

Student L8A1

In this activity, you will be setting up DNS records using BIND9 on a Linux Ubuntu Server. The guide will take you through the basic setup. This tutorial uses “example.com” as the Fully Qualified Domain Name (FQDN). Make sure to change “example.com” to your FQDN any time you see it in the tutorial in files or filenames.

A sample DNS Zone file can be found here.

Primary Master Server configuration:

In this, BIND9 will be configured as the primary master for the domain **example.com**. Simply replace *example.com* with your fully qualified domain name.

Zone File

1. To add a DNS zone to BIND9, turning BIND9 into a Primary Master server, all you have to do is edit **/etc/bind/named.conf.local**:

```
[...]  
  
zone "example.com" {  
  
    type master;  
  
    file "/etc/bind/db.example.com";  
  
};  
  
[...]
```

2. Now use an existing zone file as a template:

Type the command: `sudo cp /etc/bind/db.local /etc/bind/db.example.com`

Edit the new zone file **/etc/bind/db.example.com** change localhost. to the FQDN of your server, leaving the additional "." at the end. Change 127.0.0.1 to the nameserver's IP

Address and root.localhost to a valid email address, but with a “.” instead of the “@”. also leaving the “.” at the end.

3. Also, create an **A record** for *example.com* the name server in this example:

```
;  
; BIND data file for local loopback interface  
;  
$TTL 604800  
@ IN SOA ns.example.com. root.example.com. (  
1 ; Serial  
604800 ; Refresh  
86400 ; Retry  
2419200 ; Expire  
604800 ) ; Negative Cache TTL  
;  
@ IN NS ns.example.com.  
ns IN A 192.168.1.10  
;also list other computers  
box IN A 192.168.1.21
```

NOTE: You must increment the serial number every time you make changes to the zone file. If you make multiple changes before restarting BIND9, simply increment the serial once.

Now, you can add DNS records to the bottom of the zone.

Tip: Many people like to use the last date edited as the serial of a zone, such as 2005010100 which is *yyyymmddss* (where *s* is serial)

4. Once you've made a change to the zone file BIND9 will need to be restarted for the changes to

take effect:

Type the command: `sudo /etc/init.d/bind9 restart`

Reverse Zone File:

Now that the zone file is setup and resolving names to IP Addresses a Reverse zone is also required. A Reverse zone allows DNS to convert from an address to a name.

5. Edit `/etc/bind/named.conf.local` and add the following:

```
zone "1.168.192.in-addr.arpa" {  
  
    type master;  
  
    notify no;  
  
    file "/etc/bind/db.192";  
  
};
```

Note: replace **1.168.192** with the first three octets of whatever private network you are using. Also, name the zone file **db.192** in the example appropriately.

6. Now create the 192 file:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

7. Next edit `/etc/bind/db.192` changing basically the same options as in `/etc/bind/db.example.com`:

```
;  
  
; BIND reverse data file for local loopback interface  
  
;  
  
$TTL 604800  
  
@ IN SOA ns.example.com. root.example.com. (  
  
2 ; Serial
```

```
604800      ; Refresh
86400       ; Retry
2419200     ; Expire
604800 )    ; Negative Cache TTL
;
@           IN      NS      ns.
10         IN      PTR     ns.example.com.
; also list other computers
21         IN      PTR     box.example.com.
```

NOTE: The serial number in the reverse zone needs to be incremented on each changes as well. For each **A record** you configure in `/etc/bind/db.example.com` you need to create a **PTR record** in `/etc/bind/db.192`.

8. After creating the reverse zone file restart **bind9**:

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

Testing

You should now be able to ping **example.com** and have it resolve to the host configured above:

```
ping example.com
```

You can also use the **named-checkzone** utility that is part of the **bind9** package:

```
named-checkzone example.com /etc/bind/db.example.com
```

and

```
named-checkzone 1.168.192.in-addr.arpa. /etc/bind/db.192
```

This is a great way to make sure you haven't made any mistakes before restarting **bind9**.

You can use the **dig** utility to test the reverse zone as well as the new domain name:

```
dig 1.168.192.in-addr.arpa. AXFR
```

You should see output resolving *1.168.192.in-addr.arpa*. to your nameserver.

Copyright © 1995-2015, Iowa State University of Science and Technology. All rights reserved.