Отчёт по лабораторной работе №2

Настройка DNS-сервера

Владимир Базлов

Содержание

Список иллюстраций

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 настройка кэширующего DNS-сервера BIND

1. Загружена операционная система и выполнен переход в каталог проекта.
2. Виртуальная машина *server* успешно запущена средствами Vagrant.
3. Выполнен вход под пользователем и произведён переход в режим суперпользователя.
4. На виртуальную машину установлены пакеты BIND и bind-utils.
5. Проверена работа внешних DNS-серверов при помощи утилиты `dig`.
   На экран выводятся секции запроса: QUESTION и ANSWER.
   ANSWER содержит несколько A-записей — IP-адреса ресурса. Запрос отправляется на DNS, указанный в `resolv.conf`.

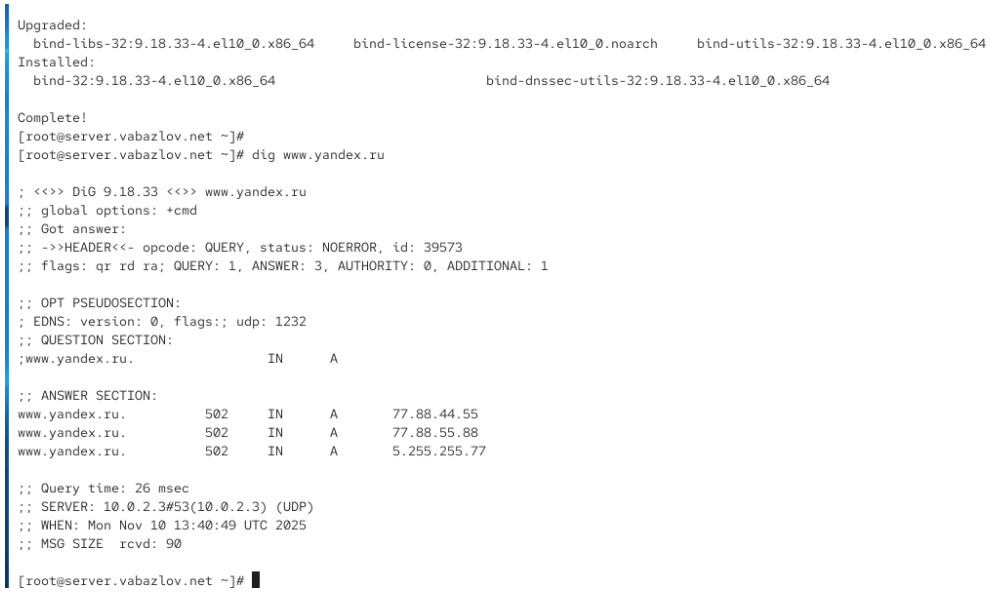


Рис. 2.1: Запрос к внешнему DNS — dig www.yandex.ru

Проанализированы файлы конфигурации:

- `/etc/resolv.conf` — настройки DNS резолвера для системы;
- `/etc/named.conf` — основной конфигурационный файл службы BIND;
- `/var/named/named.ca` — содержит список корневых DNS-серверов;
- `/var/named/named.localhost` и `/var/named/named.loopback` — файлы локальных зон.

Файл `/etc/named.conf` содержит параметры работы сервера: интерфейсы прослушивания, разрешение запросов, пути хранения файлов.

```
[root@server.vabazlov.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
        */
        recursion yes;

        dnssec-validation yes;

        managed-keys-directory "/var/named/dynamic";
```

Рис. 2.2: Файл /etc/named.conf

Файл `/var/named/named.ca` содержит список корневых name-server.

```
[root@server.vabazlov.net ~]#
[root@server.vabazlov.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
;
; FORMERLY TERP.UMD.EDU
```

Рис. 2.3: Файл /var/named/named.ca

Файлы локальных зон содержат записи localhost и loopback.

```
[root@server.vabazlov.net ~]#
[root@server.vabazlov.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.vabazlov.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.vabazlov.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search vabazlov.net
nameserver 10.0.2.3
[root@server.vabazlov.net ~]#
```

Рис. 2.4: Файлы named.localhost и named.loopback

DNS-сервер запущен и добавлен в автозапуск.

Был выполнен сравнительный DNS-запрос:

- `dig www.yandex.ru` — запрос отправляется на внешний DNS-сервер;
- `dig @127.0.0.1 www.yandex.ru` — запрос направляется на локальный BIND.

В выводе заметно отличие: при обращении к локальному серверу увеличено время выполнения первого запроса, так как он формирует кэш.

```
[root@server.vabazlov.net ~]# systemctl start named
[root@server.vabazlov.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.vabazlov.net ~]# dig @127.0.0.1 www.yandex.ru
;; communications error to 127.0.0.1#53: timed out
;; 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: 25242
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 01839f3071098a87010000006911ec3f2ae95ffd03233598 (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       77.88.55.88
www.yandex.ru.          600     IN      A       77.88.44.55

;; Query time: 1315 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Nov 10 13:44:31 UTC 2025
;; MSG SIZE  rcvd: 118

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

Рис. 2.5: Сравнение запросов dig www.yandex.ru и dig [**127.0.0.1?**]

В настройках интерфейса `eth0` изменён используемый DNS-сервер — теперь это `127.0.0.1`.

После сохранения конфигурации файл `/etc/resolv.conf` обновился.

```
[root@server.vabazlov.net ~]#
[root@server.vabazlov.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, hostna
me, 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.vabazlov.net ~]# systemctl restart NetworkManager
[root@server.vabazlov.net ~]#
[root@server.vabazlov.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search vabazlov.net
nameserver 127.0.0.1
[root@server.vabazlov.net ~]#
```

Рис. 2.6: Изменение resolv.conf через nmcli

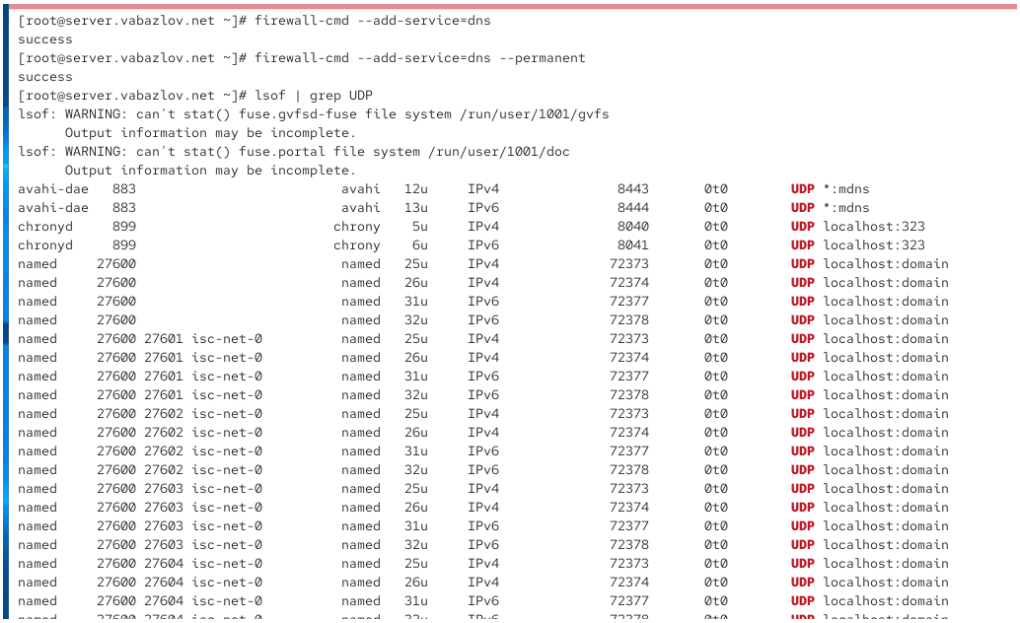
В `/etc/named.conf` внесены изменения:

- сервер начинает слушать все интерфейсы, а не только `127.0.0.1`,

- разрешены DNS-запросы от адресов внутренней сети (`192.168.0.0/16`).

Рис. 2.7: Изменения allow-query и listen-on

Для разрешения DNS-трафика в firewall добавлена служба DNS. Проверено, что процесс `named` слушает порт 53 по UDP — запросы теперь проходят через локальный DNS-сервер.



```
[root@server.vabazlov.net ~]# firewall-cmd --add-service=dns
success
[root@server.vabazlov.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.vabazlov.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   883                         avahi   12u     IPv4              8443       0t0       UDP *:mdns
avahi-dae   883                         avahi   13u     IPv6              8444       0t0       UDP *:mdns
chronyd     899                        chrony    5u     IPv4              8040       0t0       UDP localhost:323
chronyd     899                        chrony    6u     IPv6              8041       0t0       UDP localhost:323
named     27600                         named   25u     IPv4             72373       0t0       UDP localhost:domain
named     27600                         named   26u     IPv4             72374       0t0       UDP localhost:domain
named     27600                         named   31u     IPv6             72377       0t0       UDP localhost:domain
named     27600                         named   32u     IPv6             72378       0t0       UDP localhost:domain
named     27600 27601 isc-net-0         named   25u     IPv4             72373       0t0       UDP localhost:domain
named     27600 27601 isc-net-0         named   26u     IPv4             72374       0t0       UDP localhost:domain
named     27600 27601 isc-net-0         named   31u     IPv6             72377       0t0       UDP localhost:domain
named     27600 27601 isc-net-0         named   32u     IPv6             72378       0t0       UDP localhost:domain
named     27600 27602 isc-net-0         named   25u     IPv4             72373       0t0       UDP localhost:domain
named     27600 27602 isc-net-0         named   26u     IPv4             72374       0t0       UDP localhost:domain
named     27600 27602 isc-net-0         named   31u     IPv6             72377       0t0       UDP localhost:domain
named     27600 27602 isc-net-0         named   32u     IPv6             72378       0t0       UDP localhost:domain
named     27600 27603 isc-net-0         named   25u     IPv4             72373       0t0       UDP localhost:domain
named     27600 27603 isc-net-0         named   26u     IPv4             72374       0t0       UDP localhost:domain
named     27600 27603 isc-net-0         named   31u     IPv6             72377       0t0       UDP localhost:domain
named     27600 27603 isc-net-0         named   32u     IPv6             72378       0t0       UDP localhost:domain
named     27600 27604 isc-net-0         named   25u     IPv4             72373       0t0       UDP localhost:domain
named     27600 27604 isc-net-0         named   26u     IPv4             72374       0t0       UDP localhost:domain
named     27600 27604 isc-net-0         named   31u     IPv6             72377       0t0       UDP localhost:domain
```

Рис. 2.8: DNS слушает порт 53 (UDP)

2.2 Конфигурирование первичного DNS-сервера

В каталог `/etc/named` был скопирован шаблон `named.rfc1912.zones` и переименован в `vabazlov.net`.

Файл включён в основную конфигурацию `/etc/named.conf` через строку:

```
include "/etc/named/vabazlov.net";
```

В файле заменены стандартные локальные зоны на зоны домена `vabazlov.net`:

- прямая зона: `vabazlov.net`
- обратная зона: `1.168.192.in-addr.arpa`

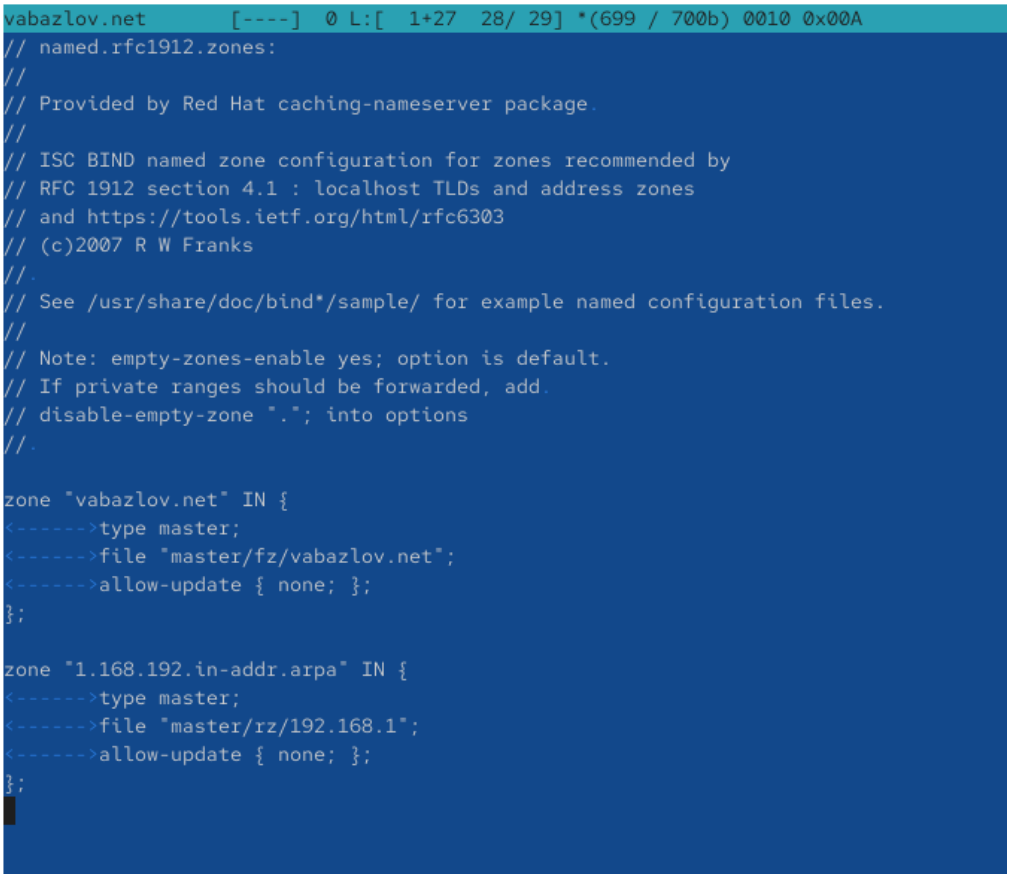


Рис. 2.9: Файл конфигурации зон vabazlov.net

В `/var/named` созданы каталоги:

- `master/fz` — файлы прямой зоны
- `master/rz` — файлы обратной зоны

Файлы шаблонов были скопированы и переименованы.

Файл **/var/named/master/fz/vabazlov.net** был изменён:

- задан домен `vabazlov.net`
- указан DNS-сервер `server.vabazlov.net`
- записи типа `A` указывают на адрес `192.168.1.1`
- добавлена запись сервера `ns`

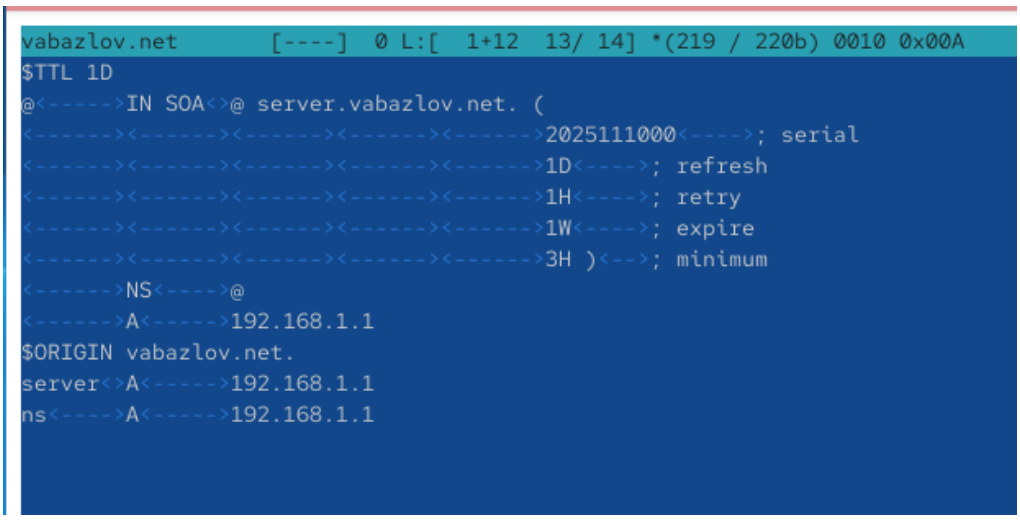


Рис. 2.10: Файл прямой зоны vabazlov.net

Файл **/var/named/master/rz/192.168.1** был изменён:

- домен обратной зоны `1.168.192.in-addr.arpa.`
- запись `PTR` сопоставляет IP-адресу доменное имя

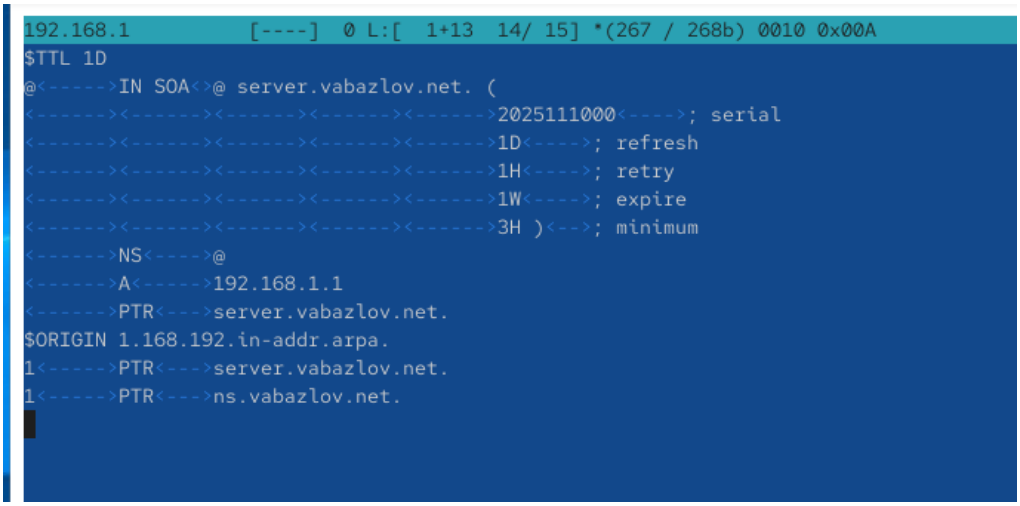


Рис. 2.11: Файл обратной зоны 192.168.1

После создания файлов были настроены права доступа и восстановлены SELinux-метки.

После перезапуска службы BIND сервер загрузил новые зоны:

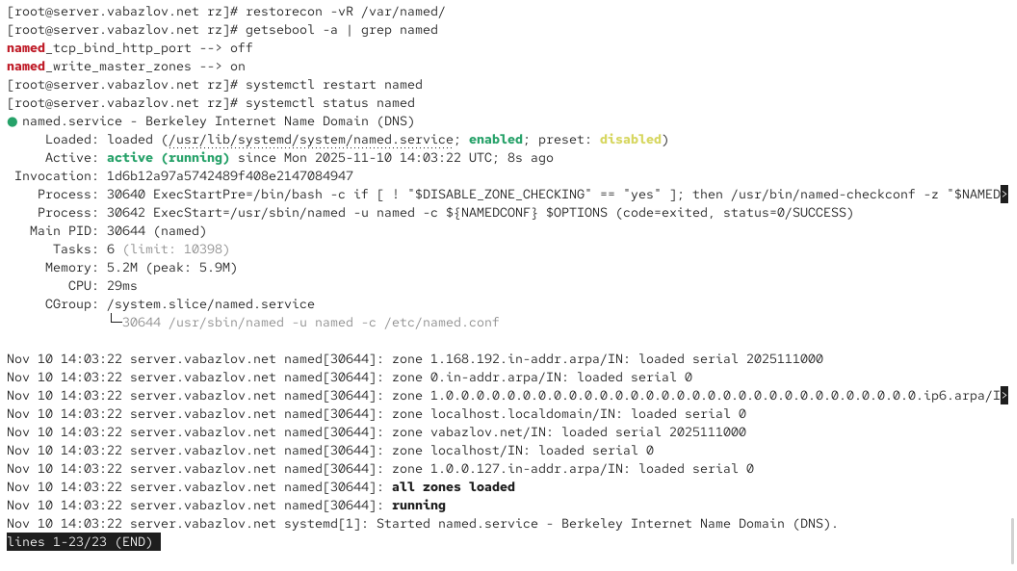


Рис. 2.12: Перезапуск named и загрузка зон

Запрос через `dig` для `ns.vabazlov.net` возвращает A-запись с IP-адресом сервера:

```
[root@server.vabazlov.net rz]# dig ns.vabazlov.net

; <<>> DiG 9.18.33 <<>> ns.vabazlov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54361
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ecf04997e5304528010000006911f0d5c1558a64a43ef101 (good)
;; QUESTION SECTION:
;ns.vabazlov.net.               IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Nov 10 14:04:05 UTC 2025
;; MSG SIZE  rcvd: 88

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

Рис. 2.13: Проверка dig

Команды `host` подтверждают корректную работу прямой и обратной зоны:

```
[root@server.vabazlov.net rz]# host -a vabazlov.net
Trying "vabazlov.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27892
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
vabazlov.net.           86400   IN      SOA     vabazlov.net. server.vabazlov.net. 2025111000 86400 3600 604800 10800
vabazlov.net.           86400   IN      NS      vabazlov.net.
vabazlov.net.           86400   IN      A       192.168.1.1

Received 103 bytes from 127.0.0.1#53 in 0 ms
[root@server.vabazlov.net rz]# host -t A vabazlov.net
vabazlov.net has address 192.168.1.1
[root@server.vabazlov.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.vabazlov.net.
1.1.168.192.in-addr.arpa domain name pointer ns.vabazlov.net.
[root@server.vabazlov.net rz]#
```

Рис. 2.14: Проверки host

2.3 Подготовка конфигурации для автоматического развёртывания

В каталоге `/vagrant/provision/server/dns` создана структура:

- `/etc/named/` — конфигурационные файлы
- `/var/named/master/` — зоны

В каталоге создан provisioning-скрипт `dns.sh`.

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

Рис. 2.15: Копирование конфигурации в Vagrant окружение

Содержимое `dns.sh` включает:

- установку пакетов
- копирование конфигураций
- настройку SELinux
- применение DNS-настроек к `eth0`

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install bind bind-utils
echo "Copy configuration files"
cp -R /vagrant/provision/server/dns/etc/* /etc
cp -R /vagrant/provision/server/dns/var/named/* /var/named
chown -R named:named /etc/named
chown -R named:named /var/named
restorecon -vR /etc
restorecon -vR /var/named
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent
echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1
echo "Change dns server address"
nmcli connection edit "eth0" <<EOF
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
EOF

systemctl restart NetworkManager
echo "Start named service"
systemctl enable named
systemctl start named
```

Рис. 2.16: dns.sh — provisioning-script

3 Контрольные вопросы

1. **Что такое DNS?**

   DNS — это распределённая система доменных имён, которая преобразует удобные для человека доменные имена (например, `example.com`) в IP-адреса, используемые сетевыми устройствами.

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

   Кэширующий DNS-сервер сохраняет ответы на DNS-запросы, сокращая время обработки повторных запросов и уменьшая нагрузку на внешние DNS-серверы.

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

   Прямая зона сопоставляет доменные имена IP-адресам (A-записи), тогда как обратная зона сопоставляет IP-адреса доменным именам (PTR-записи).

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

   Основные каталоги: `/etc/named.conf` — главный конфигурационный файл, `/etc/named/` — настройки зон, `/var/named/` — файлы DNS-зон. Файлы определяют поведение сервера, зоны доменов и записи.

5. **Что указывается в файле resolv.conf?**

   В `resolv.conf` указываются DNS-серверы, которые используются системой для выполнения DNS-запросов.

6. **Какие типы записи описания ресурсов есть в DNS и для чего они ис-**

пользуются?

Основные: `A` — соответствие имени IP-адресу, `PTR` — обратное соответствие IP-адреса имени, `NS` — указание DNS-серверов зоны, `SOA` — административная информация о зоне, `MX` — почтовые серверы.

7. **Для чего используется домен in-addr.arpa?**
   Для обратного DNS-разрешения — поиска доменного имени по IP-адресу.

8. **Для чего нужен демон named?**
   `named` — сервис BIND, который обрабатывает DNS-запросы и управляет DNS-зонами.

9. **В чём заключаются основные функции slave-сервера и master-сервера?**
   Master хранит оригинальные файлы зоны, slave получает их копии и обслуживает запросы в режиме репликации.

10. **Какие параметры отвечают за время обновления зоны?**
    В записи `SOA`: `serial`, `refresh`, `retry`, `expire`, `minimum`.

11. **Как обеспечить защиту зоны от скачивания и просмотра?**
    Ограничить доступ к зонам через `allow-transfer` и включить ACL.

12. **Какая запись RR применяется при создании почтовых серверов?**
    `MX` — Mail Exchanger.

13. **Как протестировать работу сервера доменных имён?**
    С помощью утилит `dig`, `nslookup`, `host`.

14. **Как запустить, перезапустить или остановить службу в системе?**
    Через `systemctl`: `start`, `restart`, `stop`, `status`.

15. **Как посмотреть отладочную информацию при запуске службы?**
    Использовать `systemctl status` или `journalctl -xe`.

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

    В журнале systemd (`journalctl`). Просмотр: `journalctl -f`, `journalctl -xe`.

17. **Как посмотреть, какие файлы использует процесс?**

    Использовать `lsof` или `ls /proc/<PID>/fd`. Например: `lsof -p <PID>`.

18. **Примеры изменения сетевого соединения с помощью nmcli.**

    Установка DNS: `nmcli connection modify eth0 ipv4.dns 127.0.0.1`
    Отключение авто-DNS: `nmcli connection modify eth0 ipv4.ignore-auto-dns yes`

19. **Что такое SELinux?**

    SELinux — механизм принудительного контроля доступа, ограничивающий действия процессов относительно файлов и ресурсов.

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

    Метка SELinux определяет политику доступа процесса к объектам и используется системой безопасности.

21. **Как восстановить контекст SELinux после изменений в файлах?**

    Командой `restorecon -Rv <путь>`.

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

    Использовать `audit2allow` для генерации модулей из логов блокировок SELinux.

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

    Это параметр, позволяющий включать или отключать определённые функции политик SELinux.

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

    Команда `getsebool -a`.

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

    `setsebool имя_переключателя on/off`, для постоянного изменения `setsebool -P`.

4 Заключение

В процессе выполнения работы был развёрнут и настроен первичный DNS-сервер на базе BIND. Созданы и сконфигурированы прямая и обратная зоны домена, внесены необходимые записи типа A и PTR. DNS-сервер был включён в автозагрузку, настроены сетевые параметры и межсетевой экран, обеспечена корректная работа SELinux. Проведено тестирование с использованием утилит `dig` и `host`, что подтвердило успешное разрешение доменных имён и функционирование зон.