Конфигурирование Unbound
---

1. Залогиньтесь на вашу машину с кэширующим сервером при помощи SSH/Putty/...:

    (для группы 1, вам следует использовать resolv.grp1.dns.nsrc.org, и т.д.)

    $ ssh sysadm@resolv.grpXX.dns.nsrc.org

    *** ПОЖАЛУЙСТА УБЕДИТЕСЬ, ЧТО ВЫ ЗАЛОГИНИЛИСЬ НА МАШИНУ 'RESOLV', А ***
    *** НЕ НА 'AUTH1' ИЛИ 'AUTH2' ***

2. На resolv:

    $ cd /usr/local/etc/unbound/

    Сейчас у вас выбор из двух вариантов. Вы можете создать unbound.conf
    с нуля, используя пример внизу (вариант I), или вы можете вручную
    отредактировать существующий `unbound.conf`, если хотите.

    Вариант I проще, но выбор за вами!

    Вариант I:

    Если вы хотите сохранить немного времени:

    Создайте файл unbound.conf, и скопируйте туда следующее:

--- линия отреза ---

```
server:
        verbosity: 1
        # интерфейсы (по IP), на которых unbound будет отвечать на запросы
        interface: 0.0.0.0

        # какие клиенты могут осуществлять на (рекурсивные) запросы
        access-control: 10.10.0.0/16 allow

        # Если вы укажете "", unbound не будет делать chroot.  Путь не должен
заканчиваться на "/".
        chroot: ""

        # file to read root hints from.
        root-hints: "/usr/local/etc/unbound/named.root"

        # a number of locally served zones can be configured.
            local-zone: "10.10.in-addr.arpa." nodefault

remote-control:

        # Enable remote control with unbound-control(8) here.
        control-enable: yes

        # what interfaces are listened to for remote control.
        control-interface: 0.0.0.0

        # port number for remote control operations.
        control-port: 953
```

```
        # unbound control files
        server-key-file: "/usr/local/etc/unbound/unbound_server.key"
        server-cert-file: "/usr/local/etc/unbound/unbound_server.pem"
        control-key-file: "/usr/local/etc/unbound/unbound_control.key"
        control-cert-file: "/usr/local/etc/unbound/unbound_control.pem"

--------------------------- линия отреза -----------------------------

    Вариант II:

    Если вам хочется сделать изменение вручную...  В противном случае
    перейдите к следующему шагу!

    $ sudo cp unbound.conf.sample unbound.conf
    Замечание: Используйте ваш любимый редактор: ee, jed, joe, vi, ...

    $ sudo ee unbound.conf
или
    $ sudo vi unbound.conf

    ... и сделайте следующие изменения:

    a) сконфигурируйте "слушающие" интерфейсы - найдите строчки типа:

        # interface: ...
        # interface: ...

    и прямо под ними, добавьте строку:

        interface: 0.0.0.0

    b) контроль доступа - найдите строчки типа:

        # access-control: ...
        # access-control: ...

    и прямо под ними, добавьте строку:

        access-control: 10.20.0.0/16 allow

    c) защита с помощью chroot - найдите строку:

        # chroot: "/usr/local/etc/unbound"

    и прямо под ней, добавьте строку:

        chroot: ""

    Замечание: Обычно мы бы не стали отключать chroot, являющийся защитным
          механизмом, но нам нужно это сделать на время лабораторной работы,
          из-за ограничений используемой виртуальной среды.  В настоящей
          конфигурации, мы бы не стали этого делать.

    d) задайте файл root-hints - найдите строчку:

        # root-hints: ""

    и прямо под ней, добавьте строку:
```

```
    root-hints: "/usr/local/etc/unbound/named.root"
```

e) разрешите зону 20.10.in-addr.arpa - найдите строчку:

```
    # local-data-ptr: "192.0.2.3 www.example.com"
```

и прямо под ней, добавьте строку:

```
    local-zone: "20.10.in-addr.arpa." nodefault
```

f) включите удаленное управление - найдите строчку:

```
    # control-enable: no
```

и ИЗМЕНИТЕ ее (удалив # в начале строки) на:

```
    control-enable: yes
```

- найдите строчку:

```
    # control-interface: 127.0.0.1
```

и ИЗМЕНИТЕ ее на:

```
    control-interface: 0.0.0.0
```

- найдите строчку:

```
    # control-port: 8953
```

и ИЗМЕНИТЕ ее на:

```
    control-port: 953
```

- наконец, уберите комментарии из следующих четырех строк:

```
    # server-key-file: "/usr/local/etc/unbound/unbound_server.key"
станет
    server-key-file: "/usr/local/etc/unbound/unbound_server.key"

    # server-cert-file: "/usr/local/etc/unbound/unbound_server.pem"
станет
    server-cert-file: "/usr/local/etc/unbound/unbound_server.pem"

    # control-key-file: "/usr/local/etc/unbound/unbound_control.key"
станет
    control-key-file: "/usr/local/etc/unbound/unbound_control.key"

    # control-cert-file: "/usr/local/etc/unbound/unbound_control.pem"
станет
    control-cert-file: "/usr/local/etc/unbound/unbound_control.pem"
```

Сохраните файл, выйдите из редактора.

Вам все еще нужно скопировать файл named.root туда, где unbound сможет его найти.

```
    $ cd /usr/local/etc/unbound
```

```
        $ sudo cp /etc/namedb/named.root .
```

3. Создайте управляющие ключи:

```
    $ sudo unbound-control-setup
```

4. Проверьте правильность конфигурации:

```
    $ sudo unbound-checkconf
```

5. Отредактируйте /etc/rc.conf и добавьте:

```
    unbound_enable="YES"
```

6. Запустите unbound!

```
    $ sudo service unbound start
```

7. Поменяйте ваш /etc/resolv.conf так, что он использует свеженастроенный Unbound, на этой машине (RESOLV), а такжи и на AUTH1 и на AUTH2:

```
    # vi /etc/resolv.conf
```

    Поменяйте строку DNS-сервера на:

```
        nameserver 10.20.XX.3
```

    ... где XX - номер вашей группы

8. Тестирование

```
    $ dig
    $ dig noc.dns.nsrc.org
```

        Убедитесь, что вы видите SERVER: ...(10.20.XX.3) в конце вывода команды dig.

```
    $ dig version.bind txt chaos
```

    Что показывает dig?

9. Убедитесь, что BIND на AUTH1 НЕ ЯВЛЯЕТСЯ рекурсивным.

   Замечание: Вам НЕ нужно этого делать, если только вы не включили рекурсию в вашей конфигурации BIND.

   Итак, нам нужно зайти на машину AUTH1, и поменять resolv.conf.

   Залогиньтесь на ваш мастер (auth1.grpX.dns.nsrc.org), и измените /etc/resolv.conf так, что он теперь использует свеженастроенный unbound:

```
    $ sudo ee /etc/resolv.conf
```

И сделайте его похожим на вот это:

```
    search dns.nsrc.org
    nameserver 10.20.X.3
```

... где X - номер вашей группы

Затем убедитесь, что вы можете находить информацию об именах *.dns.nsrc.org:

$ dig noc.dns.nsrc.org

Проверьте раздел SERVER: в конце вывода команды dig, чтобы убедиться,
что правильный сервер был запрошен

Наконец, выключите рекурсию на машине AUTH1.

Редактируйте /etc/namedb/named.conf (sudo ee ...) и сделайте следующие изменения:

Было:

```
allow-recursion { 127.0.0.1; 10.20.0.0/16; };
```

Должно быть:

```
// allow-recursion { 127.0.0.1; 10.20.0.0/16; };
recursion no;
```

Если этих строк нет в файле, не волнуйтесь, а просто пропустите этот шаг!

Сохраните файл, и перезапустите named:

$ sudo service named restart