

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2**

**«НАСТРОЙКА DNS-СЕРВЕРА »**

*дисциплина: Администрирование сетевых подсистем*

Студент: Саргсян Арам Грачьевич

Группа: НПИбд 02-20

**МОСКВА**

2022 г.

## ЦЕЛЬ РАБОТЫ:

ПРИОБРЕТЕНИЕ ПРАКТИЧЕСКИХ НАВЫКОВ ПО УСТАНОВКЕ И КОНФИГУРИРОВАНИЮ DNS-СЕРВЕРА, УСВОЕНИЕ ПРИНЦИПОВ РАБОТЫ СИСТЕМЫ ДОМЕННЫХ ИМЕН

## ХОД РАБОТЫ

- 1) Я запустил виртуальную машину server, зашел в свой аккаунт, открыл терминал, в режиме суперпользователя установил bind, bind-utils (Рис. 1).

```
[agsargsyan@server.agsargsyan.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.

[sudo] password for agsargsyan:
[root@server.agsargsyan.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 9   12 kB/s | 15 kB   00:01
Extra Packages for Enterprise Linux 9   4.9 MB/s | 11 MB   00:02
Rocky Linux 9 - BaseOS                  7.8 kB/s | 3.6 kB   00:00
Rocky Linux 9 - [ === ] --- B/s | 0 B    -:-- ETA
```

Рис. 1

- 2) Сделал запрос к DNS адресу [www.yandex.ru](http://www.yandex.ru), в отчете мы видим результат зпроса, запрос проходит через порт 53, статус без ошибки, ip адреса шлюза и источника (Рис. 2).

```
; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48253
;; 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: 3 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Fri Nov 11 13:48:50 UTC 2022
;; MSG SIZE rcvd: 95
```

Рис. 2

- 3) Запустил DNS-сервер, включил запуск DNS-сервера в автозапуск при загрузке системы (Рис. 3).

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

Рис. 3

- 4) Просмотрел отличие выведенной на экран информации при выполнении команд `dig www.yandex.ru` и `dig @127.0.0.1 www.yandex.ru`, время запроса увеличилась вдвое (Рис. 4).

```
; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26639
;; 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      5.255.255.70
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      77.88.55.60

;; Query time: 6 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Fri Nov 11 13:51:22 UTC 2022
;; MSG SIZE rcvd: 95

[root@server.agsargsyan.net ~]# dig
```

Рис. 4

- 5) Сделал DNS-сервер сервером по умолчанию, перезапустил NetworkManager (Рис. 5).

```
[root@server.agsargsyan.net ~]# 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), 802-1x, 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 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully up
dated.
nmcli> quit
[root@server.agsargsyan.net ~]# systemctl restart NetworkManager
[root@server.agsargsyan.net ~]#
```

Рис. 5

- 6) Настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server, для этого внес изменения в файл /etc/named.conf (Рис. 6).

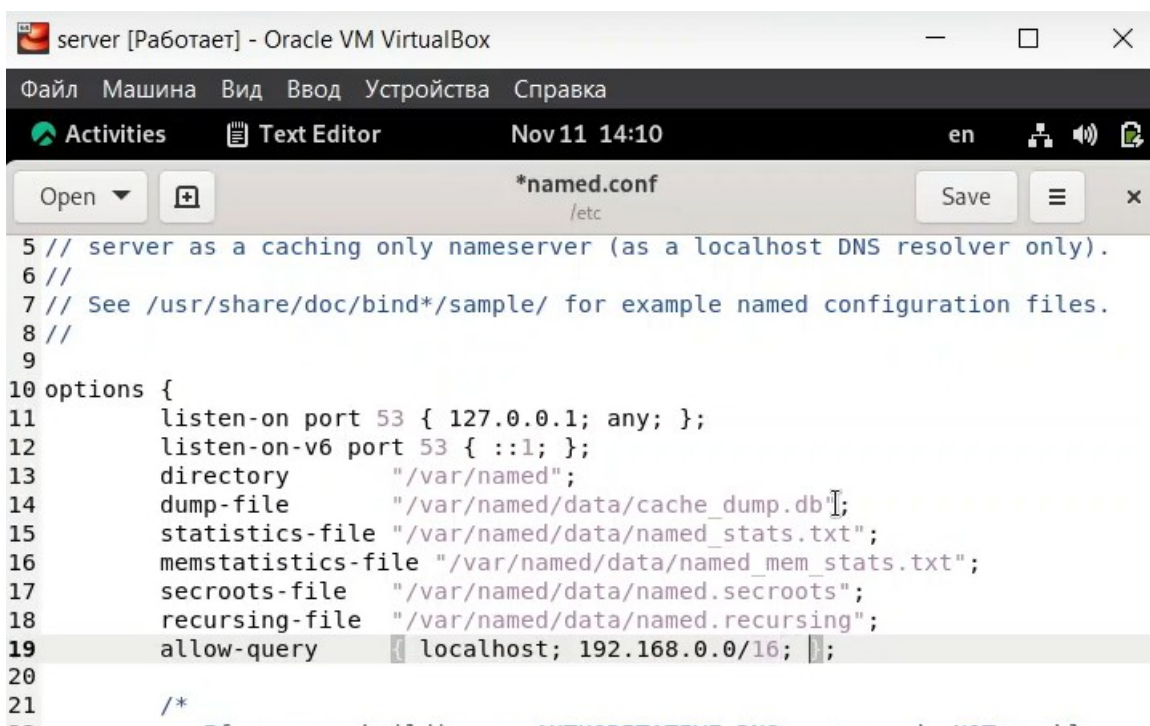


Рис. 6

- 7) Внес изменения в настройки межсетевого экрана узла server, разрешив работу с DNS (Рис. 7).

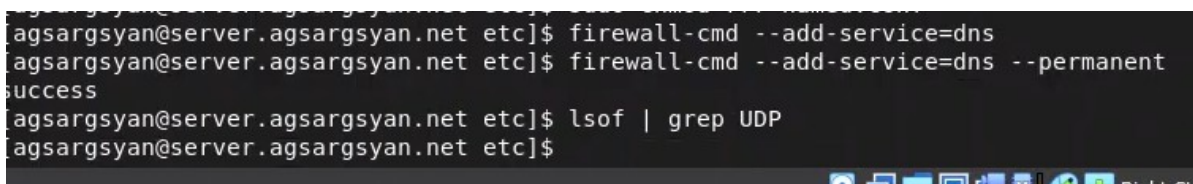


Рис. 7

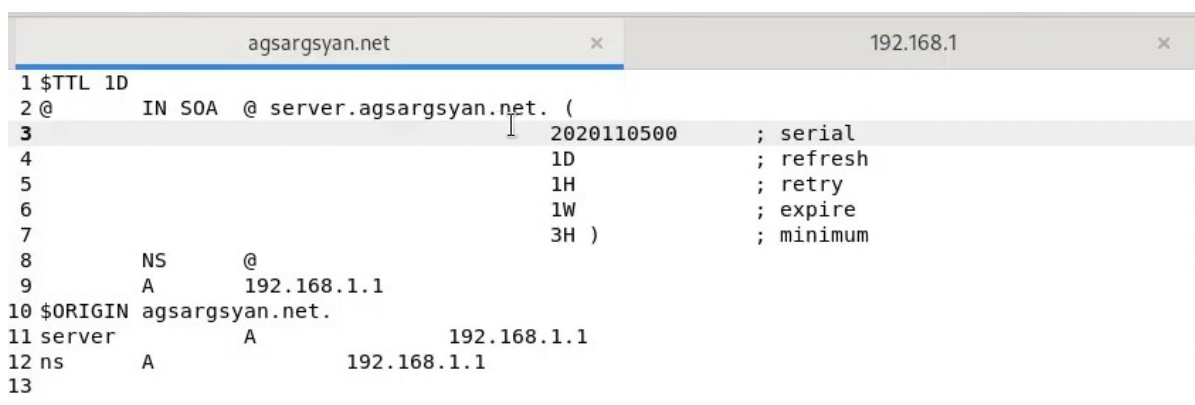
- 8) Скопировал шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименовал его в agsargsyan.net, поменял содержимое файла для дальнейшей работы (Рис. 8).



```
1 zone "agsargsyan.net" IN {
2     type master;
3     file "master/fz/agsargsyan.net";
4     allow-update { none; };
5 };
6
7
8 zone "1.168.192.in-addr.arpa" IN {
9     type master;
10    file "master/rz/192.168.1";
11    allow-update { none; };
12 };
13
```

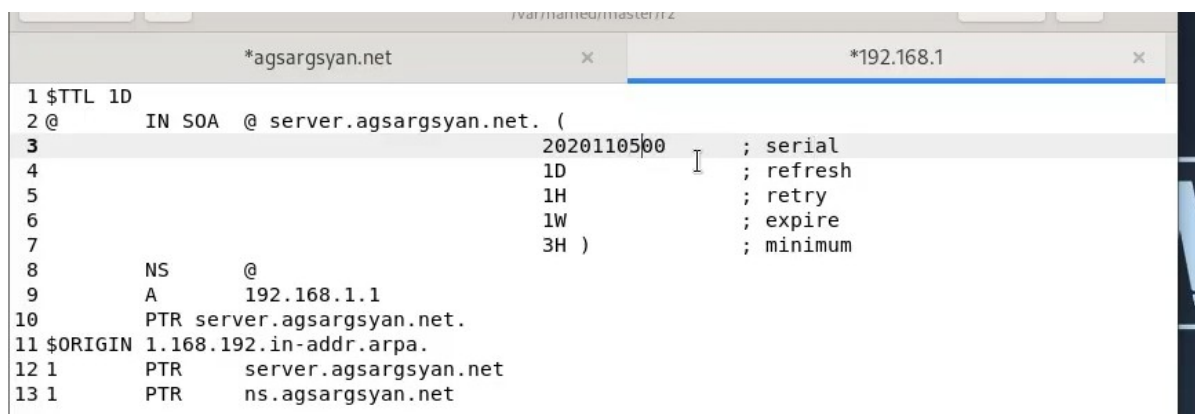
Рис. 8

9) В каталоге /var/named создал подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно, создал нужные файлы и поменял всё содержимое (Рис. 9-10).



```
1 $TTL 1D
2 @      IN SOA  @ server.agsargsyan.net. (
3         2020110500      ; serial
4         1D              ; refresh
5         1H              ; retry
6         1W              ; expire
7         3H              ; minimum
8     NS      @
9     A       192.168.1.1
10 $ORIGIN agsargsyan.net.
11 server    A       192.168.1.1
12 ns        A       192.168.1.1
13
```

Рис. 9



```
1 $TTL 1D
2 @      IN SOA  @ server.agsargsyan.net. (
3         2020110500      ; serial
4         1D              ; refresh
5         1H              ; retry
6         1W              ; expire
7         3H              ; minimum
8     NS      @
9     A       192.168.1.1
10 PTR      server.agsargsyan.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1        PTR      server.agsargsyan.net
13 1        PTR      ns.agsargsyan.net
```

Рис. 10

10) Исправили права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать (Рис. 11).



```

chown: changing ownership of /etc/named : operation not permitted
[agsargsyan@server.agsargsyan.net ~]$ sudo chown -R named:named /etc/named
[sudo] password for agsargsyan:
[agsargsyan@server.agsargsyan.net ~]$ sudo chown -R named:named /var/named
[agsargsyan@server.agsargsyan.net ~]$

```

Рис. 11

- 11) Восстановили метки измененных файлов в SELinux, проверил состояния переключателей SELinux, и дал named разрешение на запись в файлы DNS-зоны (Рис. 12).

```

[agsargsyan@server.agsargsyan.net ~]$ sudo 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
[agsargsyan@server.agsargsyan.net ~]$ sudo restorecon -vR /var/named
[agsargsyan@server.agsargsyan.net ~]$ getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[agsargsyan@server.agsargsyan.net ~]$ setsebool named_write_master_zones 1
Could not change active booleans. Please try as root: Permission denied
[agsargsyan@server.agsargsyan.net ~]$ sudo setsebool -P named_write_master_zones 1
[agsargsyan@server.agsargsyan.net ~]$

```

Рис. 12

- 12) В дополнительном терминале запустил в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы (Рис. 13).

```

[agsargsyan@server.agsargsyan.net ~]$ journalctl -x -f
Nov 11 17:44:42 server.agsargsyan.net kernel: SELinux: policy capability extended_socket_classes=1
Nov 11 17:44:42 server.agsargsyan.net kernel: SELinux: policy capability always_check_networkark=0
Nov 11 17:44:42 server.agsargsyan.net kernel: SELinux: policy capability cgroup_seclabel=1
Nov 11 17:44:42 server.agsargsyan.net kernel: SELinux: policy capability nnp_nosuid_transition=1
Nov 11 17:44:42 server.agsargsyan.net kernel: SELinux: policy capability genfs_seclabel_symlinks=0
Nov 11 17:44:42 server.agsargsyan.net setsebool[9570]: The named_write_master_zones policy boolean was changed to 1 by root
Nov 11 17:44:42 server.agsargsyan.net sudo[9568]: pam_unix(sudo:session): session closed for user root
Nov 11 17:44:52 server.agsargsyan.net dbus-broker-launch[2000]: avc: op=load_policy lsm=selinux seqno=4 res=1
Nov 11 17:44:52 server.agsargsyan.net systemd[1923]: selinux: avc: op=load_policy lsm=selinux seqno=4 res=1
Nov 11 17:44:52 server.agsargsyan.net systemd[1923]: Started VTE child process 9582 launched by gnome-terminal-server process 9113.
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit UNIT has finished successfully.

The job identifier is 1114.

```

Рис. 13

- 13) В первом терминале перезапустил DNS-сервер (Рис. 14).

```

[agsargsyan@server.agsargsyan.net ~]$ sudo systemctl restart named
[agsargsyan@server.agsargsyan.net ~]$

```

Рис. 14

- 14) При помощи dig получил описание DNS-зоны с сервера ns.agsargsyan.net (Рис. 15-16).

```
[agsargsyan@server.agsargsyan.net ~]$ sudo dig ns.agsargsyan.net
[sudo] password for agsargsyan:

; <<>> DiG 9.16.23-RH <<>> ns.agsargsyan.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52282
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 2104770401c0ba0501000000636e8a992ad25570b913b3c9 (good)
;; QUESTION SECTION:
ns.agsargsyan.net.          IN      A

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

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 11 17:47:05 UTC 2022
;; MSG SIZE rcvd: 90

[agsargsyan@server.agsargsyan.net ~]$ sudo host -l agsargsyan.net
agsargsyan.net name server agsargsyan.net.
agsargsyan.net has address 192.168.1.1
ns.agsargsyan.net has address 192.168.1.1
server.agsargsyan.net has address 192.168.1.1
[agsargsyan@server.agsargsyan.net ~]$ sudo host -a
```

Рис. 15

```
[agsargsyan@server.agsargsyan.net ~]$ sudo host -l agsargsyan.net
agsargsyan.net name server agsargsyan.net.
agsargsyan.net has address 192.168.1.1
ns.agsargsyan.net has address 192.168.1.1
server.agsargsyan.net has address 192.168.1.1
[agsargsyan@server.agsargsyan.net ~]$ sudo host -a agsargsyan.net
Trying "agsargsyan.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36980
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
agsargsyan.net.          IN      ANY

;; ANSWER SECTION:
agsargsyan.net.         86400   IN      SOA     agsargsyan.net. server.agsargsyan.net. 20201
10500 86400 3600 604800 10800
agsargsyan.net.         86400   IN      NS      agsargsyan.net.
agsargsyan.net.         86400   IN      A       192.168.1.1

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

Received 121 bytes from 127.0.0.1#53 in 2 ms
[agsargsyan@server.agsargsyan.net ~]$ host -t A agsargsyan.net
agsargsyan.net has address 192.168.1.1
[agsargsyan@server.agsargsyan.net ~]$ host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.agsargsyan.net.1.168.192.in-addr.arpa.
1.1.168.192.in-addr.arpa domain name pointer ns.agsargsyan.net.1.168.192.in-addr.arpa.
[agsargsyan@server.agsargsyan.net ~]$
```

Рис. 16

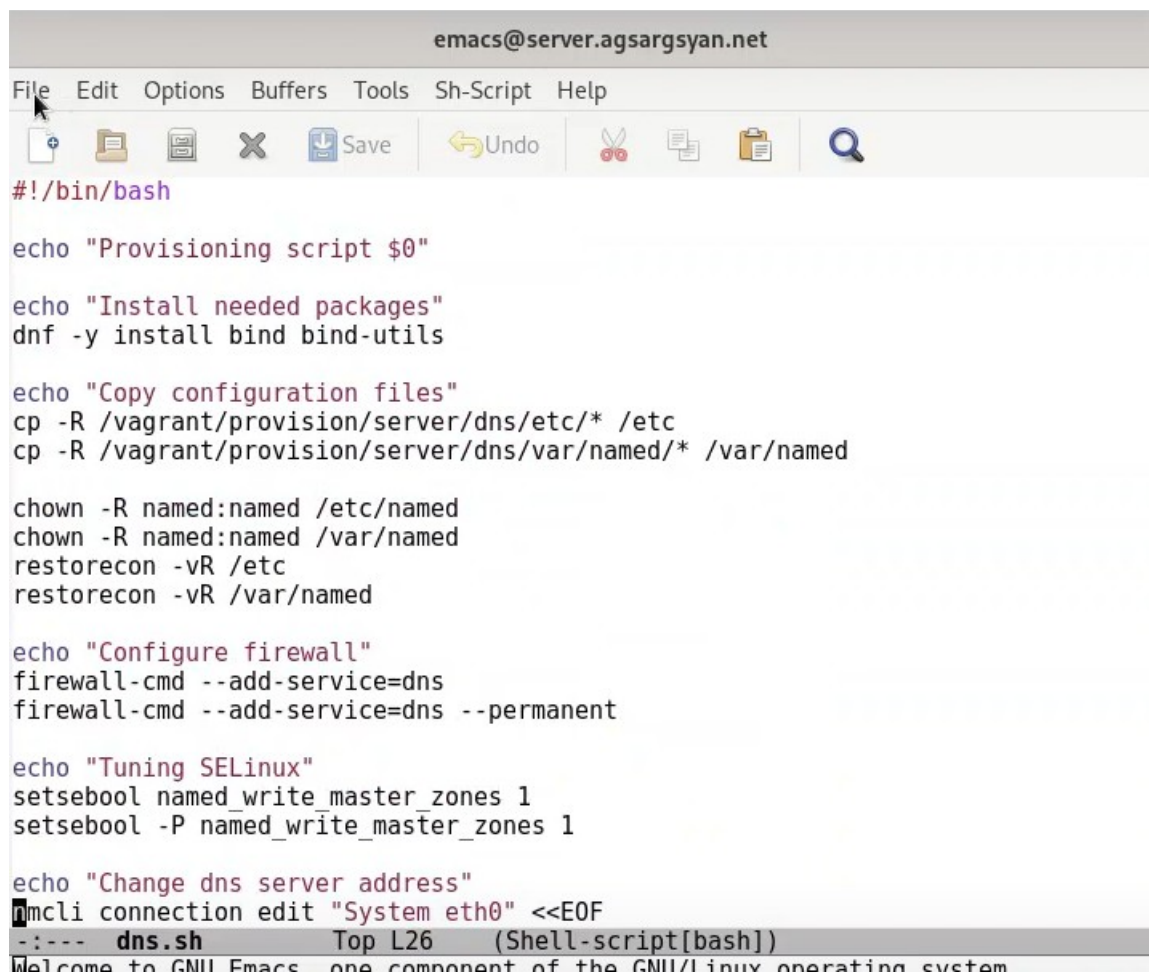
- 15) На виртуальной машине server перешел в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создал в нём

каталог `dns`, в который поместил в соответствующие каталоги конфигурационные файлы DNS, создал файл `dns.sh` и сделал его исполняемым (Рис. 17).

```
[agsargsyan@server.agsargsyan.net ~]$ cd /vagrant
[agsargsyan@server.agsargsyan.net vagrant]$ mkdir -p /vagrant/provision/server/dns/etc/named
[agsargsyan@server.agsargsyan.net vagrant]$ mkdir -p /vagrant/provision/server/dns/var/named/master/
[agsargsyan@server.agsargsyan.net vagrant]$ cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[agsargsyan@server.agsargsyan.net vagrant]$ cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master
[agsargsyan@server.agsargsyan.net vagrant]$ cp -R /etc/named/* /vagrant/provision/server/dns/etc/
cp: target '/vagrant/provision/server/dns/etc/' is not a directory
[agsargsyan@server.agsargsyan.net vagrant]$ cp -R /etc/named/* /vagrant/provision/server/dns/etc/
[agsargsyan@server.agsargsyan.net vagrant]$ cd /provision/server
bash: cd: /provision/server: No such file or directory
[agsargsyan@server.agsargsyan.net vagrant]$ cd provision
[agsargsyan@server.agsargsyan.net provision]$ cd server
[agsargsyan@server.agsargsyan.net server]$ touch dns.sh
[agsargsyan@server.agsargsyan.net server]$ chmod +x dns.sh
[agsargsyan@server.agsargsyan.net server]$
```

Рис. 17

16) Прописал в нём необходимый скрипт (Рис. 18).



The screenshot shows the Emacs editor interface with the title bar `emacs@server.agsargsyan.net`. The menu bar includes `File`, `Edit`, `Options`, `Buffers`, `Tools`, `Sh-Script`, and `Help`. The toolbar contains icons for file operations and editing. The main text area displays a shell script for provisioning a DNS server. The script includes commands for installing packages, copying configuration files, setting permissions, configuring the firewall, tuning SELinux, and changing the DNS server address. The script is saved as `dns.sh` in the `System` connection.

```
#!/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
-:--- dns.sh Top L26 (Shell-script[bash])
Welcome to GNU Emacs, one component of the GNU/Linux operating system
```

Рис. 18

17) Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` в разделе конфигурации для сервера добавил нужные строки (Рис. 19).





```
*Vagrantfile – Блокнот
Файл  Правка  Формат  Вид  Справка

path: "provision/default/01-user.sh"

# Server configuration
config.vm.define "server", autostart: false do |server|
  server.vm.box = "rocky9"
  server.vm.hostname = 'server'

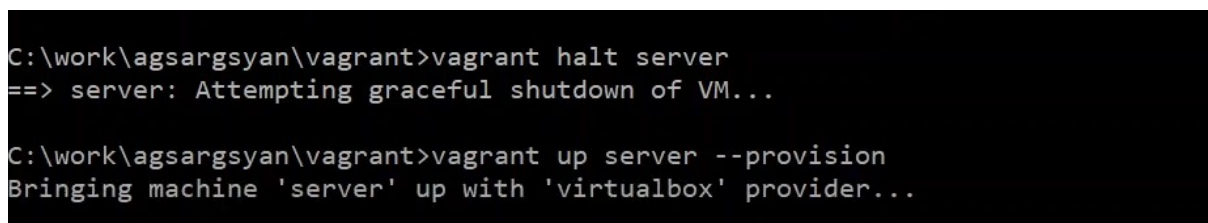
  server.ssh.insert_key = false
  server.ssh.username = 'vagrant'
  server.ssh.password = 'vagrant'

  server.vm.network :private_network, ip: "192.168.1.1", vir

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

Рис. 19

18)Перезагрузил машину для сохранения настроек (Рис. 19).



```
C:\work\agsargsyan\vagrant>vagrant halt server
==> server: Attempting graceful shutdown of VM...

C:\work\agsargsyan\vagrant>vagrant up server --provision
Bringing machine 'server' up with 'virtualbox' provider...
```

Рис. 20

## ОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ

### 1. Что такое DNS?

DNS — система доменных имён, распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес и наоборот.

### 2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.

### 3. Чем отличается прямая DNS-зона от обратной?

Задача поиска доменного имени по IP-адресу является обратной к прямой задаче — поиску IP-адреса по доменному имени. Прямая решается в DNS при

помощи записей типа A (Address). Обратная же при помощи записей-указателей типа PTR (Pointer), которые совместно с записями SOA и NS составляют описание так называемой «обратной» зоны.

#### **4. В каких каталогах и файлах располагаются настройки DNS-сервера?**

**Кратко охарактеризуйте, за что они отвечают.**

В файле `host.conf` содержатся опции программы-определителя, в файле `resolv.conf` содержатся адреса серверов имен, к которым имеет доступ данная система. Файл `named.ca` организует кэширование для сервера имен.

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

В файле `resolv.conf` содержатся адреса серверов имен, к которым имеет доступ данная система.

#### **6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?**

- SOA-запись — указывает на авторитативность для зоны
- NS-запись — перечисляет DNS-серверы зоны
- A — отображение имён узлов в адреса
- PTR — отображение адресов в имена узлов
- CNAME — каноническое имя (для псевдонимов)
- MX — отображение имён почтовых серверов

#### **7. Для чего используется домен `in-addr.arpa`?**

Для отображения IP-адресов IPv4 в пространство доменных имен

#### **8. Для чего нужен демон `named`?**

Демон `named` может реализовывать функции серверов любого типа: `master`, `slave`, `cache`.

#### **9. В чём заключаются основные функции `slave`-сервера и `master`-сервера?**

`master` — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых

`slave` — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.

**10. Какие параметры отвечают за время обновления зоны?**

За обновление отвечает третий параметр в файле `agsargsyan.net`

**11. Как обеспечить защиту зоны от скачивания и просмотра?**

Задать подходящие права доступа на чтение и запись.

**12. Какая запись RR применяется при создании почтовых серверов?**

При создании почтовых серверов используют `A` записи.

**13. Как протестировать работу сервера доменных имён?**

При помощи утилиты `host`

**14. Как запустить, перезапустить или остановить какую-либо службу в системе?**

Использовать в терминале команды `systemctl start, restart, stop`.

**15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?**

Посмотреть в `journalctl`.

**16. Где храниться отладочная информация по работе системы и служб?  
Как её посмотреть?**

В журнале

**17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров.**

**18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса `nmcli`.**

```
nmcli connection edit System\ eth0
remove ipv4.dns set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
```

**19. Что такое SELinux?**

(SELinux) - это модуль безопасности ядра Linux, который обеспечивает механизм поддержки политик безопасности контроля доступа, включая обязательные элементы управления доступом (MAC).

**20. Что такое контекст (метка) SELinux?**

Каждый файл, процесс, каталог и порт имеют специальную метку

безопасности, известную как контекст SELinux, который является именем, используемым для определения, может ли процесс получить доступ к файлу, каталогу или порту.

**21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?**

Нужно использовать команду `restorecon`.

**22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?**

Использовать команду `chown -R`

**23. Что такое булевый переключатель в SELinux?**

Способ настройки файлов модуля.

**24. Как посмотреть список переключателей SELinux и их состояние?**

Команда `getsebool -a | grep named`

**25. Как изменить значение переключателя SELinux**

Необходимо использовать команду `setsebool`.

## **ВЫВОД**

Я установил и сконфигурировал DNS-сервер, и разобрался с основными принципами системы доменных имён.