

Лабораторная работа №2

Настройка DNS-сервера

Демидова Екатерина Алексеевна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Установка DNS-сервера	6
3.2	Конфигурирование кэширующего DNS-сервера	8
3.2.1	Конфигурирование кэширующего DNS-сервера при отсут- ствии фильтрации DNS-запросов маршрутизаторами . . .	8
3.2.2	Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами	16
3.2.3	Конфигурирование первичного DNS-сервера	17
3.2.4	Анализ работы DNS-сервера	21
3.2.5	Внесение изменений в настройки внутреннего окружения виртуальной машины	22
4	Контрольные вопросы	25
5	Выводы	33

Список иллюстраций

3.1	Установка утилит на виртуальной машине server	6
3.2	Запрос к DNS-адресу www.yandex.ru	7
3.3	Запуск dns-сервера и выполнение команд dig	14
3.4	Изменение адреса сервера	15
3.5	Настройка направления DNS-запросов от всех узлов внутренней сети	15
3.6	Внесение изменения в настройки и проверка их корректности . .	16
3.7	Изменение файла named.conf	17
3.8	Копирование и переименование файла DNS-зон	17
3.9	Изменение файла eademidova.net	18
3.10	Добавление подкаталогов для файлов прямой и обратной зоны и копирование шаблона прямой зоны	18
3.11	Изменение файла прямой зоны	19
3.12	Копирование и переименования шаблона обратной DNS-зоны . .	19
3.13	Изменение файла обратной зоны	20
3.14	Восстановление меток безопасности и проверка состояния пере- ключателей в SELinux	20
3.15	Запуск расширенного лога системных сообщений	21
3.16	Перезапуск DNS-сервера	21
3.17	Описание DNS-зоны с сервера ns.eademidova.net	22
3.18	Проверка корректности работы DNS-сервера	22
3.19	Создание каталога dns и перенос в него файлов, создание dns.sh .	23
3.20	Изменение файла dns.sh	23
3.21	Изменение файла Vagrantfile	24
4.1	Пример использования lsof	29
4.2	Изменение адреса сервера	30

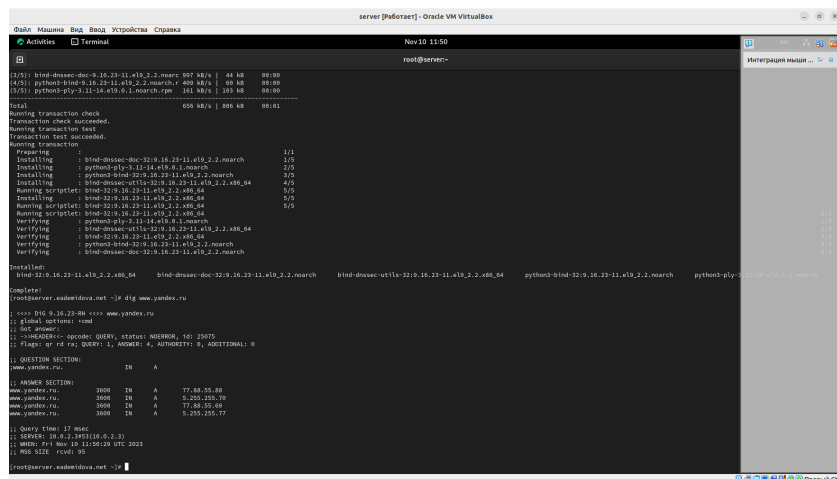
1 Цель работы

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

2 Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils.
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер.
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер.
4. При помощи утилит dig и host проанализируйте работу DNS-сервера.
5. Напишите скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile

С помощью утилиты dig сделаем запрос к DNS-адресу www.yandex.ru(рис. 3.2):



```
Nov 10 11:50
root@server-
3/5: bind-dnssec-dbg-9.16.23-11.el9_2.2.noarch 987 kB/s | 44 kB 00:00
4/5: python3-bind-9.16.23-11.el9_2.2.noarch.r 409 kB/s | 68 kB 00:00
5/5: python3-py-9.16.23-11.el9_2.2.noarch.rpm 181 kB/s | 193 kB 00:00
-----
Total: 656 kB/s | 806 kB 00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : bind-dnssec-dbg-9.16.23-11.el9_2.2.noarch 1/1
Installing : python3-py-9.16.23-11.el9_2.2.noarch 2/5
Installing : python3-bind-9.16.23-11.el9_2.2.noarch 3/5
Installing : bind-dnssec-attls-12.0.10-2.2.el9_2.2.noarch 4/5
Running scriptlet: bind-9.16.23-11.el9_2.2.noarch 5/5
Installing : bind-12.0.10-2.2.el9_2.2.noarch 6/5
Running scriptlet: bind-12.0.10-2.2.el9_2.2.noarch 7/5
Verifying : python3-py-9.16.23-11.el9_2.2.noarch 1/1
Verifying : bind-dnssec-attls-12.0.10-2.2.el9_2.2.noarch 2/5
Verifying : bind-12.0.10-2.2.el9_2.2.noarch 3/5
Verifying : python3-bind-9.16.23-11.el9_2.2.noarch 4/5
Verifying : bind-dnssec-dbg-9.16.23-11.el9_2.2.noarch 5/5
Installed:
bind-12.0.10-2.2.el9_2.2.noarch bind-dnssec-attls-12.0.10-2.2.el9_2.2.noarch python3-bind-9.16.23-11.el9_2.2.noarch python3-py-9.16.23-11.el9_2.2.noarch
Complete!
root@server-nadmedova.net ~# dig www.yandex.ru
; <<>>> DIG 9.16.23-RH <>> www.yandex.ru
; global options: none
; GET answer:
; ==HEADER== opcode: QUERY, status: NOERROR, tid: 25075
; flags: qr rd ra QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0
; QUESTION SECTION:
; www.yandex.ru. IN A
; ANSWER SECTION:
www.yandex.ru. 3000 IN A 77.88.55.89
www.yandex.ru. 3000 IN A 5.255.255.70
www.yandex.ru. 3000 IN A 77.88.55.89
www.yandex.ru. 3000 IN A 5.255.255.77
; Query time: 17 msec
; SERVER: 10.0.2.15(10.0.2.15)
; WHEN: Fri Nov 10 11:50:24 UTC 2023
; MSG SIZE rcvd: 95
root@server-nadmedova.net ~#
```

Рис. 3.2: Запрос к DNS-адресу www.yandex.ru

Проанализируем вывод:

HEADER — отображает информацию о версии утилиты, ID запроса, полученных ошибках и использованных флагах вывода, о количестве запросов, обращений к DNS-серверу.

В нашем случае версия утилиты Dig 9.16.23-RH, затем написан адрес, к которому мы делаем запрос. В следующей строке указаны глобальные опции, используемые командой, у нас это cmd+, говорящая, что нужно отображать аргументы при анализе. В следующей строке указан код операции(opcode) как запрос(QUERY), статус без ошибок и ID процесса – 25075. В следующей строке указаны флаги qr(указывающий, что мы производим запрос), rd{сервер не авторитетный, поэтому он выполнит рекурсивный запрос, чтобы найти ответ}. ra(указывает, что сервер поддерживает рекурсивный запрос), количество запросов – 1, ответов – 4, сервер не авторитетный(указано 0).

QUESTION SECTION — секция, которая отображает текущий запрос. В ней указан адрес, которому производится запрос, указан тип ресурсной записи A(адрес IPv4),

ANSWER SECTION — секция, в которой отображается результат обработки

созданного запроса (в данном случае это IP-адрес домена). Также можно увидеть адрес, тип ресурсной записи, адреса домена, описано 4 запроса. Затем указано время запроса – 17 мс, адрес сервера, дата запроса и размер запроса.

3.2 Конфигурирование кэширующего DNS-сервера

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

В отчёте проанализируем построчно содержание файлов `/etc/resolv.conf`, `/etc/named.conf`, `/var/named/named.ca`, `/var/named/named.localhost`, `/var/named/named.loopback`.

Рассмотрим `/etc/resolv.conf`. В нём указано имя сервера и его адрес:

```
# Generated by NetworkManager
search eademidova.net
nameserver 10.0.2.3
```

Рассмотрим `/etc/named.conf` (анализ указан комментариями к строкам):

```
//
// 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.
//

\\ опции
options {
    listen-on port 53 { 127.0.0.1; }; \\ адрес IPv4 DNS-порта, с которого идет э
```



```

listen-on-v6 port 53 { ::1; }; \\ \\ адрес IPv6 порта, с которого идет запрос
directory "/var/named"; \\ путь к директории
dump-file "/var/named/data/cache_dump.db"; \\ путь к файлу с кэшем дампа памяти
statistics-file "/var/named/data/named_stats.txt"; \\ путь к файлу статистики
memstatistics-file "/var/named/data/named_mem_stats.txt"; \\ путь к файлу, где хранятся статистики
secroots-file "/var/named/data/named.secroots"; \\ путь к файлу, в который записываются секреты
recursing-file "/var/named/data/named.recursing"; \\ путь к файлу, который используется для рекурсии

\\ разрешение запросов локальному хосту
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 control to limit queries to your legitimate users. Failing to do so will cause your server to become part of large scale DNS amplification attacks. Implementing BCP38 within your network would greatly reduce such attack surface
*/

\\рекурсия задана
recursion yes;

\\ проверка безопасности dns задана
dnssec-validation yes;

managed-keys-directory "/var/named/dynamic"; \\ задает директорию ключей управления
geoip-directory "/usr/share/GeoIP"; \\ задает директорию, содержащую GeoIP

```

```

pid-file "/run/named/named.pid"; \\ Указывает путь к файлу, в который сервер
session-keyfile "/run/named/session.key"; \\ Указывает путь к файлу, в которо

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

\\ channel связывает методы вывода, параметры формата и уровни серьезности с имен

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic; \\ указана динамическая серьезность, сервер име
    };
};

\\ класс зоны IN, тип hint

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

\\ подключение файлов

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

Рассмотрим содержимое файла /var/named/named.ca:

```
; <<>> DiG 9.11.3-RedHat-9.11.3-3.fc27 <<>> +bufsize=1200 +norec @a.root-
```

```

servers.net \\ указана версия dig
; (2 servers found) \\ количество найденных серверов
;; global options: +cmd \\ глобальная опция
;; Got answer: \\ получен ответ
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46900 \\ тип сообщения запрос
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27 \\ выслан

;; OPT PSEUDOSECTION: \\псевдораздел(часть раздела additional)
; EDNS: version: 0, flags:; udp: 1472 \\ версия EDNS6 флаги и размер UDP пакета
;; QUESTION SECTION:
; .                IN  NS

\\ раздел с полученными ответами
;; ANSWER SECTION:
.                518400  IN  NS  a.root-servers.net. \\ указан NS — запись, содержащая
.                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.

\\ В этом разделе мы получаем IP-адреса серверов имен из предыдущего раздела
;; ADDITIONAL SECTION:

```

```

a.root-servers.net. 518400 IN A 198.41.0.4 \\ A - указаны адреса версии 4
b.root-servers.net. 518400 IN A 199.9.14.201
c.root-servers.net. 518400 IN A 192.33.4.12
d.root-servers.net. 518400 IN A 199.7.91.13
e.root-servers.net. 518400 IN A 192.203.230.10
f.root-servers.net. 518400 IN A 192.5.5.241
g.root-servers.net. 518400 IN A 192.112.36.4
h.root-servers.net. 518400 IN A 198.97.190.53
i.root-servers.net. 518400 IN A 192.36.148.17
j.root-servers.net. 518400 IN A 192.58.128.30
k.root-servers.net. 518400 IN A 193.0.14.129
l.root-servers.net. 518400 IN A 199.7.83.42
m.root-servers.net. 518400 IN A 202.12.27.33
a.root-servers.net. 518400 IN AAAA 2001:503:ba3e::2:30 \\ Аффф - указаны адр
b.root-servers.net. 518400 IN AAAA 2001:500:200::b
c.root-servers.net. 518400 IN AAAA 2001:500:2::c
d.root-servers.net. 518400 IN AAAA 2001:500:2d::d
e.root-servers.net. 518400 IN AAAA 2001:500:a8::e
f.root-servers.net. 518400 IN AAAA 2001:500:2f::f
g.root-servers.net. 518400 IN AAAA 2001:500:12::d0d
h.root-servers.net. 518400 IN AAAA 2001:500:1::53
i.root-servers.net. 518400 IN AAAA 2001:7fe::53
j.root-servers.net. 518400 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 518400 IN AAAA 2001:7fd::1
l.root-servers.net. 518400 IN AAAA 2001:500:9f::42
m.root-servers.net. 518400 IN AAAA 2001:dc3::35

```

```
;; Query time: 24 msec \\ время запроса
```

```
;; SERVER: 198.41.0.4#53(198.41.0.4) \\ адрес сервера
```

```
;; WHEN: Thu Apr 05 15:57:34 CEST 2018 \\дата запроса
;; MSG SIZE rcvd: 811 \\ размер сообщения
```

Рассмотрим содержимое файла /var/named/named.loopback. В нём указаны:

- Запись начала полномочий (SOA), которая указывает начало зоны и включает имя хоста, на котором находится файл данных name.local.
- Запись сервера имен (NS), идентифицирующая главный и подчиненные серверы имен DNS.
- Указаны адреса IPv4 и IPv6 локального хоста.
- PTR-запись для локального хоста

```
$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.
```

Запустим DNS-сервер, включим запуск DNS-сервера в автозапуск при загрузке системы. Проанализируем отличие в выведенной на экран информации при выполнении команд `dig www.yandex.ru` и `dig [127.0.0.1?] www.yandex.ru` (рис. 3.3):

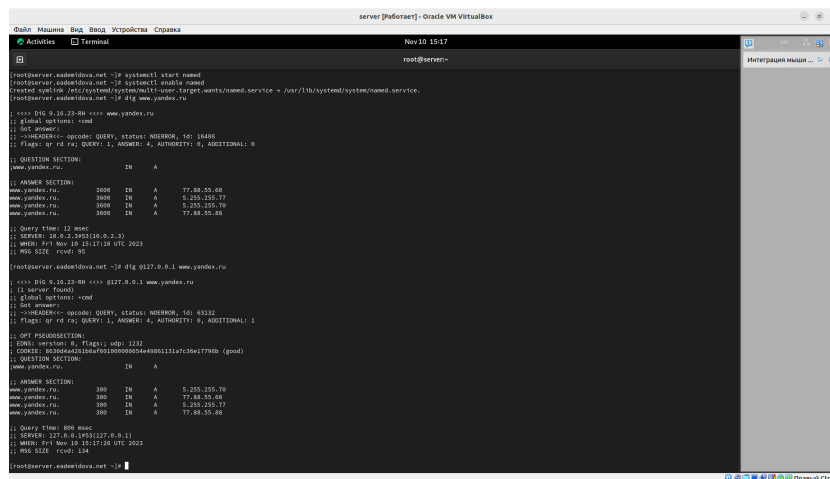


Рис. 3.3: Запуск dns-сервера и выполнение команд dig

При указании опрашиваемого адреса в строке с адресом сервера написан адрес, который указывали, также указаны куки. Время запроса увеличивается.

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`, затем сделаем тоже самое для соединения `System eth0`. Затем запустим `NetworkManager` и проверим наличие изменений в файле `etc/resolv.conf` (адрес сервера изменился на заданный нами) (рис. 3.4):

```
[root@server.eadimidova.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, 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' (7e9d53f3-08ca-4107-918c-dd8379b0a5e4) successfully updated.
nmcli> quit
[root@server.eadimidova.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-lx, 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' (5fb6bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
[root@server.eadimidova.net ~]# systemctl restart NetworkManager
[root@server.eadimidova.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search eadimidova.net
nameserver 127.0.0.1
[root@server.eadimidova.net ~]#
```

Рис. 3.4: Изменение адреса сервера

Требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесем изменения в файл /etc/named.conf(рис. 3.5):

```
mc [root@server.eadimidova.net]:/etc
named.conf [-M--] 52 L: [ 5+18 23/ 60] *(794 /1743b) 0032 0x020 [
// 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 recursion.
<----->- If you are building a RECURSIVE (caching) DNS server, you need to enable.
<-----> recursion..

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Qui
```

Рис. 3.5: Настройка направления DNS-запросов от всех узлов внутренней сети

Внесем изменения в настройки межсетевого экрана узла server, разрешив работу с DNS и убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53(3.6):

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

```

avahi-daemon	562	avahi	12u	IPv4	18774	0t0	UDP *:mdns	
avahi-daemon	562	avahi	13u	IPv6	18775	0t0	UDP *:mdns	
avahi-daemon	562	avahi	14u	IPv4	18776	0t0	UDP *:45613	
avahi-daemon	562	avahi	15u	IPv6	18777	0t0	UDP *:52048	
chronyd	583	chrony	5u	IPv4	18629	0t0	UDP localhost:323	
chronyd	583	chrony	6u	IPv6	18630	0t0	UDP localhost:323	
named	10369	named	16u	IPv4	75512	0t0	UDP localhost:domain	
named	10369	named	19u	IPv6	75514	0t0	UDP localhost:domain	
named	10369 10370	isc-net-0	named	16u	IPv4	75512	0t0	UDP localhost:domain
named	10369 10370	isc-net-0	named	19u	IPv6	75514	0t0	UDP localhost:domain
named	10369 10371	isc-timer	named	16u	IPv4	75512	0t0	UDP localhost:domain
named	10369 10371	isc-timer	named	19u	IPv6	75514	0t0	UDP localhost:domain
named	10369 10372	isc-socket	named	16u	IPv4	75512	0t0	UDP localhost:domain
named	10369 10372	isc-socket	named	19u	IPv6	75514	0t0	UDP localhost:domain
named	10369 10403	isc-net-0	named	16u	IPv4	75512	0t0	UDP localhost:domain
named	10369 10403	isc-net-0	named	19u	IPv6	75514	0t0	UDP localhost:domain
NetworkManager	10582	root	27u	IPv4	78208	0t0	UDP server.eademidova.net:bootpc->_gateway:bootps	
NetworkManager	10582 10588	psm	root	27u	IPv4	78208	0t0	UDP server.eademidova.net:bootpc->_gateway:bootps
NetworkManager	10582 10589	gdbus	root	27u	IPv4	78208	0t0	UDP server.eademidova.net:bootpc->_gateway:bootps

```
[root@server.eademidova.net etc]#
```

Рис. 3.6: Внесение изменения в настройки и проверка их корректности

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

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

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

Текущий список DNS-серверов можно получить, введя на локальном хосте (на котором развёртывается образ виртуальной машины) следующую команду:

```
cat /etc/resolv.conf
```

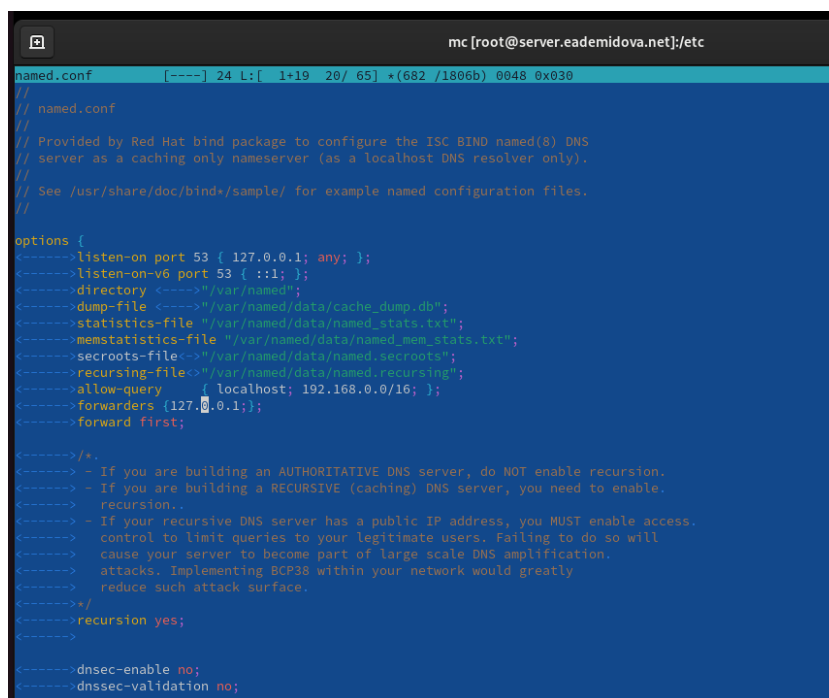
Мы получили следующие данные для конфигурационного файла `named.conf` виртуальной машины `server` (рис. 3.7):

```
forwarders { 127.0.0.1; };
forward first;
```


Кроме того, возможно вышестоящий DNS-сервер может не поддерживать технологию DNSSEC, тогда следует в конфигурационном файле `named.conf` указать следующие настройки(рис. 3.7):

```
dnssec-enable no;
```

```
dnssec-validation no;
```



```
named.conf [----] 24 L: [ 1+19 20/ 65] *(682 /1806b) 0048 0x030
// 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; 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;

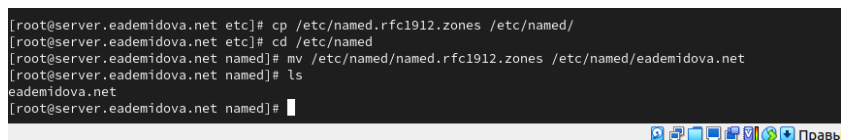
<----->*/
<----->- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
<----->- If you are building a RECURSIVE (caching) DNS server, you need to enable.
<----->recursion..
<----->- If your recursive DNS server has a public IP address, you MUST enable access.
<----->control to limit queries to your legitimate users. Failing to do so will
<----->cause your server to become part of large scale DNS amplification.
<----->attacks. Implementing BCP38 within your network would greatly
<----->reduce such attack surface.
<----->*/
<----->recursion yes;

<----->dnssec-enable no;
<----->dnssec-validation no;
```

Рис. 3.7: Изменение файла `named.conf`

3.2.3 Конфигурирование первичного DNS-сервера

Скопируем шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименуем его в `eademidova.net` (3.8):



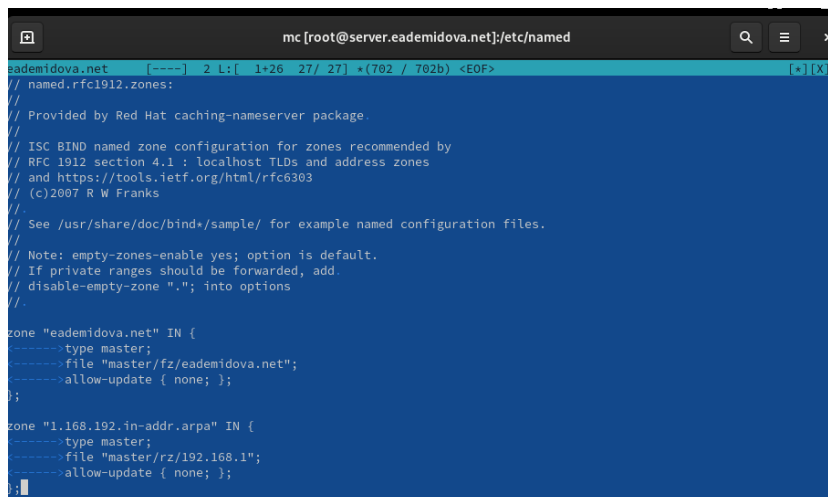
```
[root@server.eademidova.net etc]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.eademidova.net etc]# cd /etc/named
[root@server.eademidova.net named]# mv /etc/named/named.rfc1912.zones /etc/named/eademidova.net
[root@server.eademidova.net named]# ls
eademidova.net
[root@server.eademidova.net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

Рис. 3.8: Копирование и переименование файла DNS-зон

Включим файл описания зоны /etc/named/eademidova.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку:

```
include "/etc/named/user.net";
```

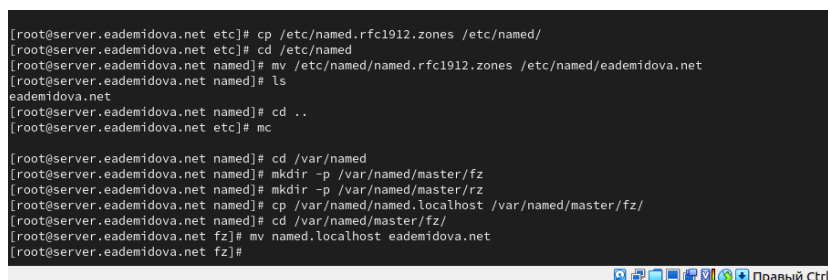
Внесём изменения в файл eademidova.net(рис. 3.9):



```
mc [root@server.eademidova.net]:/etc/named
eademidova.net [-----] 2 L: [ 1+26 27/ 27] *(702 / 702b) <EOF> [X]
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package.
//
// 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 files.
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add
// disable-empty-zone "."; into options
//
zone "eademidova.net" IN {
-----type master;
-----file "master/fz/eademidova.net";
-----allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
-----type master;
-----file "master/rz/192.168.1";
-----allow-update { none; };
};
```

Рис. 3.9: Изменение файла eademidova.net

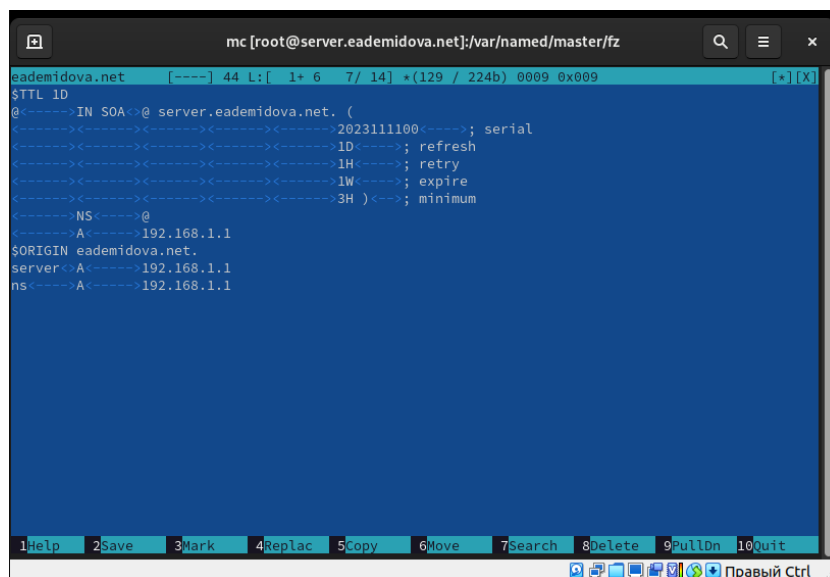
В каталоге /var/named создадим подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно, а затем скопируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуем его в eademidova.net(рис. 3.10):



```
[root@server.eademidova.net etc]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.eademidova.net etc]# cd /etc/named
[root@server.eademidova.net named]# mv /etc/named/named.rfc1912.zones /etc/named/eademidova.net
[root@server.eademidova.net named]# ls
eademidova.net
[root@server.eademidova.net named]# cd ..
[root@server.eademidova.net etc]# mc
[root@server.eademidova.net named]# cd /var/named
[root@server.eademidova.net named]# mkdir -p /var/named/master/fz
[root@server.eademidova.net named]# mkdir -p /var/named/master/rz
[root@server.eademidova.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.eademidova.net named]# cd /var/named/master/fz/
[root@server.eademidova.net fz]# mv named.localhost eademidova.net
[root@server.eademidova.net fz]#
```

Рис. 3.10: Добавление подкаталогов для файлов прямой и обратной зоны и копирование шаблона прямой зоны

Изменим файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны(рис. 3.11):

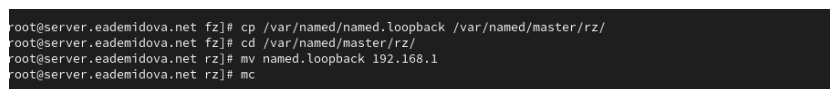


```
mc [root@server.eademidova.net]:/var/named/master/fz
eademidova.net  [----] 44 L: [ 1+ 6 7/ 14] *(129 / 224b) 0009 0x009  [*] [X]
$TTL 1D
@<----->IN SOA<-->@ server.eademidova.net. (
<-----><-----><-----><-----><----->2023111100<----->; serial
<-----><-----><-----><-----><----->1D<----->; refresh
<-----><-----><-----><-----><----->1H<----->; retry
<-----><-----><-----><-----><----->1W<----->; expire
<-----><-----><-----><-----><----->3H<----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
$ORIGIN eademidova.net.
server<-->A<----->192.168.1.1
ns<----->A<----->192.168.1.1

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
Правый Ctrl
```

Рис. 3.11: Изменение файла прямой зоны

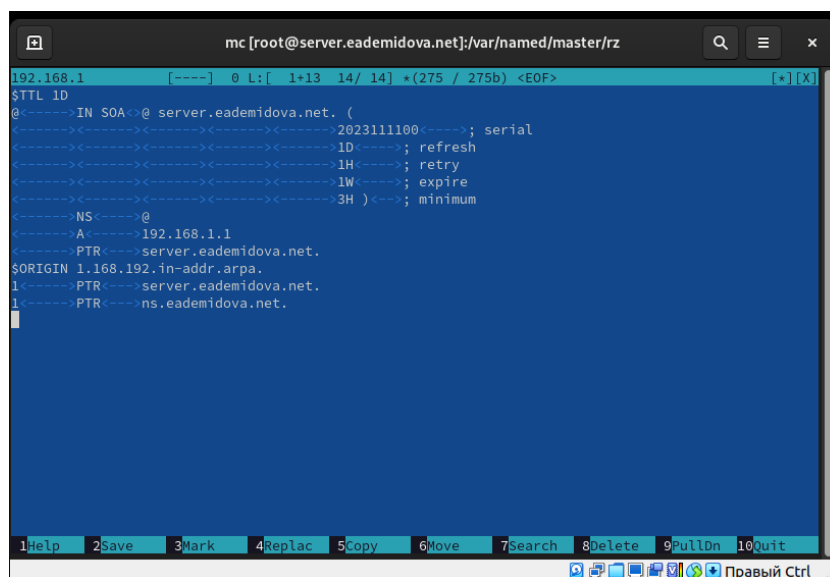
Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1(рис. 3.12):



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

Рис. 3.12: Копирование и переименования шаблона обратной DNS-зоны

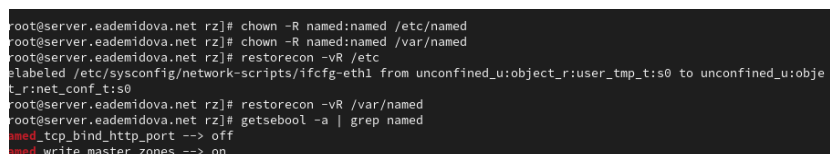
Изменим файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны(рис. 3.13):



```
mc [root@server.eademidova.net]:/var/named/master/rz
192.168.1 0 L: 1+13 14/ 14] *(275 / 275b) <EOF> [*] [X]
$TTL 1D
@<----->IN SOA<@ server.eademidova.net. (
<----->2023111100<----->; serial
<----->1D<----->; refresh
<----->1H<----->; retry
<----->1W<----->; expire
<----->3H<----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
<----->PTR<----->server.eademidova.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<----->PTR<----->server.eademidova.net.
1<----->PTR<----->ns.eademidova.net.
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
Правый Ctrl
```

Рис. 3.13: Изменение файла обратной зоны

После изменения доступа к конфигурационным файлам named корректно восстановим специальные метки безопасности в SELinux, затем проверим состояние переключателей(рис. 3.14)



```
root@server.eademidova.net rz]# chown -R named:named /etc/named
root@server.eademidova.net rz]# chown -R named:named /var/named
root@server.eademidova.net rz]# restorecon -vR /etc
labeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:obje
t_r:net_conf_t:s0
root@server.eademidova.net rz]# restorecon -vR /var/named
root@server.eademidova.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
```

Рис. 3.14: Восстановление меток безопасности и проверка состояния переключателей в SELinux

Во дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы(3.15):

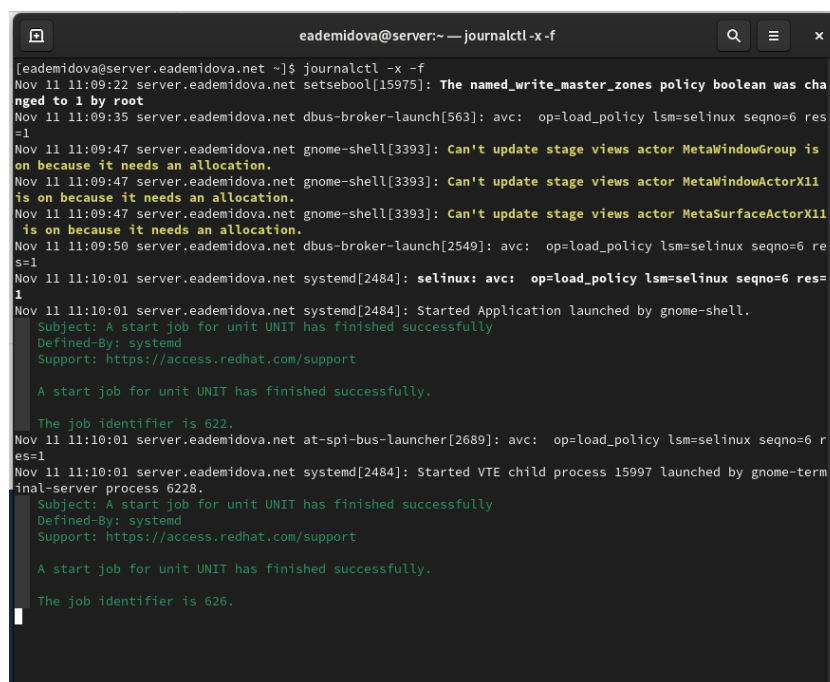


Рис. 3.15: Запуск расширенного лога системных сообщений

Перезапустим DNS-сервер(3.16):

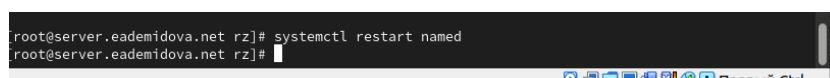


Рис. 3.16: Перезапуск DNS-сервера

3.2.4 Анализ работы DNS-сервера

При помощи утилиты dig получим описание DNS-зоны с сервера ns.eademidova.net(3.17):

```
root@server.eademidova.net rz]# systemctl restart named
root@server.eademidova.net rz]# dig ns.eademidova.net

<<> DiG 9.16.23-RH <<> ns.eademidova.net
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 53214
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
EDNS: version: 0, flags:; udp: 1232
COOKIE: 0ef3f1f9d05737d01000000654f671a5101a42f7026ed8f (good)
;; QUESTION SECTION:
ns.eademidova.net.          IN      A

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

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Sat Nov 11 11:35:54 UTC 2023
; MSG SIZE rcvd: 90

root@server.eademidova.net rz]#
```

Рис. 3.17: Описание DNS-зоны с сервера ns.eademidova.net

При помощи утилиты `host` проанализируем корректность работы DNS-сервера, можно увидеть, что все внесённые нами изменения в работу сервера учтены(3.21):

```
[root@server.eademidova.net rz]# host -l eademidova.net
eademidova.net name server eademidova.net.
eademidova.net has address 192.168.1.1
ns.eademidova.net has address 192.168.1.1
server.eademidova.net has address 192.168.1.1
[root@server.eademidova.net rz]# host -a eademidova.net
Trying "eademidova.net"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 13333
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
eademidova.net.          IN      ANY

;; ANSWER SECTION:
eademidova.net.        86400  IN      SOA      eademidova.net. server.eademidova.net. 2023111100 86400 3600 604800 10800
eademidova.net.        86400  IN      NS       eademidova.net.
eademidova.net.        86400  IN      A        192.168.1.1

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

Received 121 bytes from 127.0.0.1#53 in 0 ms
[root@server.eademidova.net rz]# host -t A eademidova.net
eademidova.net has address 192.168.1.1
[root@server.eademidova.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.eademidova.net.
1.1.168.192.in-addr.arpa domain name pointer server.eademidova.net.
[root@server.eademidova.net rz]#
```

Рис. 3.18: Проверка корректности работы DNS-сервера

3.2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине `server` перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём ка-

талог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS, а затем в каталоге /vagrant/provision/server создадим исполняемый файл dns.sh(3.19):

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

Рис. 3.19: Создание каталога dns и перенос в него файлов, создание dns.sh

Запишем в dns.sh следующий скрипт(3.20):

```
mc [root@server.eademidova.net]:/vagrant/provision/server
dns.sh  [-M--] 11 L: 1+ 0 1/ 30) *(11 / 813b) 0010 0x00A
#!/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 "Restart NetworkManager"
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
```

Рис. 3.20: Изменение файла dns.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в разделе конфигурации для сервера(??):

```

[root@server.eademidova.net rz]# host -l eademidova.net
eademidova.net name server eademidova.net.
eademidova.net has address 192.168.1.1
ns.eademidova.net has address 192.168.1.1
server.eademidova.net has address 192.168.1.1
[root@server.eademidova.net rz]# host -a eademidova.net
Trying "eademidova.net"
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 13333
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
eademidova.net.      86400   IN      SOA     eademidova.net. server.eademidova.net. 2023111100 86400 3600 604800 10800
eademidova.net.      86400   IN      NS      eademidova.net.
eademidova.net.      86400   IN      A       192.168.1.1

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

Received 121 bytes from 127.0.0.1#53 in 0 ms
[root@server.eademidova.net rz]# host -t A eademidova.net
eademidova.net has address 192.168.1.1
[root@server.eademidova.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.eademidova.net.
1.1.168.192.in-addr.arpa domain name pointer server.eademidova.net.
[root@server.eademidova.net rz]#

```

Рис. 3.21: Изменение файла Vagrantfile

4 Контрольные вопросы

1. Что такое DNS?

Система доменных имён (Domain Name System, DNS) — распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес, и наоборот.

2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.

3. Чем отличается прямая DNS-зона от обратной?

Прямая DNS зона - зона хранения записей соответствия доменного имени ip адресу. Обратная DNS зона - зона хранения записей соответствия ip адреса доменному имени.

4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.

В каталоге /etc хранится файл `named.conf`, в котором есть информация об опциях сервера, его разрешениях, настройках безопасности и подключены файлы зон. В каталоге /named хранится файл описания DNS-зон, также в каталоге /var/named хранится файл `named.loopback`, описывающий обратную зону, и файл `named.localhost`, описывающий прямую зону.

5. Что указывается в файле resolv.conf?

В этом файле указывается имя сервера и его адрес, например:

```
# Generated by NetworkManager
search eademidova.net
nameserver 10.0.2.3
```

6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?

Основные типы ресурсных записей (Resource Records):

- А-запись — задает преобразование имени хоста в IP-адрес.
- MX-запись — определяет почтовый ретранслятор для доменного имени, т.е. узел, который обработает или передаст дальше почтовые сообщения, предназначенные адресату в указанном домене. При наличии нескольких MX-записей сначала происходит попытка доставить почту на ретранслятор с наименьшим приоритетом.
- NS-записи — определяют DNS-серверы, которые являются авторитативными для данной зоны.
- CNAME-запись — определяет отображение псевдонима в каноническое имя узла.
- SRV-запись — позволяет получить имя для искомой службы, а также протокол, по которому эта служба работает.
- TXT-запись — содержит общую текстовую информацию. Эти записи могут использоваться в любых целях, например, для указания месторасположения хоста.
- AAAA-запись — задает преобразование имени хоста в IPV6-адрес.
- SSHFP-запись — используется для хранения слепка ключей SSH в DNS.

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

Домен in-addr.arpa используется для всех сетей TCP/IP, основанным на адресации протокола Интернета 4 (IPv4).

8. Для чего нужен демон named?

Демон named отвечает на запросы об именах машин и их IP-адресах. Если named не знает ответа на какой-либо запрос, он опрашивает другие серверы и помещает их ответы в кэш. Этот демон, кроме того, отвечает за выполнение зонных пересылок, обеспечивающих копирование данных между серверами одного домена. Запросы демона named используют протокол UDP и порт 53. Если объем ответов превышает 512 байтов, то для их доставки используется протокол TCP. В зонных пересылках между серверами также применяется протокол TCP.

9. В чём заключаются основные функции slave-сервера и master-сервера?

Главный (master) — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых; ведомый (slave) — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны.

10. Какие параметры отвечают за время обновления зоны?

SOA-запись (Start of Authority) — начальная запись зоны, которая указывает местоположение эталонной записи о домене. Она хранит параметр TTL – время, в течение которого информация будет кэшироваться другими DNS-серверами. Также параметр Refresh – время (в секундах) ожидания ответа вторичного DNS перед запросом SOA-записи с первичных серверов. По истечении данного времени вторичный DNS обращается к первичному для получения копии текущей SOA-записи. Первичный DNS-сервер выполняет этот запрос. Вторичный DNS-сервер сравнивает полученный серийный номер зоны с имеющимся. Если они отличаются, то осуществляется запрос к первичному DNS-серверу на трансфер зоны. И Expire – время (в секундах), в течение которого вторичный DNS будет

пытаться завершить синхронизацию зоны с первичным. Если это время истечет до того, как синхронизация закончится, то зона на вторичном DNS-сервере перестанет обслуживать запросы об этой зоне.

11. Как обеспечить защиту зоны от скачивания и просмотра?

Можно делать следующее для защиты данных DNS доменов с помощью DNSSEC:

- Подписывать зоны или удалить подпись в соответствии со спецификациями DNSSEC
- (Необязательно) Указывать индивидуальные настройки для создания ключей
- Получать уведомления
- Просматривать и копировать записи ресурсов DS
- Просматривать и копировать наборы записей ресурсов DNSKEY.

12. Какая запись RR применяется при создании почтовых серверов?

Запись MX (от англ. mail exchanger) — тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP.

13. Как протестировать работу сервера доменных имён?

Для этого можно воспользоваться командой `nslookup`, которая позволяет получить информацию о DNS-записях для заданного домена или IP-адреса.

14. Как запустить, перезапустить или остановить какую-либо службу в системе?

- `systemctl restart named` - перезапустить DNS-сервер
- `systemctl stop named` - перезапустить DNS-сервер
- `systemctl start named` - перезапустить DNS-сервер

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

В дополнительном терминале запустит в режиме реального времени расширенный лог системных сообщений:

```
journalctl -x -f
```

16. Где храниться отладочная информация по работе системы и служб? Как её посмотреть?

Журналы службы находятся в директории “/var/log/” в виде обычных текстовых файлов.

17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите пример.

lsof – есокращение от LiSt of Open Files, утилита эта служит для вывода информации о том, какие файлы используются теми или иными процессами.

Пример использования с командой grep(4.2):

```
[root@server.eademidova.net ~]# mc etc/named.conf
[root@server.eademidova.net etc]# firewall-cmd --add-service=dns
success
[root@server.eademidova.net etc]# firewall-cmd --add-service=dns --permanent
success
[root@server.eademidova.net etc]# sof | grep UDP
bash: sof: command not found...
[root@server.eademidova.net etc]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
  avahi-daemon 562      avahi 12u    IPv4 18774      0t0  UDP *:mdns
  avahi-daemon 562      avahi 13u    IPv6 18775      0t0  UDP *:mdns
  avahi-daemon 562      avahi 14u    IPv4 18776      0t0  UDP *:45613
  avahi-daemon 562      avahi 15u    IPv6 18777      0t0  UDP *:52048
  chronyd      583      chrony 5u     IPv4 18620      0t0  UDP localhost:323
  chronyd      583      chrony 6u     IPv6 18630      0t0  UDP localhost:323
  named        10369    named 16u    IPv4 75512      0t0  UDP localhost:domain
  named        10369    named 19u    IPv6 75514      0t0  UDP localhost:domain
  named        10369 10370 tsc-net-0 named 16u    IPv4 75512      0t0  UDP localhost:domain
  named        10369 10370 tsc-net-0 named 19u    IPv6 75514      0t0  UDP localhost:domain
  named        10369 10371 tsc-timer named 16u    IPv4 75512      0t0  UDP localhost:domain
  named        10369 10371 tsc-timer named 19u    IPv6 75514      0t0  UDP localhost:domain
  named        10369 10372 tsc-socket named 16u    IPv4 75512      0t0  UDP localhost:domain
  named        10369 10372 tsc-socket named 19u    IPv6 75514      0t0  UDP localhost:domain
  named        10369 10483 tsc-net-0 named 16u    IPv4 75512      0t0  UDP localhost:domain
  named        10369 10483 tsc-net-0 named 19u    IPv6 75514      0t0  UDP localhost:domain
  NetworkMa   10582    root 27u    IPv4 78208      0t0  UDP server.eademidova.net:bootpc->_gateway:bootps
  NetworkMa   10582 10589 gmain  root 27u    IPv4 78208      0t0  UDP server.eademidova.net:bootpc->_gateway:bootps
[root@server.eademidova.net etc]#
```

Рис. 4.1: Пример использования lsof

18. Приведите примеры по изменению сетевого соединения при помощи командного интерфейса nmcli.

Два примера о изменению сетевого соединения при помощи командного интерфейса nmcli(рис. 4.2):

```

[root@server.eademidova.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, 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' (7e9d53f3-08ca-4107-918c-dd8379b0a5e4) successfully updated.
nmcli> quit
[root@server.eademidova.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-lx, 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' (5fb66bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
[root@server.eademidova.net ~]# systemctl restart NetworkManager
[root@server.eademidova.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search eademidova.net
nameserver 127.0.0.1
[root@server.eademidova.net ~]#

```

Рис. 4.2: Изменение адреса сервера

19. Что такое SELinux?

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.

20. Что такое контекст (метка) SELinux?

SELinux — это система принудительного управления доступом, что означает, что каждый процесс имеет метку (label). Каждый файл, каталог и системный объект так же имеют метки. Правила политики управляют доступом между промаркированными процессами и объектами.

Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами

21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?

После изменения доступа к конфигурационным файлам named требуется корректно восстановить их метки в SELinux:

```
restorecon -vR /etc
```

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

Для проверки состояния переключателей SELinux, относящихся к named, надо ввести:

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

При необходимости дать named разрешение на запись в файлы DNS-зоны:

```
setsebool named_write_master_zones 1
```

```
setsebool -P named_write_master_zones 1
```

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

Чтобы создать необходимые политики:

1. Создайте новый файл с исходным кодом политики SELinux (.te файл). Данный файл определяет ограничения, относящиеся к описываемому модулю.
2. При необходимости отредактируйте сгенерированный исходный файл политики [module_name].te, а затем, используя утилиту checkmodule, создайте бинарное представление (.mod файл) исходного файла локальной политики.
3. Создайте устанавливаемый модуль политики (.pp файл) с помощью утилиты semodule_package.
4. Для установки созданного модуля политики воспользуйтесь утилитой semodule.
5. Что такое булевый переключатель в SELinux?

Булевый переключатель в SELinux - это параметр, который управляет разрешениями безопасности на уровне SELinux. Он может быть включен (true) или выключен (false) и используется для разрешения или запрещения определенных действий.

24. Как посмотреть список переключателей SELinux и их состояние?

Для просмотра списка переключателей SELinux и их состояния можно использовать команду “`semanage boolean -l`” в терминале.

25. Как изменить значение переключателя SELinux?

Чтобы изменить значение переключателя SELinux, можно использовать команду “`setsebool`”. Например, для включения переключателя с именем “`httpd_can_network_connect`” можно выполнить команду “`setsebool -P httpd_can_network_connect 1`”. Здесь -P указывает, что изменение должно быть постоянным (постоянно сохраняться после перезагрузки).

5 Выводы

В результате выполнения данной работы были приобретены практические навыки по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.