

Memòria pràctica 2

1 Introducció

En aquesta pràctica hem configurat un servidor de DNS tan de forma local com autoritària. El programa utilitzat per tal d'aconseguir aquest objectiu es el programa bind9, un servidor de DNS.

En un primer moment, cap màquina disposava de un servidor de noms definit, així que encara que hi havia connexió a Internet, (pings funcionaven) no hi havia cap servei que en el cas de que introduíssim un nom, per exemple `www.google.com`, pogués preguntar quina és la IP d'aquest nom. Per tan el primer pas va ser modificar el arxiu `resolv.conf` trobat a:

```
/etc/resolv.conf
```

Un cop modificat estem al document, escriurem un servidor de DNS extern. Per exemple el DNS públic de google.

```
nameserver 8.8.8.8
```

D'aquesta forma ja disposem d'un servei de resolució de noms.

2 Configuració

Un cop ja hem instal·lat l'aplicació bind9, ja disposem d'un servidor de noms local, això significa que podem tornar a l'arxiu `resolv.conf` i canviar el que tenim per:

```
nameserver 127.0.0.1
```

Indicant així que el servidor de noms local és la propia màquina.

Ara que ja disposem de un DNS local configurarem un DNS autoritatiu. Aquest DNS serà l'encarregat de gestionar el domini `gn.asi.itic.cat`. Per realitzar això primer de tot tenim que configurar la ip de la nostra màquina virtual perquè segueixi el següent format:

```
172.20.gn.4
```

en el cas del servidor autoritatiu primari, i

```
172.20.gn.5
```

en el cas del secundari. Un cop ja tenim les IP's configurades passarem a configurar els fitxers necessaris. El primer fitxer que configurarem serà:

/etc/bind/named.conf.local

En aquest arxiu es configuren totes les configuracions locals. Per exemple en el nostre cas tindriem el següent:

```
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "g2.asi.itic.cat" {
    type master;
    file "/etc/bind/db.g2";
    allow-transfer {
        172.20.2.5;
    };
};

zone "2.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172";
};
```

En aquest arxiu configurem la zona g2.asi.itic.cat. Ja que aquest document es part del DNS primari es de tipus master, i l'arxiu de configuració es troba a:

/etc/bind/g2

D'altra banda també hi ha la configuració de la zona encarregada del DNS invers.

2.1 Configuració DNS primari

Un cop hem definit la zona és hora de configurar el DNS autoritatiu. Per fer-ho obrir l'arxiu `/etc/bind/g2` i l'editem.

```
$TTL      1w
g2.asi.itic.cat.      IN      SOA      dns1.g2.asi.itic.cat.  sergicarol35.gmail.
                                2015031201      ; Serial
                                2h              ; Refresh
                                1h              ; Retry
                                1w              ; Expire
                                1w )            ; Negative Cache TTL

;
;
; SERVER NAME
;
;

g2.asi.itic.cat.      NS      dns1.g2.asi.itic.cat.
g2.asi.itic.cat.      NS      dns2.g2.asi.itic.cat.

;
;
; MAPA DE NOMS
;
;

dns1.g2.asi.itic.cat.  A      172.20.2.4
dns2.g2.asi.itic.cat.  A      172.20.2.5
```

En aquest arxiu estem dient que la nostra zona de autoritat és la de `g2.asi.itic.cat`, a continuació diem una serie de parametres, com per exemple any,mes,dia,hora de la última modificació, així com cada quant és te que refrescar, quant expira...

A continuació definim el Server Name. En aquest apartat definim quins "sub-grups" volem crear. En el nostre cas hem creat un subgrup per cada maquina virtual (`dns1` i `dns2`). D'aquesta forma li estem dient que `g2.asi.itic.cat` dona servei a `dns1.g2.asi.itic.cat` i a `dns2.g2.asi.itic.cat`.

Finalment tenim el mapa de noms, aquí definim la IP de cada nom definit anteriorment, de tal forma que els dominis amb nom `dns1.g2.asi.itic.cat` aniran a parar a `172.20.2.4`

Un cop definit aquest arxiu podem definir el servidor secundari (slave)

2.2 Configuració DNS secundari

Per tal de definir el DNS secundari tenim que mirar un altre cop com definim la zona del DNS primari. 2 Veiem com indiquem que volem un allow-transfer a 172.20.2.5 , que es la IP del nostre servidor secundari. D'aquesta forma li diem que aquesta zona es pot transferir a un altre servidor.

En el DNS secundari també tenim que modificar l'arxiu `/etc/bind/named.conf.local` de la següent forma:

```
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "g2.asi.itic.cat" {  
    type slave;  
    file "secundari.g2.asi.itic.cat";  
    masters { 172.20.2.4; };  
};  
  
zone "2.20.172.in-addr.arpa" {  
    type slave;  
    file "local.g2.asi.itic.cat";  
    masters { 172.20.2.4; };  
};
```

Aquí podem veure com estem definint la zona `g2.asi.itic.cat` de tipus esclau i dient que el master es el 172.20.2.4. Això tan ho fem per la zona normal com la inversa.

El servidor secundari no necessita configurar cap més arxiu.

3 Proves

A conitnuació hi han un seguit de proves realitzades amb la eina "dig"

```
root@dns1:/home/sergi# dig dns1.g8.asi.itic.cat

;<<> DiG 9.9.5-9-Debian <<> dns1.g8.asi.itic.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28807
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns1.g8.asi.itic.cat.      IN      A
;; ANSWER SECTION:
dns1.g8.asi.itic.cat.  604777 IN      A      172.20.8.4
;; AUTHORITY SECTION:
g8.asi.itic.cat.      10767 IN      NS      ns.g8.asi.itic.cat.
g8.asi.itic.cat.      10767 IN      NS      ns2.g8.asi.itic.cat.
;; ADDITIONAL SECTION:
ns.g8.asi.itic.cat.   10767 IN      A      172.20.8.4
ns2.g8.asi.itic.cat.  10767 IN      A      172.20.8.5

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 09 15:11:39 CET 2015
;; MSG SIZE rcvd: 132

root@dns1:/home/sergi#
```

En la imatge anterior veiem com podem fer un dig a dns1.g8.asi.itic.cat. També podem fer-ne un a dns2.g8.asi.itic.cat:

```
root@dns1:/home/sergi# dig dns2.g8.asi.itic.cat

;<<> DiG 9.9.5-9-Debian <<> dns2.g8.asi.itic.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns2.g8.asi.itic.cat.      IN      A
;; ANSWER SECTION:
dns2.g8.asi.itic.cat.  604758 IN      A      172.20.8.5
;; AUTHORITY SECTION:
g8.asi.itic.cat.      10758 IN      NS      ns.g8.asi.itic.cat.
g8.asi.itic.cat.      10758 IN      NS      ns2.g8.asi.itic.cat.
;; ADDITIONAL SECTION:
ns.g8.asi.itic.cat.   10758 IN      A      172.20.8.4
ns2.g8.asi.itic.cat.  10758 IN      A      172.20.8.5

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 09 15:11:48 CET 2015
;; MSG SIZE rcvd: 132

root@dns1:/home/sergi#
```

Així com un al nostre propi dns1.g2.asi.itic.cat

```

root@dns1:/home/sergi# dig dns1.g4.asi.itic.cat
^Croot@dns1:/home/sergi# dig dns1.g2.asi.itic.cat

; <<> DiG 9.9.5-9-Debian <<> dns1.g2.asi.itic.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17264
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns1.g2.asi.itic.cat.      IN      A
;; ANSWER SECTION:
dns1.g2.asi.itic.cat.  604800 IN      A      172.20.2.4
;; AUTHORITY SECTION:
g2.asi.itic.cat.      604800 IN      NS      dns2.g2.asi.itic.cat.
g2.asi.itic.cat.      604800 IN      NS      dns1.g2.asi.itic.cat.
;; ADDITIONAL SECTION:
dns2.g2.asi.itic.cat. 604800 IN      A      172.20.2.5
;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 09 15:12:02 CET 2015
;; MSG SIZE rcvd: 114
root@dns1:/home/sergi#

```

A conitnuació fem un dig a g8.asi.itic.cat

```

root@dns2:/home/sergi# dig g8.asi.itic.cat

; <<> DiG 9.9.5-9-Debian <<> g8.asi.itic.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52521
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;g8.asi.itic.cat.      IN      A
;; AUTHORITY SECTION:
g8.asi.itic.cat.      10800 IN      SOA     dns1.g8.asi.itic.cat. sistemes.asi.itic.cat. 2015030903 7200 3600 604800 604800
;; Query time: 155 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 09 15:28:28 CET 2015
;; MSG SIZE rcvd: 94
root@dns2:/home/sergi#

```

També podem veure com fer el mateix a g7.asi.itic.cat funciona:

```

sergi@dns1:~$ dig g7.asi.itic.cat

; <<> DiG 9.9.5-9-Debian <<> g7.asi.itic.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30047
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;g7.asi.itic.cat.                IN      A

;; AUTHORITY SECTION:
g7.asi.itic.cat.                10800   IN      SOA     dns1.g7.asi.itic.cat. quercusroses.g7.asi.itic.cat.g7.asi.itic.cat. 2015031101 7200 3600 604800 604800

;; Query time: 461 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Mar 11 13:28:16 CET 2015
;; MSG SIZE rcvd: 114

sergi@dns1:~$

```

4 DNS invers

Finalment configurarem el DNS invers. El dns invers, com el sue nom indica ens permet buscar el nom de un domini apartir de una adreça IP. Per exemple buscar el DNS invers de 172.20.2.4 tindria que donar com a resposta dns1.g2.asi.itic.cat. La configuració d'aquest arxiu es una mica peculiar, ja que si recuperem el que haviem descrit en el fitxer `/etc/bind/named.conf.local` podem veure el següent.

```

zone "2.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172";
};

```

Podem veure com la definició de la zona ja és peculiar, ja que aquesta té els 3 primers digits de la IP de la maquina inversament. L'arxiu de configuració sera el db.172

En l'arxiu i trobem el següent:

```

$TTL      604800
@         IN      SOA      dns1.g2.asi.itic.cat.  sergicarol35.gmail.com. (
                                201503111          ; Serial
                                604800             ; Refresh
                                86400              ; Retry
                                2419200            ; Expire
                                604800 )           ; Negative Cache TTL
;

                IN      NS      g2.asi.itic.cat.

4          IN      PTR      dns1.g2.asi.itic.cat.
5          IN      PTR      dns2.g2.asi.itic.cat.

```

Aquí definim la configuració del DNS invers. Podem veure que es una configuració mes curta que les anteriors. Basicament diem que les IP's que hem definit a la zona (172.20.2) que acabin amb 4 es refereixen a dns1.g2.asi.itic.cat, i les que acaben en 5 es refereixen a dns2.g2.asi.itic.cat.

Per tal de provar això podem utilitzar un altre cop la eina dig amb l'opció -x o sino host 172.20.2.4

```

root@dns1:/home/sergi# dig -x 172.20.2.4
; <<> DiG 9.9.5-9-Debian <<> -x 172.20.2.4
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 37089
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;4.2.20.172.in-addr.arpa.      IN      PTR
;; ANSWER SECTION:
4.2.20.172.in-addr.arpa. 604800 IN      PTR      dns1.g2.asi.itic.cat.
;; AUTHORITY SECTION:
2.20.172.in-addr.arpa. 604800 IN      NS      g2.asi.itic.cat.
;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Mar 12 18:56:39 CET 2015
;; MSG SIZE rcvd: 100
root@dns1:/home/sergi#

```

Podem veure com a la secció de answer hi ha el nom de la maquina, dns1.g2.asi.itic.cat i com la autoritat de aquest subdomini pertany a g2.asi.itic.cat.

5 Conclusions

Finalment han quedat que les maquines tenen connexió a internet tan utilitzant IP's com utilitzant noms de domini. L'únic inconvenient es que el bind9 no s'inicia amb les aplicacions de startup, tenint que activar-lo manualment, ja que sino s'activa el servei de noms no esta disponible.

D'altre banda en el cas de que creessim una nova maquina virtual n'hi hauria suficient ficant com a servidor local de DNS una de les dues maquines configurades, dns1 o dns2.