



### **Цель работы:**

Закрепить понимание принципов работы DNS, получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux;

### **Требования:**

Установленная на компьютере среда виртуализации ORACLE Virtual Box с виртуальной машиной Linux Cent OS 7 (выполнять работу можно в любой ОС Linux, но все описания будут даваться для CentOS 7).

### **Инструментальные средства:**

*Утилиты: firewall-cmd systemctl ip ping journalctlss netstat lsof dig*

*Файлы: /etc/named.conf, /etc/named*

*Утилиты работы с текстом: echo, grep, sed*

*Редакторы: vi, nano*

### **Порядок выполнения работы:**

#### **Часть 1. Подготовка и проверка конфигурации.**

В VirtualBox:

1. Сделайте связанный клон виртуальной машины. Одну машину назовите с7-1, другой с7-2
2. Для виртуальной машины с7-1 добавьте второй сетевой интерфейс.
3. Подключите сетевой интерфейс с7-2 и новый сетевой интерфейс с7-1 к внутренней сети intnet.
4. Подключите исходный сетевой интерфейс с7-1 к NAT. В Linux:
5. Для внутренней сети задайте для машин с7-1 и с7-2 адреса 10.0.0.1 и 10.0.0.2 с маской 255.255.255.0.
6. Для исходного интерфейса с7-1 оставьте получение адреса автоматически от dhcp сервера VirtualBox
7. Для обоих хостов отключите использование ipv6.
8. Задайте имена хостов, советуящие именам виртуальных машин.

9. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
10. Убедитесь, что на c7-2 в качестве шлюза по умолчанию и DNS задан адрес c7-1.
11. Установите на машине c7-1 пакеты bind и bind-utils

### **Часть 2. Получение информации из DNS с помощью утилиты dig**

1. На хосте c7-1 с выполните команду dig www.itmo.ru. В консольном выводе изучите состав секций HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER: 192.168.0.1, WHEN и MSG SIZE. Соотнесите значения полей секции HEADER со значениями остальных полей. (!)
2. На хосте c7-1 с помощью утилиты dig решите следующие задачи (!):
  - a. Выведите только результат разрешения имени www.itmo.ru (только IP адрес)
  - b. Выведите на экран подробную информацию о разрешении имени, с выводом всех промежуточных серверов, определите какой именно DNS сервер вернул IP адрес хоста.
  - c. Выведите конфигурационную запись (SOA) домена itmo.ru, определите, значения каждого из числовых параметров записи, что они означают?
  - d. Определите, какие сервера обрабатывают почту домена itmo.ru.
  - e. Определите какие DNS сервера обслуживают зону itmo.ru и какие у них ip адреса.
  - f. Значение записи в зоне обратного просмотра для 87.250.250.242.
  - g. Определите количество серверов, поддерживающих корневую зону.

### **Часть 3. Настройка кэширующего DNS сервера**

Цель этой части – настроить хост c7-1 как кэширующий DNS сервер для хоста c7-2.

1. С помощью утилиты firewall-cmd разрешите службе dns получать доступ к сети.
2. С помощью systemctl включите и запустите службу bind (она называется named)

3. Отредактируйте /etc/named.conf так, чтобы:
  - a. Сервер отвечал на IPv4 адресе из вашей локальной сети
  - b. Не работал поверх IPv6
  - c. Позволял обычные и рекурсивные запросы только с ip адресов вашей локальной сети (между c7-1 и c7-2) и с самого хоста c7-1.
  - d. Делал рекурсивные запросы.
  - e. Вместо версии сервера выводил при запросе «My Own DNS Server»
4. Проверьте разрешение имен на хосте c7-2.

#### **Часть 4. Создание собственной доменной зоны**

1. Отредактируйте /etc/named.conf так, чтобы добавить зону на сервер зону домена <fio>.local, где <fio> - ваши инициалы, причем ваш сервер должен быть для этого домена основным, не допускать трансфер зоны, разрешать все обновления и хранить зону в файле /var/named/<fio>.local.db
2. Для проверки файла конфигурации используйте утилиту named-checkconf
3. Создайте файл <fio>.local.db, содержащий следующие параметры для домена <fio>.local:
  - a. Имя основного DNS сервера ns1
  - b. E-mail администратора [hostmaster@<fio>.local](mailto:hostmaster@<fio>.local)
  - c. Серийный номер зоны по шаблону YYYYMMDDhh
  - d. Время обновления реплики 43200
  - e. Время до повторной попытки 3600
  - f. Время работы реплики без обновления 3600000
  - g. Минимальный TTL 300
  - h. Ip адрес ns1 равный внутреннему IP хоста c7-1
  - i. Имя gate с IP равным внутреннему IP хоста c7-1
  - j. Псевдоним www, направляющий клиента на хост gate.<fio>.local.
4. Для проверки файла зоны используйте утилиту named-checkzone
5. На хосте c7-2 проверьте, что все записи в вашем домене работают

### Артефакты:

#### 1. Тексты команд и консольные выводы команд Части 2 п.2.

##### Часть №1

Настройка IP-адресов:

# Для c7-1

```
sudo ip addr add 10.0.0.1/24 dev <имя_интерфейса_внутренней_сети>
```

```
root@c7-1:/home/vboxuser# ip addr add 10.0.0.1/24 dev enp0s8
```

```
sudo ip link set <имя_интерфейса_внутренней_сети> up
```

```
root@c7-1:/home/vboxuser# ip link set enp0s8 up
```

# Для c7-2

```
sudo ip addr add 10.0.0.2/24 dev <имя_интерфейса_внутренней_сети>
```

```
root@c7-2:/home/vboxuser# ip addr add 10.0.0.2/24 dev enp0s3
```

```
sudo ip link set <имя_интерфейса_внутренней_сети> up
```

```
root@c7-2:/home/vboxuser# ip link set enp0s3 up
```

Отключение IPv6 на обоих хостах:

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
```

```
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

```
root@c7-1:/home/vboxuser/labs/lab1# sysctl -w net.ipv6.conf.all.disable_ipv6=1
```

```
net.ipv6.conf.all.disable_ipv6 = 1
```

```
root@c7-1:/home/vboxuser/labs/lab1# sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

```
net.ipv6.conf.default.disable_ipv6 = 1
```

```
root@c7-1:/home/vboxuser/labs/lab1#
```

```
root@c7-2:/home/vboxuser# sysctl -w net.ipv6.conf.all.disable_ipv6=1
```

```
net.ipv6.conf.all.disable_ipv6 = 1
```

```
root@c7-2:/home/vboxuser# sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

```
net.ipv6.conf.default.disable_ipv6 = 1
```

```
root@c7-2:/home/vboxuser#
```

Задание имен хостов:

```
echo "10.0.0.1 c7-1" | sudo tee -a /etc/hosts
```

```
echo "10.0.0.2 c7-2" | sudo tee -a /etc/hosts
```

```
root@c7-1:/home/vboxuser/labs/lab1# echo "10.0.0.1 c7-1" | sudo tee -a /etc/hosts
10.0.0.1 c7-1
```

```
root@c7-1:/home/vboxuser/labs/lab1# echo "10.0.0.1 c7-2" | sudo tee -a /etc/hosts
10.0.0.1 c7-2
```

```
root@c7-2:/home/vboxuser# echo "10.0.0.1 c7-1" | sudo tee -a /etc/hosts
10.0.0.1 c7-1
```

```
root@c7-2:/home/vboxuser# echo "10.0.0.1 c7-2" | sudo tee -a /etc/hosts
10.0.0.1 c7-2
```

Проверка доступности хостов:

с c7-1 на c7-2:

```
ping 10.0.0.2
```

```
root@c7-1:/home/vboxuser/labs/lab1# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.87 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=9.30 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.01 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.750 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=1.04 ms
^C
--- 10.0.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5406ms
rtt min/avg/max/mdev = 0.750/2.498/9.304/3.063 ms
root@c7-1:/home/vboxuser/labs/lab1#
```

с c7-2 на c7-1:

```
ping 10.0.0.1
```

```
root@c7-2:/home/vboxuser# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.55 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.853 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.532 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.818 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=3.03 ms
^C
--- 10.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5149ms
rtt min/avg/max/mdev = 0.532/1.314/3.031/0.828 ms
```

Настройка шлюза и DNS:

Убедимся, что на c7-2 задан шлюз и DNS, указывающий на c7-1:

```
echo "nameserver 10.0.0.1" | sudo tee /etc/resolv.conf
```

```
root@c7-2:/home/vboxuser# echo "nameserver 10.0.0.1" | sudo tee /etc/resolv.conf
nameserver 10.0.0.1
```

Установка пакетов bind и bind-utils:

```
sudo apt install bind bind-utils -y
```

Часть №2

Команда dig:

```
dig www.itmo.ru
```

```

(root@kali)-[/home/kali]
# dig www.itmo.ru

; <<>> DiG 9.19.21-1+b1-Debian <<>> www.itmo.ru
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 54208
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;www.itmo.ru.                IN      A

;; ANSWER SECTION:
www.itmo.ru.                7200    IN      A      51.250.54.78

;; AUTHORITY SECTION:
itmo.ru.                    7200    IN      NS      ns5.itmo.ru.
itmo.ru.                    7200    IN      NS      ns3.itmo.ru.
itmo.ru.                    7200    IN      NS      ns2.itmo.ru.
itmo.ru.                    7200    IN      NS      ns.itmo.ru.

;; ADDITIONAL SECTION:
ns.itmo.ru.                 7200    IN      A      77.234.194.2
ns2.itmo.ru.                7200    IN      A      77.234.221.75
ns3.itmo.ru.                7200    IN      A      77.234.216.2
ns5.itmo.ru.                7200    IN      A      51.250.74.203

;; Query time: 40 msec
;; SERVER: 77.234.194.2#53(77.234.194.2) (UDP)
;; WHEN: Thu Oct 31 01:50:30 EDT 2024
;; MSG SIZE rcvd: 191

```

Решение задач с dig:

а. Получить только IP-адрес:

dig +short [www.itmo.ru](http://www.itmo.ru)

```

(root@kali)-[/home/kali]
# dig +short www.itmo.ru
51.250.54.78

```

б. Подробная информация о разрешении:

dig +trace [www.itmo.ru](http://www.itmo.ru)

```

(root@kali) ~ [~/home/kali]
# dig +trace www.itmo.ru

; <<>> DiG 9.19.21-1+b1-Debian <<>> +trace www.itmo.ru
;; global options: +cmd
.          395697 IN      NS      c.root-servers.net.
.          395697 IN      NS      g.root-servers.net.
.          395697 IN      NS      m.root-servers.net.
.          395697 IN      NS      k.root-servers.net.
.          395697 IN      NS      e.root-servers.net.
.          395697 IN      NS      d.root-servers.net.
.          395697 IN      NS      j.root-servers.net.
.          395697 IN      NS      l.root-servers.net.
.          395697 IN      NS      f.root-servers.net.
.          395697 IN      NS      b.root-servers.net.
.          395697 IN      NS      h.root-servers.net.
.          395697 IN      NS      a.root-servers.net.
.          395697 IN      NS      i.root-servers.net.
.          461270 IN      RRSIG   NS 8 0 518400 20241112050000 20241030040000 61050 .
.          cmlv1sSI44B1+bMH9U1yc+ZxSN+W2asMWeGhCIRBSa5jjZP+ejKF+KUa Yg7H7XFRwX0J3Cwa5P1CxaJVLhwIXL3jInmpl2R
.          jdELXki8FGkDcaJO 24ToMo/dD+gCtrRnJ0or0a7*5t53t+Innk7*0zIaKz8/e+0foANFD8aj tCkZLJkIKh110qkxHZgLwJ
.          B0Zy7Zs5qpY7ZUxBwhMhYL670cdFxd6bz v2B/Gm3aCB0P0i+MSgI70Kpa3hg76QoWAT0kZdrib4+cwUL1ULV4+Fn3 T35sqry
.          97Y/YD0u/fm4NMrgMNCCK3uvCdVQHnk0pHnNn6LSuDqQLeGen wm7s6g==
;; Received 1097 bytes from 77.234.194.2#53(77.234.194.2) in 60 ms

ru.        172800 IN      NS      a.dns.ripn.net.
ru.        172800 IN      NS      b.dns.ripn.net.
ru.        172800 IN      NS      d.dns.ripn.net.
ru.        172800 IN      NS      e.dns.ripn.net.
ru.        172800 IN      NS      f.dns.ripn.net.
ru.        86400  IN      DS      43786 8 2 3C597475440908C7441905F69E32D8C9B18EA48C
BDAA33C094356191 20CED431
ru.        86400  IN      RRSIG   DS 8 1 86400 20241113050000 20241031040000 61050 .
.          hWIEtERw4vy83xoyeS+ToaAunI3edtI0ajsB3SR1RATCgfh0J194ArI/ lFWw/QuillQAOTRdY6Rk92IMkST7v85ZuPndY8KUn
.          l6T4tGrZTa3hibvi g8adODz/iXDMryoYB1jX5QAxahmufTajX6E1JI3XFnSAcdeXz9od45u bUhxDco1YJiJTSLI8EyMu2WS
.          IC17xy+vu/d4Wt3R8bTv5Txx85L885j1 TnyEhczpGUOSq3HCW9X/ml5cxh+a3uWnMnPeF/Ow0eSfdHMWS8Xqm5Lk4 k2kFx44Q
.          80tiI67mTealdldEIHCXauLi/q6T9W039yboXCvvrZJP146 1k5MbA==
;; Received 687 bytes from 192.5.5.241#53(f.root-servers.net) in 20 ms

;; UDP setup with 2001:678:14:0:193:232:156:17#53(2001:678:14:0:193:232:156:17) for www.itmo.ru fa
iled: network unreachable.
;; no servers could be reached

;; UDP setup with 2001:678:14:0:193:232:156:17#53(2001:678:14:0:193:232:156:17) for www.itmo.ru fa
iled: network unreachable.
;; no servers could be reached

;; UDP setup with 2001:678:14:0:193:232:156:17#53(2001:678:14:0:193:232:156:17) for www.itmo.ru fa
iled: network unreachable.
ITMO.RU.   345600 IN      NS      ns5.itmo.RU.
ITMO.RU.   345600 IN      NS      ns.itmo.RU.
ITMO.RU.   345600 IN      NS      ns3.itmo.RU.
J20C0QKHU3ACUMNKST289FF06U25Q91.ru. 3600 IN NSEC3 1 1 0 - J21LULR2UNPA28SERE28OVNJJ67QP7V NS SOA
RRSIG DNSKEY NSEC3PARAM
J20C0QKHU3ACUMNKST289FF06U25Q91.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241110155306 20240930123609 27
405 ru. Ksy8MA5pKCKJAUCd5UWcRhiv9rtgaepA+diU9VwFE8/PzrPqMhwliX cFpm7I+SZY9mDnj6LK3XQWUxLiojK/yQ
EnbGXkRSaihjK3idLVldqW FfVqalhr/Oul3I0R6ZEvwrs59QnOp3G/HeUJGnLAr/xNFHBggJZdo63qJ QvA=
4QJ9CUIHI1PRLBLSRNMVEV8A49G4SB54.ru. 3600 IN NSEC3 1 1 0 - 4Q55GUB220P82AUVPLRJJ0IK4REULVB2 NS DS
RRSIG
4QJ9CUIHI1PRLBLSRNMVEV8A49G4SB54.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241106123026 20240930123609 27
405 ru. hKq3BpKPz3b/oMFu+5UvyrEaHBF+r8jsrz1MBZEWrrPbPkwahMtBexIf0 LJIG7UKEV6+5z/XF85KSLmWAB13aYJKNZ
uB1UiHtCKm/JSGCigD2uqjl CNPwleIuje6+meNnPgGeZE6pbmSoki2bFWLGlB8eTwKMbfhq+onxo+w8Xc PAs=
;; Received 640 bytes from 193.232.156.17#53(f.dns.ripn.net) in 180 ms

www.itmo.ru. 7200 IN      A      51.250.54.78
itmo.ru.    7200 IN      NS      ns3.itmo.ru.
itmo.ru.    7200 IN      NS      ns5.itmo.ru.
itmo.ru.    7200 IN      NS      ns.itmo.ru.
itmo.ru.    7200 IN      NS      ns2.itmo.ru.
;; Received 219 bytes from 51.250.74.203#53(ns5.itmo.RU) in 24 ms

```

### с. Конфигурационная запись (SOA):

dig soa itmo.ru

```

(root@kali) ~ [~/home/kali]
# dig soa www.itmo.ru

; <<>> DiG 9.19.21-1+b1-Debian <<>> soa www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32658
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;www.itmo.ru.          IN      SOA

;; AUTHORITY SECTION:
itmo.ru.              3600 IN      SOA      ns.itmo.ru. hostmaster.itmo.ru. 2024102902 3600 18
00 86400 3600

;; Query time: 16 msec
;; SERVER: 77.234.194.2#53(77.234.194.2) (UDP)
;; WHEN: Thu Oct 31 01:53:01 EDT 2024
;; MSG SIZE rcvd: 90

```

### d. Определение почтовых серверов:

dig mx itmo.ru



```
(root@kali)~[/home/kali]
# dig mx www.itmo.ru

;<<>> DiG 9.19.21-1+b1-Debian <<>> mx www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46316
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.itmo.ru.                IN      MX

;; AUTHORITY SECTION:
itmo.ru.                     3600    IN      SOA     ns.itmo.ru. hostmaster.itmo.ru. 2024102902 3600 18
00 86400 3600

;; Query time: 16 msec
;; SERVER: 77.234.194.2#53(77.234.194.2) (UDP)
;; WHEN: Thu Oct 31 01:53:43 EDT 2024
;; MSG SIZE rcvd: 90
```

е. Определение DNS-серверов:

`dig ns itmo.ru`

```
(root@kali)~[/home/kali]
# dig ns www.itmo.ru

;<<>> DiG 9.19.21-1+b1-Debian <<>> ns www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 8175
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.itmo.ru.                IN      NS

;; AUTHORITY SECTION:
itmo.ru.                     3600    IN      SOA     ns.itmo.ru. hostmaster.itmo.ru. 2024102902 3600 18
00 86400 3600

;; Query time: 0 msec
;; SERVER: 77.234.194.2#53(77.234.194.2) (UDP)
;; WHEN: Thu Oct 31 01:54:14 EDT 2024
;; MSG SIZE rcvd: 90
```

ф. Запись в зоне обратного просмотра:

`dig -x 87.250.250.242`

```
(root@kali)~[/home/kali]
# dig -x 87.250.250.242

;<<>> DiG 9.19.21-1+b1-Debian <<>> -x 87.250.250.242
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 64686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;242.250.250.87.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
242.250.250.87.in-addr.arpa. 300 IN    PTR     ns1.yandex-app.com.

;; AUTHORITY SECTION:
250.250.87.in-addr.arpa. 34081 IN    NS      ns3.yandex.ru.
250.250.87.in-addr.arpa. 34081 IN    NS      ns4.yandex.ru.

;; ADDITIONAL SECTION:
ns3.YANDEX.ru.             222574 IN     A       87.250.250.1
ns3.YANDEX.ru.             1320   IN     AAAA    2a02:6b8::1001
ns4.YANDEX.ru.             222574 IN     A       77.88.21.1
ns4.YANDEX.ru.             1320   IN     AAAA    2a02:6b8:0:1::1:1

;; Query time: 28 msec
;; SERVER: 77.234.194.2#53(77.234.194.2) (UDP)
;; WHEN: Thu Oct 31 01:56:42 EDT 2024
;; MSG SIZE rcvd: 236
```

г. Количество серверов, поддерживающих корневую зону:

`dig +short ns .`

```
(root@kali)-[/home/kali]
# dig +short ns .
m.root-servers.net.
d.root-servers.net.
a.root-servers.net.
g.root-servers.net.
f.root-servers.net.
k.root-servers.net.
c.root-servers.net.
l.root-servers.net.
i.root-servers.net.
h.root-servers.net.
j.root-servers.net.
b.root-servers.net.
e.root-servers.net.
```

## 2. Конфигурационный файл /etc/named.conf из Части 3, п.3.

### Часть №3

Разрешение доступа через firewall-cmd:

```
sudo firewall-cmd --permanent --add-service=dns
```

```
sudo firewall-cmd --reload
```

Запуск службы bind:

```
sudo systemctl enable named
```

```
sudo systemctl start named
```

```
(root@kali)-[/home/kali]
# sudo systemctl enable named
Synchronizing state of named.service with SysV service script with /usr/lib/systemd/systemd-sysv-installer.
Executing: /usr/lib/systemd/systemd-sysv-install enable named
Created symlink /etc/systemd/system/bind9.service → /usr/lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.

(root@kali)-[/home/kali]
# sudo systemctl start named
```

```
(root@kali)-[/home/kali]
# sudo systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-10-31 02:35:53 EDT; 1min 10s ago
     Docs: man:named(8)
   Main PID: 22943 (named)
    Status: "running"
     Tasks: 18 (limit: 4610)
    Memory: 39.9M (peak: 40.1M)
       CPU: 99ms
    CGroup: /system.slice/named.service
            └─22943 /usr/sbin/named -f -u bind
```

Редактирование /etc/bind/named.conf.options:

```

GNU nano 8.0 /etc/bind/named.conf.options *
options {
    // Addresses and ports on which the DNS server will listen for requests
    listen-on port 53 { 10.0.0.1; }; // Only on the internal IP address of c7-1
    listen-on-v6 { none; }; // Disable IPv6

    // Allow DNS queries only from the specified subnet and localhost
    allow-query { localhost; 10.0.0.0/24; };

    // Enable recursion so the server can perform requests for the host c7-2
    recursion yes;

    // Set cache TTL for requests
    max-cache-ttl 86400; // Maximum caching time - 1 day
    max-ncache-ttl 3600; // Maximum negative caching time - 1 hour

    // Enable security settings
    dnssec-validation auto; // Enable DNSSEC for auth checks

    // Replace server version information
    version "My Own DNS Server";
};

```

**listen-on port 53 { 10.0.0.1; };** — ограничивает сервер для обработки запросов только на IP-адресе 10.0.0.1.

**listen-on-v6 { none; };** — отключает поддержку IPv6.

**allow-query { localhost; 10.0.0.0/24; };** — разрешает принимать DNS-запросы только с подсети 10.0.0.0/24 и с локального хоста (для безопасности).

**recursion yes;** — включает рекурсию, чтобы c7-1 мог выполнять запросы и получать ответы от других DNS-серверов для клиентов.

**max-cache-ttl 86400;** и **max-ncache-ttl 3600;** — задают параметры времени кэширования для положительных и отрицательных ответов соответственно.

**dnssec-validation auto;** — включает автоматическую проверку подлинности с использованием DNSSEC.

**version "My Own DNS Server";** — скрывает реальную версию BIND и возвращает заданное значение при запросе версии сервера.

После редактирования файла выполняем проверку и перезапуск DNS-сервер для применения изменений:

```

sudo named-checkconf /etc/bind/named.conf.options
sudo systemctl restart bind9

```

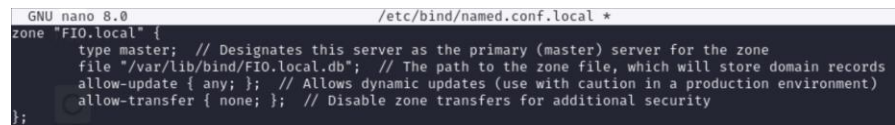
3. Параметры, добавленные в файл /etc/named.conf в Части 4. п. 3.

4. Файл зоны, созданный в Части 4

Часть №4

Обновление /etc/bind/named.conf.local для добавления новой зоны:

```
sudo nano /etc/bind/named.conf.local
```



```
GNU nano 8.0 /etc/bind/named.conf.local *
zone "fio.local" {
    type master; // Designates this server as the primary (master) server for the zone
    file "/var/lib/bind/fio.local.db"; // The path to the zone file, which will store domain records
    allow-update { any; }; // Allows dynamic updates (use with caution in a production environment)
    allow-transfer { none; }; // Disable zone transfers for additional security
};
```

**zone "<fio>.local"** — объявляет начало новой зоны с именем <fio>.local. Данная зона будет обслуживаться DNS-сервером, который выполняет роль основного для этой зоны.

**type master;** — указывает, что этот сервер является главным сервером имен (Master DNS) для указанной зоны. Главный сервер отвечает за хранение и обслуживание записей зоны, а также за распространение изменений вторичным серверам.

**file "/var/lib/bind/<fio>.local.db";** — задает путь к файлу зоны, в котором будут храниться DNS-записи для домена <fio>.local. Этот файл должен быть создан и настроен отдельно для включения SOA-записи, а также любых других записей, таких как A-записи, NS-записи, CNAME-записи и т. д.

**allow-update { any; };** — разрешает динамические обновления записей в зоне от любого источника. Этот параметр делает возможным добавление и изменение DNS-записей в зоне в режиме реального времени. В производственной сети рекомендуется ограничить доступ для динамических обновлений из соображений безопасности.

**allow-transfer { none; };** — запрещает передачу зоны другим DNS-серверам. Это повышает безопасность зоны, поскольку предотвращает копирование данных зоны потенциально небезопасными серверами или серверами, которые не имеют права получать эти данные.

Проверка конфигурации на наличие синтаксических ошибок:

```
sudo named-checkconf /etc/bind/named.conf.local
```

```
(root@kali)-[/home/kali]
# named-checkconf /etc/bind/named.conf.local

(root@kali)-[/home/kali]
#
```

Создание файла зоны:

Создаём файл зоны, который будет содержать все записи DNS для пользовательского домена:

```
sudo nano /var/lib/bind/<fio>.local.db
```

```
GNU nano 8.0 /etc/bind/FIO.local.db *
$TTL 300 ; Default Time-To-Live for all records in this zone (300 seconds)

@      IN SOA ns1.FIO.local. hostmaster.FIO.local. (
        2024110101 ; Serial (format: YYYYMMDDnn, when nn is an incremental number for updates)
        43200      ; Refresh interval (in seconds)
        3600       ; Retry interval (in seconds)
        3600000    ; Expiry time (in seconds)
        300        ; Minimum TTL (in seconds)
)

; Define the primary name server for the zone
@      IN NS  ns1.FIO.local.

; Define IP addresses for key hosts in the zone
ns1 IN A   10.0.0.1 ; ns1 host IP (Primary DNS server)
gate IN A  10.0.0.1 ; gate host IP

; Create a CNAME for www that points to the gate host
www IN CNAME gate
```

**\$TTL 300** — TTL (Time to Live) по умолчанию для всех записей в зоне.

**Запись SOA** — определяет начало авторизации (SOA) для зоны:

**Serial** — используется для контроля версий файла зоны.

**Refresh** — интервал, через который вторичный сервер DNS проверяет обновления.

**Retry** — время, через которое вторичный DNS будет пытаться повторить неудачное обновление.

**Expiry** — время, по истечении которого данные зоны будут считаться устаревшими, если связь с основным DNS потеряна.

**Minimum TTL** — минимальное TTL для кэширования отрицательных ответов.

**NS-запись** — указывает ns1.<fio>.local как основной сервер имен для домена.

**A-записи** — сопоставляют IP-адреса для ns1 и gate.

**CNAME-запись** — создает псевдоним `www`, указывающий на `gate`, так что `www.<fio>.local` будет указывать на IP-адрес `gate.<fio>.local`

Проверка файла зоны на ошибки синтаксиса:

```
sudo named-checkzone FIO.local /var/lib/bind/FIO.local.db
```

```
(root@kali)-[/home/kali]
# named-checkconf FIO.local /var/lib/bind/FIO.local.db
```

Перезапуск службы BIND:

```
sudo systemctl restart bind9
```

### **Вопросы и задания:**

1. Опишите, как в выводе команды `dig` соотносятся секции `HEADER`, `QUESTION SECTION`, `ANSWER SECTION`, `AUTHORITY SECTION`, `SERVER`, `WHEN` и `MSG SIZE` с полями секции `HEADER`. Опишите назначение каждой секции.

*Ответ:* Команда `dig` (Domain Information Groper) используется для запроса DNS-записей. В её выводе представлены различные секции, каждая из которых имеет своё назначение.

#### **1.1 HEADER**

Секция **HEADER** содержит метаданные запроса и ответа. Она включает такие поля, как:

- **id:** Уникальный идентификатор запроса, используемый для соответствия между запросом и ответом.
- **qr:** Флаг, указывающий, является ли сообщение ответом (1) или запросом (0).
- **opcode:** Тип запроса (обычно `QUERY`).
- **aa:** Флаг, указывающий, является ли ответ авторитетным (1) или нет (0).
- **tc:** Флаг, указывающий, что ответ обрезан.
- **rd:** Флаг рекурсивного запроса.
- **ra:** Флаг, указывающий, что сервер поддерживает рекурсивные запросы.
- **z:** Зарезервировано для будущего использования.

- **rcode:** Код ответа (например, NOERROR, NXDOMAIN и т.д.).
- **qdcount:** Количество вопросов в секции QUESTION.
- **ancount:** Количество ответов в секции ANSWER.
- **nscount:** Количество записей в секции AUTHORITY.
- **arcount:** Количество записей в секции ADDITIONAL.

## 1.2 QUESTION SECTION

Секция **QUESTION SECTION** содержит запрашиваемую информацию. Она включает в себя:

- **NAME:** Имя запрашиваемого домена.
- **TYPE:** Тип записи (A, AAAA, MX, и т.д.).
- **CLASS:** Класс записи (обычно IN для Internet).

## 1.3 ANSWER SECTION

Секция **ANSWER SECTION** содержит ответ на запрос. Каждая запись включает:

- **NAME:** Имя запрашиваемого домена.
- **TTL:** Время жизни записи, указывающее, как долго она может кэшироваться.
- **CLASS:** Класс записи (обычно IN).
- **TYPE:** Тип записи (например, A, AAAA).
- **DATA:** Данные, связанные с записью (например, IP-адрес для записи A).

## 1.4 AUTHORITY SECTION

Секция **AUTHORITY SECTION** содержит информацию об авторитетных DNS-серверах для запрашиваемого домена. Она включает записи о серверах имен (NS) и их IP-адресах, которые могут дать дополнительные сведения о домене.

## 1.5 ADDITIONAL SECTION

Секция **ADDITIONAL** (если присутствует) содержит дополнительные записи, которые могут быть полезны. Например, IP-адреса авторитетных DNS-серверов из секции AUTHORITY.

## 1.6 SERVER

Поле **SERVER** указывает на DNS-сервер, к которому был сделан запрос. Здесь отображается IP-адрес или имя сервера, использованного для разрешения запроса.

### 1.7 WHEN

Поле **WHEN** показывает дату и время выполнения запроса. Это полезно для аудита и отладки.

### 1.8 MSG SIZE

Поле **MSG SIZE** указывает размер ответа в байтах. Это может быть полезно для оценки объема данных, возвращаемых в ответе.

2. Как по ответу утилиты dig в Части 3 можно понять, что ответ получен именно от вашего кэширующего DNS сервера?

*Ответ:* чтобы понять, что ответ получен от вашего кэширующего DNS сервера, нужно обратить внимание на следующие аспекты в выводе dig:

1. Секция HEADER: если поле `qr` равно 1, это означает, что ответ получен от DNS-сервера.
2. ID: Идентификатор в секции HEADER должен совпадать с ID, который был отправлен в запросе. Это подтверждает, что ответ соответствует вашему запросу.
3. SERVER: IP-адрес в поле SERVER должен совпадать с IP-адресом вашего кэширующего DNS сервера.
4. Секция ANSWER: если вы видите ожидаемые записи (например, A или CNAME) в секции ANSWER, это подтверждает, что кэширующий сервер обработал запрос и вернул данные.
5. Метаданные (например, TTL): если значение TTL (в секции ANSWER) невелико, это может указывать на то, что данные были кэшированы на вашем DNS-сервере, а не получены из первоисточника.

Если все эти условия соблюдаются, вы можете быть уверены, что ответ пришёл от вашего кэширующего DNS сервера.