Настройка кэширующего DNS в Ubuntu

Для начала скачаем и установим сам bind:

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

Останавливаем демон Bind:

```
sudo /etc/init.d/bind9 stop
```

Затем поправим resolv.conf:

```
sudo vim /etc/resolv.conf
```

Приводим к виду:

```
domain mydomen.com
search com
#nameserver 192.168.0.100
#nameserver 192.168.0.99
#nameserver 11.12.13.14
nameserver 127.0.0.1
```

Далее правим named.conf.options:

```
sudo vim /etc/bind/named.conf.options
```

Приводим к виду:

```
options {
 directory "/var/cache/bind";
forward first;
```

```
 forwarders {
192.168.0.100; 11.12.13.14; 192.168.0.99;
};

 // 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 {
 //      0.0.0.0;
 // };

 auth-nxdomain no;    # conform to RFC1035
 listen-on-v6 { any; };
};
```

В целях безопасности рекомендуется запускать Bind в chroot окружении.Так и поступим.Для начала отредактируем bind9:

```
    sudo vim /etc/default/bind9
```

Приводим к виду:

```
    # run resolvconf?
RESOLVCONF=yes

# startup options for the server
OPTIONS="-u bind -t /var/lib/named"
```

Создаем необходимые директории:

```
    sudo mkdir -p /var/lib/named/etc
sudo mkdir /var/lib/named/dev
sudo mkdir -p /var/lib/named/var/cache/bind
sudo mkdir -p /var/lib/named/var/run/bind/run
```

Перенесем файлы конфигов:

```
sudo mv /etc/bind /var/lib/named/etc
```

создаем ссылку:

```
sudo ln -s /var/lib/named/etc/bind /etc/bind
```

создадим необходимые девайсы и права на каталоги:

```
sudo mknod /var/lib/named/dev/null c 1 3
sudo mknod /var/lib/named/dev/random c 1 8
sudo chmod 666 /var/lib/named/dev/null /var/lib/named/dev/random
sudo chown -R bind:bind /var/lib/named/var/*
sudo chown -R bind:bind /var/lib/named/etc/bind
```

редактируем стартовый скрипт демона syslog:

```
sudo vim /etc/init.d/sysklogd
```

Ищем вот этот кусок:

```
....
else
 # By default, run syslogd under the syslog user
 SYSLOGD="${SYSLOGD} -u ${USER}"
fi
....
```

Приводим его к виду:

```
...
 else
 # By default, run syslogd under the syslog user
 SYSLOGD="${SYSLOGD} -u ${USER} -a /var/lib/named/dev/log"
 fi
 ...
```

и перезапускаем syslog:

```
sudo /etc/init.d/sysklogd restart
```

Далее останавливаем демон apparmor:

```
sudo /etc/init.d/apparmor stop
```

Редактируем файл /etc/apparmor.d/usr.sbin.named
который приводится к виду:

```
# vim:syntax=apparmor
# Last Modified: Fri Jun  1 16:43:22 2007
#include <tunables/global>

/usr/sbin/named {
 #include <abstractions/base>
 #include <abstractions/nameservice>

 capability net_bind_service,
 capability setgid,
 capability setuid,
 capability sys_chroot,
 #capability sys_resource,

 # /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,
 /var/lib/named/etc/bind/** r,
 /var/lib/bind/** rw,
 /var/lib/bind/ rw,
 /var/cache/bind/** rw,
 /var/cache/bind/ rw,

 # gssapi
 /etc/krb5.keytab kr,
 /etc/bind/krb5.keytab kr,

 # dnscvsutil package
 /var/lib/dnscvsutil/compiled/** rw,

 /proc/net/if_inet6 r,
 /proc/*/net/if_inet6 r,
 /usr/sbin/named mr,
 #/var/run/bind/run/named.pid w,
 /var/lib/named/var/run/bind/run/named.pid w,
 # support for resolvconf
```

```
 #/var/run/bind/named.options r,
 /var/lib/named/var/run/bind/named.options r,
 /var/lib/named/dev/null rw,
 /var/lib/named/dev/random rw,
 # some people like to put logs in /var/log/named/ instead of having
 # syslog do the heavy lifting.
 /var/log/named/** rw,
 /var/log/named/ rw,
}
```

После внесения изменений демоны apparmor и bind стартуются:

```
    sudo/etc/init.d/apparmor start
sudo/etc/init.d/bind9 start
```

И рестартуем сетевые интерфейсы:

```
    sudo /etc/init.d/networking restart
```

P.S. Не забываем курить логи (cat /var/log/syslog)