

Bind Configuration

While some people may have some concerns about it, BIND is the defacto standard for Internet DNS serving. Although it's config files may look confusing at first, a little experience shows you that it is actually complex, and there's nothing you can do about it. However, most people won't have to deal with anything that hard to use. So here's a little article on a quick and dirty start to Bind.

Basically, configuring BIND required 3 parts:

- The Invocation - How do you start it, and what parameters do you send it?
 - The /etc/named.conf file - This controls how bind responds to queries
 - The Zone Files - This is the info it should be handing out
- Easy enough. Let's begin. Starting Bind

The Bind daemon is called "named", following standard *NIX conventions of a short, mildly descriptive name, followed by a "d" to denote that it is a daemon, or a background process. In RedHat, or most RPM based distributions, you'll find bind being started by the /etc/init.d/named script. This script has some parameters that are contained in /etc/sysconfig/named. By default, the file has this information in it: # Currently, you can use the following options:

```
# ROOTDIR="/some/where" -- will run named in a chroot environment.
#           you must set up the chroot environment before
#           doing this.
# OPTIONS="whatever" -- These additional options will be passed to named
#           at startup. Don't add -t here, use ROOTDIR instead.
ROOTDIR=/var/named/chroot
```

What this is telling you, is that 1] it's running in a chroot'ed environmet and 2] the files are located in /var/named/chroot. Using chroot you limit your exposure to damage should the process become compromised by an external attacker. If someone did get in, and the software is written correctly, and there are no malicious or exploitable programs in the chroot jail, and there are no kernel hax available, the attacker can only play in a really, really small sandbox.

Other *NIX distros will have their own special way of invoking bind (svcadm on Solaris, /etc/rc.something on legacy distros using the old BSD boot process), but you can usually find out how it's being started by doing a # ps -ef | grep named

```
named 15286 1 0 Aug07 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

So here you can tell that bind is running as user "named" and that it wants to be chrooted to /var/named/chroot. Keep this in mind. The Config File

Generally called /etc/named.conf, the config file has all your master config info that bind might need after starting. This is mostly things like, "Who am I answering DNS requests for?", "Where is the data I'm supplying located?", "What zones do I know about?", "Am I the master for any of them?". So here's the thing... we're running in a chrooted jail, so doesn't bind need this file after it starts? The answer is "Yes" it does, so clearly, it needs to be in the jail. In RedHat, this is exactly what happens:

```
[root@admin01 etc]# ls -l named.conf
lrwxrwxrwx 1 root root 32 May 31 2005 named.conf ->
/var/named/chroot/etc/named.conf
```

So, the file is conveniently located in /etc for most of us who've been using it long before it ever had the chroot feature built in, but in reality, the actual file is in /var/named/chroot/etc, where the running version can get a hold of it. This will rarely be a concern, though, since the distribution maker has already handled all those details for you. Just remember not to overwrite the symbolic link or things will not work correctly.

Let's take a look at the beginings of the file:

```
options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    /*
    * If there is a firewall between you and nameservers you want
    * to talk to, you might need to uncomment the query-source
    * directive below. Previous versions of BIND always asked
    * questions using port 53, but BIND 8.1 uses an unprivileged
    * port by default.
    */
    // query-source address * port 53;
    allow-recursion { localnets; };
    forward first;
```

```

forwarders {
    x.x.x.x;
    z.z.z.z;
};
allow-transfer { y.y.y.y; };

```

The first 3 lines give you the basics. Where to find the files it needs for data, and where to keep temp data. The allow-recursion string tells it that, by default, only allow queries about stuff it doesn't directly know about to hosts that are on networks local to the host it's on. forward first tells Bind to first try its list of forwarders for recursive queries. The forwarders list contains the list of other name servers to try for recursive queries. The allow transfer line tells Bind who's allowed to do wholesale zone transfers; you usually list all your secondary/slave name servers here.

There are many parameters available for Bind configuration. You'll rarely need any others, but I'll list a few at the end.

```

Now, let's get to the good part. Adding a zone. This is an example for a zone that this server is the master for.
zone "enfoldit.com" {
    type master;
    file "enfoldit.com.zone";
};

```

That's it. This tells bind to look for the file "enfoldit.com.zone" in the data directory (defined above as /var/named) for zone information for "enfoldit.com".

```

If this is not the primary DNS server, but a duplicate of it, you'll need a slave zone:
zone "enfoldit.com" {
    type slave;
    masters { 217.160.241.30; };
    file "slaves/enfoldit.com.zone";
};

```

This tells it to grab the data from 217.160.241.30, and drop that data in the data directory as "slaves/enfoldit.com.zone". The master server will need to allow this server to do the transfer since it's disabled by default. You do this by putting an allow transfer clause in the master options, or in the zone definition. The Zone File

First thing, if you're running chroot, you'll need to put your files in the chroot directory tree, not in /var/named directly. You can't put the files in /var/named, and then symlink them to the chroot dir. Most people will, however, symlink the files in the chroot dir to /var/named so they don't forget where they went. an example: # touch /var/named/chroot/var/named/enfoldit.com.zone # cd /var/named # ln -s chroot/var/named/enfoldit.com.zone

```

Now, with that out of the way, your basic zone file:; First we specify how long all the records get Cached for
; Here we're doing it for an hour. You shouldn't go lower
; than about 15 minutes
$TTL 1h

```

```

; Next, we have the Start of Authority Record which
; gives the DNS servers info about who's hosting
; and how often the check for updates
; The '@' means "whichever zone we're being used for"

```

```

@ IN SOA enfoldit.com. email.enfoldit.com. (
    2006050200 ; Serial
    1d ; Refresh
    2h ; Retry
    1d ; Expire
    1h ) ; Minimum

```

```

; Over here we have more info for the '@' domain
; You can be explicit and put the machine name before each
; entry, but most people do not

```

```

    IN NS dns1.enfoldit.com.
    IN NS dns2.enfoldit.com.
    IN MX 10 mail.enfoldit.com. IN A 217.160.241.30
; 'www.enfoldit.com' is defined as being the same as
; 'enfoldit.com'
www IN CNAME enfoldit.com.

```

```
; 'dns1.enfoldit.com' is defined as being at 217.160.241.30
dns1      IN  A   217.160.241.30
; 'dns2.enfoldit.com' is defined as being at 217.160.241.30
; note that the name is spelled out here, rather than
; just doing the relative path thing.
dns2.enfoldit.com. IN  A   217.160.241.30
```

A little confusing at first, but really not too much of a big deal. First thing you need to know is that: Absolute domain names end in a '.'; Relative ones do not.

Quick note here... many times you'll see a file with "\$ORIGIN something.com." in it. "\$ORIGIN" states that all entries in the file going forward will be relative to the parameter. Now, by default, all entries in a zone file are set with an implicit \$ORIGIN to whatever zone they are for, which is why we didn't need to specify a complete name every time. When Bind writes out zone files (for instance, if you have DNS dynamic updates turned on and people register with your system), it will use the \$ORIGIN far more often than humans will use. Be aware. The up shot of all this, if you've got a CNAME or another record pointing to a completely different domain, the definition better end a '.:www IN CNAME www.othersite.org.

```
ns1      IN  NS   ns1.afonsoconsulting.com.
```

If it doesn't, then you'll be going to www.othersite.org.whatever.domain.com. SOA Record

Let's take a look at the section for "enfoldit.com". Now, Bind will replace the "@" with the name of the zone it's looking for. so the first entry can be re-written as: enfoldit.com. IN SOA enfoldit.com. email.enfoldit.com. (

```
2006050200 ; Serial.
1d         ; Refresh.
2h         ; Retry.
3d         ; Expire.
1h )      ; Minimum.
```

So, the SOA record here tells us that for enfoldit.com, this record is authoritative for "enfoldit.com", and that the admin is email@enfoldit.com. Slaves will update themselves once a day, and retry every 2 hours up to 3 days more in case the transfer fails. Default TTL that should be allowed is 1 hour (although this setting is usually ignored since \$TTL is the first thing defined in the file). The serial number is important in that it needs to get bigger everytime the file changes so that slave servers see a newer version, and therefore instigate a new zone transfer. NS Records

Next, you'll want to define NS records. These tell the DNS system who are the authoritative name servers for that domain. Nothing special here, just supply the DNS names of your name servers. If they are your own servers, specify the names here and make sure to define the A records for them later on in the file. Don't use CNAMEs for these entries. MX Records

The MX records specify who gets your domain's e-mail. the format is: @ IN MX 10 mail

```
^      ^ ^ ^ ^ ^
```

```
|      | | | + Host name of your mail server
|      | | | + The server's Cost (lower is preferred)
|      | | + Mail server record
|      | + Internet Record
+ The DNS name this mail record is for
```

Only thing of note here is to have an MX record for each mail server you have. Again, this points to a DNS name, so you may need to define an A record later in the file. It's not recommended to point it to a CNAME here. Also, if you have subdomains, or even individual hosts, you can point them to their own mail servers by adding their own MX records. A

```
Recordshostname IN A 192.168.0.1
                IN A 192.168.0.2
```

Here's an example of a host called 'hostname' that has 2 different IP Addresses. Really, no rocket science here. Reverse DNS

So now we can go from domain name to IP address. Great. What about the other way around?

This is called reverse DNS, and it's accomplished through special zone names. Say you want to do RDNS for 192.168.2.1. The DNS subsystem does a query for PTR records for the address "1.2.168.192.in-addr.arpa". How do you set this up? Just create it as a zone. So your named.conf file will contain: zone "2.168.192.IN-ADDR.ARPA" {

```
type master;
file "2.168.192.in-addr.arpa.zone";
};
```

And your /var/named/chroot/var/named/2.168.192.in-addr.arpa.zone file will have:\$TTL 3600

```
@ IN SOA 2.168.129.IN-ADDR.ARPA. email.enfoldit.local. (
    2002042301 ; Serial
    86400 ; Refresh
    14400 ; Retry
    86400 ; Expire
    86400 ) ; Minimum
@ IN NS ns1.enfoldit.com.
@ IN NS ns2.enfoldit.com.
```

```
1 IN PTR gateway.enfoldit.local.
2 IN PTR dansmom.enfoldit.local.
```

Same SOA structure (no MX or A records since that's not needed). The PTR records just state the domain name for a given IP address. Again, since the file is relative by default, you just need to put in the numbers, and then define the PTR record, however, the PTR lines could be re-written as:1.2.168.192.in-addr.arpa. IN PTR gateway.enfoldit.com.

should you wish.

Now, here's the catch: If someone has 2 clients, one with an address space at x.x.x.0-127 and another at x.x.x.128-255, how would they each get thier own RDNS service? Answer: Not without a lot of annoyance. You see, you can't get more fine grained using this system than the bocks of 255 addresses since that's where the periods go in normal IP Addresses. so, not fun. A detailed guide is available here, and explains what you need to go through to make it all work.Putting it all together

Assuming Bind was working outof the box, it's running, and you haven't messed up the zone files or config file too much, you should be able to use "rndc reload" to load everything. Test it by doing a few queries:[root /var/named]# dig

```
@yournameserver.net enfoldit.com; <<>> DiG 9.2.4 <<>> @yournameserver.net enfoldit.com
```

```
;; global options: printcmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40495
```

```
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0;; QUESTION SECTION:
```

```
;enfoldit.com. IN A;; ANSWER SECTION:
```

```
enfoldit.com. 3600 IN A 217.160.241.30;; AUTHORITY SECTION:
```

```
enfoldit.com. 3600 IN NS park19.secureserver.net.
```

```
enfoldit.com. 3600 IN NS park20.secureserver.net.;; Query time: 24 msec
```

```
;; SERVER: 68.178.211.114#53(park20.secureserver.net)
```

```
;; WHEN: Wed Aug 9 07:25:30 2006
```

```
;; MSG SIZE rcvd: 103
```

```
[root /var/named]# dig @yournameserver.net enfoldit.com MX; <<>> DiG 9.2.4 <<>> @yournameserver.net enfoldit.com
MX
```

```
;; global options: printcmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19959
```

```
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0;; QUESTION SECTION:
```

```
;enfoldit.com. IN MX;; ANSWER SECTION:
```

```
enfoldit.com. 3600 IN MX 0 mail.enfoldit.com.;; AUTHORITY SECTION:
```

```
enfoldit.com. 3600 IN NS park19.secureserver.net.
```

```
enfoldit.com. 3600 IN NS park20.secureserver.net.;; Query time: 18 msec
```

```
;; SERVER: 68.178.211.114#53(park20.secureserver.net)
```

```
;; WHEN: Wed Aug 9 07:26:27 2006
```

```
;; MSG SIZE rcvd: 144Links
```

```
- Bind Homepage: http://www.isc.org/sw/bind/
```

```
- SOA record info: http://support.microsoft.com/?kbid=163971
```

```
- Reverse Zone information: http://www.apnic.net/db/revdel.html
```

```
- O'Reilly Book on DNS: At Amazon
```