

# **Отчёт по лабораторной работе 2**

**Настройка DNS-сервера**

Элсаиед Адел

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение</b>	<b>6</b>
2.1	Установка и конфигурирование кэширующего DNS-сервера (BIND)	6
<b>3</b>	<b>Выполнение</b>	<b>15</b>
3.1	Конфигурирование первичного DNS-сервера . . . . .	15
3.2	Анализ работы DNS-сервера . . . . .	20
3.3	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	21
<b>4</b>	<b>Вывод</b>	<b>24</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>25</b>

# Список иллюстраций

2.1	Установка пакетов bind и bind-utils . . . . .	7
2.2	DNS-запрос dig www.yandex.ru . . . . .	8
2.3	Файлы resolv.conf и named.conf . . . . .	9
2.4	Файл named.ca . . . . .	10
2.5	Файлы named.localhost и named.loopback . . . . .	11
2.6	DNS-запрос через локальный сервер . . . . .	12
2.7	Настройка DNS через NetworkManager . . . . .	12
2.8	Изменение конфигурации named.conf . . . . .	13
2.9	Проверка работы DNS-сервера через lsof . . . . .	14
3.1	Подключение файла зон в named.conf . . . . .	16
3.2	Описание прямой и обратной зон . . . . .	17
3.3	Файл прямой зоны elsaiedadel.net . . . . .	18
3.4	Файл обратной зоны 192.168.1 . . . . .	19
3.5	Настройка SELinux для named . . . . .	19
3.6	Проверка A-записи ns.elsaiedadel.net . . . . .	20
3.7	Проверка DNS-зоны утилитой host . . . . .	21
3.8	Подготовка каталогов и копирование конфигурации . . . . .	22
3.9	Скрипт автоматической настройки DNS-сервера . . . . .	23

## **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 и конфигурирование кэширующего DNS-сервера (BIND)

1. После загрузки операционной системы выполнен переход в рабочий каталог проекта с виртуальными машинами. Далее была запущена виртуальная машина **server**. После завершения загрузки системы выполнен вход под ранее созданным пользователем и осуществлён переход в режим суперпользователя.
2. На виртуальной машине `server` произведена установка пакетов `bind` и `bind-utils` с использованием менеджера пакетов `DNF`. В процессе установки система автоматически разрешила зависимости и успешно установила необходимые компоненты DNS-сервера BIND и вспомогательные утилиты.

```
[sudo] password for elsaiedadel:
[root@server.elsaiedadel.net ~]# dnf -y install bind bind-utils
Last metadata expiration check: 0:08:47 ago on Fri 02 Jan 2026 08:58:24 AM UTC.
Package bind-utils-32:9.18.33-10.el10_1.2.x86_64 is already installed.
Dependencies resolved.
=====
Package                        Architecture      Version           Repository        Size
=====
Installing:
  bind                        x86_64            32:9.18.33-10.el10_1.2    appstream         333 k
Installing weak dependencies:
  bind-dnssec-utils          x86_64            32:9.18.33-10.el10_1.2    appstream         151 k
=====
Transaction Summary
=====
Install 2 Packages

Total download size: 483 k
Installed size: 1.3 M
Downloading Packages:
(1/2): bind-dnssec-utils-9.18.33-10.el10_1.2.x86_64.rpm        1.9 MB/s | 151 kB    00:00
(2/2): bind-9.18.33-10.el10_1.2.x86_64.rpm                    2.6 MB/s | 333 kB    00:00
-----
Total                                                           923 kB/s | 483 kB    00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                                    1/1
  Installing     : bind-dnssec-utils-32:9.18.33-10.el10_1.2.x86_64    1/2
  Running scriptlet: bind-32:9.18.33-10.el10_1.2.x86_64              2/2
  Installing     : bind-32:9.18.33-10.el10_1.2.x86_64              2/2
  Running scriptlet: bind-32:9.18.33-10.el10_1.2.x86_64              2/2
```

Рис. 2.1: Установка пакетов bind и bind-utils

3. В качестве проверки работоспособности DNS-разрешения имён выполнен запрос к доменному имени `www.yandex.ru` с использованием утилиты `dig`. В результате был получен корректный DNS-ответ со статусом `NOERROR`, содержащий несколько А-записей с IP-адресами серверов Яндекса.

В выводе команды:

- строка `HEADER` указывает на успешную обработку DNS-запроса;
- `opcode QUERY` означает стандартный запрос на разрешение имени;
- статус `NOERROR` свидетельствует об отсутствии ошибок;
- флаги `rd` и `ra` показывают, что была запрошена и выполнена рекурсия;
- секция `QUESTION SECTION` содержит исходный DNS-запрос;
- секция `ANSWER SECTION` содержит IP-адреса, соответствующие доменному имени;
- строка `SERVER` указывает DNS-сервер, использованный для обработки запроса;
- параметр `Query time` отражает время выполнения запроса.

```

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14492
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                56      IN      A      5.255.255.77
www.yandex.ru.                56      IN      A      77.88.44.55
www.yandex.ru.                56      IN      A      77.88.55.88

;; Query time: 28 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Fri Jan 02 09:07:40 UTC 2026
;; MSG SIZE rcvd: 90

[root@server.elsaiedadel.net ~]#

```

Рис. 2.2: DNS-запрос dig www.yandex.ru

4. Выполнен анализ файла /etc/resolv.conf. Данный файл автоматически сгенерирован NetworkManager и содержит домен поиска elsaiedadel.net, а также IP-адрес DNS-сервера, используемого системой по умолчанию.

Также проанализирован файл /etc/named.conf, содержащий основную конфигурацию DNS-сервера BIND. В конфигурации определены параметры прослушивания порта 53 на локальном интерфейсе, рабочий каталог сервера, файлы статистики и ограничения на обработку DNS-запросов только от localhost.

```

[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search elsaiedadel.net
nameserver 10.0.2.3
[root@server.elsaiedadel.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.
    - 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.
    */
}

```

Рис. 2.3: Файлы resolv.conf и named.conf

5. Проанализирован файл /var/named/named.ca, содержащий информацию о корневых DNS-серверах Интернета. Данный файл используется для начальной инициализации кэша DNS-сервера и включает список корневых серверов зоны, их имена и IPv4/IPv6-адреса.

```

[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.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
;
.                3600000      NS      C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000      A      192.33.4.12
C.ROOT-SERVERS.NET. 3600000      AAAA   2001:500:2::c

```

Рис. 2.4: Файл named.ca

#### 6. Проанализированы файлы /var/named/named.localhost и /var/named/named.loopback.

В них описана локальная зона localhost, определены записи SOA, NS, а также A и AAAA-записи для адресов 127.0.0.1 и ::1, обеспечивающие корректную работу локального DNS-разрешения.

```

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

```

Рис. 2.5: Файлы named.localhost и named.loopback

7. Выполнен DNS-запрос с явным указанием локального DNS-сервера по адресу 127.0.0.1. В результате получен ответ со статусом SERVFAIL, что указывает на отсутствие корректной обработки рекурсивных запросов локальным DNS-сервером на данном этапе.

Отличие данного запроса от запроса без указания сервера заключается в том, что в этом случае запрос обрабатывается непосредственно локальным DNS-сервером, а не внешним DNS-сервером, полученным по DHCP.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 11124
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: b322f7f10df2b23c0100000069578c16b29105ec077c44b1 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; Query time: 4058 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Jan 02 09:12:54 UTC 2026
;; MSG SIZE rcvd: 70

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

Рис. 2.6: DNS-запрос через локальный сервер

8. Для назначения DNS-сервера сервером по умолчанию выполнена настройка сетевого соединения eth0 с использованием NetworkManager. Были удалены автоматически полученные DNS-адреса, отключено их автоматическое применение и явно задан DNS-сервер 127.0.0.1. После перезапуска NetworkManager изменения были подтверждены в файле /etc/resolv.conf.

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

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

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

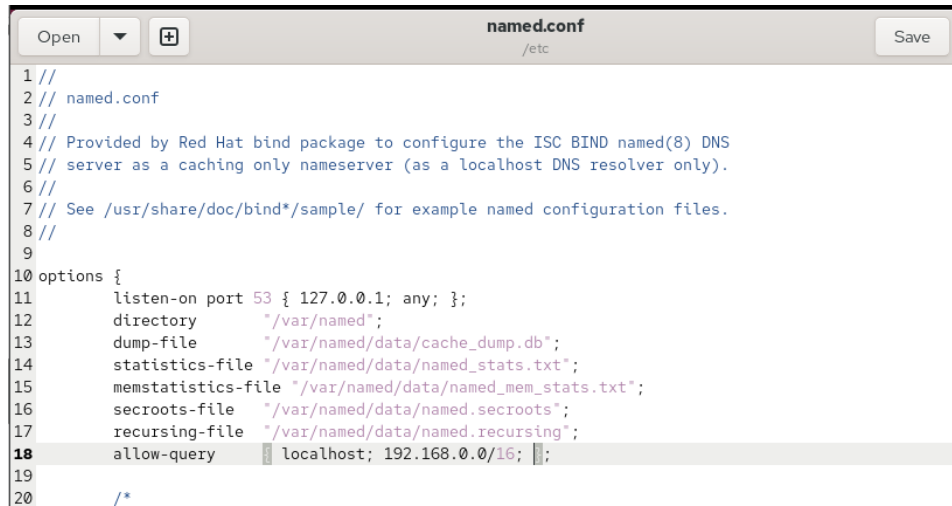
Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4, ipv6, prefix-delegation, 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.elsaiedadel.net ~]# systemctl restart NetworkManager
[root@server.elsaiedadel.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search elsaiedadel.net
nameserver 127.0.0.1
[root@server.elsaiedadel.net ~]#
```

Рис. 2.7: Настройка DNS через NetworkManager

9. Для обеспечения обработки DNS-запросов от всех узлов внутренней сети

выполнено редактирование файла `/etc/named.conf`. Параметр прослушивания был изменён для работы на всех сетевых интерфейсах, а директива `allow-query` дополнена разрешением запросов от подсети `192.168.0.0/16`.



```
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     directory      "/var/named";
13     dump-file      "/var/named/data/cache_dump.db";
14     statistics-file "/var/named/data/named_stats.txt";
15     memstatistics-file "/var/named/data/named_mem_stats.txt";
16     secroots-file  "/var/named/data/named.secroots";
17     recursing-file  "/var/named/data/named.recursing";
18     allow-query     localhost; 192.168.0.0/16;
19
20 /*
```

Рис. 2.8: Изменение конфигурации `named.conf`

10. В настройках межсетевого экрана сервера разрешена служба DNS. Изменения применены как для текущей сессии, так и на постоянной основе.
11. Для подтверждения корректной работы DNS-сервера выполнена проверка прослушивания UDP-порта 53. В выводе команды зафиксировано, что процесс `named` активно использует порт 53, что подтверждает прохождение DNS-запросов через узел `server` и корректную работу кэширующего DNS-сервера.

```

[1000@server.elsaiedadel.net ~]$
[1000@server.elsaiedadel.net ~]$ firewall-cmd --add-service=dns
success
[1000@server.elsaiedadel.net ~]$ firewall-cmd --add-service=dns --permanent
success
[1000@server.elsaiedadel.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-daemon 1090          avahi  12u      IPv4        8944      0t0      UDP *:mdns
avahi-daemon 1090          avahi  13u      IPv6        8945      0t0      UDP *:mdns
chronyd       1159          chrony  5u       IPv4       10196     0t0      UDP localhost:323
chronyd       1159          chrony  6u       IPv6       10197     0t0      UDP localhost:323
named         14085         named  25u      IPv4       54250     0t0      UDP localhost:domain
named         14085         named  26u      IPv4       54251     0t0      UDP localhost:domain
named         14085         named  31u      IPv6       54254     0t0      UDP localhost:domain
named         14085         named  32u      IPv6       54255     0t0      UDP localhost:domain
named         14085 14086 isc-net-0  named  25u      IPv4       54250     0t0      UDP localhost:domain
named         14085 14086 isc-net-0  named  26u      IPv4       54251     0t0      UDP localhost:domain
named         14085 14086 isc-net-0  named  31u      IPv6       54254     0t0      UDP localhost:domain
named         14085 14086 isc-net-0  named  32u      IPv6       54255     0t0      UDP localhost:domain
named         14085 14087 isc-net-0  named  25u      IPv4       54250     0t0      UDP localhost:domain
named         14085 14087 isc-net-0  named  26u      IPv4       54251     0t0      UDP localhost:domain
named         14085 14087 isc-net-0  named  31u      IPv6       54254     0t0      UDP localhost:domain
named         14085 14087 isc-net-0  named  32u      IPv6       54255     0t0      UDP localhost:domain
named         14085 14088 isc-net-0  named  25u      IPv4       54250     0t0      UDP localhost:domain
named         14085 14088 isc-net-0  named  26u      IPv4       54251     0t0      UDP localhost:domain
named         14085 14088 isc-net-0  named  31u      IPv6       54254     0t0      UDP localhost:domain
named         14085 14088 isc-net-0  named  32u      IPv6       54255     0t0      UDP localhost:domain
named         14085 14089 isc-net-0  named  25u      IPv4       54250     0t0      UDP localhost:domain
named         14085 14089 isc-net-0  named  26u      IPv4       54251     0t0      UDP localhost:domain

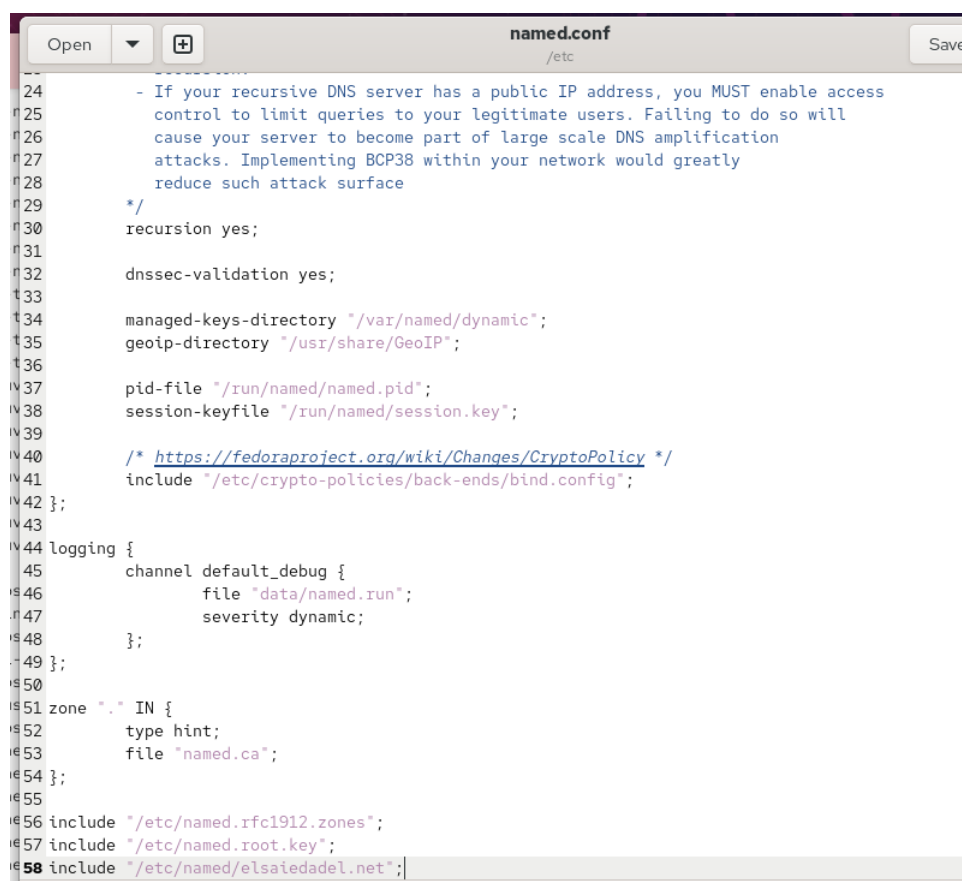
```

Рис. 2.9: Проверка работы DNS-сервера через lsof

## 3 Выполнение

### 3.1 Конфигурирование первичного DNS-сервера

1. Для конфигурирования первичного DNS-сервера выполнено копирование шаблона описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` с последующим переименованием файла в `elsaiedadel.net`. Данный файл предназначен для описания прямой и обратной DNS-зон пользователя.
2. Файл описания зон `elsaiedadel.net` был подключён в основной конфигурационный файл DNS-сервера `/etc/named.conf` путём добавления директивы `include` в конце файла. Это позволило DNS-серверу учитывать пользовательские зоны при запуске.

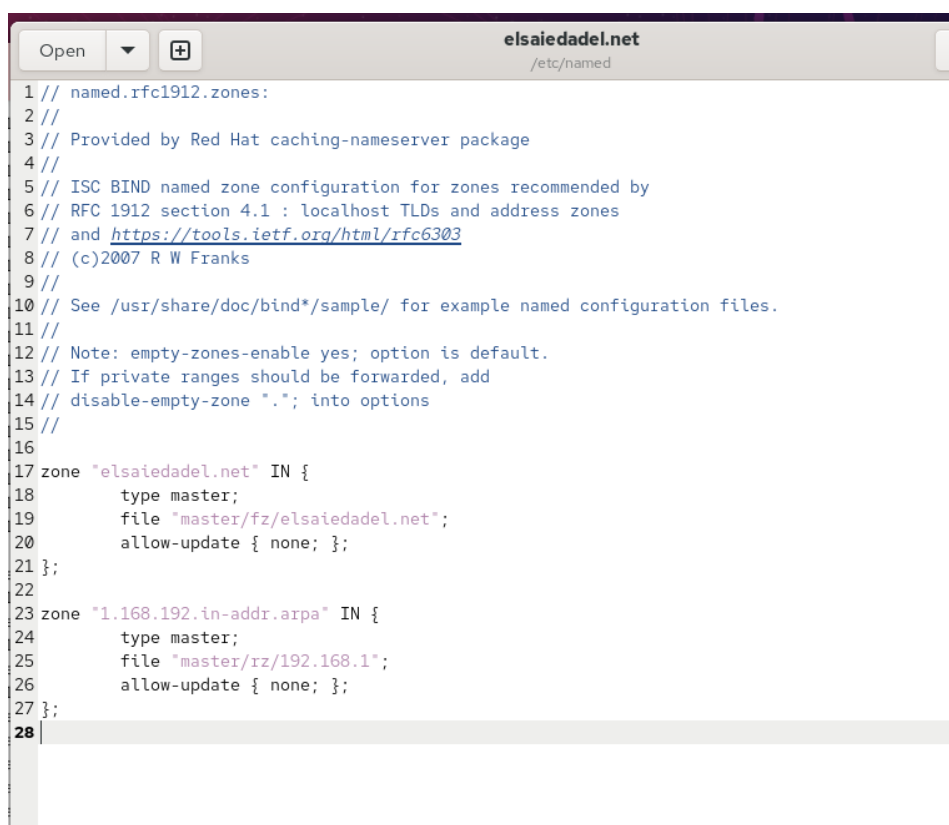


```
24 - If your recursive DNS server has a public IP address, you MUST enable access
25 control to limit queries to your legitimate users. Failing to do so will
26 cause your server to become part of large scale DNS amplification
27 attacks. Implementing BCP38 within your network would greatly
28 reduce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

Рис. 3.1: Подключение файла зон в named.conf

3. В файле /etc/named/elsaiedadel.net выполнено редактирование шаблоновых зон. Вместо стандартной зоны localhost.localdomain была описана прямая зона elsaiedadel.net с типом master и указанием файла зоны master/fz/elsaiedadel.net.

Аналогично вместо зоны обратной петли 127.0.0.1 была определена обратная зона 1.168.192.in-addr.arpa с файлом зоны master/rz/192.168.1. Все прочие записи из файла были удалены.

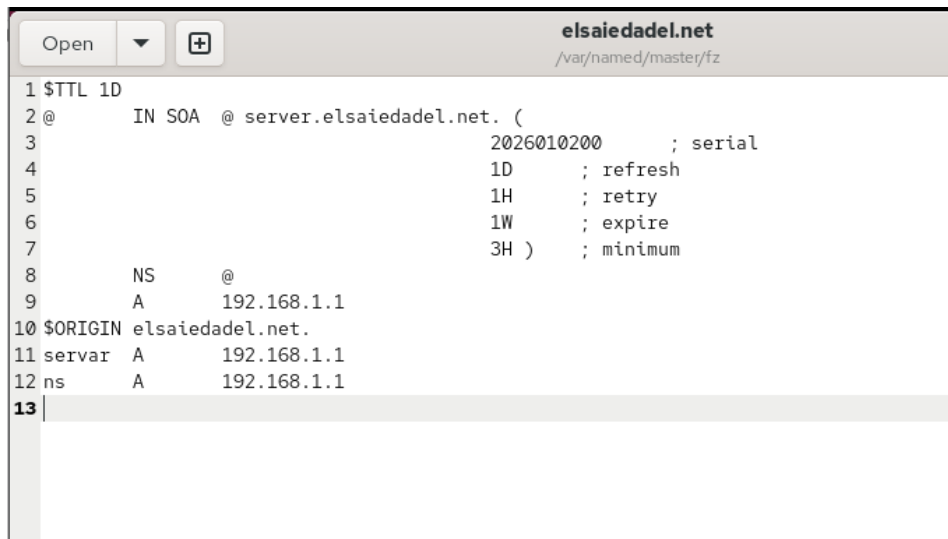


```
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /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 "elsaiedadel.net" IN {
18     type master;
19     file "master/fz/elsaiedadel.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 };
28
```

Рис. 3.2: Описание прямой и обратной зон

4. В каталоге /var/named были созданы подкаталоги master/fz и master/rz, предназначенные для хранения файлов прямой и обратной DNS-зон соответственно. Данная структура соответствует рекомендуемой иерархии BIND для мастер-зон.
5. Шаблон файла прямой зоны named.localhost был скопирован в каталог /var/named/master/fz и переименован в elsaiedadel.net. После этого файл был отредактирован с учётом параметров пользовательского домена.
6. В файле /var/named/master/fz/elsaiedadel.net были внесены следующие изменения:
  - DNS-имя сервера в записи SOA изменено на server.elsaiedadel.net;
  - серийный номер зоны задан в формате ГТГТММДДВВ;
  - А-запись изменена с адреса 127.0.0.1 на 192.168.1.1;

- директива \$ORIGIN установлена в значение elsaiedadel.net.;
- добавлены A-записи для узлов server и ns с адресом 192.168.1.1.



```

1 $TTL 1D
2 @      IN SOA  @ server.elsaiedadel.net. (
3                                     2026010200      ; serial
4                                     1D              ; refresh
5                                     1H              ; retry
6                                     1W              ; expire
7                                     3H              ; minimum
8      NS      @
9      A      192.168.1.1
10 $ORIGIN elsaiedadel.net.
11 server A    192.168.1.1
12 ns     A    192.168.1.1
13

```

Рис. 3.3: Файл прямой зоны elsaiedadel.net

7. Шаблон файла обратной зоны named.loopback был скопирован в каталог /var/named/master/rz и переименован в 192.168.1. Далее файл был отредактирован для описания обратного разрешения адресов.
8. В файле /var/named/master/rz/192.168.1 были выполнены следующие изменения:
  - DNS-имя сервера в записи SOA изменено на server.elsaiedadel.net;
  - серийный номер зоны приведён к требуемому формату;
  - адрес в A-записи изменён на 192.168.1.1;
  - директива \$ORIGIN установлена в значение 1.168.192.in-addr.arpa.;
  - добавлены PTR-записи, сопоставляющие IP-адрес 192.168.1.1 с именами server.elsaiedadel.net и ns.elsaiedadel.net.

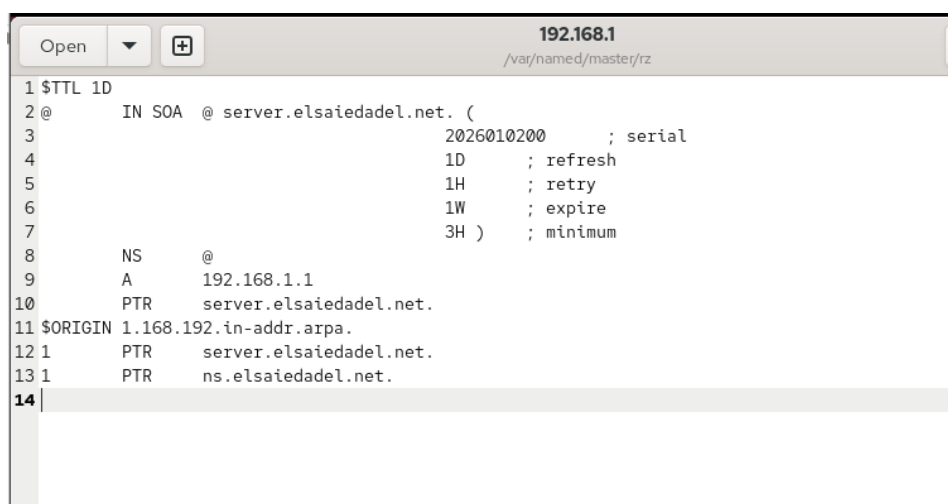


Рис. 3.4: Файл обратной зоны 192.168.1

9. Для обеспечения корректного доступа DNS-сервера к конфигурационным файлам и файлам зон были изменены права собственности каталогов /etc/named и /var/named. Владелльцем файлов назначен пользователь и группа named.
10. После изменения конфигурационных файлов выполнено восстановление контекстов безопасности SELinux для каталогов /etc и /var/named. Также проверено состояние SELinux-переключателей, относящихся к службе named. Демону named было разрешено выполнять запись в файлы мастер-зон.

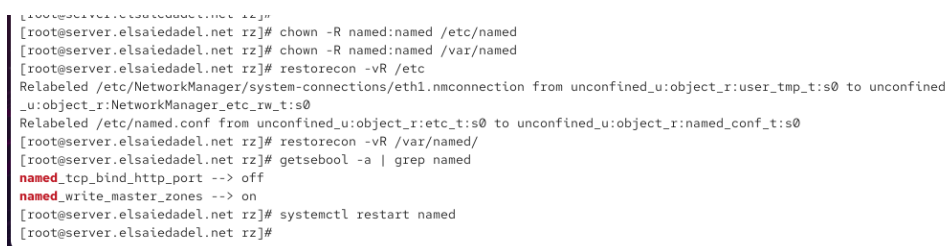


Рис. 3.5: Настройка SELinux для named

11. Для контроля корректности работы DNS-сервера в дополнительном терминале был запущен просмотр системного журнала в режиме реального

времени. После этого DNS-сервер был перезапущен. В журнале системных сообщений ошибок не зафиксировано, что свидетельствует о корректной конфигурации первичного DNS-сервера.

## 3.2 Анализ работы DNS-сервера

1. Для проверки корректности работы первичного DNS-сервера выполнен запрос к DNS-имени ns.elsaiedadel.net с использованием утилиты dig. В ответе сервера получен статус NOERROR, что свидетельствует об успешной обработке запроса.

В секции ANSWER SECTION присутствует A-запись, сопоставляющая имя ns.elsaiedadel.net с IP-адресом 192.168.1.1.

Флаг aa указывает, что ответ является авторитативным, а строка SERVER подтверждает, что запрос был обработан локальным DNS-сервером по адресу 127.0.0.1.

```
[root@server.elsaiedadel.net rz]#  
[root@server.elsaiedadel.net rz]# dig ns.elsaiedadel.net  
  
; <<>> DiG 9.18.33 <<>> ns.elsaiedadel.net  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3309  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: f8f4853fef263133010000006957913eb071bc0354d335fe (good)  
;; QUESTION SECTION:  
;ns.elsaiedadel.net.          IN      A  
  
;; ANSWER SECTION:  
ns.elsaiedadel.net.      86400  IN      A      192.168.1.1  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)  
;; WHEN: Fri Jan 02 09:34:54 UTC 2026  
;; MSG SIZE rcvd: 91  
  
[root@server.elsaiedadel.net rz]#
```

Рис. 3.6: Проверка A-записи ns.elsaiedadel.net

2. Для дополнительной проверки корректности конфигурации DNS-сервера выполнен анализ с использованием утилиты `host`.

Команда `host -l elsaiedadel.net` вывела список DNS-записей зоны, подтвердив наличие сервера имён, а также корректное сопоставление доменных имён `server.elsaiedadel.net` и `ns.elsaiedadel.net` с IP-адресом `192.168.1.1`.

Команда `host -a elsaiedadel.net` вернула подробное описание зоны, включая записи SOA, NS и A, что подтверждает корректную настройку прямой зоны.

Команда `host -t A elsaiedadel.net` подтвердила наличие A-записи для домена `elsaiedadel.net`.

Команда `host -t PTR 192.168.1.1` успешно разрешила IP-адрес в доменные имена `server.elsaiedadel.net` и `ns.elsaiedadel.net`, что свидетельствует о корректной настройке обратной DNS-зоны.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net rz]# host -l elsaiedadel.net
elsaiedadel.net name server elsaiedadel.net.
elsaiedadel.net has address 192.168.1.1
ns.elsaiedadel.net has address 192.168.1.1
server.elsaiedadel.net has address 192.168.1.1
[root@server.elsaiedadel.net rz]# host -a elsaiedadel.net
Trying "elsaiedadel.net"
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 32390
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
elsaiedadel.net.          86400   IN      SOA      elsaiedadel.net. server.elsaiedadel.net. 2026010200 86400 3600 604800 108
00
elsaiedadel.net.          86400   IN      NS       elsaiedadel.net.
elsaiedadel.net.          86400   IN      A        192.168.1.1

Received 106 bytes from 127.0.0.1#53 in 1 ms
[root@server.elsaiedadel.net rz]# host -t A elsaiedadel.net
elsaiedadel.net has address 192.168.1.1
[root@server.elsaiedadel.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.elsaiedadel.net.
1.1.168.192.in-addr.arpa domain name pointer ns.elsaiedadel.net.
[root@server.elsaiedadel.net rz]#
```

Рис. 3.7: Проверка DNS-зоны утилитой `host`

### 3.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

3. Для подготовки автоматической инициализации DNS-сервера при запуске виртуальной машины выполнен переход в каталог `/vagrant`. В нём была

создана иерархия каталогов `provision/server/dns`, предназначенная для хранения конфигурационных файлов DNS-сервера.

В соответствующие подкаталоги были скопированы файлы конфигурации из каталогов `/etc/named` и `/var/named/master`, используемые ранее при ручной настройке DNS-сервера.

```
[root@server.elsaiedadel.net rz]#  
[root@server.elsaiedadel.net rz]# cd /vagrant/  
[root@server.elsaiedadel.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named  
[root@server.elsaiedadel.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master  
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/  
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named /vagrant/provision/server/dns/etc/  
named.conf          named.rfc1912.zones  named.root.key  
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named/elsaiedadel.net /vagrant/provision/server/dns/etc/named/  
[root@server.elsaiedadel.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/  
[root@server.elsaiedadel.net vagrant]# cd provision/server/  
[root@server.elsaiedadel.net server]# touch dns.sh  
[root@server.elsaiedadel.net server]# chmod +x dns.sh  
[root@server.elsaiedadel.net server]#
```

Рис. 3.8: Подготовка каталогов и копирование конфигурации

4. В каталоге `/vagrant/provision/server` был создан исполняемый файл `dns.sh`, предназначенный для автоматической установки и настройки DNS-сервера. В скрипт были включены действия по установке пакетов `bind` и `bind-utils`, копированию конфигурационных файлов, настройке прав доступа, восстановлению контекстов безопасности SELinux, настройке межсетевого экрана, конфигурированию DNS-сервера по умолчанию для сетевого интерфейса, а также запуску и включению службы `named` в автозагрузку.

Данный скрипт полностью воспроизводит ранее выполненные действия по ручной установке и настройке 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 "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
30

```

Рис. 3.9: Скрипт автоматической настройки DNS-сервера

5. Для обеспечения автоматического выполнения созданного скрипта при запуске виртуальной машины server в конфигурационный файл Vagrantfile был добавлен provisioning-блок shell. Это позволяет при каждом запуске виртуальной машины автоматически разворачивать и настраивать DNS-сервер без необходимости ручного вмешательства.

В результате выполненных действий DNS-сервер корректно функционирует как первичный и кэширующий сервер, обслуживает прямую и обратную зоны, а также автоматически настраивается при развёртывании виртуальной машины.

## 4 Вывод

В ходе выполнения лабораторной работы был установлен, настроен и протестирован DNS-сервер на базе BIND. Реализована работа кэширующего и первичного DNS-сервера, выполнена настройка прямой и обратной DNS-зон, обеспечена корректная обработка DNS-запросов от локального узла и внутренней виртуальной сети. Проведена проверка работы сервера с использованием утилит `dig` и `host`, подтверждена корректность разрешения имён и обратного разрешения IP-адресов. Дополнительно выполнена автоматизация настройки DNS-сервера с использованием `provisioning`-скрипта, что обеспечивает воспроизводимость и удобство развёртывания сервиса. В результате DNS-сервер функционирует стабильно и соответствует требованиям задания.

## 5 Контрольные вопросы

### 1. Что такое DNS?

DNS (Domain Name System) — это распределённая иерархическая система доменных имён, предназначенная для преобразования символьных доменных имён в IP-адреса и обратно, а также для хранения и предоставления различной служебной информации о сетевых ресурсах.

### 2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер принимает запросы от клиентов, при необходимости запрашивает информацию у других DNS-серверов и сохраняет полученные ответы в кэше. Это позволяет ускорить последующие запросы и снизить нагрузку на внешние DNS-серверы.

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

Прямая DNS-зона предназначена для сопоставления доменных имён IP-адресам. Обратная DNS-зона используется для сопоставления IP-адресов доменным именам и применяется, например, при проверке подлинности узлов.

### 4. В каких каталогах и файлах располагаются настройки DNS-сервера?

**Кратко охарактеризуйте их назначение.**

Основные настройки располагаются в файле `/etc/named.conf`, который содержит общую конфигурацию сервера и подключение зон.

Файлы зон обычно хранятся в каталоге `/var/named` и его подкаталогах.

Файл `/etc/resolv.conf` содержит настройки DNS-клиента.

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

В файле `/etc/resolv.conf` указываются адреса DNS-серверов, используемых си-

стемой, а также домен поиска, применяемый при разрешении имён.

**6. Какие типы записей описания ресурсов есть в DNS и для чего они используются?**

A — сопоставляет имя IPv4-адресу.

AAAA — сопоставляет имя IPv6-адресу.

NS — указывает серверы имён зоны.

SOA — содержит служебную информацию о зоне.

PTR — используется для обратного разрешения IP-адресов.

MX — указывает почтовые серверы домена.

CNAME — создаёт псевдоним доменного имени.

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

Домен in-addr.arpa используется для организации обратного DNS-разрешения IPv4-адресов, то есть преобразования IP-адреса в доменное имя.

**8. Для чего нужен демон named?**

Демон named является основной службой DNS-сервера BIND. Он обрабатывает DNS-запросы, управляет зонами, кэшем и взаимодействует с другими DNS-серверами.

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

Master-сервер является основным источником данных DNS-зоны и хранит её оригинальные файлы.

Slave-сервер получает копию зоны с master-сервера и используется для повышения отказоустойчивости и распределения нагрузки.

**10. Какие параметры отвечают за время обновления зоны?**

За время обновления зоны отвечают параметры записи SOA: refresh, retry, expire и minimum.

**11. Как обеспечить защиту зоны от скачивания и просмотра?**

Защита обеспечивается настройкой директив allow-transfer и allow-query, а также ограничением доступа по IP-адресам и использованием межсетевого экрана.

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

Для описания почтовых серверов используется запись типа MX (Mail Exchange).

### **13. Как протестировать работу сервера доменных имён?**

Работу DNS-сервера можно протестировать с помощью утилит `dig`, `host` и `nslookup`, выполнив запросы к различным типам DNS-записей.

### **14. Как запустить, перезапустить или остановить какую-либо службу в системе?**

Для управления службами используется `systemd`. Запуск, перезапуск и остановка служб выполняются с помощью соответствующих команд управления сервисами.

### **15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?**

Отладочную информацию можно просмотреть через системный журнал, а также запустив сервис с повышенным уровнем логирования.

### **16. Где хранится отладочная информация по работе системы и служб? Как её посмотреть?**

Отладочная информация хранится в системном журнале. Для её просмотра используется журнал системных сообщений.

### **17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите примеры.**

Для этого можно использовать утилиты `lsdf` или `fuser`, которые отображают файлы и порты, используемые процессами.

### **18. Приведите несколько примеров по изменению сетевого соединения при помощи `nmcli`.**

С помощью `nmcli` можно изменять DNS-серверы, включать или отключать автоматическое получение параметров, изменять IP-адреса и перезапускать сетевые соединения.

### **19. Что такое SELinux?**

SELinux — это подсистема безопасности Linux, реализующая механизм мандатного управления доступом на основе политик безопасности.

### **20. Что такое контекст (метка) SELinux?**

Контекст SELinux — это метка безопасности, присваиваемая процессам и файлам, определяющая допустимые операции доступа.

### **21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?**

Контекст SELinux восстанавливается с помощью утилиты `restorecon`, которая назначает файлам корректные метки безопасности.

### **22. Как создать разрешающие правила политики SELinux из файлов журналов?**

Для создания разрешающих правил используются утилиты анализа журналов SELinux, которые формируют модули политики на основе сообщений о запретах.

### **23. Что такое булевый переключатель в SELinux?**

Булевый переключатель SELinux — это параметр, позволяющий динамически изменять поведение политики безопасности без её полной переработки.

### **24. Как посмотреть список переключателей SELinux и их состояние?**

Список булевых переключателей и их текущее состояние можно посмотреть с помощью специальной утилиты управления SELinux.

### **25. Как изменить значение переключателя SELinux?**

Значение булевого переключателя изменяется с помощью команды управления SELinux, с возможностью применения изменений временно или на постоянной основе.