

Отчёт по лабораторной работе №2

Администрирование сетевых подсистем

Ищенко Ирина Олеговна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	20
4	Ответы на контрольные вопросы	21

Список иллюстраций

2.1	Запуск VM	6
2.2	Установка bind	7
2.3	dig	7
2.4	named.conf	8
2.5	named.ca	8
2.6	named.localhost	9
2.7	Запуск сервера	9
2.8	dig	10
2.9	Изменение настроек сетевого соединения eth0	11
2.10	Перезапуск NetworkManager и просмотр файла	11
2.11	Внесение изменений в файл /etc/named.conf	12
2.12	Внесение изменений в настройки межсетевого экрана узла server, проверка	12
2.13	Редактирование named.conf	13
2.14	Команды	13
2.15	Редактирование файла /etc/named/ioithenko.net	14
2.16	Создание каталогов, копирование шаблона прямой зоны, переименование	14
2.17	Редактирование /var/named/master/fz/ioithenko.net	15
2.18	Копирование шаблона обратной зоны, переименование	15
2.19	Редактирование /var/named/master/rz/192.168.1	16
2.20	Изменение прав доступа, восстановление меток SELinux, проверка	16
2.21	Описание DNS-зоны с сервера ns.ioithenko.net	17
2.22	Анализ корректности работы DNS-сервера	17
2.23	Анализ корректности работы DNS-сервера	17
2.24	Анализ корректности работы DNS-сервера	18
2.25	Размещение конфигурационных файлов в каталог /vagrant/provision/server/dns	18
2.26	Редактирование скрипта dns.sh	19
2.27	Редактирование Vagrantfile	19

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом: `cd /var/tmp/ioithenko/vagrant` Далее запустим виртуальную машину `server`: `vagrant up server` (рис. 2.1).

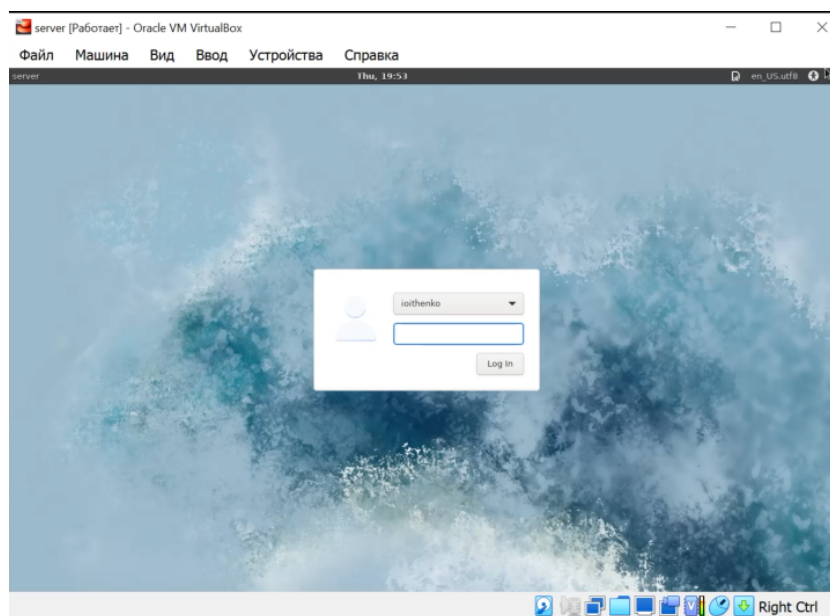
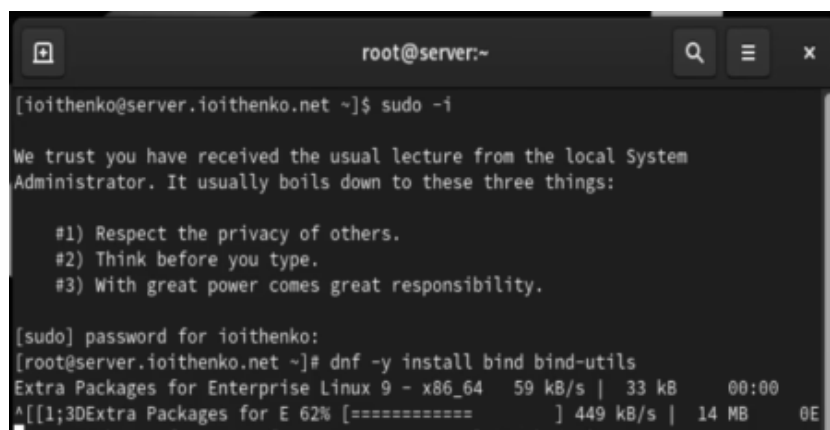


Рис. 2.1: Запуск ВМ

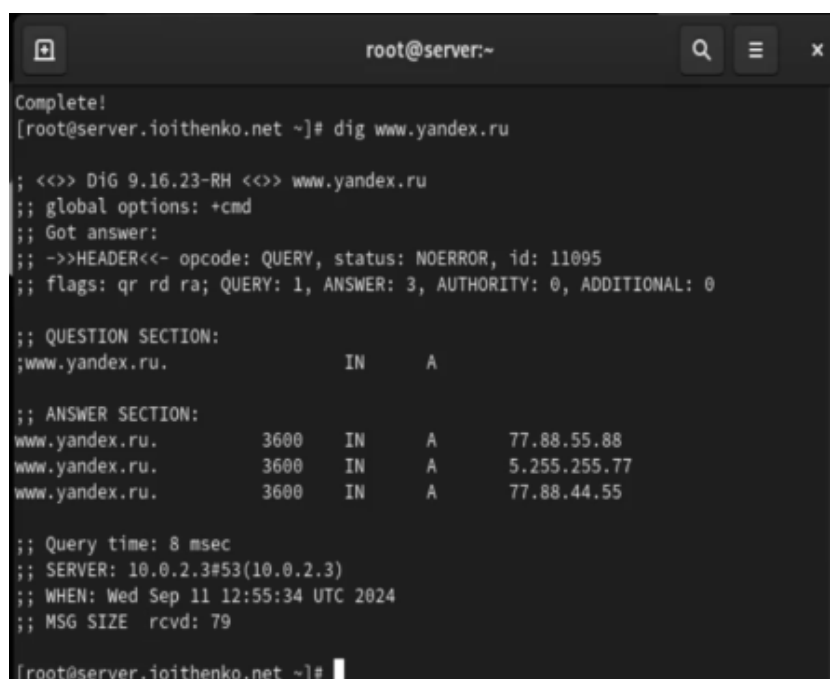
Перейдём в режим суперпользователя: `sudo -i` И установим `bind` и `bind-utils` (рис. 2.2): `dnf -y install bind bind-utils`



```
root@server:~  
[ioithenko@server.ioithenko.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 ioithenko:  
[root@server.ioithenko.net ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 59 kB/s | 33 kB 00:00  
^[[1;3DExtra Packages for E 62% [=====] 449 kB/s | 14 MB 0E  
Extra Packages for E 62% [=====] 449 kB/s | 14 MB 0E
```

Рис. 2.2: Установка bind

С помощью утилиты dig сделаем запрос к DNSадресу www.yandex.ru (рис. 2.3):
dig www.yandex.ru



```
root@server:~  
Complete!  
[root@server.ioithenko.net ~]# dig www.yandex.ru  
  
; <<>> DiG 9.16.23-RH <<>> www.yandex.ru  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11095  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;www.yandex.ru. IN A  
  
;; ANSWER SECTION:  
www.yandex.ru. 3600 IN A 77.88.55.88  
www.yandex.ru. 3600 IN A 5.255.255.77  
www.yandex.ru. 3600 IN A 77.88.44.55  
  
;; Query time: 8 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Wed Sep 11 12:55:34 UTC 2024  
;; MSG SIZE rcvd: 79  
  
[root@server.ioithenko.net ~]#
```

Рис. 2.3: dig

Просмотрим содержание файлов `/etc/resolv.conf`, `/etc/named.conf` (рис. 2.4),
`/var/named/named.ca` (рис. 2.5), `/var/named/named.localhost`, `/var/named/named.loopback`
(рис. 2.6).

```
[root@server.ioithenko.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; };
}
```

Рис. 2.4: named.conf

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

; <<>> DiG 9.18.20 <<>> -4 +tcp +nored +nostats @d.root-servers.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47286
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1450
;; 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.
```

Рис. 2.5: named.ca


```

[root@server.ioithenko.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.ioithenko.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

```

Рис. 2.6: named.localhost

Запустим DNS-сервер: `systemctl start named` Включим запуск DNS-сервера в автозапуск при загрузке системы (рис. 2.7): `systemctl enable named`

```

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

```

Рис. 2.7: Запуск сервера

`dig [127.0.0.1?] www.yandex.ru`. Выводится более подробная информация (рис. 2.8):

```
root@server:~  
[root@server.ioithenko.net ~]# dig @127.0.0.1 www.yandex.ru  
  
; <<> DiG 9.16.23-RH <<> @127.0.0.1 www.yandex.ru  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17675  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 1232  
; COOKIE: 9297481dc0e3b1470100000066e1946900e612b76ad34100 (good)  
;; QUESTION SECTION:  
;www.yandex.ru.                IN      A  
  
;; ANSWER SECTION:  
www.yandex.ru.                600     IN      A      5.255.255.77  
www.yandex.ru.                600     IN      A      77.88.44.55  
www.yandex.ru.                600     IN      A      77.88.55.88  
  
;; Query time: 552 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Wed Sep 11 13:00:25 UTC 2024
```

Рис. 2.8: dig

Сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить 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. 2.9).

Перезапускаем NetworkManager и проверяем наличие изменений в файле /etc/resolv.conf (рис. 2.10).

```

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

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

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

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

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-
-lx, dcb, sriov, ethtool, match, ipv4, ipv6, hostname, link, 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' (26191b97-32fc-41fd-8f79-0e2901b0e876) successfully updated.
nmcli> quit
[root@server.ioithenko.net ~]# systemctl restart NetworkManager
[root@server.ioithenko.net ~]#

```

Рис. 2.9: Изменение настроек сетевого соединения eth0

```

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

```

Рис. 2.10: Перезапуск NetworkManager и просмотр файла

Вносим изменения в файл /etc/named.conf (рис. 2.11).

```
root@server:~  
// server as a caching only nameserver (as a localhost DNS resolver only).  
//  
// See /usr/share/doc/bind*/sample/ for example named configuration files.  
//  
options {  
    listen-on port 53 { 127.0.0.1; any; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file "/var/named/data/named.secroots";  
    recursing-file "/var/named/data/named.recursing";  
    allow-query { localhost; 192.168.0.0/16; };  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recur  
sion.  
    - If you are building a RECURSIVE (caching) DNS server, you need to en  
able  
    recursion.  
*/
```

Рис. 2.11: Внесение изменений в файл /etc/named.conf

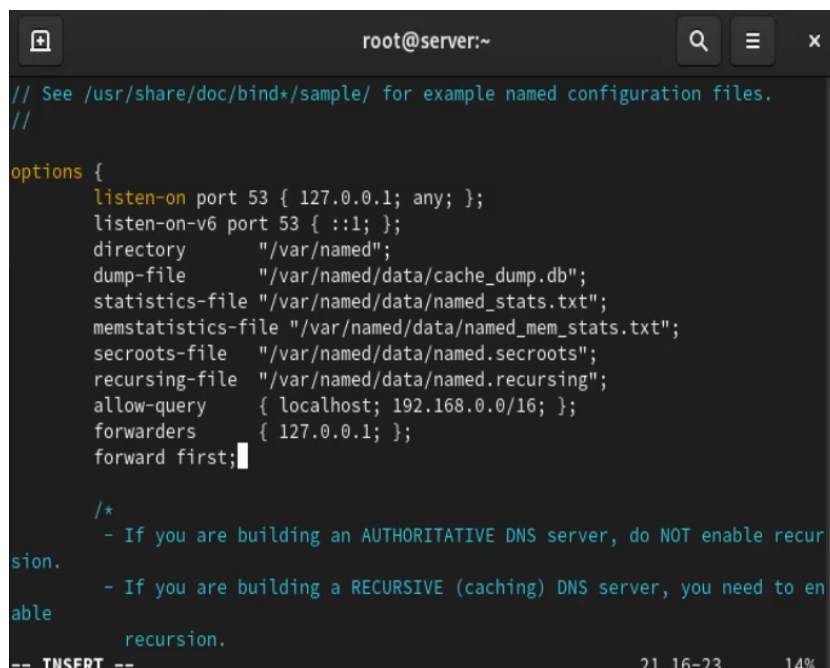
Вносим изменения в настройки межсетевого экрана узла server, разрешив работу с DNS. Убеждаемся, что DNS-запросы идут через узел server, который прослушивает порт 53 (рис. 2.12).

```
[root@server.ioithenko.net ~]# firewall-cmd --add-service=dns  
success  
[root@server.ioithenko.net ~]# firewall-cmd --add-service=dns --permanent  
success  
[root@server.ioithenko.net ~]# lsof | grep UDP  
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs  
Output information may be incomplete.  
avahi-daemon 570      0t0      UDP *:mdns          avahi    12u    IPv4          19659  
avahi-daemon 570      0t0      UDP *:mdns          avahi    13u    IPv6          19660  
avahi-daemon 570      0t0      UDP *:46069        avahi    14u    IPv4          19661  
avahi-daemon 570      0t0      UDP *:33616        avahi    15u    IPv6          19662  
chronyd       610      0t0      UDP localhost:323    chrony    5u    IPv4          19759  
chronyd       610      0t0      UDP localhost:323    chrony    6u    IPv6          19760
```

Рис. 2.12: Внесение изменений в настройки межсетевого экрана узла server, проверка

Для конфигурирования кэширующего DNS-сервера при наличии фильтрации

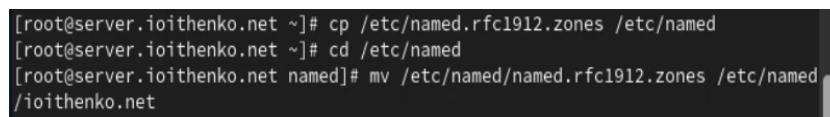
DNS-запросов маршрутизаторами вносим изменения в файл `named.conf` (рис. 2.13)



```
root@server:~  
// See /usr/share/doc/bind+sample/ for example named configuration files.  
//  
options {  
    listen-on port 53 { 127.0.0.1; any; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file "/var/named/data/named.secroots";  
    recursing-file "/var/named/data/named.recursing";  
    allow-query { localhost; 192.168.0.0/16; };  
    forwarders { 127.0.0.1; };  
    forward first;  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recur  
sion.  
    - If you are building a RECURSIVE (caching) DNS server, you need to en  
able  
    recursion.  
-- INSERT --
```

Рис. 2.13: Редактирование `named.conf`

Вводим команды(рис. 2.14): `cp /etc/named.rfc1912.zones /etc/named/` `cd /etc/named` `mv /etc/named/named.rfc1912.zones /etc/named/ioithenko.net`

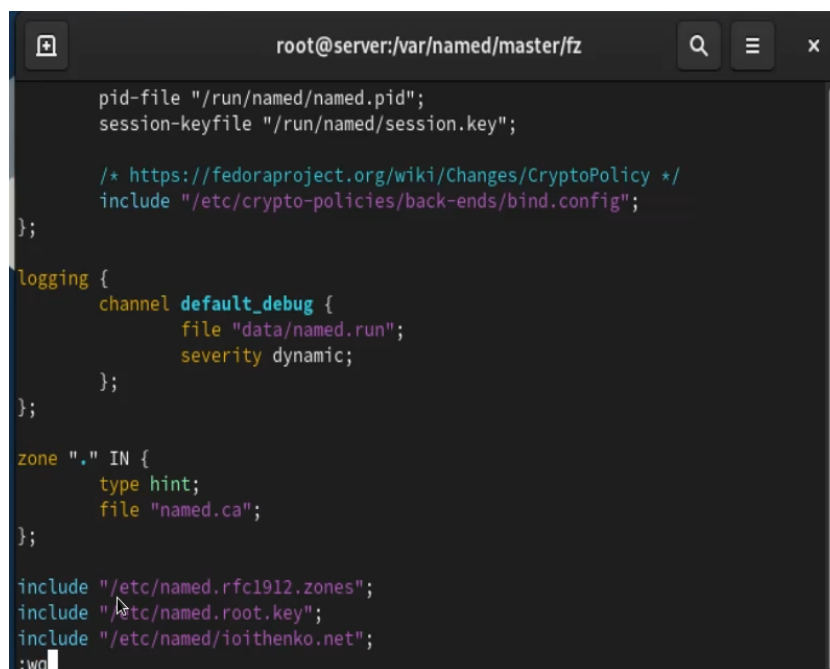


```
[root@server.ioithenko.net ~]# cp /etc/named.rfc1912.zones /etc/named  
[root@server.ioithenko.net ~]# cd /etc/named  
[root@server.ioithenko.net named]# mv /etc/named/named.rfc1912.zones /etc/named  
/ioithenko.net
```

Рис. 2.14: Команды

Включаем файл описания зоны `/etc/named/ioithenko.net` в конфигурационном файле DNS `/etc/named.conf`, добавив в нём в конце строку: `include "/etc/named/ioithenko.net";`.

Редактируем файл `/etc/named/ioithenko.net` (рис. 2.15)



```
root@server:/var/named/master/fz
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";

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

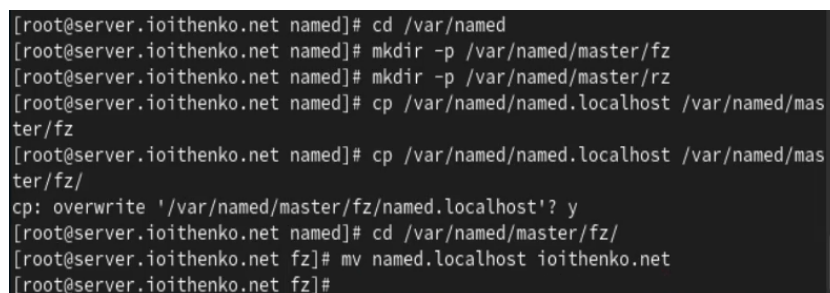
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

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

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/ioithenko.net";
:wq
```

Рис. 2.15: Редактирование файла /etc/named/ioithenko.net

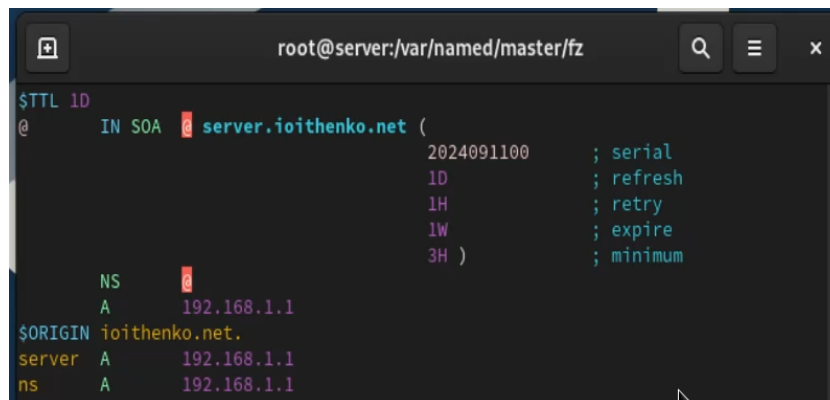
В каталоге /var/named создаем подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно. Копируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz, переименовав его в ioithenko.net (рис. 2.16).



```
[root@server.ioithenko.net named]# cd /var/named
[root@server.ioithenko.net named]# mkdir -p /var/named/master/fz
[root@server.ioithenko.net named]# mkdir -p /var/named/master/rz
[root@server.ioithenko.net named]# cp /var/named/named.localhost /var/named/master/fz
[root@server.ioithenko.net named]# cp /var/named/named.localhost /var/named/master/rz/
cp: overwrite '/var/named/master/fz/named.localhost'? y
[root@server.ioithenko.net named]# cd /var/named/master/fz/
[root@server.ioithenko.net fz]# mv named.localhost ioithenko.net
[root@server.ioithenko.net fz]#
```

Рис. 2.16: Создание каталогов, копирование шаблона прямой зоны, переименование

Изменяем файл /var/named/master/fz/ioithenko.net (рис. 2.17).

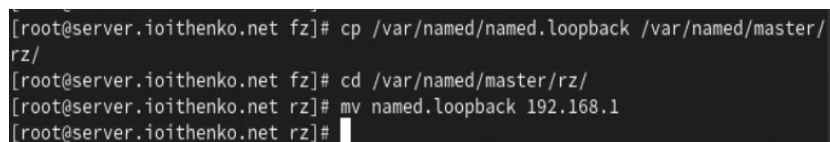


```
root@server:/var/named/master/fz
$TTL 1D
@      IN SOA  server.ioithenko.net (
                                2024091100      ; serial
                                1D               ; refresh
                                1H               ; retry
                                1W               ; expire
                                3H )             ; minimum

    NS   server.ioithenko.net.
    A    192.168.1.1
$ORIGIN ioithenko.net.
server  A    192.168.1.1
ns      A    192.168.1.1
```

Рис. 2.17: Редактирование /var/named/master/fz/ioithenko.net

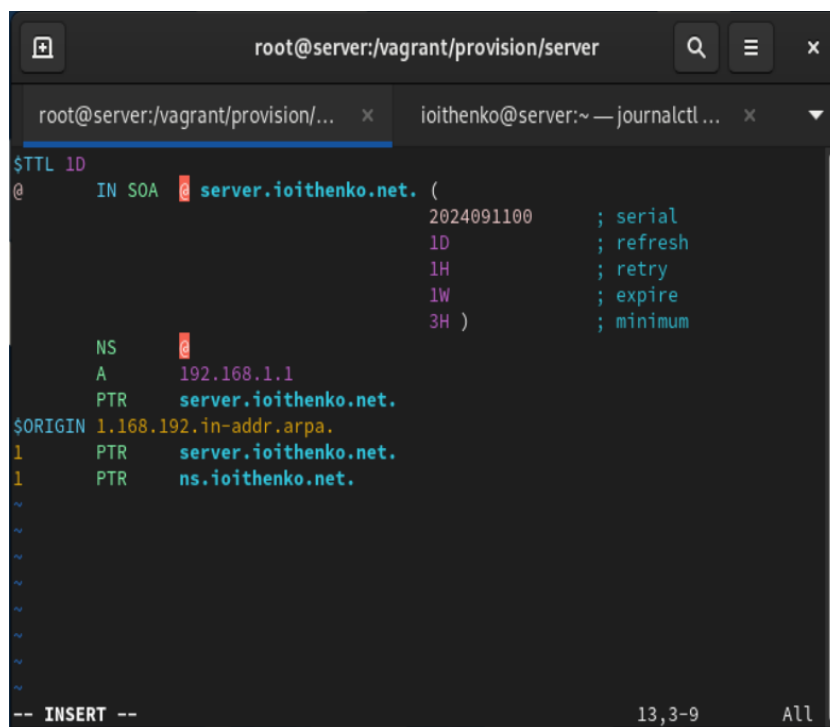
Копируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуйте его в 192.168.1 (рис. 2.18).



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

Рис. 2.18: Копирование шаблона обратной зоны, переименование

Изменяем файл /var/named/master/rz/192.168.1 (рис. 2.19).

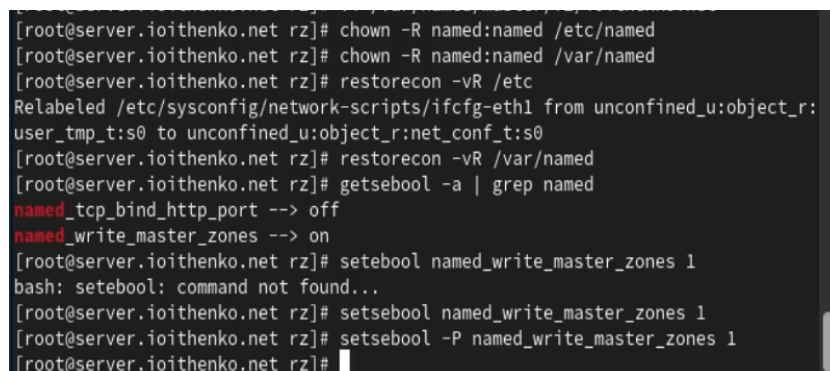


```
root@server:/vagrant/provision/server
root@server:/vagrant/provision/... x ioithenko@server:~ — journalctl ... x
$TTL 1D
@      IN SOA  server.ioithenko.net. (
                                2024091100      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H )              ; minimum

      NS   server.ioithenko.net.
      A    192.168.1.1
      PTR  server.ioithenko.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR  server.ioithenko.net.
1      PTR  ns.ioithenko.net.
~
~
~
~
~
~
-- INSERT -- 13,3-9 All
```

Рис. 2.19: Редактирование /var/named/master/rz/192.168.1

Изменяем права доступа, восстанавливаем метки SELinux, проверяем (рис. 2.20).



```
[root@server.ioithenko.net rz]# chown -R named:named /etc/named
[root@server.ioithenko.net rz]# chown -R named:named /var/named
[root@server.ioithenko.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
[root@server.ioithenko.net rz]# restorecon -vR /var/named
[root@server.ioithenko.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ioithenko.net rz]# setsebool named_write_master_zones 1
bash: setsebool: command not found...
[root@server.ioithenko.net rz]# setsebool named_write_master_zones 1
[root@server.ioithenko.net rz]# setsebool -P named_write_master_zones 1
[root@server.ioithenko.net rz]#
```

Рис. 2.20: Изменение прав доступа, восстановление меток SELinux, проверка

Во втором терминале открываем лог системных сообщений. В первом терминале перезапускаем DNS-сервер. После исправления всех ошибок и опечаток DNS-сервер запускается успешно. При помощи утилиты dig получаем описание DNS-зоны с сервера ns.ioithenko.net (рис. 2.21).


```

[root@server.ioithenko.net rz]# systemctl restart named
[root@server.ioithenko.net rz]# dig ns.ioithenko.net

; <<> DiG 9.16.23-RH <<> ns.ioithenko.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 36561
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 764a4ab7134134fc0100000066e1a0964e949cd6f1893123 (good)
;; QUESTION SECTION:
ns.ioithenko.net.          IN      A

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

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Sep 11 13:52:22 UTC 2024

```

Рис. 2.21: Описание DNS-зоны с сервера ns.ioithenko.net

Анализируем корректность работы DNS-сервера (рис. 2.22), (рис. 2.23), (рис. 2.24).

```

[root@server.ioithenko.net rz]# host -l ioithenko.net
ioithenko.net name server ioithenko.net.
ioithenko.net has address 192.168.1.1
ns.ioithenko.net has address 192.168.1.1
server.ioithenko.net has address 192.168.1.1

```

Рис. 2.22: Анализ корректности работы DNS-сервера

```

[root@server.ioithenko.net rz]# host -a ioithenko.net
Trying "ioithenko.net"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 43325
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
ioithenko.net.          IN      ANY

;; ANSWER SECTION:
ioithenko.net.          86400   IN      SOA      ioithenko.net. server.ioithenko.net. 2024091100 86400 3600 604800 10800
ioithenko.net.          86400   IN      NS       ioithenko.net.
ioithenko.net.          86400   IN      A        192.168.1.1

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

Received 120 bytes from 127.0.0.1#53 in 12 ms
[root@server.ioithenko.net rz]# host -t A ioithenko.net
ioithenko.net has address 192.168.1.1

```

Рис. 2.23: Анализ корректности работы DNS-сервера

```
[root@server.ioithenko.net server]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ioithenko.net.
1.1.168.192.in-addr.arpa domain name pointer server.ioithenko.net.
```

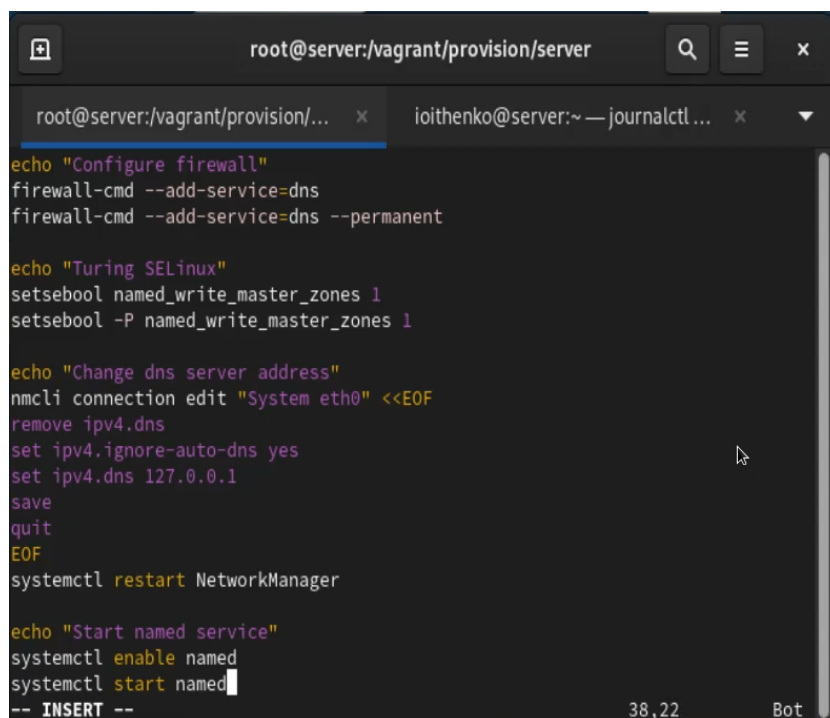
Рис. 2.24: Анализ корректности работы DNS-сервера

Переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создаем в нём каталог `dns`, в который помещаем в соответствующие каталоги конфигурационные файлы DNS (рис. 2.25).

```
[root@server.ioithenko.net rz]# cd /vagrant
[root@server.ioithenko.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.ioithenko.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
[root@server.ioithenko.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.ioithenko.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.ioithenko.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.ioithenko.net vagrant]# cd /vagrant/provision/server
[root@server.ioithenko.net server]# touch dns.sh
[root@server.ioithenko.net server]# chmod +x dns.sh
[root@server.ioithenko.net server]#
```

Рис. 2.25: Размещение конфигурационных файлов в каталог `/vagrant/provision/server/dns`

Создаем скрипт `dns.sh` (рис. 2.26).



```
root@server:/vagrant/provision/server
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

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

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

echo "Start named service"
systemctl enable named
systemctl start named
-- INSERT --
38,22 Bot
```

Рис. 2.26: Редактирование скрипта dns.sh

Для отработки созданного скрипта во время загрузки виртуальной машины в конфигурационном файле Vagrantfile вносим изменения в разделе конфигурации для сервера (рис. 2.27).



```
Vagrantfile - Блокнот
Файл Правка Формат Вид Справка
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"
```

Рис. 2.27: Редактирование Vagrantfile

3 Выводы

В ходе лабораторной работы я приобрела практические навыки по установке и конфигурированию DNSсервера, усвоила принципы работы системы доменных имён.

4 Ответы на контрольные вопросы

1. Что такое DNS?

DNS - это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса компьютерами для идентификации друг друга в сети.

2. Каково назначение кэширующего DNS-сервера?

Задача сервера - 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` .

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

Использовать опции `-d` или `-v` при запуске службы.

16. Где хранится 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.

`lsof -p` или `fuser -v` .

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

Примеры включают `nmcli connection up|down` .

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 .`

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

Использовать `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 <on|off>`.