Цель работы

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

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

Выполнение лабораторной работы

Загрузим операционную систему и перейдем в рабочий каталог с проектом: `cd C:\Users\dasha\work\study\tbmanturov\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:

```
[root@server.tbmanturov.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 10 - x86_64  30 kB/s |  34 kB     00:01
Extra Packages for Enterprise Linux 10 - x86_64 3.5 MB/s | 5.5 MB     00:01
```

Установка bind и bind-utils в режиме суперпользователя

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

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35394
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          480     IN      A       5.255.255.77
www.yandex.ru.          480     IN      A       77.88.44.55
```

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:

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

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`:

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

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):

```
[root@server.tbmanturov.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' (0a05b32b-3b8e-49f7-a76f-e48bb4a7ff13) successfully updated.
nmcli> quit
```

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:

```
[root@server.tbmanturov.net ~]# nmcli con
NAME  UUID                                  TYPE      DEVICE
eth0  0a05b32b-3b8e-49f7-a76f-e48bb4a7ff13  ethernet  eth0
eth1  d975d3c4-34b9-413d-b001-958ff55ba0a0  ethernet  eth1
lo    214bbc8b-8f13-41ef-9e94-2bd23924ee0c  loopback  lo
[root@server.tbmanturov.net ~]# sys
```

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:

```
[root@server.tbmanturov.net ~]# nmcli con
NAME  UUID                                  TYPE      DEVICE
eth0  0a05b32b-3b8e-49f7-a76f-e48bb4a7ff13  ethernet  eth0
eth1  d975d3c4-34b9-413d-b001-958ff55ba0a0  ethernet  eth1
lo    214bbc8b-8f13-41ef-9e94-2bd23924ee0c  loopback  lo
[root@server.tbmanturov.net ~]# sys
```

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;
```

```
 GNU nano 8.1                  /etc/named.conf                  Modified
//
// 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; };
```

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:

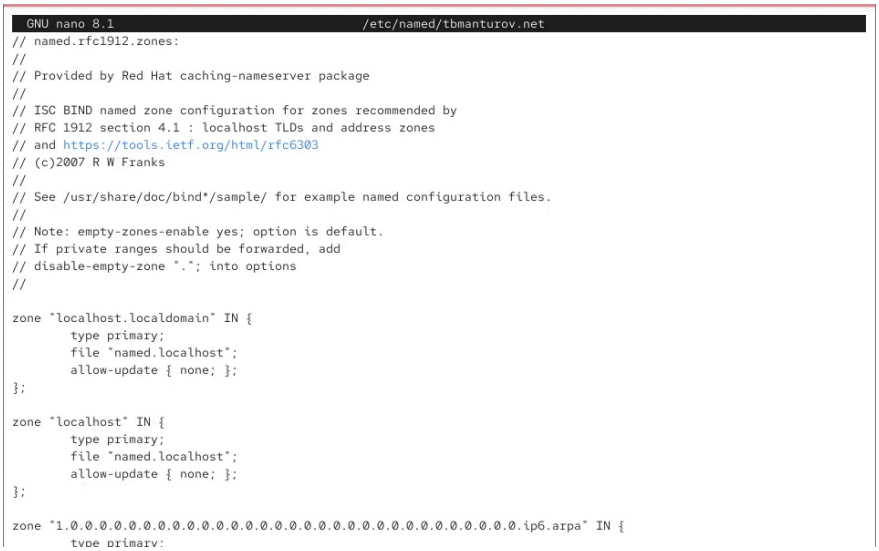
```
[root@server.tbmanturov.net etc]# cp /etc/named.rfc1912.zones /etc/named && mv /etc/named.rfc1912.zones /etc/named/tb
manturov.net
```

Окно терминала

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

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

Внесём изменения в файл tbmanturov.net:



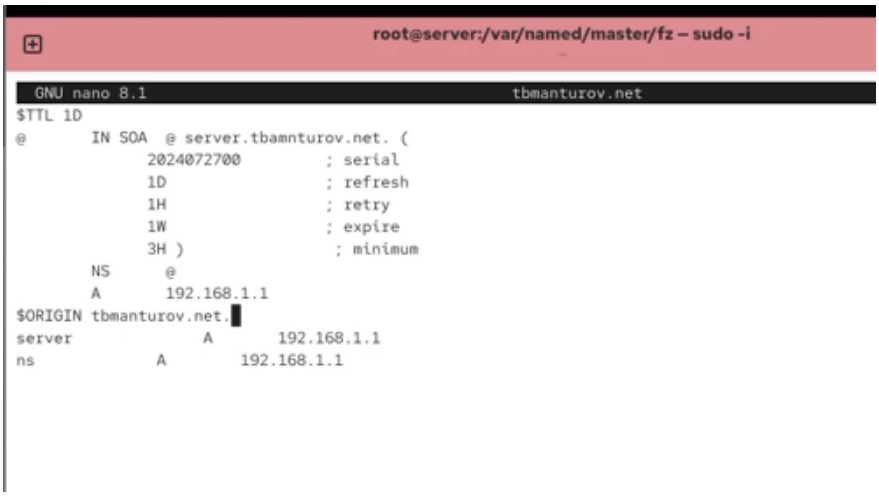
Изменение скрипта

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:

```
[root@server.tbmanturov.net etc]# cd /var/named
[root@server.tbmanturov.net named]# mkdir -p /var/named/master/fz
[root@server.tbmanturov.net named]# mkdir -p /var/named/master/rz
```

Изменение скрипта

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



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:

```
[root@server.tbmanturov.net rz]# chown -R named:named /etc/named
[root@server.tbmanturov.net rz]# chown -R named:named /var/named
[root@server.tbmanturov.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_
Relabeled /etc/lvm/devices/backup/system.devices-20251111.170239.0005
tem_u:object_r:lvm_etc_t:s0
```

Восстановление меток безопасности и проверка состояния переключателей в SELinux

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:

```
[root@server.tbmanturov.net rz]# restorecon -vR /
```

Запуск расширенного лога системных сообщений

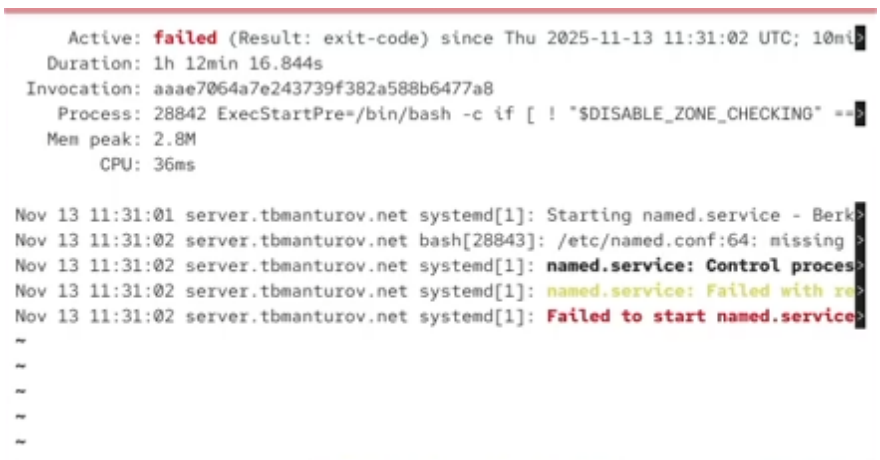
В случае ошибок перезапустим DNS-сервер:

```
[root@server.tbmanturov.net rz]# setsebool -P nam
[root@server.tbmanturov.net rz]# systenctl restar
```

Перезапуск сервера

Анализ работы DNS-сервера

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



Утилита dig

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

```
; <<>> DiG 9.18.33 <<>> ns.tbmanturov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43430
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a484b36515b47794010000006915c47716d14b6430a4c706 (good)
;; QUESTION SECTION:
;ns.tbmanturov.net.             IN      A

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

;; Query time: 6 msec
;; SERVER: ::1#53(::1) (UDP)
```

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:

```
[root@server.tbmanturov.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc
/named
[root@server.tbmanturov.net vagrant]# mkdir -p /vagrant/provision/server/dns/var
/named/master/
[root@server.tbmanturov.net vagrant]# cp -R /etc/named.conf /vagrant/provision/s
```

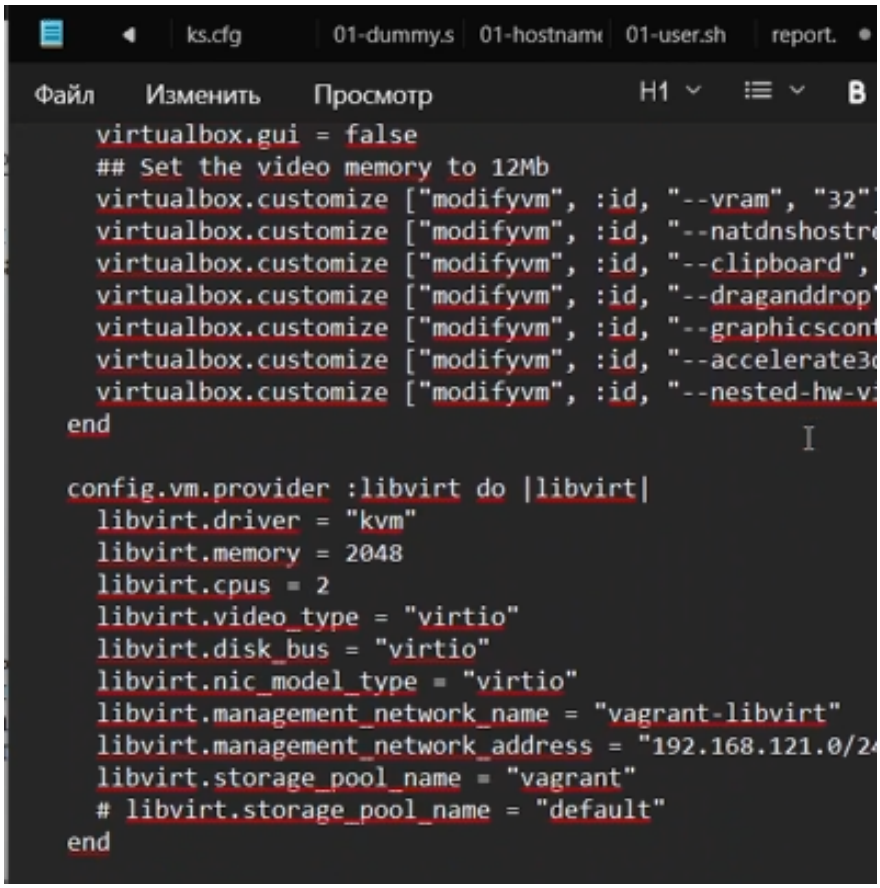
Создание каталога dns и перенос в него файлов, создание dns.sh

Запишем в dns.sh следующий скрипт:

```
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

Выводы

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