

Настройка DNS-сервера BIND

Лабораторная работа №2

Гафоров Нурмухаммад

11.11.2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Получить навыки установки и конфигурирования **DNS-сервера BIND**, освоить работу с прямыми и обратными зонами.

Ход выполнения

Установка BIND и проверка DNS

- Установлены пакеты bind и bind-utils.
- Выполнен первый DNS-запрос с помощью dig.
- Получены записи домена и IP-адреса внешнего DNS.

```
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)
```

Анализ конфигурационных файлов

- `/etc/resolv.conf` — DNS сервера по умолчанию.
- `/etc/named.conf` — основной конфигурационный файл BIND.
- `/var/named/*` — шаблоны зон и системные зоны.

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

Запуск и проверка DNS-сервера

- DNS-служба запущена и добавлена в автозагрузку.
- Проверен локальный DNS-резолвинг (**dig @127.0.0.1**).

```
[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: db138c752bf17596010000006913123a4e921b2a2832fcdd (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 ~]#
```

Назначение DNS-сервера по умолчанию

- Настроено сетевое соединение `eth0` через `nmcli`.
- Установлен DNS: `127.0.0.1`.
- Перезапущен `NetworkManager`.

```
[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-lx, 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 ~]# █
```


Открытие DNS для локальной сети

- В `named.conf` разрешены запросы из сети `192.168.0.0/16`.
- В firewall разрешён сервис DNS.



```
*named.conf
/etc

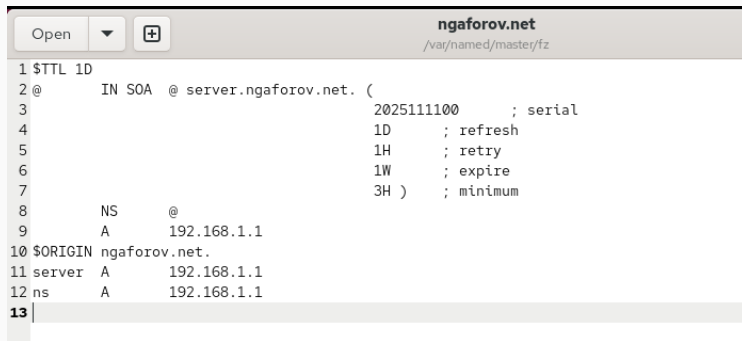
1 //
2 // named.conf
3 //
4 // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5 // server as a caching only nameserver (as a localhost DNS resolver only).
6 //
7 // See /usr/share/doc/bind*/sample/ for example named configuration files.
8 //
9
10 options {
11     listen-on port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

Создание файла зон

- Создан новый файл зоны.
- Подключён в `/etc/named.conf`.

```
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";
```

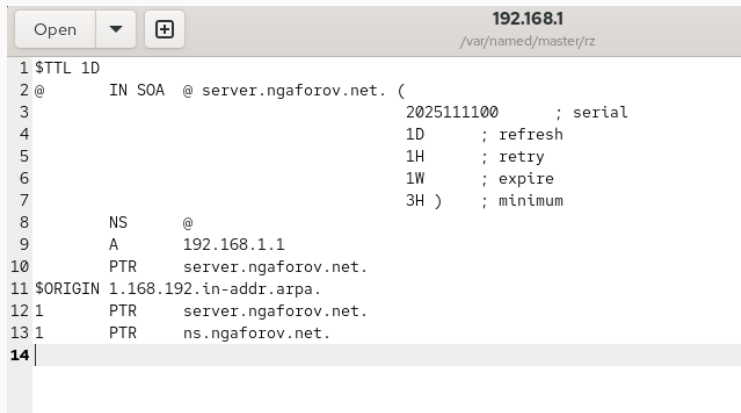
- Создана зона `ngaforov.net`.
- Добавлены записи: SOA, NS, A.



```
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. 7: Файл прямой зоны

- Создана зона 1.168.192.in-addr.arpa.
- Добавлены PTR-записи.



The screenshot shows a DNS configuration editor window. At the top, there is a header bar with the filename **192.168.1** and the path `/var/named/master/rz`. Below the header, the editor displays the contents of the reverse zone file. The file starts with a comment line `1 $TTL 1D`. The main section is enclosed in parentheses and begins with `2 @ IN SOA @ server.ngaforov.net. (`. This is followed by several parameters: `3 2025111100 ; serial`, `4 1D ; refresh`, `5 1H ; retry`, `6 1W ; expire`, and `7 3H) ; minimum`. After the closing parenthesis, there are three record lines: `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.`, and `13 1 PTR ns.ngaforov.net.`. The line number **14** is at the end of the visible text, with a cursor positioned at the start of the next line.

```
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. 8: Файл обратной зоны

- Исправлены контексты файлов через **restorecon**.
- Разрешена запись в зоны с помощью **setsebool**.

```
[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. 9: SELinux и права

- `dig ns.ngaforov.net` — возвращает IP.
- `host -l ngaforov.net` — выводит записи зоны.

```
[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]#
```

- Конфигурационные файлы сохранены в `/vagrant/provision/server/dns`.
- Создан скрипт `dns.sh`, выполняющий автоматическую настройку.

```
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
```

Выводы

- Установлен DNS-сервер BIND.
- Настроены прямые и обратные зоны.
- Проверена работа DNS через **dig** и **host**.
- Выполнена подготовка автоматического provisioning.

DNS-сервер функционирует как **master-сервер зоны** и корректно обрабатывает запросы.