How to setup a LAN DNS server using Bind9 under Debian Etch and Ubuntu 8.04

Submitted by Richard on Sat, 07/05/2008 - 00:41

This is a step by step tutorial on how to install and configure DNS server for your LAN using bind9. The DNS server will provide caching and name resolution as well as reverse name resolution for your local network. In this tutorial, we will use the domain "debian.lan" and this will be the domain of your local network. The domain "debian.lan is not accessible from the internet; its private ip address is "192.168.100.1".

Installing bind9 and dns utilities

I assume that you already have a working Debian Etch or Ubuntu 8.04 installation. Lets install the bind9 package and dns utilities from Debian repository.

```
apt-get install bind9 dnsutils
```

Configure your Linux system

Add this information to your */etc/hostname*

```
echo "main.debian.lan" > /etc/hostname
```

Edit your */etc/hosts*

```
127.0.0.1       localhost.localdomain   localhost
192.168.100.1   main.debian.lan main
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Edit your */etc/resolv.conf*

```
vi /etc/resolv.conf
```

and add this information.

```
search debian.lan
nameserver 127.0.0.1
nameserver 192.168.100.1
```

About Me

I'm a network and system administrator. I have a strong interest in Technology, Linux, Open Source and Photography. I spend my spare time hacking on my system, blogging, learning new stuff to improve my knowledge and to help me in my day to day activities. I also love travelling, playing tennis and watching movies.

More...

Subscribe to Feeds

87 readers BY FEEDBURNER

Enter your email address:

Subscribe

Delivered by FeedBurner

Categories

```
nameserver xxx.xxx.xxx.xxx
nameserver xxx.xxx.xxx.xxx
```

This is where Linux looks to find out how it should perform DNS lookups.

Lets create a zone

The zone files (or database files) are the heart of your BIND system. This is where all the information is stored on what hostname goes with what ip address.
Before we create a zone file, lets edit first the local configuration file */etc/bind/named.conf.local*.

```
vi /etc/bind/named.conf.local
```

and the zone file data.

```
//
// Do any local configuration here
//

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

zone "debian.lan" {
        type master;
        file "db.debian.lan";
};

zone "100.168.192.in-addr.arpa" {
        type master;
        file "db.192.168.100";
};
```

Lets start creating a zone file in */var/cache/bind/* directory. Create a file called db.debian.lan

```
vi /var/cache/bind/db.debian.lan
```

And add the following entry

```
$TTL 604800
@ IN SOA main.debian.lan. admin.debian.lan. (
                2008080101      ;serial
                04800           ;refresh
                86400           ;retry
                2419200         ;expire
                604800          ;negative cache TTL
                )
@       IN      NS      main.debian.lan.
@       IN      A       192.168.100.1
@       IN      MX      10      main.debian.lan.
main    IN      A       192.168.100.1
www     IN      CNAME   main
ubuntu  IN      A       192.168.100.2
```

Lets create the reverse DNS zone file called *db.192.168.100*

```
vi /var/cache/bind/db.192.168.100
```

and the the following entry.

```
$TTL 604800
@ IN SOA main.debian.lan. admin.debian.lan. (
                2008080101      ;serial
                604800          ;refresh
                86400           ;retry
                2419200         ;expire
                604800          ;negative cache TTL
                )
@       IN      NS      main.debian.lan.
@       IN      A       192.168.100.1
1       IN      PTR     main.debian.lan.
2       IN      PTR     ubuntu.debian.lan.
```

The zone files are created, you can check your zone file configurations using these utilities:

```
named-checkzone main.debian.lan /var/cache/bind/db.debian.lan
named-checkconf /etc/bind/named.conf.local
```

Lets edit the file */etc/bind/named.conf.options*

```
vi /etc/bind/named.conf.options
```

Uncomment the line *forwarders* and add your ISP's DNS server.

```
forwarders {
                202.78.97.41;
                202.78.97.3;
        };
```

Lets restart our DNS server, and test using the tool *dig*.

```
/etc/init.d/bind9 restart
dig debian.lan
```

You should see the following message

```
; <<>> DiG 9.3.4 <<>> debian.lan
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54950
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIO

;; QUESTION SECTION:
;debian.lan.                    IN      A

;; ANSWER SECTION:
debian.lan.             64800   IN      A       192.168.100.1

;; AUTHORITY SECTION:
debian.lan.             64800   IN      NS      main.debian.lan.

;; ADDITIONAL SECTION:
main.debian.lan.        64800   IN      A       192.168.100.1

;; Query time: 1 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
;; WHEN: Tue Aug  5 09:33:40 2008
;; MSG SIZE  rcvd: 79
```

Test your reverse DNS

```
dig -x debian.lan
```

If you see this message, you have successfully installed the DNS server.

```
; <<>> DiG 9.3.4 <<>> -x debian.lan
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42510
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL

;; QUESTION SECTION:
;lan.debian.in-addr.arpa.       IN      PTR

;; AUTHORITY SECTION:
in-addr.arpa.           10800   IN      SOA     A.ROOT-SERVERS.NE

;; Query time: 952 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
;; WHEN: Tue Aug  5 09:34:25 2008
;; MSG SIZE  rcvd: 108
```

You can also check your DNS *nslookup* and *host* command.

```
nslookup debian.lan
nslookup 192.168.100.1
```

```
host debian.lan
host 192.168.0.1
```

All computers in the LAN are going to use 192.168.100.1 as a nameserver, this can be set manually by setting statically:

```
vi /etc/resolv.conf
```

then put this information.

```
nameserver 192.168.100.1
```

Have fun!
Sources:
http://www.debian.org/doc/manuals/network-administrator/ch-bind.html
http://www.aboutdebian.com/dns.htm

Bind Debian DNS Howtos Linux Ubuntu

Printer-friendly version ShareThis PDF version

Similar By Terms

How to Setup DHCP Server with Dynamic DNS using Bind9 in Debian Etch and Ubuntu 8.04
How to Set Up Apache 2 Name-based Virtual Host on Debian Etch and Ubuntu 8.04
How to install minicom in Debian or Ubuntu to configure Cisco switches and routers through the console port
How to Create Self-signed SSL Certifcate using OpenSSL in Debian Etch and Ubuntu 8.04
How to Configure Apache to Password Protect your Web Directory
How to Install Asterisk 1.4 and Asterisk GUI in Ubuntu 6.06 LTS Server and Debian Etch
How to Configure your Debian Etch or Ubuntu 8.04 box as an Internet Gateway/Router using IP Masquerading

Links

Red Hat
CentOS
Fedora Project
Fedora Forum
Fedora Solved
Planet Fedora
Planet CentOS
The Open Source Way
OpenSource.com
Linux.com
PacketLife
Rich 'n Ritch - Serendipity Seekers

Monthly archive

April 2014 (3)
March 2013 (2)
August 2011 (2)
July 2011 (2)
March 2011 (2)
October 2010 (2)
September 2010 (1)
August 2010 (5)
July 2010 (7)
March 2010 (1)
February 2010 (3)
November 2009 (3)
more

Recent Articles

How to reset Cisco 2960 switch password without losing your configuration
How to reset Cisco 2960 switch to default settings
How to install minicom in Fedora 20 to configure Cisco switches and routers through the console port
50 Best Free and High Quality Games available on Fedora
It's been a long time since my last post but now I'm back again
How to install World of Padman in Fedora 14
How to install Urban Terror in Fedora 14
Play DotA clone Heroes of Newerth on Linux Natively For Free
100 Best Free and High Quality Linux Games
How to install Oracle Java Runtime Environment in Fedora 14 (64-bit)
more

Recent Docs

How to create wifi Hotspot system using Chillispot, Freeradius 2 and Fedora 12
Debian Etch Gateway with Layer7 and IPP2P for P2P Blocking