DNS делегирование - упражнение

В этом упражнении, мы создадим новый домен верхнего уровня в
нашем корне.
Например: MYTLD

В создадите DNS-сервер мастер на вашей собственной машине, и кто-то другой
предоставит слейв-сервер. Потом вы попросите администратора для домена
уровня выше вашего (корня) делегировать ваш домен вам.

Замечание: нижеследующие должно быть сделано с правами администратора,
как пользователь "root" - воспользуйтесь sudo -s

Первым делом, убедитесь что имя вашей машины сконфигурировано
правильно. Воспользуйтесь командой 'hostname' - например,
на auth1.grpXX.dns.nsrc.org, если вы наберете:

```
 # hostname
```

Вы должны увидеть

```
  auth1.grpXX.dns.nsrc.org
```

Если нет, то сконфигурируйте ваш сервер с правильным именем:
например, для auth1.grp25.dns.nsrc.org, наберите:

```
 # hostname auth1.grp25.dns.nsrc.org
```

Не забудьте заменить "grpXX" на правильный номер группы!

Отредактируйте /etc/rc.conf (используя "vi" либо "ee", т.е.: ee /etc/rc.conf),
и обновите "hostname":

```
  hostname="auth1.grpXX.dns.nsrc.org"
```

В файле /etc/hosts, вы должны видеть строчку:

```
  10.20.X.1   auth1.grpXX auth1.grpXX.dns.nsrc.org
```

Упражнение

*   Выберите имя нового домена, запишите его где-нибудь

    т.е.: "MYTLD" или "EARTH" - все что угодно.

    (НЕ выбирайте существующее имя PC, например `auth1.grpXX` в качестве вашего
домена)

    Это может быть например именем вашей страны, кодом страны, названием
    фирмы, и т.д., но ПОМНИТЕ, что кто-то другой может выбрать то же
    самое имя! Кто первым встал, того и тапки.

*   Если вы используете web интерфейс для регистрации (RZM):

    Зарегистрируйте ваш новый домен используя контроллер корневой зоны
    по адресу https://rzm.dnssek.org/

Имя пользователя - ваш MYTLD
Пароль придумайте любой, но не забудьте его для последующих
упражнений. Нажмите кнопку "Signup".

Следующая страница является примером двухфакторной системы безопасности.
Если преподаватель не сказал обратного, оставьте поле "verification code"
пустым и просто нажмите "Proceed". Вы сможете вернуться на эту страницу
позднее для конфигурации вашего талона безопасности (например, Google
Authenticator),
если хочется.

Нажмите logout на следующей странице. Вы введете информацию позднее.

* Найдите кого-то, кто согласится быть слейвом для вашего домена. Пожалуйста
найдите кого-нибудь далеко от вас (не за вашим столом) (Не забудьте RFC2182:
вторичные сервера должны быть на удаленных сетях, но здесь мы будем работать
в одной "плоской" сети). Вы можете иметь более одного слейва, если захотите.

* Создайте файл вашей зоны в `/etc/namedb/master/MYTLD`
(где MYTLD - ваш выбранныей домен) -- вы можете просто
скопировать раздел ниже -- но не забудьте заменить
XXX на ваш IP:

*** Помните, что вам нужно иметь права администратора для создания
*** этого файла, например
***
*** $ cd /etc/namedb/master
*** $ sudo vi MYTLD
***
*** (вы можете использовать любой редактор вместо vi,
*** например joe либо ee)

```
- - - - - - - - - - - - - линия отреза - - - - - - - - - - - -

$TTL 2m
@       IN      SOA     auth1.grpXX.dns.nsrc.org. your.email.address. (
                        2012022301    ; Serial - замените 20120223 текущей датой
                        10m           ; Refresh
                        5m            ; Retry
                        4w            ; Expire
                        2m )          ; Negative

        IN      NS      auth1.grpXXX.dns.nsrc.org.   ; мастер
        IN      NS      auth1.grpYYY.dns.nsrc.org.   ; слейв

www     IN      A       10.20.XXX.1             ; ваш собственный IP

- - - - - - - - - - - - - линия отреза - - - - - - - - - - - -
```

Замените `your.email.address.` вашим домашним E-mail адресом, так что
user@domain.name будет user.domain.name

XXX и YYY это IP-адреса вашей группы и вашего слейва, соответственно.

Мы специально выбрали маленькие значения для TTL, времени обновления,
и времени повтора, для того чтобы исправление ошибок было проще в
условиях класса. Для реального домены вы наверняка будете использовать
бОльшие значения.

*   Отредактируйте `/etc/namedb/named.conf` и сделайте следующее:

  ***   Помните, что вам нужно иметь права администратора для редактирования
  ***   этого файла, например:
  ***
  *** $ cd /etc/namedb
  *** $ sudo vi named.conf
  ***
  ***   (вы можете использовать любой редактор вместо vi,
  ***   например joe либо ee)

    - Если такая строка все еще в файле, УБЕРИТЕ ее:

         listen-on { 127.0.0.1; };

    ... и добавьте другую строку в раздел параметров:

        allow-query { any; };

    ... таким образом ваш DNS-сервер будет отвечать на запросы по сети

    - Добавьте раздел, конфигурирующий вашу машину как мастера для
      вашего домена, добавив что-то вроде нижеследующего в самом конце
      файла:

      zone "MYTLD" {
        type master;
        file "/etc/namedb/master/MYTLD";
      };

    Обращайте внимание на ';' и '}' !

*   Убедитесь, что ваш файл конфигурации и файл зоны корректны:

        # named-checkconf
        # named-checkzone MYTLD /etc/namedb/master/MYTLD

    * Если обнаружены ошибки, исправьте их! *

*   Если это еще не сделано, разрешите named в конфигурации вашего сервера,
    отредактировав файл /etc/rc.conf и добавив следующее:

     ** Снова, не забудьте, вы должны иметь права администратора

        named_chrootdir=""
        named_enable="YES"

    - Потом запустите/перезапустите named при помощи

        # service named restart

    Проверьте результат, выполнив

        # tail /var/log/messages

    Используя dig, проверьте что MYTLD теперь настроен на вашей машине:

        # dig @10.20.XX.1 MYTLD. NS

Где "XX" - номер группы для вашей машины.

Вы можете также проверить состояние DNS-сервера используя rndc:

```
# rndc status
```

- Если обнаружены ошибки, исправьте их. Некоторые ошибки конфигурации могут привести к тому, что named не сможет запуститься; в этом случае вам придется перезапустить его после исправления проблемы:

```
# service named restart
```

* Помогите вашим слейвам с конфигурацией для вашего домена, и сконфигурируйте свой DNS-сервер как слейв, если вас попросит другая группа.

Здесь большая часть того, что вам нужно добавить для этого в named.conf:

```
zone "MYTLD" {
   type slave;
   masters { 10.20.XXX.1; };
   file "/etc/namedb/slave/MYTLD";
};
```

... где XXX - номер группы, которая будет мастером.

Если вы изменили ваш `named.conf` таким образом, что вы теперь слейв для кого-то другого, убедитесь в отсутствии ошибок в `/var/log/messages` после перезапуска вашего DNS-сервера.

Вам понадобится каталог для слейвов с правильными правами доступа и владельцем; bind будет хранить там копию файла зоны, полученной от мастера.

* Проверьте что вы и ваши слейвы выдают авторитетные ответы для вашего домена:

```
# dig +norec @10.20.XXX.1 MYTLD. SOA
# dig +norec @10.20.YYY.1 MYTLD. SOA
```

Убедитесь, что вы получаете AA (авторитетный ответ) от обоих серверов, и что серийные номера совпадают.

* Теперь вы готовы запросить делегирование:

а) если используется RZM:

Посетите https://rzm.dnssek.org/

Залогиньтесь, используя имя пользователя и пароль, которые вы указали в начале упражнения. Нажмите "Proceed".

Введите ваш DNS-сервер, например auth1.grpXX.dns.nsrc.org, и его IP адрес, например 10.20.X.1

Нажмите "Update". Если все прошло как надо, ваш ввод должен появиться с иконкой документа рядом с ним, указывая на то, что проверка прошла успешно и что информация была добавлена в корневой файл зоны.

Вы также увидите строку с иконкой "глаза", указывающую на то,

что другой сервер, ваш слейв, был замечен.
Если информация для слейва выглядит правильной, например, это
auth2.grpYY.dns.nsrc.org, нажмите на "глаз", чтобы получить отметку
о проверке, и потом нажмите на "Update", чтобы добавить и эту
информацию в корневую зону.

b) если вы не используете RZM:

Дайте преподавателю листок бумаги со следующей информацией:

Имя домена: _____

Мастер-сервер: auth1.grp___.dns.nsrc.org

Слейв-сервер: auth1.grp___.dns.nsrc.org

* Вы не получите делегирования до тех пор пока преподаватель не проверит, что:

- все ваши серверы являются авторитетными для вашего домена
- на них на всех совпадает серийный номер в записи SOA
- Записи NS внутри зоны совпадают со списком серверов для которых
  вы запрашиваете делегировние
- Слейв (или слейвы) находятся в другом конце комнаты :)

=> Это называется "правилами по эксплуатации"!

* Когда вы получили делегирование, попытайтесь найти имя www.MYTLD:

- На вашей собственной машине
- На чьей-то другой машине (которая НЕ является вашим слейвом):

```
# dig @10.20.XXX.230 www.MYTLD       (где MYTLD - ваш домен)
```

* Добавьте новую ресурсную запись в ваш файл зоны. Не забудьте поменять серийный номер.
Проверьте, что ваши слейвы обновились. Попробуйте сделать запрос для этого нового имени.