

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2**

**Настройка DNS-сервера**

дисциплина: Администрирование Сетевых Подсистем

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

## Цель работы:

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

## Выполнение работы:

### 1. Установка DNS-сервера

1. Загрузите вашу операционную систему и перейдите в рабочий каталог с проектом:

```
cd /var/tmp/user_name/vagrant
```

2. Запустите виртуальную машину server:

```
make server (или, если вы работаете под ОС Windows, то vagrant up server).
```

```
PS D:\work\kreachna\vagrant> vagrant up server
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: Preparing master VM for linked clones...
server: This is a one time operation. Once the master VM is prepared,
server: it will be used as a base for linked clones, making the creation
server: of new VMs take milliseconds on a modern system.
==> server: Importing base box 'rocky9'...
```

3. На виртуальной машине server войдите под созданным вами в предыдущей работе пользователем и откройте терминал. Перейдите в режим суперпользователя:

```
sudo -i
```

```
[kreachna@server.kreachna.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 kreachna:
```

4. Установите bind и bind-utils:

```
dnf -y install bind bind-utils
```

```
[root@server.kreachna.net ~]# dnf -y install bind bind-utils
Last metadata expiration check: 1:15:39 ago on Sat 12 Nov 2022 02:05:27 PM UTC.
Package bind-utils-32:9.16.23-1.el9_0.1.x86_64 is already installed.
Dependencies resolved.
=====
Package                Arch          Version          Repository      Size
=====
Installing:
bind                   x86_64        32:9.16.23-1.el9_0.1  appstream      489 k
Installing dependencies:
bind-dnssec-doc        noarch        32:9.16.23-1.el9_0.1  appstream       46 k
python3-bind           noarch        32:9.16.23-1.el9_0.1  appstream       61 k
python3-ply            noarch        3.11-14.el9          appstream      103 k
Installing weak dependencies:
bind-dnssec-utils      x86_64        32:9.16.23-1.el9_0.1  appstream      114 k

Transaction Summary
=====
Install 5 Packages

Total download size: 813 k
Installed size: 2.5 M
Downloading Packages:
(1/5): python3-ply-3.11-14.el9.noarch.rpm                229 kB/s | 103 kB    00:00
(2/5): bind-9.16.23-1.el9_0.1.x86_64.rpm                 1.0 MB/s | 489 kB    00:00
(3/5): bind-dnssec-utils-9.16.23-1.el9_0.1.x86_64.rpm   232 kB/s | 114 kB    00:00
(4/5): bind-dnssec-doc-9.16.23-1.el9_0.1.noarch.rpm     1.6 MB/s | 46 kB     00:00
(5/5): python3-bind-9.16.23-1.el9_0.1.noarch.rpm        1.1 MB/s | 61 kB     00:00
-----
Total                                                    766 kB/s | 813 kB    00:01
Running transaction check
Transaction check succeeded.
```

5. В качестве упражнения с помощью утилиты dig сделайте запрос, например, к DNS-адресу [www.yandex.ru](http://www.yandex.ru):

dig [www.yandex.ru](http://www.yandex.ru)

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

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40368
;; 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      77.88.55.70
www.yandex.ru.                3600    IN      A      77.88.55.66
www.yandex.ru.                3600    IN      A      5.255.255.50
www.yandex.ru.                3600    IN      A      5.255.255.55

;; Query time: 4 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 12 15:21:57 UTC 2022
;; MSG SIZE rcvd: 95
```

## 2. Конфигурирование кэширующего DNS-сервера

### 2.1. Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

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

- `/etc/resolv.conf` – Содержит указание на поиск `nssedov.net` – локального домена, а также адрес сервера имен в Интернет.
- `/etc/named.conf`:

Оператор `options` определяет параметры глобальной конфигурации сервера и устанавливает значения по умолчанию для других операторов.

```
options {  
    listen-on port 53 { 127.0.0.1; };  
    // Задаёт сетевой интерфейс, по которому named прослушивает запросы, и адрес сети.
```

```
    listen-on-v6 port 53 { ::1; };  
    // Задаёт сетевой интерфейс, по которому named прослушивает запросы, и адрес IPv6 сети.
```

```
    directory "/var/named";  
    // Задаёт рабочий каталог для named.
```

```
    dump-file "/var/named/data/cachedump.db";  
    // Задаёт дамп файл.
```

```
    statistics-file "/var/named/data/namedstats.txt";  
    // Задаёт альтернативное расположение файлов статистики.
```

```
    memstatistics-file  
    "/var/named/data/named_mem_stats.txt";  
    // Имя файла со статистикой использования памяти.
```

```
    allow-query { localhost; };  
    // Указывает клиентов, которым разрешено запрашивать информацию об этой зоне. По умолчанию разрешены все запросы.
```

```
    recursion yes;  
    // Опция, разрешающая или запрещающая рекурсию.
```

`dnssec-enable yes;` Включение или отключение `dnssec` (функция позволяет криптографически подписывать зоны с помощью ключа зоны) на уровне сервера.

`dnssec-validation yes;` Проверка корректности ответов.

`/* Путь до ключа ISC DLV */`

`bindkeys-file "/etc/named.iscdlv.key";` Альтернативный репозиторий для доверенных ключей.

`managed-keys-directory "/var/named/dynamic";` Каталог ключей управления.

`pid-file "/run/named/named.pid";` Задаёт расположение файла идентификатора процесса, созданного `named`.

`session-keyfile "/run/named/session.key";` Каталог сеансовых ключей.

`};`

`logging {` Ведение журнала.

`channel default_debug {` Канал, который обрабатывает отладочные сообщения

`file "data/named.run";` Файл отладочных сообщений

`severity dynamic;` Версия журнала

`};`

`};`

`zone "." IN {` Описание оператора зоны, идентифицируемой "."

`type hint;` `hint` - специальный тип зоны, используемый для указания на корневые серверы имен, которые разрешают запросы, когда зона не известна иначе. Никакая конфигурация, кроме значения по умолчанию, не требуется с помощью зоны подсказки.

`file "named.ca";` Файл, на который даётся указание на чтение сервисом `named`.

`};`

`/*Подключение файлов описания зон*/`

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

- /var/named/named.ca:

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без ошибок, id – 17380, использовались флаги qr aa, запрос отправлен один, ответов получено тринадцать.

Информация AUTHORITY SECTION (содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени) и ADDITIONAL SECTION (содержит IP-адреса серверов доменных имен, перечисленных в предыдущей секции). Представлены 27 элементов.

QUESTION SECTION (секция запроса): Показывает наличие запроса на A-запись;  
ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS.

Последняя секция — это статистика по запросу (служебная информация) - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.

- /var/named/named.localhost

\$TTL 1d - время, в течение которого DNS-запись для определенного хоста остается в кэш-памяти DNS-сервера после того, как последний установил соответствующий IP-адрес хоста. В данном случае 1 день.

SOA-запись — указывает на авторитативность для зоны;

name.invalid — почтовый адрес лица, осуществляющего администрирование зоны;

0; serial — серийный номер файла зоны в нотации ГТГТММДДВВ (учёт изменений файла описания зоны);

1D; refresh — интервал времени, после которого slave-сервер обязан обратиться к master-серверу с запросом на верификацию своего описания зоны (1 день);

1H; retry — интервал времени, после которого slave-сервер должен повторить попытку синхронизировать описание зоны с master сервером (1 час);

1W; expire — интервал времени, после которого slave-сервер должен прекратить обслуживание запросов к зоне, если он не смог в течение этого времени верифицировать описание зоны, используя информацию с master сервера (1 неделя);

3Н; minimum — время негативного кэширования (negative caching), т.е. время кэширования ответов, которые утверждают, что установить соответствие между доменным именем и IP-адресом нельзя (3 часа).

NS @-доменное имя сервера

A 127.0.0. - IP-адрес машины

AAAA ::1 - IPv6 -адрес

- /var/named/named.loopback

Описание первой части совпадает с описанием предыдущего файла ((4)/var/named/named.localhost)

PTR localhost — доменное имя хоста.

2. Запустите DNS-сервер:

```
systemctl start named
```

3. Включите запуск DNS-сервера в автозапуск при загрузке системы:

```
systemctl enable named
```

4. Проанализируйте в отчёте отличие в выведенной на экран информации при выполнении команд

```
dig www.yandex.ru
```

и

```
dig @127.0.0.1 www.yandex.ru
```

```
[root@server.kreachna.net ~]# systemctl start named
[root@server.kreachna.net ~]# systemctl enable named
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.
[root@server.kreachna.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: 57426
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1c17420e2f33be3301000000636fba79197e16aee45ffa9a (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                300     IN      A       5.255.255.50
www.yandex.ru.                300     IN      A       77.88.55.66
www.yandex.ru.                300     IN      A       77.88.55.70
www.yandex.ru.                300     IN      A       5.255.255.55

;; Query time: 273 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 12 15:23:37 UTC 2022
;; MSG SIZE rcvd: 134
```

5. Сделайте DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить настройки сетевого соединения System 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:

```
nmcli connection edit System\ eth0
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
```

6. Перезапустите NetworkManager:

```
systemctl restart NetworkManager
```

```
[root@server.kreachna.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, 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.kreachna.net ~]# systemctl restart NetworkManager
```

7. Требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесите изменения в файл /etc/named.conf, заменив строку



```
root@server:/ x mc [root@server.kreachna.net]:/etc x
named.conf [-M--] 55 L:[ 1+18 19/ 60] *(664 /1743b) 0010 0x00A [
//
// 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; };
```

8. Внесите изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:

```
[root@server.kreachna.net /]# firewall-cmd --add-service=dns
Warning: ALREADY_ENABLED: 'dns' already in 'public'
success
[root@server.kreachna.net /]# firewall-cmd --add-service=dns --permanent
success
```

9. Убедитесь, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используйте команду lsof:

```
[root@server.kreachna.net /]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1003/gvfs
Output information may be incomplete.
avahi-daemon 547      avahi    12u      IPv4      18032     0t0      UDP *:mdns
avahi-daemon 547      avahi    13u      IPv6      18033     0t0      UDP *:mdns
avahi-daemon 547      avahi    14u      IPv4      18034     0t0      UDP *:5375
avahi-daemon 547      avahi    15u      IPv6      18035     0t0      UDP *:34275
chronyd       558      chrony   5u       IPv4      17861     0t0      UDP localhost:323
chronyd       558      chrony   6u       IPv6      17862     0t0      UDP localhost:323
named         5668     named    16u      IPv4      33581     0t0      UDP localhost:domain
named         5668     named    19u      IPv6      33583     0t0      UDP localhost:domain
named         5668 5669 isc-net-0 16u      IPv4      33581     0t0      UDP localhost:domain
named         5668 5669 isc-net-0 19u      IPv6      33583     0t0      UDP localhost:domain
named         5668 5670 isc-timer 16u      IPv4      33581     0t0      UDP localhost:domain
named         5668 5670 isc-timer 19u      IPv6      33583     0t0      UDP localhost:domain
named         5668 5671 isc-socke 16u      IPv4      33581     0t0      UDP localhost:domain
named         5668 5671 isc-socke 19u      IPv6      33583     0t0      UDP localhost:domain
named         5668 5694 isc-net-0 16u      IPv4      33581     0t0      UDP localhost:domain
```

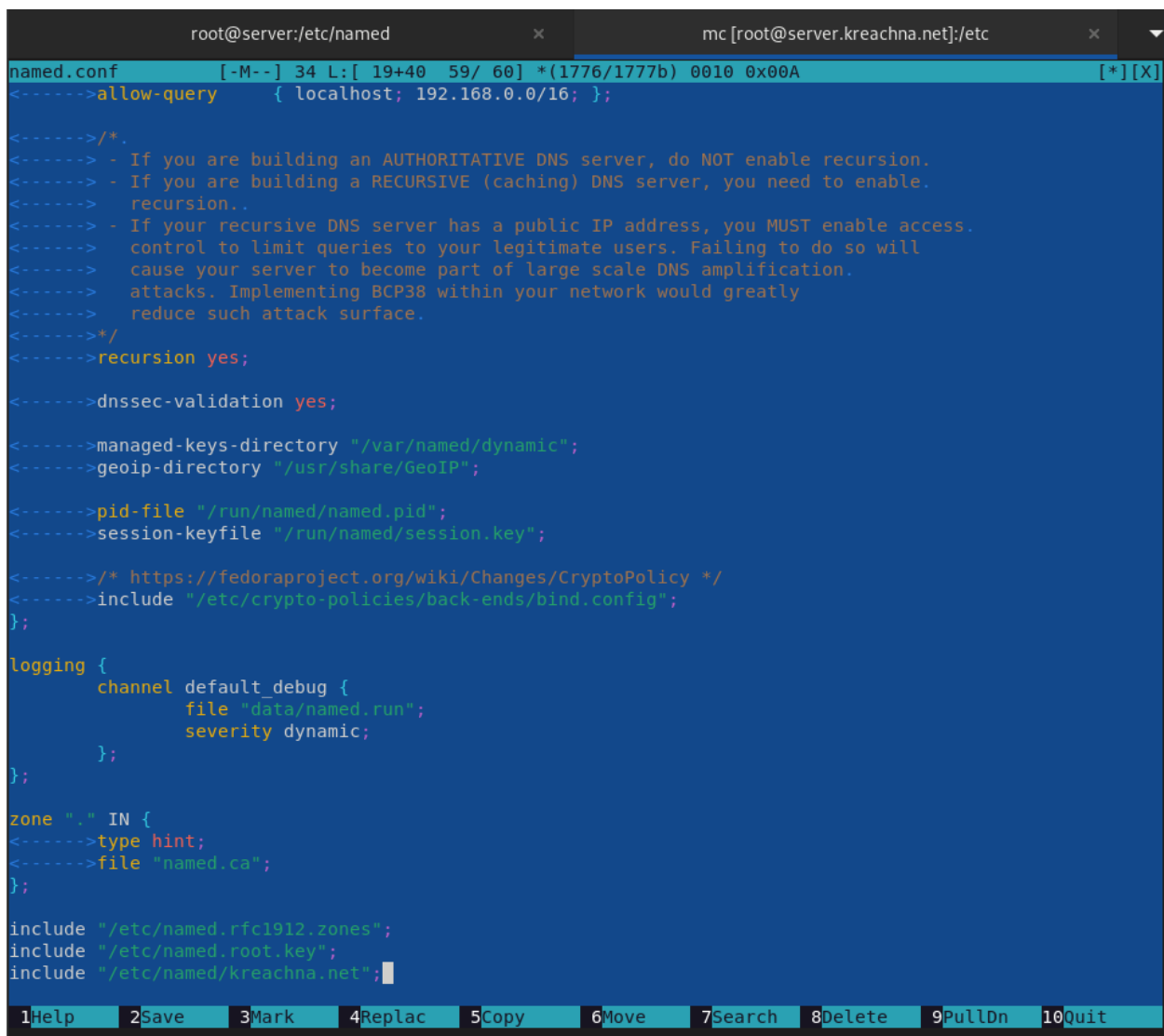
## 2.2. Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами

## 2.3. Конфигурирование первичного DNS-сервера

1. Скопируйте шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименуйте его в `user.net` (вместо `user` укажите свой логи):

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

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



```
root@server:/etc/named x mc [root@server.kreachna.net]:/etc x  
named.conf [-M--] 34 L: [ 19+40 59/ 60] *(1776/1777b) 0010 0x00A [*][X]  
<----->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..  
<-----> - 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-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 {  
        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/kreachna.net";
```

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

3. Откройте файл `/etc/named/user.net` на редактирование и вместо зоны

```

kreachna.net      [-M--]  0 L:[ 5+23 28/ 29] *(699 / 700b) 0010 0x00A
// 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 "kreachna.net" IN {
<----->type master;
<----->file "master/fz/kreachna.net";
<----->allow-update { none; };
};

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

```

4. В каталоге /var/named создайте подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно:

```

[root@server.kreachna.net ~]# cd /var/named
[root@server.kreachna.net named]# mkdir -p /var/named/master/fz
[root@server.kreachna.net named]# mkdir -p /var/named/master/rz

```

5. Скопируйте шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуйте его в user.net (вместо user укажите свой логин):

```

[root@server.kreachna.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.kreachna.net named]# cd /var/named/master/fz/
[root@server.kreachna.net fz]# mv named.localhost kreachna.net

```

6. Измените файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны. В этом файле DNS-имя сервера @ name.invalid. должно быть заменено на @ server.user.net. (вместо user должен быть указан ваш логин); формат серийного номера ГТГГММДДВВ (ГТГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии) [1]; адрес в А-записи должен быть заменён с 127.0.0.1 на 192.168.1.1; в директиве \$ORIGIN должно быть задано текущее имя домена user.net. (вместо user должен быть указан ваш логин), а затем указаны имена и адреса серверов в этом домене в виде А-записей DNS (на данном этапе должен быть прописан сервер с именем ns и адресом 192.168.1.1). При этом внимательно отнеситесь к синтаксису в этом файле, а именно к пробелам и табуляции. В результате должен получиться файл следующего содержания:

```
root@server:/var/named/master/fz  x  mc [root@server.kreachna.net]:/var/na...  x  ▾
kreachna.net  [----] 35 L:[ 1+11 12/ 13] *(220 / 221b) 0010 0x00A [*][X]
$TTL 1D
@<----->IN SOA<@ server.kreachna.net. (
<-----><-----><-----><-----><----->2020110500<----->; serial
<-----><-----><-----><-----><----->1D<----->; refresh
<-----><-----><-----><-----><----->1H<----->; retry
<-----><-----><-----><-----><----->1W<----->; expire
<-----><-----><-----><-----><----->3H )<----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
$ORIGIN kreachna.net.
server<----->A<----->192.168.1.1
ns<-----><----->A<----->192.168.1.1
```

7. Скопируйте шаблон обратной DNS-зоны `named.loopback` из каталога `/var/named` в каталог `/var/named/master/rz` и переименуйте его в `192.168.1`:

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

8. Измените файл `/var/named/master/rz/192.168.1`, указав необходимые DNS-записи для обратной зоны. В этом файле DNS-имя сервера `@ name.invalid.` должно быть заменено на `@ server.user.net.` (вместо `user` должен быть указан ваш логин); формат серийного номера `ГГГГММДДВВ` (`ГГГГ` — год, `ММ` — месяц, `ДД` — день, `ВВ` — номер ревизии); адрес в `A`-записи должен быть заменён с `127.0.0.1` на `192.168.1.1`; в директиве `$ORIGIN` должно быть задано название обратной зоны в виде `1.168.192.in-addr.arpa.`, затем заданы `PTR`-записи (на данном этапе должна быть задана `PTR` запись, ставящая в соответствие адресу `192.168.1.1` DNS-адрес `ns.user.net`). В результате должен получиться файл следующего содержания:

```
root@server:/var/named/master/rz  x  mc [root@server.kreachna.net]:/var/na...  x  ▾
192.168.1  [----] 32 L:[ 1+12 13/ 14] *(266 / 267b) 0010 0x00A [*][X]
$TTL 1D
@<----->IN SOA<@ server.kreachna.net. (
<-----><-----><-----><-----><----->2020110500<----->; serial
<-----><-----><-----><-----><----->1D<----->; refresh
<-----><-----><-----><-----><----->1H<----->; retry
<-----><-----><-----><-----><----->1W<----->; expire
<-----><-----><-----><-----><----->3H )<----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
<----->PTR<---->server.kreachna.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<----->PTR<---->server.kreachna.net.
1<----->PTR<---->ns.kreachna.net.
```

9. Далее требуется исправить права доступа к файлам в каталогах `/etc/named` и `/var/named`, чтобы демон `named` мог с ними работать:

```
chown -R named:named /etc/named
```

```
chown -R named:named /var/named
```

```
[root@server.kreachna.net rz]# chown -R named:named /etc/named
[root@server.kreachna.net rz]# chown -R named:named /var/named
```

10. 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:

```
[root@server.kreachna.net rz]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:u
ser_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@server.kreachna.net rz]# restorecon -vR /var/named
[root@server.kreachna.net rz]#
[root@server.kreachna.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.kreachna.net rz]# setsebool named_write_master_zones 1
[root@server.kreachna.net rz]# setsebool -P named_write_master_zones 1
```

11. Во дополнительном терминале запустите в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:

```
root@server:/vagrant x mc [root@server.kreac... x root@server:~ x
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# journalctl -x -f
Nov 12 18:34:10 server.kreachna.net kernel: SELinux: policy capability genfs_se
clabel_symlinks=0
Nov 12 18:34:10 server.kreachna.net setsebool[9258]: The named_write_master_zone
s policy boolean was changed to 1 by root
Nov 12 18:34:28 server.kreachna.net dbus-broker-launch[7654]: avc: op=load_polic
y lsm=selinux seqno=6 res=1
Nov 12 18:34:28 server.kreachna.net systemd[7628]: selinux: avc: op=load_policy
lsm=selinux seqno=6 res=1
Nov 12 18:34:28 server.kreachna.net systemd[7628]: Started VTE child process 926
5 launched by gnome-terminal-server process 8383.
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit UNIT has finished successfully.

The job identifier is 590.
Nov 12 18:34:35 server.kreachna.net sudo[9291]: kreachna : TTY=pts/3 ; PWD=/root
; USER=root ; COMMAND=/bin/bash
Nov 12 18:34:35 server.kreachna.net dbus-broker-launch[546]: avc: op=load_polic
y lsm=selinux seqno=6 res=1

root@server:/vagrant x mc [root@server.kreac... x root@server:~ x
[root@server.kreachna.net rz]# systemctl restart named
[root@server.kreachna.net rz]#
```

## 2.4. Анализ работы DNS-сервера

1. При помощи утилиты dig получите описание DNS-зоны с сервера ns.user.net (вместо user должен быть указан ваш логин):

```
dig ns.user.net
```

```
root@server:/vagrant x mc [root@server.kreac... x root@server:~
[root@server.kreachna.net ~]# dig ns.kreachna.net

; <<>> DiG 9.16.23-RH <<>> ns.kreachna.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14272
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cf4a9e23314096e601000000636fe7c5b5f33523d3554ffb (good)
;; QUESTION SECTION:
;ns.kreachna.net.                IN      A

;; ANSWER SECTION:
ns.kreachna.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 12 18:36:53 UTC 2022
;; MSG SIZE rcvd: 88
```

2. При помощи утилиты host проанализируйте корректность работы DNS-сервера:

```
[root@server.kreachna.net ~]# host -l kreachna.net
kreachna.net name server kreachna.net.
kreachna.net has address 192.168.1.1
ns.kreachna.net has address 192.168.1.1
server.kreachna.net has address 192.168.1.1
[root@server.kreachna.net ~]# host -a kreachna.net
Trying "kreachna.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5895
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
kreachna.net.                86400   IN      SOA     kreachna.net. server.kreachna.net.
t. 2020110500 86400 3600 604800 10800
kreachna.net.                86400   IN      NS      kreachna.net.
kreachna.net.                86400   IN      A       192.168.1.1

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

Received 119 bytes from 127.0.0.1#53 in 1 ms
```

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

## 2.5. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dns, в который поместите в соответствующие каталоги конфигурационные файлы DNS:

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

2. В каталоге /vagrant/provision/server создайте исполняемый файл dns.sh:

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



```
dns.sh x
1  #!/bin/bash
2  echo "Provisioning script $0"
3
4  echo "Install needed packages"
5  dnf -y install bind bind-utils
6
7  echo "Copy configuration files"
8  cp -R /vagrant/provision/server/dns/etc/* /etc
9  cp -R /vagrant/provision/server/dns/var/named/* /var/named
10
11  chown -R named:named /etc/named
12  chown -R named:named /var/named
13
14  restorecon -vR /etc
15  restorecon -vR /var/named
16
17  echo "Configure firewall"
18  firewall-cmd --add-service=dns
19  firewall-cmd --add-service=dns --permanent
20
21  echo "Tuning SELinux"
22  setsebool named_write_master_zones 1
23  setsebool -P named_write_master_zones 1
24
25  echo "Change dns server address"
26  nmcli connection edit "System eth0" <<EOF
27
28  remove ipv4.dns
29  set ipv4.ignore-auto-dns yes
30  set ipv4.dns 127.0.0.1
31  save
32  quit
33  EOF
34  systemctl restart NetworkManager
35
36  echo "Start named service"
37  systemctl enable named
38  systemctl start named
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

```
dns.sh x Vagrantfile x
22
23
24  # Server configuration
25  config.vm.define "server", autostart: false do |server|
26    server.vm.box = "rocky9"
27    server.vm.hostname = 'server'
28
29    server.ssh.insert_key = false
30    server.ssh.username = 'vagrant'
31    server.ssh.password = 'vagrant'
32
33    server.vm.network :private_network, ip: "192.168.1.1", virtualbox____intnet: true
34
35    server.vm.provision "server dummy",
36      type: "shell",
37      preserve_order: true,
38      path: "provision/server/01-dummy.sh"
39
40    server.vm.provision "server dns",
41      type: "shell"
42      preserve_order: true
43      path: "provision/server/dns.sh"
```

## Контрольные вопросы:

1. Что такое 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?  
Задача поиска доменного имени по IP-адресу является обратной к прямой задаче — поиску IP-адреса по доменному имени. Прямая решается в DNS при помощи записей типа A (Address). Обратная же при помощи записей-указателей типа PTR (Pointer), которые совместно с записями SOA и NS составляют описание так называемой «обратной» зоны.
4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.  
В файле `host.conf` содержатся опции программы-определителя, в файле `resolv.conf` содержатся адреса серверов имен, к которым имеет доступ данная система. Файл `named.ca` организует кэширование для сервера имен.
5. Что указывается в файле `resolv.conf`?  
В файле `resolv.conf` содержатся адреса серверов имен, к которым имеет доступ данная система.
6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?
  - SOA-запись — указывает на авторитативность для зоны
  - NS-запись — перечисляет DNS-серверы зоны
  - A — отображение имён узлов в адреса
  - PTR — отображение адресов в имена узлов
  - CNAME — каноническое имя (для псевдонимов)
  - MX — отображение имён почтовых серверов
7. Для чего используется домен `in-addr.arpa`?  
Для отображения IP-адресов IPv4 в пространство доменных имен
8. Для чего нужен демон `named`?

Демон `named` может реализовывать функции серверов любого типа: `master`, `slave`, `cache`.

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

- `master` — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых
- `slave` — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.

10. Какие параметры отвечают за время обновления зоны?

За обновление отвечает третий параметр в файле `kreachna.net`

11. Как обеспечить защиту зоны от скачивания и просмотра?

Задать подходящие права доступа на чтение и запись.

12. Какая запись `RR` применяется при создании почтовых серверов?

При создании почтовых серверов используют `A` записи.

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

Использовать в терминале команды `systemctl start, restart, stop`.

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

Посмотреть в `journalctl`.

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

```
nmcli connection edit System\ eth0
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
```

16. Что такое `SELinux`?

(`SELinux`) - это модуль безопасности ядра `Linux`, который обеспечивает механизм поддержки политик безопасности контроля доступа, включая обязательные элементы управления доступом (`MAC`).

17. Что такое контекст (метка) `SELinux`?

Каждый файл, процесс, каталог и порт имеют специальную метку безопасности,

известную как контекст SELinux, который является именем, используемым для определения, может ли процесс получить доступ к файлу, каталогу или порту.

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

restorecon.

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

Использовать команду `chown -R`

20. Что такое булевый переключатель в SELinux?

21. Как посмотреть список переключателей SELinux и их состояние?

Команда `getsebool -a | grep named`

22. Как изменить значение переключателя SELinux

Необходимо использовать команду `setsebool`.

## **Вывод**

Я установила и сконфигурировала DNS-сервер, и разобрался с основными принципами системы доменных имён.