

Лабораторная работа №2

Настройка DNS-сервера

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	20

Список иллюстраций

3.1	Команда <code>make server-up</code>	6
3.2	Установка <code>bind</code> и <code>bind-utils</code> в режиме суперпользователя	6
3.3	Команда <code>dig</code>	7
3.4	Файлы <code>loopback</code> и <code>localhost</code>	8
3.5	Команда <code>dig</code>	9
3.6	Изменение адреса <code>dns</code> -сервера	10
3.7	Изменение адреса <code>dns</code> -сервера	10
3.8	Изменение скрипта	10
3.9	Внесение изменений	11
3.10	Изменение скрипта	12
3.11	Окно терминала	12
3.12	Изменение скрипта	13
3.13	Изменение скрипта	13
3.14	Изменение скрипта	14
3.15	Изменение скрипта	14
3.16	Изменение скрипта	15
3.17	Восстановление меток безопасности и проверка состояния переключателей в SELinux	15
3.18	Запуск расширенного лога системных сообщений	16
3.19	Перезапуск сервера	16
3.20	Утилита <code>dig</code>	17
3.21	Утилита <code>host</code>	17
3.22	Создание каталога <code>dns</code> и перенос в него файлов, создание <code>dns.sh</code>	18
3.23	Изменение скрипта	18
3.24	Изменение <code>Vagrantfile</code>	19

1 Цель работы

Приобрести практические навыки по установке и конфигурированию DNS-сервера, усвоить принципы 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

3 Выполнение лабораторной работы

Загрузим операционную систему и перейдем в рабочий каталог с проектом:
`cd C:\Users\dasha\work\study\dmbelicheva\vagrant\` Затем запустим виртуальную машину `server` с помощью команды: `make server-up` На виртуальной машине `server` войдем под созданным в предыдущей работе пользователем и откроем терминал. Перейдем в режим суперпользователя и установим `bind` и `bind-utils`:

```
dasha@DESKTOP-0358D70 MSYS /c/users/dasha/work/study/dmbelicheva/vagrant
$ make server-up
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".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 work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".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 work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
server: Adapter 1: nat
server: Adapter 2: intnet
==> server: Forwarding ports...
server: 22 (guest) => 2222 (host) (adapter 1)
==> server: Running 'pre-boot' VM customizations
```

Рис. 3.1: Команда `make server-up`

```
root@server:~
[dmbelicheva@server.dmbelicheva.net ~]$ sudo -i
[sudo] password for dmbelicheva:
[root@server.dmbelicheva.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 9 - x86_64 12 kB/s | 11 kB 00:00
Extra Packages for Enterprise Linux 9 - x86_64 4.0 MB/s | 20 MB 00:04
```

Рис. 3.2: Установка `bind` и `bind-utils` в режиме суперпользователя

С помощью утилиты `dig` сделаем запрос к DNS-адресу `www.yandex.ru`:

```
[root@server.dmbelicheva.net ~]# dig www.yandex.ru

; <<> DiG 9.16.23-RH <<> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5977
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                3600    IN      A      77.88.55.88
www.yandex.ru.                3600    IN      A      77.88.55.60
www.yandex.ru.                3600    IN      A      5.255.255.70
www.yandex.ru.                3600    IN      A      5.255.255.77

;; Query time: 10 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 11 14:16:24 UTC 2023
;; MSG SIZE rcvd: 95
```

Рис. 3.3: Команда dig

Давайте рассмотрим разделы данного вывода подробнее:

- **HEADER (заголовок):** показывает версию dig, глобальные опции используемые с командой и другую дополнительную информацию
- **QUESTION SECTION (секция запроса):** Показывает наш запрос, то есть мы запросили показать A-запись (команда dig без параметров) для домена www.yandex.ru
- **ANSWER SECTION (секция ответа):** Показывает ответ полученный от DNS, в нашем случае показывает A-запись для www.yandex.ru Последняя секция это статистика по запросу (служебная информация)- время выполнения запроса (10 мс), имя DNS-сервера который запрашивался, когда был создан запрос и размер сообщения

Конфигурирование кэширующего DNS-сервера

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 dmbelicheva.net
```

nameserver 10.0.2.3

Рассмотрим содержимое файла `/var/named/named.localhost`. В нём есть:

- 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.

В файле `/var/named/named.loopback` все аналогично, только добавляется:

- PTR-запись для локального хоста

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

Рис. 3.4: Файлы `loopback` и `localhost`

Далее 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`:


```
[root@server.dmbelicheva.net ~]# dig www.yandex.ru

;<<> DiG 9.16.23-RH <<> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5422
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                3600    IN      A      77.88.55.88
www.yandex.ru.                3600    IN      A      5.255.255.70
www.yandex.ru.                3600    IN      A      77.88.55.60
www.yandex.ru.                3600    IN      A      5.255.255.77

;; Query time: 7 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 11 15:37:04 UTC 2023
;; MSG SIZE rcvd: 95

[root@server.dmbelicheva.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: 54474
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;EDNS: version: 0, flags:; udp: 1232
;COOKIE: 74db22a239f573ee01000000654f9fbb2cd8ed508af81ef8 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                300     IN      A      5.255.255.70
www.yandex.ru.                300     IN      A      5.255.255.77
www.yandex.ru.                300     IN      A      77.88.55.88
www.yandex.ru.                300     IN      A      77.88.55.60

;; Query time: 653 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 11 15:37:31 UTC 2023
;; MSG SIZE rcvd: 134
```

Рис. 3.5: Команда dig

При указании опрашиваемого адреса в строке с адресом сервера написан адрес, который указывали, также указаны куки, а время запроса увеличилось.

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):

```

[root@server.dmbelicheva.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 [<settings>.<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, 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' (d18d46cb-18cd-4f51-bb7b-4c35caa7c786) successfully updated.
nmcli> quit
[root@server.dmbelicheva.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 [<settings>.<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, 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.dmbelicheva.net ~]#

```

Рис. 3.6: Изменение адреса dns-сервера

```

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

```

Рис. 3.7: Изменение адреса dns-сервера

Настроим 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:

```

GNU nano 5.6.1 /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; 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

```

Рис. 3.8: Изменение скрипта

Внесем изменения в настройки межсетевого экрана узла server, разрешив ра-

боту с DNS и убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53:

```
[root@server.dmbelicheva.net ~]# firewall-cmd --add-service=dns
success
[root@server.dmbelicheva.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.dmbelicheva.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
avahi-daemon 562      avahi    12u    IPv4      18760    0t0      UDP *:mdns
avahi-daemon 562      avahi    13u    IPv6      18761    0t0      UDP *:mdns
avahi-daemon 562      avahi    14u    IPv4      18762    0t0      UDP *:46522
avahi-daemon 562      avahi    15u    IPv6      18763    0t0      UDP *:45440
chronyd      586      chrony   5u     IPv4      18658    0t0      UDP localhost:323
chronyd      586      chrony   6u     IPv6      18659    0t0      UDP localhost:323
named        8308     named    16u    IPv4      56604    0t0      UDP localhost:domain
named        8308     named    19u    IPv6      56606    0t0      UDP localhost:domain
named        8308 8309 isc-net-0 named    16u    IPv4      56604    0t0      UDP localhost:domain
named        8308 8309 isc-net-0 named    19u    IPv6      56606    0t0      UDP localhost:domain
named        8308 8310 isc-timer named    16u    IPv4      56604    0t0      UDP localhost:domain
named        8308 8310 isc-timer named    19u    IPv6      56606    0t0      UDP localhost:domain
named        8308 8311 isc-socket named    16u    IPv4      56604    0t0      UDP localhost:domain
named        8308 8311 isc-socket named    19u    IPv6      56606    0t0      UDP localhost:domain
named        8308 8349 isc-net-0 named    16u    IPv4      56604    0t0      UDP localhost:domain
named        8308 8349 isc-net-0 named    19u    IPv6      56606    0t0      UDP localhost:domain
NetworkManager 8831     root     27u    IPv4      66911    0t0      UDP server.dmbelicheva.net:53
net:bootpc->_gateway:bootps root     27u    IPv4      66911    0t0      UDP server.dmbelicheva.net:53
net:bootpc->_gateway:bootps root     27u    IPv4      66911    0t0      UDP server.dmbelicheva.net:53
net:bootpc->_gateway:bootps root     27u    IPv4      66911    0t0      UDP server.dmbelicheva.net:53
```

Рис. 3.9: Внесение изменений

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:

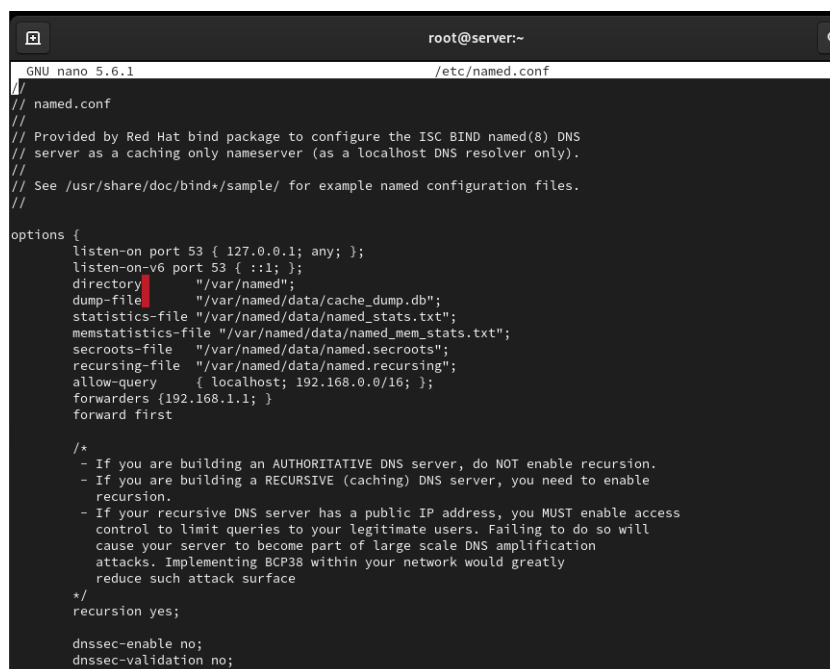
```
forwarders { список DNS-серверов };
forward first;
```

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`:

```
forwarders { 198.168.1.1; };
forward first;
```



```
GNU nano 5.6.1 /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; 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.secrets";
    recursing-file "/var/named/data/named.recursing";
    allow-query { localhost; 192.168.0.0/16; };
    forwarders {192.168.1.1; }
    forward first

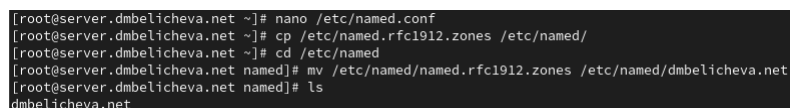
    /*
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
    - If you are building a RECURSIVE (caching) DNS server, you need to enable
    recursion.
    - If your recursive DNS server has a public IP address, you MUST enable access
    control to limit queries to your legitimate 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. 3.10: Изменение скрипта

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`:



```
[root@server.dmbelicheva.net ~]# nano /etc/named.conf
[root@server.dmbelicheva.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.dmbelicheva.net ~]# cd /etc/named
[root@server.dmbelicheva.net named]# mv /etc/named/named.rfc1912.zones /etc/named/dmbelicheva.net
[root@server.dmbelicheva.net named]# ls
dmbelicheva.net
```

Рис. 3.11: Окно терминала

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

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

```
root@server:/etc/named
GNU nano 5.6.1 /etc/named.conf
recursing-file "/var/named/data/named.recursing";
allow-query { localhost; 192.168.0.0/16; };
forwarders {192.168.1.1; }
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;

dnsssec-enable no;
dnsssec-validation no;

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 {
        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/dmbelicheva.net";
```

Рис. 3.12: Изменение скрипта

Внесём изменения в файл dmbelicheva.net:

```
root@server:/etc/named
GNU nano 5.6.1 dmbelicheva.net
// 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 "dmbelicheva.net" IN {
    type master;
    file "master/fz/dmbelicheva.net";
    allow-update { none; };
};

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

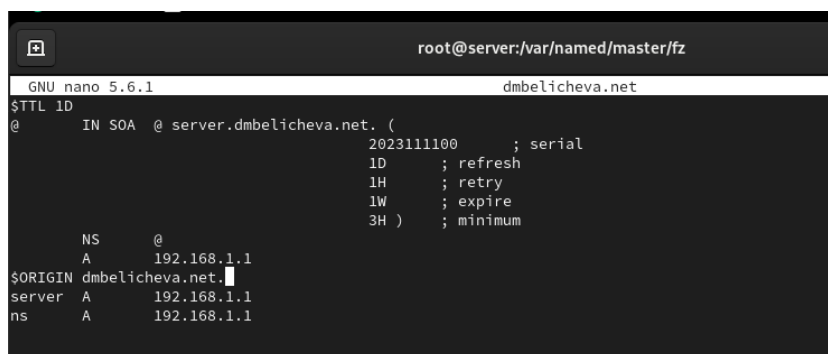
Рис. 3.13: Изменение скрипта

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:

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

Рис. 3.14: Изменение скрипта

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

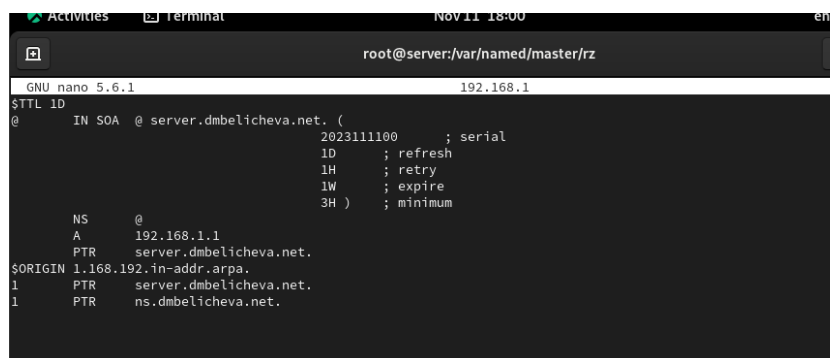


```
GNU nano 5.6.1 dmbelicheva.net
$TTL 1D
@      IN SOA  @ server.dmbelicheva.net. (
                                2023111100      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )   ; minimum

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

Рис. 3.15: Изменение скрипта

Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1, а также изменим файл:

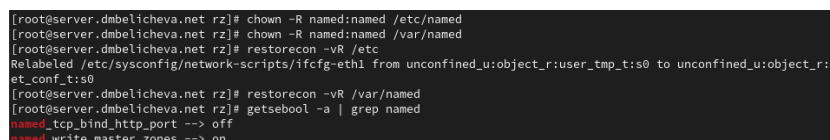


```
GNU nano 5.6.1 192.168.1
$TTL 1D
@      IN SOA  @ server.dmbelicheva.net. (
                                2023111100 ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

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

Рис. 3.16: Изменение скрипта

После изменения доступа к конфигурационным файлам named корректно восстановим специальные метки безопасности в SELinux, затем проверим состояние переключателей:



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

Рис. 3.17: Восстановление меток безопасности и проверка состояния переключателей в SELinux

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:

```
dmbelicheva@server:~$ journalctl -x -f
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaWindowGroup is on
se it needs an allocation.
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaWindowActorX11 is
cause it needs an allocation.
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaSurfaceActorX11 i
ecause it needs an allocation.
^C
dmbelicheva@server.dmbelicheva.net ~]$ journalctl -x -f
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: network unreachable resolving './DNSKEY/IN': 2001:500:1:1:
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: managed-keys-zone: Key 20326 for zone . is now trusted (a
nce timer complete)
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: timed out resolving './DNSKEY/IN': 192.168.1.1#53
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3
0#53
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: network unreachable resolving './DNSKEY/IN': 2001:503:c27
#53
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: network unreachable resolving './DNSKEY/IN': 2001:500:2f:
Nov 11 18:37:26 server.dmbelicheva.net named[10912]: network unreachable resolving './DNSKEY/IN': 2001:500:12:
3
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaWindowGroup is on
se it needs an allocation.
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaWindowActorX11 is
cause it needs an allocation.
Nov 11 18:37:30 server.dmbelicheva.net gnome-shell[5218]: Can't update stage views actor MetaSurfaceActorX11 i
ecause it needs an allocation.
Nov 11 18:40:12 server.dmbelicheva.net systemd[1]: Starting dnf makecache...
Subject: A start job for unit dnf-makecache.service has begun execution
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit dnf-makecache.service has begun execution.

The job identifier is 4740.
Nov 11 18:40:14 server.dmbelicheva.net dnf[10949]: Metadata timer caching disabled when running on a battery.
Nov 11 18:40:14 server.dmbelicheva.net systemd[1]: dnf-makecache.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://access.redhat.com/support

The unit dnf-makecache.service has successfully entered the 'dead' state.
Nov 11 18:40:14 server.dmbelicheva.net systemd[1]: Finished dnf makecache.
Subject: A start job for unit dnf-makecache.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit dnf-makecache.service has finished successfully.

The job identifier is 4740.
```

Рис. 3.18: Запуск расширенного лога системных сообщений

В случае ошибок перезапустим DNS-сервер:

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

Рис. 3.19: Перезапуск сервера

Анализ работы DNS-сервера

При помощи утилиты dig получим описание DNS-зоны с сервера ns.dmbelicheva.net:


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

; <<> DiG 9.16.23-RH <<> ns.dmbelicheva.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7956
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 28d93565e735d0fc01000000654fcb0040c5e70b1bf52b62 (good)
;; QUESTION SECTION:
;ns.dmbelicheva.net.                IN      A

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

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 11 18:42:08 UTC 2023
;; MSG SIZE rcvd: 91
```

Рис. 3.20: Утилита dig

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

```
[root@server.dmbelicheva.net rz]# host -l dmbelicheva.net
dmbelicheva.net name server dmbelicheva.net.
dmbelicheva.net has address 192.168.1.1
ns.dmbelicheva.net has address 192.168.1.1
server.dmbelicheva.net has address 192.168.1.1
[root@server.dmbelicheva.net rz]# host -a dmbelicheva.net
Trying "dmbelicheva.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28251
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
dmbelicheva.net.                86400   IN      SOA     dmbelicheva.net. server.dmbelicheva.net. 2023111100 86400 3600 60480
0 10800
dmbelicheva.net.                86400   IN      NS      dmbelicheva.net.
dmbelicheva.net.                86400   IN      A       192.168.1.1

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

Received 122 bytes from 127.0.0.1#53 in 8 ms
[root@server.dmbelicheva.net rz]# host -t A dmbelicheva.net
dmbelicheva.net has address 192.168.1.1
[root@server.dmbelicheva.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.dmbelicheva.net.
1.1.168.192.in-addr.arpa domain name pointer ns.dmbelicheva.net.
[root@server.dmbelicheva.net rz]#
```

Рис. 3.21: Утилита host

Внесение изменений в настройки внутреннего окружения виртуальной машины

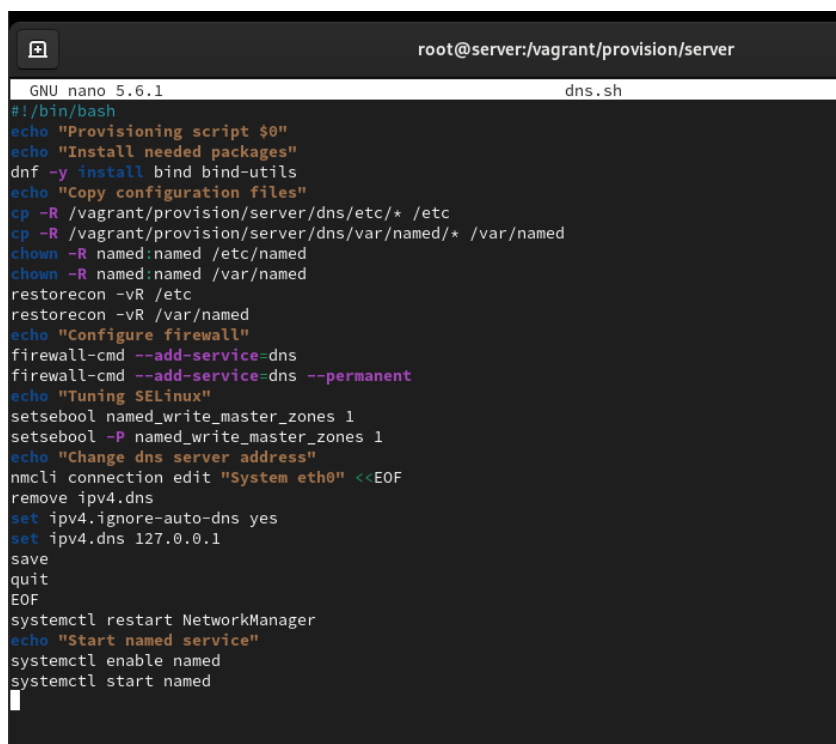
На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём ка-

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

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

Рис. 3.22: Создание каталога dns и перенос в него файлов, создание dns.sh

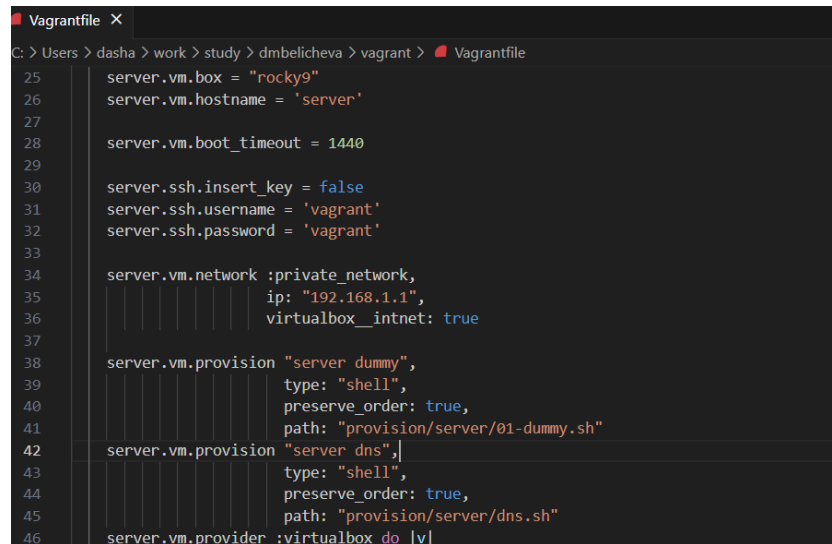
Запишем в dns.sh следующий скрипт:



```
GNU nano 5.6.1 dns.sh
#!/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. 3.23: Изменение скрипта

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



The image shows a code editor window titled 'Vagrantfile'. The editor displays a Vagrantfile configuration for a VM named 'server'. The configuration includes settings for the VM box, hostname, boot timeout, SSH settings, network configuration, and provision scripts. The file is edited in a dark-themed editor with line numbers on the left.

```
25 server.vm.box = "rocky9"
26 server.vm.hostname = 'server'
27
28 server.vm.boot_timeout = 1440
29
30 server.ssh.insert_key = false
31 server.ssh.username = 'vagrant'
32 server.ssh.password = 'vagrant'
33
34 server.vm.network :private_network,
35 | ip: "192.168.1.1",
36 | virtualbox____intnet: true
37
38 server.vm.provision "server dummy",
39 | type: "shell",
40 | preserve_order: true,
41 | path: "provision/server/01-dummy.sh"
42 server.vm.provision "server dns",
43 | type: "shell",
44 | preserve_order: true,
45 | path: "provision/server/dns.sh"
46 server.vm.provider :virtualbox do |v|
```

Рис. 3.24: Изменение Vagrantfile

4 Выводы

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