Лабораторная работа №2

НастройкаDNS-сервера

Жукова Арина Александровна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение практических навыков по установке и конфигурированию DNS сервера, усвоение принциповработысистемыдоменныхимён.

2 Задание

1. Установитенавиртуальноймашинеserver DNS-серверbind иbind-utils.
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер .
3. Сконфигурируйтенавиртуальноймашинеserver первичныйDNS-сервер.
4. При помощи утилит dig и host проанализируйте работу DNS-сервера.
5. Напишите скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile.

3 Теоретическое введение

DNS (Domain Name System) — это распределённая система, которая преобразует доменные имена (например, `www.example.com`) в IP-адреса (например, `192.168.1.1`) и наоборот. Она обеспечивает работу интернета, позволяя пользователям обращаться к ресурсам по удобным именам, а не по числовым адресам.

Основные компоненты DNS:

1. **DNS-сервер** — программа, хранящая информацию о доменных зонах и обрабатывающая запросы. Наиболее популярным решением является BIND (Berkeley Internet Name Domain).
2. **DNS-клиент** — программа или библиотека, отправляющая запросы к DNS-серверам.
3. **Доменная зона** — часть доменного пространства, управляемая администратором. Зоны делятся на:
    - **Прямые зоны** — сопоставляют имена с IP-адресами.
    - **Обратные зоны** — сопоставляют IP-адреса с именами (например, через домен `in-addr.arpa`).

Типы DNS-серверов: - **Primary Master** — основной сервер, загружающий данные зоны из локальных файлов. - **Secondary Master** — резервный сервер, получающий данные зоны от основного. - **Кэширующий** — сервер, обрабатывающий запросы клиентов и кэширующий ответы для ускорения работы.

Основные типы DNS-записей (RR — Resource Records): - **SOA** — информация о зоне и её администраторе. - **NS** — указание на серверы имён для зоны. - **A** — сопоставление имени с IPv4-адресом. - **PTR** — обратное сопоставление IP-адреса с именем. - **CNAME** — создание псевдонимов для имён. - **MX** — указание почтовых серверов для домена.

Утилиты диагностики: - **dig** — мощная утилита для выполнения DNS-запросов и анализа ответов. - **host** — простая утилита для разрешения имён и проверки зон.

DNS играет ключевую роль в обеспечении стабильности и безопасности интернета, а её настройка требует понимания принципов работы зон, типов записей и взаимодействия между серверами.

4 Выполнение лабораторной работы

4.1 Установка DNS-сервера

1. На виртуальной машине server войдите под созданным вами в предыдущей работе пользователем и откройте терминал. Перейдите в режим суперпользователя (рис. 4.1).

```
[aazhukova@server.aazhukova.net ~]$ sudo -i
[sudo] password for aazhukova:
[root@server.aazhukova.net ~]#
```

Рисунок 4.1: Вход в режим суперпользователя

2. Установите bind и bind-utils (рис. 4.2).

```
[aazhukova@server.aazhukova.net ~]$ sudo -i
[root@server.aazhukova.net ~]# dnf -y install bind bind-utils
Last metadata expiration check: 0:31:29 ago on Thu 06 Nov 2025 06:17:31 AM UTC.
Package bind-32:9.18.33-4.el10_0.x86_64 is already installed.
Package bind-utils-32:9.18.33-4.el10_0.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@server.aazhukova.net ~]#
```

Рисунок 4.2: Установка

3. В качестве упражнения с помощью утилиты dig сделайте запрос к DNS-адресу www.yandex.ru (рис. 4.3).

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17255
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          59      IN      A       5.255.255.77
www.yandex.ru.          59      IN      A       77.88.44.55
www.yandex.ru.          59      IN      A       77.88.55.88

;; Query time: 78 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Thu Nov 06 06:49:22 UTC 2025
;; MSG SIZE  rcvd: 90
```

Рисунок 4.3: запрос к DNS-адресу

4.2 Конфигурирование кэширующего DNS-сервера

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

1. Анализ файлов

```
[root@server.aazhukova.net etc]# cat resolv.conf
# Generated by NetworkManager
search naukanet.ru aazhukova.net
nameserver 10.0.2.3
```

Рисунок 4.4: /etc/resolv.conf

`search naukanet.ru aazhukova.net`

- Директива search: определяет домены для автоматического дополнения коротких имён хостов

- При запросе короткого имени будет последовательно проверяться с суффиксами:
  - имя.naukanet.ru
  - имя.aazhukova.net

```
nameserver 10.0.2.3
```

- Директива nameserver: указывает DNS-сервер для разрешения имён
- Используется сервер с IP-адресом 10.0.2.3

```
[root@server.aazhukova.net etc]# cat 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.
```

Рисунок 4.5: /etc/named.conf

```
; FORMERLY NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
G.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:12::d0d
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     198.97.190.53
H.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
```

Рисунок 4.6: /var/named/named.ca3

```
; FORMERLY NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.     3600000      AAAA  2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.     3600000      AAAA  2001:7fd::1
;
; OPERATED BY ICANN
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:9f::42
;
```

Рисунок 4.7: /var/named/named.ca4

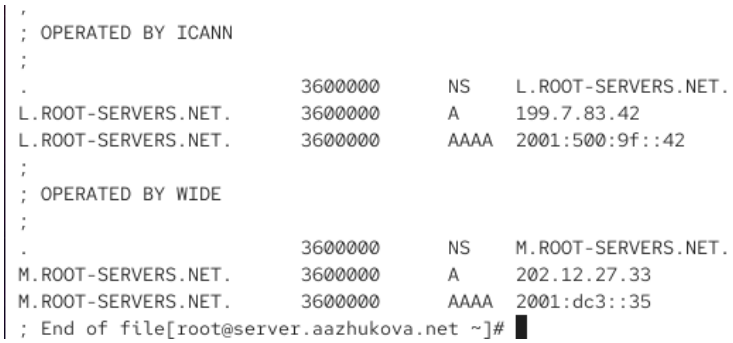

Рисунок 4.8: /var/named/named.ca5

```
options {     listen-on port 53 { 127.0.0.1; };
```

- listen-on: сервер слушает на порту 53 только на localhost (127.0.0.1)

```
listen-on-v6 port 53 { ::1; };
```

- listen-on-v6: слушает на IPv6 localhost (::1)

```
directory "/var/named";
```

- directory: рабочий каталог BIND - /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_st
secroots-file  "/var/named/data/named.secroots";         recursing-file
"/var/named/data/named.recursing";
```

- Пути к различным служебным файлам:
  - дамп кэша
  - статистика
  - статистика памяти
  - secure roots
  - рекурсивные запросы

```
allow-query { localhost; };
```

- allow-query: разрешает DNS-запросы только с localhost

```
[root@server.aazhukova.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
;
```

Рисунок 4.9: /var/named/named.ca

```
A.ROOT-SERVERS.NET.     36000000     NS     A.ROOT-SERVERS.NET.
```

- NS-запись: сервер A.ROOT-SERVERS.NET является корневым сервером имён
- TTL: 36000000 секунд

```
A.ROOT-SERVERS.NET.     36000000     A     198.41.0.4
```

- A-запись: IPv4-адрес сервера A.ROOT-SERVERS.NET - 198.41.0.4

```
A.ROOT-SERVERS.NET.     36000000     AAAA  2001:503:ba3e::2:30
```

- AAAA-запись: IPv6-адрес сервера A.ROOT-SERVERS.NET

```
; 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
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
E.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:a8::e
```

Рисунок 4.10: /var/named/named.ca2

`B.ROOT-SERVERS.NET. 36000000 NS B.ROOT-SERVERS.NET. B.ROOT-SERVERS.NET. 36000000 A 170.247.170.2`

- Корневой сервер B с IPv4-адресом 170.247.170.2

`C.ROOT-SERVERS.NET. 36000000 NS C.ROOT-SERVERS.NET. C.ROOT-SERVERS.NET. 36000000 A 192.33.4.12`

- Корневой сервер C с IPv4-адресом 192.33.4.12

```
; End of file[root@server.aazhukova.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.aazhukova.net ~]#
```

Рисунок 4.11: /var/named/named.localhost

`$TTL 1D`

- **Директива $TTL**: устанавливает время жизни (Time To Live) по умолчанию для всех записей зоны - 1 день

```
@    IN SOA @ rname.invalid. (
```

- **SOA-запись** (Start of Authority):
  - `@` - символ, обозначающий текущую зону (в данном случае localhost)
  - `IN` - класс Internet
  - `SOA` - тип записи (начало зоны)
  - `@` - primary master сервер для зоны
  - `rname.invalid.` - контактное лицо (в формате email, где @ заменён на точку)

```
0    ; serial
```

- **Serial** - серийный номер зоны (0) - используется для отслеживания изменений

```
1D    ; refresh
```

- **Refresh** - интервал обновления (1 день) - как часто secondary сервер должен проверять актуальность зоны

```
1H    ; retry
```

- **Retry** - интервал повтора (1 час) - как часто повторять попытку при неудачном обновлении

```
1W    ; expire
```

- **Expire** - время истечения (1 неделя) - через какое время данные считаются устаревшими, если нет связи с master

```
3H )    ; minimum
```

- **Minimum** - время негативного кэширования (3 часа) - время кэширования отрицательных ответов

```
NS @
```

- **NS-запись** (Name Server): указывает, что DNS-сервером для этой зоны является текущий сервер (`@`)

```
A    127.0.0.1
```

- **A-запись** (Address): сопоставляет имя хоста `localhost` с IPv4-адресом `127.0.0.1`

```
AAAA ::1
```

- **AAAA-запись**: сопоставляет имя хоста `localhost` с IPv6-адресом `::1`

```
[root@server.aazhukova.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.
```

Рисунок 4.12: /var/named/named.loopback

```
$TTL 1D
```

- **Директива $TTL**: время жизни записей - 1 день

```
@    IN SOA @ rname.invalid. (
```

- **SOA-запись** с теми же параметрами, что и в прямой зоне

```
    0    ; serial
    1D    ; refresh
    1H    ; retry
    1W    ; expire
    3H )    ; minimum
```

- Параметры SOA идентичны файлу named.localhost

```
NS    @
```

- **NS-запись**: DNS-сервер для обратной зоны

```
A    127.0.0.1
```

- **A-запись**: IPv4-адрес (может быть избыточным в обратной зоне)

```
AAAA    ::1
```

- **AAAA-запись**: IPv6-адрес

```
PTR    localhost.
```

- **PTR-запись** (Pointer): обратное преобразование - сопоставляет IP-адрес `127.0.0.1` с доменным именем `localhost.`
- Обратите внимание на точку в конце - это FQDN (полное доменное имя)

2. Запустите DNS-сервер, Включите запуск DNS-сервера в автозапуск при загрузке системы (рис. 4.13).

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

Рисунок 4.13: запуск DNS-сервера

3. Анализ различий

```
[root@server.aazhukova.net ~]# systemctl start named
[root@server.aazhukova.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/
system/named.service'.
[root@server.aazhukova.net ~]# dig www.yandex.ru

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31406
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          415     IN      A       77.88.44.55
www.yandex.ru.          415     IN      A       77.88.55.88
www.yandex.ru.          415     IN      A       5.255.255.77

;; Query time: 23 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Thu Nov 06 07:05:30 UTC 2025
;; MSG SIZE  rcvd: 90
```

Рисунок 4.14: dig www.yandex.ru

```
[root@server.aazhukova.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: 39897
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 35eac8a38e24f84501000000690c48f14f9d66e4de3a9da8 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

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

;; Query time: 3230 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 06 07:06:25 UTC 2025
;; MSG SIZE  rcvd: 118
```

Рисунок 4.15: dig **127.0.0.1** www.yandex.ru

4.2.1.1 Команда 1: `dig www.yandex.ru`

```
;; Query time: 23 msec
```

- **Время выполнения**: очень быстрое - 23 мсек

```
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
```

- **Сервер**: запрос отправлен на внешний DNS-сервер `10.0.2.3`

```
www.yandex.ru.    415   IN    A    77.88.44.55
www.yandex.ru.    415   IN    A    77.88.55.88
www.yandex.ru.    415   IN    A    5.255.255.77
```

- **TTL**: 415 секунд - уменьшенное значение, так как ответ получен из кэша

4.2.1.2 Команда 2: `dig @127.0.0.1 www.yandex.ru`

```
;; communications error to 127.0.0.1#53: timed out
```

- **Ошибка соединения**: таймаут при обращении к localhost
- **Причина**: DNS-сервер на 127.0.0.1 не отвечает или отвечает медленно

```
;; Query time: 3230 msec
```

- **Время выполнения**: очень медленное - 3230 мсек (3.2 секунды)
- **Причина**: длительные попытки соединения с локальным сервером

```
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
```

- **Сервер**: запрос отправлен на локальный DNS-сервер `127.0.0.1`

```
www.yandex.ru.    600    IN    A    77.88.44.55
www.yandex.ru.    600    IN    A    5.255.255.77
www.yandex.ru.    600    IN    A    77.88.55.88
```

- **TTL**: 600 секунд - исходное значение TTL от авторитетного сервера

```
; COOKIE: 35eac8a38e24f84501000000690c48f14f9d66e4de3a9da8 (good)
```

- **DNS cookie**: присутствует механизм защиты от амплификации DNS

4.2.1.3 Ключевые различия и выводы:

4.2.1.3.1 1. Производительность:

- **Внешний DNS (10.0.2.3)**: 23 мс - отличная скорость
- **Локальный DNS (127.0.0.1)**: 3230 мс - крайне медленная работа

4.2.1.3.2 2. Состояние сервиса:

- Локальный DNS-сервер `named` запущен, но работает некорректно
- Наблюдаются проблемы с производительностью или конфигурацией

4.2.1.3.3 3. Источник данных:

- **10.0.2.3**: ответ из кэша (TTL = 415)
- **127.0.0.1**: ответ с исходным TTL (600), что указывает на прямой запрос к авторитетным серверам

4.2.1.3.4 4. Сетевые проблемы:

- Таймаут при обращении к 127.0.0.1 свидетельствует о:
  - Неправильной конфигурации BIND
  - Проблемах с брандмауэром
  - SELinux блокирует соединение
  - Сервер не слушает на 127.0.0.1

4. Сделайте DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить настройки сетевого соединения eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0.1. Сделайте тоже самое для соединения System eth0 (если оно активно). Перезапустите NetworkManager (рис. 4.16).

```
[root@server.aazhukova.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, matc
h, 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' (323fd428-cb16-4cd5-90c4-d94afb75c855) successfully updated.
nmcli> quit
[root@server.aazhukova.net ~]# nmcil connection edit System\ eth0
bash: nmcil: command not found...
Similar command is: 'nmcli'
[root@server.aazhukova.net ~]# nmcli connection edit System\ eth0
Error: Unknown connection 'System eth0'.
[root@server.aazhukova.net ~]# systemctl restart NetworkManager
[root@server.aazhukova.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search aazhukova.net
nameserver 127.0.0.1
[root@server.aazhukova.net ~]#
```

Рисунок 4.16: DNS-сервер сервер по умолчанию

5. 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(рис. 4.17).

```
 GNU nano 8.1                                /etc/named.conf                                Modified
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 192.168.0.0/16; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           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
```

Рисунок 4.17: направление DNS-запросов от всех узлов внутренней сети

6. Внесите изменения в настройки межсетевого экрана узла server, разрешив работу с DNS(рис. 4.18).

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

Рисунок 4.18: настройки межсетевого экрана узла server

7. Убедитесь, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используйте команду lsof(рис. 4.19).

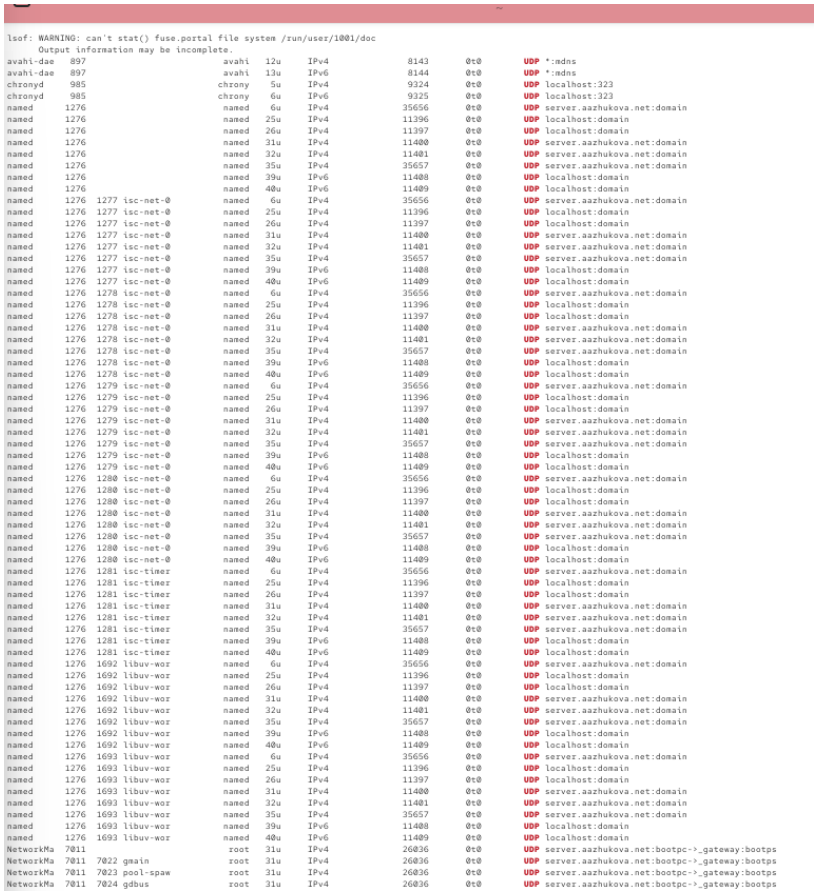

Рисунок 4.19: команда lsof

4.3 Конфигурирование первичного DNS-сервера

1. Скопируйте шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуйте его в aazhukova.net (рис. 4.20).

Рисунок 4.20: копирование шаблона описания DNS-зон

2. Включите файл описания зоны /etc/named/user.net в конфигурационном файле DNS /etc/named.conf(рис. 4.21).

Рисунок 4.21: /etc/named.conf

3. Откройте файл /etc/named/user.net на редактирование и пропишите свою прямую зону, пропишите свою обратную зону(рис. 4.22).

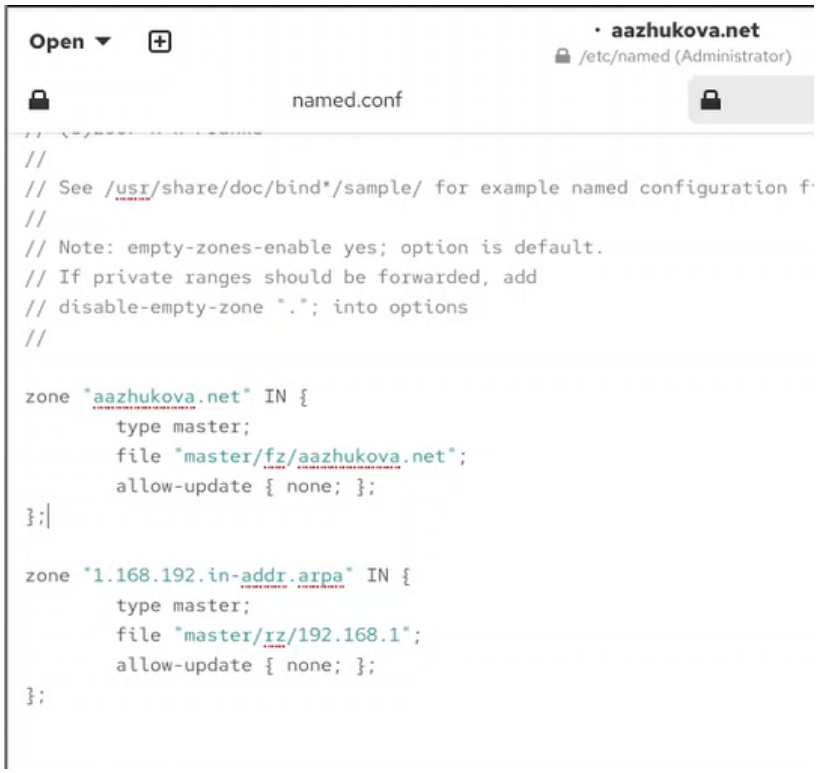

Рисунок 4.22: /etc/named/aazhukova.net

4. В каталоге /var/named создайте подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно(рис. 4.23).

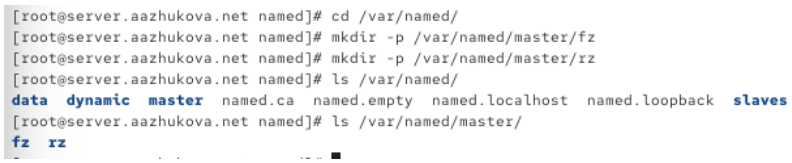

Рисунок 4.23: каталог /var/named

5. Измените файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны(**?@fig-00**).

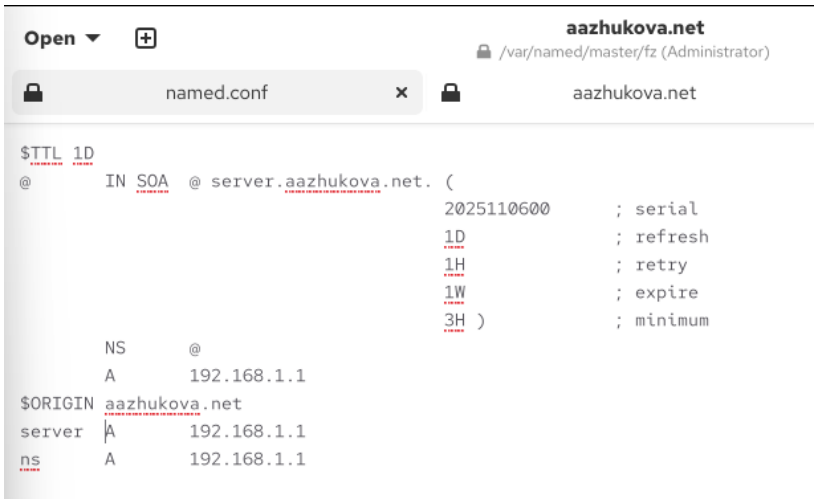

Рисунок 4.24: /var/named/master/fz/aazhukova.net

6. Измените файл /var/named/master/rz/192.168.1, указав необходимые DNS-записи для обратной зоны (рис. 4.25).

Рисунок 4.25: /var/named/master/rz/192.168.1

7. Далее требуется исправить права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать. . 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. Для проверки состояния переключателей SELinux, относящихся к named (рис. 4.26).

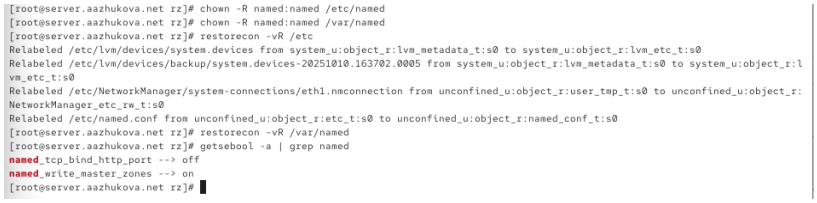

Рисунок 4.26: Состояния переключателей SELinux

8. В дополнительном терминале запустите в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы и в первом терминале перезапустите DNS-сервер (рис. 4.27).

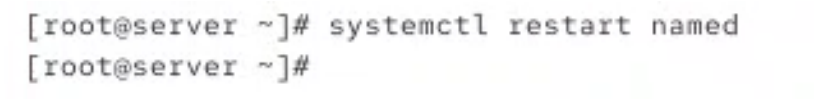

Рисунок 4.27: перезапуск DNS-сервер

4.4 Анализ работы DNS-сервера

1. При помощи утилиты dig получите описание DNS-зоны с сервера ns.user.net (рис. 4.28).

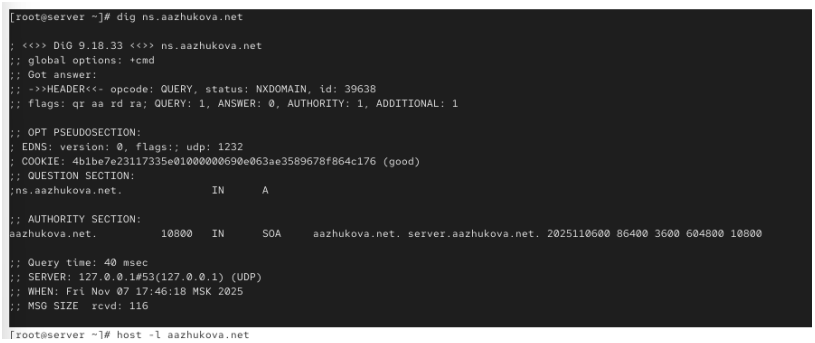

Рисунок 4.28: описание DNS-зоны с сервера

2. При помощи утилиты host проанализируйте корректность работы DNS-сервера (рис. 4.29).

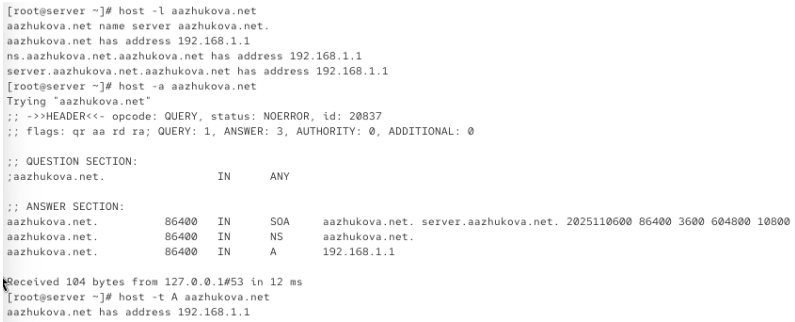

Рисунок 4.29: утилиты host

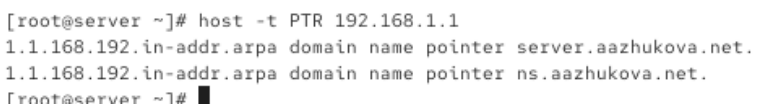

Рисунок 4.30: утилиты host

4.4.0.1 1. Команда `host -l aazhukova.net`

aazhukova.net name server aazhukova.net.

aazhukova.net has address 192.168.1.1

ns.aazhukova.net.aazhukova.net has address 192.168.1.1

server.aazhukova.net.aazhukova.net has address 192.168.1.1

Анализ: - **Зонный трансфер работает** - сервер отдаёт все записи зоны - **Обнаружены 3 A-записи** для домена aazhukova.net: - `aazhukova.net` → `192.168.1.1` - `ns.aazhukova.net` → `192.168.1.1` - `server.aazhukova.net` → `192.168.1.1` - **Потенциальная проблема**: все хосты указывают на один IP-адрес

4.4.0.2 2. Команда `host -a aazhukova.net` (все записи)

```
Trying 'aazhukova.net'
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20837
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
```

Анализ флагов ответа: - `qr` - это ответ (query response) - `aa` - **авторитетный ответ** (authoritative answer) - сервер авторитативен для зоны - `rd` - рекурсия запрошена (recursion desired) - `ra` - рекурсия доступна (recursion available)

```
;; QUESTION SECTION:
;aazhukova.net. IN ANY


;; ANSWER SECTION:
aazhukova.net. 86400 IN SOA aazhukova.net. server.aazhukova.net. 2025110600 86400 3600 6
aazhukova.net. 86400 IN NS aazhukova.net.
aazhukova.net. 86400 IN A 192.168.1.1
```

Анализ записей: - **SOA-запись** корректна: - Primary server: `aazhukova.net` - Contact: `server.aazhukova.net` (email: server@aazhukova.net) - Serial: `2025110600` (формат ГГГГММДДВВ) - Refresh: 86400 сек (1 день) - Retry: 3600 сек (1 час) - Expire: 604800 сек (1 неделя) - Minimum: 10800 сек (3 часа)

- **NS-запись**: `aazhukova.net` является своим DNS-сервером
- **A-запись**: домен указывает на `192.168.1.1`

```
Received 104 bytes from 127.0.0.1#53 in 12 ms
```

- **Быстрый ответ** - 12 мс от локального сервера

4.4.0.3 3. Команда `host -t A aazhukova.net` (только A-запись)

```
aazhukova.net has address 192.168.1.1
```

- **A-запись разрешается корректно**

4.4.0.4 4. Команда `host -t PTR 192.168.1.1` (обратное разрешение)

```
1.1.168.192.in-addr.arpa domain name pointer server.aazhukova.net
1.1.168.192.in-addr.arpa domain name pointer ns.aazhukova.net
```

- **Обратная зона работает корректно**
- **Две PTR-записи** для IP 192.168.1.1:
  - `server.aazhukova.net`
  - `ns.aazhukova.net`

4.4.1 Вывод

DNS-сервер настроен корректно, все основные функции работают properly. Конфигурация соответствует требованиям лабораторной работы.

4.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dns, в который поместите в соответствующие каталоги конфигурационные файлы DNS (рис. 4.31).

```
[root@server.aazhukova.net ~]# cd /vagrant/provision/server/
[root@server.aazhukova.net server]# ls
01-dummy.sh  02-forward.sh  dns  dns.sh
```

Рисунок 4.31: /vagrant/provision/server/

2. . В каталоге /vagrant/provision/server создайте исполняемый файл dns.sh (рис. 4.32).

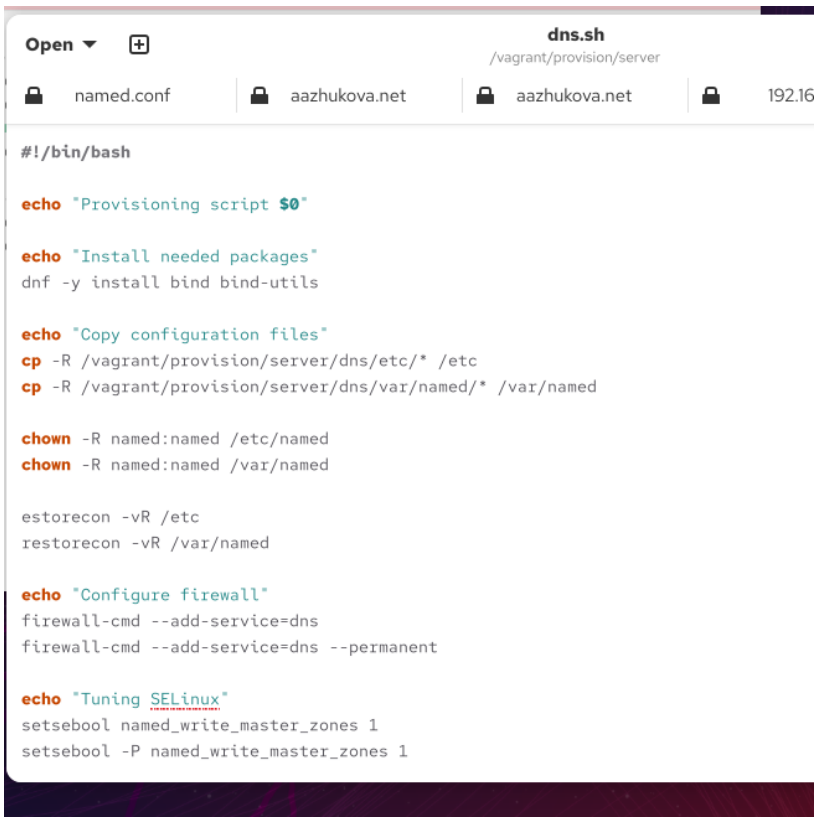

Рисунок 4.32: файл dns.sh

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера(рис. 4.33).

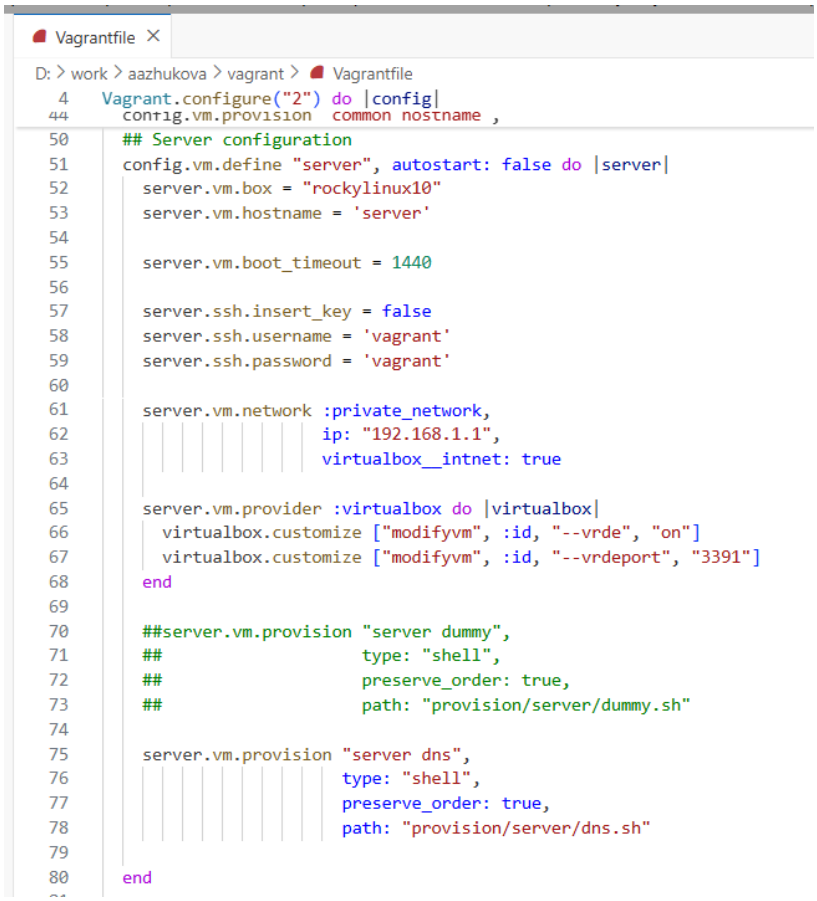

Рисунок 4.33: Vagrantfile

5 Выводы

Я приобрела практические навыки по установке и конфигурированию DNS-сервера, усвоила принципов работы системы доменных имён.

6 Ответы на контрольные вопросы

1. **Что такое DNS?** DNS (Domain Name System) — это распределённая система (распределённая база данных), которая преобразует доменные имена хостов в IP-адреса и наоборот.

2. **Каково назначение кэширующего DNS-сервера?** Назначение кэширующего DNS-сервера — принимать рекурсивные запросы от клиентов и выполнять их с помощью нерекурсивных запросов к авторитетным серверам, кэшируя результаты для ускорения последующих аналогичных запросов.

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

   - **Прямая зона** сопоставляет доменное имя с IP-адресом (записи A, AAAA).
   - **Обратная зона** сопоставляет IP-адрес с доменным именем (записи PTR) и используется в специальном домене `in-addr.arpa`.

4. **В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.**

   - `/etc/named.conf` — главный конфигурационный файл DNS-сервера BIND, определяет основные параметры, зоны и правила доступа.
   - `/etc/named/` — каталог для дополнительных конфигурационных файлов зон (например, `/etc/named/user.net`).
   - `/var/named/` — каталог для файлов данных зон (прямых и обратных).

- `/var/named/named.ca` — файл с корневыми серверами DNS.
- `/var/named/named.localhost`, `/var/named/named.loopback` — шаблоны для создания файлов зон.

5. **Что указывается в файле resolv.conf?** В файле `/etc/resolv.conf` указываются IP-адреса DNS-серверов, которые использует система для разрешения доменных имён.

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

   - **SOA** (Start of Authority) — указывает на авторитетность сервера для зоны и содержит управляющие параметры.
   - **NS** (Name Server) — указывает на DNS-серверы, обслуживающие домен.
   - **A** (Address) — сопоставляет имя хоста с IPv4-адресом.
   - **PTR** (Pointer) — сопоставляет IP-адрес с доменным именем (для обратных зон).
   - **CNAME** (Canonical Name) — задаёт каноническое имя (псевдоним) для хоста.
   - **MX** (Mail Exchanger) — указывает почтовые серверы для домена.

7. **Для чего используется домен in-addr.arpa?** Домен `in-addr.arpa` используется для организации обратного просмотра DNS (reverse DNS lookup), то есть для сопоставления IP-адресов с доменными именами.

8. **Для чего нужен демон named?** Демон `named` — это сервис DNS-сервера BIND (Berkeley Internet Name Domain), который отвечает на DNS-запросы и управляет зонами.

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

- **Master-сервер** (primary) — хранит основную (авторитетную) копию данных зоны и загружает их из файла на диске.
- **Slave-сервер** (secondary) — получает данные зоны от master-сервера через механизм зонных трансферов, обеспечивая избыточность и надежность.

10. **Какие параметры отвечают за время обновления зоны?** В SOA-записи:
    - `refresh` — интервал, через который slave-сервер проверяет актуальность зоны у master.
    - `retry` — интервал повторной попытки связи с master после сбоя.
    - `expire` — время, после которого данные зоны на slave считаются устаревшими, если нет связи с master.
    - `minimum` — время негативного кэширования.
11. **Как обеспечить защиту зоны от скачивания и просмотра?** Защита обеспечивается настройками контроля доступа в `named.conf` (директивы `allow-query`, `allow-transfer`), использованием TSIG-ключей для авторизации трансферов и настройкой брандмауэра.
12. **Какая запись RR применяется при создании почтовых серверов?** Для почтовых серверов применяется запись типа **MX** (Mail Exchanger).
13. **Как протестировать работу сервера доменных имён?** Работу DNS-сервера тестируют с помощью утилит `dig` и `host`, отправляя запросы разных типов (A, PTR, MX, NS) и проверяя корректность и полноту ответов.
14. **Как запустить, перезапустить или остановить какую-либо службу в системе?** Используются команды `systemctl`:
    - `systemctl start <service_name>`
    - `systemctl restart <service_name>`

- `systemctl stop <service_name>`

15. **Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?** Отладочную информацию можно посмотреть с помощью команды `journalctl -u <service_name>` или в реальном времени с помощью `journalctl -x -f` при перезапуске службы.

16. **Где храниться отладочная информация по работе системы и служб? Как её посмотреть?** Отладочная информация хранится в журналах systemd (journald). Просмотреть её можно с помощью утилиты `journalctl`.

17. **Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров.** Для этого используется утилита `lsof`. Примеры:

    - `lsof -p <PID>` — показать файлы, используемые процессом с указанным ID.
    - `lsof | grep UDP` — найти процессы, использующие UDP-сокеты (например, DNS-сервер на порту 53).

18. **Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli.**

    - `nmcli connection edit "eth0"` — войти в интерактивный режим редактирования соединения.
    - `nmcli connection show` — показать все сетевые соединения.
    - `nmcli connection modify "eth0" ipv4.dns "8.8.8.8"` — установить DNS-сервер.

19. **Что такое SELinux?** SELinux (Security-Enhanced Linux) — это механизм принудительного контроля доступа, который обеспечивает

дополнительную безопасность, разграничивая доступ процессов и пользователей к объектам (файлам, сокетам и т.д.) на основе политик.

20. **Что такое контекст (метка) SELinux?** Контекст (метка) SELinux — это специальный атрибут (например, `system_u:object_r:named_zone_t:s0`), присваиваемый каждому процессу и файлу в системе. SELinux использует эти метки для принятия решений о разрешении или запрете операций.

21. **Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?** Для восстановления контекста используется команда `restorecon`:

    - `restorecon -vR /etc/named` — рекурсивно восстановить контекст для каталога `/etc/named`.

22. **Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?** Для генерации правил на основе записей в логах используется утилита `audit2allow`.

23. **Что такое булевый переключатель в SELinux?** Булевый переключатель (boolean) в SELinux — это параметр, который позволяет динамически изменять поведение политики безопасности без её перекомпиляции. Например, `named_write_master_zones` разрешает демону `named` запись в мастер-зоны.

24. **Как посмотреть список переключателей SELinux и их состояние?** Для просмотра списка и состояния переключателей используется команда:

    - `getsebool -a | grep named`

25. **Как изменить значение переключателя SELinux?** Для изменения значения переключателя используется команда `setsebool`:

- `setsebool -P named_write_master_zones 1` — установить переключатель в значение 1 (включить) с сохранением (`-P`) после перезагрузки.

Список литературы

1. Barr D. Common DNS Operational and Configuration Errors: RFC / RFC Editor. — 02/1996. — DOI: 10.17487/rfc1912.
2. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / M. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: https: //docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/ index.html (дата обр. 13.09.2021).
3. Systemd. — 2015. — URL: https://wiki.archlinux.org/index.php/Systemd (visited on 09/13/2021).
4. Костромин В. А. Утилита lsof — инструмент администратора. — URL: http : / / rus - linux.net/kos.php?name=/papers/lsof/lsof.html (дата обр. 13.09.2021).
5. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: http : //wiki.opennet.ru/Systemd (дата обр. 13.09.2021).
6. Сайт проекта NetworkManager. — URL: https : / / wiki . gnome . org / Projects / NetworkManager (visited on 09/13/2021).
7. Сайт проекта nmcli. — URL: https://developer.gnome.org/NetworkManager/stable/nmcli.html (visited on 09/13/2021).