Laboratoare Administarea Retelelor de Calculatoare

Serverul DNS

Instalarea serverului Bind9

- Un server DNS are rolul de a transalta numele de adresa in adresa IP.
- De exemplu google.ro → 1.2.3.4, pentru ca reteaua nu comunica pe nume ci pe adrese IP iar calculatorul nu poate intelege direct numele.
- Distributia folosita este ubuntu si putem instala ruland ca root comanda “apt install bind9.
- Locul unde gasim fisierele de configuratie este /etc/bind
- Fisierul de configurare al modului in care lucreaza serverul este named.conf.options.

```
root@ubuntu22-server:/etc/bind# apt install bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  bind-doc resolvconf
The following NEW packages will be installed:
  bind9
0 upgraded, 1 newly installed, 0 to remove and 193 not upgraded.
Need to get 251 kB of archives.
After this operation, 928 kB of additional disk space will be used.
Get:1 http://lv.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9 amd64 1:9.18.1-1ubuntu1.3 [251 kB]
Fetched 251 kB in 0s (729 kB/s)
Selecting previously unselected package bind9.
(Reading database ... 73255 files and directories currently installed.)
Preparing to unpack .../bind9_1%3a9.18.1-1ubuntu1.3_amd64.deb ...
Unpacking bind9 (1:9.18.1-1ubuntu1.3) ...
Setting up bind9 (1:9.18.1-1ubuntu1.3) ...
```

```
root@ubuntu22-server:/etc/bind# pwd
/etc/bind
root@ubuntu22-server:/etc/bind# ls
bind.keys  db.127  db.empty  named.conf                named.conf.local    rndc.key
db.0       db.255  db.local  named.conf.default-zones  named.conf.options  zones.rfc1918
root@ubuntu22-server:/etc/bind#
```

```
root@ubuntu22-server:/etc/bind# cat named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

Instalarea serverului Bind9

- Putem porni serverul ruland comanda “systemctl start bind9”
- Dupa care facem o diagnoza rapida ruland comanda dig dns @dns-server (dig bing.com @192.168.122.232)
- Putem vedea ca primim un raspuns de la server asta idicand ca serverul este pornit si primeste cereri.
- Acum am vrea sa ne facem propriul nostru nume care se mai numeste si zona, serverul vine cu cateva zone implicite.

```
abaddon@abaddon in ~ took 193ms
λ dig bing.com @192.168.122.232

; <<>> DiG 9.18.12 <<>> bing.com @192.168.122.232
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45327
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d84e7184a0beb57801000000640ef5be5cbf055e590b2b32 (good)
;; QUESTION SECTION:
;bing.com.                      IN      A

;; ANSWER SECTION:
bing.com.               3600    IN      A       13.107.21.200
bing.com.               3600    IN      A       204.79.197.200

;; Query time: 242 msec
;; SERVER: 192.168.122.232#53(192.168.122.232) (UDP)
;; WHEN: Mon Mar 13 12:06:53 EET 2023
;; MSG SIZE  rcvd: 97
```

Configurarea serverului Bind9

- Pentru a face o zona noua facem un fisier de exemplu student.utm (acesta fiind si zona)
- In care completam detaliile minim neceare pentru o zona valida.

```
  GNU nano 6.2                                                  student.utm
;
; Fisierul zona pentru numele student.utm
;TTL spune cat timp au voie resolverele sa tina cashuita inregistrarea
$TTL    604800
; De aici incepe autoritatea zonei defininid serialul care trebuie sa fie unic pe server
;timpul de refresh, retry, expire si TTL
@       IN      SOA     student.utm. root.student.utm. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
;Intrarile de zona.
@       IN      NS      student.utm.
@       IN      A       192.168.122.61
```

Configurarea serverului Bind9

- Ca serverul sa stie de noua noastra zona trebuie sa adaugam o intrare in “named.conf.default-zones”
- Unde ii zicem ce tip de inregitrare este si localtia fisierului de zona.

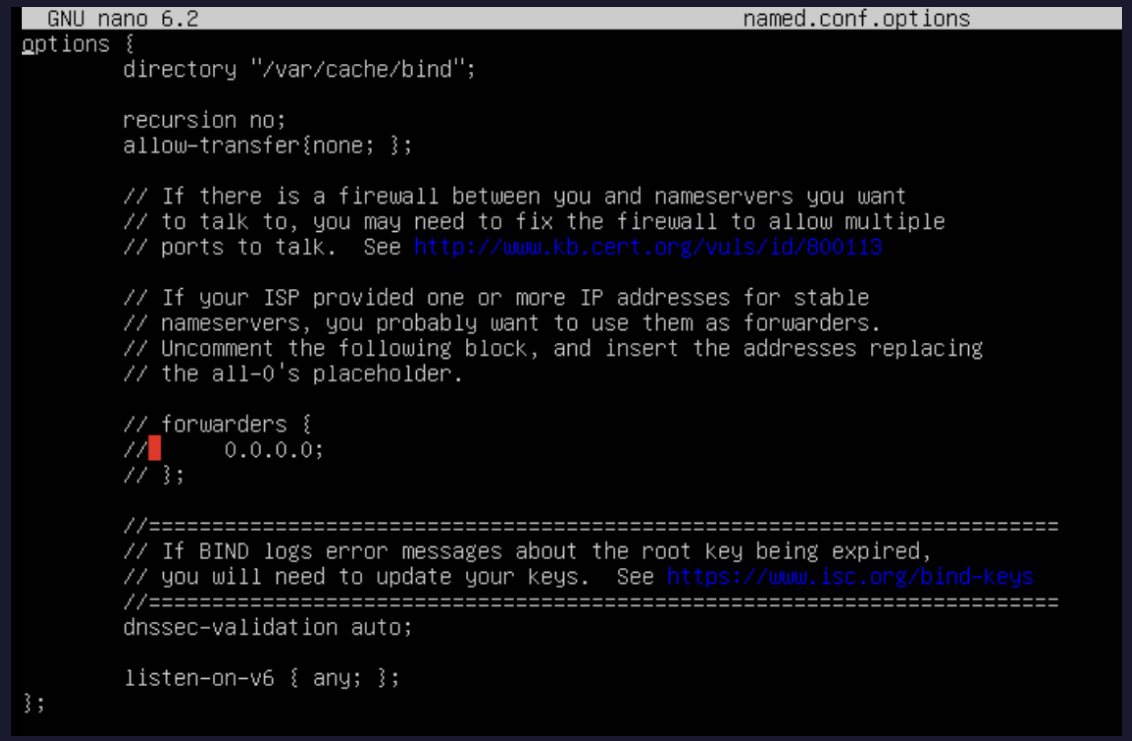
```
zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};


zone "student.utm" {
        type master;
        file "/etc/bind/student.utm";
};
```

Configurarea serverului Bind9 ca autoritativ.

- Dupa cum am vazut la primul test serverul nostru raspundea la orice zona lucur pe care nu il vrem in cazul in care este autoritativ adica sa respunda doar la zonele pe care le administreaza.
- Asa ca in fisierul named.conf.options vom adauga in zona options {} urmatoarele linii:

  recursion no;

  allow-transfer {none; };
- Resetam serverul “systemctl restart bind9”



Configurarea serverului Bind9 ca autoritativ.

- Testam noile setari si putem observa ca nu mai primim un raspuns pentru bing.com doar pentru student.utm

```
abaddon@abaddon in ~ took 23ms
λ dig student.utm @192.168.122.232

; <<>> DiG 9.18.12 <<>> student.utm @192.168.122.232
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48398
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2a820678fd04770b01000000640efe96ad3c1618817de8b3 (good)
;; QUESTION SECTION:
;student.utm.                   IN      A

;; ANSWER SECTION:
student.utm.            604800  IN      A       192.168.122.61

;; Query time: 0 msec
;; SERVER: 192.168.122.232#53(192.168.122.232) (UDP)
;; WHEN: Mon Mar 13 12:44:37 EET 2023
;; MSG SIZE  rcvd: 84
```

```
abaddon@abaddon in ~ took 22ms
λ dig bing.com @192.168.122.232

; <<>> DiG 9.18.12 <<>> bing.com @192.168.122.232
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 31036
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9c35a7afdbf5f79e01000000640efea0ca0b384dd486661a (good)
;; QUESTION SECTION:
;bing.com.                      IN      A

;; Query time: 0 msec
;; SERVER: 192.168.122.232#53(192.168.122.232) (UDP)
;; WHEN: Mon Mar 13 12:44:47 EET 2023
;; MSG SIZE  rcvd: 65
```

Adaugarea subdomeniilor si tipuri de inregistrari.

- Am adaugat zonei cate o inregistrare din cele mai folosite.
- Sam permis zone transfers pentru a putea folosi argumentul axfr ca sa vedem toata zona.

```
  GNU nano 6.2                                          student.utm
;
; Fisierul zona pentru numele student.utm
;TTL spune cat timp au voie resolverele sa tina cashuita inregistrarea
$TTL    604800
; De aici incepe autoritatea zonei defininid serialul care trebuie sa fie unic pe server
;timpul de refresh, retry, expire si TTL
@       IN      SOA     student.utm. root.student.utm. (
                              10         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
;
;Intrarile de zona.
@       IN      NS      student.utm.
192.168.33.1    IN      NS      ns2.student.utm.
router.student.utm.     IN      A       192.168.122.60
@       IN      A       192.168.122.61
www     IN      CNAME   student.utm.
mail1.student.utm. IN   A 192.168.33.2
mail2.student.utm. IN   A 192.168.33.3
@       IN      MX      10      mail1.student.utm.
@       IN      MX      20      mail2.student.utm.
192.168.122.61.student.utm. IN  PTR srv1.student.utm.
```

```
┌─abaddon@abaddon in ~ took 26ms
└─λ dig axfr student.utm @192.168.122.232

; <<>> DiG 9.18.12 <<>> axfr student.utm @192.168.122.232
;; global options: +cmd
student.utm.            604800  IN      SOA     student.utm. root.student.utm. 10 604800 86400 2419200 604800
student.utm.            604800  IN      MX      10 mail1.student.utm.
student.utm.            604800  IN      MX      20 mail2.student.utm.
student.utm.            604800  IN      A       192.168.122.61
student.utm.            604800  IN      NS      student.utm.
192.168.33.1.student.utm. 604800 IN     NS      ns2.student.utm.
192.168.122.61.student.utm. 604800 IN   PTR     srv1.student.utm.
mail1.student.utm.      604800  IN      A       192.168.33.2
mail2.student.utm.      604800  IN      A       192.168.33.3
router.student.utm.     604800  IN      A       192.168.122.60
www.student.utm.        604800  IN      CNAME   student.utm.
student.utm.            604800  IN      SOA     student.utm. root.student.utm. 10 604800 86400 2419200 604800
;; Query time: 0 msec
;; SERVER: 192.168.122.232#53(192.168.122.232) (TCP)
;; WHEN: Mon Mar 13 13:05:11 EET 2023
;; XFR size: 12 records (messages 1, bytes 379)
```