

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2

дисциплина: Администрирование сетевых подсистем

Настройка DNS-сервера

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы

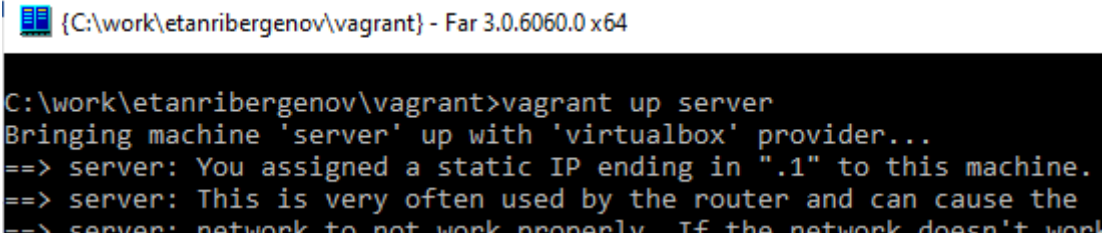
Приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

Ход работы

1. Установка DNS-сервера

- 1) Запустите виртуальную машину server:

```
vagrant up server
```



```
{C:\work\etanribergenov\vagrant} - Far 3.0.6060.0 x64  
C:\work\etanribergenov\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
```

Рис. 1. Запуск VM Server

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

```
sudo -i
```

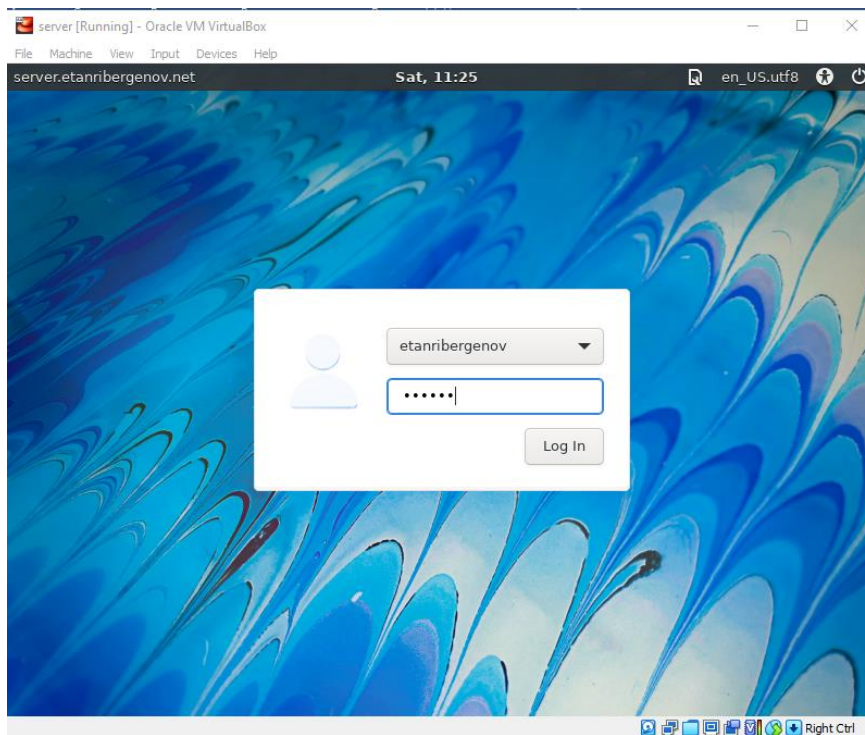


Рис. 2. Вход в систему

```
root@server:~  
[etanribergenov@server.etanribergenov.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 etanribergenov:  
[root@server.etanribergenov.net ~]#
```

Рис. 3. Переход в режим суперпользователя

3) Установите bind и bind-utils

```
root@server:~  
[root@server.etanribergenov.net ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 17 kB/s | 24 kB 00:01  
Extra Packages for Enterprise Linux 9 - x86_64 2.3 MB/s | 14 MB 00:06  
Rocky Linux 9 - BaseOS 671 B/s | 4.1 kB 00:06  
Rocky Linux 9 - BaseOS 445 kB/s | 1.8 MB 00:04  
Rocky Linux 9 - AppStream 2.8 kB/s | 4.5 kB 00:01  
Rocky Linux 9 - AppStream 874 kB/s | 6.6 MB 00:07  
Rocky Linux 9 - Extras 2.6 kB/s | 2.9 kB 00:01  
Rocky Linux 9 - Extras 4.0 kB/s | 8.5 kB 00:02  
Last metadata expiration check: 0:00:01 ago on Sat 18 Feb 2023 11:34:52 AM 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	32:9.16.23-5.el9_1	appstream	488 k
Upgrading:				
bind-libs	x86_64	32:9.16.23-5.el9_1	appstream	1.2 M
bind-license	noarch	32:9.16.23-5.el9_1	appstream	14 k
bind-utils	x86_64	32:9.16.23-5.el9_1	appstream	200 k
Installing dependencies:				
bind-dnssec-doc	noarch	32:9.16.23-5.el9_1	appstream	46 k
ovn3-bind	noarch	32:9.16.23-5.el9_1	appstream	62 k

Рис. 4. Установка bind и bind-utils

- 4) В качестве упражнения с помощью утилиты dig сделайте запрос, например, к DNS
- а
 - д Работа dig с DNS-адресом www.yandex.ru
 - р Глобальные настройки: командная строка
 - е Получен ответ с кодом операции, статусом и id
 - е Используемые флаги; 1 запрос; 4 ответа, приоритет 0, дополнительного 0.
 - у Раздел вопросов
 - Домен www.yandex.ru , класс сети - IN (интернет), запрос A
 - Раздел ответов: 4 ответа с домена яндекс с классом сети IN, A-запросом, с ip-адресами доменов
 - Далее указаны время совершения запроса, сервер, когда был произведён запрос и размер сообщения

```

Complete!
[root@server.etanribergenov.net ~]# dig www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41937
;; 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      77.88.55.60
www.yandex.ru.                3600    IN      A      5.255.255.70
www.yandex.ru.                3600    IN      A      77.88.55.88
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 Feb 18 11:42:17 UTC 2023
;; MSG SIZE rcvd: 95

[root@server.etanribergenov.net ~]#

```

Рис. 5. Запрос к DNS-адресу www.yandex.ru

2. Конфигурирование кэширующего DNS-сервера

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

1) Проанализируйте построчно содержание файлов /etc/resolv.conf, /etc/named.conf,

- Файл /etc/resolv.conf:

Создан сетевым менеджером, доменное имя, адрес домена.

Файл /etc/named.conf:

Показаны опции, доступна рекурсия, подтверждение dns защиты включено, каталог с ключами, каталог с ip адресом, файл id процесса, файл ключа сессии, запись процессов

- Файл /var/named/named.ca:

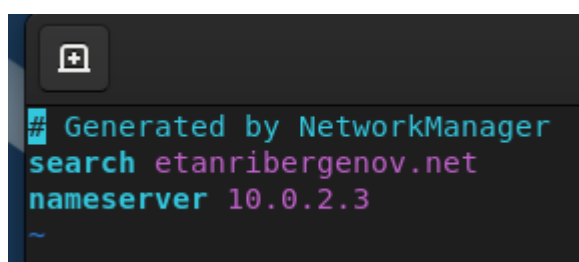
Информация о запросе, раздел вопросов, раздел ответов и раздел дополнительного, тех. данные о запросе (время, размер)

- Файл /var/named/named.localhost:

Указаны класс сети и типы запроса с разными параметрами.

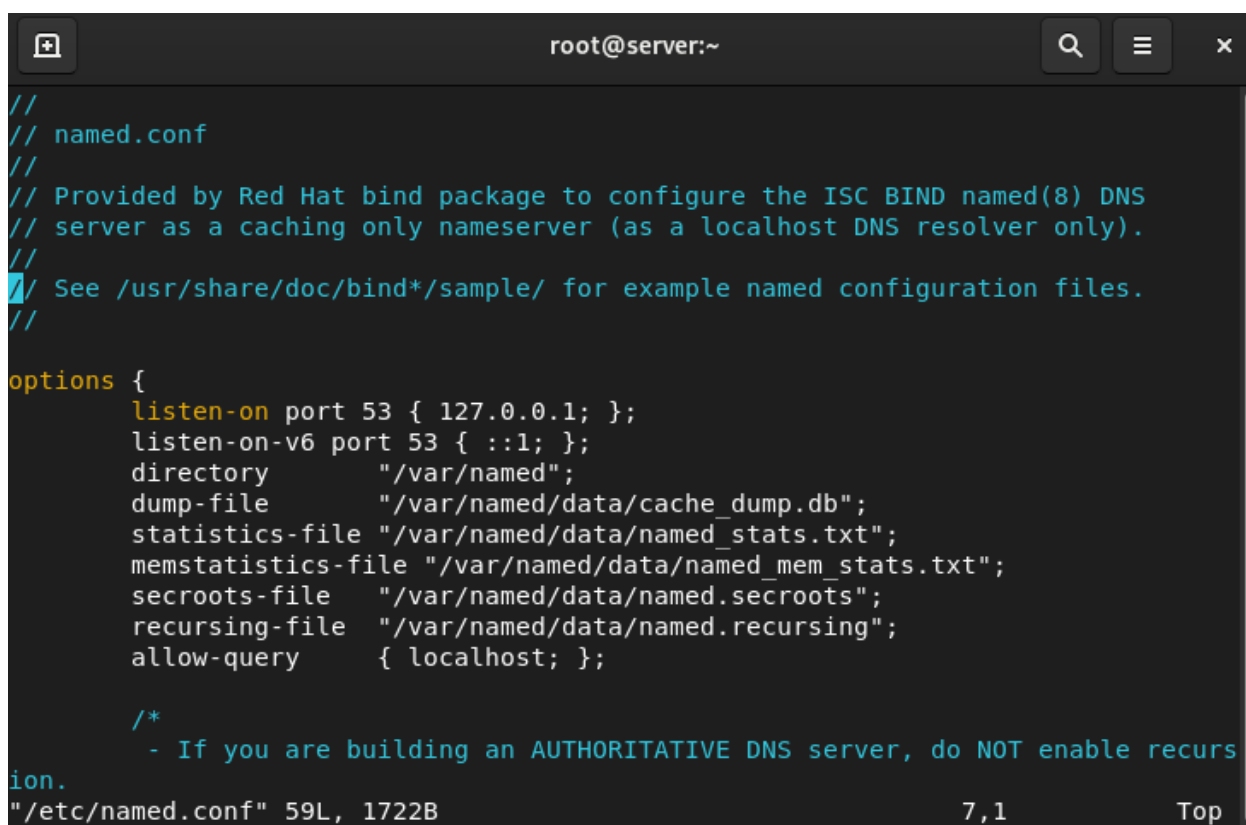
- Файл /var/named/named.loopback:

То же, что и у предыдущего, но есть указатель - localhost



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

Рис. 6. Файл /etc/resolv.conf



```
root@server:~
//
// 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; };

    /*
     * If you are building an AUTHORITATIVE DNS server, do NOT enable recurs
ion.
*/
}

"/etc/named.conf" 59L, 1722B 7,1 Top
```

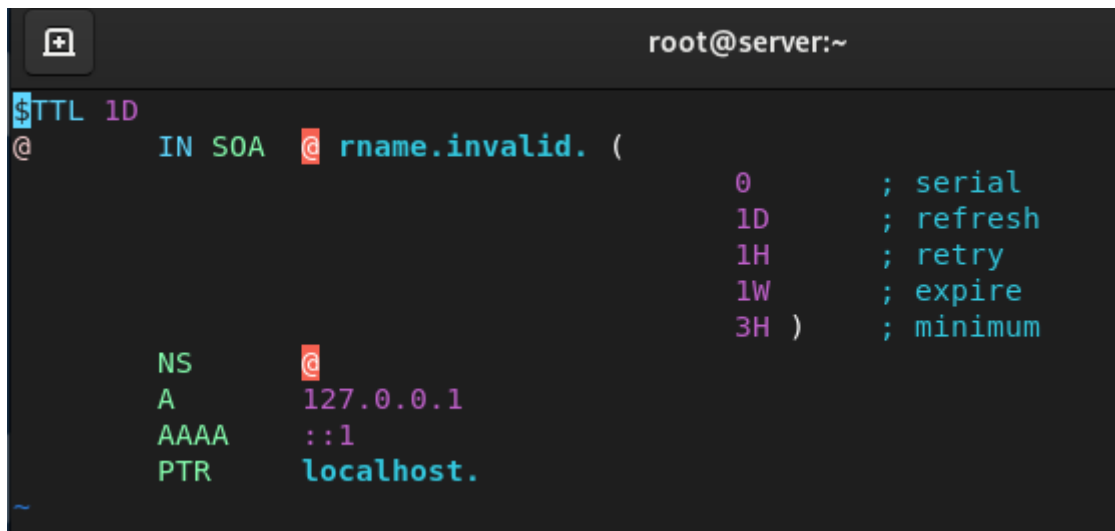
Рис. 7. Файл /etc/named.conf

```
root@server:~  
; <<>> DiG 9.11.3-RedHat-9.11.3-3.fc27 <<>> +bufsize=1200 +norec @a.root-servers  
.net  
; (2 servers found)  
;; global options: +cmd  
; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46900  
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1472  
;; 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.  
518400 IN NS e.root-servers.net.  
518400 IN NS f.root-servers.net.  
518400 IN NS g.root-servers.net.  
518400 IN NS h.root-servers.net.  
5,1 Top
```

Рис. 8. Файл /var/named/named.ca

```
root@server:~  
$TTL 1D  
@ IN SOA @ rname.invalid. (  
0 ; serial  
1D ; refresh  
1H ; retry  
1W ; expire  
3H ) ; minimum  
  
NS @  
A 127.0.0.1  
AAAA ::1
```

Рис. 9. Файл /var/named/named.localhost

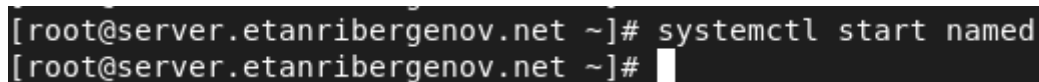


```
root@server:~  
$TTL 1D  
@ IN SOA @ rname.invalid. (  
                                0      ; serial  
                                1D     ; refresh  
                                1H     ; retry  
                                1W     ; expire  
                                3H )   ; minimum  
NS  @  
A   127.0.0.1  
AAAA ::1  
PTR localhost.
```

Рис. 10. Файл /var/named/named.loopback

- 2) Запустите DNS-сервер:

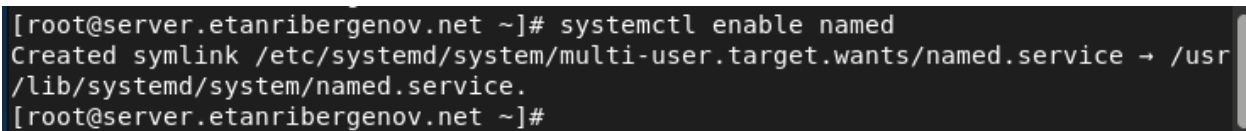
`systemctl start named`



```
[root@server.etanribergenov.net ~]# systemctl start named  
[root@server.etanribergenov.net ~]#
```

Рис. 11. Запуск DNS-сервера

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



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

Рис. 12. Включение запуска DNS-сервера в автозапуск при загрузке системы

- 4) Проанализируйте в отчёте отличие в выведенной на экран информации при выполнении команд
и

Во втором случае вывелся какой-то псевдо раздел с информацией о версии, использованных флагов, uid и куки. В конце различаются размеры сообщений.


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

;; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24300
;; 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      5.255.255.80
www.yandex.ru.                3600    IN      A      77.88.55.55
www.yandex.ru.                3600    IN      A      5.255.255.88
www.yandex.ru.                3600    IN      A      77.88.55.50

;; Query time: 6 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Feb 18 12:42:39 UTC 2023
;; MSG SIZE rcvd: 95

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

Рис. 13. Первый вариант применения команды dig

```
root@server:~  
[root@server.etanribergenov.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: 41425  
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 18069067f25916f70100000063f0c82245909aca6bf52127 (good)  
;; QUESTION SECTION:  
;www.yandex.ru.                IN      A  
  
;; ANSWER SECTION:  
www.yandex.ru.                300     IN      A      77.88.55.50  
www.yandex.ru.                300     IN      A      5.255.255.80  
www.yandex.ru.                300     IN      A      77.88.55.55  
www.yandex.ru.                300     IN      A      5.255.255.88  
  
;; Query time: 721 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
.. WHEN: Sat Feb 18 12:44:18 UTC 2023
```

Рис. 14. Второй вариант применения команды dig

- 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
```

```
[root@server.etanribergenov.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, d
cb, sriov, ethtool, match, ipv4, ipv6, hostname, tc, proxy
nmcli>
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.etanribergenov.net ~]#
```

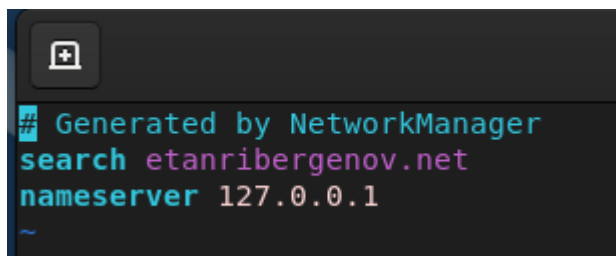
Рис. 15. Назначение DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети

6) Перезапустите NetworkManager:

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

Рис. 16. Перезапуск NetworkManager

Проверил изменение в файле /etc/resolv.conf: изменился DNS-адрес



```
# Generated by NetworkManager
search etanribergenov.net
nameserver 127.0.0.1
~
```

Рис. 17. Файл etc/resolv.conf

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 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;

```
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. 18. Изменения в файле /etc/named.conf

- 8) Внесите изменения в настройки межсетевого экрана узла server, разрешив работу с

```
firewall-cmd --add-service=dns
```

```
firewall-cmd --add-service=dns --permanent
```

```
[root@server.etanribergenov.net ~]# firewall-cmd --add-service=dns
success
[root@server.etanribergenov.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.etanribergenov.net ~]#
```

Рис. 19. Разрешение работы межсетевого экрана узла server с dns

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

```
root@server:~  
[root@server.etanribergenov.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 556 avahi 12u IPv4 18149  
0t0 UDP *:mdns  
avahi-dae 556 avahi 13u IPv6 18150  
0t0 UDP *:mdns  
avahi-dae 556 avahi 14u IPv4 18151  
0t0 UDP *:55041  
avahi-dae 556 avahi 15u IPv6 18152  
0t0 UDP *:41913  
chronyd 593 chrony 5u IPv4 18136  
0t0 UDP localhost:323  
chronyd 593 chrony 6u IPv6 18137  
0t0 UDP localhost:323  
named 40805 named 16u IPv4 73097  
0t0 UDP localhost:domain  
named 40805 named 19u IPv6 73099  
0t0 UDP localhost:domain  
named 40805 40806 isc-net-0 named 16u IPv4 73097  
0t0 UDP localhost:domain  
named 40805 40806 isc-net-0 named 19u IPv6 73099  
0t0 UDP localhost:domain  
named 40805 40807 isc-timer named 16u IPv4 73097
```

Рис. 20. Вывод команды lsof | grep UDP

```
NetworkMa 40994 root 26u IPv4 75364  
0t0 UDP server.etanribergenov.net:bootpc->_gateway:bootps  
NetworkMa 40994 40995 gmain root 26u IPv4 75364  
0t0 UDP server.etanribergenov.net:bootpc->_gateway:bootps  
NetworkMa 40994 40996 gdbus root 26u IPv4 75364  
0t0 UDP server.etanribergenov.net:bootpc->_gateway:bootps  
[root@server.etanribergenov.net ~]#
```

Рис. 21. Вывод команды lsof | grep UDP: запросы идут через узел server

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 логин)

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

Рис. 22. Копирование и переименование шаблона named.rfc1912.zones

2. Включите файл описания зоны /etc/named/user.net в конфигурационном файле DNS

е
т
с
н
а
м
е

```
include "/etc/named.rfc1912.zones";  
include "/etc/named.root.key";  
include "/etc/named/etanribergenov.net";  
:wq
```

д **Рис. 23. Включение файла описания зоны в конфигурационном файле DNS**
conf, добавив в нём в конце строку: include "/etc/named/user.net"; (вместо user укажите
свой логин).

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

```
zone "localhost.localdomain" IN {  
type master;  
file "named.localhost";  
allow-update { none; };  
};
```

пропишите свою прямую зону:

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

Далее, вместо зоны

z
b
fi
p
t
in

пропишите свою обратную зону:

lv
th
p
p
h

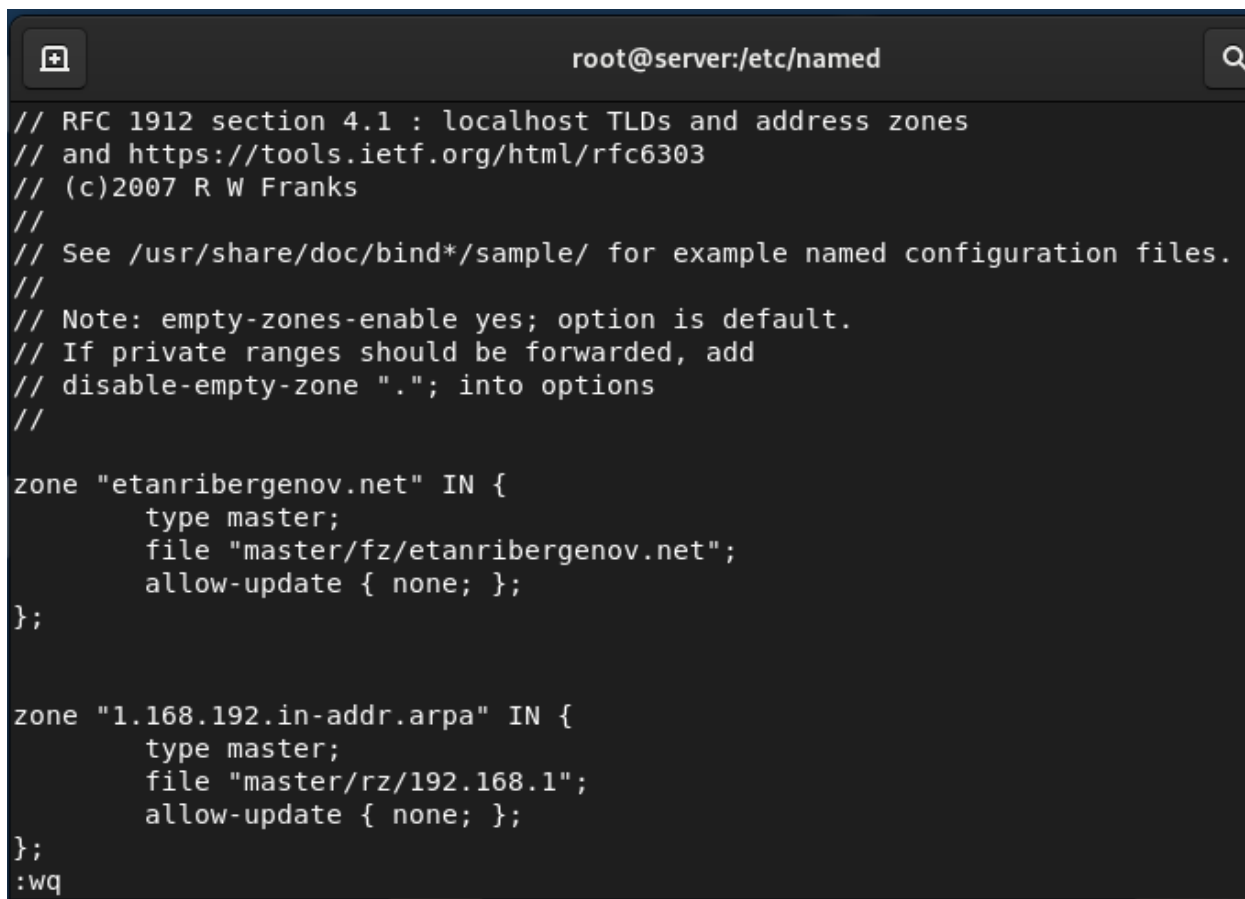
a

l

l

Остальные записи в файле /etc/named/user.net удалите.

w



```
root@server:/etc/named

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

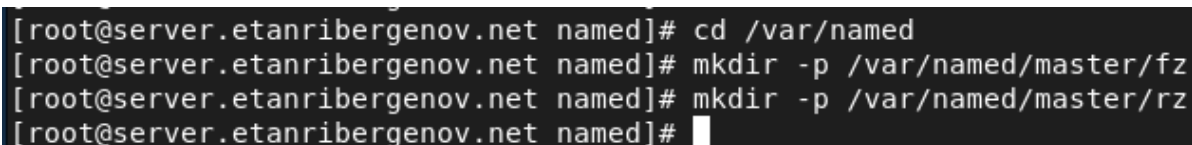
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "master/rz/192.168.1";
    allow-update { none; };
};
:wq
```

Рис. 24. Файл /etc/named/etanribergenov.net после редактирования

4. В каталоге /var/named создайте 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
```



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

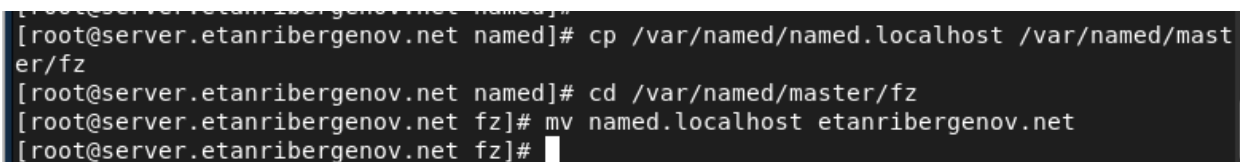
Рис. 25. Создание подкаталогов

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):

```
cp /var/named/named.localhost /var/named/master/fz/
```

```
cd /var/named/master/fz/
```

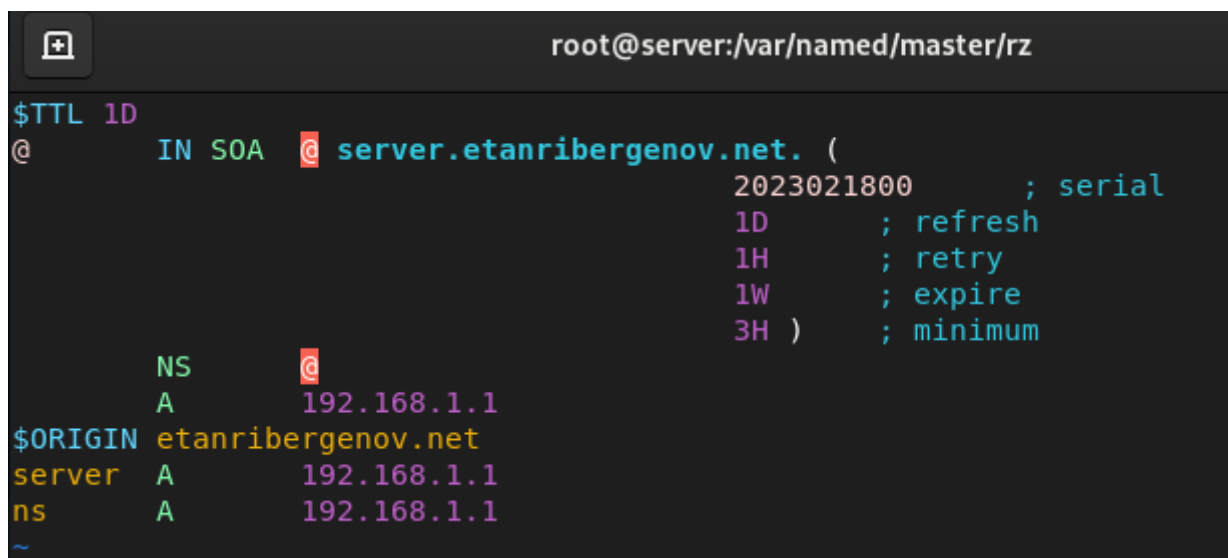
```
mv named.localhost user.net
```



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

Рис. 26. Копирование и переименование шаблона прямой DNS-зоны

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 ГГГГММДДВВ (ГГГГ — 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.



```
root@server:/var/named/master/rz
$TTL 1D
@      IN SOA  @ server.etanribergenov.net. (
                                2023021800      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H )              ; minimum

      NS      @
      A       192.168.1.1
$ORIGIN etanribergenov.net
server A      192.168.1.1
ns     A      192.168.1.1
~
```

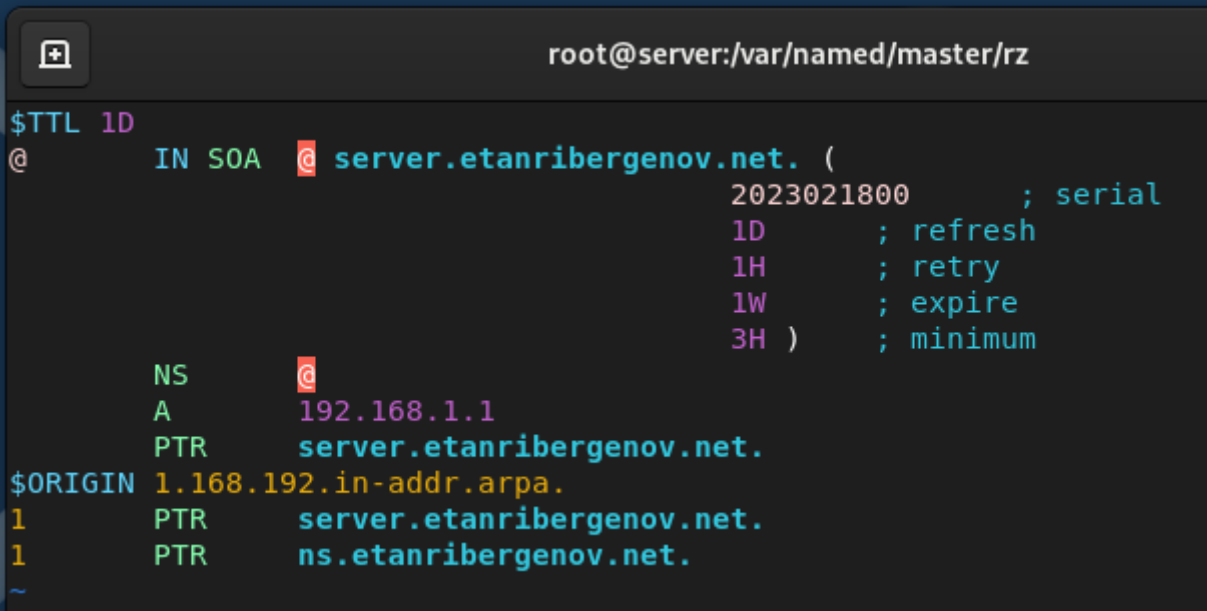
Рис. 27. Файл `/var/named/master/fz/user.net` после редактирования

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

Рис. 28. Копирование и переименование шаблона обратной DNS-зоны.

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`).



```
root@server:/var/named/master/rz
$TTL 1D
@      IN SOA  @ server.etanribergenov.net. (
                                2023021800      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H                ; minimum
    NS   @
    A    192.168.1.1
    PTR  server.etanribergenov.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR  server.etanribergenov.net.
1      PTR  ns.etanribergenov.net.
~
```

Рис. 29. Файл 192.168.1 после редактирования

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

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

Рис. 30. Изменения прав доступа к файлам

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.etanribergenov.net rz]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_t
mp_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@server.etanribergenov.net rz]# restorecon -vR /var/named
```

Рис. 31. Корректное восстановление меток файлов named в SELinux

Для проверки состояния переключателей SELinux, относящихся к named, введите:

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

Рис. 32. Проверка состояния переключателей SELinux, относящихся к named

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

```
setsebool named_write_master_zones 1
```

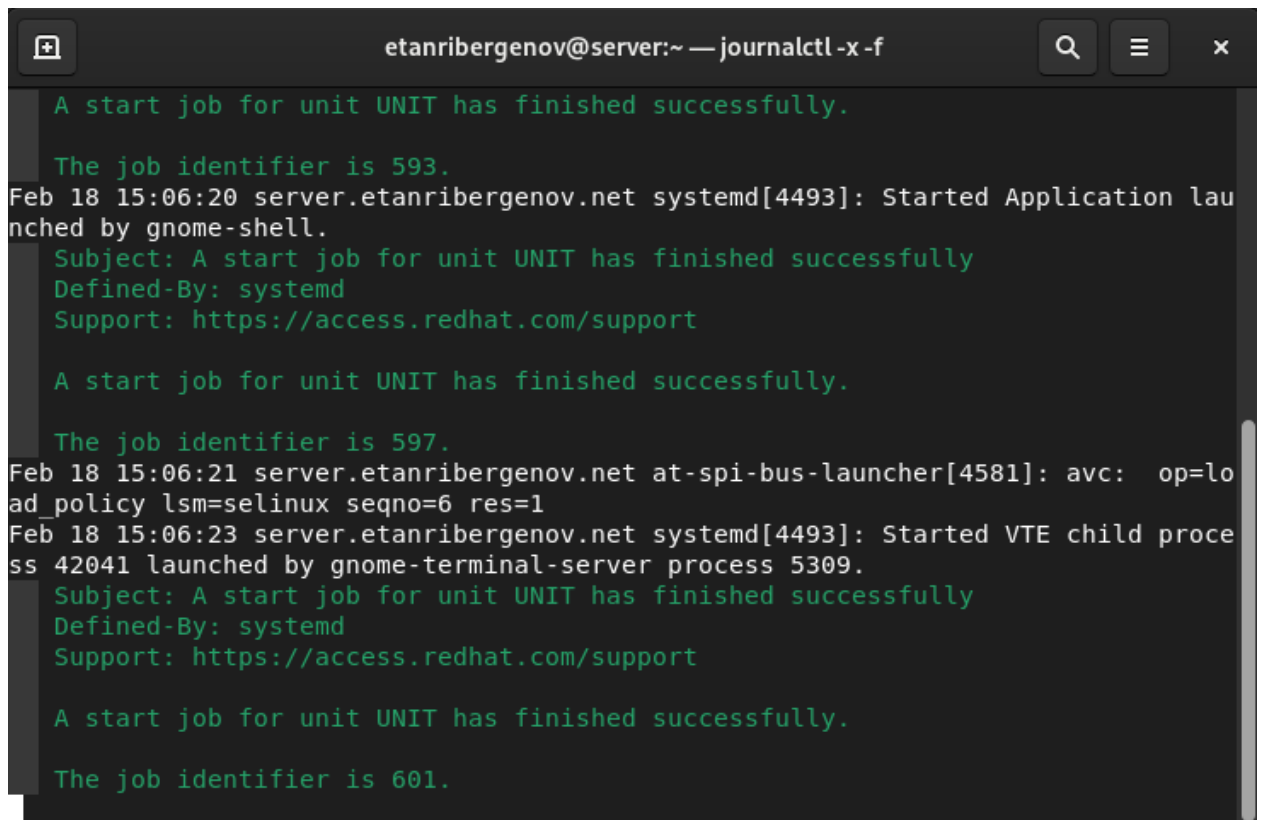
```
setsebool -P named_write_master_zones 1
```

```
[root@server.etanribergenov.net rz]# setsebool named_write_master_zones 1
[root@server.etanribergenov.net rz]# setsebool -P named_write_master_zones 1
[root@server.etanribergenov.net rz]#
```

Рис. 33. Разрешение named на запись в файлы DNS-зоны

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

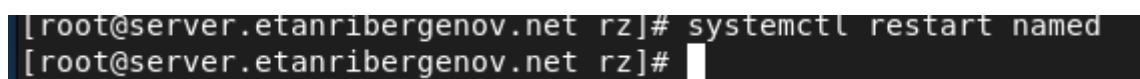
```
-f
```

A terminal window titled 'etanribergenov@server:~ — journalctl -x -f'. The output shows system logs with green text for success messages. The logs include timestamps like 'Feb 18 15:06:20' and 'Feb 18 15:06:21', and messages from 'systemd[4493]' and 'at-spi-bus-launcher[4581]'. Success messages state 'A start job for unit UNIT has finished successfully.' and provide job identifiers 593, 597, and 601. A support URL 'https://access.redhat.com/support' is also visible.

```
etanribergenov@server:~ — journalctl -x -f
A start job for unit UNIT has finished successfully.
The job identifier is 593.
Feb 18 15:06:20 server.etanribergenov.net systemd[4493]: Started Application lau
nched by gnome-shell.
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 597.
Feb 18 15:06:21 server.etanribergenov.net at-spi-bus-launcher[4581]: avc: op=lo
ad_policy lsm=selinux seqno=6 res=1
Feb 18 15:06:23 server.etanribergenov.net systemd[4493]: Started VTE child proce
ss 42041 launched by gnome-terminal-server process 5309.
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 601.
```

Рис. 34. Расширенный лог системных сообщений в дополнительном терминале

и в первом терминале перезапустите DNS-сервер:

A terminal window showing the command 'systemctl restart named' being executed as root. The prompt is '[root@server.etanribergenov.net rz]#'.

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

Рис. 35. Перезапуск DNS-сервера в первом терминале


```
root@server:/var/named/master/rz
[root@server.etanribergenov.net rz]# dig ns.etanribergenov.net

; <<>> DiG 9.16.23-RH <<>> ns.etanribergenov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10014
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7160097c7247a7580100000063f0ebc92832d381b0f4df3d (good)
;; QUESTION SECTION:
;ns.etanribergenov.net.      IN      A

;; AUTHORITY SECTION:
etanribergenov.net.      10800   IN      SOA     etanribergenov.net. server.etanriberg
enov.net. 2023021800 86400 3600 604800 10800

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Feb 18 15:16:25 UTC 2023
;; MSG SIZE rcvd: 121

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

Рис. 37. Описание DNS-зоны с сервера ns.etanribergenov.net

При помощи утилиты host проанализируйте корректность работы DNS-сервера:

```
[root@server.etanribergenov.net rz]# host -l etanribergenov.net
etanribergenov.net name server etanribergenov.net.
etanribergenov.net has address 192.168.1.1
ns.etanribergenov.net.etanribergenov.net has address 192.168.1.1
server.etanribergenov.net.etanribergenov.net has address 192.168.1.1
```

Рис. 38. Все хосты в домене

```
[root@server.etanribergenov.net rz]# host -a etanribergenov.net
Trying "etanribergenov.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6074
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
etanribergenov.net.  86400   IN      SOA      etanribergenov.net. server.etanribergenov.net. 2023021800 86400 3600 604800 10800
etanribergenov.net.  86400   IN      NS       etanribergenov.net.
etanribergenov.net.  86400   IN      A        192.168.1.1

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

Received 125 bytes from 127.0.0.1#53 in 4 ms
```

Рис. 39. Расширенная информация о домене

```
[root@server.etanribergenov.net rz]# host -t A etanribergenov.net
etanribergenov.net has address 192.168.1.1
```

Рис. 40. IPv4-адрес домена

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

Рис. 41. Указатель доменного имени серверов

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

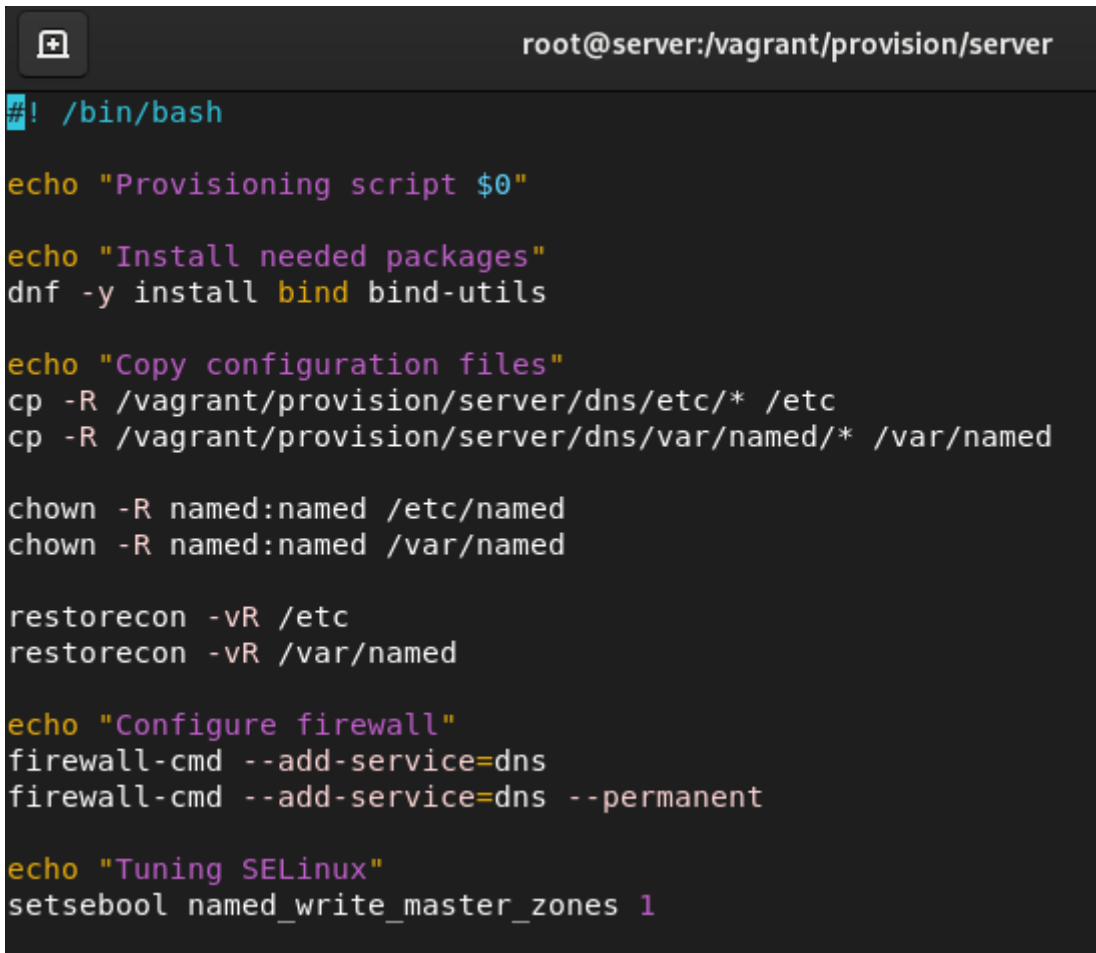
```
[root@server.etanribergenov.net rz]# cd /vagrant
[root@server.etanribergenov.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/
named
[root@server.etanribergenov.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/
named/master/
[root@server.etanribergenov.net vagrant]# cp -R /etc/named.conf /vagrant/provision/se
rver/dns/etc/
[root@server.etanribergenov.net vagrant]# cp -R /etc/named/* /vagrant/provision/serve
r/dns/etc/named/
[root@server.etanribergenov.net vagrant]# cp -R /var/named/master/* /vagrant/provisio
n/server/dns/var/named/master
[root@server.etanribergenov.net vagrant]#
```

Рис. 42. Создание каталогов и копирование конфигурационных файлов DNS

2. В каталоге `/vagrant/provision/server` создайте исполняемый файл `dns.sh`. Открыв его на редактирование, пропишите в нём скрипт.

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

Рис. 43. Создание исполняемого файла

A terminal window with a dark background. The title bar shows a window icon and the text 'root@server:/vagrant/provision/server'. The terminal content is a shell script for provisioning a DNS server. It starts with a comment and a prompt, followed by echo statements for each section: 'Provisioning script \$0', 'Install needed packages', 'Copy configuration files', 'Configure firewall', and 'Tuning SELinux'. The commands include installing bind and bind-utils, copying configuration files from the vagrant directory to /etc and /var/named, setting permissions for the named user, restoring permissions for /etc and /var/named, adding the dns service to the firewall, and setting SELinux permissions for the named user to write master zones.

```
root@server:/vagrant/provision/server

#! /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

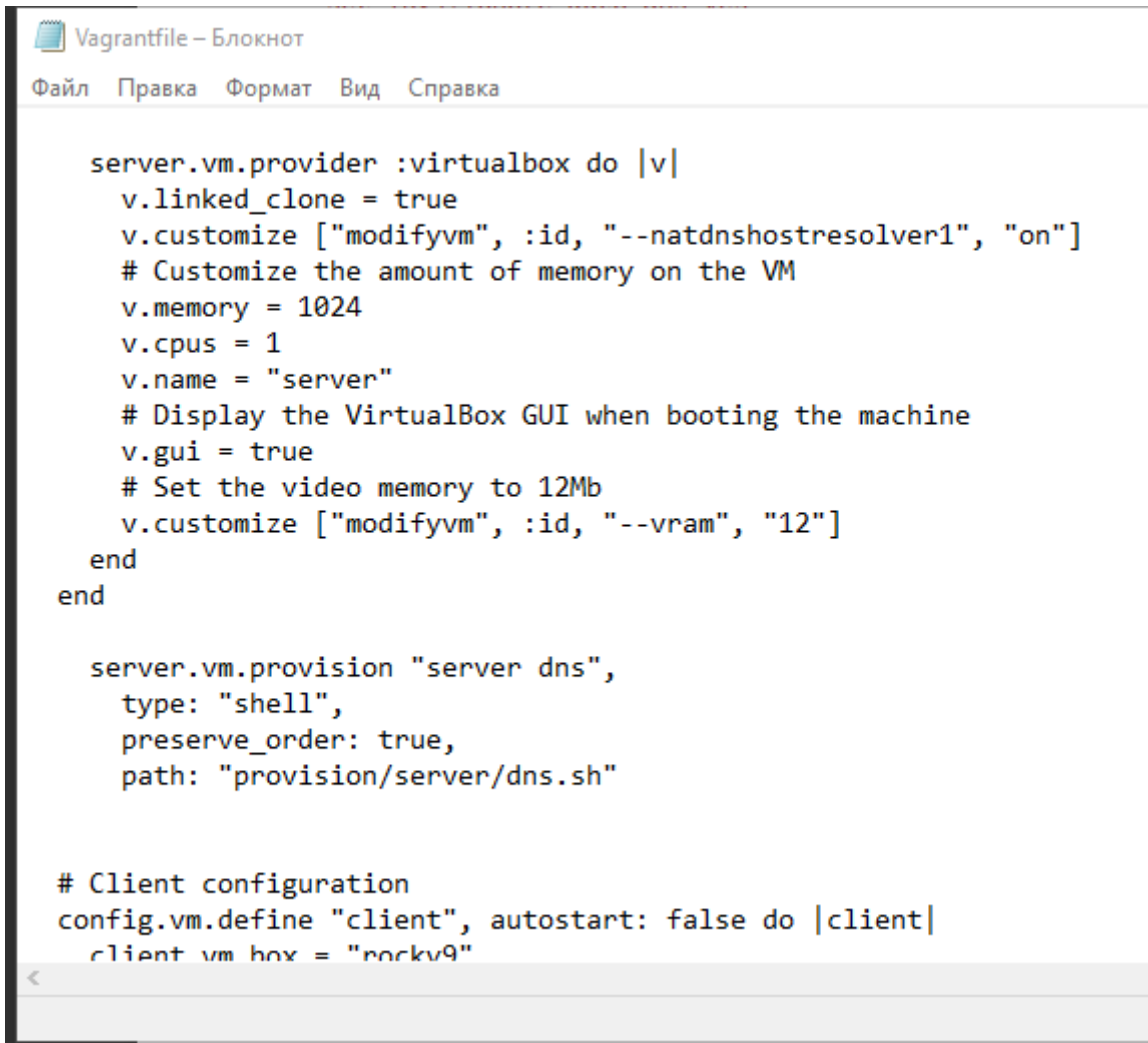
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

echo "Tuning SELinux"
setsebool named_write_master_zones 1
```

Рис. 44. Скрипт (начало)

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

```
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
  v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
  # Customize the amount of memory on the VM
  v.memory = 1024
  v.cpus = 1
  v.name = "server"
  # Display the VirtualBox GUI when booting the machine
  v.gui = true
  # Set the video memory to 12Mb
  v.customize ["modifyvm", :id, "--vram", "12"]
end
end

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

# Client configuration
config.vm.define "client", autostart: false do |client|
  client.vm.box = "rocky9"
end
```

Рис. 45. Конф. файл Vagrantfile после редактирования

Ответы на контрольные вопросы

1. Система доменных имён (Domain Name System, DNS) — распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес и наоборот.
2. Прямая зона DNS позволяет сопоставить DNS-имя. Обратная же зона DNS преобразовывает IP-адрес в имя.
3. В каталоге /etc/bind. Основной файл конфигурации - это /etc/bind/named.conf.

4. Содержит информацию, которая позволяет компьютеру преобразовывать буквенно-цифровые доменные имена в цифровые IP адреса.
5. А-запись — одна из самых важных записей. Именно эта запись указывает на IP-адрес сервера, который привязан к доменному имени.

MX-запись — указывает на сервер, который будет использован при отсылке доменной электронной почты.

NS-запись — указывает на DNS-сервер домена.

CNAME-запись — позволяет одному из поддоменов дублировать DNS-записи своего родителя.

6. Домен in-addr.arpa предназначен для определения имен по их IP-адресам.
7. Демон named отвечает на запросы об именах машин и их IP-адресах.
8. главный (master) — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых; ведомый (slave) — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.
9. Какие параметры отвечают за время обновления зоны?
10. Изменить права доступа.
11. PTR.
12. Утилитой host.
13. Утилитой systemctl.
14. Утилитой journalctl.
15. Дамп-файл.
16. Как посмотреть, какие файлы использует в своей работе тот или иной процесс?

) — это система принудительного контроля доступа, реализованная на уровне ядра. Каждый файл, процесс, каталог и порт имеют специальную метку безопасности, известную как контекст SELinux, который является именем, используемым для

19. ~~Утилита getsebool~~ ~~Утилита getsebool~~... ли процесс получить доступ к файлу, каталогу или порту.
20. Командой chown.
21. Переключатель вкл/выкл.
—a
23. setsebool.

Вывод

В результате выполнения лабораторной работы я приобрёл практические навыки по установке и конфигурированию DNS-сервера, усвоил принципы работы системы доменных имён.