



Documentació DNS

30/09/2021

—

Alex Garrido Hernandez

SMX2n G1 M7

2021-2022

Índex

1. Explica perquè serveix el servei DNS	2
2. Fitxer hosts	2
3. Instal·lació del servei DNS	4
4. Com es diu el servei, quin usuari l'executa, quin port fa servir?	5
5. Quins fitxers fem servir per configurar el servei?	6
6. Eines de comprovació	7
7. Configuració d'un domini amb tots els registres	9
- Configuració de la zona	9
- Tipus de registres, creació de registres	10
8. Configuració d'un domini invers i verificació	11
9. Activació dels forwarders	12
10. Delegació de zona	13
- *ORIGIN*	14
11. Servidor master, slave i verificació.	15
12. Banc de proves (com comprovar que tot funciona, i com detectar els errors)	16
13. Esquema activitat global	17
15. Anàlisi de casos	18

1. Explica per què serveix el servei DNS

La principal idea perquè utilitzem el DNS és bàsicament per escurçar aquelles adreces IP's dels llocs web a on volem accedir.

Per a un humà és més fàcil recordar paraules que números, per això, quan volem accedir a Google no posem 142.250.184.4.

És clar que per això no trobarem mai dos llocs webs diferents amb la mateixa IP, ja que podria crear un conflicte.

2. Fitxer hosts

1. Per començar, el que farem serà saber quina IP té Google, per això utilitzarem la comanda `< host www.google.es >`.

```
user@debian:~$ host www.google.es
www.google.es has address 142.250.200.131
www.google.es has IPv6 address 2a00:1450:4003:80f::2003
user@debian:~$ sudo nano /etc/hosts
```

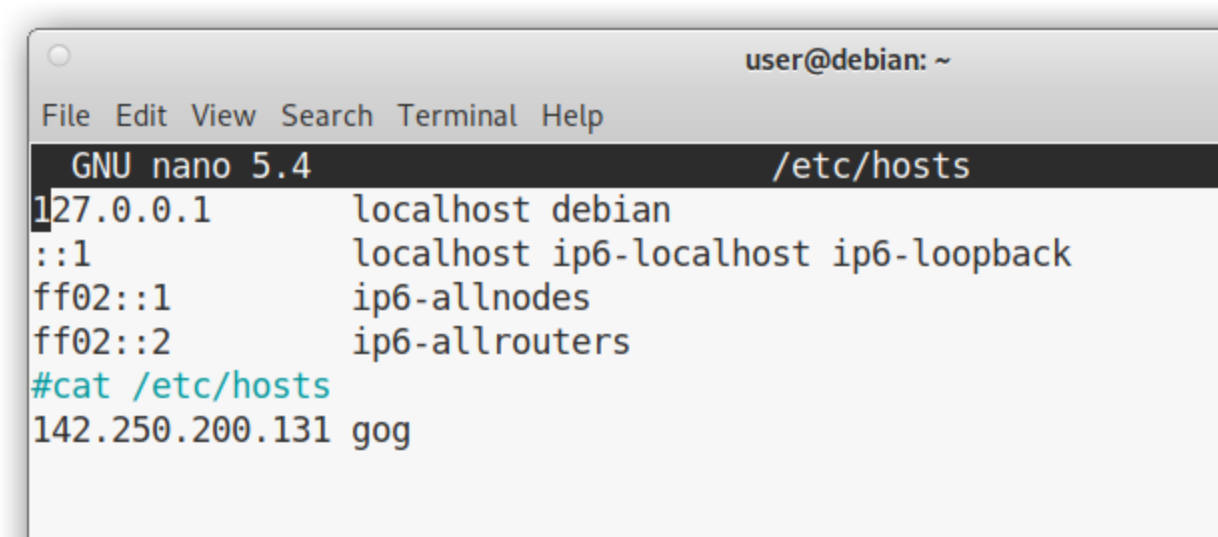
2. A continuació, entrarem al fitxer `/etc/hosts` i haurem d'escriure:

```
# nano /etc/hosts
```

142.250.200.131 gog → "gog" serà la paraula que haurem de buscar al navegador.

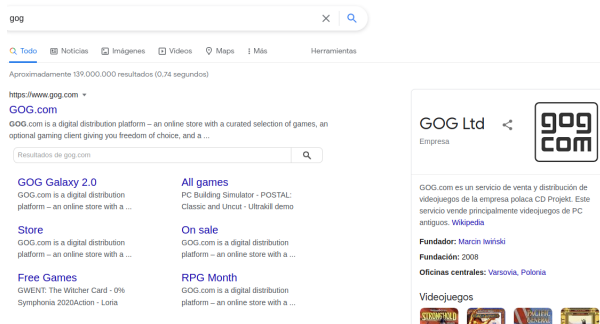
Per entrar a editar aquest fitxer, farem la comanda `< sudo nano /etc/hosts >`

Editem aquest fitxer per assignar a un IP un nom en concret o escurçat.

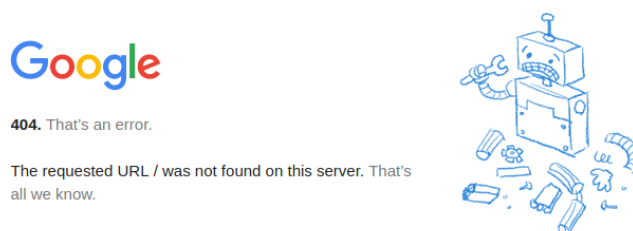


```
user@debian: ~
File Edit View Search Terminal Help
GNU nano 5.4 /etc/hosts
127.0.0.1    localhost debian
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
#cat /etc/hosts
142.250.200.131 gog
```

3. Si ara busquem “gog” al navegador veurem que no funciona.



4. En canvi si busquem <https://gog> ens sortirà el següent.



5. A continuació, si volem bloquejar la publicitat el que farem ser redirigir l'enllaç dels anuncis de la pàgina. Per això utilitzarem “Inspeccionar” i agafarem l'enllaç de l'anunci.

Per això després haurem de redirigir a la IP 0.0.0.0.

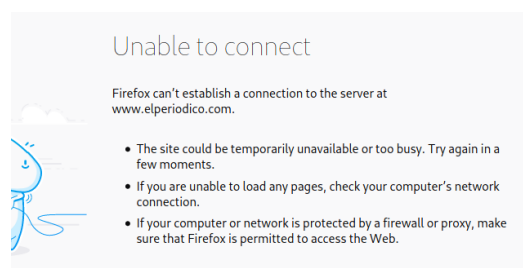
#Bloquear acceso a la publicidad
0.0.0.0 <https://googleads.g.doubleclick.net>

Si fem un ping a 0.0.0.0 veurem que ens respon el “localhost”.

```
user@debian:~$ ping 0.0.0.0
PING 0.0.0.0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.039 ms
```

Si volem bloquejar una pàgina web haurem de posar el link de la pàgina.

#Bloquear pàgina web
0.0.0.0 www.elperiodico.com



3. Instal·lació del servei DNS

Començarem obrint el terminal i introduïrem la següent comanda **<sudo apt install dnsutils bind9 nmap -y>**.

És molt important abans fer un **<sudo apt get update>** perquè el repositori s'actualitzi.

Ja ho havia instal·lat anteriorment

```
user@debian:~$ sudo apt install dnsutils bind9 nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.16.15-1).
dnsutils is already the newest version (1:9.16.15-1).
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2).
The following package was automatically installed and is no longer required:
  libeatmydata1
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
user@debian:~$ █
```

4. Com es diu el servei, quin usuari l'executa, quin port fa servir?

Bind9

Aquest servei s'utilitza per saber en quin estat està el servei i quin tipus d'errors podem tenir. Aquí tenim un exemple:

```
root@debian:/etc/bind# systemctl restart bind9
root@debian:/etc/bind# systemctl start bind9
root@debian:/etc/bind# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-08 10:19:34 UTC; 3s ago
     Docs: man:named(8)
    Main PID: 4230 (named)
      Tasks: 14 (limit: 9120)
     Memory: 50.6M
        CPU: 47ms
    CGroup: /system.slice/named.service
            └─4230 /usr/sbin/named -f -u bind

Oct 08 10:19:34 debian named[4230]: configuring command channel from '/etc/bind/rndc.key'
Oct 08 10:19:34 debian named[4230]: command channel listening on ::1#953
Oct 08 10:19:34 debian named[4230]: managed-keys-zone: loaded serial 4
Oct 08 10:19:34 debian named[4230]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone localhost/IN: loaded serial 2
Oct 08 10:19:34 debian named[4230]: zone smx2.agarrido.org/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: all zones loaded
```

Nmap

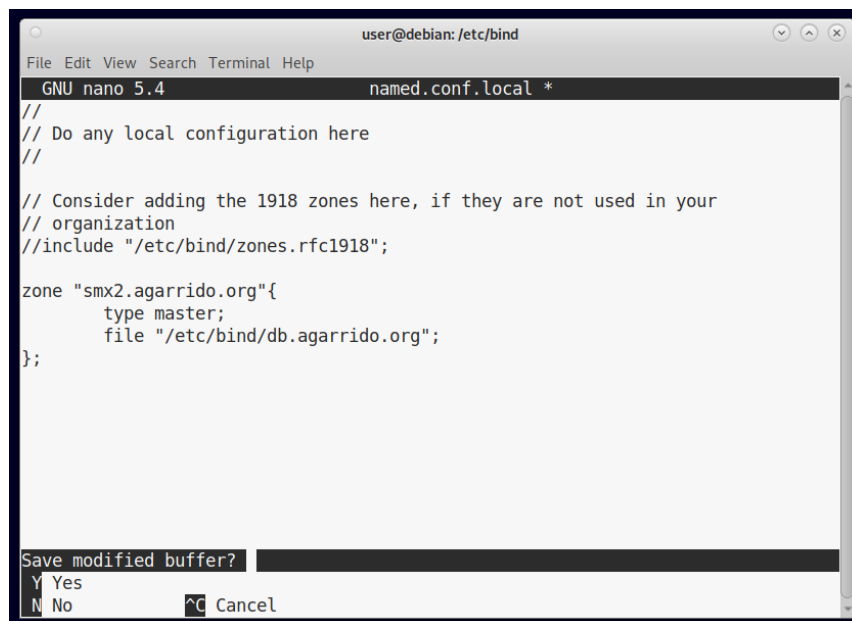
Aquest servei serveix per identificar quin port fa servir "x" IP, en aquest cas he posat la meua IP per veure que el port "domain" és el servidor que tenim obert. Fa servir el port 53.

```
root@debian:/etc/bind# nmap 192.168.203.21
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-08 10:53 UTC
Nmap scan report for 192.168.203.21
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
```

5. Quins fitxers fem servir per configurar el servei?

named.conf.local

Aquest fitxer l'utilitzem com hem vist abans, per crear la nostra zona a on ubicarem el servidor.



```

user@debian: /etc/bind
GNU nano 5.4      named.conf.local *
//
// 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 "smx2.agarrido.org"{
    type master;
    file "/etc/bind/db.agarrido.org";
};

Save modified buffer?
Y Yes
N No      ^C Cancel
  
```

La nostra zona en aquest cas s'anomenarà **smx2.agarrido.org** i la base de dades es guardarà com **db.agarrido.org**.

db.agarrido.org

Aquest és el fitxer on guardarem tots els recursos que necessitem la nostra base de dades. Podrem denominar si tenim un recurs de servidor de correu, o si tenim diferents PC's connectats al nostre servidor.

named.conf.options

Aquest arxiu serveix per configurar els forwarders. Els forwarders serveixen com a segona opció de cerca de DNS

resolv.conf

Aquest arxiu serveix a quin servidor DNS preguntarem a l'hora de buscar, si aquest no troba res, preguntarà als forwarders.

6. Eines de comprovació

ping: Aquesta eina l'utilitzarem per saber si tenim connexió amb allò que especifiquem

```
root@debian:/etc/bind# ping google.com
PING google.com (142.250.185.14) 56(84) bytes of data:
64 bytes from mad41s11-in-f14.1e100.net (142.250.185.14): icmp_seq=1 ttl=110 time=11.2 ms
64 bytes from mad41s11-in-f14.1e100.net (142.250.185.14): icmp_seq=2 ttl=110 time=11.5 ms
64 bytes from mad41s11-in-f14.1e100.net (142.250.185.14): icmp_seq=3 ttl=110 time=11.6 ms
^C
```

systemctl "" bind: Aquesta eina serveix per veure si tenim el nostre servidor en marxa i si hem obtingut cap error pel camí. Com podem veure, no tenim cap línia vermella en la part inferior de la comanda i el servei està "Active (running)".

```
root@debian:/etc/bind# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-08 10:19:34 UTC; 48min ago
     Docs: man:named(8)
    Main PID: 4230 (named)
      Tasks: 14 (limit: 9120)
     Memory: 67.1M
        CPU: 289ms
    CGroup: /system.slice/named.service
            └─4230 /usr/sbin/named -f -u bind

Oct 08 10:19:34 debian named[4230]: configuring command channel from '/etc/bind/rndc.key'
Oct 08 10:19:34 debian named[4230]: command channel listening on ::1#953
Oct 08 10:19:34 debian named[4230]: managed-keys-zone: loaded serial 4
Oct 08 10:19:34 debian named[4230]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone localhost/IN: loaded serial 2
Oct 08 10:19:34 debian named[4230]: zone smx2.agarrido.org/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct 08 10:19:34 debian named[4230]: all zones loaded
Oct 08 10:19:34 debian named[4230]: running
root@debian:/etc/bind# █
```

host: Aquesta eina serveix per a quines IP's tenen el lloc web que demanem, en aquest cas també podem veure quins servidors de correu té google.com

```
root@debian:/etc/bind# host google.com
google.com has address 142.250.185.14
google.com has IPv6 address 2a00:1450:4003:803::200e
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
root@debian:/etc/bind# █
```


dig: Aquesta eina serveix per veure si el teu servidor o la IP demanada et contesta.

```
root@debian:/etc/bind# dig 192.168.203.21

; <<> DiG 9.16.15-Debian <<> 192.168.203.21
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49490
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e743dd7aefff6ad521e2fb6d6160273a83066bcee110d903 (good)
;; QUESTION SECTION:
;192.168.203.21.                IN      A

;; AUTHORITY SECTION:
.                10800    IN      SOA      a.root-servers.net. nstld.verisign-grs.com.
2021100800 1800 900 604800 86400

;; Query time: 7 msec
;; SERVER: 192.168.0.100#53(192.168.0.100)
;; WHEN: Fri Oct 08 11:10:50 UTC 2021
;; MSG SIZE rcvd: 146
```

nslookup: Podríem dir que és la mateixa eina que “dig” però més antiga i menys complexa.

```
root@debian:/etc# nslookup google.com
^C
root@debian:/etc# nano resolv.conf
root@debian:/etc# nslookup google.com
Server:          192.168.0.100
Address:         192.168.0.100#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.185.14
Name:   google.com
Address: 2a00:1450:4003:803::200e
```

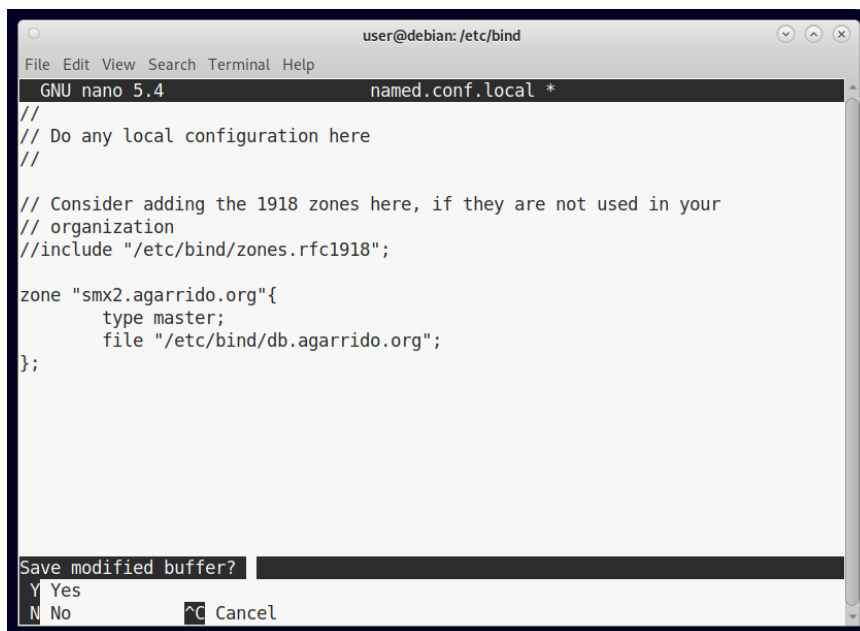
7. Configuració d'un domini amb tots els registres

- Configuració de la zona

1. Per crear una zona haurem de saber que modificarem l'arxiu "named.conf.local"

Aquest arxiu serveix per crear una zona, això vol dir que li donarem lloc al nostre servidor.

Començarem obrint l'arxiu situant-nos a **/etc/bind** → amb la comanda → ***nano named.conf.local***



```
user@debian: /etc/bind
GNU nano 5.4 named.conf.local *
//
// 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 "smx2.agarrido.org"{
    type master;
    file "/etc/bind/db.agarrido.org";
};

Save modified buffer?
Y Yes
N No ^C Cancel
```

2. Continuarem canviant el nom a la zona predeterminada que ve a l'arxiu, en aquest cas he posat "smx2.agarrido.org"

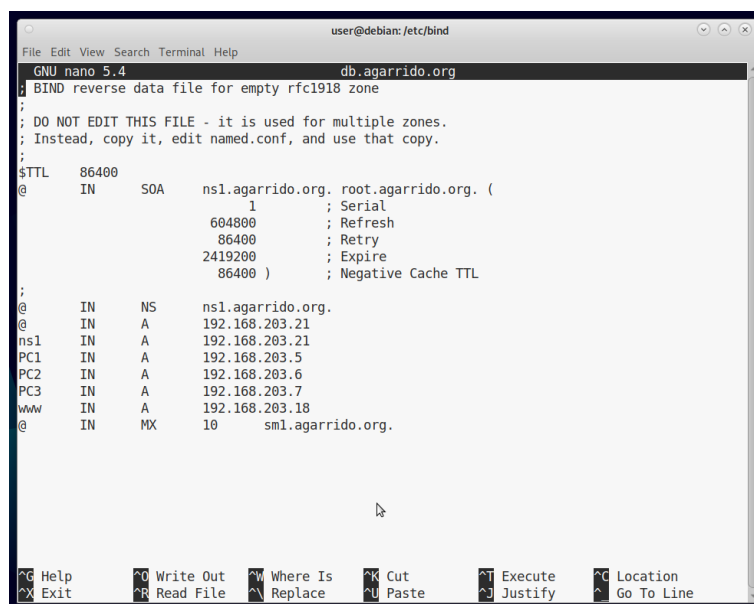
Haurem d'indicar al document a on guardarem la nostra base de dades del servidor, per això indicarem la ruta: **file *"/etc/bind/db.agarrido.org"***

- Tipus de registres, creació de registres

1. Una vegada hem creat la zona del nostre servidor, haurem d'indicar quins serveis tindrà la nostra base de dades (del servidor)

Existeixen diferents tipus de registres:

- **Registre SOA:** Indica que el fitxer de zona és autoritativa de les dades de la zona. És obligatori sempre
- **Registre NS:** NameServer defineix els noms per a les zones
- **Registre A:** Address el que fa és associar un nom a una IP.
- **Registre MX:** Aquest registre serveix per definir un servidor de correu, normalment posem una prioritat, per exemple el núm. 10, però no és obligatori posar una prioritat alta.
- **Registre CNAME:** Els registres de recurs CNAME o canonical name (nom canònic) associen un àlies a un nom canònic.



```

user@debian: /etc/bind
GNU nano 5.4 db.agarrido.org
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
@         IN      SOA      ns1.agarrido.org. root.agarrido.org. (
; Serial
1
; Refresh
604800
; Retry
86400
; Expire
2419200
; Negative Cache TTL
86400 )
;
@         IN      NS       ns1.agarrido.org.
@         IN      A        192.168.203.21
ns1       IN      A        192.168.203.21
PC1       IN      A        192.168.203.5
PC2       IN      A        192.168.203.6
PC3       IN      A        192.168.203.7
www       IN      A        192.168.203.18
@         IN      MX       10      sm1.agarrido.org.

```

En aquest cas hem anomenat PC1, PC2, PC3 a aquelles màquines que volem simular per donar un entorn més realista al nostre servidor. Com podem veure, l'arxiu de la base de dades s'anomena **db.agarrido.org**.

8. Configuració d'un domini invers i verificació

Un domini invers serveix per al mateix que un directe, en el cas de la directa; ens demanen una IP a través d'un domini.

La inversa ens demanaran un domini a través d'una IP.

- **Resolució directa:** tenim el nom, i volem saber la IP.
- **Resolució inversa:** tenim la IP, volem saber el nom.

Començarem configurant el fitxer **named.conf.local** i haurem de crear una nova zona inversa, per això posarem els dos primers octets de la zona, en aquest cas és **168.192**.

És molt important que aquesta nova zona l'associem a la mateixa base de dades que tenim.

```
zone "smx2.agarrido.cat"{
    type master;
    file "/etc/bind/db.smx2.agarrido.cat";
    allow-transfer {192.168.203.20;};
};

zone "168.192.in-addr.arpa."{
    type master;
    file "/etc/bind/db.smx2.agarrido.cat";
};
```

A continuació anirem a la base de dades i haurem de posar un **Registre PTR** que servira per donar nom a aquesta IP.

```
;
@      IN      NS      dns1.smx2.agarrido.cat.
@      IN      A       192.168.203.21
www    IN      A       192.168.0.100
19.203 IN      PTR     dns1.smx2.polan.org.
```

9. Activació dels forwarders

Per fer una activació de forwarders el primer que haurem de fer serà entrar al fitxer **named.conf.options**. Amb aquest fitxer el que haurem de canviar serà la IP del forwarder per delegar la zona en cas d'error.

En el meu cas serà la IP **192.168.0.100**

EXTRA

Com podem observar, a sota hi ha una paraula anomenada "**dnssec-validation no**", això servirà per desactivar una seguretat que té el DNS.

```

user@debian: /etc/bind
File Edit View Search Terminal Help
GNU nano 5.4 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 {
        192.168.0.100;
    };

    //=====
    // 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 no;

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

```

10. Delegació de zona

Per delegar una zona haurem de tenir en compte els forwarders. Una delegació de zona consisteix és el fet que si no troba la informació en la nostra pròpia zona creada, anirà a l'arxiu **named.conf.options** situat a **/etc/bind** i buscarà aquelles IP's per intentar resoldre la informació.

```
forwarders {
    192.168.0.100;
};
```

En el meu cas, la meva delegació de zona serà **192.168.0.100** que és la IP de l'institut.

Però també podem posar una altra IP per fer una delegació de zona, en el meu cas, pot ser la IP del meu company. **Hem de tenir en compte el fitxer resolv.conf del company.**

```
forwarders {
    192.168.0.100;192.168.203.20;
};
```

Un fitxer molt important és el **resolv.conf**. Si a aquest fitxer li diem que el nostre servidor és **192.168.0.100**, ens resoldrà la informació demanada.

Si en el meu cas posem que la IP del servidor és la nostra (**192.168.203.21**), com no poder resoldre la informació demanada, anirà al fitxer de forwarders i veurà que està posada les IP's **192.168.0.100** i **192.168.203.20**.

```
user@debian: /etc
File Edit View Search Terminal Help
GNU nano 5.4 resolv.conf
# Generated by NetworkManager
search thico.cat
nameserver 192.168.0.100
```

ORIGIN

Utilitzarem el mode ORIGIN a la base de dades com a objectiu de donar un nom a aquell domini. Hem de saber que donarem aquest nom com “per defecte” a tots els registres de la nostra base de dades. Això vol dir:

```
$ORIGIN agarrido.org.

@      IN      SOA    ns1 root (

@      IN      NS     ns1

@      IN      A      192.168.203.21

www    IN      A      192.168.8.33
```

El nostre NS que s'anomena ns1, en realitat s'anomena ns1.agarrido.org

També es pot fer servir per escurçar paraules a la nostra base de dades. Adjunto imatge d'exemple.

```
GNU nano 5.4
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
$ORIGIN   agarrido.org.
@         IN      SOA    ns1 root (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        86400 )    ; Negative Cache TTL
;
@         IN      NS     ns1
@         IN      A      192.168.203.21
www       IN      A      192.168.8.33

$ORIGIN   pepito.org
@         IN      NS     ns2
@         IN      A      192.168.203.20
www       IN      A      192.168.8.44
█
```

11. Servidor master, slave i verificació.

Per crear un servidor Slave, haurem de donar permís al nostre fitxer de zona a la màquina que volem transferir. En el meu cas, he agafat com a servidor Slave la màquina del Joel Martínez.

Molt important saber que si volem permetre una transferència al Slave, obrirem l'arxiu de la zona i haurem d'escriure el següent:

```
GNU nano 5.4                                named.conf.local *
```

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

//ZONA ALUMNE.CAT

zone "alumne1.cat"{
    type master;
    file "/etc/bind/db.alumne1.cat";
    allow-transfer {192.168.203.20};
};
```

Això vol dir que en el cas de passes cap cosa en el meu servidor dns, farà una transferència a l'IP **192.168.203.20** (Joel Martínez).

En la màquina Slave, el seu arxiu de zona haurà de ser diferent amb el que hem posat nosaltres. En aquest cas ell haurà de donar permís Slave a la meua IP.

```
GNU nano 5.4                                named.conf.local *
```

```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "alumne.cat"{
    type master;
    file "/etc/bind/alumne.cat";
};

//zone "168.192.in-addr.arpa"{
//    type master;
//    file "/etc/bind/db.alumne.cat";
//};

zone "alumne1.cat"{
    type slave;
    masters; {192.168.203.21};
};
```

Com podem veure, a la zona **alumne1.cat** ha donat permís Slave a la meua IP.

Hem de tenir en compte els possibles errors amb l'arxiu `named.conf` on tindrà que

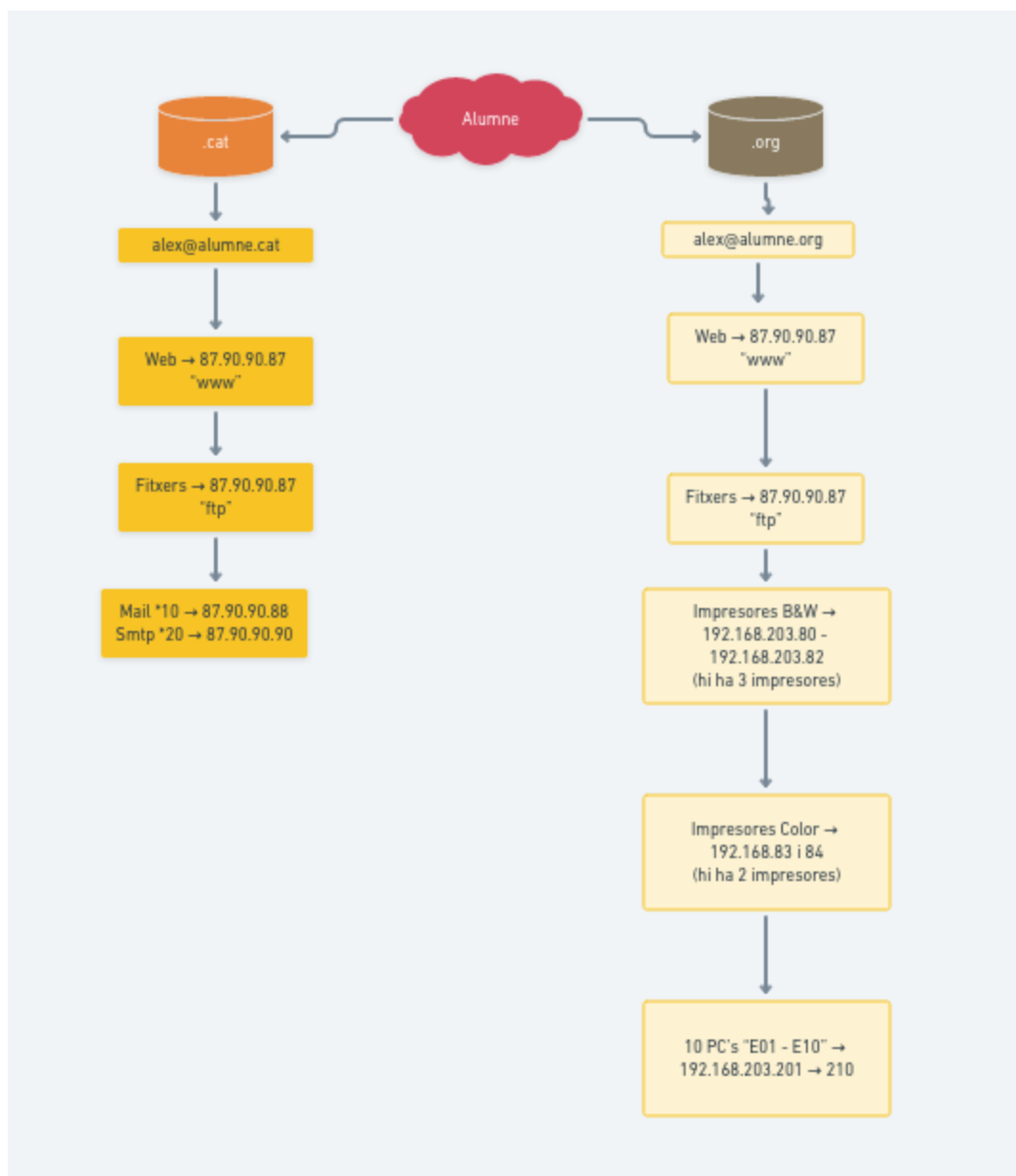
Múltiples entités comparten el mismo nivel de acceso a los datos, pero tal vez algunas llaves

Les autres axes cardinaux de la taxinomie sont également allés avec leurs corollaires : la

13. Esquema activitat global

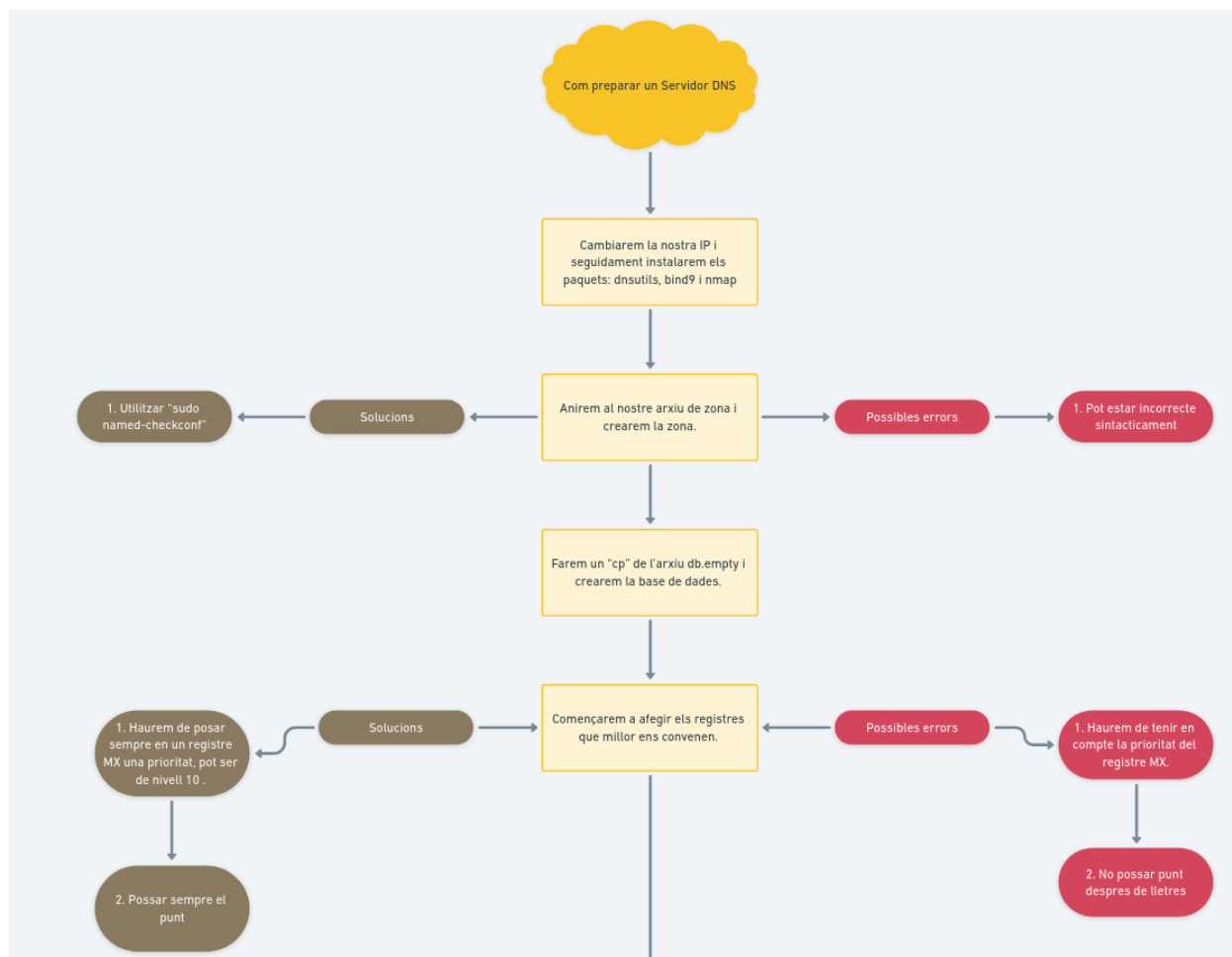
Per fer aquest esquema sobre l'activitat global, he fet servir l'aplicació **Whimiscal**.

Aquesta activitat global, ens demanava fer un domini públic i un domini privat amb diferents recursos. Adjunto la imatge de l'esquema.



Hem de tenir molt en compte les IP's i sobretot la preferència dels mails, el número de PC's i els tipus d'impresores depenent amb les seves IP's...

15. Anàlisi de casos



CONTINUACIÓ



