Originally the Domain Register took care of any DNS entries relating to the Domain selected - kartbuilding.net

Contents

To setup Bind9 locally:

```
apt-get install bind9
```

This should install and work ok. Note: Firewall rules are required. See Firewall section. In order to start using bind locally, edit /etc/resolv.conf

```
search domainname.com
nameserver 127.0.0.1
```

(The "search domainname.com" allows you to ping/access subdomain names without typing in the entire address. I.E. ping www will ping www.domainname.com)
Restart bind: - /etc/init.d/bind9 restart

Test and ping google etc. Bind should be resolving internet addresses. If not - Check Firewall.

Configing Bind (version 9):

Check to see if the following is referenced in /etc/bind/named.conf

```
include "/etc/bind/named.conf.local"; is in /etc/bind/named.conf
```

Edit the following file:

```
vi /etc/bind/named.conf.local
//This file contains all local and changable info.
//Begin File - by creating the following entry:
//----------- Begin Kartbuilding.net ------------
zone "kartbuilding.net" {
       type master;
       file "/etc/bind/zones/kartbuilding.net.zone";
       allow-transfer { 88.211.211.211; };   ; Note this line is only for a secondary nameserver, al
};

//The next is the reverse DNS entry.
```

```
zone "1.201.136.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/136.201.1.db";
};
//------------ End of kartbuilding.net ----------
```

Create the kartbuilding.net.zone file:

```
vi /etc/bind/zones/kartbuilding.net.zone
//Begin file --------------------------------
$TTL 3h

@       IN      SOA             ns.kartbuilding.net. root.kartbuilding.net. (
                2006120702      ; counter/ Serial    ; in the format YYYYMMDDCC where CC - counter 1
                20m             ; refresh
                15m             ; Retry Interval
                1w              ; Expire
                1h )            ; Negative Cache TTL

        IN      NS      ns.kartbuilding.net.        ; must the name of the name server used to regis
;        IN      NS      ns1.secondary nameserver.  ; A semi-colon is used to comment out lines in b
        IN      MX      10      mail.burkesys.com.

ns      IN      A       136.201.1.250
mail    IN      A       88.198.194.194
wiki    IN      A       88.198.194.194
monitor IN      A       136.201.1.250
www     IN      A       88.198.194.194
@       IN      A       136.201.1.250   ; the @ is for the no www name. E.g. http://kartbuilding.net
www.portal      IN      A       136.201.1.250
//End file ------------------------------------
```

Create Reverse DNS lookup file: This is just for reverse DNS lookups. Reverse DNS entries also have to be made with your ISP - as reverse DNS entries come from them.

```
vi /etc/bind/zones/136.201.1.db
//Start of file -------------------------
@       IN      SOA     kartbuilding.net. root.kartbuilding.net. (
                3       ; counter/ Serial
                15m     ; refresh
                15m     ; Retry Interval
                1w      ; Expire
                1h )    ; Negative Cache TTL

        IN      NS      ns.kartbuilding.net.

250     IN      PTR     servername.kartbuilding.net.
//End of file ---------------------------
```

Start bind and Test:

```
/etc/init.d/bind start
CHECK LOGS::
tail /var/log/daemon.log

Test with dig, nslookup and ping.
To test with nslookup, at the prompt type in "set type=mx" to query mx records. Similiarly, "set typ
Go to http://www.dnsstuff.com and carryout a DNS report.
```

If you don't have bind installed you wont have nslookup and you'll get:

```
-bash: nslookup: command not found
```

To solve this:

```
apt-get install dnsutils
```

Setting up A Secondary DNS

Having a secondary DNS is very important, especially if your services (web,mail,db etc) are running off different boxes. The www could be up, but if DNS goes down - no www traffic :-(

There is **very little** to setting up a secondary dns entry/server. It takes care of everything, e.g. updating etc. from master to slave itself.

Config Master To setup the master (main or primary DNS server) the following must be added:

```
vi /etc/bind/zones/kartbuilding.net.zone
allow-transfer { 88.211.211.211; };
//where the above ip is the secondary dns server's.
```

Config Slave Of course bind will have to be installed and it could be perhaps serving out dns for another domain! Edit the following file:

```
vi /etc/bind/named.conf.local
//add the following lines:

zone "kartbuilding.net" {
        type slave;
        file "/etc/bind/slaves/kartbuilding.net.zone";
        masters { 136.201.1.250; };
        allow-transfer { 136.201.1.250; };
};
```

The /etc/bind/slaves directory must be created, and also bind must be given permission to write to this slaves directory. This is because bind runs as user bind - and can only edit files it owns, or if the directory is chmod'd 775.

```
mkdir /etc/bind/slaves
chown bind:bind /etc/bind/slaves
//I chose to change ownership of this file rather than chmod it 775.
```

The allow-transfer should be included even for the slave zone files, otherwise anyone could do a zone transfer and lookup all your sub domains. See: DNS_-_Bind9#Prevent_DNS_lookup_of_sub_domains

Thats it! Secondary DNS setup. Restart/reload bind on both servers. **Check /var/log/daemon.log for updates'** Check also after the slave updates from the master. The slave will place dns files in /etc/bind/slaves/

bind slave error: permission denied

On a Ubuntu box, I was getting:

```
bind dumping master file: /etc/bind/zones/slaves/: open: permission denied
```

Solution: http://smaftoul.wordpress.com/2009/04/17/ubuntu-and-bind-acting-as-slave/

```
vi /etc/apparmor.d/usr.sbin.named
#add in:
  /etc/bind/zones/slaves/** rw,
```

Slow DNS lookup issues with bind9

If ping or netstat etc. takes a long time to return an ip - there is a problem. Carry out the following test:

```
dig www.burkesys.com
```

Identify the time taken. Try the same test on a different computer (your local one etc.). If it takes 2000+ msec (milliseconds) this is poor. After looking at problems found here: http://www.unixadmintalk.com/f59/bind-9-2-4-1-very-slow-resolving-uncached-querres-129112/index2.html and http://v6fix.net/db/bind9-ipv6-transport.html I realised bind9 was doing a lookup via ipv6. Although ipv6 is enabled in my default debian install, there is no ipv6 network. Bind9 however does a lookup over ipv6 first, then times out and tries ipv4.

Solutions: Disable ipv6 on Debian Sarge, or Disable ipv6 bind lookup, or use a different dns server for lookups.
It is difficult to cleanly disable ipv6 on Sarge, requiring reboot and trial and error.
In order to Disable ipv6 lookup on bind9 with Debian Sarge - a recompile is required. If you are using debian packages (like me) this is not ideal.
The default bind9 that ships with Debian Etch (9.3.2-P1.0-1) can easily be configured to use ipv4 by:

```
vi /etc/default/bind9
OPTIONS="-4 -u bind"
//-4 = to use ipv4 only.
```

As I was using Debian Sarge, and wanted a quick solution to my DNS lookup times, I decided to use my ISP dns server *only* for lookups. This entry is in /etc/resolv.conf and I put the following syntax:

```
search domainname.com
nameserver 43.111.98.12
nameserver 43.111.21.45
```

Bind will still serve out all domain names when requested. The above simply uses the ISP's dns server for lookups on the server.

Solving Problems, Failings and Warnings from DNS report by www.dnsstuff.com

Open DNS servers fail warnings

Typically bind will allow any other server/ip to query it and use it as a DNS server for its queries. Therefore - a foreign server could be doing a dns lookup for hundreds of domains etc. and may overload your dns server! Here is how to solve this:

```
vi /etc/bind/named.conf.options
//put the following as the very first line (note the ip of secondary dns server):
acl recurseallow { 136.201.1.250; 127.0.0.1; 88.211.211.211; };
// at the bottom of the same file put:
        //recursion no;
       allow-recursion { recurseallow; };
```

Debian squeeze by default will only allow localhost and localnets to perform dns lookups. To allow a particular IP or IP range to carry out dns lookups with your dns server, you need to add the following:

```
vi /etc/bind/named.conf.options
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
        //..........
       auth-nxdomain no;    # conform to RFC1035
       listen-on-v6 { any; };
       allow-recursion { ip.address.range/26; 172.20.20.0/24; ip.address; };
};
```

Ref: http://debianserver.wikidot.com/squeeze:intranet-dns-cache

```
#On fedora, its a little different due to how the named options are stored. Here is the config:
vi /etc/named.conf
options {
       pid-file "/var/named/chroot/var/run/named/named.pid";
       directory "/var/named/chroot/var/named";
       auth-nxdomain no;
       //The following it to have a closed DNS Server.
       allow-recursion { localhost; };
};
//
// a caching only nameserver config
//
zone "." {.................
```

Thats it. You now have a closed DNS server.

Old Config Example and Other Information

Make the following file: - /etc/bind/kartbuilding.net

```
    $TTL 3h
    @       IN      SOA     kartbuilding.net. root.kartbuilding.net. (
                         2006100659         ; Serial (A simple Counter to Increment after changing t
                                15m         ; Refresh
                                15m         ; Retry
                                 1w         ; Expire
```

```
                                1h )       ; Default TTL

            NS      ns.kartbuilding.net.
            MX      10 mail.kartbuilding.net.
            A       136.201.1.250

    ;Main domains
    ns  A       136.201.1.250
    wiki        A       136.201.1.250
    mail        A       136.201.1.250
    mrtg        A       136.201.1.250
    www         A       136.201.1.250
    misc        A       136.201.1.250
    lists       A       136.201.1.250

    ;Sub Mail domains
    lists       MX      5 lists
```

To Flush all DNS entries from CACHE ->

```
rndc flush
```

To Efficiently RELOAD DNS after adding a DNS entry ->

```
rndc reload   //use this instead of reloading all of bind
rndc reload domain.com   //use this to reload just the domain.com config file
```

Prevent DNS lookup of sub domains

The "host" utility, which is default with debian, will attempt to perform a zone transfer in order to look at all of the sub domains! The syntax is:

```
host -l domain.com ip.of.their.ns.server
#to find all of the authorative ns servers do the following:
nslookup
> set type=ns
> domain.com
```

Another tool to do domain lookups is:

```
dig -t axfr
```

Typically it is an oversight which allows the above, especially on secondary ns's. The following line needs to be added to the slave dns entries:

```
vi /etc/bind/named.conf.local
#add the following for each slave zone, including the master ip address for example.
allow-transfer { some.ip.address.of.yours.eg.master.ns; };
```

DNS - Config Used: http://www.debian.org/doc/manuals/network-administrator/ch-bind.html

DNS - Basic Config: http://www.debian-administration.org/articles/206#comment_8

DNS - Linux DNS Server VIDEO TUTORIAL - Explains all pieces: http://www.cbt4free.org/videos.php