Администрирование сетевых подсистем

Настройка DNS-сервера

Метвалли Ахмед Фарг Набеех

19 сентября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Приобрести практические навыки по установке и конфигурации DNS-сервера, а также закрепить теоретические знания о принципах работы системы доменных имён.

Выполнение лабораторной работы

Развертывание DNS-сервера

```
Installed:
  bind-32:9.18.33-3.el10.x86_64    bind-dnssec-utils-32:9.18.33-3.el10.x86_64

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3169
;; 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.          578     IN      A       77.88.44.55
www.yandex.ru.          578     IN      A       77.88.55.88
www.yandex.ru.          578     IN      A       5.255.255.77

;; Query time: 18 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Sep 17 08:25:49 UTC 2025
;; MSG SIZE  rcvd: 90

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

Анализ конфигурации

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

Конфигурация кэширующего DNS

```
[root@server.ahmedfarg.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.ahmedfarg.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: 40729
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c8b7d8364bc561730100000068ca70f1ece672ac66f65153 (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: 4075 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Sep 17 08:27:29 UTC 2025
;; MSG SIZE  rcvd: 118

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


Рис. 2: Сравнение dig запросов

Настройка подключения

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.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, ip
v4, 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.ahmedfarg.net ~]# systemctl restart NetworkManager
[root@server.ahmedfarg.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ahmedfarg.net
nameserver 127.0.0.1
[root@server.ahmedfarg.net ~]#
```

Рис. 4: Настройка подключения через nmcli

Изменения в конфигурации

```
//
// 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
```

Рис. 5: Изменения в named.conf

Проверка работы сервиса

```
[root@server.ahmedfarg.net ~]# gedit /etc/named.conf
[root@server.ahmedfarg.net ~]# firewall-cmd --add-service=dns
success
[root@server.ahmedfarg.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.ahmedfarg.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   887                        avahi   12u     IPv4              7922       0t0        UDP *:mdns
avahi-dae   887                        avahi   13u     IPv6              7923       0t0        UDP *:mdns
chronyd     949                       chrony    5u     IPv4              8721       0t0        UDP localhost:32
3
chronyd     949                       chrony    6u     IPv6              8722       0t0        UDP localhost:32
3
named     28507                         named   25u     IPv4             77234       0t0        UDP localhost:do
main
named     28507                         named   26u     IPv4             77235       0t0        UDP localhost:do
main
named     28507                         named   31u     IPv6             77238       0t0        UDP localhost:do
main
named     28507                         named   32u     IPv6             77239       0t0        UDP localhost:do
main
named     28507 28508 isc-net-0         named   25u     IPv4             77234       0t0        UDP localhost:do
```

Рис. 6: Проверка работы DNS через lsof

Настройка основного DNS-сервера

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and https://tools.ietf.org/html/rfc6303
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add
// disable-empty-zone "."; into options
//

zone "ahmedfarg.net" IN {
        type master;
        file "master/fz/ahmedfarg.net";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "master/rz/192.168.1";
        allow-update { none; };
};
```

Файл прямой зоны

Open

ahmedfarg.net
/var/named/master/fz

```
1  $TTL 1D
2  @       IN SOA  @ server.ahmedfarg.net. (
3                                           2025091700      ; serial
4                                           1D      ; refresh
5                                           1H      ; retry
6                                           1W      ; expire
7                                           3H )    ; minimum
8          NS      @
9          A       192.168.1.1
10 $ORIGIN ahmedfarg.net.
11 server  A       192.168.1.1
12 ns      A       192.168.1.1
13
```

Рис. 8: Файл прямой зоны ahmedfarg.net

Файл обратной зоны

Open

192.168.1
/var/named/master/rz

```
1 $TTL 1D
2 @       IN SOA  @ server.ahmedfarg.net. (
3                                         2025091700      ; serial
4                                         1D      ; refresh
5                                         1H      ; retry
6                                         1W      ; expire
7                                         3H )    ; minimum
8         NS      @
9         A       192.168.1.1
10        PTR     server.ahmedfarg.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1      PTR     server.ahmedfarg.net.
13 1      PTR     ns.ahmedfarg.net.
14
```

Рис. 9: Файл обратной зоны 192.168.1

Настройка SELinux и прав

```
[root@server.ahmedfarg.net rz]#
[root@server.ahmedfarg.net rz]# chown -R named:named /etc/named
[root@server.ahmedfarg.net rz]# chown -R named:named /var/named
[root@server.ahmedfarg.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-20250917.080347.0005 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 unc
onfined_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.ahmedfarg.net rz]# restorecon -vR /var/named/
[root@server.ahmedfarg.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ahmedfarg.net rz]# systemctl restart named
[root@server.ahmedfarg.net rz]#
```

Рис. 10: Настройка прав и SELinux

Проверка работоспособности

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

; <<>> DiG 9.18.33 <<>> ns.ahmedfarg.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40098
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 73b5b079eeb4e4240100000068ca757f64fba67aa528b284 (good)
;; QUESTION SECTION:
;ns.ahmedfarg.net.              IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Sep 17 08:46:55 UTC 2025
;; MSG SIZE  rcvd: 89

[root@server.ahmedfarg.net rz]#
```

Проверка записей зоны

```
[root@server.ahmedfarg.net rz]# host -l ahmedfarg.net
ahmedfarg.net name server ahmedfarg.net.
ahmedfarg.net has address 192.168.1.1
ns.ahmedfarg.net has address 192.168.1.1
server.ahmedfarg.net has address 192.168.1.1
[root@server.ahmedfarg.net rz]# host -a ahmedfarg.net
Trying "ahmedfarg.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23958
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
ahmedfarg.net.          86400   IN      SOA     ahmedfarg.net. server.ahmedfarg.net. 2025091700 86400 3600 604800
10800
ahmedfarg.net.          86400   IN      NS      ahmedfarg.net.
ahmedfarg.net.          86400   IN      A       192.168.1.1

Received 104 bytes from 127.0.0.1#53 in 1 ms
[root@server.ahmedfarg.net rz]# host -t A ahmedfarg.net
ahmedfarg.net has address 192.168.1.1
[root@server.ahmedfarg.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ahmedfarg.net.
1.1.168.192.in-addr.arpa domain name pointer server.ahmedfarg.net.
[root@server.ahmedfarg.net rz]#
```

Рис. 12: Проверка зоны через host

Выводы по проделанной работе

Вывод

В ходе работы был установлен и сконфигурирован DNS-сервер на базе **BIND**. Настроены прямая и обратная зоны, протестирована корректность работы резолвера и кэширующего режима. Создан скрипт для Vagrant, обеспечивший автоматизацию настройки и сокращение времени развертывания.