

Отчет по лабораторной работе №2

Настройка DNS-сервера

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Установка DNS-сервера	5
2.2	Конфигурирование кэширующего DNS-сервера	6
2.3	Конфигурирование первичного DNS-сервера	11
2.4	Анализ работы DNS-сервера	14
2.5	Внесение изменений в настройки внутреннего окружения виртуальной машины	15
3	Выводы	17
4	Ответы на контрольные вопросы	18

Список иллюстраций

2.1	Установка bind, bind-utils	5
2.2	Использование dig	6
2.3	/etc/resolv.conf, /etc/named.conf	6
2.4	/var/named/named.ca	7
2.5	/var/named/named.localhost, /var/named/named.loopback	7
2.6	Использование dig (2)	8
2.7	Изменение настроек сетевого соединения eth0	9
2.8	Изменение настроек сетевого соединения System eth0	9
2.9	Перезапуск NetworkManager и просмотр файла	10
2.10	Внесение изменений в файл /etc/named.conf	10
2.11	Внесение изменений в настройки межсетевого экрана узла server, проверка	11
2.12	Редактирование named.conf	11
2.13	Редактирование файла /etc/named/user.net	12
2.14	Создание каталогов, копирование шаблона прямой зоны, переименование	12
2.15	Редактирование /var/named/master/fz/ngalacan.net	13
2.16	Копирование шаблона обратной зоны, переименование	13
2.17	Редактирование /var/named/master/rz/192.168.1	13
2.18	Изменение прав доступа, восстановление меток SELinux, проверка	13
2.19	Запуск DNS-сервера после исправления ошибок	14
2.20	Описание DNS-зоны с сервера ns.ngalacan.net	14
2.21	Анализ корректности работы DNS-сервера	15
2.22	Размещение конфигурационных файлов в каталог /vagrant/provision/server/dns	15
2.23	Редактирование скрипта dns.sh	16
2.24	Редактирование Vagrantfile	16

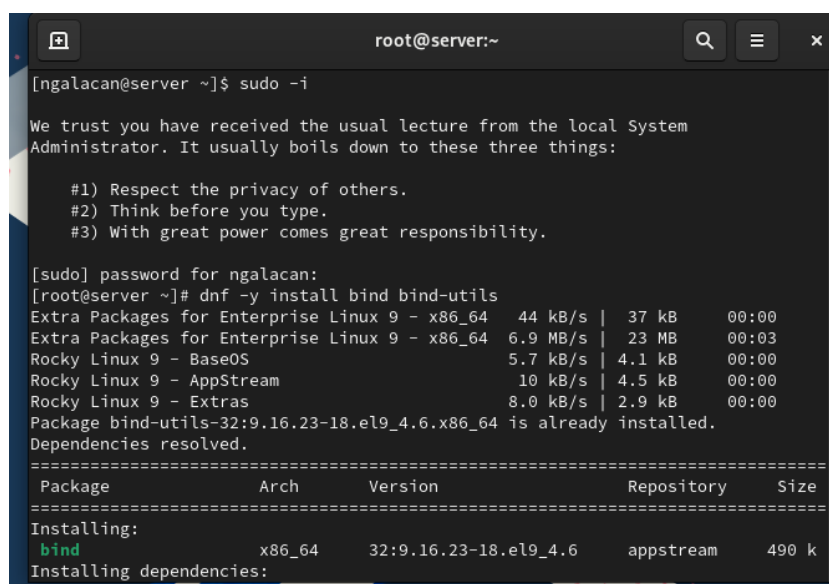
1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Установка DNS-сервера

Запускаю VM через рабочий каталог. На VM server вхожу под собственным пользователем и перехожу в режим суперпользователя. Устанавливаю bind и bind-utils (рис. 2.1).



```
root@server:~  
[ngalacan@server ~]$ 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.  
  
[sudo] password for ngalacan:  
[root@server ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 44 kB/s | 37 kB 00:00  
Extra Packages for Enterprise Linux 9 - x86_64 6.9 MB/s | 23 MB 00:03  
Rocky Linux 9 - BaseOS 5.7 kB/s | 4.1 kB 00:00  
Rocky Linux 9 - AppStream 10 kB/s | 4.5 kB 00:00  
Rocky Linux 9 - Extras 8.0 kB/s | 2.9 kB 00:00  
Package bind-utils-32:9.16.23-18.el9_4.6.x86_64 is already installed.  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
bind	x86_64	32:9.16.23-18.el9_4.6	appstream	490 k
Installing dependencies:				

```
=====
```

Рис. 2.1: Установка bind, bind-utils

С помощью утилиты dig делаю запрос к DNS-адресу (рис. 2.2)

```
root@server:~  
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: 58758  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, 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      5.255.255.77  
www.yandex.ru.                3600    IN      A      77.88.44.55  
  
;; Query time: 11 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Mon Sep 09 15:37:05 UTC 2024  
;; MSG SIZE rcvd: 79  
  
[root@server ~]#
```

Рис. 2.2: Использование dig

2.2 Конфигурирование кэширующего DNS-сервера

Просматриваю файлы `/etc/resolv.conf`, `/etc/named.conf` (рис. 2.3), `/var/named/named.ca` (рис. 2.4), `/var/named/named.localhost`, `/var/named/named.loopback` (рис. 2.5).

```
root@server:~  
[root@server ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
nameserver 10.0.2.3  
[root@server ~]# cat /etc/named/conf  
cat: /etc/named/conf: No such file or directory  
[root@server ~]# 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; };  
}
```

Рис. 2.3: `/etc/resolv.conf`, `/etc/named.conf`

```
root@server:~  
include "/etc/named.root.key";  
[root@server ~]# cat /var/named/named.ca  
;  
<<> DiG 9.18.20 <<> -4 +tcp +nored +nostats @d.root-servers.net  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 47286  
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27  
;  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 1450  
;; QUESTION SECTION:  
;;  
;;  
;; 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.
```

Рис. 2.4: /var/named/named.ca

```
root@server:~  
n.root-servers.net. 518400 IN AAAA 2001:dc3::35  
[root@server ~]# cat /var/named/named.localhost  
$TTL ID  
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 ID  
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 ~]#
```

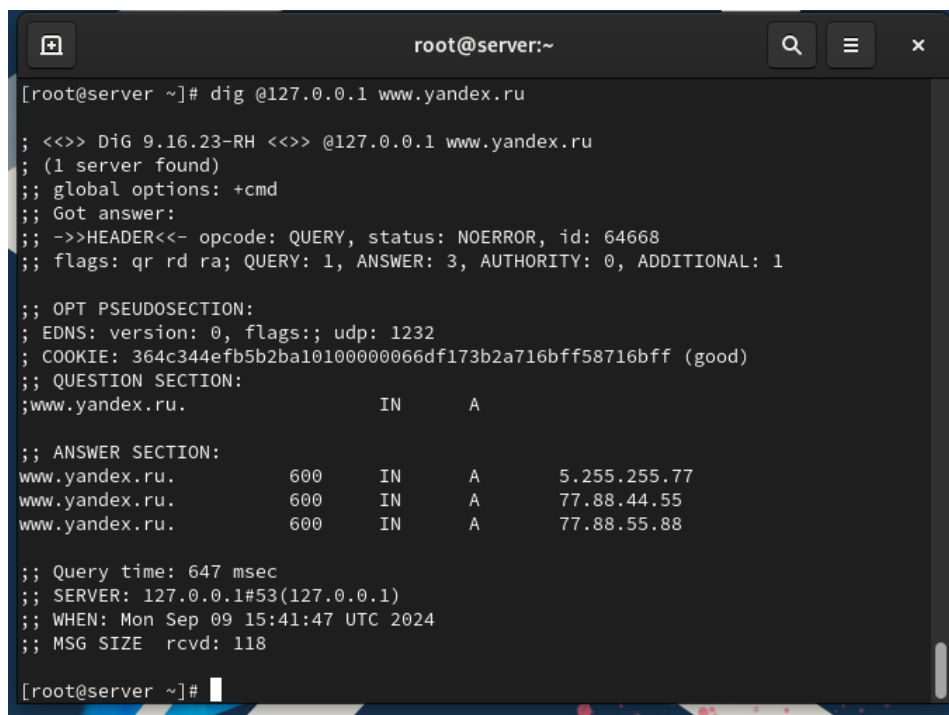
Рис. 2.5: /var/named/named.localhost, /var/named/named.loopback

Запускаю DNS-сервер и включаю в автозапуск:

```
systemctl start named
```

```
systemctl enable named
```

Ввожу `dig @127.0.0.1 www.yandex.ru` и анализирую отличия в информации от рис. 2.2. В данном случае выводится больше данных (рис. 2.6).



```
[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: 64668
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 364c344efb5b2ba10100000066df173b2a716bff58716bff (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: 647 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep 09 15:41:47 UTC 2024
;; MSG SIZE rcvd: 118

[root@server ~]#
```

Рис. 2.6: Использование dig (2)

Сделаю DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить настройки сетевого соединения `eth0` в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес `127.0.0.1` (рис. 2.7). То же самое делаю для System `eth0` (рис. 2.8)


```
root@server:~  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Mon Sep 09 15:41:47 UTC 2024  
;; MSG SIZE rcvd: 118  
  
[root@server ~]#  
[root@server ~]#  
[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), 802-1  
x, 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' (8ba39c28-bf3b-438e-88a2-5b2895449f53) successfully updated.  
nmcli> quit  
[root@server ~]#
```

Рис. 2.7: Изменение настроек сетевого соединения eth0

```
[root@server ~]# nmcli connection edit System\ eth0  
  
==| nmcli interactive connection editor |==  
  
Editing existing '802-3-ethernet' connection: 'System 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), 802-1  
x, 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 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully upda  
ted.  
nmcli> quit  
[root@server ~]#
```

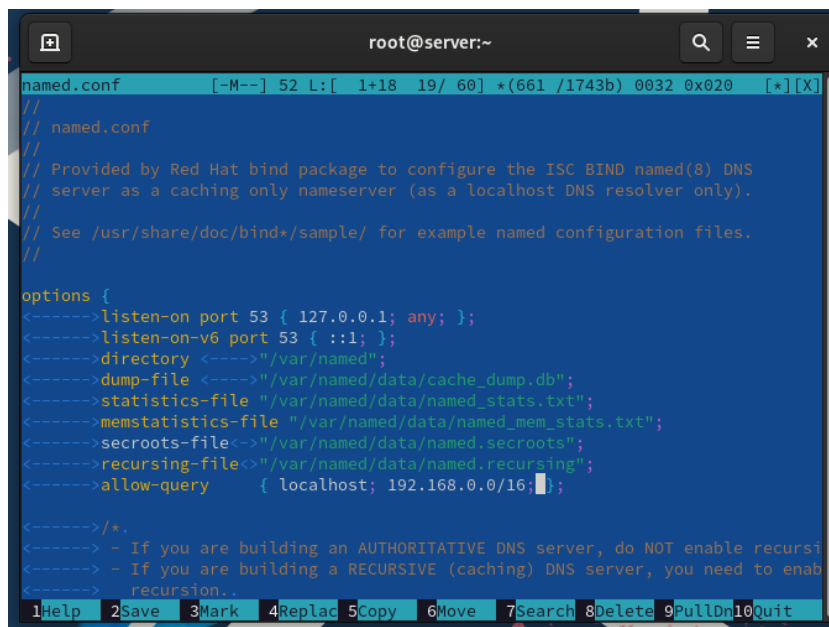
Рис. 2.8: Изменение настроек сетевого соединения System eth0

Перезапускаю NetworkManager и проверяю наличие изменений в файле /etc/resolv.conf (рис. 2.9).

```
[root@server ~]# systemctl restart NetworkManager
[root@server ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 127.0.0.1
[root@server ~]#
```

Рис. 2.9: Перезапуск NetworkManager и просмотр файла

Вношу изменения в файл /etc/named.conf (рис. 2.10).



```
named.conf  [-M--] 52 L:[ 1+18 19/ 60] *(661 /1743b) 0032 0x020 [*][X]
//
// 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 recursi
<----->- If you are building a RECURSIVE (caching) DNS server, you need to enab
<-----> recursion..
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

Рис. 2.10: Внесение изменений в файл /etc/named.conf

Вношу изменения в настройки межсетевого экрана узла server, разрешив работу с DNS. Убеждаюсь, что DNS-запросы идут через узел server, который прослушивает порт 53 (рис. 2.11).

```
root@server:~  
[root@server ~]# firewall-cmd --add-service=dns  
success  
[root@server ~]# firewall-cmd --add-service=dns --permanent  
success  
[root@server ~]# lsof | grep UDP  
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs  
Output information may be incomplete.  
avahi-dae 561          avahi 12u  IPv4  19702    0t0  UDP *:mdns  
avahi-dae 561          avahi 13u  IPv6  19703    0t0  UDP *:mdns  
avahi-dae 561          avahi 14u  IPv4  19704    0t0  UDP *:50219  
avahi-dae 561          avahi 15u  IPv6  19705    0t0  UDP *:47422  
chronydc 580          chrony 5u   IPv4  19638    0t0  UDP localhost:323  
chronydc 580          chrony 6u   IPv6  19639    0t0  UDP localhost:323  
named     6213          named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213          named 24u  IPv6  35175    0t0  UDP localhost:domain  
named     6213 6214 isc-net-0  named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213 6214 isc-net-0  named 24u  IPv6  35175    0t0  UDP localhost:domain  
named     6213 6215 isc-net-0  named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213 6215 isc-net-0  named 24u  IPv6  35175    0t0  UDP localhost:domain  
named     6213 6216 isc-timer  named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213 6216 isc-timer  named 24u  IPv6  35175    0t0  UDP localhost:domain  
named     6213 6217 isc-socket named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213 6217 isc-socket named 24u  IPv6  35175    0t0  UDP localhost:domain  
named     6213 6246 isc-net-0  named 21u  IPv4  35173    0t0  UDP localhost:domain  
named     6213 6246 isc-net-0  named 24u  IPv6  35175    0t0  UDP localhost:domain  
NetworkMa 6355          root  27u   IPv4  40057    0t0  UDP server:bootpc->.ga  
teway:bootps  
NetworkMa 6355 6362 gmain    root  27u   IPv4  40057    0t0  UDP server:bootpc->.ga  
teway:bootps
```

Рис. 2.11: Внесение изменений в настройки межсетевого экрана узла server, проверка

Для конфигурирования кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами вношу изменения в файл `named.conf` (рис. 2.12)

```
root@server:~  
named.conf [-M--] 29 L: [ 7+16 23/ 64 ] *(748 /1827b) 0010 0x00A  
// 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; };  
    <----->forwarders { 127.0.0.1 };  
    <----->forward first;  
    <----->dnssec-enable no;  
    <----->dnssec-validation no;  
    <----->};  
    <-----># 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.  
    <----->};  
};
```

Рис. 2.12: Редактирование `named.conf`

2.3 Конфигурирование первичного DNS-сервера

Ввожу команды:

```
cp /etc/named.rfc1912.zones /etc/named/
cd /etc/named
mv /etc/named/named.rfc1912.zones /etc/named/ngalacan.net
```

Включаю файл описания зоны `/etc/named/ngalacan.net` в конфигурационном файле DNS `/etc/named.conf`, добавив в нём в конце строку: `include "/etc/named/user.net";`.

Редактирую файл `/etc/named/user.net` (рис. 2.13)



Рис. 2.13: Редактирование файла `/etc/named/user.net`

В каталоге `/var/named` создаю подкаталоги `master/fz` и `master/rz`, в которых будут располагаться файлы прямой и обратной зоны соответственно. Копирую шаблон прямой DNS-зоны `named.localhost` из каталога `/var/named` в каталог `/var/named/master/fz`, переименовав его в `ngalacan.net` (рис. 2.14).

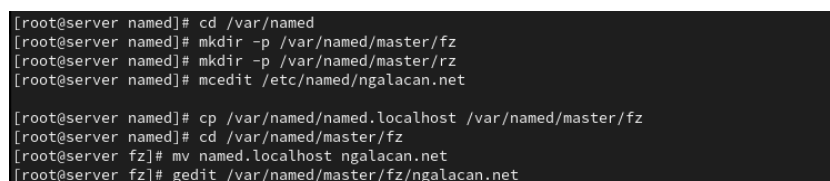


Рис. 2.14: Создание каталогов, копирование шаблона прямой зоны, переименование

Изменяю файл `/var/named/master/fz/ngalacan.net` (рис. 2.15).

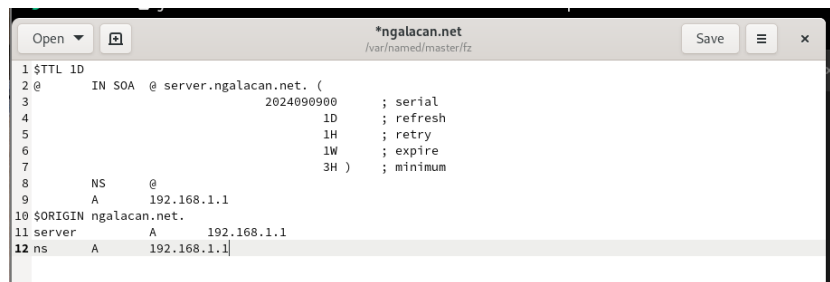


Рис. 2.15: Редактирование /var/named/master/fz/ngalacan.net

Копирую шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуйте его в 192.168.1 (рис. 2.16).

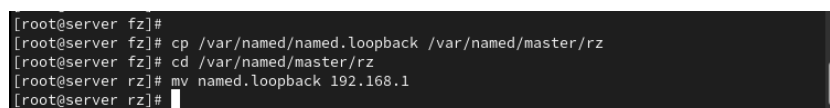


Рис. 2.16: Копирование шаблона обратной зоны, переименование

Изменяю файл /var/named/master/rz/192.168.1 (рис. 2.17).

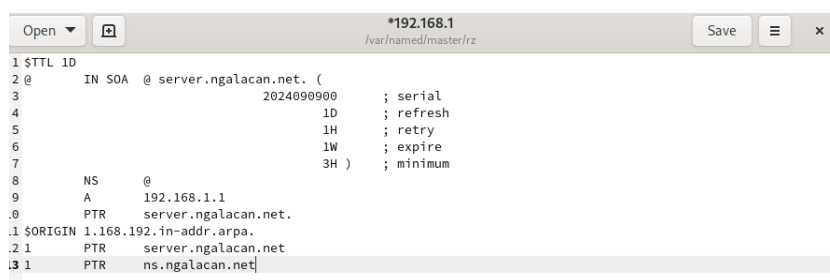


Рис. 2.17: Редактирование /var/named/master/rz/192.168.1

Изменяю права доступа, восстанавливаю метки SELinux, проверяю (рис. 2.18).

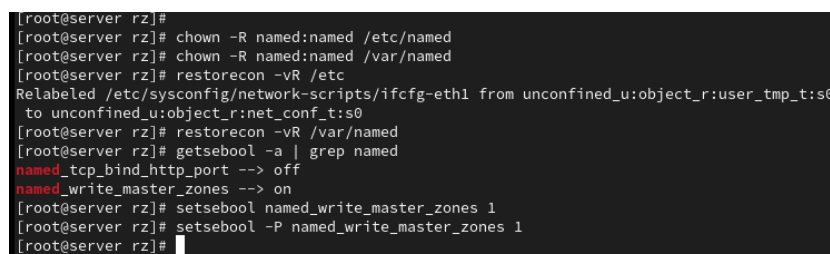
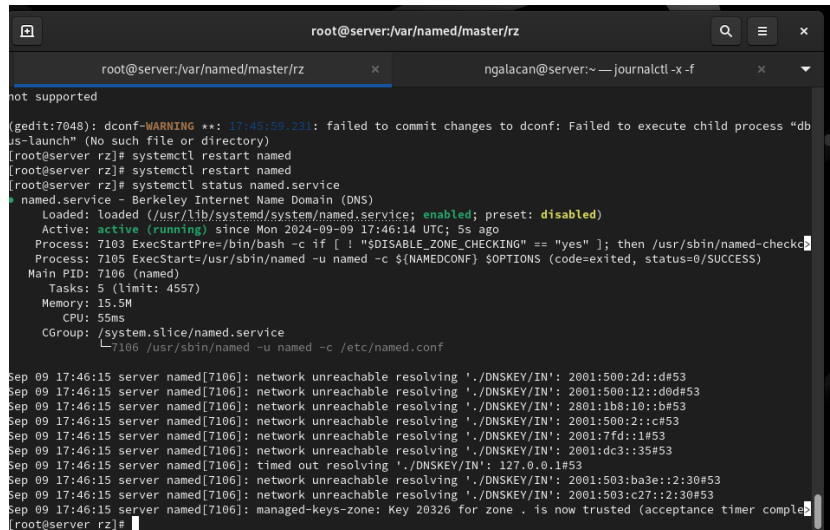


Рис. 2.18: Изменение прав доступа, восстановление меток SELinux, проверка

Во втором терминале открываю лог системных сообщений. В первом терминале перезапускаю DNS-сервер. После исправления всех ошибок и опечаток DNS-сервер запускается успешно (рис. 2.19).



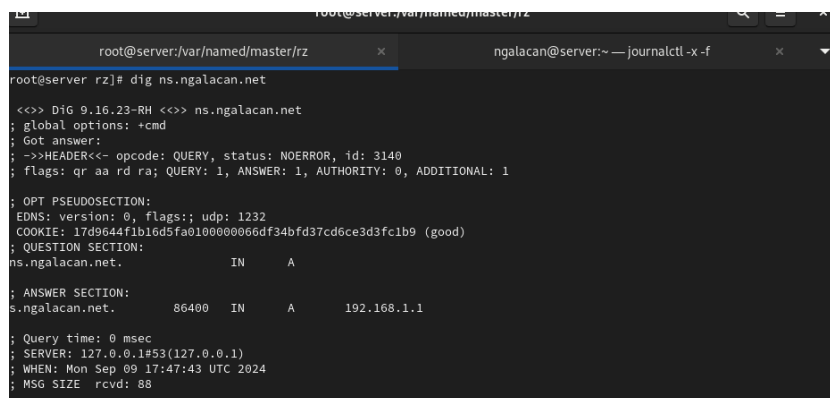
```
root@server:/var/named/master/rz
not supported
(gedit:7048): dconf-WARNING **: 17:45:59.231: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
[root@server rz]# systemctl restart named
[root@server rz]# systemctl status named.service
named.service - Berkeley Internet Name Domain (DNS)
Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
Active: active (running) since Mon 2024-09-09 17:46:14 UTC; 5s ago
Process: 7103 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkc
Process: 7105 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7106 (named)
Tasks: 5 (limit: 4557)
Memory: 15.5M
CPU: 55ms
CGroup: /system.slice/named.service
└─7106 /usr/sbin/named -u named -c /etc/named.conf

Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:1b8:10::b#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:7fd:1#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:dc3:35#53
Sep 09 17:46:15 server named[7106]: timed out resolving './DNSKEY/IN': 127.0.0.1#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Sep 09 17:46:15 server named[7106]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Sep 09 17:46:15 server named[7106]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
[root@server rz]#
```

Рис. 2.19: Запуск DNS-сервера после исправления ошибок

2.4 Анализ работы DNS-сервера

При помощи утилиты dig получаю описание DNS-зоны с сервера ns.ngalacan.net (рис. 2.20).



```
root@server:/var/named/master/rz
root@server rz]# dig ns.ngalacan.net

<<>> DiG 9.16.23-RH <<>> ns.ngalacan.net
; global options: +cmd
; Got answer:
; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 3140
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
EDNS: version: 0, flags:; udp: 1232
COOKIE: 17d9644f1b16d5fa0100000066df34bfd37cd6ce3d3fc1b9 (good)
; QUESTION SECTION:
ns.ngalacan.net.                IN      A

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

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Mon Sep 09 17:47:43 UTC 2024
; MSG SIZE rcvd: 88
```

Рис. 2.20: Описание DNS-зоны с сервера ns.ngalacan.net

Анализирую корректность работы DNS-сервера (рис. 2.21).

```
[root@server rz]# host -l ngalacan.net
ngalacan.net name server ngalacan.net.
ngalacan.net has address 192.168.1.1
ns.ngalacan.net has address 192.168.1.1
server.ngalacan.net has address 192.168.1.1
[root@server rz]# host -a ngalacan.net
Trying "ngalacan.net"
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 46020
; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
ngalacan.net.      86400   IN      SOA     ngalacan.net. server.ngalacan.net. 2024090900 86400 3600 604800 1080
0
ngalacan.net.      86400   IN      NS      ngalacan.net.
ngalacan.net.      86400   IN      A       192.168.1.1

;; ADDITIONAL SECTION:
ngalacan.net.      86400   IN      A       192.168.1.1

Received 119 bytes from 127.0.0.1#53 in 10 ms
[root@server rz]# host -t A ngalacan.net
ngalacan.net has address 192.168.1.1
[root@server rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ngalacan.net.1.168.192.in-addr.arpa.
1.1.168.192.in-addr.arpa domain name pointer server.ngalacan.net.1.168.192.in-addr.arpa.
[root@server rz]#
```

Рис. 2.21: Анализ корректности работы DNS-сервера

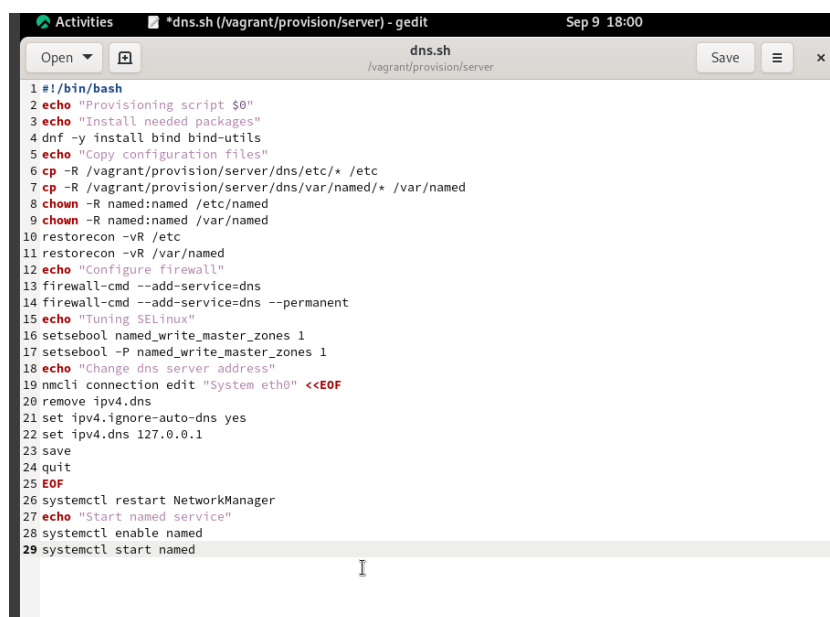
2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

Перехожу в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создаю в нём каталог `dns`, в который помещаю в соответствующие каталоги конфигурационные файлы DNS (рис. 2.22).

```
[root@server ~]# cd /vagrant
[root@server vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master
[root@server vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master
[root@server vagrant]# cd /vagrant/provision
[root@server provision]# cd /server
-bash: cd: /server: No such file or directory
[root@server provision]# cd /server
-bash: cd: /server: No such file or directory
[root@server provision]# cd server
[root@server server]# touch dns.sh
[root@server server]# chmod +x dns.sh
[root@server server]#
```

Рис. 2.22: Размещение конфигурационных файлов в каталог `/vagrant/provision/server/dns`

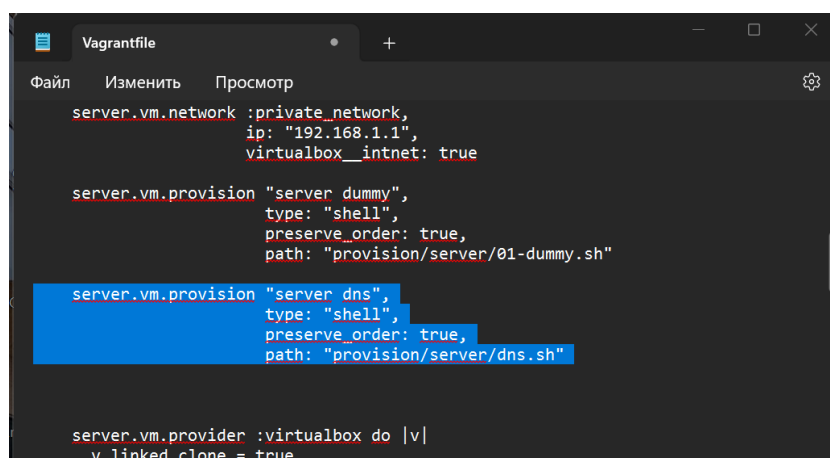
Создаю скрипт `dns.sh` (рис. 2.23).

A screenshot of a terminal window titled "dns.sh (/vagrant/provision/server) - gedit". The window shows a shell script with 29 lines of code. The script starts with a shebang and includes several echo statements for logging. It then uses dnf to install bind and bind-utils, copies configuration files from /etc to /var/named, and sets permissions. It also configures the firewall to allow DNS traffic and starts the named service. The script ends with EOF.

```
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 "System 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
25 EOF
26 systemctl restart NetworkManager
27 echo "Start named service"
28 systemctl enable named
29 systemctl start named
```

Рис. 2.23: Редактирование скрипта dns.sh

Для отработки созданного скрипта во время загрузки виртуальной машины в конфигурационном файле Vagrantfile вношу изменения в разделе конфигурации для сервера (рис. 2.24).

A screenshot of a text editor window titled "Vagrantfile". The window shows the Vagrantfile configuration. The "server.vm.network" section is highlighted in blue. The "server.vm.provision" section is also highlighted in blue, showing the configuration for the "server dns" provisioner. The "server.vm.provider" section is also highlighted in blue, showing the configuration for the "virtualbox" provider.

```
server.vm.network :private_network,
  ip: "192.168.1.1",
  virtualbox____intnet: true

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"

server.vm.provider :virtualbox do |v|
  v.linked_clone = true
```

Рис. 2.24: Редактирование Vagrantfile

3 Выводы

В результате выполнения работы были приобретены практические навыки по установке и конфигурированию DNS-сервера, усвоены принципы работы системы доменных имён.

4 Ответы на контрольные вопросы

1. Что такое DNS?

- Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса компьютерами для идентификации друг друга в сети.

2. Каково назначение кэширующего DNS-сервера?

- Его задача - хранить результаты предыдущих DNS-запросов в памяти. Когда клиент делает запрос, кэширующий DNS проверяет свой кэш, и если он содержит соответствующую информацию, сервер возвращает ее без необходимости обращаться к другим DNS-серверам. Это ускоряет процесс запроса.

3. Чем отличается прямая DNS-зона от обратной?

- Прямая зона преобразует доменные имена в IP-адреса, обратная зона выполняет обратное: преобразует IP-адреса в доменные имена.

4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.

- В Linux-системах обычно используется файл `/etc/named.conf` для общих настроек. Зоны хранятся в файлах в каталоге `/var/named/`, например, `/var/named/example.com.zone`.

5. Что указывается в файле `resolv.conf`?

- Содержит информацию о DNS-серверах, используемых системой, а также о параметрах конфигурации.
6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?
- A (IPv4-адрес), AAAA (IPv6-адрес), CNAME (каноническое имя), MX (почтовый сервер), NS (имя сервера), PTR (обратная запись), SOA (начальная запись зоны), TXT (текстовая информация).
7. Для чего используется домен in-addr.arpa?
- Используется для обратного маппинга IP-адресов в доменные имена.
8. Для чего нужен демон named?
- Это DNS-сервер, реализация BIND (Berkeley Internet Name Domain).
9. В чём заключаются основные функции slave-сервера и master-сервера?
- Master-сервер хранит оригинальные записи зоны, slave-серверы получают копии данных от master-сервера.
10. Какие параметры отвечают за время обновления зоны?
- refresh, retry, expire, и minimum.
11. Как обеспечить защиту зоны от скачивания и просмотра?
- Это может включать в себя использование TSIG (Transaction SIGnatures) для аутентификации между серверами.
12. Какая запись RR применяется при создании почтовых серверов?
- MX (Mail Exchange).

13. Как протестировать работу сервера доменных имён?
- Используйте команды `nslookup`, `dig`, или `host`.
14. Как запустить, перезапустить или остановить какую-либо службу в системе?
- `systemctl start|stop|restart` .
15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?
- Используйте опции, такие как `-d` или `-v` при запуске службы.
16. Где хранится отладочная информация по работе системы и служб? Как её посмотреть?
- В системных журналах, доступных через `journalctl`.
17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров.
- `lsdf -p` или `fuser -v` .
18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса `nmcli`.
- Примеры включают `nmcli connection up|down` .
19. Что такое SELinux?
- Это мандатный контроль доступа для ядра Linux.
20. Что такое контекст (метка) SELinux?
- Метка, определяющая, какие ресурсы могут быть доступны процессу или объекту.

21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?
- `restorecon -Rv`.
22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?
- Используйте `audit2allow`.
23. Что такое булевый переключатель в SELinux?
- Это параметр, который включает или отключает определенные аспекты защиты SELinux.
24. Как посмотреть список переключателей SELinux и их состояние?
- `getsebool -a`.
25. Как изменить значение переключателя SELinux?
- `setsebool -P <on|off>`.