DNS (Bind9)

Установка

- Debian

  `apt install bind9`

  `apt install bind9utils dnsutils`

- CentOS

  `apt install bind`

  `apt install bind-utils`

Связанные файлы

- Debian
  - **/etc/bind/** - директория файлов конфигурации и примеров файлов зон
    - **./named.conf** - подключение следующих файлов:
      - **./named.conf.options** - параметры работы DNS-сервера
      - **./named.conf.default-zones** - перечисление зон
  - **/etc/default/bind9** - изменение стартовых опций

- CentOS
  - **/etc/named.conf** - опции сервера и подключение файла зон
  - **/etc/named.rfc1912.zones** - перечисление зон
  - **/var/named** - стандартное расположение файлов зон (шаблонов)

Утилиты для управления сервером

1. named-checkconf

2. named-checkzone

3. rndc ...

Конфигурирование

- Опции (***дописать***)
  - **Debian** (/etc/bind/named.conf.options)

    Настройки можно оставить по умолчанию

Может понадобиться раскоментировать зону **forwarders**, чтобы определить сервера для пересылки запросов выходящих за рамки обслуживаемой зоны

- **CentOS** (/etc/named.conf)

  Настройки можно оставить по умолчанию.

  Можно добавить параметр **allow-query {any; }** для принятия запросов из любых источников

https://serveradmin.ru/nastroyka-dns-servera-bind-v-centos-7/

- Файл определения зон
  - **Debian** (/etc/bind/named.conf.default-zones) и **CentOS** (/etc/named.rfc1912.zones)

    Файл содержит перечисление зон в виде блоков с параметрами (тип, файл, опции):

    1. **Имя зоны**
       - Прямая

```
zone "skill39.wsr" {
...
 };
```

       - Обратная

```
 zone "20.16.172.in-addr.arpa" {
...
};
```

    2. **Тип зоны**

```
    type [master, slave, hint, stub]
```

    - **master** - сервер является первичным уполномоченным сервером для данной зоны, т.е. загружает содержимое зоны из файла зоны, указанного опцией **file**
      - **slave** - сервер является вторичным уполномоченным сервером для данной зоны; содержимое зоны считывается от одного из серверов, указанных в опции **masters**; указание имени файла в опции **file** позволяет сохранять резервную копию зоны в файле
    - **hint** - позволяет задать с помощью опции **file** имя файла, содержащего описание корневой зоны; этот файл можно взять в Internic; сервер при загрузке обращается к одному из корневых серверов, перечисленных в этом файле, для получения текущего списка корневых серверов; полученный список используется в течении указанного TTL; для класса IN имеется встроенный список предполагаемых корневых серверов
      - **stub** - использовался в предыдущих версиях BIND для упрощения настройки; использовать не рекомендуется
    3. **Файл**

```
file "/opt/dns/skill39.wsr.db"
```

    Имя файла, в котором хранится содержимое зоны.

    4. **Masters**

```
masters {172.16.20.10; }
```

Адреса и номера портов серверов, с которых брать содержимое зоны (порт 53 по умолчанию). Номер порта перед списком задает общий номер порта для всех серверов; если указано несколько серверов, то они опрашиваются все, а зона запрашивается с того из них, у кого она имеет наибольший серийный номер; указание ключа позволяет проверять правильность передачи с помощью цифровой подписи TSIG

дорасписать опции

- Файл зоны
  - **Debian** (примеры находятся /etc/bind/db.*) и **CentOS** (примеры находятся /var/named/named. *)

    db.local

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1

```

    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
```

    , где:

    - $TTL - Время актуальности записей в секундах. Необходим, чтобы указать другим DNS-серверам, как долго стоит хранить запись у себя в кэше. Слишком малое значение увеличит нагрузку на сервер, а большое приведет к слишком длительному процессу изменения записи.

- @ - переменная, хранящая имя зоны.
- IN - класс. Всегда используется IN (Internet). Указывает на тип сети.
- localhost. - Собственно доменное имя хоста. Может записываться без домена — он будет дописан автоматически. Также может быть записан полностью с доменом — в таком случае необходимо поставить точку на конце, например, mail.test.local. Если не указывается или обозначается знаком собаки (@), запись создается для имени зоны (в данном случае, test.local).
- root.localhost. - лицо ответственное за данную зону
- SOA-запись:
  - **Serial** — порядковый номер изменения. **Его необходимо каждый раз менять вручную при редактировании файла**. С помощью него вторичный сервер (если такой есть), может определить, что были изменения и начать процесс копирования настроек.
  - **Refresh** указывает вторичным серверам, через какой промежуток времени они должны сделать запрос на обновление зоны.
  - **Retry** говорит вторичным серверам, как часто повторять попытки на обновление зоны, если первичный сервер не смог дать ответ (сервис был недоступен).
  - **Expire** — время в секундах, которое может работать вторичный сервер, если недоступен первичный. Если данный период истечет, а вторичный сервер так и не смог обновить зону, он должен прекратить отвечать на запросы.
- Типы записей

```
@       IN      NS      localhost.
test    IN      A       172.16.20.1
serv    IN      CNAME   test
1       IN      PTR     test.localhost.
```

Основные типы записей, использующиеся в DNS:

1. **A** — сопоставляет имени узла соответствующий IP-адрес.
2. **NS** — указатель на DNS-сервера, которые обслуживают данную зону.
3. **MX** — почтовая запись. Указывает на почтовые сервера, которые обслуживают домен. Поддерживает приоритизацию — при указании нескольких записей, клиент будет ориентироваться на значение той, для которой указано меньшее число.
4. **CNAME** — aliase или псевдоним. Перенаправляет запрос на другую запись.
5. **TXT** — произвольная запись. Чаще всего используется для настройки средств повышения качества отправки почтовых сообщений.

- Дополнительные настройки
  - Debian

    Apparmor (права доступа)

```
nano /etc/apparmor.d/usr.sbin.named
```

Необходимо указать путь по которому располагаются файлы зон (если он отличается от стандартного) и уровень прав.

```
  # /etc/bind should be read-only for bind
  # /var/lib/bind is for dynamically updated zone (and journal) files.
  # /var/cache/bind is for slave/stub data, since we're not the origin of it.
  # See /usr/share/doc/bind9/README.Debian.gz
  /etc/bind/** r,
  /opt/dns/** rw,
  /var/lib/bind/** rw,
  /var/lib/bind/ rw,
  /var/cache/bind/** lrw,
  /var/cache/bind/ rw,
```

В нашем случае это строка `/opt/dns/** rw,`

- CentOS

  Firewalld

  Гасим его при первой возможности

```
systemctl stop firewalld.service
systemctl disable firewalld.service
```

- Запуск сервера
  - Debian

```
systemctl start bind9.service
```

  - CentOS

```
systemctl start named.service
```

Проверка

- nslookup

  Проверка прямой зоны - `nslookup ns1.skill39.wsr`

  Проверка обратной зоны - `nslookup 172.16.20.10`

- dig

Источники:

- http://www.bog.pp.ru/work/bind.html
- https://serveradmin.ru/nastroyka-dns-servera-bind-v-centos-7/#_bind_slave_zone
- https://wiki.yola.ru/bind/bind
- https://www.dmosk.ru/miniinstruktions.php?mini=bind-primary

- https://howitmake.ru/blog/ubuntu/128.html