

Отчёт по лабораторной работе 2

Настройка DNS-сервера

Гафоров Нурмухаммад

Содержание

1	Введение	6
1.1	Цель работы	6
2	Ход выполнения	7
2.1	Установка DNS-сервера	7
2.2	Анализ конфигурационных файлов	8
2.3	Запуск и проверка работы DNS-сервера	11
2.4	Назначение локального DNS-сервера по умолчанию	12
2.5	Открытие доступа к DNS в локальной сети	13
2.6	Настройка межсетевого экрана	14
2.7	Создание файла зон	15
2.8	Прямая зона	17
2.9	Обратная зона	17
2.10	Настройка SELinux и прав доступа	18
2.11	Проверка работы DNS-сервера	18
2.12	Подготовка файлов для автоматизации	20
3	Вывод	22
3.1	Контрольные вопросы	22
3.1.1	1. Что такое DNS?	22
3.1.2	2. Каково назначение кэширующего DNS-сервера?	22
3.1.3	3. Чем отличается прямая DNS-зона от обратной?	22
3.1.4	4. В каких каталогах и файлах располагаются настройки DNS-сервера?	23
3.1.5	5. Что указывается в файле resolv.conf?	23
3.1.6	6. Какие типы записи описания ресурсов есть в DNS?	23
3.1.7	7. Для чего используется домен in-addr.arpa?	23
3.1.8	8. Для чего нужен демон named?	23
3.1.9	9. В чём заключаются функции master-сервера и slave-сервера?	24
3.1.10	10. Какие параметры отвечают за время обновления зоны?	24
3.1.11	11. Как обеспечить защиту зоны от скачивания и просмотра?	24
3.1.12	12. Какая запись RR применяется при создании почтовых серверов?	24
3.1.13	13. Как протестировать работу сервера доменных имён?	24
3.1.14	14. Как запустить, перезапустить или остановить службу?	24
3.1.15	15. Как посмотреть отладочную информацию при запуске сервиса?	25

3.1.16	16. Где хранится отладочная информация?	25
3.1.17	17. Как посмотреть, какие файлы использует процесс? . . .	25
3.1.18	18. Примеры изменения сетевого соединения через nmcli: .	25
3.1.19	19. Что такое SELinux?	25
3.1.20	20. Что такое контекст (метка) SELinux?	25
3.1.21	21. Как восстановить контекст SELinux?	25
3.1.22	22. Как создать разрешающие правила из журналов?	26
3.1.23	23. Что такое булевый переключатель SELinux?	26
3.1.24	24. Как посмотреть список переключателей SELinux?	26
3.1.25	25. Как изменить состояние переключателя?	26

Список иллюстраций

2.1	Результат первичного DNS-запроса (внешний DNS)	8
2.2	Файл named.conf	9
2.3	Файл named.ca	10
2.4	Файлы named.localhost и named.loopback	11
2.5	Запрос через локальный DNS-сервер	12
2.6	Изменение DNS через nmcli	13
2.7	Изменение подсети в named.conf	14
2.8	DNS-порт прослушивается	15
2.9	Подключение файла зоны в named.conf	16
2.10	Файл зоны ngaforov.net	16
2.11	Файл прямой зоны	17
2.12	Файл обратной зоны	17
2.13	Настройка SELinux и прав доступа	18
2.14	Результат запроса dig	19
2.15	Результаты проверки зоны через host	20
2.16	Provisioning-скрипт dns.sh	21

Список таблиц

1 Введение

1.1 Цель работы

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

2 Ход выполнения

После загрузки виртуальной машины `server` был выполнен вход под ранее созданным пользователем и произведён переход в режим суперпользователя.

2.1 Установка DNS-сервера

Через диспетчер пакетов была выполнена установка пакетов `bind` и `bind-utils`. Для проверки работы DNS было осуществлено обращение к внешнему DNS-серверу с использованием утилиты `dig`. Команда отобразила:

- запрос типа A — резолвинг доменного имени в IPv4-адрес;
- секцию ANSWER SECTION с несколькими IP-адресами, принадлежащими домену;
- блок SERVER, содержащий IP-адрес DNS-сервера, обслужившего запрос.

```

Upgraded:
  bind-libs-32:9.18.33-4.el10_0.x86_64          bind-license-32:9.18.33-4.el10_0.noarch
  bind-utils-32:9.18.33-4.el10_0.x86_64
Installed:
  bind-32:9.18.33-4.el10_0.x86_64          bind-dnssec-utils-32:9.18.33-4.el10_0.x86_64

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46036
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.yandex.ru.                387     IN      A      5.255.255.77
www.yandex.ru.                387     IN      A      77.88.44.55
www.yandex.ru.                387     IN      A      77.88.55.88

;; Query time: 10 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Tue Nov 11 10:35:07 UTC 2025
;; MSG SIZE rcvd: 90

[root@server.ngaforov.net ~]# █

```

Рис. 2.1: Результат первичного DNS-запроса (внешний DNS)

2.2 Анализ конфигурационных файлов

Содержимое `/etc/resolv.conf` показало текущие DNS-сервера, используемые системой.

В конфигурационном файле `/etc/named.conf` обнаружены параметры, определяющие режим работы DNS-сервера: директории хранения, файлы статистики, политики доступа.


```

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

```

Рис. 2.2: Файл named.conf

Файл `/var/named/named.ca` содержит перечень корневых серверов DNS, необходимых для построения цепочки DNS-разрешения.

```

[root@server.ngaforov.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 named.ca

В файлах /var/named/named.localhost и /var/named/named.loopback описаны локальные зоны для обратного и прямого резолвинга адресов loopback-интерфейса.

```

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

```

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

2.3 Запуск и проверка работы DNS-сервера

DNS-сервер был запущен и добавлен в автозагрузку.

После этого была выполнена проверка с использованием `dig`, но теперь запрос направлялся непосредственно на локальный DNS-сервер по адресу 127.0.0.1. В результате:

- запрос был обработан без обращения напрямую к внешнему DNS,
- IP-адреса домена были успешно получены.

```

[root@server.ngaforov.net ~]#
[root@server.ngaforov.net ~]# systemctl start named
[root@server.ngaforov.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.ngaforov.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: 21071
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: db138c752bf1759601000006913123a4e921b2a2832fcdd (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

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

;; Query time: 3232 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Nov 11 10:38:50 UTC 2025
;; MSG SIZE rcvd: 118

[root@server.ngaforov.net ~]#

```

Рис. 2.5: Запрос через локальный DNS-сервер

2.4 Назначение локального DNS-сервера по умолчанию

Были изменены параметры сетевого интерфейса eth0 через NetworkManager. Сервер получил настройку использования 127.0.0.1 как DNS-сервера по умолчанию. После перезапуска NetworkManager это отразилось в файле /etc/resolv.conf.

```

[server.ngaforov.net ~]#
[root@server.ngaforov.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, i
pv4, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns
Enter 'ignore-auto-dns' value: yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.ngaforov.net ~]#
[root@server.ngaforov.net ~]#
[root@server.ngaforov.net ~]# systemctl restart NetworkManager
[root@server.ngaforov.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ngaforov.net
nameserver 127.0.0.1
[root@server.ngaforov.net ~]#

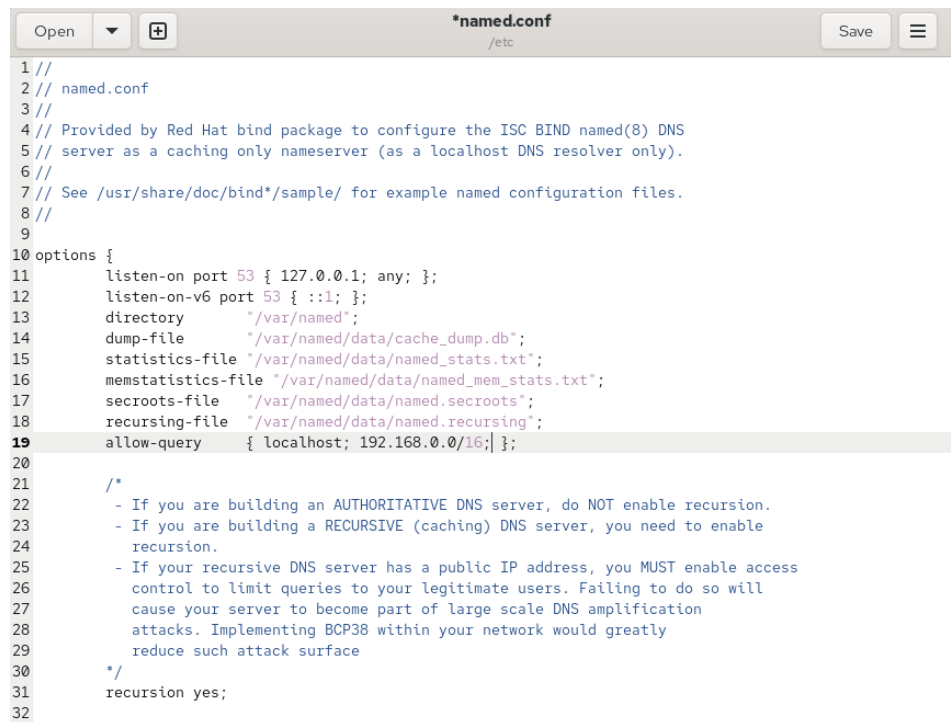
```

Рис. 2.6: Изменение DNS через nmcli

2.5 Открытие доступа к DNS в локальной сети

Для разрешения обработки запросов не только от localhost была внесена корректировка в /etc/named.conf:

- адрес, на котором принимает запросы DNS-сервер, расширен до any;
- разрешён доступ клиентам локальной сети 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     listen-on-v6 port 53 { ::1; };
13     directory      "/var/named";
14     dump-file       "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file   "/var/named/data/named.secroots";
18     recursing-file   "/var/named/data/named.recursing";
19     allow-query      { localhost; 192.168.0.0/16; };
20
21     /*
22     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
23     - If you are building a RECURSIVE (caching) DNS server, you need to enable
24     recursion.
25     - If your recursive DNS server has a public IP address, you MUST enable access
26     control to limit queries to your legitimate users. Failing to do so will
27     cause your server to become part of large scale DNS amplification
28     attacks. Implementing BCP38 within your network would greatly
29     reduce such attack surface
30     */
31     recursion yes;
32 }
```

Рис. 2.7: Изменение подсети в named.conf

2.6 Настройка межсетевого экрана

Через firewall был разрешён DNS-трафик, после чего проверено, что сервер прослушивает порт 53 по UDP.

```

[root@server.ngaforov.net ~]#
[root@server.ngaforov.net ~]# firewall-cmd --add-service=dns
success
[root@server.ngaforov.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.ngaforov.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  890          avahi  12u  IPv4           9220      0t0      UDP *:mdns
avahi-dae  890          avahi  13u  IPv6           9221      0t0      UDP *:mdns
chronyd    940          chrony  5u   IPv4           9321      0t0      UDP localhost:3
23
chronyd    940          chrony  6u   IPv6           9322      0t0      UDP localhost:3
23
named      27637         named  25u  IPv4          73768      0t0      UDP localhost:d
omain
named      27637         named  26u  IPv4          73769      0t0      UDP localhost:d
omain
named      27637         named  31u  IPv6          73772      0t0      UDP localhost:d
omain
named      27637         named  32u  IPv6          73773      0t0      UDP localhost:d
omain
named      27637 27638 isc-net-0    named  25u  IPv4          73768      0t0      UDP localhost:d
omain
named      27637 27638 isc-net-0    named  26u  IPv4          73769      0t0      UDP localhost:d

```

Рис. 2.8: DNS-порт прослушивается

2.7 Создание файла зон

В каталоге `/etc/named` был создан файл конфигурации DNS-зон, основанный на шаблоне `named.rfc1912.zones`. В конце основного конфигурационного файла `/etc/named.conf` была добавлена строка, подключающая новый файл описания зон.

```

43 };
44
45 logging {
46     channel default_debug {
47         file "data/named.run";
48         severity dynamic;
49     };
50 };
51
52 zone "." IN {
53     type hint;
54     file "named.ca";
55 };
56
57 include "/etc/named.rfc1912.zones";
58 include "/etc/named.root.key";
59 include "/etc/named/ngaforov.net";

```

Рис. 2.9: Подключение файла зоны в named.conf

Файл `/etc/named/ngaforov.net` был отредактирован: удалены стандартные зоны localhost, добавлены зоны прямого и обратного разрешения.



```

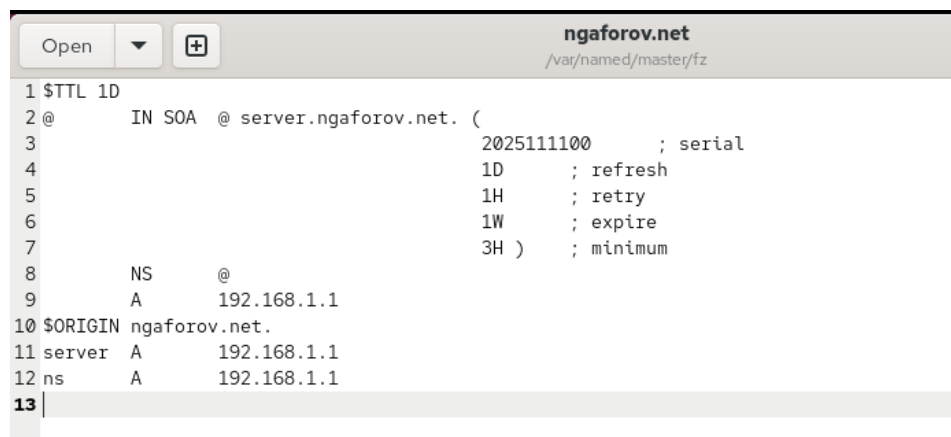
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ 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 "ngaforov.net" IN {
18     type master;
19     file "master/fz/ngaforov.net";
20     allow-update { none; };
21 };
22
23
24 zone "1.168.192.in-addr.arpa" IN {
25     type master;
26     file "master/rz/192.168.1";
27     allow-update { none; };
28 };

```

Рис. 2.10: Файл зоны ngaforov.net

2.8 Прямая зона

В каталоге `/var/named/master/fz` был создан файл зоны с именем `ngaforov.net`, содержащий описание SOA-записи и A-записей сервера и NS-записей.



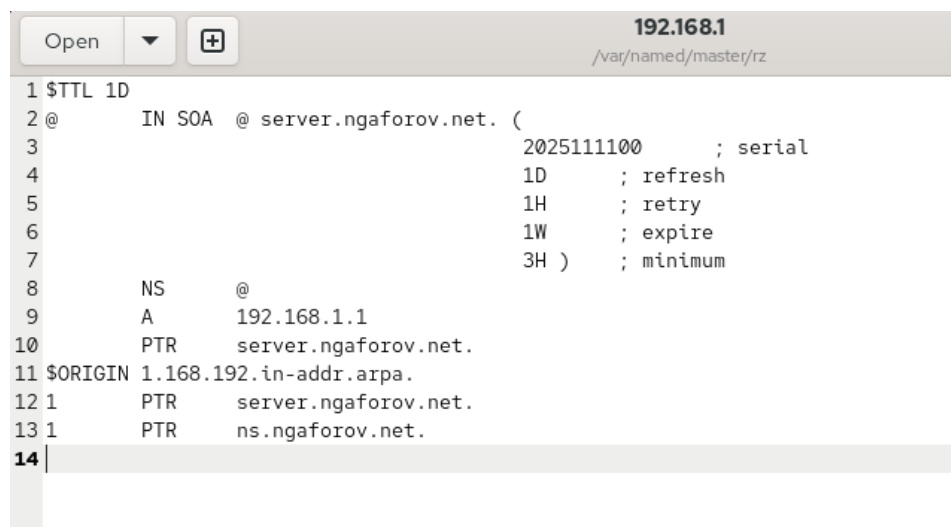
```
Open  ▾  +  ngaforov.net
/var/named/master/fz

1 $TTL 1D
2 @      IN SOA  @ server.ngaforov.net. (
3                                     2025111100      ; serial
4                                     1D              ; refresh
5                                     1H              ; retry
6                                     1W              ; expire
7                                     3H )            ; minimum
8      NS   @
9      A    192.168.1.1
10 $ORIGIN ngaforov.net.
11 server  A    192.168.1.1
12 ns      A    192.168.1.1
13 |
```

Рис. 2.11: Файл прямой зоны

2.9 Обратная зона

В каталоге `/var/named/master/rz` был создан файл обратной зоны с указанием соответствия адресов PTR-записям.



```
Open  ▾  +  192.168.1
/var/named/master/rz

1 $TTL 1D
2 @      IN SOA  @ server.ngaforov.net. (
3                                     2025111100      ; serial
4                                     1D              ; refresh
5                                     1H              ; retry
6                                     1W              ; expire
7                                     3H )            ; minimum
8      NS   @
9      A    192.168.1.1
10     PTR   server.ngaforov.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1       PTR   server.ngaforov.net.
13 1       PTR   ns.ngaforov.net.
14 |
```

Рис. 2.12: Файл обратной зоны

2.10 Настройка SELinux и прав доступа

Для корректной работы службы DNS права доступа к каталогам были переданы пользователю и группе named. После изменения контексты SELinux были восстановлены:

```
[root@server.ngaforov.net rz]#  
[root@server.ngaforov.net rz]# chown -R named:named /etc/named  
[root@server.ngaforov.net rz]# chown -R named:named /var/named  
[root@server.ngaforov.net rz]# restorecon -vR /etc  
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0  
Relabeled /etc/lvm/devices/backup/system.devices-20251111.102251.0005 from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0  
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:NetworkManager_etc_rw_t:s0  
Relabeled /etc/named.conf from unconfined_u:object_r:etc_t:s0 to unconfined_u:object_r:named_conf_t:s0  
[root@server.ngaforov.net rz]# restorecon -vR /var/named  
[root@server.ngaforov.net rz]# getsebool -a | grep named  
named_tcp_bind_http_port --> off  
named_write_master_zones --> on  
[root@server.ngaforov.net rz]# systemctl restart named  
[root@server.ngaforov.net rz]#
```

Рис. 2.13: Настройка SELinux и прав доступа

2.11 Проверка работы DNS-сервера

После перезапуска DNS-службы был выполнен тестовый запрос через dig, подтверждающий, что DNS-сервер корректно возвращает А-запись для ns.ngaforov.net.

```

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

; <<>> DiG 9.18.33 <<>> ns.ngaforov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46856
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7da307da4d02790c010000006913168ec8340a8170419f4e (good)
;; QUESTION SECTION:
;ns.ngaforov.net.                IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Nov 11 10:57:18 UTC 2025
;; MSG SIZE rcvd: 88

[root@server.ngaforov.net rz]# █

```

Рис. 2.14: Результат запроса dig

Затем с помощью утилиты host были проверены:

- вывод полной зоны,
- запись A,
- запись PTR.

```

[root@server.ngaforov.net rz]#
[root@server.ngaforov.net rz]# host -l ngaforov.net
ngaforov.net name server ngaforov.net.
ngaforov.net has address 192.168.1.1
ns.ngaforov.net has address 192.168.1.1
server.ngaforov.net has address 192.168.1.1
[root@server.ngaforov.net rz]# host -a ngaforov.net
Trying "ngaforov.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37449
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
ngaforov.net.                86400   IN      SOA     ngaforov.net. server.ngaforov.net. 2025111100 86400 3600 604800 1
0800
ngaforov.net.                86400   IN      NS      ngaforov.net.
ngaforov.net.                86400   IN      A       192.168.1.1

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

```

Рис. 2.15: Результаты проверки зоны через host

2.12 Подготовка файлов для автоматизации

В каталоге `/vagrant/provision/server/dns` были размещены конфигурационные файлы DNS, предназначенные для автоматизированного развёртывания сервера через Vagrant provisioning-скрипт.

Создан файл `dns.sh`, в который включены команды установки пакетов, настройки BIND, SELinux и сетевых параметров.

```

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

```

Рис. 2.16: Provisioning-скрипт dns.sh

3 Вывод

В ходе работы был развёрнут и настроен первичный DNS-сервер BIND. Созданы прямые и обратные зоны, выполнена корректировка SELinux и проверена работоспособность с помощью `dig` и `host`. DNS-сервер корректно обрабатывает запросы и функционирует в роли master-сервера.

3.1 Контрольные вопросы

3.1.1 1. Что такое DNS?

DNS (Domain Name System) — распределённая система, преобразующая доменные имена в IP-адреса и обратно.

3.1.2 2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер запрашивает данные у внешних DNS и временно сохраняет их, уменьшая количество запросов в интернет и ускоряя последующие ответы.

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

Прямая зона преобразует доменное имя → в IP-адрес (A-записи).
Обратная зона преобразует IP-адрес → в доменное имя (PTR-записи).

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

- `/etc/named.conf` — основной конфигурационный файл BIND.
- `/etc/named/` — дополнительные файлы настроек зон.
- `/var/named/` — файлы DNS-зон (прямые и обратные зоны).

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

Содержит список DNS-серверов, используемых системой для резолвинга.

3.1.6 6. Какие типы записи описания ресурсов есть в DNS?

- **A** — доменное имя → IPv4-адрес.
- **AAAA** — доменное имя → IPv6-адрес.
- **NS** — указание DNS-серверов зоны.
- **SOA** — сведения о зоне (серийный номер, времена обновления).
- **PTR** — обратное преобразование адреса в имя.
- **MX** — почтовый сервер домена.
- **CNAME** — алиас (псевдоним доменного имени).

3.1.7 7. Для чего используется домен `in-addr.arpa`?

Для обратного DNS-разрешения (поиск имени по IP-адресу).

3.1.8 8. Для чего нужен демон `named`?

`named` — служба BIND, обрабатывающая DNS-запросы.

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

- **Master** хранит оригинальные файлы зон и разрешает изменения.
- **Slave** получает копию зоны с master-сервера и обеспечивает отказоустойчивость.

3.1.10 10. Какие параметры отвечают за время обновления зоны?

В секции **SOA**: - refresh — интервал обновления, - retry — повторная попытка, - expire — срок актуальности зоны на slave.

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

Ограничить доступ настройками allow-transfer { ... } и allow-query { ... } в зоне.

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

MX (Mail eXchanger).

3.1.13 13. Как протестировать работу сервера доменных имён?

Через утилиты: - dig - host - nslookup

3.1.14 14. Как запустить, перезапустить или остановить службу?

Через systemd: - systemctl start - systemctl restart - systemctl stop

3.1.15 15. Как посмотреть отладочную информацию при запуске сервиса?

Просмотреть лог: `journalctl -xe`

3.1.16 16. Где хранится отладочная информация?

В системных логах `journald`: `journalctl -u`

3.1.17 17. Как посмотреть, какие файлы использует процесс?

Команда: `lsof -p`

3.1.18 18. Примеры изменения сетевого соединения через nmcli:

- просмотр соединений: `nmcli connection show`
- изменение DNS: `nmcli connection edit eth0`

3.1.19 19. Что такое SELinux?

SELinux — подсистема безопасности, контролирующая доступ процессов к ресурсам.

3.1.20 20. Что такое контекст (метка) SELinux?

Это атрибут файла или процесса, определяющий уровень доступа.

3.1.21 21. Как восстановить контекст SELinux?

`restorecon -vR /путь`

3.1.22 22. Как создать разрешающие правила из журналов?

С помощью: `audit2allow`

3.1.23 23. Что такое булевый переключатель SELinux?

Настройка SELinux, регулирующая поведение политики безопасности.

3.1.24 24. Как посмотреть список переключателей SELinux?

`getsebool -a`

3.1.25 25. Как изменить состояние переключателя?

`setsebool`

`on/off`