Лабораторная работа 2

Генералов Даниил, НПИбд-01-21, 1032202280

2023

[1]RUDN University, Moscow, Russian Federation

Задание

Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils (см. раздел 2.4.1).

Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils (см. раздел 2.4.1).
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер (см. раздел 2.4.2).

Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils (см. раздел 2.4.1).
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер (см. раздел 2.4.2).
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер (см. раздел 2.4.3).

Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils (см. раздел 2.4.1).
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер (см. раздел 2.4.2).
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер (см. раздел 2.4.3).
4. При помощи утилит dig и host проанализируйте работу DNS-сервера (см. раздел 2.4.4).

Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils (см. раздел 2.4.1).
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер (см. раздел 2.4.2).
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер (см. раздел 2.4.3).
4. При помощи утилит dig и host проанализируйте работу DNS-сервера (см. раздел 2.4.4).
5. Напишите скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile (см. раздел 2.4.5).

Выполнение

Vagrant

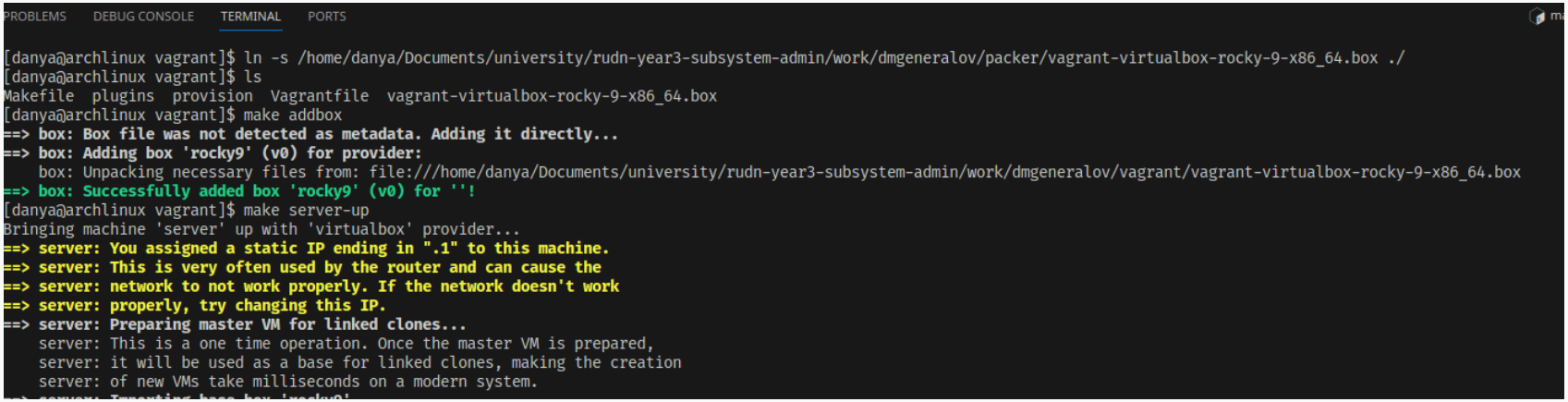
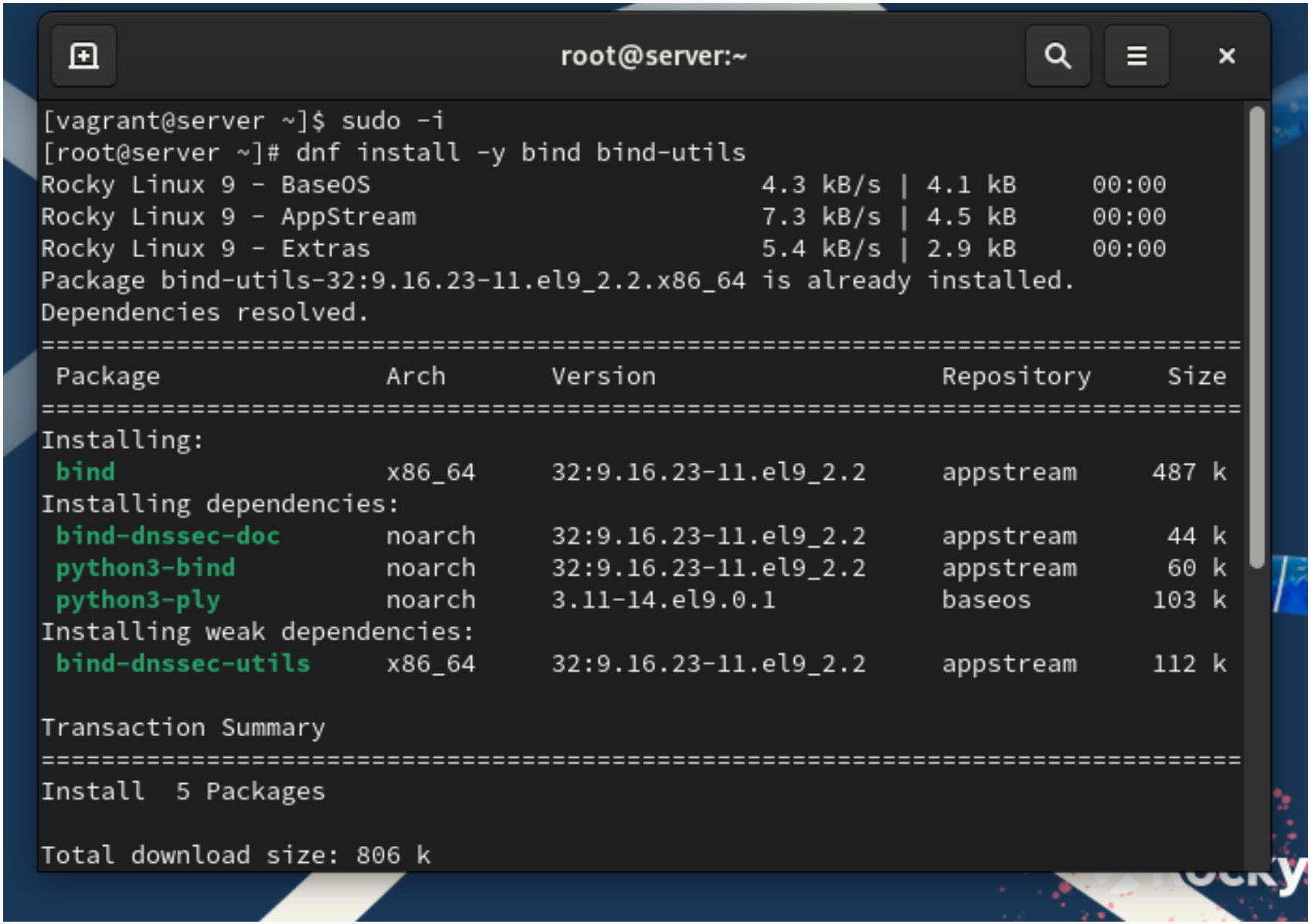


Рис. 1: vagrant

DNF


root@server:~
[vagrant@server ~]$ sudo -i
[root@server ~]# dnf install -y bind bind-utils
Rocky Linux 9 - BaseOS 4.3 kB/s | 4.1 kB 00:00
Rocky Linux 9 - AppStream 7.3 kB/s | 4.5 kB 00:00
Rocky Linux 9 - Extras 5.4 kB/s | 2.9 kB 00:00
Package bind-utils-32:9.16.23-11.el9_2.2.x86_64 is already installed.
Dependencies resolved.
Package Arch Version Repository Size
Installing:
bind x86_64 32:9.16.23-11.el9_2.2 appstream 487 k
Installing dependencies:
bind-dnssec-doc noarch 32:9.16.23-11.el9_2.2 appstream 44 k
python3-bind noarch 32:9.16.23-11.el9_2.2 appstream 60 k
python3-ply noarch 3.11-14.el9.0.1 baseos 103 k
Installing weak dependencies:
bind-dnssec-utils x86_64 32:9.16.23-11.el9_2.2 appstream 112 k
Transaction Summary
Install 5 Packages
Total download size: 806 k

dig

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

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12266
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       77.88.55.88
www.yandex.ru.          3600    IN      A       5.255.255.70
www.yandex.ru.          3600    IN      A       77.88.55.60
www.yandex.ru.          3600    IN      A       5.255.255.77

;; Query time: 40 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 11 11:22:07 UTC 2023
;; MSG SIZE  rcvd: 95

[root@server ~]#
```

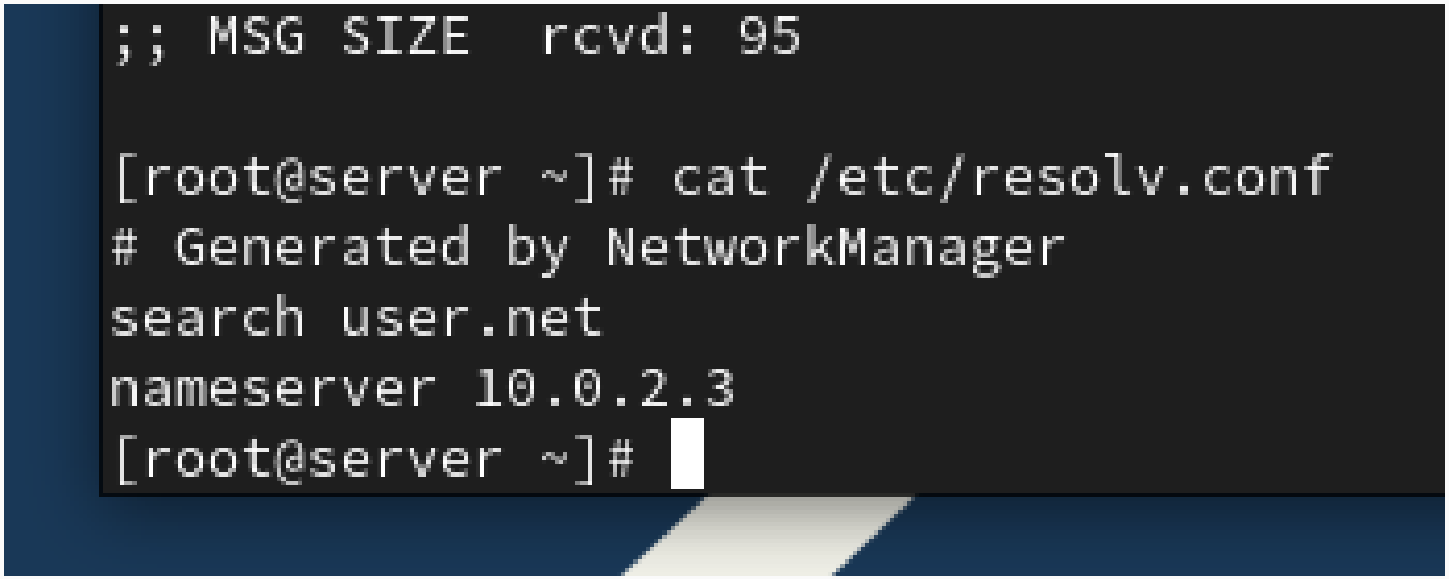

;; MSG SIZE rcvd: 95
[root@server ~]# cat /etc/resolv.conf
Generated by NetworkManager
search user.net
nameserver 10.0.2.3
[root@server ~]#

Рис. 4: resolv

BIND

```
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";
```

BIND

```
; <<>> DiG 9.11.3-RedHat-9.11.3-3.fc27 <<>> +bufsize=1200 +norec @a.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46900
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
```

BIND

```
[root@server ~]# 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 ~]# 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 ~]#
```

dig

```
; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62747
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       77.88.55.60
www.yandex.ru.          3600    IN      A       5.255.255.70
www.yandex.ru.          3600    IN      A       5.255.255.77
www.yandex.ru.          3600    IN      A       77.88.55.88

;; Query time: 9 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 11 11:46:09 UTC 2023
;; MSG SIZE  rcvd: 95

[root@server ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 9483
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

Рис. 8: dig

```
ORMERR resolving './NS/IN': 199.7.83.42#53
etwork unreachable resolving './NS/IN': 2001:503:c27::2:30#53
ORMERR resolving './NS/IN': 198.97.190.53#53
ORMERR resolving './NS/IN': 192.33.4.12#53
ORMERR resolving './NS/IN': 192.5.5.241#53
ORMERR resolving './NS/IN': 199.7.91.13#53
esolver priming query complete
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:dc3::35#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:7fd::1#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:503:ba3e::2:30#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:9f::42#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:1::53#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:2::c#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:2f::f#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:2d::d#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:7fe::53#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:200::b#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:a8::e#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:500:12::d0d#53
etwork unreachable resolving '_.yandex.ru/A/IN': 2001:503:c27::2:30#53
etwork unreachable resolving './NS/IN': 2001:dc3::35#53
etwork unreachable resolving './NS/IN': 2001:7fe::53#53
etwork unreachable resolving './NS/IN': 2001:7fd::1#53
etwork unreachable resolving './NS/IN': 2001:500:a8::e#53
etwork unreachable resolving './NS/IN': 2001:500:12::d0d#53
```

Рис. 9: named

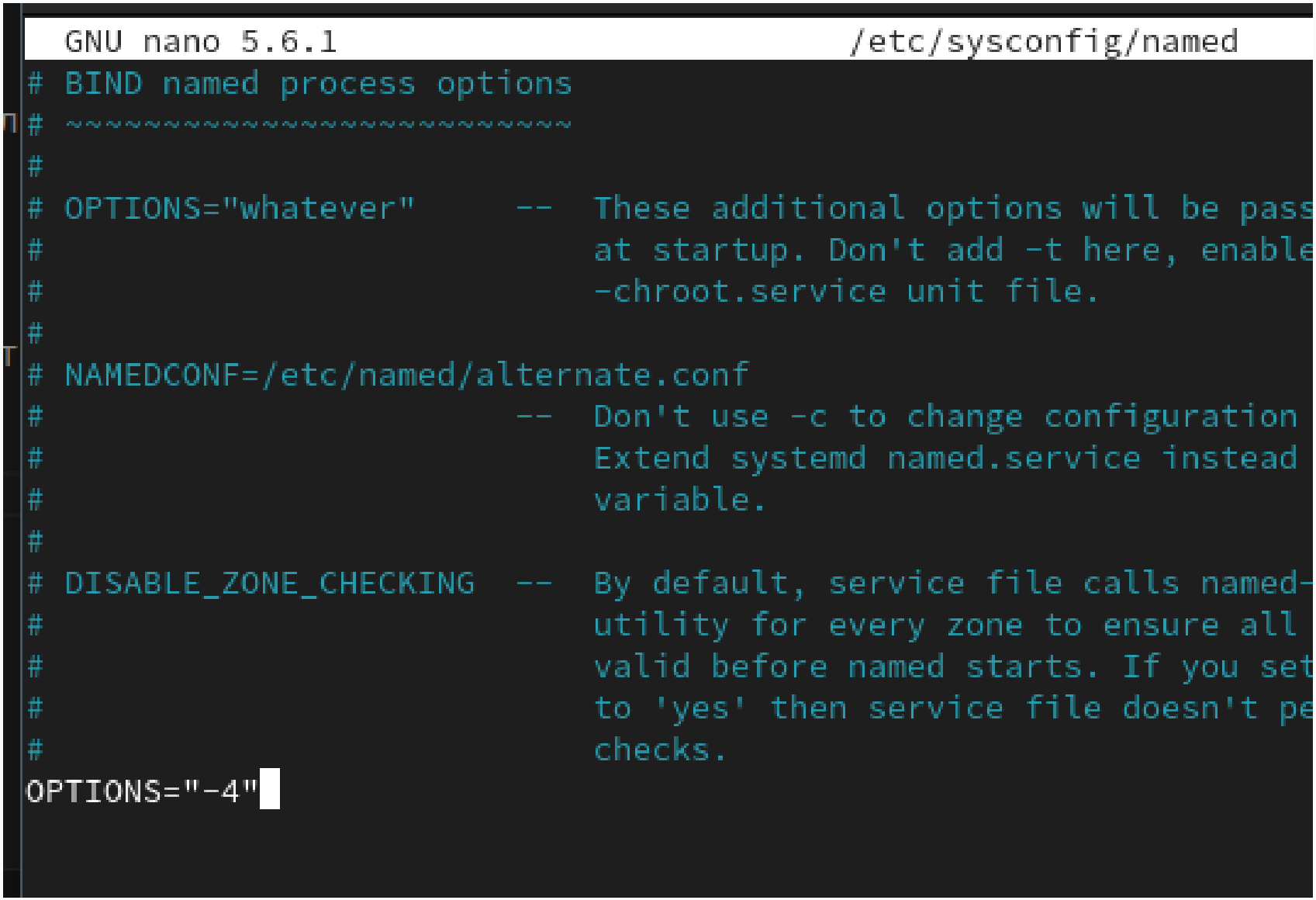

GNU nano 5.6.1 /etc/sysconfig/named
BIND named process options
~~~~~~~~~~~~~~~~~~~~~~~~~~
#
OPTIONS="whatever" -- These additional options will be pass
at startup. Don't add -t here, enable
-chroot.service unit file.
#
NAMEDCONF=/etc/named/alternate.conf
-- Don't use -c to change configuration
Extend systemd named.service instead
variable.
#
# DISABLE_ZONE_CHECKING -- By default, service file calls named-
# utility for every zone to ensure all
# valid before named starts. If you set
# to 'yes' then service file doesn't pe
# checks.
OPTIONS="-4"

Рис. 10: named

Wireshark

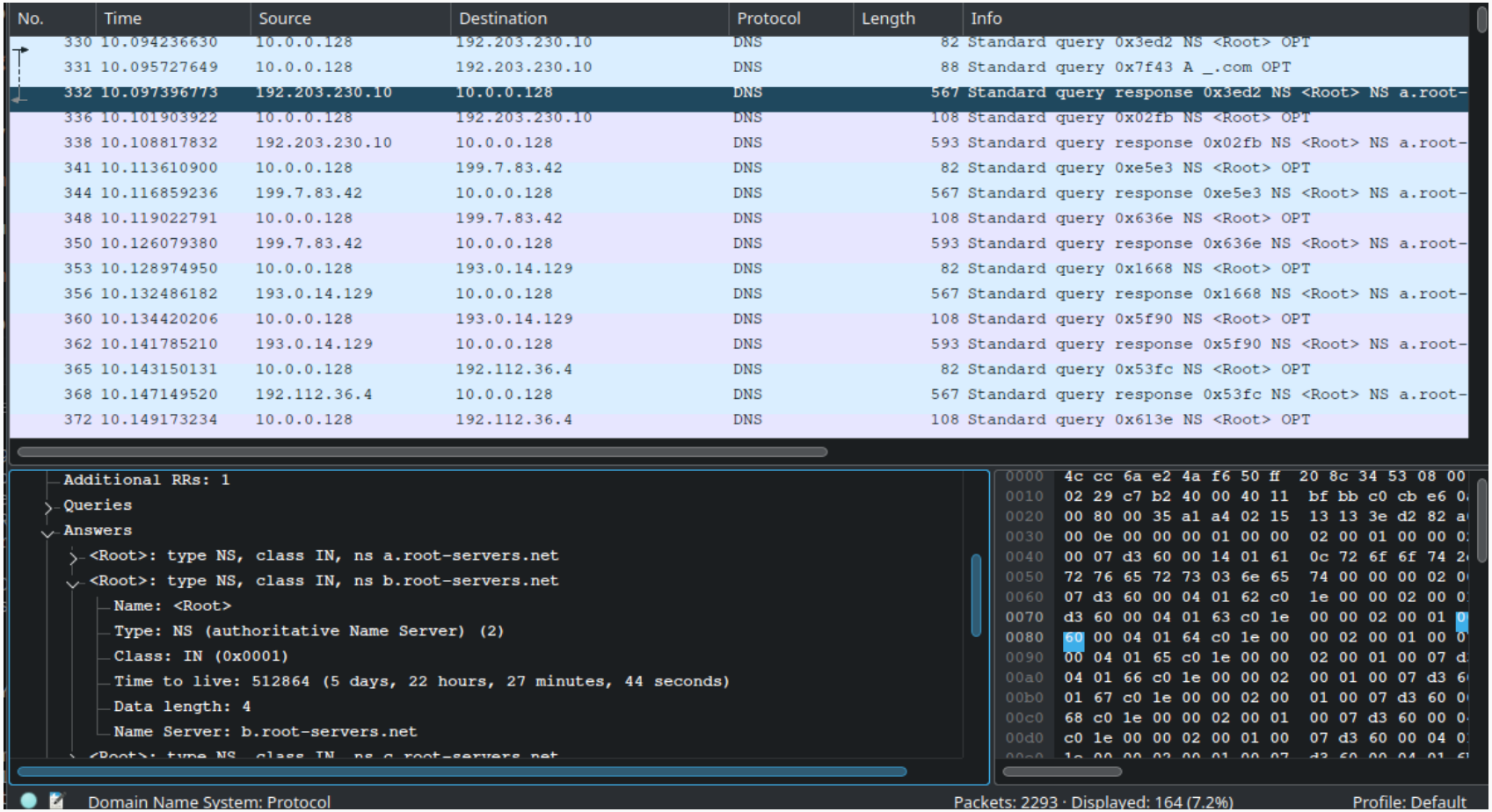


Рис. 11: wireshark

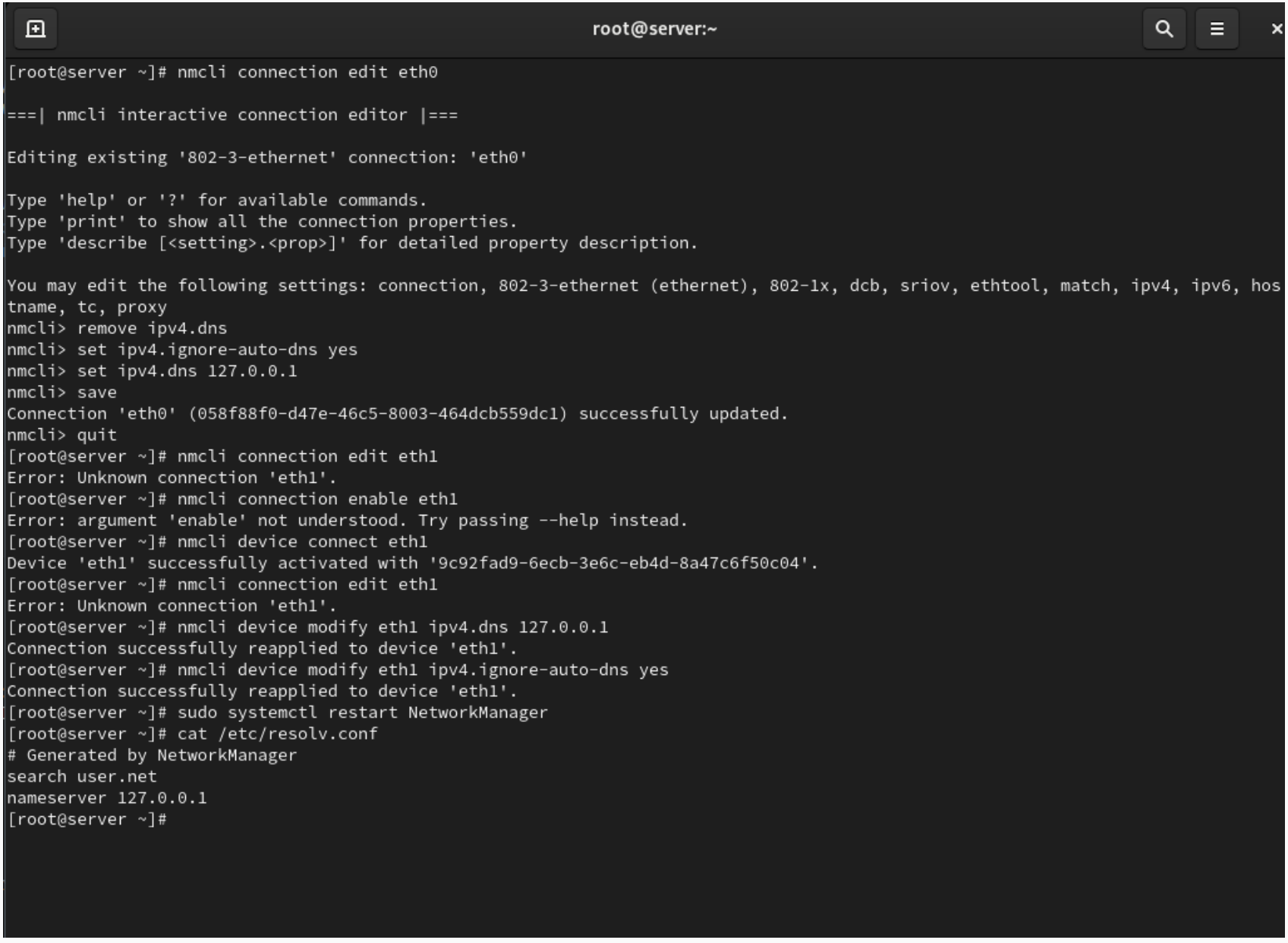
```
        recursion.
         - If your recursive DNS server has a public IP address, you
           control to limit queries to your legitimate users. Failing
           cause your server to become part of large scale DNS amplif
           attacks. Implementing BCP38 within your network would grea
           reduce such attack surface
        */
        recursion yes;

        forwarders { 1.1.1.1;1.0.0.1 };
        forward first;

        dnssec-enable no;
        dnssec-validation no;

        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";
```

Рис. 12: named

dig

```
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       77.88.55.88
www.yandex.ru.          3600    IN      A       5.255.255.77
www.yandex.ru.          3600    IN      A       5.255.255.70
www.yandex.ru.          3600    IN      A       77.88.55.60

;; Query time: 15 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Nov 11 12:13:48 UTC 2023
;; MSG SIZE  rcvd: 95

[root@server ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3257
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cf7fbe24c08bf68101000000654f6ffd3e1e57979559645e (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          158     IN      A       5.255.255.77
www.yandex.ru.          158     IN      A       77.88.55.60
www.yandex.ru.          158     IN      A       77.88.55.88
www.yandex.ru.          158     IN      A       5.255.255.70

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 11 12:13:49 UTC 2023
;; MSG SIZE  rcvd: 134

[root@server ~]#
```

nmcli


root@server:~
[root@server ~]# 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, 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' (058f88f0-d47e-46c5-8003-464dcb559dc1) successfully updated.
nmcli> quit
[root@server ~]# nmcli connection edit eth1
Error: Unknown connection 'eth1'.
[root@server ~]# nmcli connection enable eth1
Error: argument 'enable' not understood. Try passing --help instead.
[root@server ~]# nmcli device connect eth1
Device 'eth1' successfully activated with '9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04'.
[root@server ~]# nmcli connection edit eth1
Error: Unknown connection 'eth1'.
[root@server ~]# nmcli device modify eth1 ipv4.dns 127.0.0.1
Connection successfully reapplied to device 'eth1'.
[root@server ~]# nmcli device modify eth1 ipv4.ignore-auto-dns yes
Connection successfully reapplied to device 'eth1'.
[root@server ~]# sudo systemctl restart NetworkManager
[root@server ~]# cat /etc/resolv.conf
Generated by NetworkManager
search user.net
nameserver 127.0.0.1
[root@server ~]#

```
// See /usr/share/doc/bind*/sample/ for example named configuratio
//

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; 192.0.0.0/16; };

        /*
```

Рис. 15: named

```
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

include "/etc/named/dmgeneralov.net";
```

Рис. 16: named

```
  GNU nano 5.6.1                                  /etc/named/dmgeneralov.net
zone "dmgeneralov.net" IN {
        type master;
        file "master/fz/dmgeneralov.net";
        allow-update { none; };
};

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

Рис. 17: named

```
  GNU nano 5.6.1                                /var/named/master/fz/dmgeneralov.net
$TTL 1D
@       IN SOA  @ server.dmgeneralov.net. (
                                        2023111100      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
$ORIGIN dmgeneralov.net.

server  A       192.168.1.1
ns      A       192.168.1.1
```

Рис. 18: named

```
  GNU nano 5.6.1                                  /var/named/master/rz/192.168.1
$TTL 1D
@       IN SOA  @ server.dmgeneralov.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        PTR     server.dmgeneralov.net.

$ORIGIN 1.168.192.in-addr.arpa.
1       PTR     server.dmgeneralov.net.
1       PTR     ns.dmgeneralov.net.
```

Рис. 19: named

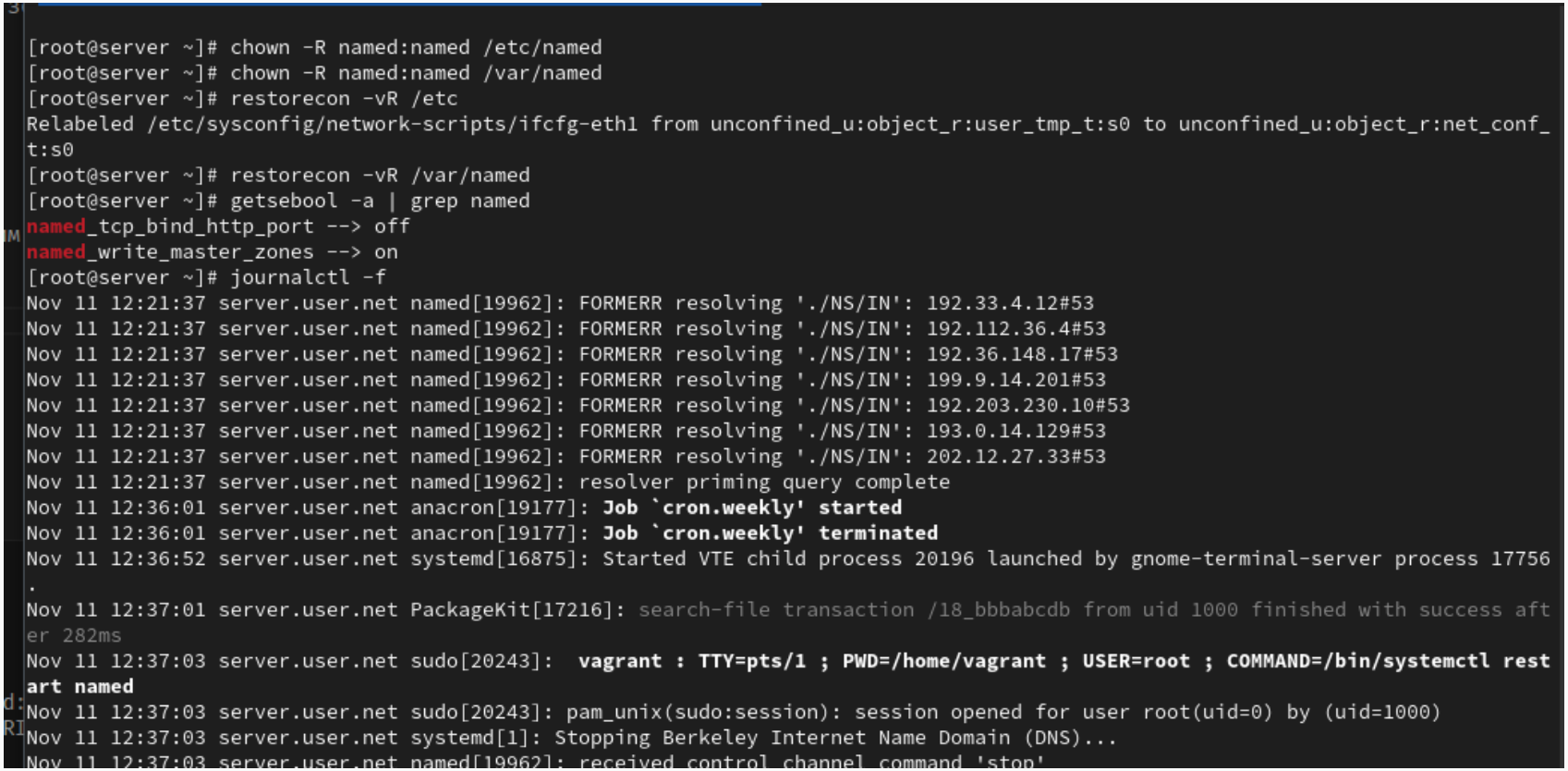

[root@server ~]# chown -R named:named /etc/named
[root@server ~]# chown -R named:named /var/named
[root@server ~]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@server ~]# restorecon -vR /var/named
[root@server ~]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server ~]# journalctl -f
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 192.33.4.12#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 192.112.36.4#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 192.36.148.17#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 199.9.14.201#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 192.203.230.10#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 193.0.14.129#53
Nov 11 12:21:37 server.user.net named[19962]: FORMERR resolving './NS/IN': 202.12.27.33#53
Nov 11 12:21:37 server.user.net named[19962]: resolver priming query complete
Nov 11 12:36:01 server.user.net anacron[19177]: Job `cron.weekly' started
Nov 11 12:36:01 server.user.net anacron[19177]: Job `cron.weekly' terminated
Nov 11 12:36:52 server.user.net systemd[16875]: Started VTE child process 20196 launched by gnome-terminal-server process 17756.
Nov 11 12:37:01 server.user.net PackageKit[17216]: search-file transaction /18_bbbabcdb from uid 1000 finished with success after 282ms
Nov 11 12:37:03 server.user.net sudo[20243]: vagrant : TTY=pts/1 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/systemctl restart named
Nov 11 12:37:03 server.user.net sudo[20243]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Nov 11 12:37:03 server.user.net systemd[1]: Stopping Berkeley Internet Name Domain (DNS)...
Nov 11 12:37:03 server.user.net named[19962]: received control channel command 'stop'

Рис. 20: named

dig

```
[root@server ~]#
[root@server ~]# dig ns.dmgeneralov.net

; <<>> DiG 9.16.23-RH <<>> ns.dmgeneralov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11599
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 949fe95fa2e18654010000006 54f75ecf880d8bbe7e4d695 (good)
;; QUESTION SECTION:
;ns.dmgeneralov.net.            IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 11 12:39:08 UTC 2023
;; MSG SIZE  rcvd: 91

[root@server ~]# host -l dmgeneralov.net
dmgeneralov.net name server dmgeneralov.net.
dmgeneralov.net has address 192.168.1.1
ns.dmgeneralov.net has address 192.168.1.1
server.dmgeneralov.net has address 192.168.1.1
```

host

```
[root@server ~]# host -t A dmgeneralov.net
dmgeneralov.net has address 192.168.1.1
[root@server ~]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.dmgeneralov.net.
1.1.168.192.in-addr.arpa domain name pointer ns.dmgeneralov.net.
[root@server ~]#
```

Рис. 22: host

Vagrant

```
[root@server ~]# cd /vagrant
[root@server vagrant]# ls
Makefile  plugins  provision  Vagrantfile  vagrant-virtualbox-rocky-9-x86_64.box  vm
[root@server vagrant]# mkdir -p provision/server/dns/etc/named
[root@server vagrant]# mkdir -p provision/server/dns/var/named/master
[root@server vagrant]# cp -R /etc/named.conf ./provision/server/dns/etc/
[root@server vagrant]# cp -R /etc/named/* ./provision/server/dns/etc/named/
[root@server vagrant]# cp -R /var/named/master/* ./provision/server/dns/var/named/master/
[root@server vagrant]#
```

Рис. 23: vagrant

Vagrant

work > dmgeneralov > vagrant > provision > server > dns.sh

```
#!/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 "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
```

Vagrant

```
37
38      server.vm.provision "server dummy",
39                          type: "shell",
40                          preserve_order: true,
41                          path: "provision/server/01-dummy.sh"
42
43      server.vm.provision "server dns",
44                          type: "shell",
45                          preserve_order: true,
46                          path: "provision/server/dns.sh"
47
48      server.vm.provider :virtualbox do |v|
49        v.linked_clone = true
50        # Customize the amount of memory on the VM
```

Рис. 25: vagrant

Вывод

Я получил опыт настройки DNS-сервера BIND и сохранения сделанных настроек в систему Vagrant.