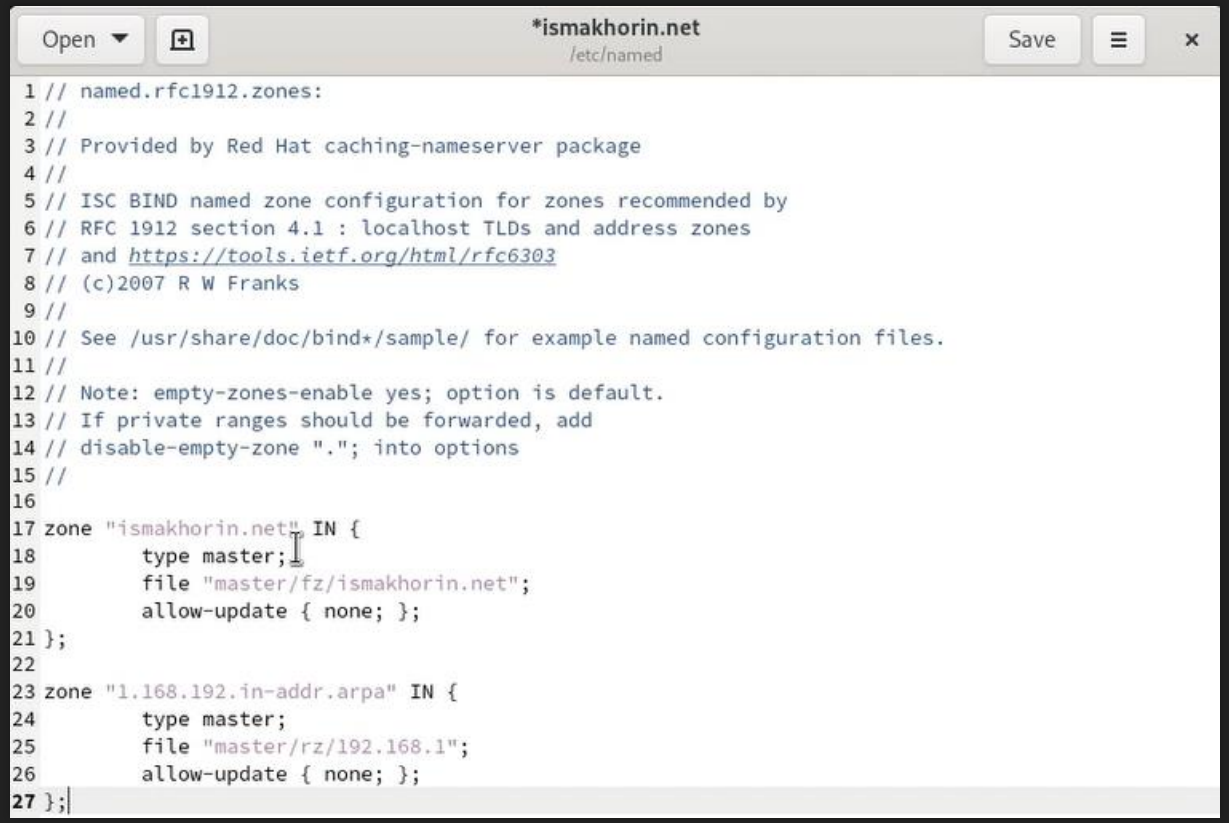


Рис. 4.3. Открытие файла /etc/named/user.net на редактирование. Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле.

Конфигурирование первичного DNS-сервера

```
[root@server.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.

Конфигурирование первичного DNS-сервера

```
[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.

Конфигурирование первичного DNS-сервера

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

Конфигурирование первичного DNS-сервера

```
[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.

Конфигурирование первичного DNS-сервера

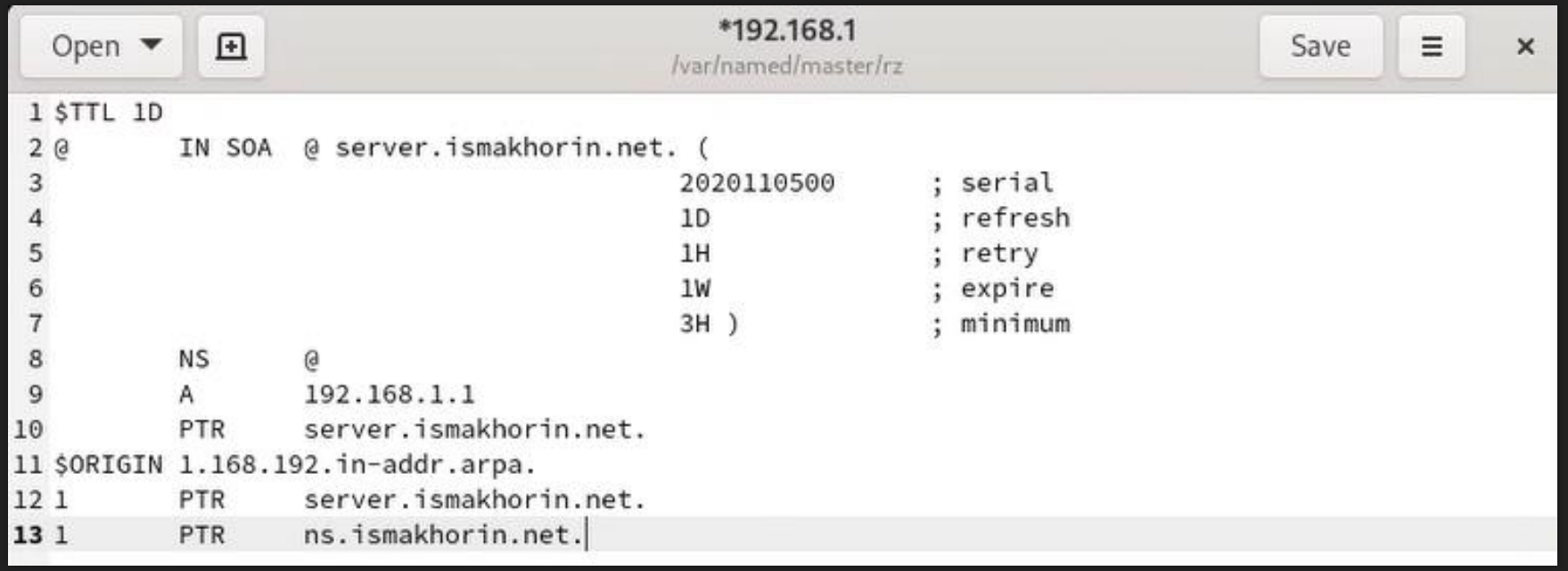


Рис. 4.8. Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны.

Конфигурирование первичного DNS-сервера

```
[root@server.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 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.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.

Конфигурирование первичного DNS-сервера

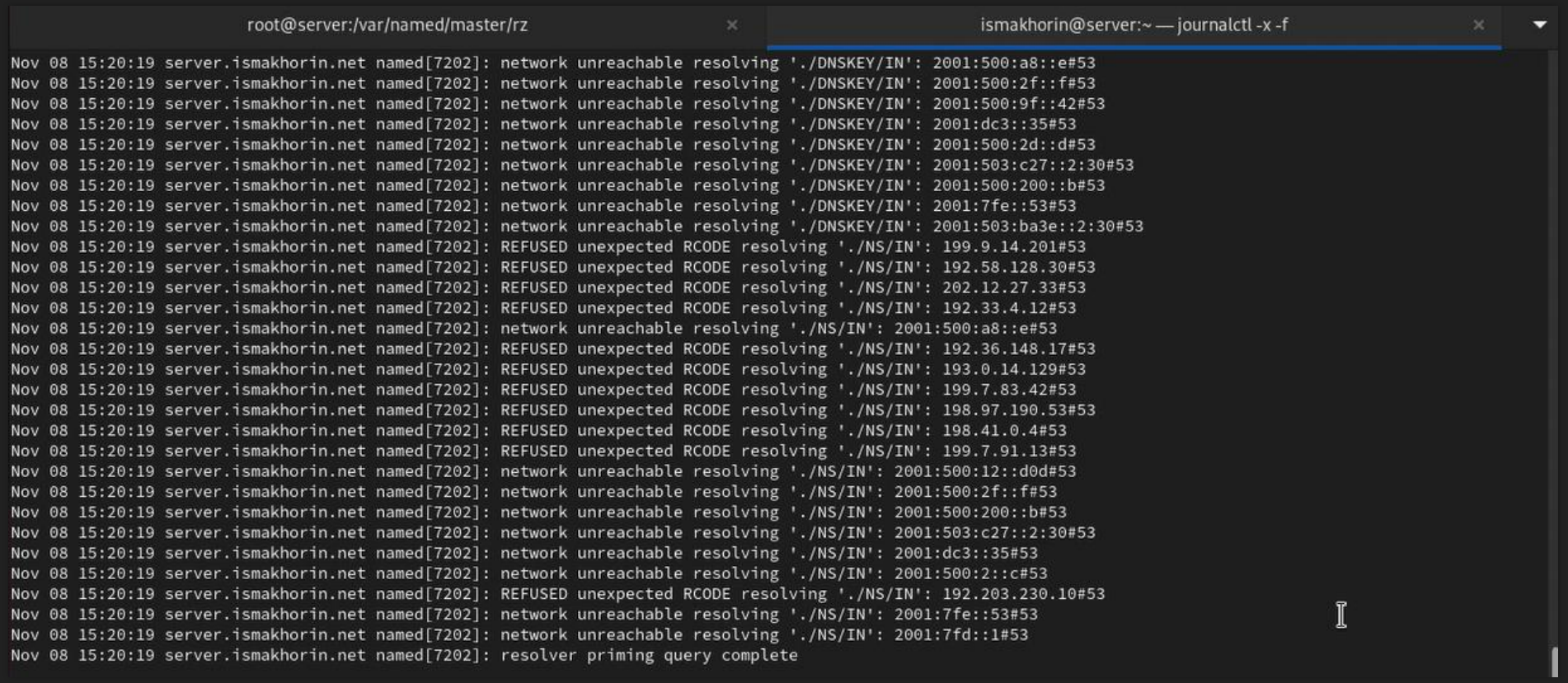


Рис. 4.10. Проверка корректности работы системы.

Анализ работы DNS-сервера

```
[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.

Анализ работы DNS-сервера

```
[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.

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

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

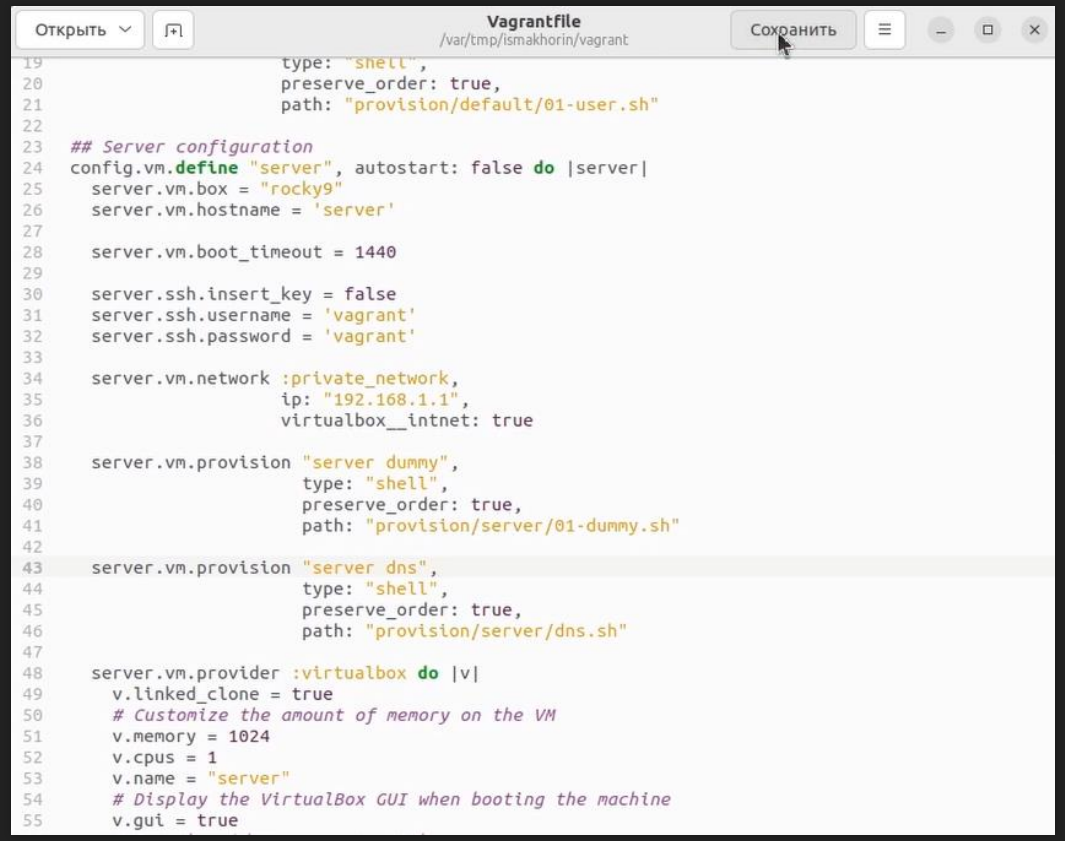
Open

*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.

Внесение изменений в настройки внутреннего окружения виртуальной машины




```
                    type: "shell",
                    preserve_order: true,
                    path: "provision/default/01-user.sh"

## 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
    # Customize the amount of memory on the VM
    v.memory = 1024
    v.cpus = 1
    v.name = "server"
    # Display the VirtualBox GUI when booting the machine
    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!