Lab Exercise 3 – Authoritative DNS Servers

Objectives:
Participants should be able to configure primary and secondary name server for a given domain name and do a zone transfer between them. This includes creating, modifying, deleting records and incrementing the Primary name server serial number. Each participant name servers should be visible from other name servers. We have a lab root and GTLD server setup. A custom lab root hint will be used.

Background:
An authoritative DNS server provides authoritative answer to DNS queries.

What You Need
Linux Server with BIND already installed (finished Lab 1). Optionally finished Lab 2.

Note:
Configure your server to be the primary (also called master) of your own domain and also a slave for servers on your right side. The server on your left will act as secondary (also called slave) for your own domain.

Steps:

1. Register your domain name and its name server's FQDN (master & slave) together with their IP addresses to the domain name registry. In our lab you should approach the instructor for registration. Instructor will also act as a GTLD server for this exercise. He will be creating the delegation of .net subdomains to every server in the lab.

2. Create a new working directory for your primary server under /var/named

```
mkdir /var/named/master
cd /var/named/master
```

3. Create a zone file for your domain under /var/named/master and add the necessary resource records like NS, A, TXT, and MX records that will determine which host is receiving mail for your domain.

```
nano /var/named/master/db.myzone.net
```

For example, if you have myzone.net as your domain, you must create db.myzone.net, with the following base contents:

```
$TTL 1d
@           SOA    NS.MYZONE.NET.  email.myzone.net.    (
                   2019111801 ;serial no.
                   30m        ;refresh
                   15m        ;retry
                   1d         ;expire
                   30m        ;negative cache ttl
                  );

                NS    ns.myzone.net.
```

```
ns          A     10.0.X.53

www         A     10.0.X.100

myzone.net.       MX 10       mail01.myzone.net.
                  MX 20       mail02.myzone.net.

mail01      A     10.0.X.200
mail02      A     10.0.X.201
```

4. Create the configuration file (named.conf). Please note that the primary zone is of "type master" while a secondary zone is of "type slave." Specify your nameserver's working directory.

   ```
   nano /etc/named.conf
   ```

   Add the following content:

   ```
   options {
      directory "/var/named/master";
      };

   zone "myzone.net" {
      type master;
      file "db.myzone.net";
      };
   ```

   Most authoritative servers are also recursive/caching servers for their own networks. If this is the case, also add the zones defined in the recursive named.conf.

   ```
    zone "." {
         type hint;
         file "root.hints";
    };


    zone "localhost" {
            type master;
            file "db.localhost";
     };
   ```

   In the lab, we will use a custom hints file. Please make sure you have a copy of this in /var/named/master folder. For reference, the content should be as follows:

   ```
   vi /var/named/master/root.hints

   .                        3600000      NS    NS.ROOT-SERVERS.NET.
   NS.ROOT-SERVERS.NET.     3600000      A     10.0.100.53
   ```

5. In /var/named/master, run Bind and see if it's running properly. Error messages will give you hints where the error is.

```
cd /var/named/master
named -g -c named.conf
```

If using /etc/named.conf, you can remove the -c option.

```
named -g
```

6. Once BIND is running, you can do some basic test using DNS tools like "dig"

To test your name server to display the SOA records for your domain.

```
dig @10.0.x.53 myzone.net SOA
```

To test your name server to display NS records

```
dig @10.0.x.53 myzone.net NS
```

To test your name server to display other resource records (A, MX, or TXT). You can also use the -t option to set the query type.

```
dig @10.0.x.53 ns1.myzone.net A

dig –t MX @10.0.x.53 myzone.net
```

Stop here for now until the instructor tells you.

Now let's setup a secondary server for your domain. Ask the group behind you to be your secondary. This means that your dns server will be master, and the dns server of the group behind will be secondary..

7. On the *primary server*, open the zone file and add the slave nameserver to be authoritative for your domain.

```
$TTL 1d
@      SOA   NS.MYZONE.NET.  email.myzone.net.   (
                    2019111801 ;serial no.
                    30m        ;refresh
                    15m        ;retry
                    1d         ;expire
                    30m        ;negative cache ttl
);

              NS    ns.myzone.net.
              NS    ns.neighbour-domain.net.

ns            A     10.0.11.53
```

Notice that you don't have to add an A record for this, because it is not part of your zone.

8. On the *secondary server*, add a new zone and add the domain of the master. In your named.conf, add the following:

```
vi named.conf
zone "neighbour-domain.net" {
      type slave;
      file "db.neighbour-domain.net";
      masters { ip-of-primary-server;
            };
      };
```

For both *primary* and *secondary*, run your DNS servers. Test that you can perform zone transfer.

```
named -g -c named.conf
```

Check the logs if zone transfer starts and is successful.

From the secondary, check that the file has been successfully copied locally.

```
cd /var/named/master
ls -al
```

9. From any DNS server, check that you can do zone transfer using dig command.

```
dig @<ip-address> ANOTHER-ZONE.NET AXFR
```

10. Switch roles then repeat steps 7-10. The group in front will be secondary for the group behind them.

Stop here for now until the instructor tells you.

11. We will now secure your zones by restricting who can get the zone file.

To do this, add the following lines in your named.conf for the zones where you are primary:

```
zone "myzone.net" {
      type master;
      file "db.myzone.net";
      allow-transfer { ip-of-secondary-server;
            };
};
```

12. Execute the same dig command again. If successful, the status in the dig output should say ***Transfer Failed***.

```
dig @<ip-address> ANOTHER-ZONE.NET AXFR
```

The complete named.conf for an authoritative+recursive server is as follows:

```
// NAMED.CONF
// global configuration
options {
      directory “/var/named/master”;
};

// root-hints
zone “.” {
      type hint;
      file “root.hints”;
};

// primary zones
zone “myzone.net” {
type master;
file “db.myzone.net”;
allow-transfer { ip-of-secondary-server;
    };
};

// secondary zones
zone “neighbour-zone.net” {
type slave;
file “db.neighbour-zone.net”;
masters { ip-of-primary-server;
      };
};

// recursive name server config
zone "localhost" {
        type master;
        file "db.localhost";
        };

zone “0.0.127.in-addr.arpa” {
      type master;
      file db.127.0.0;
};

zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.
arpa" {
        type master;
        file "db.ip6";
};
```