

Отчёт по лабораторной работе 2

Настройка DNS-сервера

Сейдалиев Тагьетдин Ровшенович

Содержание

1	Цель работы	6
2	Выполнение	7
2.1	Установка DNS-сервера	7
2.2	Конфигурирование кэширующего DNS-сервера	8
2.3	Конфигурирование первичного DNS-сервера	14
2.4	Анализ работы DNS-сервера	18
3	Внесение изменений в настройки внутреннего окружения виртуальной машины	21
4	Заключение	23
5	Контрольные вопросы	24
5.1	1. Что такое DNS?	24
5.2	2. Каково назначение кэширующего DNS-сервера?	24
5.3	3. Чем отличается прямая DNS-зона от обратной?	24
5.4	4. Где располагаются настройки DNS-сервера и за что они отвечают?	25
5.5	5. Что указывается в файле resolv.conf?	25
5.6	6. Какие типы ресурсов существуют в DNS?	25
5.7	7. Для чего используется домен in-addr.arpa?	26
5.8	8. Для чего нужен демон named?	26
5.9	9. Основные функции master- и slave-серверов	26
5.10	10. Какие параметры отвечают за время обновления зоны?	27
5.11	11. Как защитить зону от скачивания?	27
5.12	12. Какая запись используется при создании почтовых серверов?	28
5.13	13. Как протестировать работу DNS-сервера?	28
5.14	14. Как запустить, перезапустить или остановить службу?	28
5.15	15. Как посмотреть отладочную информацию при запуске сервиса?	29
5.16	16. Где хранится отладочная информация и как её посмотреть?	29
5.17	17. Как посмотреть, какие файлы использует процесс?	29
5.18	18. Примеры работы с сетевыми настройками через nmcli	30
5.19	19. Что такое SELinux?	30
5.20	20. Что такое контекст SELinux?	30
5.21	21. Как восстановить контекст SELinux после изменений?	31
5.22	22. Как создать правила SELinux на основе логов?	31
5.23	23. Что такое булевый переключатель SELinux?	31

5.24	24. Как посмотреть список переключателей и их состояние?	31
5.25	25. Как изменить значение переключателя SELinux?	32

Список иллюстраций

2.1	Результат команды dig до настройки локального DNS	8
2.2	Начальная конфигурация named.conf	9
2.3	Содержимое named.ca	10
2.4	Содержимое локальных зон	11
2.5	Результат dig через 127.0.0.1	12
2.6	Настройка DNS через nmcli	13
2.7	Изменения в named.conf	13
2.8	Прослушивание порта 53 UDP	14
2.9	Фрагмент named.conf с подключением файла зоны	15
2.10	Содержимое файла trseidalev.net	16
2.11	Прямая зона trseidalev.net	17
2.12	Обратная зона 192.168.1	17
2.13	Настройка прав и SELinux	18
2.14	Результат dig ns.trseidalev.net	19
2.15	Проверка зон через host	20
3.1	Содержимое скрипта dns.sh	22

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Установка DNS-сервера

После установки пакетов `bind` и `bind-utils` была выполнена проверка DNS-разрешения с помощью утилиты `dig` по адресу `www.yandex.ru`.

В выводе отражается типичная структура DNS-ответа:

- `HEADER` содержит идентификатор запроса, результат выполнения (`NOERROR`) и параметры запроса.
- `QUESTION SECTION` включает доменное имя и тип записи (`A`).
- `ANSWER SECTION` содержит три найденных `A`-записи с IP-адресами сервера.
- `Query time` показывает задержку ответа.
- `SERVER` указывает DNS-сервер, обработавший запрос (`10.0.2.3`).
- `MSG SIZE` — размер полученного сообщения.

```

bind-32:9.18.33-4.el10_0.x86_64      bind-dnssec-utils-32:9.18.33-4.el10_0.x86_64

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26292
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                427     IN      A      5.255.255.77
www.yandex.ru.                427     IN      A      77.88.55.88
www.yandex.ru.                427     IN      A      77.88.44.55

;; Query time: 13 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Nov 19 18:24:51 MSK 2025
;; MSG SIZE rcvd: 90

[root@server.trseidaliev.net ~]# █

```

Рис. 2.1: Результат команды dig до настройки локального DNS

2.2 Конфигурирование кэширующего DNS-сервера

Файл /etc/resolv.conf

До настройки собственного DNS-сервера хост использовал внешний DNS:

- search trseidalev.net — домен поиска;
- nameserver 10.0.2.3 — основной DNS-сервер.

Файл /etc/named.conf содержит базовую конфигурацию кэширующего DNS-сервера:

- listen-on ограничивает прослушивание портов только адресом 127.0.0.1;
- allow-query задаёт разрешение обработке запросов только с localhost;
- указаны пути к служебным файлам статистики, дампов и корневых ключей.

```
[root@server.trseidaliev.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search trseidaliev.net
nameserver 10.0.2.3
[root@server.trseidaliev.net ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { localhost; };

    /*
     - 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.
    */
}
```

Рис. 2.2: Начальная конфигурация named.conf

Файл `/var/named/named.ca` содержит список корневых DNS-серверов. В нём представлены:

- NS-записи корневых серверов;
- А и AAAA-адреса этих серверов;
- метаданные: дата обновления и версия зоны.

```

[root@server.trseidaliev.net ~]# cat /var/named/named.ca
;
; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
;
; This file is made available by InterNIC
; under anonymous FTP as
;
;     file           /domain/named.cache
;     on server      FTP.INTERNIC.NET
;
; -OR-              RS.INTERNIC.NET
;
;
; last update:      December 20, 2023
; related version of root zone: 2023122001
;
;
; FORMERLY NS.INTERNIC.NET
;
;
;
;     3600000      NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A      198.41.0.4
A.ROOT-SERVERS.NET. 3600000      AAAA   2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
;
;     3600000      NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000      A      170.247.170.2
B.ROOT-SERVERS.NET. 3600000      AAAA   2801:1b8:10::b
;
; FORMERLY C.PSI.NET

```

Рис. 2.3: Содержимое named.ca

Файл /var/named/named.localhost описывает локальную зону hostname → адрес:

- SOA — основная запись зоны;
- NS — сервер имён;
- A и AAAA для адресов 127.0.0.1 и ::1.

Файл /var/named/named.loopback отвечает за зону обратного разрешения 127.0.0.0/8:

- SOA — запись зоны;
- NS — сервер имён;
- PTR localhost — обратное разрешение.

```

[root@server.trseidaliev.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.trseidaliev.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.trseidaliev.net ~]# █

```

Рис. 2.4: Содержимое локальных зон

После запуска службы named и её добавления в автозапуск был произведён запрос через локальный DNS-сервер по адресу 127.0.0.1.

Вывод показал корректное выполнение запроса и кэширование.

```

[root@server.trseidaliev.net ~]# dig @127.0.0.1 www.yandex.ru
;; communications error to 127.0.0.1#53: timed out

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49715
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: acebd56ac6f6e55c01000000691de20350b1171eb49893b5 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

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

;; Query time: 3082 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Nov 19 18:28:03 MSK 2025
;; MSG SIZE rcvd: 118

[root@server.trseidaliev.net ~]#

```

Рис. 2.5: Результат dig через 127.0.0.1

В настройках интерфейса eth0 были изменены параметры:

- удалён внешний DNS;
- включён ignore-auto-dns;
- установлен DNS 127.0.0.1.

После перезапуска NetworkManager содержимое /etc/resolv.conf обновилось, и в нём стал указан локальный DNS.

```

[root@server.trseidaliev.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

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

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

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, eth
tool, match, ipv4, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.trseidaliev.net ~]#
[root@server.trseidaliev.net ~]# systemctl restart NetworkManager
[root@server.trseidaliev.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search trseidaliev.net
nameserver 127.0.0.1
[root@server.trseidaliev.net ~]#

```

Рис. 2.6: Настройка DNS через nmcli

В файл /etc/named.conf внесены изменения:

- listen-on расширен до 127.0.0.1 и any, что позволяет слушать порт 53 на всех интерфейсах;
- allow-query дополнен подсетью 192.168.0.0/16, что позволяет обслуживать запросы всех хостов локальной сети.

```

named.conf
/etc

1 //
2 // named.conf
3 //
4 // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5 // server as a caching only nameserver (as a localhost DNS resolver only).
6 //
7 // See /usr/share/doc/bind*/sample/ for example named configuration files.
8 //
9
10 options {
11     listen-on port 53 { 127.0.0.1; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory      "/var/named";
14     dump-file       "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file   "/var/named/data/named.secrets";
18     recursing-file  "/var/named/data/named.recursing";
19     allow-query     { localhost; 192.168.0.0/16; };
20

```

Рис. 2.7: Изменения в named.conf

Для разрешения работы DNS-сервиса в firewall были добавлены соответствующие правила для порта 53 (UDP/TCP). Это обеспечивает доступность DNS-сервера для внутренней сети.

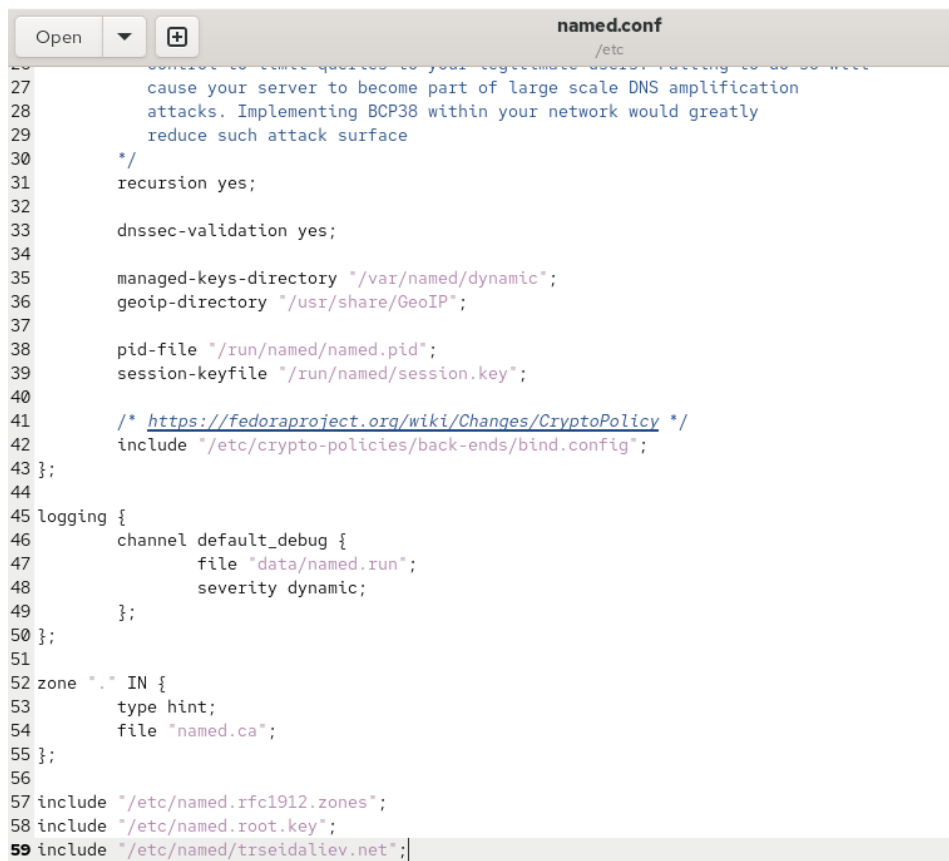
Команда `lsof` показала, что процесс `named` корректно прослушивает порт 53/udp, что подтверждает успешную настройку сервера.

```
[root@server.trseidalev.net ~]#
[root@server.trseidalev.net ~]# firewall-cmd --add-service=dns
success
[root@server.trseidalev.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.trseidalev.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
avahi-dae  881             avahi  12u  IPv4  9098      0t0  UDP *:mdns
avahi-dae  881             avahi  13u  IPv6  9099      0t0  UDP *:mdns
chronyd    12441             chrony  5u   IPv4  38624     0t0  UDP localhost:323
chronyd    12441             chrony  6u   IPv6  38625     0t0  UDP localhost:domain
named      15267             named  25u  IPv4  75500     0t0  UDP localhost:domain
named      15267             named  26u  IPv4  75501     0t0  UDP localhost:domain
named      15267             named  31u  IPv6  75504     0t0  UDP localhost:domain
named      15267             named  32u  IPv6  75505     0t0  UDP localhost:domain
named      15267 15268 isc-net-0    named  25u  IPv4  75500     0t0  UDP localhost:domain
named      15267 15268 isc-net-0    named  26u  IPv4  75501     0t0  UDP localhost:domain
named      15267 15268 isc-net-0    named  31u  IPv6  75504     0t0  UDP localhost:domain
```

Рис. 2.8: Прослушивание порта 53 UDP

2.3 Конфигурирование первичного DNS-сервера

После копирования шаблона `named.rfc1912.zones` в каталог `/etc/named` файл был переименован в `trseidalev.net`. Затем он был подключён в основном конфигурационном файле DNS-сервера посредством строки `include`.

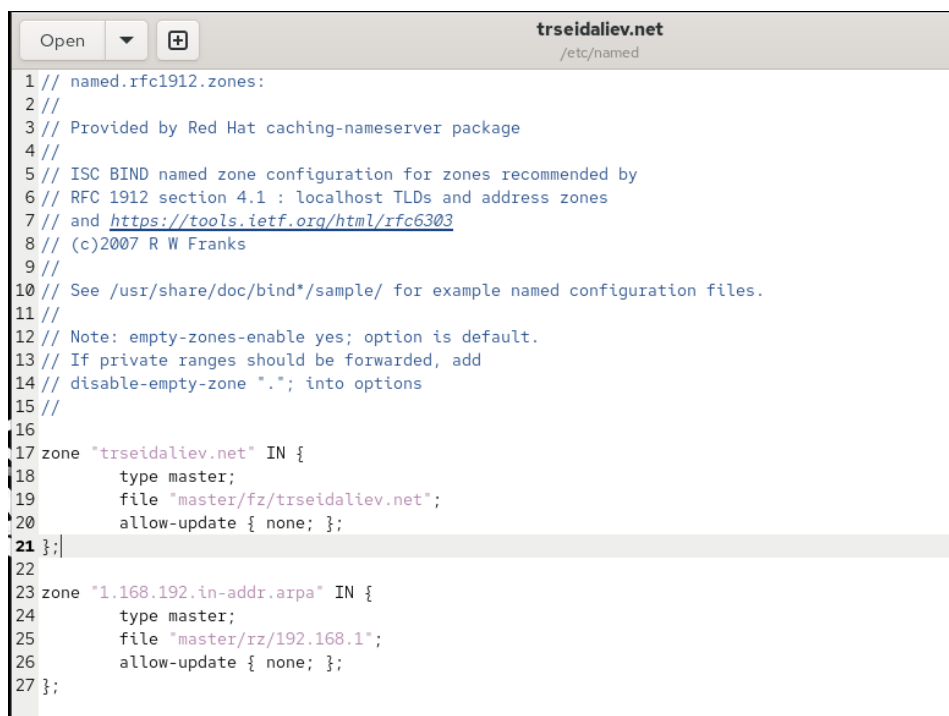


```
27      cause your server to become part of large scale DNS amplification
28      attacks. Implementing BCP38 within your network would greatly
29      reduce such attack surface
30      */
31      recursion yes;
32
33      dnssec-validation yes;
34
35      managed-keys-directory "/var/named/dynamic";
36      geoip-directory "/usr/share/GeoIP";
37
38      pid-file "/run/named/named.pid";
39      session-keyfile "/run/named/session.key";
40
41      /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
42      include "/etc/crypto-policies/back-ends/bind.config";
43 };
44
45 logging {
46     channel default_debug {
47         file "data/named.run";
48         severity dynamic;
49     };
50 };
51
52 zone "." IN {
53     type hint;
54     file "named.ca";
55 };
56
57 include "/etc/named.rfc1912.zones";
58 include "/etc/named.root.key";
59 include "/etc/named/trseidalev.net";
```

Рис. 2.9: Фрагмент named.conf с подключением файла зоны

В файле `/etc/named/trseidalev.net` были удалены все лишние записи и добавлены две зоны:

- прямая зона `trseidalev.net`;
- обратная зона `1.168.192.in-addr.arpa`.



```
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ for example named configuration files.
11 //
12 // Note: empty-zones-enable yes; option is default.
13 // If private ranges should be forwarded, add
14 // disable-empty-zone "."; into options
15 //
16
17 zone "trseidalev.net" IN {
18     type master;
19     file "master/fz/trseidalev.net";
20     allow-update { none; };
21 };
22
23 zone "1.168.192.in-addr.arpa" IN {
24     type master;
25     file "master/rz/192.168.1";
26     allow-update { none; };
27 };
```

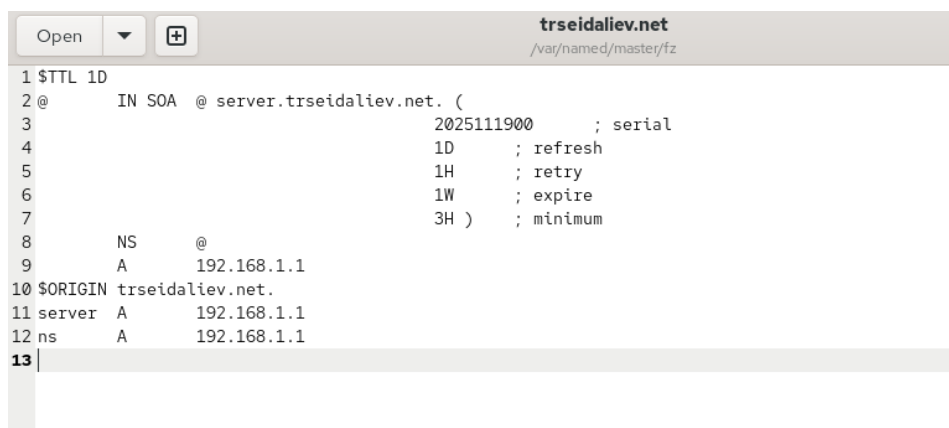
Рис. 2.10: Содержимое файла trseidalev.net

В каталоге /var/named созданы подкаталоги:

- master/fz для прямой зоны;
- master/rz для обратной зоны.

Далее в подкаталог master/fz был перенесён шаблон прямой зоны и переименован в trseidalev.net. Файл был изменён согласно требованиям: корректно прописаны SOA-запись, адрес узла, имя домена и А-записи для серверов.

Итоговое содержимое файла прямой зоны:



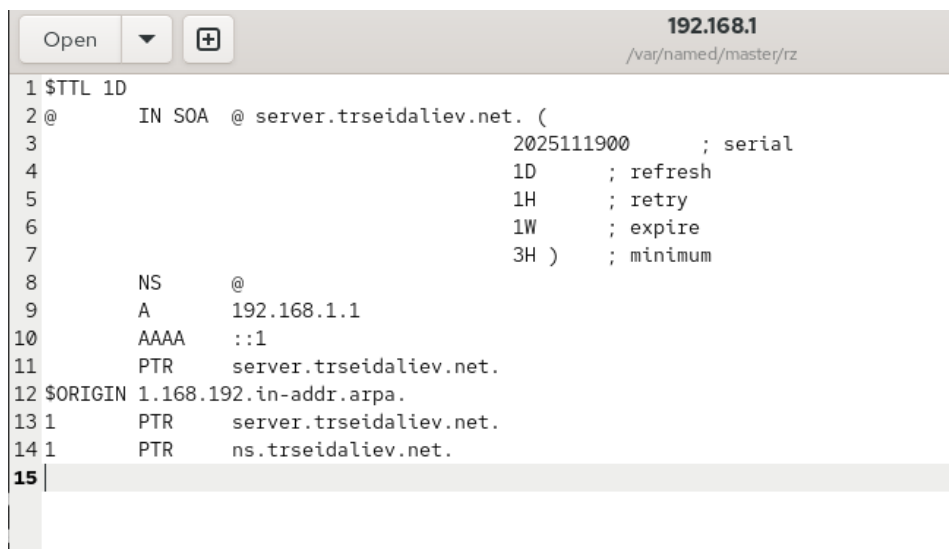
```
trseidalev.net
/var/named/master/fz

1 $TTL 1D
2 @      IN SOA  @ server.trseidalev.net. (
3                               2025111900      ; serial
4                               1D              ; refresh
5                               1H              ; retry
6                               1W              ; expire
7                               3H )            ; minimum
8      NS      @
9      A      192.168.1.1
10 $ORIGIN trseidalev.net.
11 server A    192.168.1.1
12 ns    A    192.168.1.1
13
```

Рис. 2.11: Прямая зона trseidalev.net

Шаблон обратной зоны named.loopback был перенесён в каталог master/rz и переименован в 192.168.1. После редактирования в файле были указаны необходимые PTR-записи.

Итоговый вариант файла обратной зоны:



```
192.168.1
/var/named/master/rz

1 $TTL 1D
2 @      IN SOA  @ server.trseidalev.net. (
3                               2025111900      ; serial
4                               1D              ; refresh
5                               1H              ; retry
6                               1W              ; expire
7                               3H )            ; minimum
8      NS      @
9      A      192.168.1.1
10     AAAA    ::1
11     PTR     server.trseidalev.net.
12 $ORIGIN 1.168.192.in-addr.arpa.
13 1      PTR  server.trseidalev.net.
14 1      PTR  ns.trseidalev.net.
15
```

Рис. 2.12: Обратная зона 192.168.1

Для корректной работы демона named права каталогов /etc/named и /var/named были изменены. После этого были восстановлены контексты SELinux, а также проверены переключатели для службы.

В выводе видно:

- параметр `named_write_master_zones` включён, что обеспечивает возможность записи в мастер-зоны;
- контексты SELinux восстановлены.

```
[root@server.trseidalev.net rz]#
[root@server.trseidalev.net rz]# chown -R named:named /etc/named
[root@server.trseidalev.net rz]# chown -R named:named /var/named
[root@server.trseidalev.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20251119.071804.0005 from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:NetworkManager_etc_rw_t:s0
Relabeled /etc/named.conf from unconfined_u:object_r:etc_t:s0 to unconfined_u:object_r:named_conf_t:s0
[root@server.trseidalev.net rz]# restorecon -vR /var/named/
[root@server.trseidalev.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.trseidalev.net rz]# systemctl restart named
[root@server.trseidalev.net rz]# █
```

Рис. 2.13: Настройка прав и SELinux

В отдельной консоли был запущен просмотр системного журнала в реальном времени. После перезапуска службы `named` в логах не появилось ошибок, что подтверждает корректность конфигурации прямой и обратной зон.

DNS-сервер успешно обработал файлы зон и начал обслуживать запросы.

2.4 Анализ работы DNS-сервера

Для проверки прямой зоны был выполнен запрос к адресу `ns.trseidalev.net` через локальный DNS-сервер.

Ответ содержит одну А-запись, корректно указывающую на адрес `192.168.1.1`. Это подтверждает правильность настройки файла прямой зоны.

```

[root@server.trseidalev.net rz]# dig ns.trseidalev.net

; <<>> DiG 9.18.33 <<>> ns.trseidalev.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26650
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b8e7b41eaf90d9f801000000691de62574b52c85dba228e9 (good)
;; QUESTION SECTION:
ns.trseidalev.net.          IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Nov 19 18:45:41 MSK 2025
;; MSG SIZE rcvd: 91

[root@server.trseidalev.net rz]#

```

Рис. 2.14: Результат dig ns.trseidalev.net

Команда `host -l trseidalev.net`

Эта команда выполняет перечисление всех DNS-записей в зоне.

Вывод показывает:

- А-записи `server.trseidalev.net` и `ns.trseidalev.net`;
- корректное разрешение доменных имён.

Команда `host -a trseidalev.net`

Запрос полного описания зоны (ANY) показывает:

- SOA-запись с корректными параметрами;
- NS-запись, указывающую на основной DNS-сервер;
- А-запись зоны, совпадающую с адресом сервера.

Команда `host -t A trseidalev.net`

Домен корректно разрешается в адрес `192.168.1.1`.

Команда `host -t PTR 192.168.1.1`

Обратная зона настроена корректно — IP-адрес 192.168.1.1 соответствует именам server.trseidalev.net и ns.trseidalev.net.

```
[root@server.trseidalev.net rz]# host -l trseidalev.net
trseidalev.net name server trseidalev.net.
trseidalev.net has address 192.168.1.1
ns.trseidalev.net has address 192.168.1.1
server.trseidalev.net has address 192.168.1.1
[root@server.trseidalev.net rz]# host -a trseidalev.net
Trying "trseidalev.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45820
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
trseidalev.net.          86400  IN      SOA      trseidalev.net. server.trseidalev.net. 2025111900 86400 3600 604800
10800
trseidalev.net.          86400  IN      NS       trseidalev.net.
trseidalev.net.          86400  IN      A        192.168.1.1

Received 106 bytes from 127.0.0.1#53 in 0 ms
[root@server.trseidalev.net rz]# host -t A trseidalev.net
trseidalev.net has address 192.168.1.1
[root@server.trseidalev.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.trseidalev.net.
1.1.168.192.in-addr.arpa domain name pointer server.trseidalev.net.
[root@server.trseidalev.net rz]#
```

Рис. 2.15: Проверка зон через host

3 Внесение изменений в настройки внутреннего окружения виртуальной машины

В каталоге `/vagrant/provision/server` был создан подкаталог `dns` с необходимой структурой для хранения конфигурации DNS-сервера. В него были скопированы:

- файл `named.conf`;
- содержимое каталога `/etc/named`;
- мастер-зоны из `/var/named/master/`.

Это позволяет автоматически разворачивать DNS-конфигурацию при создании виртуальной машины.

В каталоге `/vagrant/provision/server` был создан исполняемый файл `dns.sh`

Скрипт полностью автоматизирует подготовку DNS-сервера.

```

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

```

Рис. 3.1: Содержимое скрипта dns.sh

4 Заключение

В ходе выполнения работы:

- установлен и настроен кэширующий DNS-сервер на базе BIND;
- проанализированы файлы конфигурации резолвера и сервера DNS, включая прямые и обратные зоны;
- выполнена настройка локального DNS-сервера как основного для хоста и внутренней сети;
- добавлены необходимые правила в межсетевой экран и проверена работа сервиса через анализ прослушиваемых портов;
- создана и сконфигурирована прямая зона `trseidalev.net` и обратная зона `1.168.192.in-addr.arpa`;
- проверена корректность работы DNS-записей с помощью утилит `dig` и `host`;
- выполнена автоматизация конфигурации DNS-сервера с сохранением всех нужных файлов в каталог `/vagrant/provision/server/dns` и созданием скрипта `dns.sh`;
- подтверждена корректная работа DNS после перезапуска службы и анализа системного журнала.

5 Контрольные вопросы

5.1 1. Что такое DNS?

DNS — распределённая система, преобразующая доменные имена в IP-адреса и обратно.

Она обеспечивает удобный доступ к ресурсам сети, позволяя использовать имена вместо числовых адресов.

5.2 2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер сохраняет результаты ранее выполненных запросов. Это ускоряет последующие обращения, снижает нагрузку на внешние DNS-серверы и уменьшает сетевой трафик.

5.3 3. Чем отличается прямая DNS-зона от обратной?

Прямая зона сопоставляет доменные имена IP-адресам (A/AAAA-записи). Обратная зона выполняет обратное преобразование — связывает IP-адреса с доменными именами (PTR-записи).

5.4 4. Где располагаются настройки DNS-сервера и за что они отвечают?

Основные файлы:

- `/etc/named.conf` — базовая конфигурация службы `named`.
- `/etc/named/*` — описания подключаемых зон и дополнительных параметров.
- `/var/named/` — каталоги и файлы мастер- и slave-зон.
- `/var/named/master/*` — файлы прямых и обратных зон, содержащие записи DNS.

5.5 5. Что указывается в файле `resolv.conf`?

В нём задаются параметры резолвера клиента:
список DNS-серверов (`nameserver`), домен поиска (`search`) и дополнительные настройки.

5.6 6. Какие типы ресурсов существуют в DNS?

Основные записи:

- **A** — IPv4-адрес.
- **AAAA** — IPv6-адрес.

- **NS** — серверы имён зоны.
- **SOA** — начало зоны и параметры обновления.
- **PTR** — обратное разрешение IP-адресов.
- **MX** — почтовые серверы домена.
- **CNAME** — каноническое имя (псевдоним).
- **TXT** — произвольные текстовые данные.
- **SRV** — службы и их порты.

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

Для обратного DNS-разрешения IPv4-адресов — сопоставляет IP-адрес доменному имени через PTR-записи.

5.8 8. Для чего нужен демон named?

named — основной процесс BIND, выполняющий роль DNS-сервера: обрабатывает запросы, обслуживает зоны, ведёт кэш и взаимодействует с другими серверами имен.

5.9 9. Основные функции master- и slave-серверов

- **Master** хранит оригинальные файлы зон и предоставляет их для обновления slave-серверов.

- **Slave** получает зоны с master и обеспечивает отказоустойчивое обслуживание запросов.

5.10 10. Какие параметры отвечают за время обновления зоны?

В секции SOA:

- **serial** — версия зоны.
- **refresh** — период проверки изменений slave-сервером.
- **retry** — интервал повторных попыток при ошибках.
- **expire** — срок устаревания зоны.
- **minimum** — минимальный TTL для кэша.

5.11 11. Как защитить зону от скачивания?

Использовать в `named.conf` ограничения:

- ограничение transfer-запросов параметром `allow-transfer {};`
- запрет AXFR-запросов;
- использование TSIG-ключей.

5.12 12. Какая запись используется при создании почтовых серверов?

Для SMTP применяется запись **MX**.

5.13 13. Как протестировать работу DNS-сервера?

Через утилиты:

- `dig` — подробный анализ запросов;
- `host` — быстрые проверки;
- `nslookup` — диагностика DNS.

5.14 14. Как запустить, перезапустить или остановить службу?

Через `systemd`:

- `systemctl start` — запуск;
- `systemctl restart` — перезапуск;
- `systemctl stop` — остановка;
- `systemctl status` — просмотр состояния.

5.15 15. Как посмотреть отладочную информацию при запуске сервиса?

Использовать:

- `systemctl status <service>;`
- `journalctl -xe` — подробная ошибка;
- `journalctl -u <service>` — логи конкретного сервиса.

5.16 16. Где хранится отладочная информация и как её посмотреть?

Основной журнал — в systemd-логах.

Просмотр:

- `journalctl;`
- `journalctl -f` — в реальном времени;
- `journalctl -u <service>` — для конкретной службы.

5.17 17. Как посмотреть, какие файлы использует процесс?

Команды:

- `lsuf -p <PID>` — список открытых файлов;

- `lsof | grep <service>` — все файлы, связанные с сервисом;
- `ls -l /proc/<PID>/fd` — открытые файловые дескрипторы.

5.18 18. Примеры работы с сетевыми настройками через nmcli

- просмотр соединений: `nmcli connection show`;
- изменение DNS: `nmcli connection modify eth0 ipv4.dns 8.8.8.8`;
- включение/выключение интерфейса: `nmcli device connect eth0`, `nmcli device disconnect eth0`;
- изменение режима авто-DNS: `nmcli connection modify eth0 ipv4.ignore-auto-dns yes`.

5.19 19. Что такое SELinux?

SELinux — механизм контроля доступа на уровне ядра, который использует политики безопасности для ограничения действий процессов.

5.20 20. Что такое контекст SELinux?

Контекст (метка) — набор атрибутов SELinux, определяющих права объекта: тип, роль, пользователь, домен процесса.

5.21 21. Как восстановить контекст SELinux после изменений?

С помощью команды:

- `restorecon -vR <каталог>`.

5.22 22. Как создать правила SELinux на основе логов?

Использовать утилиты:

- `audit2allow` — создание разрешающего правила по сообщениям аудита;
- `audit2why` — анализ причин блокировки.

5.23 23. Что такое булевый переключатель SELinux?

Переключатель (boolean) — параметр политики SELinux, позволяющий включить или отключить определённое поведение без изменения всей политики.

5.24 24. Как посмотреть список переключателей и их состояние?

Команда:

- `getsebool -a`.

5.25 25. Как изменить значение переключателя SELinux?

ИСПОЛЬЗОВАТЬ:

- `setsebool boolean_name on/off;`
- `setsebool -P boolean_name on/off` — сохранить навсегда.