Лабораторная №2

Администрирование сетевых подсистем

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

Цель

Цель работы

- Приобретение навыков по установке и конфигурированию DNS-сервера
- Усвоение принципов работы системы доменных имён на ОС Rocky Linux

Ход работы

Подготовка

Для начала загружаем операционную систему, переходим в каталог Vagrant

```
PS C:\work\edzhibitskaya\vagrant> vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this
 machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't wo
rk
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this
 machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't wo
rk
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
```

Рис. 1: Загрузка ОС

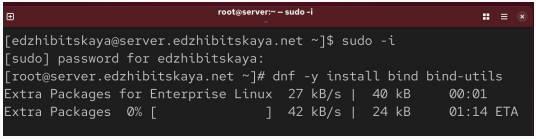


Рис. 2: bind, bind-utils

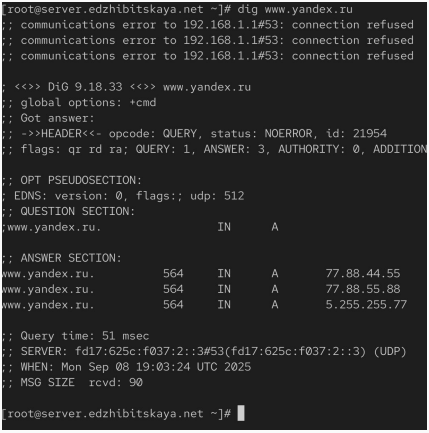


Рис. 3: Запрос к DNS-адресу Яндекса

Просмотр содержимого файлов

В файле /etc/resolv.conf указано к каким DNS-серверам обращаться для преобразования доменных имен в IP-адреса и наоборот

```
[root@server.edzhibitskaya.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search IGD_MGTS edzhibitskaya.net
nameserver 192.168.1.1
nameserver fd17:625c:f037:2::3
[root@server.edzhibitskaya.net ~]#
```

Рис. 4: Файл /etc/resolv.conf

Просмотр содержимого файлов

```
[root@server.edzhibitskaya.net ~]# 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";
```

Рис. 5: Файл /etc/named.conf

/etc/named.conf - главный конфигурационный файл демона BIND (named). Он определяет общие параметры работы DNS-сервера, зоны, которые он обслуживает, и политики доступа

Просмотр содержимого файлов

/var/named/named.localhost - это файл прямой зоны для домена localhost. Он сопоставляет имя localhost с IP-адресом 127.0.0.1

/var/named/named.loopback - это файл обратной зоны, выполняет обратное преобразование

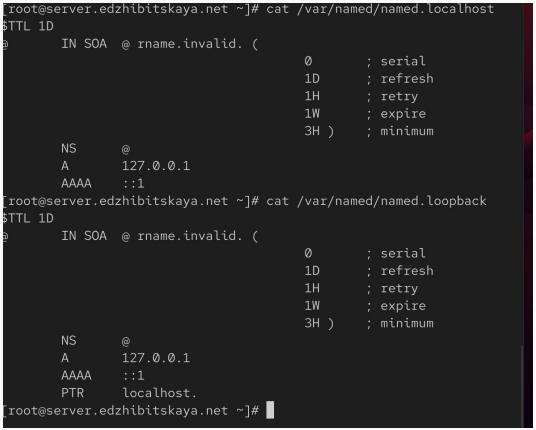


Рис. 6: Файлы named.localhost и named.loopback

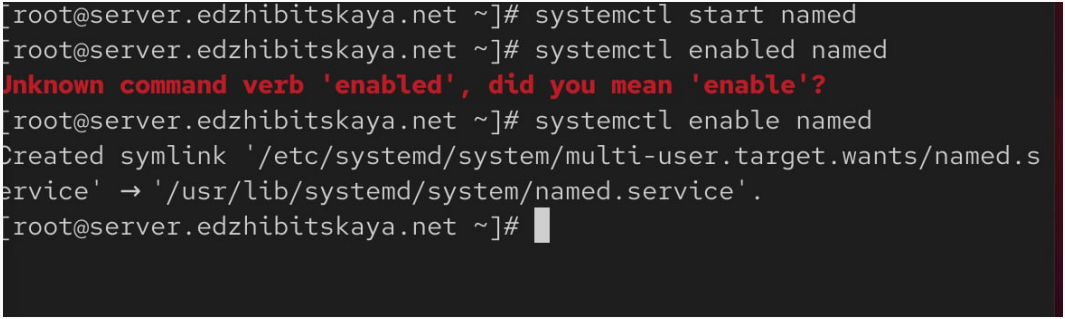


Рис. 7: Запуск сервера

Анализ dig

Проанализируем вывод команд dig www.yandex.ru и dig (127.0.0.1?) www.yandex.ru. Вторая команда дает больший вывод, так как в ней мы еще указываем к какому серверу обращаться, она помогает в отладке и диагностике конфигурации

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

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8319
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 48c3573e2e56ef880100000068bf2aa2903cc64b0e717cd1 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          600     IN      A       77.88.44.55
www.yandex.ru.          600     IN      A       77.88.55.88
www.yandex.ru.          600     IN      A       5.255.255.77

;; Query time: 359 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Sep 08 19:12:34 UTC 2025
;; MSG SIZE  rcvd: 118

[root@server.edzhibitskaya.net ~]#
```

Рис. 8: Dig www.yandex.ru

Настройка соединения

Далее сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети

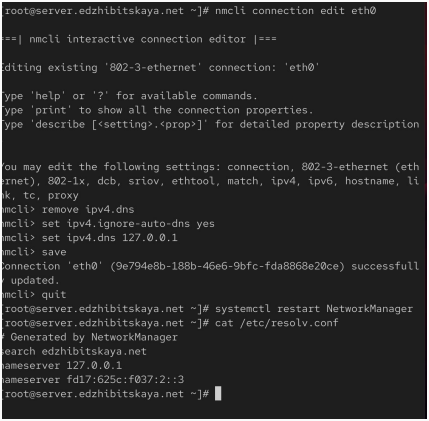


Рис. 9: Настройка соединения

Направления запросов

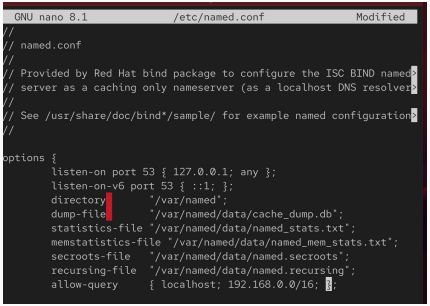


Рис. 10: Настройка направления запросов

Также настраиваем направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого редактируем файл /etc/named.conf

Работа с firewall

Вносим изменения в настройки межсетевого экрана узла server, убеждаемся, что DNS-запросы идут через узел server

```
[root@server.edzhibitskaya.net ~]# firewall-cmd --add-service=dns
success
[root@server.edzhibitskaya.net ~]# firewall-cmd --add-service=dns --
permanent
success
[root@server.edzhibitskaya.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/10
02/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1002/d
oc
      Output information may be incomplete.
avahi-dae   872                          avahi   12u     IPv4
       9463       0t0        UDP *:mdns
avahi-dae   872                          avahi   13u     IPv6
       9464       0t0        UDP *:mdns
chronyd     920                         chrony    5u     IPv4
       8650       0t0        UDP localhost:323
chronyd     920                         chrony    6u     IPv6
       8651       0t0        UDP localhost:323
wsdd      13183                    edzhibitskaya    7u     IPv4
      50425       0t0        UDP 239.255.255.250:ws-discovery
wsdd      13183                    edzhibitskaya    8u     IPv4
      50426       0t0        UDP *:32888
wsdd      13183                    edzhibitskaya    9u     IPv4
      50427       0t0        UDP server.edzhibitskaya.net:ws-discov
```

Рис. 11: Firewall

В ситуации, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер

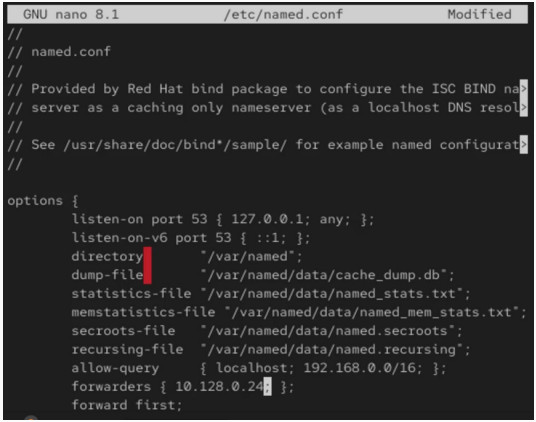


Рис. 12: Редактирование named.conf

Далее копируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименовываем его

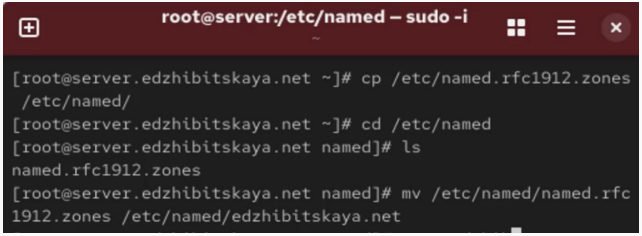


Рис. 13: Перемещение файла

Редактирование файлов

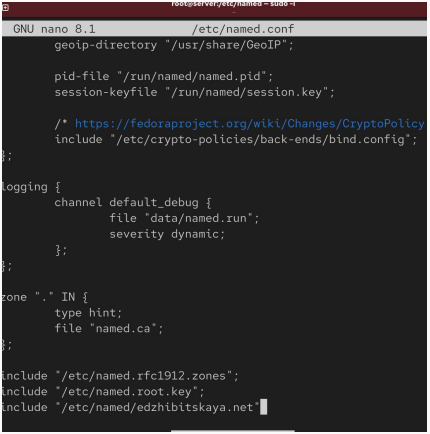


Рис. 14: /etc/named.conf

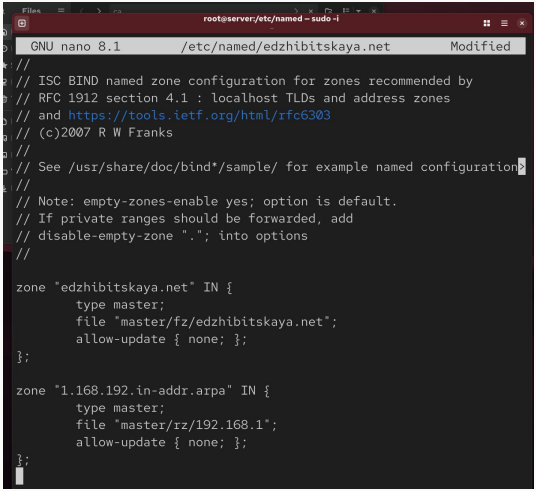


Рис. 15: /etc/named/edzhibitskaya.net

Fz и rz

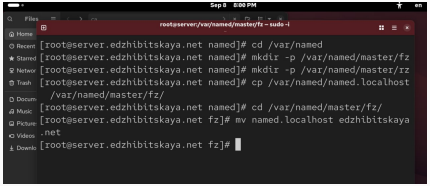


Рис. 16: Создание подкаталогов

В каталоге /var/named создаем подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно, скопируем шаблон прямой DNS-зоны named.localhost и переименуем его

Редактирование edzhibitskaya.net

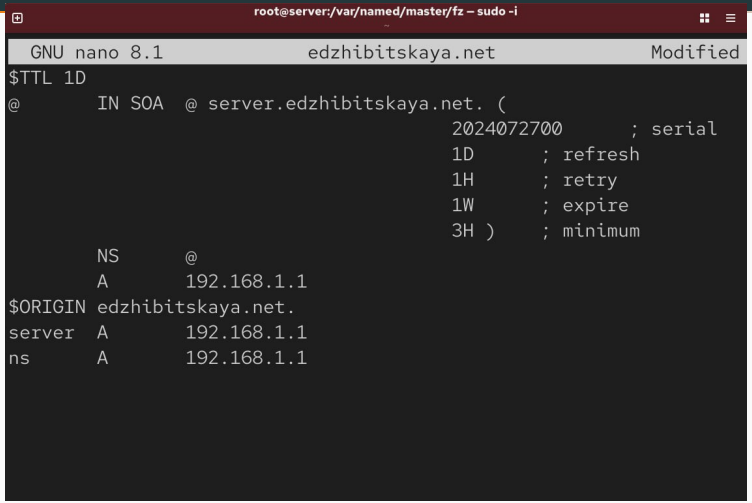


Рис. 17: edzhibitskaya.net

Работа с файлом обратной DNS-зоны

```
[root@server.edzhibitskaya.net fz]# cp /var/named/named.loopback /va
r/named/master/rz/
[root@server.edzhibitskaya.net fz]# cd /var/named/master/rz/
[root@server.edzhibitskaya.net rz]# mv named.loopback 192.168.1
[root@server.edzhibitskaya.net rz]#
```

Рис. 18: Копирование файла

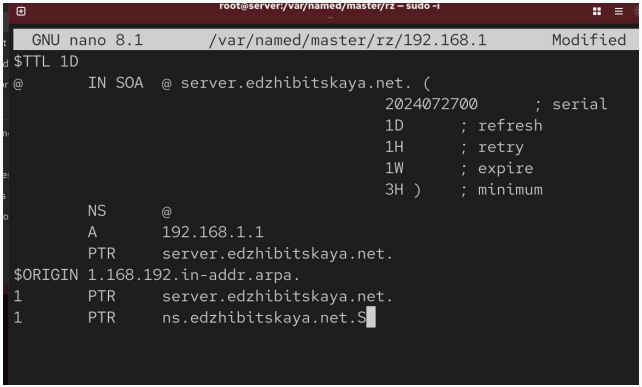


Рис. 19: 192.168.1

Наделение прав и метки SELinux

Исправляем права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать и после изменения доступа к конфигурационным файлам named корректно восстанавливаем их метки в SELinux

```
[root@server.edzhibitskaya.net rz]# chown -R named:named /etc/named
[root@server.edzhibitskaya.net rz]# chown -R named:named /var/named
[root@server.edzhibitskaya.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm
_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20250906.183832.000
5 from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_
etc_t:s0
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection f
rom unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:Net
workManager_etc_rw_t:s0
[root@server.edzhibitskaya.net rz]# restorecon -vR /var/named
[root@server.edzhibitskaya.net rz]#
```

Рис. 20: Права и метки

Переключатели и перезапуск DNS-сервера

```
[root@server.edzhibitskaya.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.edzhibitskaya.net rz]# setsebool named_write_master_zones 1
[root@server.edzhibitskaya.net rz]# setsebool -P named_write_master_zones 1
[root@server.edzhibitskaya.net rz]#
```

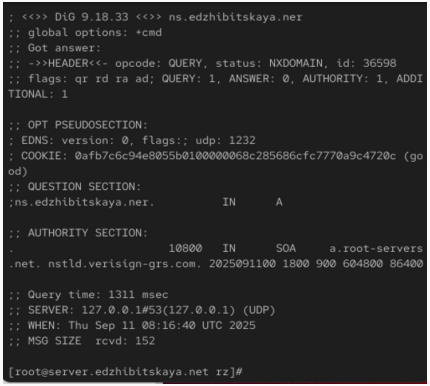
Рис. 21: Переключатели

```
[root@server.edzhibitskaya.net rz]# systemctl restart named
[root@server.edzhibitskaya.net rz]# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; e>
     Active: active (running) since Thu 2025-09-11 08:15:03 U>
 Invocation: 687cd3dba8c04d678ae2f7a22c24d10c
    Process: 23503 ExecStartPre=/bin/bash -c if [ ! "$DISABLE>
    Process: 23506 ExecStart=/usr/sbin/named -u named -c ${NA>
   Main PID: 23507 (named)
      Tasks: 6 (limit: 10373)
     Memory: 9.6M (peak: 9.8M)
        CPU: 526ms
     CGroup: /system.slice/named.service
             └─23507 /usr/sbin/named -u named -c /etc/named.c>

Sep 11 08:15:14 server.edzhibitskaya.net named[23507]: timed >
Sep 11 08:15:14 server.edzhibitskaya.net named[23507]: timed >
```

Рис. 22: Перезапуск

Анализ работы DNS-сервера



Для анализа работы DNS-сервера воспользуемся утилитами dig и host

Рис. 23: Описание DNS-зоны с сервера

Анализ работы DNS-сервера

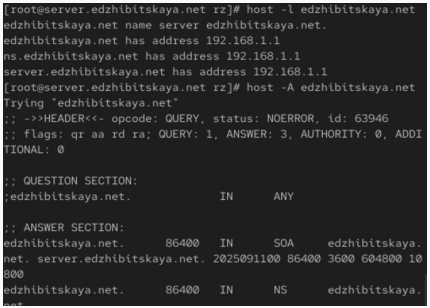


Рис. 24: host -l; host -a

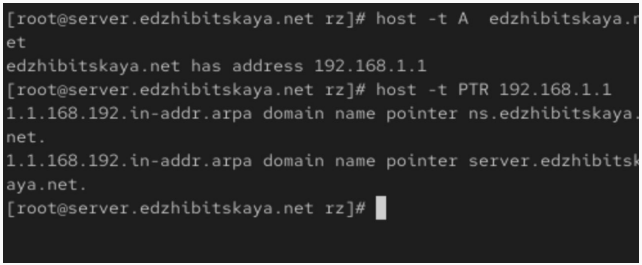


Рис. 25: host -t

Сохранение изменений

Наконец, в каталог для внесения изменений в настройки внутреннего окружения добавим необходимые директории, создадим исполняемый файл и пропишем скрипт.

```
[root@server.edzhibitskaya.net vagrant]# mkdir -p /vagrant/pro
vision/server/dns/etc/named
[root@server.edzhibitskaya.net vagrant]# mkdir -p /vagrant/pro
vision/server/dns/var/named/master/
[root@server.edzhibitskaya.net vagrant]# cp -R /etc/named.conf
 /vagrant/provision/server/dns/etc/
[root@server.edzhibitskaya.net vagrant]# cp -R /etc/named/* /v
agrant/provision/server/dns/etc/named/
[root@server.edzhibitskaya.net vagrant]# cp -R /var/named/mast
er/* /vagrant/provision/server/dns/var/named/master/
[root@server.edzhibitskaya.net vagrant]#
```

Рис. 26: Добавление изменений

Сохранение изменений

```
 GNU nano 8.1                  dns.sh                        Modifi
#!/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
```

Рис. 27: Скрипт

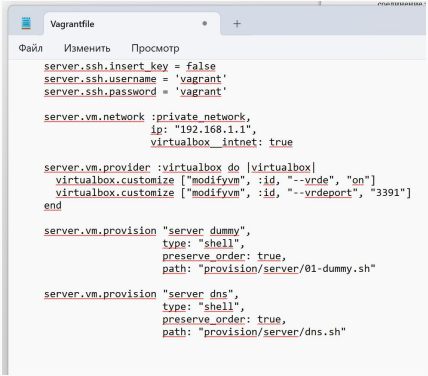


Рис. 28: Vagrantfile

Выводы

Вывод

- В ходе работы были получены навыки по установке и конфигурированию DNS-сервера и усвоены принципы работы системы доменных имён на ОС Rocky Linux