

Отчёт по лабораторной работе №2

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

1 Цель работы	6
2 Выполнение лабораторной работы	7
2.1 Установка DNS-сервера	7
2.2 Конфигурирование кэширующего DNS-сервера	8
2.3 Конфигурирование первичного DNS-сервера	15
2.4 Анализ работы DNS-сервера	21
2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины	23
3 Выводы	30

Список иллюстраций

2.1	Переход в режим суперпользователя и установка bind, bind-utils	7
2.2	Запрос с помощью утилиты dig	8
2.3	Просмотр содержания файла /etc/resolv.conf	8
2.4	Просмотр содержания файла /etc/named.conf	9
2.5	Просмотр содержания файла /var/named/named.ca	9
2.6	Просмотр содержания файла /var/named/named.localhost	9
2.7	Просмотр содержания файла /var/named/named.loopback	10
2.8	Запуск DNS-сервера, включение запуска DNS-сервера в автозапуск при загрузке системы, анализ выведенной на экран информации при выполнении команды dig www.yandex.ru и dig 127.0.0.1 www.yandex.ru	11
2.9	Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети. Повторяем действия для соединения System eth0	12
2.10	Перезапуск NetworkManager и проверка наличия изменений в файле /etc/resolv.conf	12
2.11	Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server	13
2.12	Внос изменений в настройки межсетевого экрана узла server, разрешив работу с DNS. Проверка, что DNS-запросы идут через узел server, который прослушивает порт 53	14
2.13	Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек	15
2.14	Копирование шаблона описания DNS-зон из каталога /etc в каталог /etc/named и изменение его названия	15
2.15	Включение файла описания зоны /etc/named/aamishina.net в конфигурационном файле DNS /etc/named.conf	16
2.16	Открытие файла /etc/named/user.net на редактирование. Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле	16

2.17 В каталоге /var/named создание подкаталогов master/fz и master/rz. Копирование шаблона прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и изменение его названия	17
2.18 Изменение файла /var/named/master/fz/aamishina.net, указав необходимые DNS записи для прямой зоны	18
2.19 Копирование шаблона обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и изменение его названия	18
2.20 Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны	19
2.21 Исправление прав доступа к файлам в каталогах /etc/named и /var/named, корректное восстановление их меток в SELinux, проверка состояния переключателей SELinux	20
2.22 Запуск расширенного лога системных сообщений	20
2.23 Проверка корректности работы системы	21
2.24 Перезапуск DNS-сервера	21
2.25 Получение описания DNS-зоны с сервера ns.aamishina.net.	22
2.26 Анализ корректности работы DNS-сервера	22
2.27 Переход в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога dns, в который помещаем конфигурационные файлы DNS. Создание в каталоге /vagrant/provision/server исполняемого файла dns.sh	23
2.28 Открытие файла на редактирование и прописывание в нём скрипта	25
2.29 Добавление параметров в конфигурационном файле Vagrantfile в разделе конфигурации для сервера	26

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Установка DNS-сервера

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом. Далее запустим виртуальную машину server: vagrant up server. На виртуальной машине server войдём под созданным нами в предыдущей работе пользователем и откроем терминал. Перейдём в режим суперпользователя: sudo -i и установим bind и bind-utils: dnf -y install bind bind-utils (рис. 2.1).

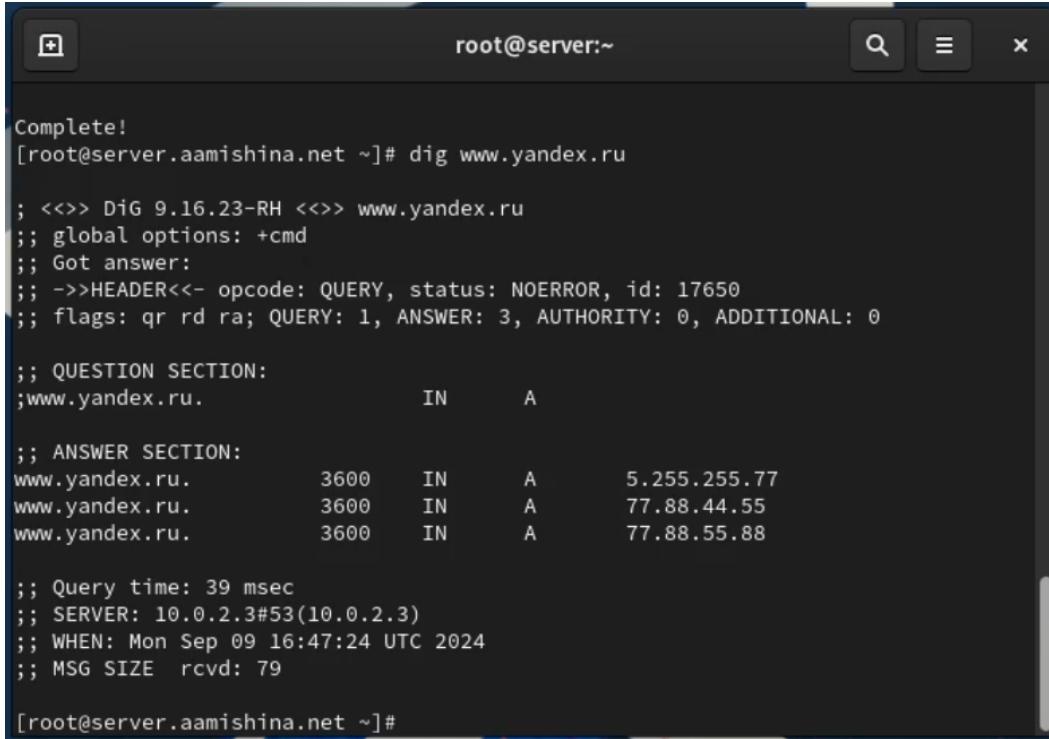
The screenshot shows a terminal window with a dark theme. The title bar says "root@server:~". The terminal content is as follows:

```
[aamishina@server.aamishina.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 aamishina:
[root@server.aamishina.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 9 - x86_64   15 kB/s | 37 kB    00:02
Extra Packages for Enterprise Linux 9 - x86_64   2.2 MB/s | 23 MB    00:10
Rocky Linux 9 - BaseOS                         8.5 kB/s | 4.1 kB   00:00
Rocky Linux 9 - AppStream                      4.5 kB/s | 4.5 kB   00:00
Rocky Linux 9 - AppStream                      1.2 MB/s | 8.0 MB   00:06
Rocky Linux 9 - Extras                         1.8 kB/s | 2.9 kB   00:01
Package bind-utils-32:9.16.23-18.el9_4.6.x86_64 is already installed.
Dependencies resolved.
=====
 Package           Arch      Version       Repository      Size
 =====
 Installing:
  bind             x86_64    32:9.16.23-18.el9_4.6    appstream     490 k
```

Рис. 2.1: Переход в режим суперпользователя и установка bind, bind-utils

С помощью утилиты dig сделаем запрос к DNS-адресу www.yandex.ru:
dig www.yandex.ru (рис. 2.2).



```
root@server:~# dig www.yandex.ru

; <>> DiG 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17650
;; 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      5.255.255.77
www.yandex.ru.        3600    IN      A      77.88.44.55
www.yandex.ru.        3600    IN      A      77.88.55.88

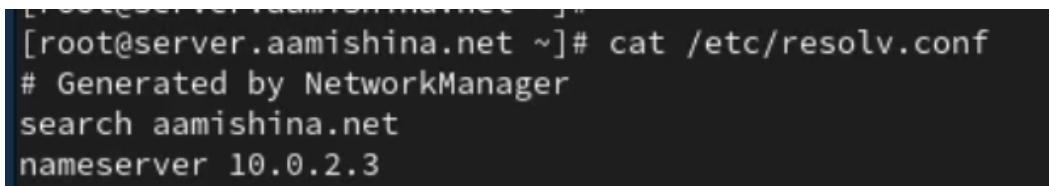
;; Query time: 39 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Mon Sep 09 16:47:24 UTC 2024
;; MSG SIZE rcvd: 79

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

Рис. 2.2: Запрос с помощью утилиты dig

2.2 Конфигурирование кэширующего DNS-сервера

Просмотрим содержание файлов /etc/resolv.conf (рис. 2.3), /etc/named.conf (рис. 2.4), /var/named/named.ca (рис. 2.5), /var/named/named.localhost (рис. 2.6), /var/named/named.loopback (рис. 2.7).



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

Рис. 2.3: Просмотр содержания файла /etc/resolv.conf

```
[root@server.aamishina.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: Просмотр содержания файла /etc/named.conf

```
[root@server.aamishina.net ~]# cat /var/named/named.ca
; <>>> DiG 9.18.20 <>> -4 +tcp +norec +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: Просмотр содержания файла /var/named/named.ca

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

Рис. 2.6: Просмотр содержания файла /var/named/named.localhost

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

Рис. 2.7: Просмотр содержания файла /var/named/named.loopback

Запустим DNS-сервер: `systemctl start named`. Включим запуск DNS-сервера в автозапуск при загрузке системы: `systemctl enable named`. Проанализируем отличие в выведенной на экран информации при выполнении команд: `dig www.yandex.ru` и `dig 127.0.0.1 www.yandex.ru` (рис. 2.8).

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

; <>> DiG 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1211
;; 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      77.88.44.55
www.yandex.ru.        3600    IN      A      77.88.55.88
www.yandex.ru.        3600    IN      A      5.255.255.77

;; Query time: 20 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Mon Sep 09 16:51:10 UTC 2024
;; MSG SIZE rcvd: 79

[root@server.aamishina.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: 45088
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 39e4212e5dc8472e0100000066df2792a87e0844485e7499 (good)
;; QUESTION SECTION:
;www.yandex.ru.          IN      A

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

;; Query time: 845 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep 09 16:51:30 UTC 2024
;; MSG SIZE rcvd: 118

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

Рис. 2.8: Запуск DNS-сервера, включение запуска DNS-сервера в автозапуск при загрузке системы, анализ выведенной на экран информации при выполнении команды `dig www.yandex.ru` и `dig 127.0.0.1 www.yandex.ru`

Сделаем DNS-сервер сервером по умолчанию для хоста `server` и внутренней виртуальной сети. Для этого 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 `127.0.0.1`. Сделаем тоже самое для соединения `System eth0` (рис. 2.9).

```
[root@server.aamishina.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' (e777ed2f-6d6c-4f97-9eac-03b7e6fc3f51) successfully updated.
nmcli> quit
[root@server.aamishina.net ~]# nmcli connection edit System\ eth0
==| nmcli interactive connection editor |==

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

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

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4,
ipv6, hostname, 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 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
[root@server.aamishina.net ~]#
```

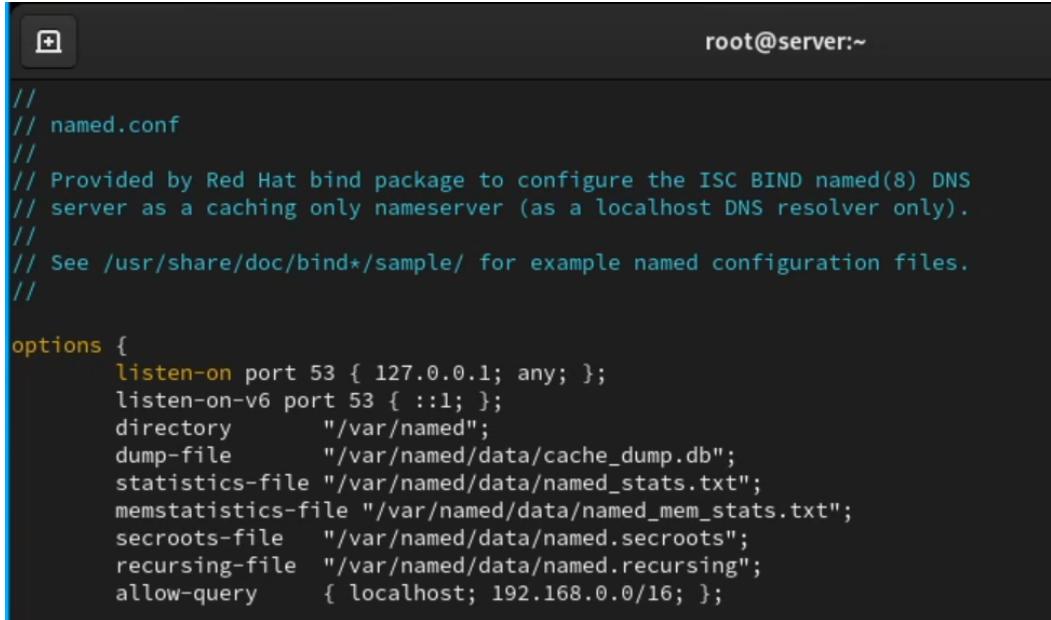
Рис. 2.9: Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети. Повторяем действия для соединения System eth0

Перезапустим NetworkManager: systemctl restart NetworkManager. Проверим наличие изменений в файле /etc/resolv.conf (рис. 2.10).

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

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

Теперь нам требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесём изменения в файл /etc/named.conf, заменив строку listen-on port 53 { 127.0.0.1; }; на listen-on port 53 { 127.0.0.1; any; }; и строку allow-query { localhost; }; на allow-query { localhost; 192.168.0.0/16; }; (рис. 2.11).



```
//  
// 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; };
```

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

Внесём изменения в настройки межсетевого экрана узла server, разрешив работу с DNS: firewall-cmd –add-service=dns и firewall-cmd –add service=dns –permanent. Убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используем команду lsof: lsof | grep UDP (рис. 2.12).

```

[root@server.aamishina.net ~]# vim /etc/named.conf
[root@server.aamishina.net ~]# firewall-cmd --add-service=dns
success
[root@server.aamishina.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.aamishina.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
avahi-dae  569          avahi   12u    IPv4          19729    0t0      UDP *:mdns
avahi-dae  569          avahi   13u    IPv6          19730    0t0      UDP *:mdns
avahi-dae  569          avahi   14u    IPv4          19731    0t0      UDP *:44520
avahi-dae  569          avahi   15u    IPv6          19732    0t0      UDP *:32951
chronyd   607          chrony  5u     IPv4          19801    0t0      UDP localhost:323
chronyd   607          chrony  6u     IPv6          19802    0t0      UDP localhost:323
named     9938          named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938          named   24u    IPv6          47384    0t0      UDP localhost:domai
n
named     9938  9939 isc-net-0  named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938  9939 isc-net-0  named   24u    IPv6          47384    0t0      UDP localhost:domai
n
named     9938  9940 isc-net-0  named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938  9940 isc-net-0  named   24u    IPv6          47384    0t0      UDP localhost:domai
n
named     9938  9941 isc-timer  named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938  9941 isc-timer  named   24u    IPv6          47384    0t0      UDP localhost:domai
n
named     9938  9942 isc-socke  named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938  9942 isc-socke  named   24u    IPv6          47384    0t0      UDP localhost:domai
n
named     9938  9970 isc-net-0  named   21u    IPv4          47382    0t0      UDP localhost:domai
n
named     9938  9970 isc-net-0  named   24u    IPv6          47384    0t0      UDP localhost:domai
NetworkMa 10006          root    27u    IPv4          50282    0t0      UDP server.aamishin
a.net:bootpc->_gateway:bootps
NetworkMa 10006 10014 gmain
a.net:bootpc->_gateway:bootps
NetworkMa 10006 10015 gibus
a.net:bootpc->_gateway:bootps
[root@server.aamishina.net ~]#

```

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

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 добавим: forwarders { список DNS-серверов }; и forward first; Кроме того, возможно вышестоящий DNS-сервер может не поддерживать технологию DNSSEC, тогда в конфигурационном файле named.conf укажем следующие настройки: dnssec-enable no; и dnssec-validation no; (рис. 2.13).

```

// 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.recurising";
    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;
/*dnssec-validation yes;*/

    managed-keys-directory "/var/named/dynamic";
    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 {
-- INSERT --

```

Рис. 2.13: Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек

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 aamishina.net: cp /etc/named.rfc1912.zones /etc/named/; cd /etc/named и mv /etc/named/named.rfc1912.zones /etc/named/aamishina.net (рис. 2.14).

```

[root@server.aamishina.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.aamishina.net ~]# cd /etc/named
[root@server.aamishina.net named]# mv /etc/named/named.rfc1912.zones /etc/named/aamishina.net
[root@server.aamishina.net named]# vim /etc/named.conf

```

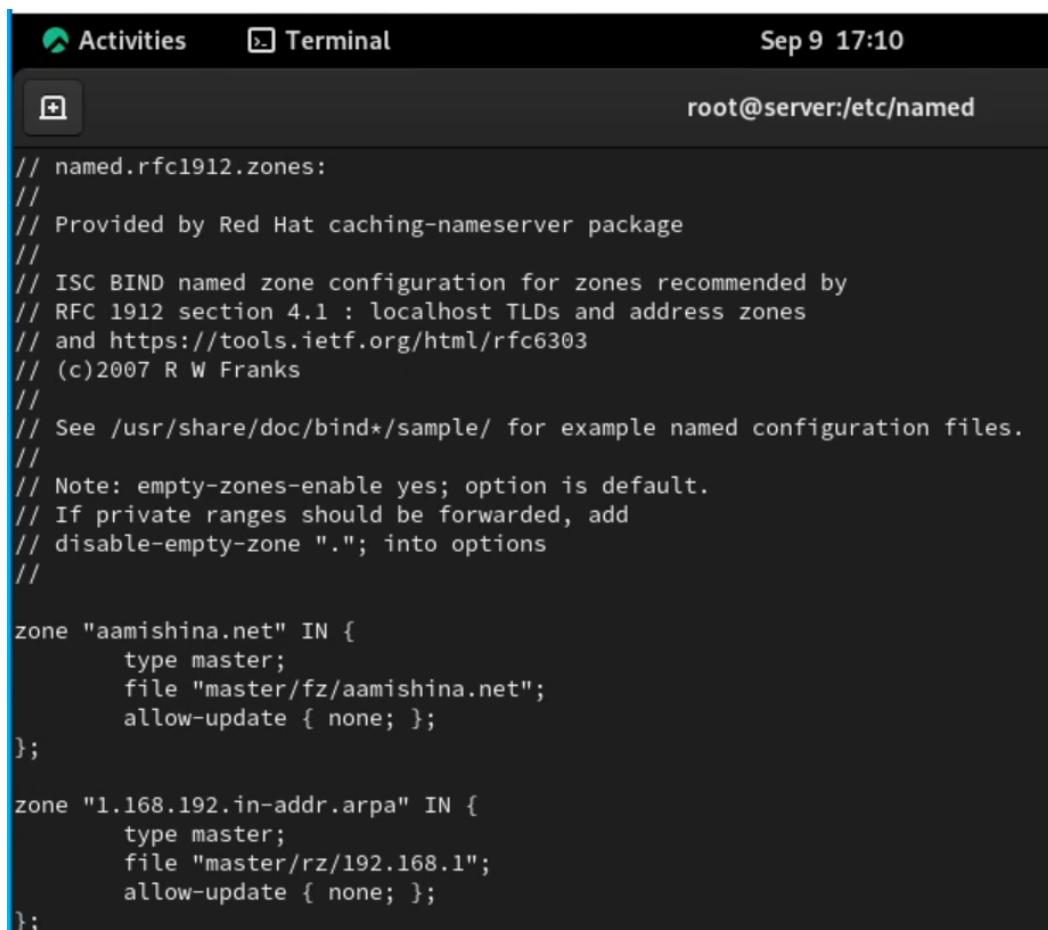
Рис. 2.14: Копирование шаблона описания DNS-зон из каталога /etc в каталог /etc/named и изменение его названия

Включим файл описания зоны /etc/named/aamishina.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку: include “/etc/named/aamishina.net” (рис. 2.15).

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/aamishina.net";
-- INSERT --
```

Рис. 2.15: Включение файла описания зоны /etc/named/aamishina.net в конфигурационном файле DNS /etc/named.conf

Откроем файл /etc/named/user.net на редактирование и вместо зоны пропишем свою прямую зону. Далее, вместо зоны пропишем свою обратную зону. Остальные записи в файле /etc/named/aamishina.net удалим (рис. 2.16).



```
// 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 "aamishina.net" IN {
    type master;
    file "master/fz/aamishina.net";
    allow-update { none; };
};

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

Рис. 2.16: Открытие файла /etc/named/user.net на редактирование. Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле

В каталоге /var/named создадим подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно: cd /var/named; mkdir -p /var/named/master/fz; mkdir -p /var/named/master/rz. Скопируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуем его в aamishina.net: cp /var/named/named.localhost /var/named/master/fz/; cd /var/named/master/fz/; mv named.localhost aamishina.net (рис. 2.17).

```
[root@server.aamishina.net named]# cd /var/named
[root@server.aamishina.net named]# mkdir -p /var/named/master/fz
[root@server.aamishina.net named]# mkdir -p /var/named/master/rz
[root@server.aamishina.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.aamishina.net named]# cd /var/named/master/fz/
[root@server.aamishina.net fz]# mv named.localhost aamishina.net
[root@server.aamishina.net fz]# ls
aamishina.net
[root@server.aamishina.net fz]# vim /var/named/master/fz/aamishina.net
```

Рис. 2.17: В каталоге /var/named создание подкаталогов master/fz и master/rz. Копирование шаблона прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и изменение его названия

Изменим файл /var/named/master/fz/aamishina.net, указав необходимые DNS записи для прямой зоны. В этом файле DNS-имя сервера @ rname.invalid. заменим на @ server.aamishina.net. Формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии) [1]; адрес в А-записи заменим с 127.0.0.1 на 192.168.1.1; в директиве ORIGIN зададим текущее имя домена aamishina.net, а затем укажем имена и адреса серверов в этом домене в виде А-записей DNS (на данном этапе пропишем сервер с именем ns и адресом 192.168.1.1) (рис. 2.18).

```
$TTL 1D
@ IN SOA @ server.aamishina.net. (
                                2024072700 ; serial
                                1D          ; refresh
                                1H          ; retry
                                1W          ; expire
                                3H          ; minimum
)
NS      @
A      192.168.1.1
$ORIGIN aamishina.net.
server A      192.168.1.1
ns     A      192.168.1.1
~
```

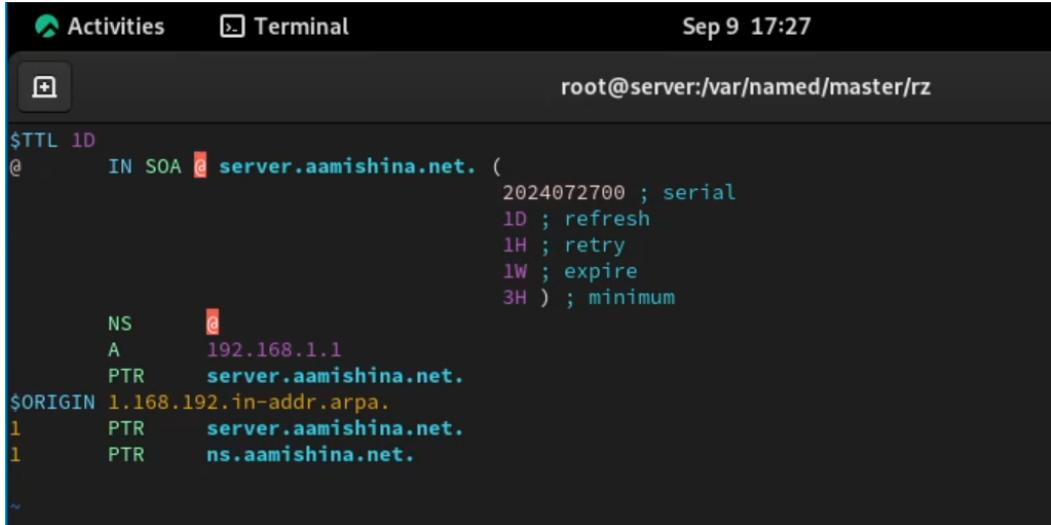
Рис. 2.18: Изменение файла /var/named/master/fz/aamishina.net, указав необходимые DNS записи для прямой зоны

Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1: cp /var/named/named.loopback /var/named/master/rz/; cd /var/named/master/rz/ и mv named.loopback 192.168.1 (рис. 2.19).

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

Рис. 2.19: Копирование шаблона обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и изменение его названия

Изменим файл /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны. В этом файле DNS-имя сервера @ rname.invalid заменим на @ server.aamishina.net. формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-записи заменим с 127.0.0.1 на 192.168.1.1; в директиве \$ORIGIN зададим название обратной зоны в виде 1.168.192.in-addr.arpa., затем зададим PTR-записи (на данном этапе зададим PTR запись, ставящая в соответствие адресу 192.168.1.1 DNS-адрес ns.aamishina.net) (рис. 2.20).



```
$TTL 1D
@ IN SOA <server.aamishina.net. (      2024072700 ; serial
                                         1D ; refresh
                                         1H ; retry
                                         1W ; expire
                                         3H ) ; minimum
          NS      <
          A      192.168.1.1
          PTR    server.aamishina.net.
$ORIGIN 1.168.192.in-addr.arpa.
1     PTR    server.aamishina.net.
1     PTR    ns.aamishina.net.

~
```

Рис. 2.20: Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны

Далее исправим права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать: chown -R named:named /etc/named и chown -R named:named /var/named. В системах с запущенным SELinux все процессы и файлы имеют специальные метки безопасности (так называемый «контекст безопасности»), используемые системой для принятия решений по доступу к этим процессам и файлам. После изменения доступа к конфигурационным файлам named требуется корректно восстановить их метки в SELinux: restorecon -vR /etc и restorecon -vR /var/named. Для проверки состояния переключателей SELinux, относящихся к named, введём: getsebool -a | grep named. Теперь дадим named разрешение на запись в файлы DNS-зоны: setsebool named_write_master_zones 1 и setsebool -P named_write_master_zones 1 (рис. 2.21).

```
[root@server.aamishina.net rz]# chown -R named:named /etc/named
[root@server.aamishina.net rz]# chown -R named:named /var/named
[root@server.aamishina.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.aamishina.net rz]# restorecon -vr /var/named
[root@server.aamishina.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.aamishina.net rz]# setsebool named_write_master_zones 1
[root@server.aamishina.net rz]# setsebool -P named_write_master_zones 1
[root@server.aamishina.net rz]#
```

Рис. 2.21: Исправление прав доступа к файлам в каталогах /etc/named и /var/named, корректное восстановление их меток в SELinux, проверка состояния переключателей SELinux

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы: journalctl -x -f (рис. 2.22), (рис. 2.23) и в первом терминале перезапустим DNS-сервер: systemctl restart named (рис. 2.24).

```
aamishina@server:~ — journalctl -x -f
root@server:~/var/named/master/rz          aamishina@server:~ — journalctl -x -f
[aamishina@server.aamishina.net ~]$ journalctl -x -f
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability open_perms=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability extended_socket_class=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability always_check_network=0
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability cgroup_seclabel=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability nnp_nosuid_transition=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability genfs_seclabel_symlinks=1
Sep 09 17:29:32 server.aamishina.net setsebool[10369]: The named_write_master_zones policy boolean was changed to 1 by root
Sep 09 17:29:46 server.aamishina.net dbus-broker-launch[8398]: avc: op=load_policy lsm=selinux seqno=6 res=
Sep 09 17:29:46 server.aamishina.net systemd[8369]: selinux: avc: op=load_policy lsm=selinux seqno=6 res=1
Sep 09 17:29:46 server.aamishina.net systemd[8369]: Started VTE child process 10376 launched by gnome-terminal-server
process 9372.
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

A start job for unit UNIT has finished successfully.

The job identifier is 528.
```

Рис. 2.22: Запуск расширенного лога системных сообщений

Рис. 2.23: Проверка корректности работы системы

```
[root@server.aamishina.net rz]# systemctl restart named  
[root@server.aamishina.net rz]#
```

Рис. 2.24: Перезапуск DNS-сервера

2.4 Анализ работы DNS-сервера

При помощи утилиты dig получим описание DNS-зоны с сервера ns.aamishina.net: dig ns.user.net (рис. 2.25).

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

; <>> DiG 9.16.23-RH <>> ns.aamishina.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14222
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0fe6f20b93ee4fad0100000066df30db6b33879431200bea (good)
;; QUESTION SECTION:
;ns.aamishina.net.           IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep 09 17:31:07 UTC 2024
;; MSG SIZE  rcvd: 89

[root@server.aamishina.net rz]#
```

Рис. 2.25: Получение описания DNS-зоны с сервера ns.aamishina.net.

При помощи утилиты host проанализируем корректность работы DNS-сервера: host -l aamishina.net; host -a aamishina.net; host -t A aamishina.net; host -t PTR 192.168.1.1 (рис. 2.26).

```
[root@server.aamishina.net rz]# host -l aamishina.net
aamishina.net name server aamishina.net.
aamishina.net has address 192.168.1.1
ns.aamishina.net has address 192.168.1.1
server.aamishina.net has address 192.168.1.1
[root@server.aamishina.net rz]# host -a aamishina.net
Trying "aamishina.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57685
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
aamishina.net.    86400   IN      SOA     aamishina.net. server.aamishina.net. 2024072700 86400 3600 604800 108
00
aamishina.net.    86400   IN      NS      aamishina.net.
aamishina.net.    86400   IN      A       192.168.1.1

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

Received 120 bytes from 127.0.0.1#53 in 0 ms
[root@server.aamishina.net rz]# host -t A aamishina.net
aamishina.net has address 192.168.1.1
[root@server.aamishina.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.aamishina.net.
1.1.168.192.in-addr.arpa domain name pointer ns.aamishina.net.
[root@server.aamishina.net rz]#
```

Рис. 2.26: Анализ корректности работы DNS-сервера

2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS: cd /vagrant; mkdir -p /vagrant/provision/server/dns/etc/named; mkdir -p /vagrant/provision/server/dns/var/named/master; cp -R /etc/named.conf /vagrant/provision/server/dns/etc/; cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/; cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/. В каталоге /vagrant/provision/server создадим исполняемый файл dns.sh: touch dns.sh и chmod +x dns.sh (рис. 2.27).

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

Рис. 2.27: Переход в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога dns, в который помещаем конфигурационные файлы DNS. Создание в каталоге /vagrant/provision/server исполняемого файла dns.sh

Откроем его на редактирование и пропишем в нём следующий скрипт (приведён в лабораторной работе). Этот скрипт, по сути, повторяет произведённые нами действия по установке и настройке DNS-сервера (рис. 2.28):

1. подставляет в нужные каталоги подготовленные вами конфигурационные файлы;

2. меняет соответствующим образом права доступа, метки безопасности SELinux и правила межсетевого экрана;
3. настраивает сетевое соединение так, чтобы сервер выступал DNS-сервером по умолчанию для узлов внутренней виртуальной сети;
4. запускает DNS-сервер;

The screenshot shows a terminal window titled "root@server:/vagrant/provision/server". The terminal content is a shell script (#!/bin/bash) used for provisioning a Vagrant server. The script performs several tasks:

- Installs needed packages (bind and bind-utils) using dnf -y install.
- Copies configuration files from /vagrant/provision/server/dns/* to /etc and /var/named.
- Changes ownership of the copied files to named:named.
- Runs restorecon on /etc and /var/named to maintain file permissions.
- Configures the firewall to add dns service.
- Tunes SELinux by setting named_write_master_zones boolean to 1.
- Changes the DNS server address for the eth0 interface using nmcli.
- Starts the named service using systemctl.

```
#!/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

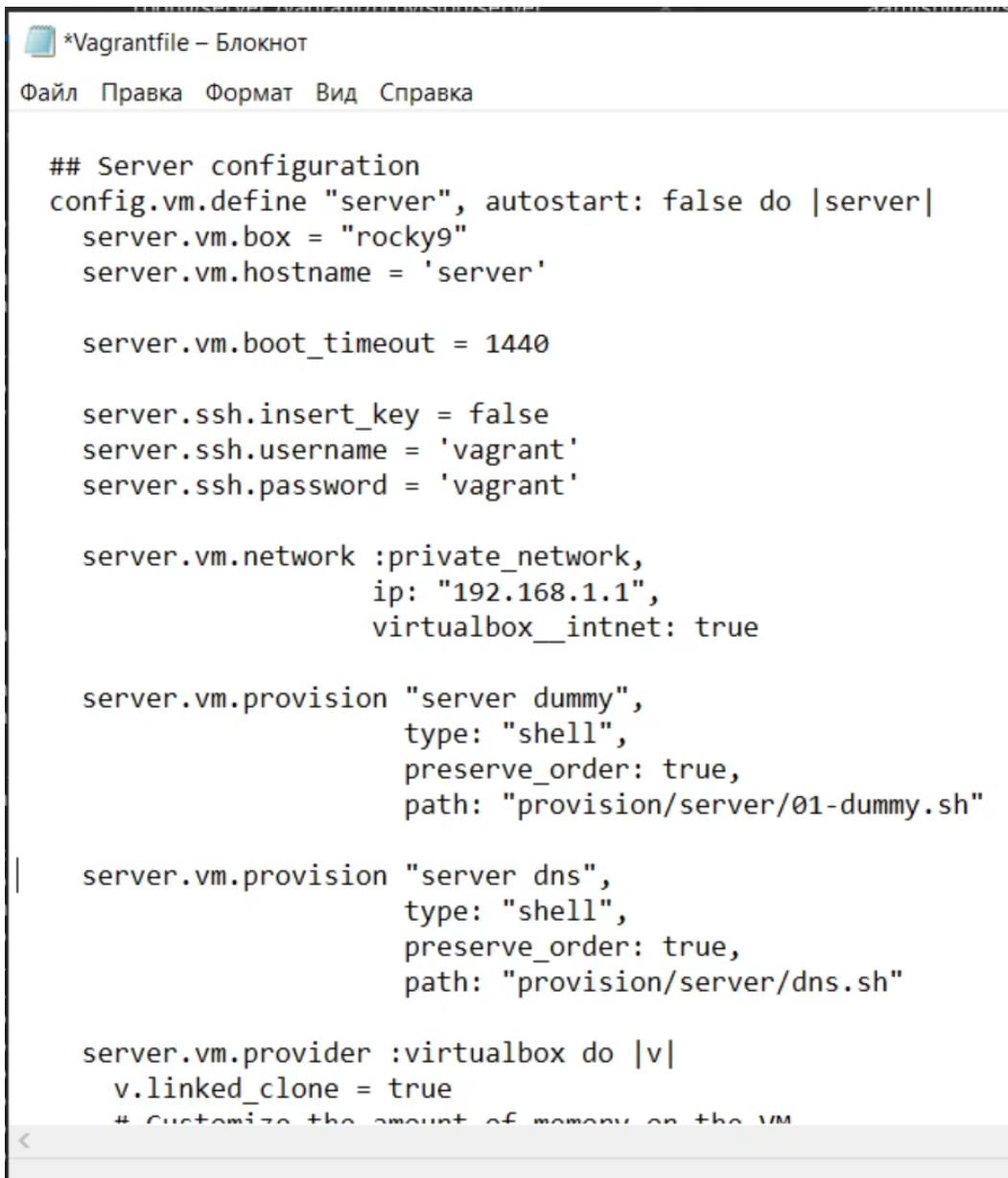
echo "Change dns server address"
nmcli connection edit "System eth0" <<EOF
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
EOF
systemctl restart NetworkManager

echo "Start named service"
systemctl enable named
systemctl start named
~
```

Рис. 2.28: Открытие файла на редактирование и прописывание в нём скрипта

Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` добавим определён-

ные параметры в разделе конфигурации для сервера (рис. 2.29).



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

## Server configuration
config.vm.define "server", autostart: false do |server|
  server.vm.box = "rocky9"
  server.vm.hostname = 'server'

  server.vm.boot_timeout = 1440

  server.ssh.insert_key = false
  server.ssh.username = 'vagrant'
  server.ssh.password = 'vagrant'

  server.vm.network :private_network,
    ip: "192.168.1.1",
    virtualbox_intnet: true

  server.vm.provision "server dummy",
    type: "shell",
    preserve_order: true,
    path: "provision/server/01-dummy.sh"

  server.vm.provision "server dns",
    type: "shell",
    preserve_order: true,
    path: "provision/server/dns.sh"

  server.vm.provider :virtualbox do |v|
    v.linked_clone = true
    # Customize the amount of memory on the VM
  end
end
```

Рис. 2.29: Добавление параметров в конфигурационном файле Vagrantfile в разделе конфигурации для сервера

Контрольные вопросы:

1. Что такое DNS? - Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса, используемые компьютерами для идентификации друг друга в сети.
2. Каково назначение кэширующего DNS-сервера? - Его задача - хра-

нить 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? - Используйте опции, такие как -d или -v при запуске службы.
16. Где храниться 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? - Используйте `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>`.

3 Выводы

В ходе выполнения данной лабораторной работы я приобрела практические навыки по установке и конфигурированию DNS-сервера, усвоила принципы работы системы доменных имён.