DNS – Bind9 manager

1. Introduction

The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
In this Lab, you will set up a DNS service consisting of a primary server. Then you will study more closely how it works

2. Install Bind9 package

You install your DNS server on your gateway Virtual machine. Be sûr that your machine has a static IP address representing your LAN. This VM is called « ns » and its FQDN is « ns.ufaz.lab »

Once we have a static IP and have rebooted the Raspi, we can install Bind DNS.

```
sudo apt-get install bind9
```

You will find all files in directory ***/etc/bind.***
Your lab domain is “ufaz.lab”. You need to announce two zones to Bind process. One for forward name resolution and one for reverse lookup.

2.1. Named zone configuration

Enter to the « named.conf.local » and add your name resolution zone called « **ufaz.lab** » and the reverse one « **x.y.z.in-addr.arpa** »

```
zone "ufaz.lab" {
type master;
notify no;
file "/etc/bind/db.lab";
};
zone "x.y.z.in-addr.arpa" {
type master;
notify no;
file "/etc/bind/db.reverse";
};
```

2.2. The zone files

As announced in the "named.conf.local" file, you have one file per zone. The zone files contain all entries as a translation table for the names of the resources in the same zone.

- **/etc/bind/db.local file :**

Complete the below file to resolve the reste of VM hosts of your plate-forme. Give a name for each VM

```
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
@ IN SOA ns.ufaz.local. root.ifaz.local. (
                    100 ; Serial
                    6H ; Refresh
                    86400 ; Retry, temps entre de essais
                    2419200 ; Expire
                    604800 ) ; Negative Cache TTL

            NS ns.ufaz.local.
            MX 10 mail.ufaz.local.

ns1     IN      A       x.x.x.x                 (x.x.x.x : IP address is the DNS server IP
address)
```

- **/etc/bind/db.reverse file :**

```
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
@ IN SOA ns.ufaz.local. root.ifaz.local. (
                    100 ; Serial
                    6H ; Refresh
                    86400 ; Retry, temps entre de essais
                    2419200 ; Expire
                    604800 ) ; Negative Cache TTL

            NS ns.ufaz.local.
            MX 10 mail.ufaz.local.
T       IN      PTR             ns.ufaz.lab.
```

Consider 10.0.0.1 the DNS IP address, if we mappe dit to x.y.z.T. The reverse resolution of this address is represented by « T » and is a pointer to « ns.ufaz.lab » in the « db.reverse » file. With the knowledge that « x.y.z » the network prefix is used to identify the reverse zone in the « named.conf.local »

- Complete this file to translate all IP addresses to their corresponding names

3. Syntax verification

Verify your syntax is working by using named-checkconf

```
named-checkconf /etc/bind/named.conf.local
```

Also double check syntax on your « db.lab » file and all others you have setup, you would do the following.

```
named-checkzone ufaz.lab  /etc/bind/db.lab
```

Output we will look as below :

```
zone lab.local/IN: loaded serial 1
OK
```

the server configuration part is completed, you must restart the service

systemctl restart bind9

Know you need to setup the clients you configured in your « db.local » file.

4. **Configure clients**

To complete the configuration, you update the /etc/resolv.conf file.

```
search ufaz.lab

nameserver x.x.x.x                    (x.x.x.x is the DNS IP address)
```

5. **DNS query test**

   You have many tools to make a DNS query, you use olny two : nslookup and dig CLI commands

   Example :

   nslookup ns.ufaz.lab

   or

   nslookup 8.8.8.8 (be sûre that you have access to Internet)

   dig @IP_of_your_DNS www.google.com ANY

   test :

   - Based on « dig » command, send a DNS query to ufaz.az to ask for mail server
   - How you can get the SOA of this domain
   - Look for the NS server of google.com
   - With scapy create a script to send a DNS query to ufaz.az