Лабораторная работа №2

Настройка DNS-сервера

Сахно Никита НФИбд-02-23

Содержание

1 Цель работы

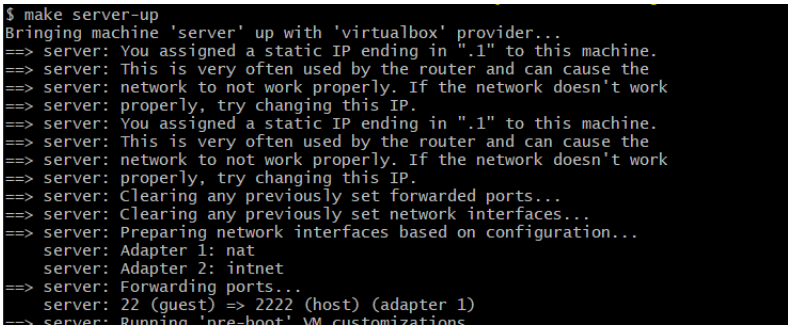
Приобрести практические навыки по установке и конфигурированию DNS-сервера, усвоить принципы работы системы доменных имён.

2 Задание

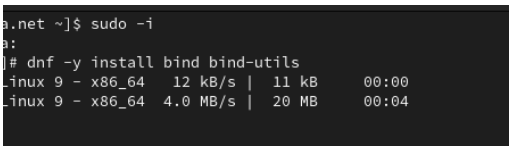
1. Установите на виртуальной машине server DNS-сервер bind и bind-utils.
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер.
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер.
4. При помощи утилит dig и host проанализируйте работу DNS-сервера.
5. Напишите скрипт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

3 Выполнение лабораторной работы

Загрузим операционную систему и перейдем в рабочий каталог с проектом: `cd C:\Users\nikita\work\study\nvsakhno\vagrant\` Затем запустим виртуальную машину server с помощью команды: `make server-up` На виртуальной машине server войдем под созданным в предыдущей работе пользователем и откроем терминал. Перейдем в режим суперпользователя и установим bind и bind-utils:

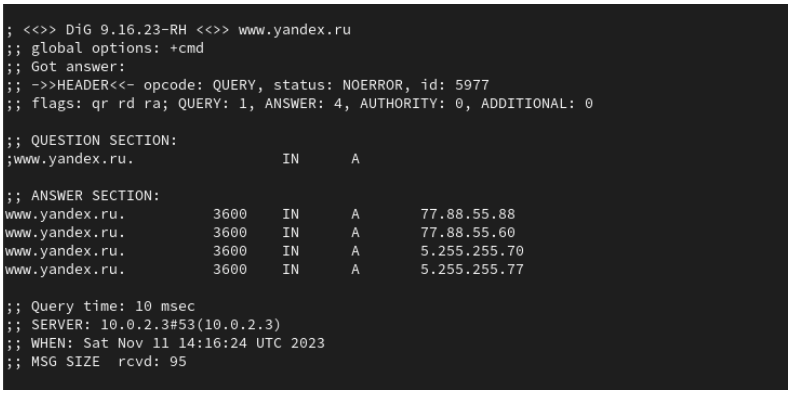


Команда make server-up



Установка bind и bind-utils в режиме суперпользователя

С помощью утилиты dig сделаем запрос к DNS-адресу www.yandex.ru:



Команда dig

Давайте рассмотрим разделы данного вывода подробней:

- HEADER (заголовок): показывает версию dig, глобальные опции используемые с командой и другую дополнительную информацию
- QUESTION SECTION (секция запроса): Показывает наш запрос, то есть мы запросили показать A-запись (команда dig без параметров) для домена www.yandex.ru
- ANSWER SECTION (секция ответа): Показывает ответ полученный от DNS, в нашем случае показывает A-запись для www.yandex.ru Последняя секция это статистика по запросу (служебная информация)- время выполнения запроса (10

мс), имя DNS-сервера который запрашивался, когда был создан запрос и размер сообщения

Конфигурирование кэширующего DNS-сервера

В отчёте проанализируем построчно содержание файлов /etc/resolv.conf, /etc/named.conf, /var/named/named.ca, /var/named/named.localhost, /var/named/named.loopback. Рассмотрим /etc/resolv.conf. В нём указано имя сервера и его адрес:

```
# Generated by NetworkManager
search dmbelicheva.net
nameserver 10.0.2.3
```

Рассмотрим содержимое файле `/var/named/named.localhost`. В нём есть:

- Запись начала полномочий (SOA), которая указывает начало зоны и включает имя хоста, на котором находится файл данных name.local.
- Запись сервера имен (NS), идентифицирующая главный и подчиненные серверы имен DNS.
- Указаны адреса IPv4 и IPv6 локального хоста.

В файле `/var/named/named.loopback` все аналогично, только добавляется:

- PTR-запись для локального хоста

```
$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.
```

Файлы loopback и localhost

Далее запустим DNS-сервер, включим запуск DNS-сервера в автозапуск при загрузке системы. Проанализируем отличие в выведенной на экран информации при выполнении команд `dig www.yandex.ru` и `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: 54474
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74db22a239f573ee01000000654f9fbb2cd8ed508af81ef8 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          300     IN      A       5.255.255.70
www.yandex.ru.          300     IN      A       5.255.255.77
www.yandex.ru.          300     IN      A       77.88.55.88
www.yandex.ru.          300     IN      A       77.88.55.60

;; Query time: 653 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 11 15:37:31 UTC 2023
;; MSG SIZE  rcvd: 134
```

Команда dig

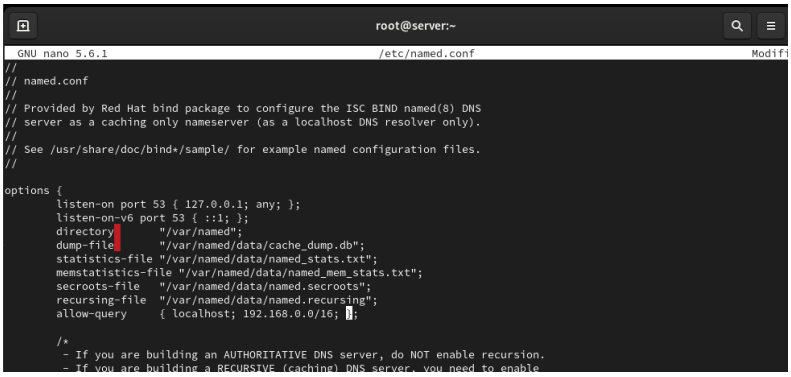
При указании опрашиваемого адреса в строке с адресом сервера написан адрес, который указывали, также указаны куки, а время запроса увеличилось.

Сделаем 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, затем сделаем тоже самое для соединения System eth0. Затем запустим NetworkManager и проверим наличие изменений в файле etc/resolv.conf(адрес сервера изменился на заданный нами):

```
===| 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' (d18d46cb-18cd-4f51-bb7b-4c35caa7c786) successfully updated.
nmcli> quit
[root@server.dmbelicheva.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 updated.
nmcli> quit
[root@server.dmbelicheva.net ~]# s
```

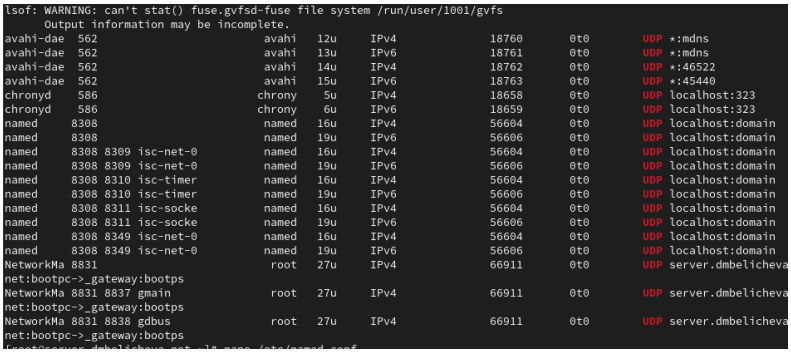
Изменение адреса dns-сервера

Настроим направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесем изменения в файл /etc/named.conf:



Изменение скрипта

Внесем изменения в настройки межсетевого экрана узла server, разрешив работу с DNS и убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53:



Внесение изменений

Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами

В случае возникновения в сети ситуации, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер. Для этого в конфигура- ционный файл named.conf в секцию options следует добавить:

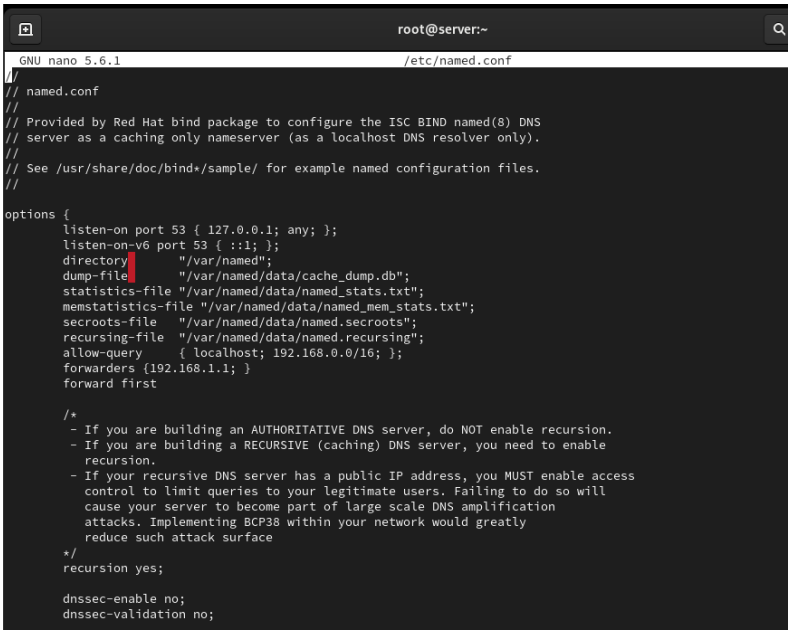
```
forwarders { список DNS-серверов };
forward first;
```

Текущий список DNS-серверов можно получить, введя на локальном хосте (на котором развёртывается образ виртуальной машины) следующую команду:

```
cat /etc/resolv.conf
```

Мы получили следующие данные для конфигурационного файла named.conf виртуальной машины server:

```
forwarders { 198.168.1.1; };
forward first;
```



Изменение скрипта

Конфигурирование первичного DNS-сервера

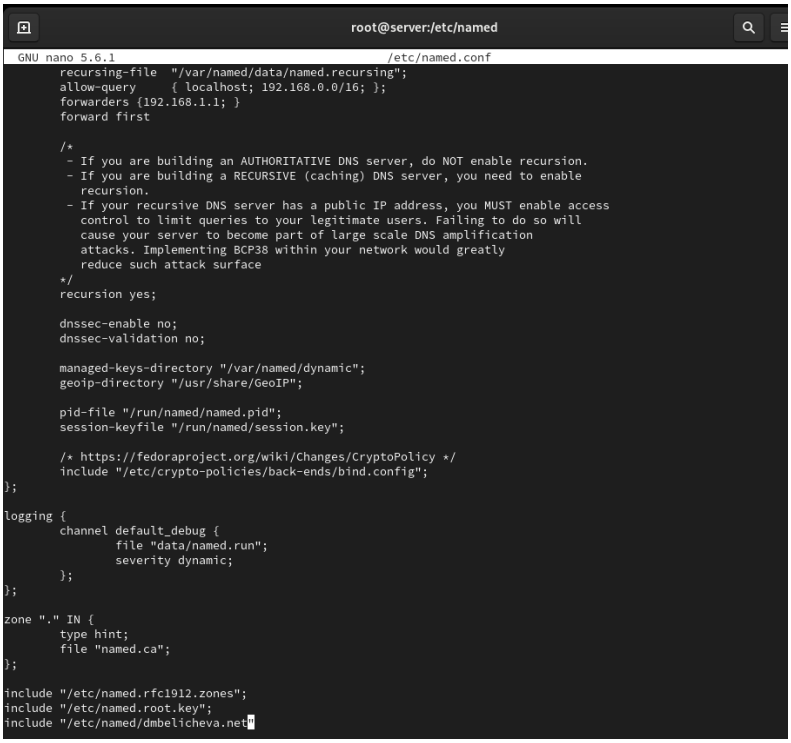
Скопируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуеме его в eademidova.net:

```
nano /etc/named.conf
cp /etc/named.rfc1912.zones /etc/named/
cd /etc/named
```

Окно терминала

Включим файл описания зоны /etc/named/nvsakhno.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку:

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



Изменение скрипта

Внесём изменения в файл nvsakhno.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 "dmbelicheva.net" IN {
        type master;
        file "master/fz/dmbelicheva.net";
        allow-update { none; };
};

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

Изменение скрипта

В каталоге /var/named создадим подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно, а затем скопируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуем его в eademidova.net:

```
cd /var/named
mkdir -p /var/named/master/fz
mkdir -p /var/named/master/rz
cp /var/named/named.localhost /var/named/master/fz/
cd /var/named/master/fz/
```

Изменение скрипта

Изменим файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны:

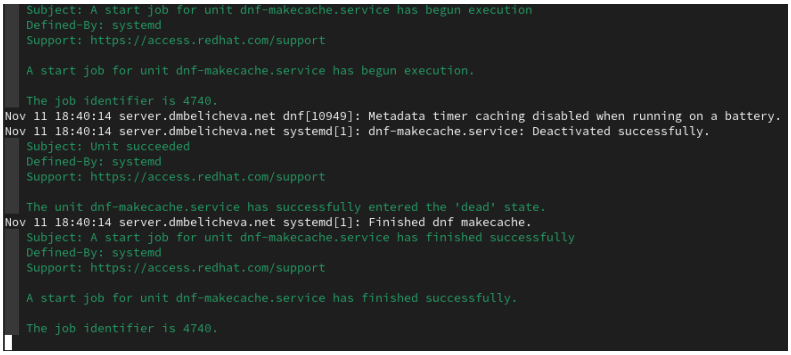
```
$TTL 1D
@       IN SOA  @ server.dmbelicheva.net. (
                                        2023111100      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
$ORIGIN dmbelicheva.net.
server  A       192.168.1.1
ns      A       192.168.1.1
```

Изменение скрипта

Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1, а также изменим файл:

Изменение скрипта

После изменения доступа к конфигурационным файлам named корректно восстановим специальные метки безопасности в SELinux, затем проверим состояние переключателей В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:



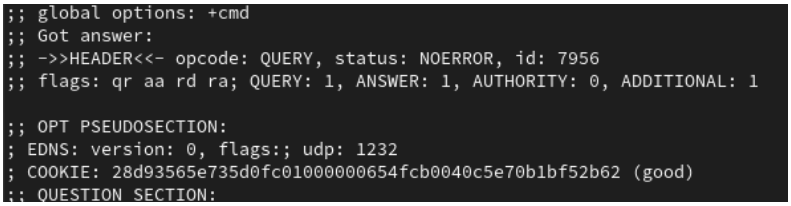
Запуск расширенного лога системных сообщений

В случае ошибок перезапустим DNS-сервер:

Перезапуск сервера

Анализ работы DNS-сервера

При помощи утилиты dig получим описание DNS-зоны с сервера ns.nvsakhno.net:



Утилита dig

При помощи утилиты host проанализируем корректность работы DNS-сервера, можно увидеть, что все внесённые нами изменения в работу сервера учтены:

Утилита host

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS, а затем в каталоге /vagrant/provision/server создадим исполняемый файл dns.sh:

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

Создание каталога dns и перенос в него файлов, создание dns.sh

Запишем в dns.sh следующий скрипт:

root@server:/vagrant/provision/server

GNU nano 5.6.1 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 "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
```

Изменение скрипта

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в разделе конфигурации для сервера:

Изменение Vagrantfile

4 Выводы

В процессе выполнения данной лабораторной работы я приобрел практические навыки по установке и конфигурированию DNS-сервера, усвоила принципы работы системы доменных имён.