

Лабораторная работа 2

Настройка DNS-сервера

Лушин Артём Андреевич

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	20
4	Контрольные вопросы	21

Список иллюстраций

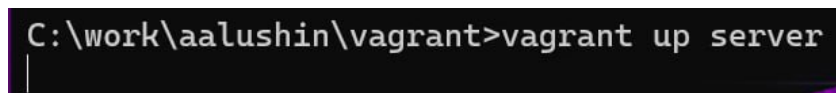
2.1	Запуск машины	5
2.2	Установка ПО	5
2.3	Запрос с яндекс	6
2.4	Анализ /etc/resolv.conf	6
2.5	Анализ /etc/named.conf	7
2.6	Содержание /var/named/named.ca	8
2.7	Содержание	9
2.8	Содержание /var/named/named.loopback	9
2.9	Запуск сервера	9
2.10	Сравнение яндекса и айпи яндекса	10
2.11	Сервер по умолчанию	11
2.12	System eth0	11
2.13	Перезапуск	11
2.14	Настройка днс-запросов	12
2.15	Изменения межсетевого экрана	12
2.16	Перенаправление запросов	13
2.17	Список серверов	13
2.18	Перенос днс-зоны	14
2.19	Внос в конфигурационный файл	14
2.20	Изменение файла днс-зоны	14
2.21	Создание файлов fz и rz	15
2.22	Файл прямой днс-зоны	15
2.23	Изменение прямой зоны	15
2.24	Обратная днс-зоны	15
2.25	Изменение обратной зоны	16
2.26	Изменение прав	16
2.27	Восстановление меток	16
2.28	Проверка на наличие ошибок	17
2.29	Описание днс-зоны	17
2.30	Корректность работы сервера	18
2.31	размещение файлов на машине	18
2.32	Скрипт в исполняющем файле	19
2.33	Изменение vagrantfile	19

1 Цель работы

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

2 Выполнение лабораторной работы

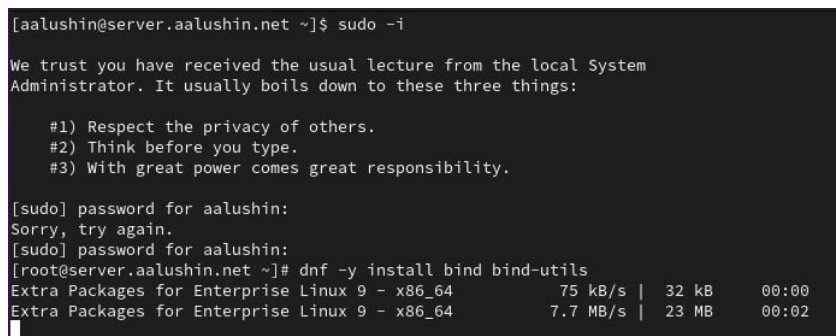
- 1) Я перешёл в каталог vagrant и запустил виртуальную машину server.



```
C:\work\aalushin\vagrant>vagrant up server
```

Рис. 2.1: Запуск машины

- 2) Я перешёл в суперпользователя и установил bind и bind-utils.



```
[aalushin@server.aalushin.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 aalushin:
Sorry, try again.
[sudo] password for aalushin:
[root@server.aalushin.net ~]# dnf -y install bind bind-utils
Extra Packages for Enterprise Linux 9 - x86_64      75 kB/s | 32 kB  00:00
Extra Packages for Enterprise Linux 9 - x86_64      7.7 MB/s | 23 MB  00:02
```

Рис. 2.2: Установка ПО

- 3) Я сделал запрос с DNS-адресу Яндекса. Проанализируем строки вывода:

- **HEADER** (заголовок): показывает версию dig, глобальные опции используемые с командой и другую дополнительную информацию
- **QUESTION SECTION**: Показывает наш запрос, то есть мы запросили показать А-запись (команда dig без параметров) для домена `www.yandex.ru`

- ANSWER SECTION: 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 (8 мс), имя DNS-сервера который запрашивался, когда был создан запрос и размер сообщения

```

; <<> DiG 9.16.23-RH <<> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32422
;; 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: 8 msec

```

Рис. 2.3: Запрос с яндекс

- 4) С помощью утилиты проанализируем содержание файла /etc/resolv.conf. Содержит имя сервера и его адрес Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.

```

[root@server.aalushin.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search aalushin.net
nameserver 127.0.0.1

```

Рис. 2.4: Анализ /etc/resolv.conf

- 5) С помощью утилиты проанализируем содержание файла /etc/named.conf. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.

```
[root@server.aalushin.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; 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 { 10.128.0.240; 80.250.174.240; };
    forward first;

    /*
     - 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
    */
    recursion yes;

    dnssec-enable no;
}
```

Рис. 2.5: Анализ /etc/named.conf

- 6) С помощью команды проанализируем содержание файла /var/named/named.ca. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.

```
[root@server.aalushin.net ~]# cat /var/named/named.ca

; <<>> DiG 9.18.20 <<>> -4 +tcp +norec +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:
;.                               IN      NS

;; 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.
.           518400 IN      NS      j.root-servers.net.
.           518400 IN      NS      k.root-servers.net.
.           518400 IN      NS      l.root-servers.net.
.           518400 IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 518400 IN      A       198.41.0.4
b.root-servers.net. 518400 IN      A       170.247.170.2
c.root-servers.net. 518400 IN      A       192.33.4.12
d.root-servers.net. 518400 IN      A       199.7.91.13
e.root-servers.net. 518400 IN      A       192.203.230.10
f.root-servers.net. 518400 IN      A       192.5.5.241
g.root-servers.net. 518400 IN      A       192.112.36.4
```

Рис. 2.6: Содержание /var/named/named.ca

7) С помощью команды проанализируем содержание файла /var/named/named.localhost.

В данном файле есть следующие строки: запись начала полномочий, которая указывает начало зоны и включает имя хоста на которых находится файл данных. Запись сервера имён, идентифицирующая главный и подчинённый серверы DNS. Указаны IP адреса локального хоста. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.


```
[root@server.aalushin.net ~]# cat /var/named/named.localhost
$TTL 1D
@      IN SOA  @ rname.invalid. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

NS     @
A      127.0.0.1
AAAA   ::1
```

Рис. 2.7: Содержание

- 8) С помощью утилиты проанализируем содержание файла /var/named/named.loopback. Данный файл практически полностью идентичен как и файл localhost, но добавляется PTR-запись для локального хоста. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.

```
[root@server.aalushin.net ~]# cat /var/named/named.loopback
$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.
```

Рис. 2.8: Содержание /var/named/named.loopback

- 9) Я запустил DNS-сервер и включил автозапуск.

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

Рис. 2.9: Запуск сервера

- 10) Сравним вывод информации после анализа `www.yandex.ru` и `127.0.0.1 www.yandex.ru`. При указании запрашиваемого адреса в строке с адресом написан адрес, который указывали, а также куки и увеличилось время запроса.

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

;<<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 58815
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 14ac631fac0a0eb30100000066e0b062872afe257388b96c (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

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

;; Query time: 1233 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 10 20:47:30 UTC 2024
;; MSG SIZE rcvd: 118

[root@server.aalushin.net ~]# 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: 55056
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: dbfdcbd32c15370f0100000066e0b07968533f570fbf6782 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                577     IN      A      5.255.255.77
www.yandex.ru.                577     IN      A      77.88.55.88
www.yandex.ru.                577     IN      A      77.88.44.55

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 10 20:47:53 UTC 2024
;; MSG SIZE rcvd: 118
```

Рис. 2.10: Сравнение яндекса и айпи яндекса

- 11) Я сделал dns-сервер по умолчанию для хоста сервер и внутренней виртуальной сети.

```
[root@server.aalushin.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' (52b757e4-3833-4753-b0eb-de0af7f26f57) successfully updated.
nmcli>
```

Рис. 2.11: Сервер по умолчанию

12) Сделал ту же операцию для соединения system eth0.

```
[root@server.aalushin.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, 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 updated.
nmcli>
```

Рис. 2.12: System eth0

13) Перезапустили NetworkManager.

```
[root@server.aalushin.net ~]# systemctl restart NetworkManager
[root@server.aalushin.net ~]#
```

Рис. 2.13: Перезапуск

14) Я настроил направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла сервер, через узел сервер.


```

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 { 10.128.0.240; 80.250.174.240; };
<----->forward first;

<----->*/.
<----->- If you are building an AUTHORITATIVE DNS server, you
<----->- If you are building a RECURSIVE (caching) DNS server, you
<----->- recursion..
<----->- If your recursive DNS server has a public IP address, you
<----->- control to limit queries to your legitimate users. Failing to
<----->- cause your server to become part of large scale
<----->- attacks. Implementing BCP38 within your network will help to
<----->- reduce such attack surface.
<----->*/
<----->recursion yes;

<----->dnssec-enable no;
<----->dnssec-validation no;

```

Рис. 2.16: Перенаправление запросов

18) Получил текущие список серверов.

```

[root@server.aalushin.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search aalushin.net
nameserver 127.0.0.1

```

Рис. 2.17: Список серверов

19) Скопировал описание днс-зоны, переместил и переименовал его.

```
[root@server.aalushin.net etc]# cp /etc/named.rfc1912.zones /etc/named/user.net
[root@server.aalushin.net etc]# cd /etc/named
[root@server.aalushin.net named]# ls
user.net
[root@server.aalushin.net named]# mv user.net aalushin.net
[root@server.aalushin.net named]# ls
aalushin.net
```

Рис. 2.18: Перенос днс-зоны

20) Включил файл описания днс-зоны в конфигурационный файл.

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/user.net";
```

Рис. 2.19: Внос в конфигурационный файл

21) Изменил файл днс-зоны, чтобы он корректно работал.

```
aalushin.net [BM--] 2 L: [ 1+ 0 1/ 29] *(2 / 700b) 0032 0x020
//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 "aalushin.net" IN {
<----->type master;
<----->file "master/fz/aalushin.net";
<----->allow-update { none; };
};

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

Рис. 2.20: Изменение файла днс-зоны

22) Создал каталоги для обратной fz и rz для файлов прямой и обратной зоны.

```
[root@server.aalushin.net named]# ls
data dynamic named.ca named.empty named.localhost named.loopback slaves
[root@server.aalushin.net named]# mkdir -p /var/named/master/fz
[root@server.aalushin.net named]# mkdir -p /var/named/master/rz
[root@server.aalushin.net named]# ls
data dynamic master named.ca named.empty named.localhost named.loopback slaves
[root@server.aalushin.net named]# ls master
fz rz
```

Рис. 2.21: Создание файлов fz и rz

23) Скопировал шаблон для прямой днс-зоны и перенёс в каталог Fz.

```
[root@server.aalushin.net named]# cp /var/named/named.localhost /var/named/master/fz
[root@server.aalushin.net named]# cd master/fz/
[root@server.aalushin.net fz]# ls
named.localhost
[root@server.aalushin.net fz]# mv named.localhost aalushin.net
[root@server.aalushin.net fz]# ls
aalushin.net
```

Рис. 2.22: Файл прямой днс-зоны

24) Изменил скрипт файла прямой зоны, чтобы он корректно работал на моей машине.

```
$TTL 1D
@<----->IN SOA<@ server.aalushin.net (
<-----><-----><-----><-----><----->2024091000<----->; serial
<-----><-----><-----><-----><----->1D<----->; refresh
<-----><-----><-----><-----><----->1H<----->; retry
<-----><-----><-----><-----><----->1W<----->; expire
<-----><-----><-----><-----><----->3H )<-->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
$ORIGIN aalushin.net.
server<@A <----->192.168.1.1
ns<----->A<----->192.168.1.1
```

Рис. 2.23: Изменение прямой зоны

25) Скопировал шаблон обратной днс-зоны и перенёс его в каталог rz.

```
[root@server.aalushin.net named]# cp /var/named/named.loopback /var/named/master/rz/
[root@server.aalushin.net named]# cd /var/named/master/rz/
[root@server.aalushin.net rz]# mv named.loopback 192.168.1
[root@server.aalushin.net rz]# ls
192.168.1
[root@server.aalushin.net rz]#
```

Рис. 2.24: Обратная днс-зоны

26) Изменил скрипт файла обратной зоны, чтобы он корректно работал.

```
192.168.1 [-M--] 36 L:[ 1+ 9 10/ 13] *(184 / 266b) 0010 0x0
$TTL 1D
@<----->IN SOA<@ server.aalushin.net. (
<-----><-----><-----><-----><----->2024091000<----->; serial
<-----><-----><-----><-----><----->1D<----->; refresh
<-----><-----><-----><-----><----->1H<----->; retry
<-----><-----><-----><-----><----->1W<----->; expire
<-----><-----><-----><-----><----->3H )<----->; minimum
<----->NS<----->@
<----->A<----->192.168.1.1
<----->PTR<----->server.aalushin.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<----->PTR<----->server.aalushin.net.
1<----->PTR<----->ns.aalushin.net.
```

Рис. 2.25: Изменение обратной зоны

27) Изменил права доступа к файлам в каталогах Etc/named и var/named, чтобы файл named мог с ними работать.

```
[root@server.aalushin.net rz]# chown -R named:named /etc/named
[root@server.aalushin.net rz]# chown -R named:named /var/named
```

Рис. 2.26: Изменение прав

28) После изменений доступа в конфигурационных файлах корректно восстановили метки безопасности в Selinux. Проверил состояние переключателей.

```
[root@server.aalushin.net rz]# 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
[root@server.aalushin.net rz]# restorecon -vR /var/named
[root@server.aalushin.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
```

Рис. 2.27: Восстановление меток

29) Запустил во втором терминале расширенный лог системных сообщений и перезапустил dns-сервер. Проверил на наличие ошибок, ошибок нет.


```

The job identifier is 3995.
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:2::c#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:503:c27::30#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:2f::f#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:7fe:53#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:9f::42#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:503:b3a3e::2:30#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:7fd:1#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:12::d0#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:2d::d#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:1::53#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:500:a8::e#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:dc3::35#53
Sep 10 12:14:13 server.aalushin.net named[10729]: network unreachable resolving /./NS/IN/: 2001:1b8:10::b#53
Sep 10 12:14:13 server.aalushin.net named[10729]: running
Sep 10 12:14:13 server.aalushin.net named[10729]: resolver pruning query complete
Sep 10 12:14:13 server.aalushin.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Subject: Unit succeeded
Defined By: systemd
Support: https://wiki.rockylinux.org/rocky/support

The unit systemd-hostnamed.service has successfully entered the 'dead' state.
Sep 10 12:14:14 server.aalushin.net named[10729]: timed out resolving /./DNSKEY/E/IN/: 10.128.0.240#53
Sep 10 12:14:14 server.aalushin.net named[10729]: REFUSED unexpected RCODE resolving /./DNSKEY/E/IN/: 80.250.174.240#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:2::c#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:503:c27::30#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:2f::f#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:7fe:53#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:9f::42#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:503:b3a3e::2:30#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:7fd:1#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:12::d0#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:2d::d#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:1::53#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:500:a8::e#53
Sep 10 12:14:14 server.aalushin.net named[10729]: network unreachable resolving /./DNSKEY/E/IN/: 2001:dc3::35#53

```

Рис. 2.28: Проверка на наличие ошибок

30) При помощи утилиты получил описание днс-зоны.

```
[root@server.aalushin.net rz]# dig ns.aalushin.net

<<> Dig 9.16.23-RH <> ns.aalushin.net
;; global options: +cmd
;; Got answer:
;;->HEADER<< opcode: QUERY, status: NXDOMAIN, id: 53939
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags; udp: 1232
;; COOKIE: a8f8b2775714a871018000066e0834fd86ac9461eb58289 (good)
;; QUESTION SECTION:
;; ns.aalushin.net.                IN      A

;; AUTHORITY SECTION:
aalushin.net.                10800   IN      SOA      aalushin.net. server.aalushin.net.aalushin.net. 2024091000 86400 3600 604800 10800

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 10 12:15:11 UTC 2024
;; MSG SIZE rcvd: 140
```

Рис. 2.29: Описание днс-зоны

31) При помощи утилиты `host` проанализировал корректность работы днс-сервера.

```
[root@server.aalushin.net rz]# host -l user.net
Host user.net not found: 9(NOTAUTH)
; Transfer failed.
[root@server.aalushin.net rz]# host -l aalushin.net
aalushin.net name server aalushin.net.
aalushin.net has address 192.168.1.1
nc.aalushin.net has address 192.168.1.1
servet.aalushin.net has address 192.168.1.1
[root@server.aalushin.net rz]# host -a aalushin.net
Trying 'aalushin.net'
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
aalushin.net.      86400   IN      SOA      aalushin.net. server.aalushin.net. 2024091000 86400 3600 604800 10800
aalushin.net.      86400   IN      NS       aalushin.net.
aalushin.net.      86400   IN      A        192.168.1.1

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

Received 144 bytes from 127.0.0.1#53 in 0 ms
[root@server.aalushin.net rz]# host -t A aalushin.net
aalushin.net has address 192.168.1.1
[root@server.aalushin.net rz]# host -t PTR aalushin.net
aalushin.net has no PTR record
[root@server.aalushin.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.aalushin.net.
1.1.168.192.in-addr.arpa domain name pointer ns.aalushin.net.
```

Рис. 2.30: Корректность работы сервера

32) Зашёл в каталог `/vagrant/provision/server/`, создал подкаталог `dns` в который поместил соответствующие подкаталоги и конфигурационные файлы. А так же создал исполняющий файл.

```
[root@server.aalushin.net vagrant]# ls
Makefile  provision  Vagrantfile
[root@server.aalushin.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.aalushin.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master
[root@server.aalushin.net vagrant]# ls provision/server/dns/
etc  var
[root@server.aalushin.net vagrant]# ls provision/server
01-dummy.sh  02-forward.sh  dns
[root@server.aalushin.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.aalushin.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named
[root@server.aalushin.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.aalushin.net vagrant]# cd provision/server/
[root@server.aalushin.net server]# touch dns.ch
[root@server.aalushin.net server]# ls
01-dummy.sh  02-forward.sh  dns  dns.ch
[root@server.aalushin.net server]# touch dns.sh
[root@server.aalushin.net server]# rm -r dns.ch
rm: remove regular empty file 'dns.ch'? y
[root@server.aalushin.net server]# ls
01-dummy.sh  02-forward.sh  dns  dns.sh
[root@server.aalushin.net server]# chmod +x dns.sh
[root@server.aalushin.net server]# ls
01-dummy.sh  02-forward.sh  dns  dns.sh
```

Рис. 2.31: размещение файлов на машине

33) Создание скрипта в исполняющем файле `dns`.

```

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

```

Рис. 2.32: Скрипт в исполняющем файле

- 34) Чтобы скрипт отрабатывал при запуске машины, внес изменения в vagrantfile.

```

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"

```

Рис. 2.33: Изменение vagrantfile

3 Вывод

Я приобрёл практические навыки по установке и конфигурированию DNS-сервера, усвоил принцип работы системы доменных имён.

4 Контрольные вопросы

1) Что такое DNS?

- Система доменных имён (Domain Name System, DNS) — 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?

- Прямая DNS зона - зона хранения записей соответствия доменного имени IP-адресу. Обратная DNS зона - зона хранения записей соответствия IP-адреса доменному имени.

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

- В каталоге /etc хранится файл named.conf, в котором есть информация об опциях сервера, его разрешениях, настройках безопасности и подключены файлы зон. В каталоге /named хранится файл описания DNS-зон, также в каталоге /var/named хранится файл named.loopback, описывающий обратную зону, и файл named.localhost, описывающий прямую зону.

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

- В этом файле указывается имя сервера и его адрес.

6) Какие типы записи описания ресурсов есть в DNS и для чего они используются?

Основные типы ресурсных записей (Resource Records):

- А-запись — задает преобразование имени хоста в IP-адрес.
- MX-запись — определяет почтовый ретранслятор для доменного имени, т.е. узел, который обработает или передаст дальше почтовые сообщения, предназначенные адресату в указанном домене. При наличии нескольких MX-записей сначала происходит попытка доставить почту на ретранслятор с наименьшим приоритетом.
- NS-записи — определяют DNS-серверы, которые являются авторитативными для данной зоны.
- CNAME-запись — определяет отображение псевдонима в каноническое имя узла.
- SRV-запись — позволяет получить имя для искомой службы, а также протокол, по которому эта служба работает.
- TXT-запись — содержит общую текстовую информацию. Эти записи могут использоваться в любых целях, например, для указания месторасположения хоста.
- AAAA-запись — задает преобразование имени хоста в IPV6-адрес.
- SSHFP-запись — используется для хранения слепок ключей SSH в DNS.

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

- Домен in-addr.arpa используется для всех сетей TCP/IP, основанным на адресации протокола Интернета 4 (IPv4).

8) Для чего нужен демон named?

- Демон named отвечает на запросы об именах машин и их IP-адресах. Если named не знает ответа на какой-либо запрос, он опрашивает другие серверы и помещает их ответы в кэш. Этот демон, кроме того, отвечает за выполнение зонных пересылок, обеспечивающих копирование данных между серверами одного домена. Запросы демона named используют протокол UDP и порт 53. Если объем ответов превышает 512 байтов, то для их доставки используется протокол TCP. В зонных пересылках между серверами также применяется протокол TCP.

9) В чём заключаются основные функции slave-сервера и master-сервера?

- Главный (master) — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых; ведомый (slave) — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны.

10) Какие параметры отвечают за время обновления зоны?

- SOA-запись (Start of Authority) — начальная запись зоны, которая указывает местоположение эталонной записи о домене. Она хранит параметр TTL – время, в течение которого информация будет кешироваться другими DNS-серверами. Также параметр Refresh – время (в секундах) ожидания ответа вторичного DNS перед запросом SOA-записи с первичных серверов. По истечении данного времени вторичный DNS обращается к первичному для получения копии текущей SOA-записи. Первичный DNS-сервер выполняет этот запрос. Вторичный DNS-сервер сравнивает полученный серийный номер зоны с имеющимся. Если они отличаются, то осуществляется запрос к

первичному DNS-серверу на трансфер зоны. И Expire – время (в секундах), в течение которого вторичный DNS будет пытаться завершить синхронизацию зоны с первичным. Если это время истечет до того, как синхронизация закончится, то зона на вторичном DNS-сервере перестанет обслуживать запросы об этой зоне.

11) Как обеспечить защиту зоны от скачивания и просмотра?

Можно делать следующее для защиты данных DNS доменов с помощью DNSSEC:

- Подписывать зоны или удалить подпись в соответствии со спецификациями DNSSEC
- (Необязательно) Указывать индивидуальные настройки для создания ключей
- Получать уведомления
- Просматривать и копировать записи ресурсов DS
- Просматривать и копировать наборы записей ресурсов DNSKEY.

12) Какая запись RR применяется при создании почтовых серверов?

- Запись MX (от англ. mail exchanger) — тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP.

13) Как протестировать работу сервера доменных имён?

- Для этого можно воспользоваться командой nslookup, которая позволяет получить информацию о DNS-записях для заданного домена или IP-адреса.

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

- `systemctl restart named` - перезапустить DNS-сервер

- `systemctl stop named` - перезапустить DNS-сервер
 - `systemctl start named` - перезапустить DNS-сервер
- 15) Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?
- В дополнительном терминале запустить в режиме реального времени расширенный лог системных сообщений: `journalctl -x -f`
- 16) Где храниться отладочная информация по работе системы и служб? Как её посмотреть?
- Журналы службы находятся в директории `“/var/log/”` в виде обычных текстовых файлов.
- 17) Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров
- `lsdf` – есокращение от `LiSt of Open Files`, утилита эта служит для вывода информации о том, какие файлы используются теми или иными процессами. В качестве примера могу привести 16 пункт моей лабораторной работы. Там мы используем команду `gtop`.
- 18) Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса `nmcli`.
- В качестве примера могу привести 11 и 12 пункты моей лабораторной.
- 19) Что такое SELinux?
- SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.

20) Что такое контекст (метка) SELinux?

- SELinux — это система принудительного управления доступом, что означает, что каждый процесс имеет метку (label). Каждый файл, каталог и системный объект так же имеют метки. Правила политики управляют доступом между промаркированными процессами и объектами.
- Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами

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

После изменения доступа к конфигурационным файлам `named` требуется корректно восстановить их метки в SELinux:

```
restorecon -vR /etc restorecon -vR /var/named
```

Для проверки состояния переключателей SELinux, относящихся к `named`, надо ввести:

```
getsebool -a | grep named
```

При необходимости дать `named` разрешение на запись в файлы DNS-зоны:

```
setsebool named_write_master_zones 1 setsebool -P named_write_master_zones 1
```

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

- Чтобы создать необходимые политики:

1. Создайте новый файл с исходным кодом политики SELinux (.te файл). Данный файл определяет ограничения, относящиеся к описываемому модулю.
2. При необходимости отредактируйте сгенерированный исходный файл политики [module_name].te, а затем, используя утилиту `checkmodule`, создайте бинарное представление (.mod файл) исходного файла локальной политики.

3. Создайте устанавливаемый модуль политики (.pp файл) с помощью утилиты `semodule_package`.
4. Для установки созданного модуля политики воспользуйтесь утилитой `semodule`.

23) Что такое булевый переключатель в SELinux?

- Булевый переключатель в SELinux - это параметр, который управляет разрешениями безопасности на уровне SELinux. Он может быть включен (true) или выключен (false) и используется для разрешения или запрещения определенных действий.

24) Как посмотреть список переключателей SELinux и их состояние?

- Для просмотра списка переключателей SELinux и их состояния можно использовать команду `"semanage boolean -l"` в терминале.

25) Как изменить значение переключателя SELinux?

- Чтобы изменить значение переключателя SELinux, можно использовать команду `"setsebool"`. Например, для включения переключателя с именем `"httpd_can_network_connect"` можно выполнить команду `"setsebool -P httpd_can_network_connect 1"`. Здесь -P указывает, что изменение должно быть постоянным (постоянно сохраняться после перезагрузки).