Лабораторная работа

Номер 2

Андрюшин Н. С.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

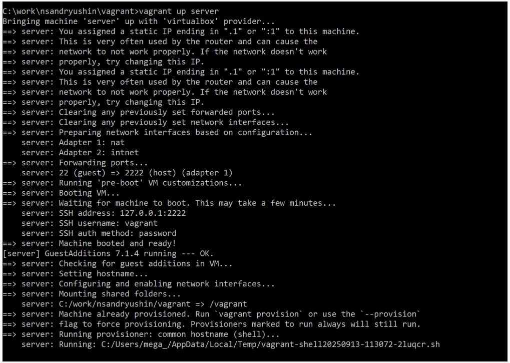
- Андрюшин Никита Сергеевич
- Студент
- Российский университет дружбы народов

Цель

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

Запуск ВМ

Для начала запустим виртуальную машину через vagrant

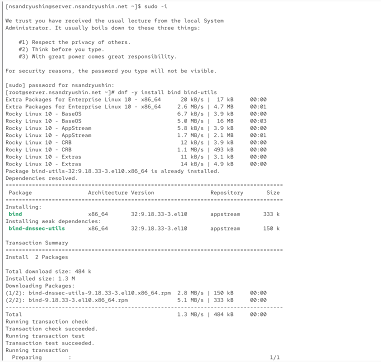


```
C:\work\nsandryushin\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
    server: Adapter 1: nat
    server: Adapter 2: intnet
==> server: Forwarding ports...
    server: 22 (guest) => 2222 (host) (adapter 1)
==> server: Running 'pre-boot' VM customizations...
==> server: Booting VM...
==> server: Waiting for machine to boot. This may take a few minutes...
    server: SSH address: 127.0.0.1:2222
    server: SSH username: vagrant
    server: SSH auth method: password
==> server: Machine booted and ready!
[server] GuestAdditions 7.1.4 running --- OK.
==> server: Checking for guest additions in VM...
==> server: Setting hostname...
==> server: Configuring and enabling network interfaces...
==> server: Mounting shared folders...
    server: C:/work/nsandryushin/vagrant => /vagrant
==> server: Machine already provisioned. Run `vagrant provision` or use the `--provision`
==> server: flag to force provisioning. Provisioners marked to run always will still run.
==> server: Running provisioner: common hostname (shell)...
    server: Running: C:/Users/mega_/AppData/Local/Temp/vagrant-shell20250913-113072-2luqcr.sh
```

Рис. 1: Запуск ВМ

Скачивание пакетов

Теперь скачаем пакет bind utils

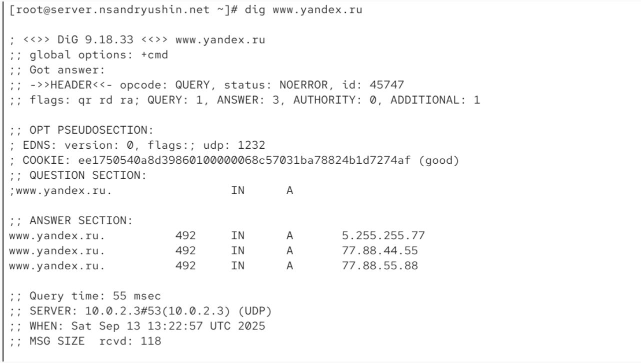


```
[nsandryushin@server.nsandryushin.net ~]$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for nsandryushin:
[root@server.nsandryushin.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 10 - x86_64      20 kB/s |  17 kB     00:00
Extra Packages for Enterprise Linux 10 - x86_64     2.6 MB/s | 4.7 MB     00:01
Rocky Linux 10 - BaseOS                             6.7 kB/s | 3.9 kB     00:00
Rocky Linux 10 - BaseOS                             5.0 MB/s |  16 MB     00:03
Rocky Linux 10 - AppStream                          5.8 kB/s | 3.9 kB     00:00
Rocky Linux 10 - AppStream                          1.7 MB/s | 2.1 MB     00:01
Rocky Linux 10 - CRB                                 12 kB/s | 3.9 kB     00:00
Rocky Linux 10 - CRB                                1.1 MB/s | 493 kB     00:00
Rocky Linux 10 - Extras                              11 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                              14 kB/s | 4.9 kB     00:00
Package bind-utils-32:9.18.33-3.el10.x86_64 is already installed.
Dependencies resolved.
====================================================================================
 Package                 Architecture Version                 Repository       Size
====================================================================================
Installing:
 bind                    x86_64       32:9.18.33-3.el10       appstream       333 k
Installing weak dependencies:
 bind-dnssec-utils       x86_64       32:9.18.33-3.el10       appstream       150 k

Transaction Summary
====================================================================================
Install  2 Packages

Total download size: 484 k
Installed size: 1.3 M
Downloading Packages:
(1/2): bind-dnssec-utils-9.18.33-3.el10.x86_64.rpm  2.8 MB/s | 150 kB     00:00
(2/2): bind-9.18.33-3.el10.x86_64.rpm               5.1 MB/s | 333 kB     00:00
------------------------------------------------------------------------------------
Total                                               1.3 MB/s | 484 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                            1/1
```

Рис. 2: Скачивание пакетов

dig ya.ru

Используем команду dig для проверки сервисов яндекса

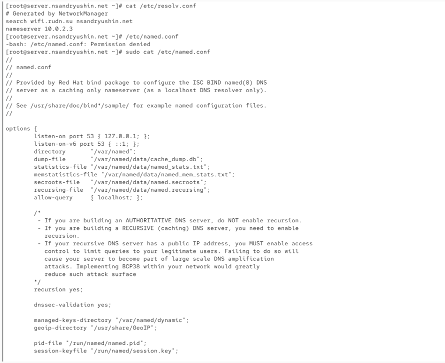


```
[root@server.nsandryushin.net ~]# dig www.yandex.ru

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45747
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ee1750540a8d39860100000068c57031ba78824b1d7274af (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          492     IN      A       5.255.255.77
www.yandex.ru.          492     IN      A       77.88.44.55
www.yandex.ru.          492     IN      A       77.88.55.88

;; Query time: 55 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat Sep 13 13:22:57 UTC 2025
;; MSG SIZE  rcvd: 118
```

Рис. 3: dig ya.ru

Файлы конфигурации

Посморим на содержание файлов конфигурации dns в etc

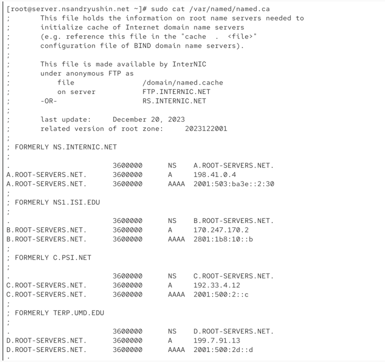


```
[root@server.nsandryushin.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search wifi.rudn.su nsandryushin.net
nameserver 10.0.2.3
[root@server.nsandryushin.net ~]# /etc/named.conf
-bash: /etc/named.conf: Permission denied
[root@server.nsandryushin.net ~]# sudo cat /etc/named.conf
//
// 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";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
```

Рис. 4: Файлы конфигурации

named.ca

Просморим теперь файл named.ca

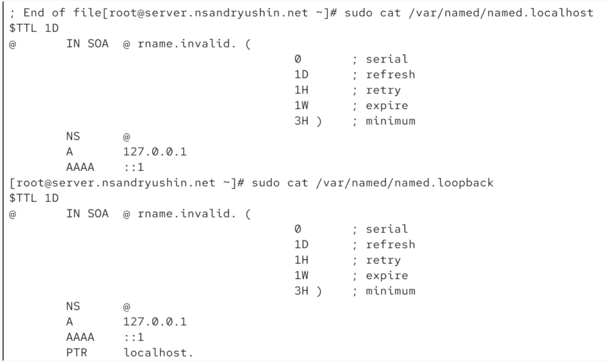


```
[root@server.nsandryushin.net ~]# sudo cat /var/named/named.ca
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name 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
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2d::d
```

Рис. 5: named.ca

named.localhost и named.loopback

Содержимое named.localhost и named.loopback

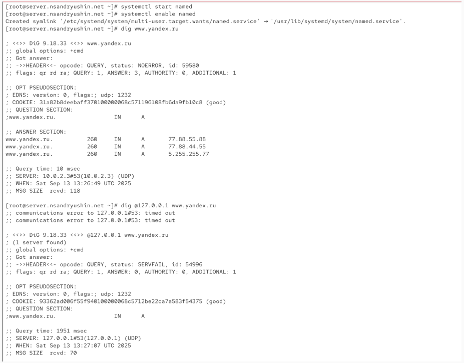


```
; End of file[root@server.nsandryushin.net ~]# sudo cat /var/named/named.localhost
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
[root@server.nsandryushin.net ~]# sudo 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.
```

Рис. 6: named.localhost и named.loopback

Запуск named

Запустим теперь named и осуществим снова dig yandex.ru

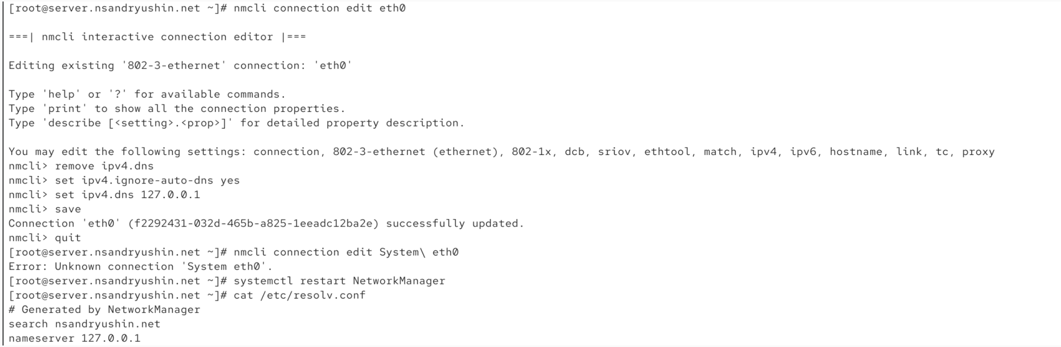


```
[root@server.nsandryushin.net ~]# systemctl start named
[root@server.nsandryushin.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.nsandryushin.net ~]# dig www.yandex.ru

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59580
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 31a82b8deebaff370100000068c571196108fb6da9fb10c8 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          260     IN      A       77.88.55.88
www.yandex.ru.          260     IN      A       77.88.44.55
www.yandex.ru.          260     IN      A       5.255.255.77

;; Query time: 10 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat Sep 13 13:26:49 UTC 2025
;; MSG SIZE  rcvd: 118

[root@server.nsandryushin.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: SERVFAIL, id: 54996
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 93362ad006f55f940100000068c5712be22ca7a583f54375 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; Query time: 1951 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sat Sep 13 13:27:07 UTC 2025
;; MSG SIZE  rcvd: 70
```

Рис. 7: Запуск named

eth0

Теперь настроим порт eth0

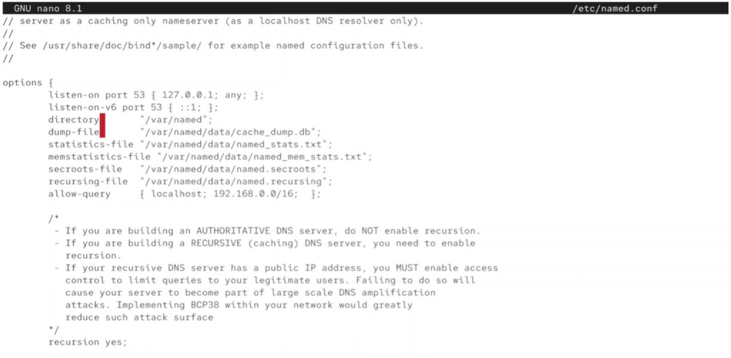


```
[root@server.nsandryushin.net ~]# nmcli connection edit eth0

===| 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, 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' (f2292431-032d-465b-a825-1eeadc12ba2e) successfully updated.
nmcli> quit
[root@server.nsandryushin.net ~]# nmcli connection edit System\ eth0
Error: Unknown connection 'System eth0'.
[root@server.nsandryushin.net ~]# systemctl restart NetworkManager
[root@server.nsandryushin.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search nsandryushin.net
nameserver 127.0.0.1
```

Рис. 8: eth0

named.conf

Откроем и отредактируем named.conf

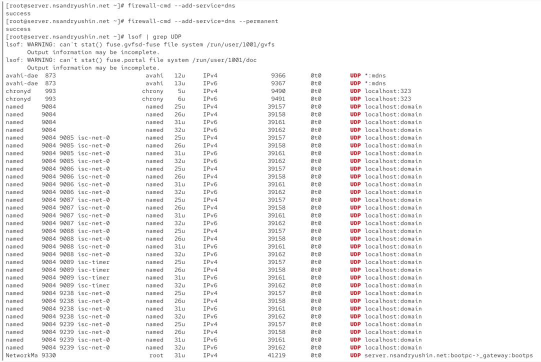


```
 GNU nano 8.1                                                                                    /etc/named.conf
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

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.
         - 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. 9: named.conf

Правила фаервола

Установим правила фаервола

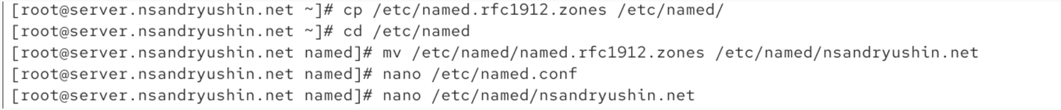


```
[root@server.nsandryushin.net ~]# firewall-cmd --add-service=dns
success
[root@server.nsandryushin.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.nsandryushin.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
avahi-dae  873                         avahi   12u     IPv4              9366       0t0        UDP *:mdns
avahi-dae  873                         avahi   13u     IPv6              9367       0t0        UDP *:mdns
chronyd    993                        chrony    5u     IPv4              9490       0t0        UDP localhost:323
chronyd    993                        chrony    6u     IPv6              9491       0t0        UDP localhost:323
named     9084                         named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084                         named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084                         named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084                         named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9085 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9085 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9085 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9085 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9086 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9086 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9086 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9086 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9087 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9087 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9087 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9087 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9088 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9088 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9088 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9088 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9089 isc-timer          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9089 isc-timer          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9089 isc-timer          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9089 isc-timer          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9238 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9238 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9238 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9238 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
named     9084 9239 isc-net-0          named   25u     IPv4             39157       0t0        UDP localhost:domain
named     9084 9239 isc-net-0          named   26u     IPv4             39158       0t0        UDP localhost:domain
named     9084 9239 isc-net-0          named   31u     IPv6             39161       0t0        UDP localhost:domain
named     9084 9239 isc-net-0          named   32u     IPv6             39162       0t0        UDP localhost:domain
NetworkMa 9330                          root   31u     IPv4             41219       0t0        UDP server.nsandryushin.net:bootpc->_gateway:bootps
```

Рис. 10: Правила фаервола

перемещение файла

Теперь переместим файл с настройкой конфига

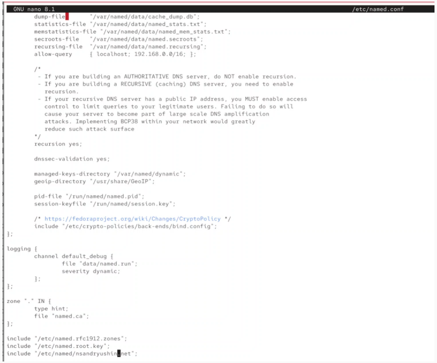


```
[root@server.nsandryushin.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.nsandryushin.net ~]# cd /etc/named
[root@server.nsandryushin.net named]# mv /etc/named/named.rfc1912.zones /etc/named/nsandryushin.net
[root@server.nsandryushin.net named]# nano /etc/named.conf
[root@server.nsandryushin.net named]# nano /etc/named/nsandryushin.net
```

Рис. 11: перемещение файла

Редактирование файла

И отредактируем наш файл под наши параметры

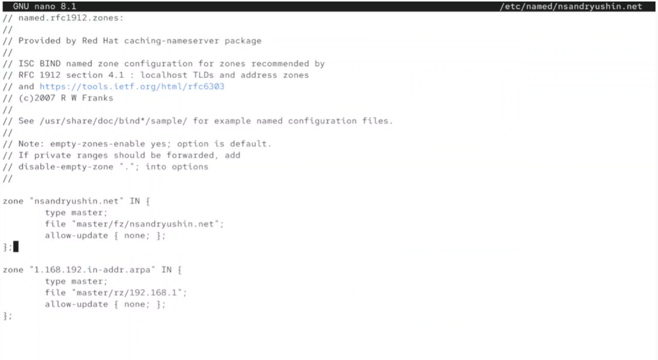


```
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 192.168.0.0/16; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - 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";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";

        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/nsandryushin.net";
```

Рис. 12: Редактирование файла

Файл зон

То же самое сделаем с файлом зон

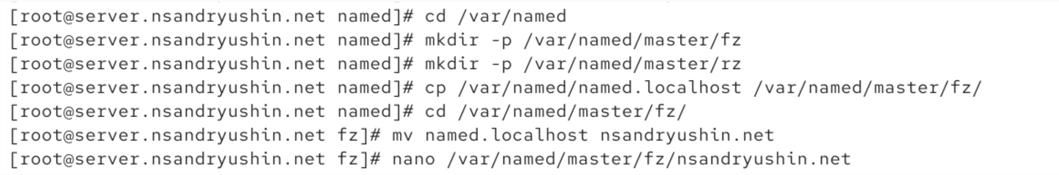


```
 GNU nano 8.1                                                  /etc/named/nsandryushin.net
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and 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 "nsandryushin.net" IN {
        type master;
        file "master/fz/nsandryushin.net";
        allow-update { none; };
};

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

Рис. 13: Файл зон

Создание папок и настроек днс

Создадим папки с настройками днс

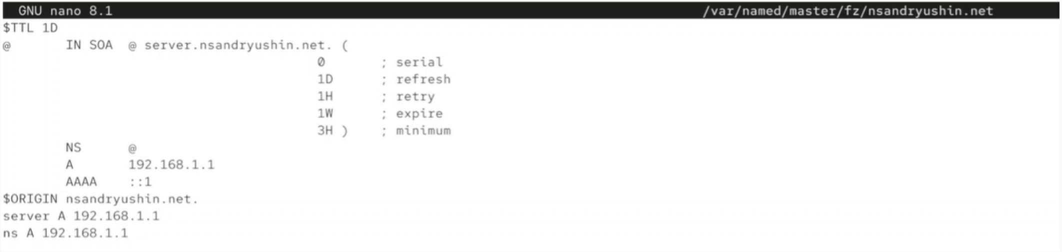


```
[root@server.nsandryushin.net named]# cd /var/named
[root@server.nsandryushin.net named]# mkdir -p /var/named/master/fz
[root@server.nsandryushin.net named]# mkdir -p /var/named/master/rz
[root@server.nsandryushin.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.nsandryushin.net named]# cd /var/named/master/fz/
[root@server.nsandryushin.net fz]# mv named.localhost nsandryushin.net
[root@server.nsandryushin.net fz]# nano /var/named/master/fz/nsandryushin.net
```

Рис. 14: Создание папок и настроек днс

nsandryushin.net

Отредактируем файл nsandryushin.net

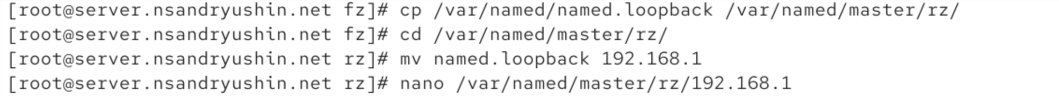


```
  GNU nano 8.1                                                                          /var/named/master/fz/nsandryushin.net
$TTL 1D
@       IN SOA  @ server.nsandryushin.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        AAAA    ::1
$ORIGIN nsandryushin.net.
server A 192.168.1.1
ns A 192.168.1.1
```

Рис. 15: nsandryushin.net

Папка rz

Теперь посмотрим на файлы из папки rz

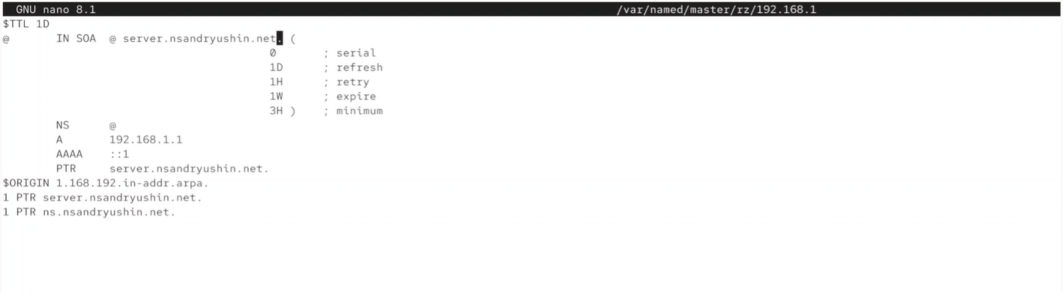


```
[root@server.nsandryushin.net fz]# cp /var/named/named.loopback /var/named/master/rz/
[root@server.nsandryushin.net fz]# cd /var/named/master/rz/
[root@server.nsandryushin.net rz]# mv named.loopback 192.168.1
[root@server.nsandryushin.net rz]# nano /var/named/master/rz/192.168.1
```

Рис. 16: Папка rz

Редактирование файла

Отредактируем следующим образом

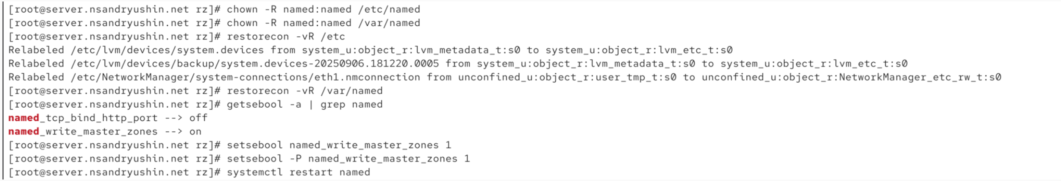


```
  GNU nano 8.1                                                                                /var/named/master/rz/192.168.1
$TTL 1D
@       IN SOA  @ server.nsandryushin.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        AAAA    ::1
        PTR     server.nsandryushin.net.
$ORIGIN 1.168.192.in-addr.arpa.
1 PTR server.nsandryushin.net.
1 PTR ns.nsandryushin.net.
```

Рис. 17: Редактирование файла

Selinux

Настроим Selinux

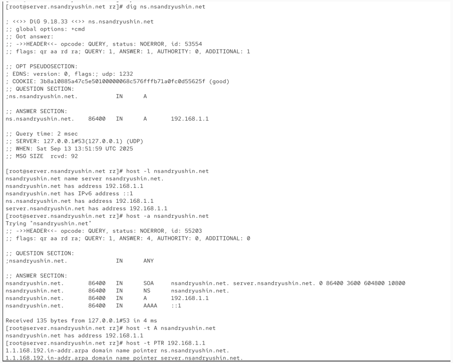


```
[root@server.nsandryushin.net rz]# chown -R named:named /etc/named
[root@server.nsandryushin.net rz]# chown -R named:named /var/named
[root@server.nsandryushin.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20250906.181220.0005 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
[root@server.nsandryushin.net rz]# restorecon -vR /var/named
[root@server.nsandryushin.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.nsandryushin.net rz]# setsebool named_write_master_zones 1
[root@server.nsandryushin.net rz]# setsebool -P named_write_master_zones 1
[root@server.nsandryushin.net rz]# systemctl restart named
```

Рис. 18: Selinux

dig

Через dig попробуем подключиться к собственному днс

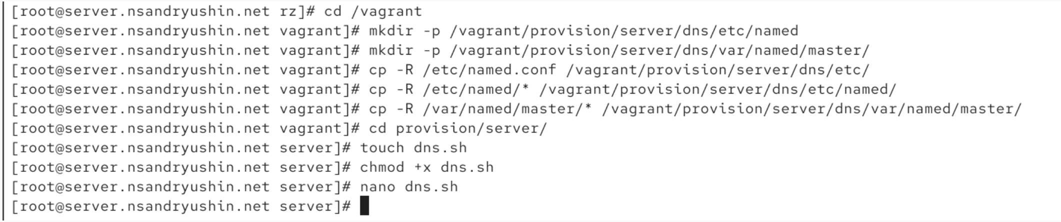


```
[root@server.nsandryushin.net rz]# dig ns.nsandryushin.net

; <<>> DiG 9.18.33 <<>> ns.nsandryushin.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53554
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3b8a10885a47c5e50100000068c576fffb71a0fc0d55625f (good)
;; QUESTION SECTION:
;ns.nsandryushin.net.           IN      A

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

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sat Sep 13 13:51:59 UTC 2025
;; MSG SIZE  rcvd: 92

[root@server.nsandryushin.net rz]# host -l nsandryushin.net
nsandryushin.net name server nsandryushin.net.
nsandryushin.net has address 192.168.1.1
nsandryushin.net has IPv6 address ::1
ns.nsandryushin.net has address 192.168.1.1
server.nsandryushin.net has address 192.168.1.1
[root@server.nsandryushin.net rz]# host -a nsandryushin.net
Trying "nsandryushin.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55203
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
nsandryushin.net.       86400   IN      SOA     nsandryushin.net. server.nsandryushin.net. 0 86400 3600 604800 10800
nsandryushin.net.       86400   IN      NS      nsandryushin.net.
nsandryushin.net.       86400   IN      A       192.168.1.1
nsandryushin.net.       86400   IN      AAAA    ::1

Received 135 bytes from 127.0.0.1#53 in 4 ms
[root@server.nsandryushin.net rz]# host -t A nsandryushin.net
nsandryushin.net has address 192.168.1.1
[root@server.nsandryushin.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.nsandryushin.net.
1.1.168.192.in-addr.arpa domain name pointer server.nsandryushin.net.
```

Рис. 19: dig

Конфиг вагрант

Оформим нашу работу как конфигурацию для вагранта

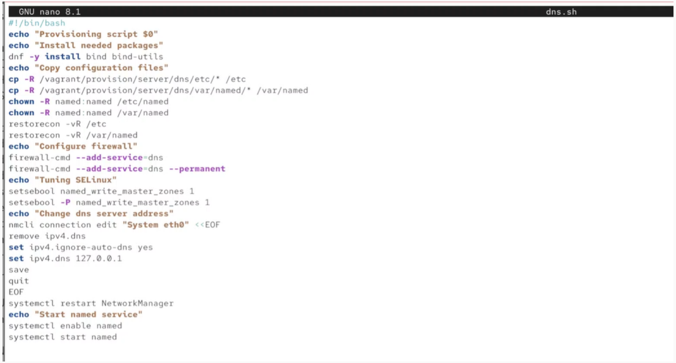


```
[root@server.nsandryushin.net rz]# cd /vagrant
[root@server.nsandryushin.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.nsandryushin.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
[root@server.nsandryushin.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.nsandryushin.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.nsandryushin.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.nsandryushin.net vagrant]# cd provision/server/
[root@server.nsandryushin.net server]# touch dns.sh
[root@server.nsandryushin.net server]# chmod +x dns.sh
[root@server.nsandryushin.net server]# nano dns.sh
[root@server.nsandryushin.net server]# █
```

Рис. 20: Конфиг вагрант

скрипт

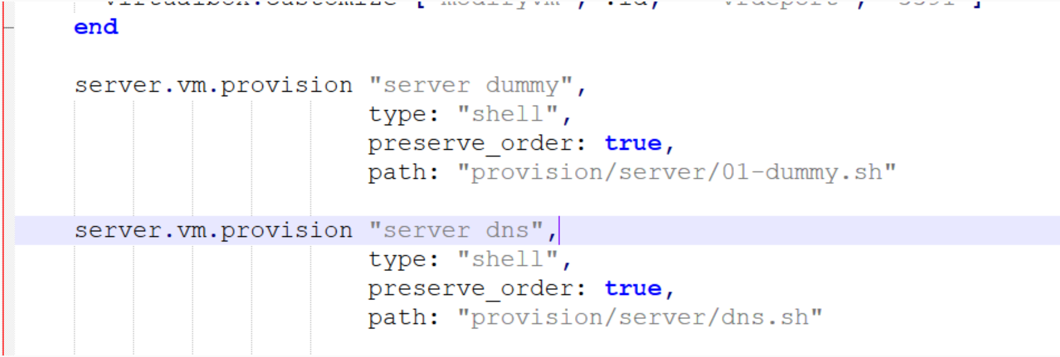
И напишем скрипт для загрузки вагранта



```
#!/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 "System 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. 21: скрипт

И в vagrantfile будем загружать этот скрипт



```
    end

    server.vm.provision "server dummy",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/01-dummy.sh"

    server.vm.provision "server dns",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/dns.sh"
```

Рис. 22: vagrantfile

Выводы

В результате выполнения работы были получены навыки настройки днс