

Лабораторная работа №2

Дисциплина: Администрирование сетевых подсистем

Жибицкая Евгения Дмитриевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Ответы на контрольные вопросы	22
4	Выводы	26
	Список литературы	27

Список иллюстраций

2.1	Загрузка ОС	6
2.2	bind, bind-utils	6
2.3	Запрос к DNS-адресу Яндекса	7
2.4	Файл /etc/resolv.conf	7
2.5	Файл /etc/named.conf	8
2.6	Файлы named.localhost и named.loopback	9
2.7	Запуск сервера	9
2.8	Dig www.yandex.ru	10
2.9	Настройка соединения	11
2.10	Настройка направления запросов	12
2.11	Firewall	12
2.12	Редактирование named.conf	13
2.13	Перемещение файла	13
2.14	/etc/named.conf	14
2.15	/etc/named/edzhibitskaya.net	15
2.16	Создание подкаталогов	15
2.17	edzhibitskaya.net	16
2.18	Копирование файла	16
2.19	192.168.1	17
2.20	Права и метки	17
2.21	Переключатели	18
2.22	Перезапуск	18
2.23	Описание DNS-зоны с сервера	19
2.24	host -l; host -a	19
2.25	host -t	20
2.26	Добавление изменений	20
2.27	Создание файла	20
2.28	Скрипт	21
2.29	Vagrantfile	21

Список таблиц

1 Цель работы

Приобретение навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён на ОС Rocky linux.

2 Выполнение лабораторной работы

Для начала загружаем операционную систему, перейдя в каталог Vagrant(рис. 2.1).

```
PS C:\work\edzhbitskaya\vagrant> vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this
machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't wo
rk
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this
machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't wo
rk
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces
```

Рис. 2.1: Загрузка ОС

Открываем терминал, переходим в режим суперпользователя и устанавливаем bind, bind-utils(рис. 2.2).

```
root@server:~ - sudo -i
[edzhbitskaya@server.edzhbitskaya.net ~]$ sudo -i
[sudo] password for edzhbitskaya:
[root@server.edzhbitskaya.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 27 kB/s | 40 kB    00:01
Extra Packages 0% [          ] 42 kB/s | 24 kB    01:14 ETA
```

Рис. 2.2: bind, bind-utils

Затем в качестве тренировки делаем запрос к DNS-адресу Яндекса(рис. 2.3).

```
[root@server.edzhibitskaya.net ~]# dig www.yandex.ru
;; communications error to 192.168.1.1#53: connection refused
;; communications error to 192.168.1.1#53: connection refused
;; communications error to 192.168.1.1#53: connection refused

<>> DiG 9.18.33 <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21954
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                564     IN      A      77.88.44.55
www.yandex.ru.                564     IN      A      77.88.55.88
www.yandex.ru.                564     IN      A      5.255.255.77

;; Query time: 51 msec
;; SERVER: fd17:625c:f037:2::3#53(fd17:625c:f037:2::3) (UDP)
;; WHEN: Mon Sep 08 19:03:24 UTC 2025
;; MSG SIZE rcvd: 90

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

Рис. 2.3: Запрос к DNS-адресу Яндекса

Затем посмотрим содержимое файлов `/etc/resolv.conf`, `/etc/named.conf`, `/var/named/named.ca`, `/var/named/named.localhost`, `/var/named/named.loopback`.

В файле `/etc/resolv.conf` указано к каким DNS-серверам обращаться для преобразования доменных имен в IP-адреса и наоборот(рис. 2.4).

```
[root@server.edzhibitskaya.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search IGD_MGTS edzhibitskaya.net
nameserver 192.168.1.1
nameserver fd17:625c:f037:2::3
[root@server.edzhibitskaya.net ~]#
```

Рис. 2.4: Файл `/etc/resolv.conf`

`/etc/named.conf` главный конфигурационный файл демона BIND (named). Он определяет общие параметры работы DNS-сервера, зоны, которые он обслуживает, и политики доступа(рис. 2.5).

```
[root@server.edzhibitskaya.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.secrets";
    recursing-file  "/var/named/data/named.recursing";

```

Рис. 2.5: Файл /etc/named.conf

/var/named/named.ca содержит список IP-адресов корневых DNS-серверов (root hints). Когда DNS-сервер не знает, куда направить запрос для какого-либо домена, он начинает поиск с этих корневых серверов

/var/named/named.localhost - это файл прямой зоны для домена localhost. Он сопоставляет имя localhost с IP-адресом 127.0.0.1

/var/named/named.loopback - это файл обратной зоны (reverse zone) для сетей IPv4 и IPv6. Он выполняет обратное преобразование: по IP-адресу 127.0.0.1 находит имя localhost(рис. 2.6).


```

[root@server.edzhbitskaya.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.edzhbitskaya.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.edzhbitskaya.net ~]#

```

Рис. 2.6: Файлы named.localhost и named.loopback

Затем запустим DNS-сервер, включим его автозапуск(рис. 2.7).

```

[root@server.edzhbitskaya.net ~]# systemctl start named
[root@server.edzhbitskaya.net ~]# systemctl enabled named
Unknown command verb 'enabled', did you mean 'enable'?
[root@server.edzhbitskaya.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.s
ervice' → '/usr/lib/systemd/system/named.service'.
[root@server.edzhbitskaya.net ~]#

```

Рис. 2.7: Запуск сервера

Проанализируем вывод команд `dig www.yandex.ru` и `dig [127.0.0.1?] www.yandex.ru`(рис. 2.8). Вторая команда дает больший вывод, так как в ней мы еще указываем к какому серверу обращаться, она помогает в отладке и диагностике конфигурации

```

[root@server.edzhibitskaya.net ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8319
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 48c3573e2e56ef880100000068bf2aa2903cc64b0e717cd1 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                600     IN      A      77.88.44.55
www.yandex.ru.                600     IN      A      77.88.55.88
www.yandex.ru.                600     IN      A      5.255.255.77

;; Query time: 359 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Sep 08 19:12:34 UTC 2025
;; MSG SIZE rcvd: 118

[root@server.edzhibitskaya.net ~]# █

```

Рис. 2.8: Dig www.yandex.ru

Далее сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети, 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 127.0.0.0. Перезапускаем менеджер, проверяем наличие изменений (рис. 2.9).

```

[root@server.edzhbitskaya.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, 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' (9e794e8b-188b-46e6-9bfc-fda8868e20ce) successfully updated.
nmcli> quit
[root@server.edzhbitskaya.net ~]# systemctl restart NetworkManager
[root@server.edzhbitskaya.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search edzhbitskaya.net
nameserver 127.0.0.1
nameserver fd17:625c:f037:2::3
[root@server.edzhbitskaya.net ~]#

```

Рис. 2.9: Настройка соединения

Также настраиваем направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого редактируем файл /etc/named.conf(рис. 2.10).

```

GNU nano 8.1 /etc/named.conf Modified
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named>
// server as a caching only nameserver (as a localhost DNS resolver>
//
// See /usr/share/doc/bind*/sample/ for example named configuration>
//
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; };
}

```

Рис. 2.10: Настройка направления запросов

Вносим изменения в настройки межсетевого экрана узла server, убеждаемся, что DNS-запросы идут через узел server(рис. 2.11).

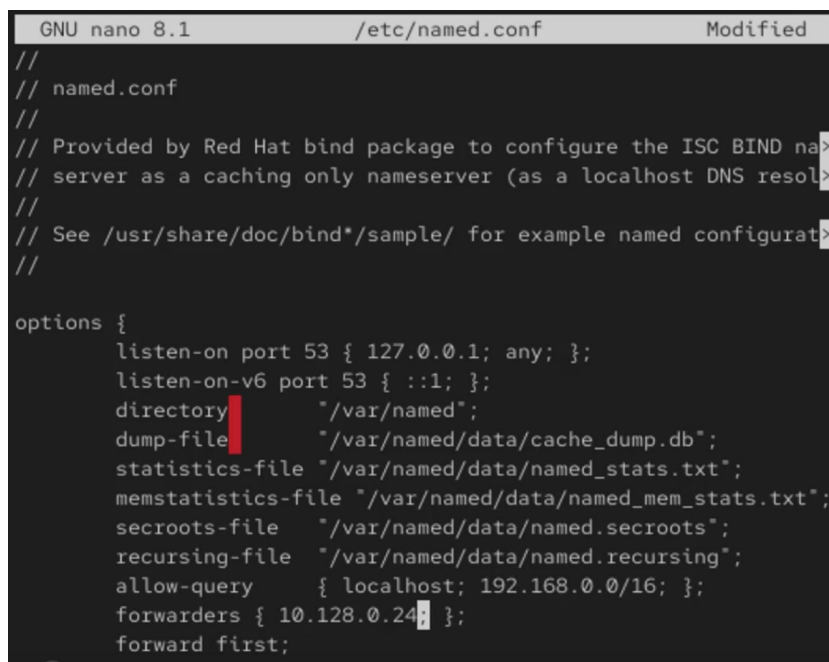
```

[root@server.edzhibitskaya.net ~]# firewall-cmd --add-service=dns
success
[root@server.edzhibitskaya.net ~]# firewall-cmd --add-service=dns --
permanent
success
[root@server.edzhibitskaya.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/10
02/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1002/d
oc
Output information may be incomplete.
avahi-dae  872          0t0      UDP *:mdns          avahi  12u    IPv4
          9463          0t0      UDP *:mdns          avahi  13u    IPv6
avahi-dae  872          0t0      UDP *:mdns          avahi  13u    IPv6
          9464          0t0      UDP *:mdns          avahi  13u    IPv6
chronyd    920          0t0      UDP localhost:323   chrony  5u     IPv4
          8650          0t0      UDP localhost:323   chrony  6u     IPv6
chronyd    920          0t0      UDP localhost:323   chrony  6u     IPv6
          8651          0t0      UDP localhost:323   chrony  6u     IPv6
wsdd       13183        0t0      UDP 239.255.255.250:ws-discovery edzhibitskaya 7u    IPv4
          50425        0t0      UDP 239.255.255.250:ws-discovery edzhibitskaya 8u    IPv4
wsdd       13183        0t0      UDP *:32888          edzhibitskaya 8u    IPv4
          50426        0t0      UDP *:32888          edzhibitskaya 9u    IPv4
wsdd       13183        0t0      UDP server.edzhibitskaya.net:ws-discov edzhibitskaya 9u    IPv4
          50427        0t0      UDP server.edzhibitskaya.net:ws-discov edzhibitskaya 9u    IPv4

```

Рис. 2.11: Firewall

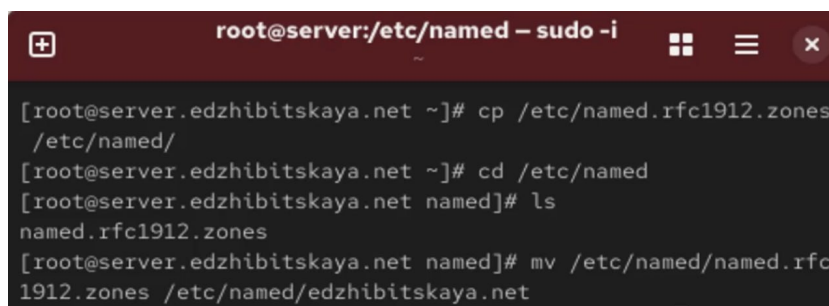
В ситуации, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер. Для этого в конфигурационный файл `named.conf` в секцию `options` добавим данные, предварительно посмотрев их на локальном хосте (рис. 2.12).



```
GNU nano 8.1 /etc/named.conf Modified
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND na>
// server as a caching only nameserver (as a localhost DNS resol>
//
// See /usr/share/doc/bind*/sample/ for example named configurat>
//
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 { 10.128.0.248; };
    forward first;
}
```

Рис. 2.12: Редактирование `named.conf`

Далее копируем шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименовываем его (рис. 2.13).

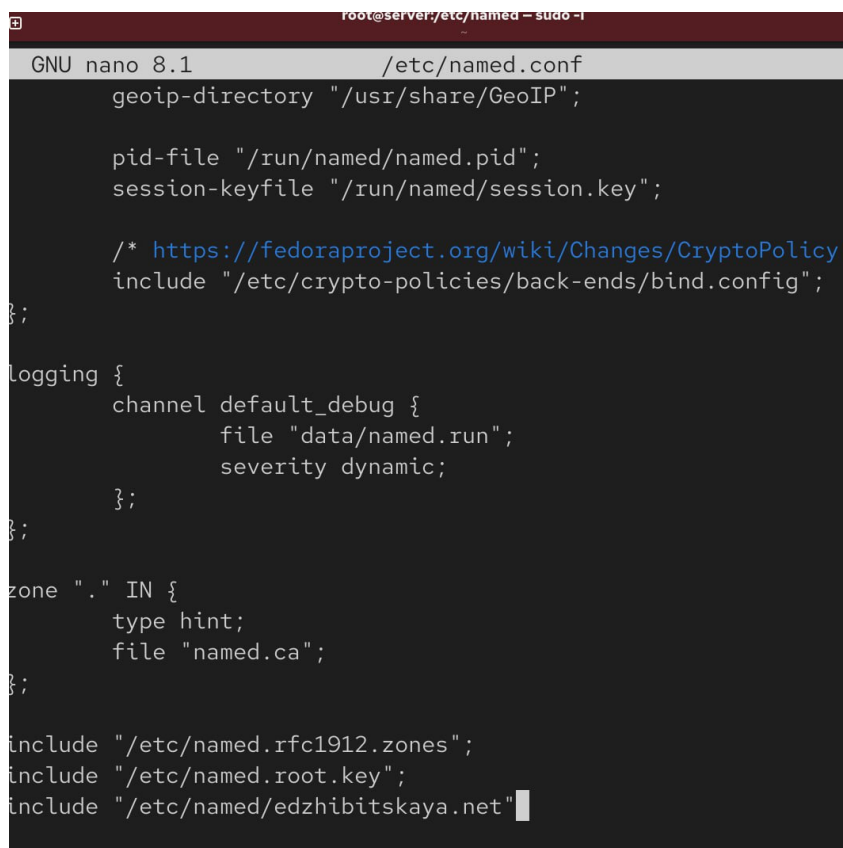


```
root@server:/etc/named - sudo -i
[root@server.edzhibitskaya.net ~]# cp /etc/named.rfc1912.zones
/etc/named/
[root@server.edzhibitskaya.net ~]# cd /etc/named
[root@server.edzhibitskaya.net named]# ls
named.rfc1912.zones
[root@server.edzhibitskaya.net named]# mv /etc/named/named.rfc
1912.zones /etc/named/edzhibitskaya.net
```

Рис. 2.13: Перемещение файла

Включим файл описания зоны `/etc/named/user.net` в конфигурационном файле

DNS /etc/named.conf(рис. 2.14), отредактируем файл /etc/named/edzhibitskaya.net(рис. 2.15).

A screenshot of a terminal window with a dark background. The title bar at the top reads 'root@server:/etc/named - sudo -i'. The terminal shows the GNU nano 8.1 editor editing the file /etc/named.conf. The visible text in the file is as follows:

```
geoip-directory "/usr/share/GeoIP";

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";
};

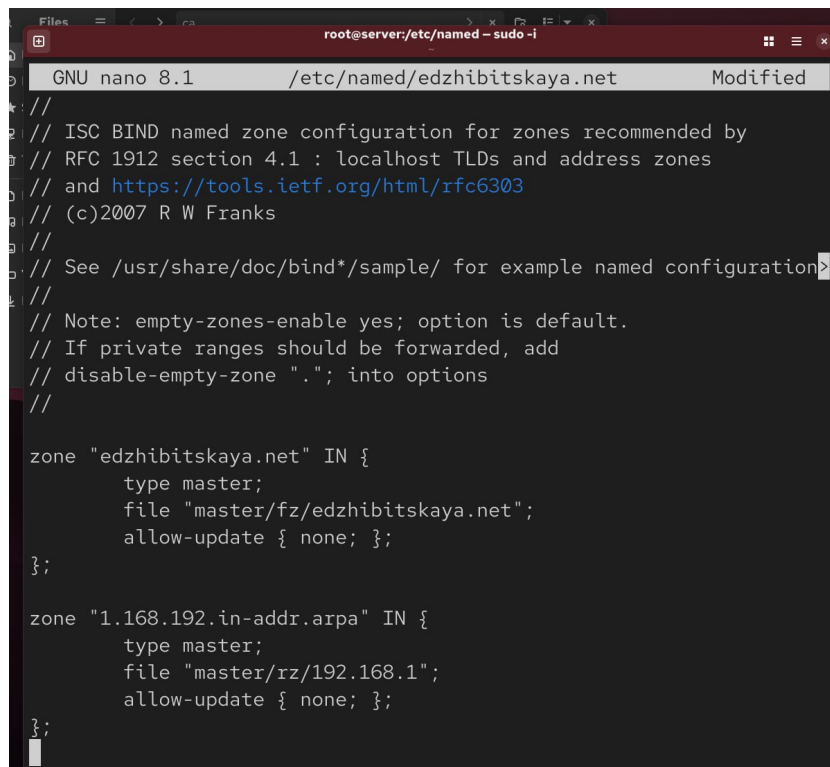
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

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

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/edzhibitskaya.net"
```

The cursor is positioned at the end of the last line.

Рис. 2.14: /etc/named.conf

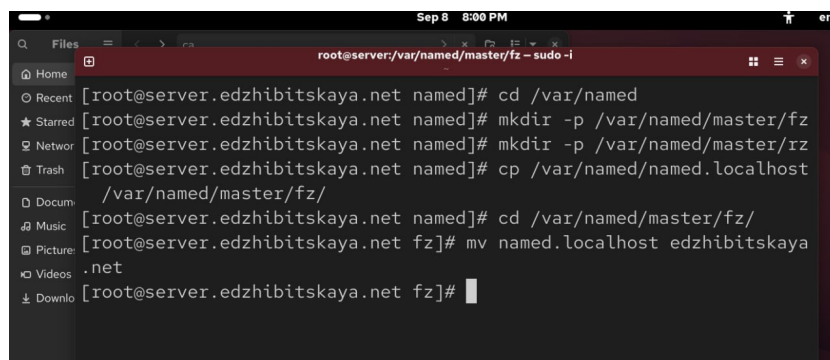


```
GNU nano 8.1 /etc/named/edzhibitskaya.net Modified
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and https://tools.ietf.org/html/rfc6303
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration>
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add
// disable-empty-zone "."; into options
//
zone "edzhibitskaya.net" IN {
    type master;
    file "master/fz/edzhibitskaya.net";
    allow-update { none; };
};

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

Рис. 2.15: /etc/named/edzhibitskaya.net

В каталоге /var/named создаем подкаталоги master/fz и master/rz, в кото-
рых будут располагаться файлы прямой и обратной зоны соответственно,
скопируем шаблон прямой DNS-зоны named.localhost и переименуем его в
edzhibitskaya.net(рис. 2.16).



```
Sep 8 8:00 PM
root@server:/var/named/master/fz - sudo -i
[root@server.edzhibitskaya.net named]# cd /var/named
[root@server.edzhibitskaya.net named]# mkdir -p /var/named/master/fz
[root@server.edzhibitskaya.net named]# mkdir -p /var/named/master/rz
[root@server.edzhibitskaya.net named]# cp /var/named/named.localhost
/var/named/master/fz/
[root@server.edzhibitskaya.net named]# cd /var/named/master/fz/
[root@server.edzhibitskaya.net fz]# mv named.localhost edzhibitskaya
.net
[root@server.edzhibitskaya.net fz]#
```

Рис. 2.16: Создание подкаталогов

Далее редактируем файл(рис. 2.17).

```
root@server:/var/named/master/fz - sudo -i
GNU nano 8.1                                edzhibitskaya.net                                Modified
$TTL 1D
@      IN SOA  @ server.edzhibitskaya.net. (
                                2024072700      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

      NS      @
      A      192.168.1.1
$ORIGIN edzhibitskaya.net.
server A      192.168.1.1
ns     A      192.168.1.1
```

Рис. 2.17: edzhibitskaya.net

Копируем шаблон обратной DNS-зоны named.loopback, переименовываем его в 192.168.1(рис. 2.18), также редактируем(рис. 2.19).

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

Рис. 2.18: Копирование файла


```
root@server:/var/named/master/rz - sudo -i
GNU nano 8.1 /var/named/master/rz/192.168.1 Modified
$TTL 1D
@      IN SOA  @ server.edzhibitskaya.net. (
                                2024072700 ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

      NS      @
      A      192.168.1.1
      PTR     server.edzhibitskaya.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR     server.edzhibitskaya.net.
1      PTR     ns.edzhibitskaya.net.S
```

Рис. 2.19: 192.168.1

Исправляем права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать и после изменения доступа к конфигурационным файлам named корректно восстанавливаем их метки в SELinux(рис. 2.20).

```
[root@server.edzhibitskaya.net rz]# chown -R named:named /etc/named
[root@server.edzhibitskaya.net rz]# chown -R named:named /var/named
[root@server.edzhibitskaya.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20250906.183832.0005 from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:NetworkManager_etc_rw_t:s0
[root@server.edzhibitskaya.net rz]# restorecon -vR /var/named
[root@server.edzhibitskaya.net rz]#
```

Рис. 2.20: Права и метки

Еще необходимо проверить состояние переключателей, дать разрешение на запись(рис. 2.21).

```
[root@server.edzhibitskaya.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.edzhibitskaya.net rz]# setsebool named_write_master_zones 1
[root@server.edzhibitskaya.net rz]# setsebool -P named_write_master_zones 1
[root@server.edzhibitskaya.net rz]#
```

Рис. 2.21: Переключатели

В дополнительном терминале запускаем в режиме реального времени расширенный лог системных сообщений и в первом терминале перезапускаем сервер(рис. 2.22).

```
[root@server.edzhibitskaya.net rz]# systemctl restart named
[root@server.edzhibitskaya.net rz]# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-09-11 08:15:03 UTC; 1min 15s ago
 Invocation: 687cd3dba8c04d678ae2f7a22c24d10c
   Process: 23503 ExecStartPre=/bin/bash -c if [ ! "$DISABLED" ]; then systemctl restart named; fi (code=0)
   Process: 23506 ExecStart=/usr/sbin/named -u named -c ${NAMED_CONF} (code=0)
  Main PID: 23507 (named)
    Tasks: 6 (limit: 10373)
   Memory: 9.6M (peak: 9.8M)
      CPU: 526ms
   CGroup: /system.slice/named.service
           └─23507 /usr/sbin/named -u named -c /etc/named.conf

Sep 11 08:15:14 server.edzhibitskaya.net named[23507]: timed out
Sep 11 08:15:14 server.edzhibitskaya.net named[23507]: timed out
```

Рис. 2.22: Перезапуск

Для анализа работы DNS-сервера воспользуемся утилитами dig и host(рис. 2.23) и (рис. 2.24), (рис. 2.25).

```

; <<>> DiG 9.18.33 <<>> ns.edzhibitskaya.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 36598
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDI
TIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0afb7c6c94e8055b0100000068c285686cfc7770a9c4720c (go
od)
;; QUESTION SECTION:
;ns.edzhibitskaya.net.          IN      A

;; AUTHORITY SECTION:
.                10800    IN      SOA      a.root-servers
.net. nstld.verisign-grs.com. 2025091100 1800 900 604800 86400

;; Query time: 1311 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Sep 11 08:16:40 UTC 2025
;; MSG SIZE rcvd: 152

[root@server.edzhibitskaya.net rz]#

```

Рис. 2.23: Описание DNS-зоны с сервера

```

[root@server.edzhibitskaya.net rz]# host -l edzhibitskaya.net
edzhibitskaya.net name server edzhibitskaya.net.
edzhibitskaya.net has address 192.168.1.1
ns.edzhibitskaya.net has address 192.168.1.1
server.edzhibitskaya.net has address 192.168.1.1
[root@server.edzhibitskaya.net rz]# host -A edzhibitskaya.net
Trying "edzhibitskaya.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63946
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDI
TIONAL: 0

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

;; ANSWER SECTION:
edzhibitskaya.net.          86400    IN      SOA      edzhibitskaya.
net. server.edzhibitskaya.net. 2025091100 86400 3600 604800 10
800
edzhibitskaya.net.          86400    IN      NS       edzhibitskaya.
net.

```

Рис. 2.24: host -l; host -a

```
[root@server.edzhibitskaya.net rz]# host -t A edzhibitskaya.net
edzhibitskaya.net has address 192.168.1.1
[root@server.edzhibitskaya.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.edzhibitskaya.net.
1.1.168.192.in-addr.arpa domain name pointer server.edzhibitskaya.net.
[root@server.edzhibitskaya.net rz]#
```

Рис. 2.25: host -t

Наконец, в каталог для внесения изменений в настройки внутреннего окружения добавим необходимые директории(рис. 2.26), создадим исполняемый файл(рис. 2.27) и пропишем скрипт(рис. 2.28).

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

Рис. 2.26: Добавление изменений

```
[root@server.edzhibitskaya.net vagrant]# cd provision/server/
[root@server.edzhibitskaya.net server]# touch dns.sh
[root@server.edzhibitskaya.net server]# chmod +x dns.sh
[root@server.edzhibitskaya.net server]# nano dns.sh
```

Рис. 2.27: Создание файла

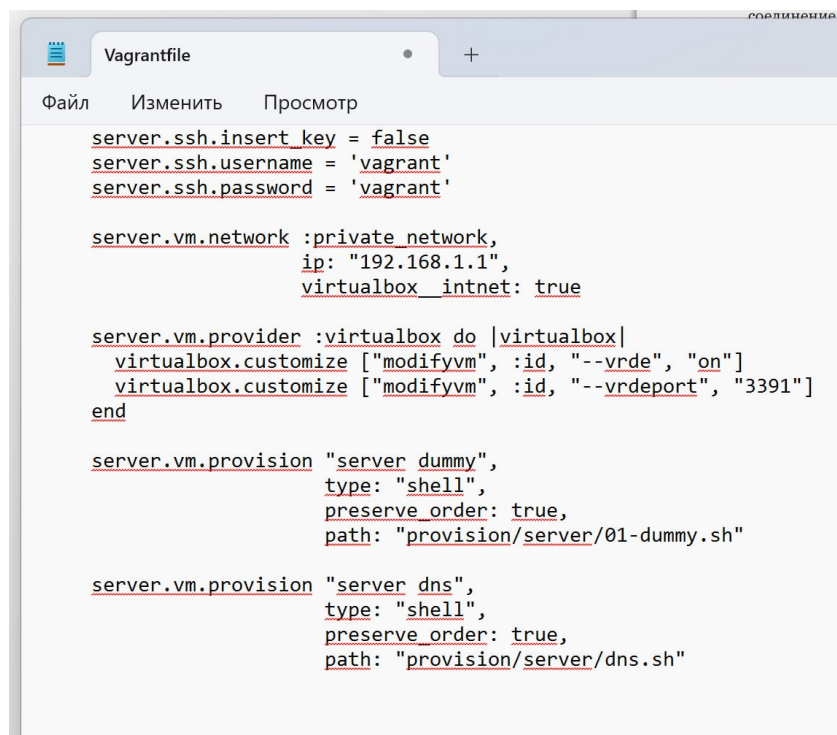
```

GNU nano 8.1                                dns.sh                                Modifi
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install bind bind-utils
echo "Copy configuration files"
cp -R /vagrant/provision/server/dns/etc/* /etc
cp -R /vagrant/provision/server/dns/var/named/* /var/named
chown -R named:named /etc/named
chown -R named:named /var/named
restorecon -vR /etc
restorecon -vR /var/named
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent
echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1
echo "Change dns server address"
nmcli connection edit "System eth0" <<EOF
remove ipv4.dns

```

Рис. 2.28: Скрипт

Внесем изменения в Vagrantfile для отработки скрипта(рис. 2.29).



```

Vagrantfile
Файл  Изменить  Просмотр
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.provider :virtualbox do |virtualbox|
  virtualbox.customize ["modifyvm", :id, "--vrde", "on"]
  virtualbox.customize ["modifyvm", :id, "--vrdeport", "3391"]
end

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. 2.29: Vagrantfile

3 Ответы на контрольные вопросы

1. Что такое DNS?

Система доменных имён, преобразующая имена в IP-адреса и обратно.

2. Каково назначение кэширующего DNS-сервера?

Кэшировать DNS-запросы для ускорения ответов и снижения сетевой нагрузки.

3. Чем отличается прямая DNS-зона от обратной?

- Прямая: имя → IP
- Обратная: IP → имя

4. В каких каталогах и файлах настройки DNS-сервера?

- `/etc/named.conf` – главный конфиг
- `/var/named/` – файлы зон (зона.db)

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

Адреса DNS-серверов для клиента: `nameserver 8.8.8.8`

6. Какие есть типы записей ресурсов?

- A – IPv4 адрес
- AAAA – IPv6 адрес

- CNAME – псевдоним
- MX – почтовый сервер
- NS – DNS-сервер зоны
- PTR – обратная запись (IP → имя)

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

Для организации обратных зон DNS (поиск имени по IP).

8. Для чего нужен демон named?

Это основная служба DNS-сервера BIND, обрабатывающая запросы.

9. Функции master/slave серверов?

- Master – авторитативный, хранит оригиналы зон
- Slave – резервный, копирует зоны с master

10. Параметры времени обновления зоны?

- refresh – время обновления
- retry – время повтора при ошибке
- expire – время устаревания
- TTL – время жизни кэша

11. Как защитить зону от скачивания?

Настроить ACL и запретить трансфер зоны для посторонних.

12. Запись для почтовых серверов?

MX (Mail Exchange).

13. Как протестировать DNS?

Команды: nslookup, dig, host.

14. Управление службами?

- systemctl start
- systemctl stop
- systemctl restart

15. Просмотр отладочной информации?

journalctl -u

16. Где хранятся логи?

/var/log/. Просмотр: journalctl, tail -f /var/log/messages

17. Какие файлы использует процесс?

lsof -p

18. Примеры nmcli:

- nmcli con up eth0
- nmcli con modify eth0 ipv4.addresses "192.168.1.10/24"

19. Что такое SELinux?

Система принудительного контроля доступа, дополняющая стандартные права.

20. Что такое контекст SELinux?

Метка безопасности, определяющая политику доступа для объекта.

21. Как восстановить контекст?

```
restorecon -Rv /путь/
```

22. Как создать правила из логов?

```
audit2allow -a -М модуль
```

23. Булевый переключатель?

Параметр, который можно включить или выключить для изменения поведения политики.

24. Список переключателей?

```
getsebool -a
```

25. Изменение переключателя?

```
setsebool -P httpd_can_network_connect on
```

4 Выводы

В ходе работы были получены навыки по установке и конфигурированию DNS-сервера, усвоены принципы работы системы доменных имён на ОС Rocky linux.

Список литературы

[ТУИС]{https://esystem.rudn.ru/pluginfile.php/2854732/mod_resource/content/8/002-dns.pdf}