

Администрирование сетевых подсистем

Настройка и анализ работы DNS-сервера BIND

Сейдалиев Тагьетдин Ровшенович

19 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить установку, конфигурирование и анализ работы DNS-сервера BIND, а также автоматизацию его настройки во внутреннем окружении VM.

Установка DNS-сервера

Проверка работы внешнего DNS

- Установлены пакеты bind и bind-utils
- Выполнен тест dig для внешнего DNS
- Проанализирована структура DNS-ответа

```
bind-32:9.18.33-4.el10_0.x86_64      bind-dnssec-utils-32:9.18.33-4.el10_0.x86_64

Installed:

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26292
;; 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.                427     IN      A      5.255.255.77
www.yandex.ru.                427     IN      A      77.88.55.88
www.yandex.ru.                427     IN      A      77.88.44.55

;; Query time: 13 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Nov 19 18:24:51 MSK 2025
```

Конфигурирование кэширующего DNS

Конфигурация resolv.conf и named.conf

- Использование внешнего nameserver
- Настройки listen-on и allow-query
- Структура служебных файлов

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

Файлы корневых и локальных зон

- named.ca — корневые DNS-серверы
- named.localhost — локальная зона
- named.loopback — обратная зона

```
[root@server.trseidaliev.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.trseidaliev.net ~]# cat /var/named/named.loopback
$TTL 1D
@      IN SOA  @ rname.invalid. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
```

Проверка работы локального DNS

- Корректный ответ сервера
- Работает кэширование запросов

```
[root@server.trseidaliev.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: 49715
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: acebd56ac6f6e55c01000000691de20350b1171eb49893b5 (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      77.88.44.55
www.yandex.ru.                 600     IN      A      77.88.55.88

;; Query time: 3082 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
```

Настройка DNS через nmcli

- Включён ignore-auto-dns
- Установлен DNS = 127.0.0.1
- resolv.conf обновлён

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

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

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

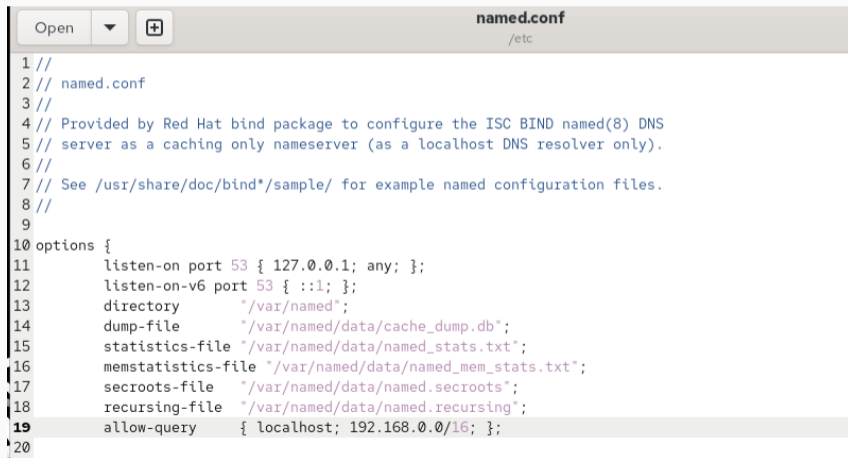
Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, eth
tool, match, 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' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.trseidaliev.net ~]#
[root@server.trseidaliev.net ~]# systemctl restart NetworkManager
[root@server.trseidaliev.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 127.0.0.1
```

Настройка доступа сети

Правки named.conf

- Прослушивание на всех интерфейсах
- Разрешение запросов от 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 }
```

Настройка firewall и проверка порта

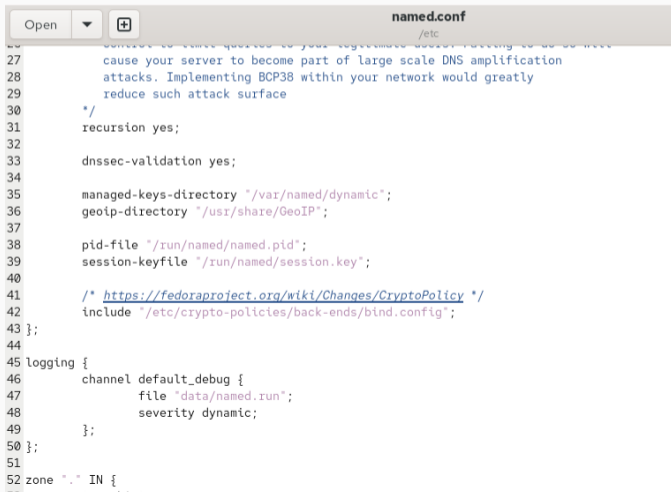
- Открыт порт 53 TCP/UDP
- named слушает порт корректно

```
[root@server.trseidaliev.net ~]#  
[root@server.trseidaliev.net ~]# firewall-cmd --add-service=dns  
success  
[root@server.trseidaliev.net ~]# firewall-cmd --add-service=dns --permanent  
success  
[root@server.trseidaliev.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  881                avahi  12u  IPv4            9098      0t0      UDP *:mdns  
avahi-dae  881                avahi  13u  IPv6            9099      0t0      UDP *:mdns  
chronyd   12441                   chrony  5u   IPv4           38624      0t0      UDP localhost:323  
chronyd   12441                   chrony  6u   IPv6           38625      0t0      UDP localhost:323  
named     15267                   named   25u  IPv4           75500      0t0      UDP localhost:domain  
  
named     15267                   named   26u  IPv4           75501      0t0      UDP localhost:domain  
  
named     15267                   named   31u  IPv6           75504      0t0      UDP localhost:domain  
  
named     15267                   named   32u  IPv6           75505      0t0      UDP localhost:domain  
  
named     15267 15268 isc-net-0    named   25u  IPv4           75500      0t0      UDP localhost:domain  
  
named     15267 15268 isc-net-0    named   26u  IPv4           75501      0t0      UDP localhost:domain  
  
named     15267 15268 isc-net-0    named   31u  IPv6           75504      0t0      UDP localhost:domain
```

Настройка первичного DNS-сервера

Подключение файла зон

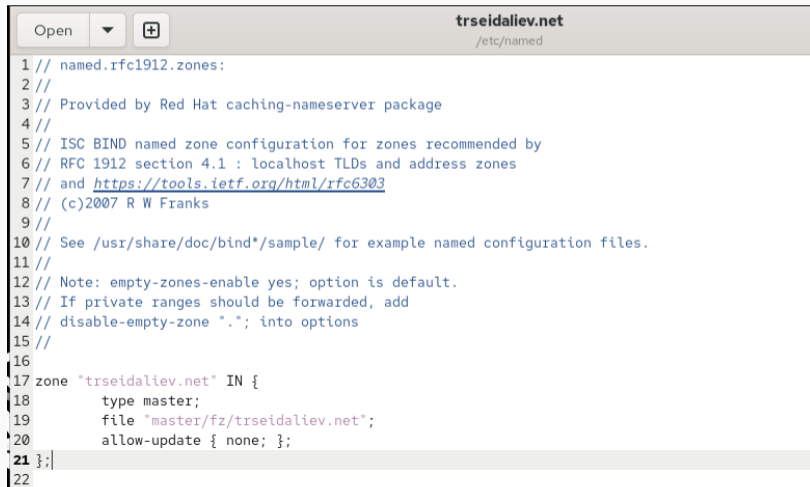
- Скопирован шаблон зон
- Добавлен include для файла trseidalev.net



```
named.conf
/etc
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
33 dnssec-validation yes;
34
35 managed-keys-directory "/var/named/dynamic";
36 geoip-directory "/usr/share/GeoIP";
37
38 pid-file "/run/named/named.pid";
39 session-keyfile "/run/named/session.key";
40
41 /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
42 include "/etc/crypto-policies/back-ends/bind.config";
43 };
44
45 logging {
46     channel default_debug {
47         file "data/named.run";
48         severity dynamic;
49     };
50 };
51
52 zone "." IN {
```

Прямая и обратная зона

- Создана зона trseidalev.net
- Создана обратная зона 1.168.192.in-addr.arpa

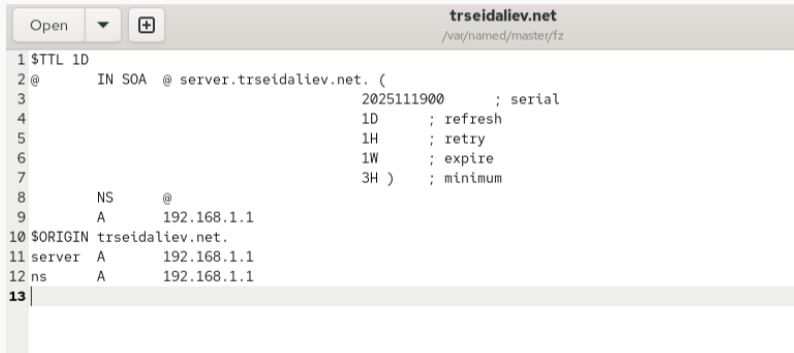


The screenshot shows a text editor window with the title bar "trseidalev.net" and the file path "/etc/named". The editor contains a BIND configuration file with the following content:

```
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 "trseidalev.net" IN {
18     type master;
19     file "master/fz/trseidalev.net";
20     allow-update { none; };
21 };
22
```

Файлы мастер-зон

- SOA-запись
- NS и A-записи
- \$ORIGIN trseidalev.net.



```
trseidalev.net
/var/named/master/fz

1 $TTL 1D
2 @      IN SOA  @ server.trseidalev.net. (
3                                     2025111900      ; serial
4                                     1D              ; refresh
5                                     1H              ; retry
6                                     1W              ; expire
7                                     3H )            ; minimum
8      NS      @
9      A      192.168.1.1
10 $ORIGIN trseidalev.net.
11 server A    192.168.1.1
12 ns     A    192.168.1.1
13
```

Рис. 10: fz зона

- PTR-записи
- Корректный SOA
- Соответствие IP ↔ имя

```
1 $TTL 1D
2 @      IN SOA  @ server.trseidaliev.net. (
3          2025111900      ; serial
4          1D              ; refresh
5          1H              ; retry
6          1W              ; expire
7          3H )            ; minimum
8      NS      @
9      A       192.168.1.1
10     AAAA    ::1
11     PTR     server.trseidaliev.net.
12 $ORIGIN 1.168.192.in-addr.arpa.
13 1        PTR     server.trseidaliev.net.
14 1        PTR     ns.trseidaliev.net.
15
```

SELinux и права

- Восстановлены контексты
- Разрешена запись в мастер-зоны
- Проверены bool-переключатели

```
[root@server.trseidaliev.net rz]#  
[root@server.trseidaliev.net rz]# chown -R named:named /etc/named  
[root@server.trseidaliev.net rz]# chown -R named:named /var/named  
[root@server.trseidaliev.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-20251119.071804.0005 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.trseidaliev.net rz]# restorecon -vR /var/named/  
[root@server.trseidaliev.net rz]# getsebool -a | grep named  
named_tcp_bind_http_port --> off  
named_write_master_zones --> on  
[root@server.trseidaliev.net rz]# systemctl restart named  
[root@server.trseidaliev.net rz]#
```

Рис. 12: selinux вывод

Анализ работы DNS

- ns.trseidalev.net → 192.168.1.1
- Корректная A-запись

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

; <<>> DiG 9.18.33 <<>> ns.trseidalev.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26650
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b8e7b41eaf90d9f801000000691de62574b52c85dba228e9 (good)
;; QUESTION SECTION:
;ns.trseidalev.net.          IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
```

Проверка host

- Листинг зоны
- ANY-запросы
- PTR-записи

```
[root@server.trseidaliyev.net rz]# host -l trseidaliyev.net
trseidaliyev.net name server trseidaliyev.net.
trseidaliyev.net has address 192.168.1.1
ns.trseidaliyev.net has address 192.168.1.1
server.trseidaliyev.net has address 192.168.1.1
[root@server.trseidaliyev.net rz]# host -a trseidaliyev.net
Trying "trseidaliyev.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45820
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
trseidaliyev.net.         86400   IN      SOA      trseidaliyev.net. server.trseidaliyev.net. 2025111900 86400 3600 604800
10800
trseidaliyev.net.         86400   IN      NS       trseidaliyev.net.
trseidaliyev.net.         86400   IN      A        192.168.1.1

Received 106 bytes from 127.0.0.1#53 in 0 ms
[root@server.trseidaliyev.net rz]# host -t A trseidaliyev.net
trseidaliyev.net has address 192.168.1.1
[root@server.trseidaliyev.net rz]# host -t PTR 192.168.1.1
```

Итоги работы

- Настроен кэширующий и первичный DNS-сервер BIND
- Созданы прямая и обратная зоны
- DNS успешно обслуживает запросы
- Настройки автоматизированы через `dns.sh`
- Проверены `dig`, `host` и работа SELinux