Lab Exercise 3 – Authoritative DNS Servers (Forwarding Zone Configuration)

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 should include creating, modifying, deleting RRs and incrementing Primary name server serial number. Each participant name servers should be visible from other name servers since we will use the lab root and GTLD server. A custom lab root hint will be used.

*Note: Configure your PC to be the primary (also called master) of your own domain and also a slave for PCs in your right side. PC in your left will act as 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 pc in the lab.

2. We need to edit our root hints file, as we are not one of the root server.
   edit the `/etc/bind/named.conf.default-zones` file and comment out the existing root hints, and add our lab root hints

   ```
   //zone "." {
   //        type hint;
   //        file "/etc/bind/db.root";
   //};
   zone "." {
       type hint;
       file "/etc/bind/lab.root";
   };
   ```

3. We now need to create a new file `/etc/bind/lab.root` with the following information:

   ```
   .                       3600000      NS    x.root-servers.net.
   x.root-servers.net.     3600000      A     10.0.50.1
   ```

   We will also need to make sure our file permissions are correct

   ```
   chown -R bind:bind /etc/bind
   ```

We also need to change some of our network settings. We can do this by editing our `/etc/netplan/10-lxc.yaml` file to include our localhost(127.0.0.1) in the dns resolvers list

```
--- snip ----
nameservers:
    search: [local]
    addresses: [127.0.0.1, 8.8.8.8, 8.8.4.4]
--- snip ---
```

Then execute `sudo netplan apply`

4. Create a new working directory for your master server under `/etc/bind`

```
cd /etc/bind
sudo mkdir zones
```

5. Create a zone file for your domain and add necessary resource records like NS record, A record, txt record, MX record that will determine which host is receiving mail for your domain.

   This lab has two TLDs, `com` and `net`. Hence, you can only choose between this two to create your 2nd level domain. In real world, you will find many more TLDs.

   For example, in this lab, if you have `groupXX.net` as your domain, you must create `db.groupXX.net`, with the following base contents:

```
$TTL 1d
@   SOA     ns.groupXX.net. email.groupXX.net.   (
            2022040601  ;serial no.
            30m     ;refresh
            15m     ;retry
            1d          ;expire
            30m     ;negative cache ttl
            )

@       IN  NS   ns.groupXX.net.

ns      IN  A       10.0.XX.1
ns      IN  AAAA    2001:db8:XX::1

www     IN  A       10.0.XX.2
www     IN  AAAA    2001:db8:XX::2

mail01  IN  A       10.0.XX.200
mail01  IN  AAAA    2001:db8:XX::200
mail02  IN  A       10.0.XX.201
mail02  IN  AAAA    2001:db8:XX::201

groupXX.net.    MX 10   mail01.groupXX.net.
```

```
groupXX.net.    MX 20   mail02.groupXX.net.

groupXX.net.    IN  TXT "groupXX Authoritative DNS Server"
```

6. Add the zone to the configuration file (`named.conf.local`). Please note that the primary zone is of "type master" while a secondary zone is of "type slave."

```
zone "groupXX.net" {
    type master;
    file "/etc/bind/zones/db.groupXX.net";
};
```

7. Change the owner to `bind` for the files in `/etc/bind/zones`

```
sudo chown -R bind:bind /etc/bind/zones
```

8. Check for any syntax errors in the config files or in the zone files.

```
named-checkconf
named-checkzone groupXX.net /etc/bind/zones
```

9. Try running bind with -g and -c named.conf and see if BIND complains for errors. Use either:

```
sudo systemctl restart bind9
```

or

```
named -g -c named.conf -u bind
```

or

```
rndc reconfig
```

10. There are couple of commands to check BIND service and logs:

```
sudo systemctl status bind9
```

or

```
sudo tail -f /var/log/syslog
```

or

```
rndc status
```

11. 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.XX.1 groupXX.net SOA
    ```

    To test your name server to display NS records

    ```
    dig @10.0.XX.1 groupXX.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.XX.1 ns.groupXX.net A
    dig -t MX @10.0.XX.1 groupXX.net
    ```

12. Setup your server as the secondary server for your neighbour.

    In your `named.conf.local`, add the following (groupYY.net is the neighbour zone):

    ```
    zone "groupYY.net" {
        type slave;
        file "/etc/bind/zones/db.groupYY.net";
        masters { 10.0.YY.1; 2001:db8:YY::1;
        };
    };
    ```

13. Secure your zones by restricting who can get the zone file.
    You can test this by trying zone transfer from another nameserver in the lab.

    ```
    dig @localhost groupYY.net AXFR
    ```

If successful, you will see all the resource records as an output.

Now, add the following line in your `named.conf.local` for the zones where you are primary:

```
zone "groupXX.net" {
    type master;
    file "db.groupXX.net";
    allow-transfer { 10.0.YY.1; 2001:db8:YY::1;
    };
};
```

Execute the same dig command again. If NOT successful, the status in the dig output should say Transfer Failed.

14. You can make `groupYY.net` (the secondary/slave server) as authorative server. For that add another NS record in the `db.groupXX.net` file:

```
$TTL 1d
@   SOA     ns.groupXX.net. email.groupXX.net.   (
          2016010101 ;serial no.

<config sniff..........>

            IN  NS   ns.groupXX.net.
            IN  NS   ns.groupYY.net.

<config sniff.........>
```

Lab Exercise 3 – Authoritative DNS Servers Created: 06 Apr 2022 Version 3.1