В этой статье мы рассмотрим один из вариантов развертывания DNS сервера для локальной сети на базе Ubuntu (у меня 14.04.3 LTS) и bind9. Для большинства других дистрибутивов отличия будут минимальны, для Debian-подобных их не будет совсем. Если вы уже ознакомились с предыдущей статьей по настройке DHCP сервера , то знаете, что изначально у меня был установлен неподдерживаемый дистрибутивом dnsmasq, который было решено заменить. Поскольку в прошлый раз я удалил dnsmasq (а он был как DHCP, так и DNS - сервером, который, кстати, не был должным образом сконфигурирован и не работал), то появилась потребность в DNS, чем я и решил на досуге заняться. Настройка DNS занимает немногим больше времени, но только из-за большего числа конфигурационных файлов.

И так, приступим. Первым делом актуализируем систему (обновим пакеты):

```
sudo apt-get update && sudo apt-get upgrade -y
```

Теперь установим DNS сервер bind9:

```
sudo apt-get install bind9
```

Теперь можно создать ключ для того, чтобы другие демоны могли обновлять DNS-записи этого сервера. Это могут быть как другие серверы в сети, так и другие сервисы этого же сервера. У меня это будет локально же установленный DHCP сервер. В теории, безопасности для, каждому сервису или серверу нужно сгенерировать свой ключ, тогда при компрометации одного из них, его можно просто заблокировать, а остальные продолжат работать. Но в моем случае обновлять записи будет только мой же DHCP сервер, так что я генерирую только один ключ:

```
dnssec-keygen -a HMAC-MD5 -b 128 -r /dev/urandom -n USER DHCP_UPDATER
```

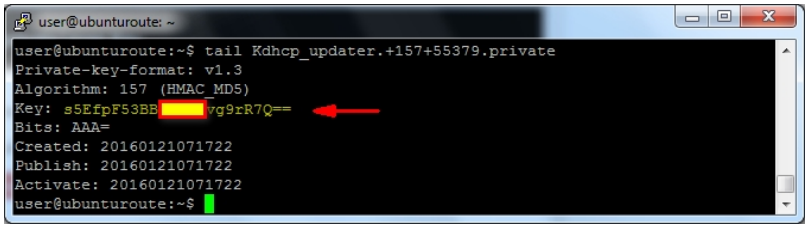
В домашнем каталоге пользователя, от которого была запущена команда появится 2 файла:

-rw------- 1 user user 54 янв. 21 12:17 Kdhcp_updater.+157+55379.key
-rw------- 1 user user 165 янв. 21 12:17 Kdhcp_updater.+157+55379.private

Файлы пусть так и лежат, они не потеряются. Чтобы посмотреть необходимый ключ, выполните:

tail Kdhcp_updater*.private

Вы увидите примерно такое содержимое, кде значение "Key" и есть требуемый ключ:



Для начала сделаем наш DNS сервер кэширующим сервером имен, то есть заставим его разрешать доменные имена, запрашивая их у вышестоящего сервера. При первом запросе доменного имени от клиента сервер будет пересылать запрос на вышестоящий сервер, а затем уже будет возвращать его из своего кэша, что несколько увеличит скорость обработки DNS-запросов для клиентов в нашей сети. Так же мы укажем серверу, на каких адресах наш DNS будет обслуживать клиентов. Для этого нужно отредактировать файл /etc/bind/named.conf.options:

sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.dist && sudo nano /etc/bind/named.conf.options

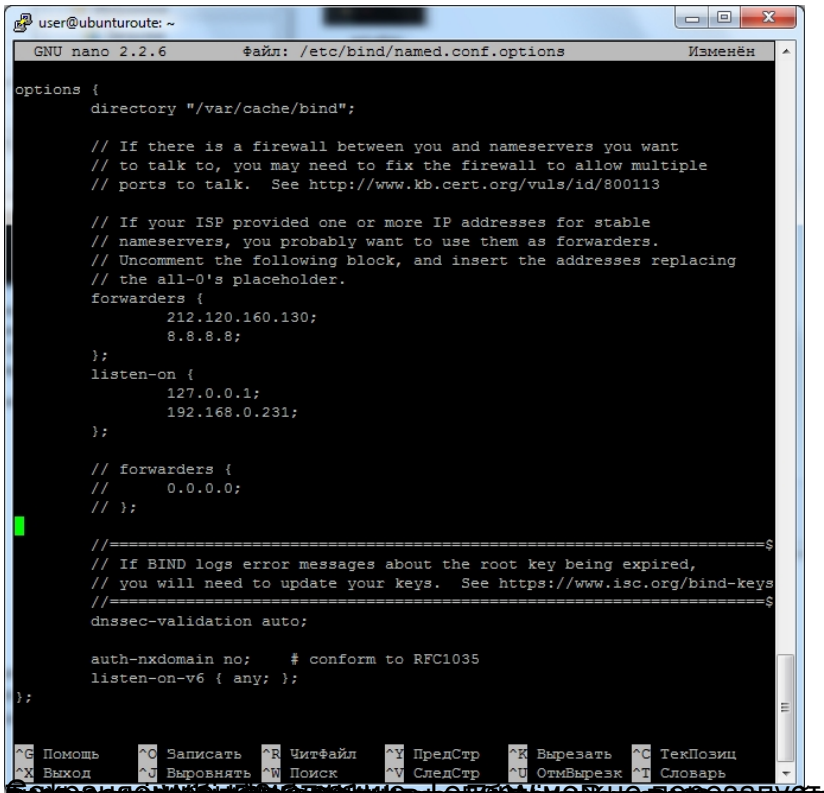
Добавим туда следующие строки:

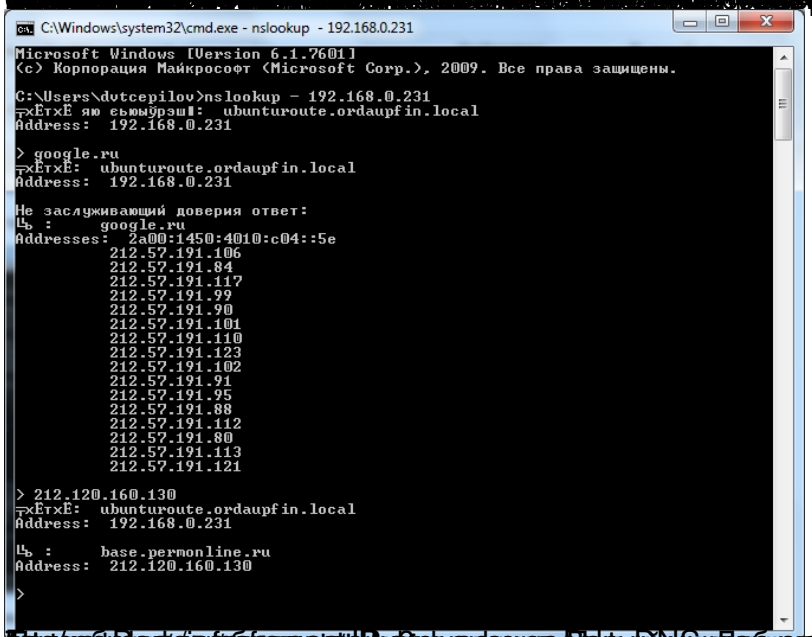
```
forwarders {
        212.120.160.130;
        8.8.8.8;
};
listen-on {
        127.0.0.1;
        192.168.0.231;
};
```

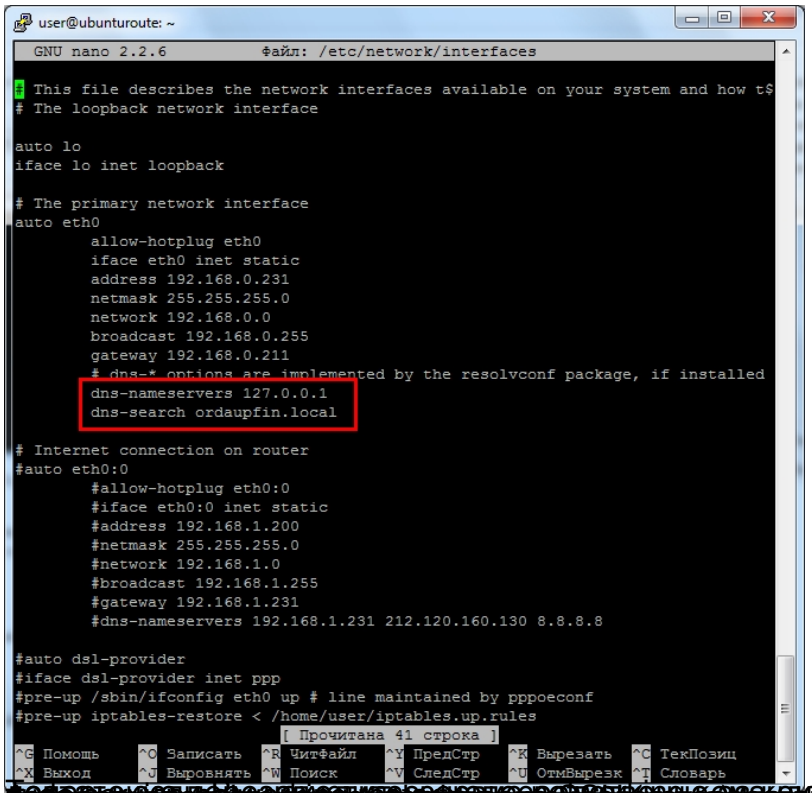
Рассмотри эти секции:

- forwarders - тут указываем вышестоящие серверы имен. Их количество не ограничено, при недоступности одного из них запросы будут пересылаться на следующий в списке. Я указал DNS своего провайдера и Google Public DNS;
- lisnen-on - адреса локальных интерфейсов, на которые сервер будет принимать DNS-запросы клиентов.

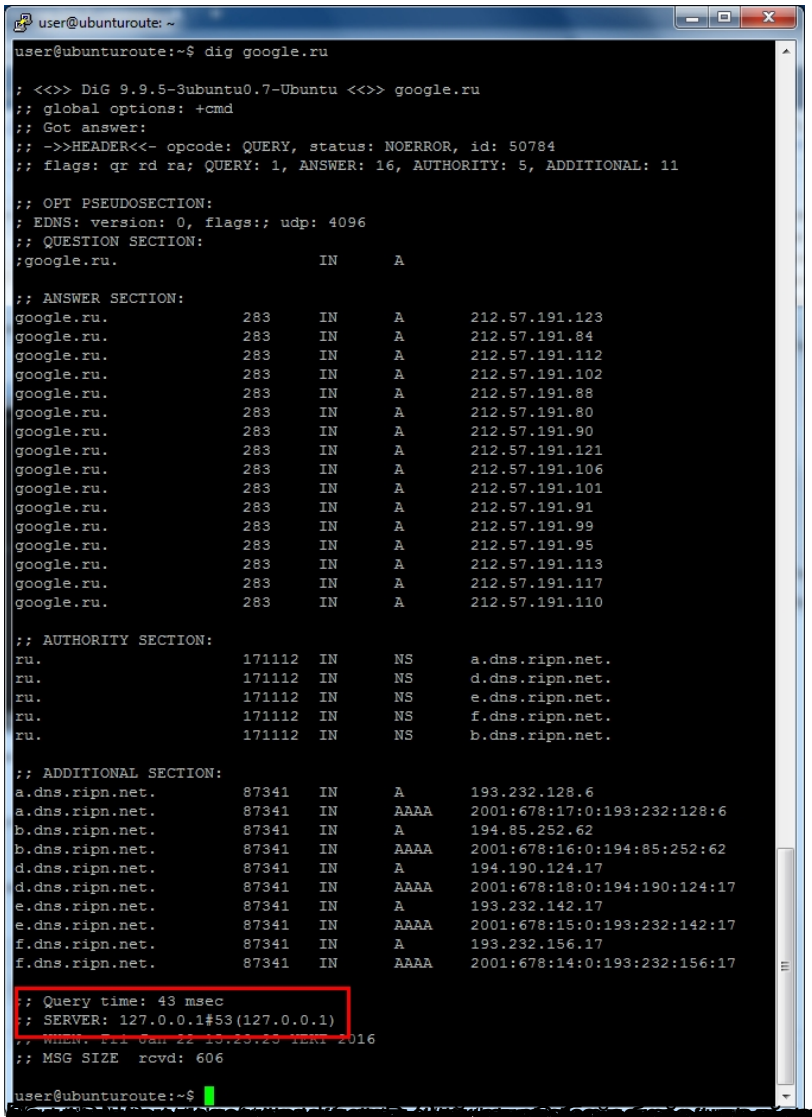
В nano это выглядит примерно так:


user@ubunturoute: ~
GNU nano 2.2.6 Файл: /etc/bind/named.conf.options Изменён
options {
directory "/var/cache/bind";
// If there is a firewall between you and nameservers you want
// to talk to, you may need to fix the firewall to allow multiple
// ports to talk. See http://www.kb.cert.org/vuls/id/800113
// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.
forwarders {
212.120.160.130;
8.8.8.8;
};
listen-on {
127.0.0.1;
192.168.0.231;
};
// forwarders {
// 0.0.0.0;
// };
//==
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//==
dnssec-validation auto;
auth-nxdomain no; # conform to RFC1035
listen-on-v6 { any; };
};
^G Помощь ^O Записать ^R ЧитФайл ^Y ПредСтр ^K Вырезать ^C ТекПозиц
^X Выход ^J Выровнять ^W Поиск ^V СледСтр ^U ОтмВырезк ^T Словарь


C:\Windows\system32\cmd.exe - nslookup - 192.168.0.231
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\dvtcepilov>nslookup - 192.168.0.231
Address: 192.168.0.231
> google.ru
Address: 192.168.0.231
Не заслуживающий доверия ответ:
Addresses: 2a00:1450:4010:c04::5e
212.57.191.106
212.57.191.84
212.57.191.117
212.57.191.99
212.57.191.90
212.57.191.101
212.57.191.110
212.57.191.123
212.57.191.102
212.57.191.91
212.57.191.95
212.57.191.88
212.57.191.112
212.57.191.80
212.57.191.113
212.57.191.121
> 212.120.160.130
Address: 192.168.0.231
Address: 212.120.160.130
>

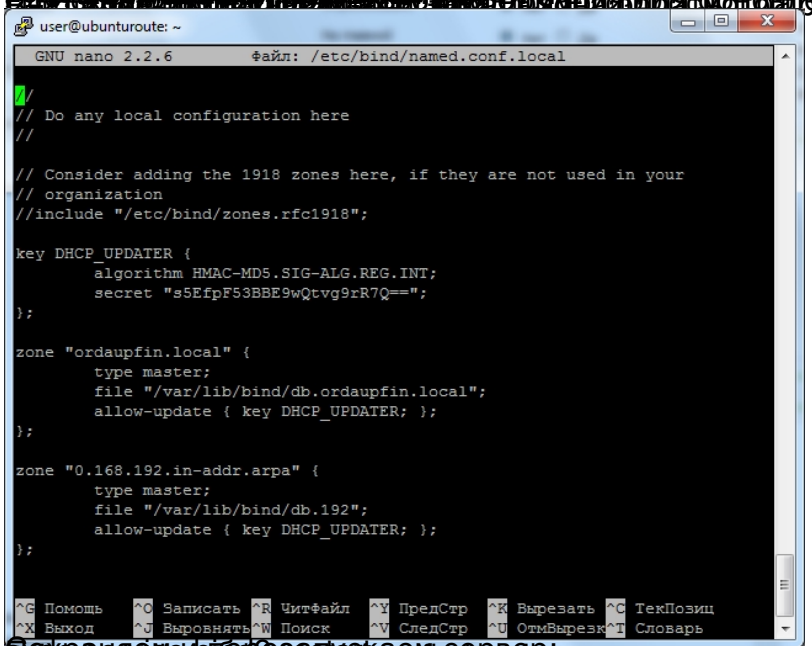


[illegible] сервера финансовому сервису [illegible] – значит все настроено правильно.



```
user@ubunturoute: ~
user@ubunturoute:~$ dig google.ru

; <<>> DiG 9.9.5-3ubuntu0.7-Ubuntu <<>> google.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50784
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 5, ADDITIONAL: 11

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

;; ANSWER SECTION:
google.ru.              283     IN      A       212.57.191.123
google.ru.              283     IN      A       212.57.191.84
google.ru.              283     IN      A       212.57.191.112
google.ru.              283     IN      A       212.57.191.102
google.ru.              283     IN      A       212.57.191.88
google.ru.              283     IN      A       212.57.191.80
google.ru.              283     IN      A       212.57.191.90
google.ru.              283     IN      A       212.57.191.121
google.ru.              283     IN      A       212.57.191.106
google.ru.              283     IN      A       212.57.191.101
google.ru.              283     IN      A       212.57.191.91
google.ru.              283     IN      A       212.57.191.99
google.ru.              283     IN      A       212.57.191.95
google.ru.              283     IN      A       212.57.191.113
google.ru.              283     IN      A       212.57.191.117
google.ru.              283     IN      A       212.57.191.110

;; AUTHORITY SECTION:
ru.                     171112  IN      NS      a.dns.ripn.net.
ru.                     171112  IN      NS      d.dns.ripn.net.
ru.                     171112  IN      NS      e.dns.ripn.net.
ru.                     171112  IN      NS      f.dns.ripn.net.
ru.                     171112  IN      NS      b.dns.ripn.net.

;; ADDITIONAL SECTION:
a.dns.ripn.net.         87341   IN      A       193.232.128.6
a.dns.ripn.net.         87341   IN      AAAA    2001:678:17:0:193:232:128:6
b.dns.ripn.net.         87341   IN      A       194.85.252.62
b.dns.ripn.net.         87341   IN      AAAA    2001:678:16:0:194:85:252:62
d.dns.ripn.net.         87341   IN      A       194.190.124.17
d.dns.ripn.net.         87341   IN      AAAA    2001:678:18:0:194:190:124:17
e.dns.ripn.net.         87341   IN      A       193.232.142.17
e.dns.ripn.net.         87341   IN      AAAA    2001:678:15:0:193:232:142:17
f.dns.ripn.net.         87341   IN      A       193.232.156.17
f.dns.ripn.net.         87341   IN      AAAA    2001:678:14:0:193:232:156:17

;; Query time: 43 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jan 22 15:25:25 YEKT 2016
;; MSG SIZE  rcvd: 606

user@ubunturoute:~$
```

ке
просмотра:
ей
записей, сюда Вы вписываете
просмотра:



```
user@ubunturoute: ~
  GNU nano 2.2.6        Файл: /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

key DHCP_UPDATER {
        algorithm HMAC-MD5.SIG-ALG.REG.INT;
        secret "s5EfpF53BBE9wQtvg9rR7Q==";
};

zone "ordaupfin.local" {
        type master;
        file "/var/lib/bind/db.ordaupfin.local";
        allow-update { key DHCP_UPDATER; };
};

zone "0.168.192.in-addr.arpa" {
        type master;
        file "/var/lib/bind/db.192";
        allow-update { key DHCP_UPDATER; };
};

^G Помощь   ^O Записать ^R Читфайл  ^Y ПредСтр  ^K Вырезать ^C ТекПозиц
^X Выход    ^J Выровнять^W Поиск    ^V СледСтр  ^U ОтмВырезк^T Словарь
```

Зоны прямого просмотра:
Зоны обратного просмотра:
name = ubunturoute.ordaupfin.local;