

# Servidor DNS Linux bind9



# BIND9

Servidor DNS Linux

Ángel David González Quintana

# Índice:

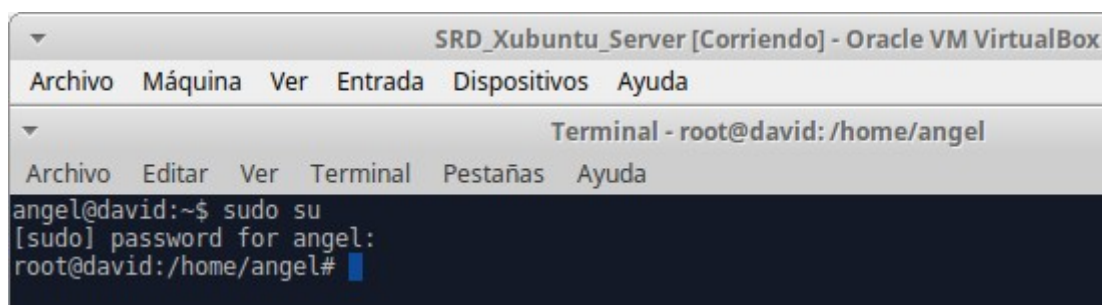
|  |    |
|--|----|
| 0. Introducción: Configurar resolv.conf.....         | 3  |
| 1. Instalación bind9.....                            | 5  |
| 2. Servidor DNS caché.....                           | 7  |
| 3. Comprobar resolución de nombres externos.....     | 8  |
| 4. Configurar DNS Maestro (Master).....              | 9  |
| 5. Crear archivos de búsqueda directa e inversa..... | 10 |
| 6. Comprobar resolución de nombres (servidor).....   | 14 |
| 7. Comprobar resolución de nombres (cliente).....    | 15 |

## 0. Introducción: Configurar resolv.conf

Resolv.conf es el archivo que se usa para resolver los DNS. Un problema con el que nos podemos encontrar es que tras cambiar el contenido de este archivo, sólo nos mantenga los cambios hasta que volvemos a iniciar el equipo.

Para conservar los cambios de resolv.conf incluso cuando hemos reiniciado, hacemos lo siguiente:

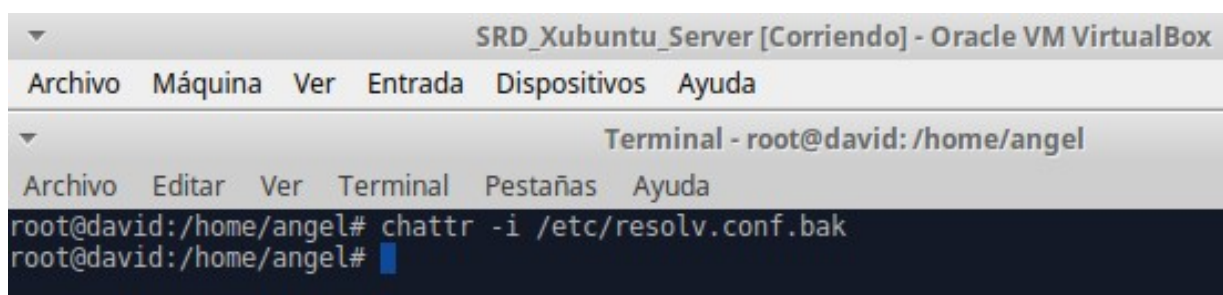
- Haremos una copia del archivo, para ello, primero usaremos el usuario root con el comando `sudo su` y haremos la copia con el comando `cp`:



```
SRD_Xubuntu_Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Terminal - root@david: /home/angel
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
angel@david:~$ sudo su
[sudo] password for angel:
root@david:/home/angel#
```

```
root@david:/home/angel# cp /etc/resolv.conf /etc/resolv.conf.bak
root@david:/home/angel# ls -la /etc/ | grep resolv.conf
lrwxrwxrwx   1 root root    29 sep 17 09:24 resolv.conf -> ../run/resolvconf/resolv.conf
-rw-r--r--   1 root root  172 oct 14 11:51 resolv.conf.bak
root@david:/home/angel#
```

- Hacemos que este nuevo archivo sea inalterable usando el comando `chattr -i`:



```
SRD_Xubuntu_Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Terminal - root@david: /home/angel
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
root@david:/home/angel# chattr -i /etc/resolv.conf.bak
root@david:/home/angel#
```

- Eliminamos el fichero original con el comando `rm` y luego copiamos el archivo restante y le ponemos el nombre del fichero original con el comando `cp`:

```
root@david:/home/angel# rm /etc/resolv.conf
root@david:/home/angel# cp /etc/resolv.conf.bak /etc/resolv.conf
root@david:/home/angel# ls -la /etc/ | grep resolv.conf
-rw-r--r--  1 root root    172 oct 14 11:53 resolv.conf
-rw-r--r--  1 root root    172 oct 14 11:51 resolv.conf.bak
root@david:/home/angel#
```

- En caso de usar la máquina virtual con la que hemos hecho la práctica del DHCP, detenemos el servicio con el comando `service isc-dhcp-server stop`:

```
angel@david:~$ sudo service isc-dhcp-server stop
angel@david:~$ sudo service isc-dhcp-server status
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since jue 2021-10-14 11:58:29 WEST; 7s ago
     Docs: man:dhcpd(8)
  Process: 1311 ExecStart=/bin/sh -ec CONFIG_FILE=/etc/dhcp/dhcpd.conf; if [ -f /etc/ltsp/dhcpd.conf
 Main PID: 1311 (code=killed, signal=TERM)

oct 14 11:54:15 david sh[1311]: Wrote 4 leases to leases file.
oct 14 11:54:15 david dhcpd[1311]: Listening on LPF/enp0s3/08:00:27:71:c6:1a/172.19.27.0/24
oct 14 11:54:15 david sh[1311]: Listening on LPF/enp0s3/08:00:27:71:c6:1a/172.19.27.0/24
oct 14 11:54:15 david dhcpd[1311]: Sending on LPF/enp0s3/08:00:27:71:c6:1a/172.19.27.0/24
oct 14 11:54:15 david sh[1311]: Sending on LPF/enp0s3/08:00:27:71:c6:1a/172.19.27.0/24
oct 14 11:54:15 david dhcpd[1311]: Sending on Socket/fallback/fallback-net
oct 14 11:54:15 david sh[1311]: Sending on Socket/fallback/fallback-net
oct 14 11:54:15 david dhcpd[1311]: Server starting service.
oct 14 11:58:29 david systemd[1]: Stopping ISC DHCP IPv4 server...
oct 14 11:58:29 david systemd[1]: Stopped ISC DHCP IPv4 server.
lines 1-17/17 (END)
```

Una vez terminado todos los pasos, reiniciamos el equipo.

**\*\* Estos son los hostname de los equipos a usar:**

| SO      | Rol             | Hostname                 |
|---------|-----------------|--------------------------|
| Xubuntu | Server - Master | <primer-apellido>27xs    |
| Xubuntu | Client          | <primer-apellido>27xc    |
| Xubuntu | Server - Slave  | <primer-apellido>27slave |

# 1. Instalación bind9

Para empezar, vamos a instalar bind9 en el servidor maestro. Para ello, primero abrimos una terminal y vamos a actualizar la lista de paquetes disponibles con el comando `apt update` (requiere usuario `root`, es decir, `nano`):

```
angel@david:~$ sudo apt update
Des:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Obj:2 http://es.archive.ubuntu.com/ubuntu xenial InRelease
Des:3 http://es.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Des:5 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metadata [93,6 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu xenial-updates/main amd64 DEP-11 Metadata [327 kB]
Des:7 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 DEP-11 Metadata [130 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 DEP-11 Metadata [281 kB]
Des:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 DEP-11 Metadata [2.468 B]
Des:10 http://es.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 DEP-11 Metadata [5.956 B]
Des:11 http://es.archive.ubuntu.com/ubuntu xenial-backports/main amd64 DEP-11 Metadata [3.328 B]
Des:12 http://es.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 DEP-11 Metadata [6.608 B]
Descargados 1.175 kB en 1s (703 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 82 paquetes. Ejecute «apt list --upgradable» para verlos.
angel@david:~$
```

Instalamos bind9 y también los paquetes requeridos por el sistema operativo con el comando `apt install` (requiere usuario `root`):

```
angel@gonzalez27xs:~$ sudo apt install bind9 bind9-doc resolvconf python-ply-doc
sudo: imposible resolver el anfitrión gonzalez27xs
[sudo] password for angel:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bind9utils libirs141
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-doc bind9utils libirs141 python-ply-doc
Se actualizarán los siguientes paquetes:
  resolvconf
1 actualizados, 5 nuevos se instalarán, 0 para eliminar y 81 no actualizados.
Se necesita descargar 907 kB de archivos.
Se utilizarán 4.872 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu xenial-updates/main amd64 resolvconf all 1.78ubuntu7 [52,7 kB]
```

Una vez instalado todos los paquetes anteriores, vamos al directorio del programa `/etc/bind` y revisamos los ficheros del directorio con el comando `ls -la`:

```
angel@gonzalez27xs:~$ cd /etc/bind
angel@gonzalez27xs:/etc/bind$ ls -la
total 68
drwxr-sr-x  2 root bind  4096 oct 14 12:01 .
drwxr-xr-x 129 root root 12288 oct 14 12:01 ..
-rw-r--r--  1 root root  3954 abr 27 14:05 bind.keys
-rw-r--r--  1 root root   237 abr 27 14:05 db.0
-rw-r--r--  1 root root   271 abr 27 14:05 db.127
-rw-r--r--  1 root root   237 abr 27 14:05 db.255
-rw-r--r--  1 root root   353 abr 27 14:05 db.empty
-rw-r--r--  1 root root   270 abr 27 14:05 db.local
-rw-r--r--  1 root root  3171 abr 27 14:05 db.root
-rw-r--r--  1 root bind   463 abr 27 14:05 named.conf
-rw-r--r--  1 root bind   490 abr 27 14:05 named.conf.default-zones
-rw-r--r--  1 root bind   165 abr 27 14:05 named.conf.local
-rw-r--r--  1 root bind   890 oct 14 12:01 named.conf.options
-rw-r-----  1 bind bind    77 oct 14 12:01 rndc.key
-rw-r--r--  1 root root  1317 abr 27 14:05 zones.rfc1918
angel@gonzalez27xs:/etc/bind$
```

Ahora vamos a indicar al equipo que el servidor DNS es él mismo. Para ello, vamos a modificar el fichero `/etc/resolv.conf` con el comando `nano` (requiere usuario `root`) y pondremos lo siguiente:

```
nameserver <ip-server>
domain <dominio>
```



```
Terminal - angel@gonzalez27xs: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
GNU nano 2.5.3      Archivo: /etc/resolv.conf      Modificado
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#   DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.1.1
nameserver 172.19.27.21
domain repcan.es
```

## 2. Servidor DNS caché

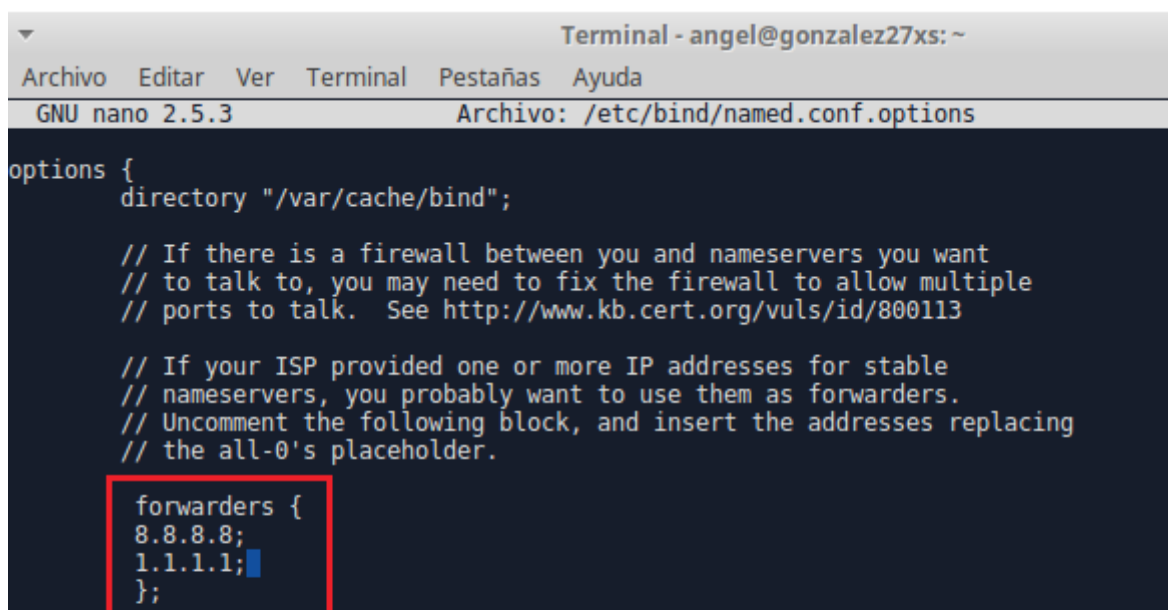
Ahora vamos a configurar el servidor como caché DNS con reenviadores de DNS públicos. Para ello, entramos en la terminal y accedemos como usuario *root* con el comando `sudo su`. Lo primero que haremos es copiar el archivo de configuración que se encarga de esta tarea (`/etc/bind/named.conf.options`) usando el comando `cp`:

```
angel@gonzalez27xs:~$ sudo su
sudo: imposible resolver el anfitrión gonzalez27xs
root@gonzalez27xs:/home/angel# cp /etc/bind/named.conf.options /etc/bind/named.conf.options.copia
```

Comprobamos los ficheros con el comando `ls -la`:

```
root@gonzalez27xs:/home/angel# ls -la /etc/bind/ | grep named.conf.options
-rw-r--r-- 1 root bind 890 oct 14 12:01 named.conf.options
-rw-r--r-- 1 root bind 890 oct 14 12:11 named.conf.options.copia
root@gonzalez27xs:/home/angel#
```

Ahora configuraremos el fichero `/etc/bind/named.conf.options` con el comando `nano` y escribiremos lo siguiente:



```
Terminal - angel@gonzalez27xs: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
GNU nano 2.5.3      Archivo: /etc/bind/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 {
        8.8.8.8;
        1.1.1.1;
    };
}
```

Una vez lo hayamos modificado, reiniciamos el servicio para comprobar que todo funciona correctamente y que no devuelve errores con el comando `service bind9 restart` (requiere usuario *root*).

```
angel@gonzalez27xs:~$ sudo service bind9 restart
```

### 3. Comprobar resolución de nombres externos

Ya que hemos configurado el servidor DNS como caché, vamos a comprobar (tanto en el cliente como en el servidor) la resolución de nombres externos a la intranet. Para ello, usaremos el comando `nslookup`:

- Servidor (prueba con servidor NBA):

```
angel@gonzalez27xs:~$ nslookup www.nba.es
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
www.nba.es      canonical name = nba.es.
Name:   nba.es
Address: 54.84.45.2
Name:   nba.es
Address: 52.52.34.204

angel@gonzalez27xs:~$
```

- Cliente (prueba con servidor Facebook):

```
angel@gonzalez27xc:~$ nslookup www.facebook.es
Server:          172.19.27.21
Address:         172.19.27.21#53

Non-authoritative answer:
www.facebook.es canonical name = www.facebook.com.
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 31.13.83.36

angel@gonzalez27xc:~$
```



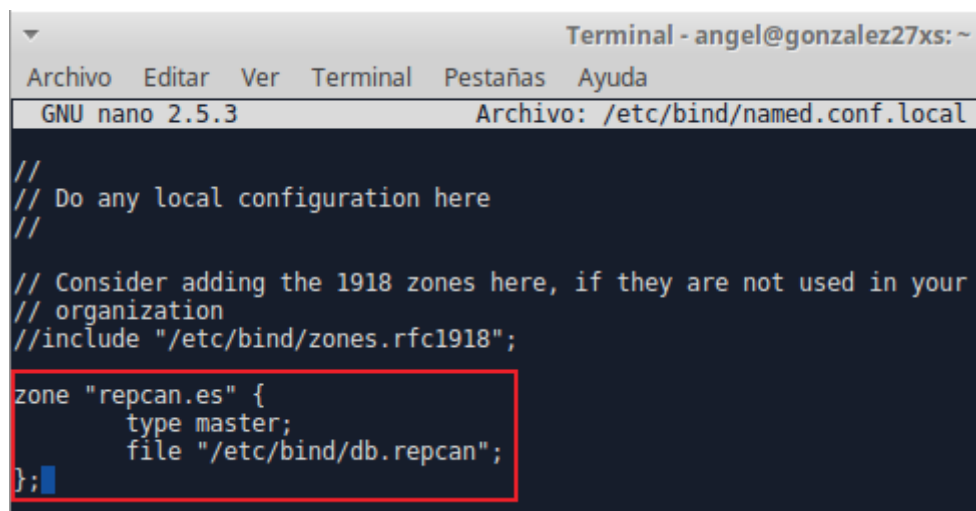
## 4. Configurar DNS Maestro (Master)

Ahora vamos a configurar el servidor como DNS maestro instalando un dominio ficticio (en mi caso, **repcan.es**).

Para comenzar, copiaremos el archivo de configuración que se encarga de esta tarea (/etc/bind/named.conf.local) para tener una copia por si pasa algún error. Usaremos el comando `cp` (requiere usuario *root*):

```
angel@gonzalez27xs:~$ sudo cp /etc/bind/named.conf.local /etc/bind/named.conf.local.copia
angel@gonzalez27xs:~$ ls -la /etc/bind | grep named.conf.local
-rw-r--r-- 1 root bind 165 abr 27 14:05 named.conf.local
-rw-r--r-- 1 root bind 165 oct 15 08:31 named.conf.local.copia
angel@gonzalez27xs:~$
```

Comenzaremos a crear la **zona de búsqueda directa** (ZBD). Para ello, editamos el fichero /etc/bind/named.conf.local con el comando `nano` (requiere usuario *root*) y escribimos lo siguiente:



```
Terminal - angel@gonzalez27xs: ~
Archivo Editar Ver Terminal Pestañas Ayuda
GNU nano 2.5.3 Archivo: /etc/bind/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 "repcan.es" {
    type master;
    file "/etc/bind/db.repcan";
};
```

Y para la **zona de búsqueda inversa** (ZBI), pondremos lo siguiente en el mismo fichero:

```
zone "19.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.19.172";
};
```

Con esto tendríamos las zonas de búsqueda directa e inversa ya creadas.

## 5. Crear archivos de búsqueda directa e inversa

### Zona de Búsqueda Directa

Es importante que el «file» haga referencia al fichero de configuración que importamos y que vamos a configurar ahora mismo. Vamos a copiar la base de datos que tenemos en «db.local» dando el nombre de «db.redlocal» que hemos definido en el fichero anterior, en mi caso, db.repcan. Usaremos el comando `cp` (requiere usuario `root`):

```
angel@gonzalez27xs:~$ sudo cp /etc/bind/db.local /etc/bind/db.repcan
angel@gonzalez27xs:~$ ls -la /etc/bind | grep db.
-rw-r--r-- 1 root root 237 abr 27 14:05 db.0
-rw-r--r-- 1 root root 271 abr 27 14:05 db.127
-rw-r--r-- 1 root root 237 abr 27 14:05 db.255
-rw-r--r-- 1 root root 353 abr 27 14:05 db.empty
-rw-r--r-- 1 root root 270 abr 27 14:05 db.local
-rw-r--r-- 1 root bind 270 oct 15 08:35 db.repcan
-rw-r--r-- 1 root root 3171 abr 27 14:05 db.root
angel@gonzalez27xs:~$
```

Modificamos el fichero de configuración que hemos adaptado a nuestro nombre de dominio y lo adaptamos a nuestros intereses. Usaremos el comando `nano` (requiere usuario `root`):

```
Terminal - angel@gonzalez27xs: ~
Archivo Editar Ver Terminal Pestañas Ayuda
GNU nano 2.5.3 Archivo: /etc/bind/db.repcan

;
; BIND data file for local loopback interface
$TTL 604800
@ IN SOA gonzalez27xs.repcan.es. root.repcan.es. (
        2      ; Serial
        604800 ; Refresh
        86400  ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS repcan.es.
@ IN MX 10 mail.repcan.es.

server A 172.19.27.253
printer A 172.19.27.250
pc1 A 172.19.27.251
pc2 A 172.19.27.252
www IN A 172.19.27.254
mail A 172.19.27.249
```

Una vez que hemos guardado el fichero de configuración, comprobamos la sintaxis con el comando `named -checkzone <redlocal> /etc/bind/db.<redlocal>`:

```
angel@gonzalez27xs:~$ named-checkzone repcan.es /etc/bind/db.repcan
zone repcan.es/IN: loaded serial 2
OK
```

Reiniciamos el proceso bind con el comando `service bind9 restart` (requiere usuario *root*):

```
angel@gonzalez27xs:~$ sudo service bind9 restart
angel@gonzalez27xs:~$
```

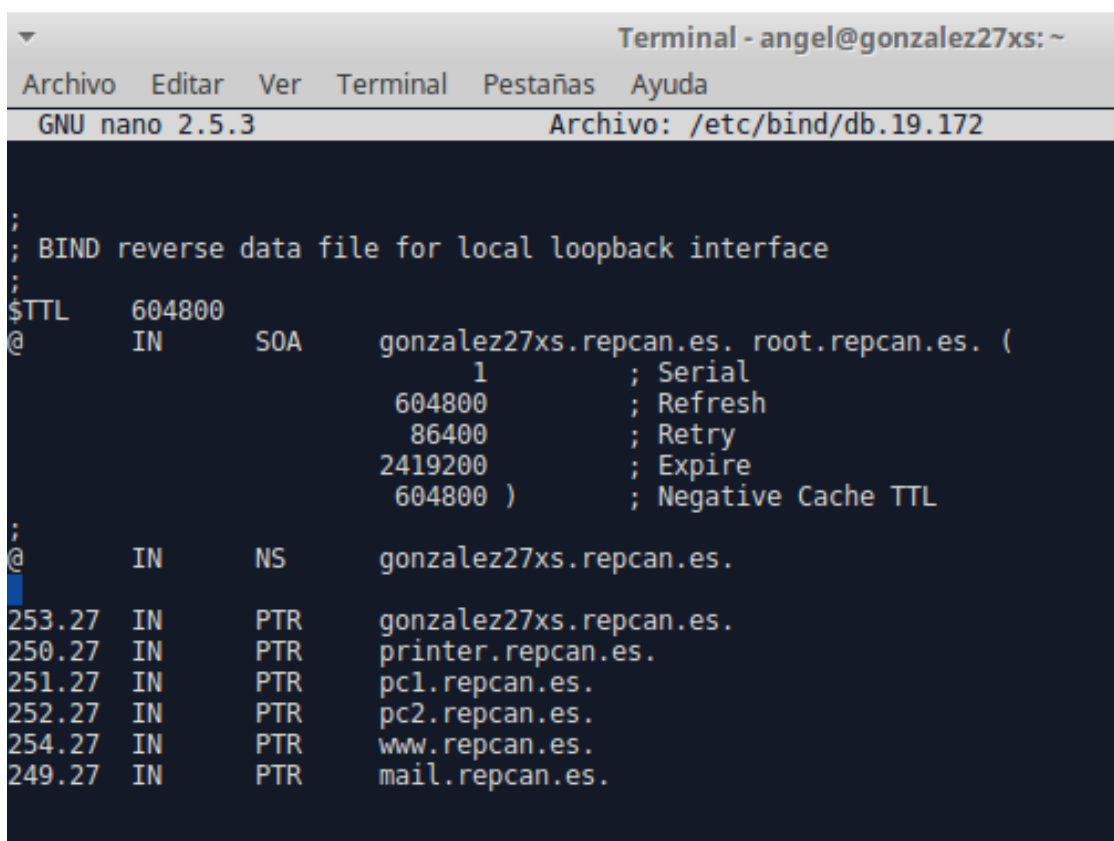
## Zona de Búsqueda Inversa

Ahora vamos a configurar el servidor DNS para que resuelva dominios a la inversa, poniendo la dirección IP y que nos diga a qué dominio pertenece dicha dirección IP.

Es importante que el «file» haga referencia al fichero de configuración que importamos y que vamos a configurar ahora mismo. Vamos a copiar la base de datos que tenemos en «db.127» dando el nombre de «db.ip-local» que hemos definido en el fichero anterior, en mi caso, db.19.172. Usaremos el comando `cp` (requiere usuario *root*):

```
angel@gonzalez27xs:~$ sudo cp /etc/bind/db.127 /etc/bind/db.19.172
angel@gonzalez27xs:~$ ls -la /etc/bind | grep 19.172
-rw-r--r--  1 root bind  271 oct 15 09:16 db.19.172
angel@gonzalez27xs:~$
```

Modificamos el fichero de configuración que hemos adaptado a nuestra IP y lo adaptamos a nuestros intereses. Usaremos el comando `nano` (requiere usuario *root*):



```
Terminal - angel@gonzalez27xs: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
GNU nano 2.5.3      Archivo: /etc/bind/db.19.172

;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@          IN      SOA      gonzalez27xs.repcan.es. root.repcan.es. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@          IN      NS       gonzalez27xs.repcan.es.
253.27     IN      PTR      gonzalez27xs.repcan.es.
250.27     IN      PTR      printer.repcan.es.
251.27     IN      PTR      pc1.repcan.es.
252.27     IN      PTR      pc2.repcan.es.
254.27     IN      PTR      www.repcan.es.
249.27     IN      PTR      mail.repcan.es.
```

Una vez que hemos guardado el fichero de configuración, comprobamos la sintaxis con el comando `named -checkzone <IP-server> /etc/bind/db.<ip-local>`:

```
angel@gonzalez27xs:~$ named-checkzone 172.19.27.253 /etc/bind/db.19.172
zone 172.19.27.253/IN: loaded serial 1
OK
```

Finalmente reiniciamos el proceso bind con el comando `service bind9 restart` (requiere usuario *root*):

```
angel@gonzalez27xs:~$ sudo service bind9 restart
angel@gonzalez27xs:~$
```

## 6. Comprobar resolución de nombres (servidor)

Ahora vamos a comprobar la resolución de nombres desde el servidor, tanto para las zonas de búsqueda directa como para las inversas. Se usará el comando `host`:

- ZBD:

```
angel@gonzalez27xs:~$ host gonzalez27xs.repcan.es
gonzalez27xs.repcan.es has address 172.19.27.253
angel@gonzalez27xs:~$ host printer.repcan.es
printer.repcan.es has address 172.19.27.250
angel@gonzalez27xs:~$ host pc1.repcan.es
pc1.repcan.es has address 172.19.27.251
angel@gonzalez27xs:~$ host pc2.repcan.es
pc2.repcan.es has address 172.19.27.252
angel@gonzalez27xs:~$
```

- ZBI:

```
angel@gonzalez27xs:~$ host 172.19.27.253
253.27.19.172.in-addr.arpa domain name pointer gonzalez27xs.repcan.es.
angel@gonzalez27xs:~$ host 172.19.27.250
250.27.19.172.in-addr.arpa domain name pointer printer.repcan.es.
angel@gonzalez27xs:~$ host 172.19.27.251
251.27.19.172.in-addr.arpa domain name pointer pc1.repcan.es.
angel@gonzalez27xs:~$ host 172.19.27.252
252.27.19.172.in-addr.arpa domain name pointer pc2.repcan.es.
angel@gonzalez27xs:~$ host 172.19.27.249
249.27.19.172.in-addr.arpa domain name pointer mail.repcan.es.
angel@gonzalez27xs:~$ host 172.19.27.254
254.27.19.172.in-addr.arpa domain name pointer www.repcan.es.
angel@gonzalez27xs:~$
```

## 7. Comprobar resolución de nombres (cliente)

Vamos a comprobar la resolución de nombres desde el cliente, tanto para las zonas de búsqueda directa como para las inversas. Se usará el comando `host`:

- ZBD:

```
angel@gonzalez27xc:~$ host printer.repcan.es
printer.repcan.es has address 172.19.27.250
angel@gonzalez27xc:~$ host pc1.repcan.es
pc1.repcan.es has address 172.19.27.251
angel@gonzalez27xc:~$ host pc2.repcan.es
pc2.repcan.es has address 172.19.27.252
angel@gonzalez27xc:~$ host gonzalez27xs.repcan.es
gonzalez27xs.repcan.es has address 172.19.27.253
angel@gonzalez27xc:~$
```

- ZBI:

```
angel@gonzalez27xc:~$ host 172.19.27.250
250.27.19.172.in-addr.arpa domain name pointer printer.repcan.es.
angel@gonzalez27xc:~$ host 172.19.27.253
253.27.19.172.in-addr.arpa domain name pointer gonzalez27xs.repcan.es.
angel@gonzalez27xc:~$ host 172.19.27.254
254.27.19.172.in-addr.arpa domain name pointer www.repcan.es.
angel@gonzalez27xc:~$ host 172.19.27.249
249.27.19.172.in-addr.arpa domain name pointer mail.repcan.es.
angel@gonzalez27xc:~$ host 172.19.27.251
251.27.19.172.in-addr.arpa domain name pointer pc1.repcan.es.
angel@gonzalez27xc:~$ host 172.19.27.252
252.27.19.172.in-addr.arpa domain name pointer pc2.repcan.es.
angel@gonzalez27xc:~$
```