

# CONFIGURACIÓN ZONAS SECUNDARIAS

**DNS**  
Domain Name System



DAVID SEGURA TRISTANCHO

2º ASIR

SRI

## INTRODUCCIÓN

En las siguientes páginas, vamos a realizar la configuración de un servidor DNS que, a su vez, va a ser secundario de otro servidor DNS. Todo ello va a efectuarse en Ubuntu. Dentro de cada servidor se dan las mismas zonas dentro de las redes originadas, eso sí, hay que saber designar al servidor primario su papel y al secundario el suyo.

### 1. Designar roles

Para empezar, dentro del directorio `/etc/bind` accedo al archivo `named.conf.local`. En el servidor primario queda de la siguiente manera:

```
GNU nano 4.8 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 "iespoligonosur.org" {
    type master;
    file "/etc/bind/db.iespsur";
    allow-transfer {10.10.10.4;};
    notify no;
};

zone "a100.iespoligonosur.org" {
    type master;
    file "/etc/bind/db.a100.iespsur.es";
    allow-transfer {10.10.10.4;};
    notify no;
};

zone "a101.iespoligonosur.org" {
    type master;
    file "/etc/bind/db.a101.iespsur.es";
    allow-transfer {10.10.10.4;};
    notify no;
};
```

Si observamos cada zona, `type master` hace alusión a la condición de maestro del servidor, mientras que dos líneas por debajo aparece `allow-transfer` seguido de una ip. Bien, `allow transfer` va a permitir la transferencia a la ip del servidor secundario. Al final de cada zona, aparece la directiva `notify`.

El estamento ***notify*** se utiliza para indicar si se enviarán o no, mensajes NOTIFY cuando recargamos una zona. Puede ir dentro de las cláusulas ***options***, ***zone*** y ***view***. Su sintaxis es la siguiente:

```
notify ( yes | no | explicit ) ;
```

Puede ser utilizado tanto en zonas maestras como esclavas. Si su valor es ***yes*** (valor por defecto), cada vez que carguemos una zona, se enviarán mensajes NOTIFY a todos los servidores de nombres definidos en los RR NS (menos a sí mismo), y a todos los equipos cuyas IP se listen en la sentencia ***also-notify***, que después explicaré. El servidor que recibe el mensaje NOTIFY procede como si el tiempo de refresco del registro SOA hubiera caducado.

Si el valor de *notify* es **no**, entonces se deshabilitan los mensajes NOTIFY. Y si el valor es **explicit**, solo se envían mensajes a las IP que se listen con la instrucción *also-notify*.

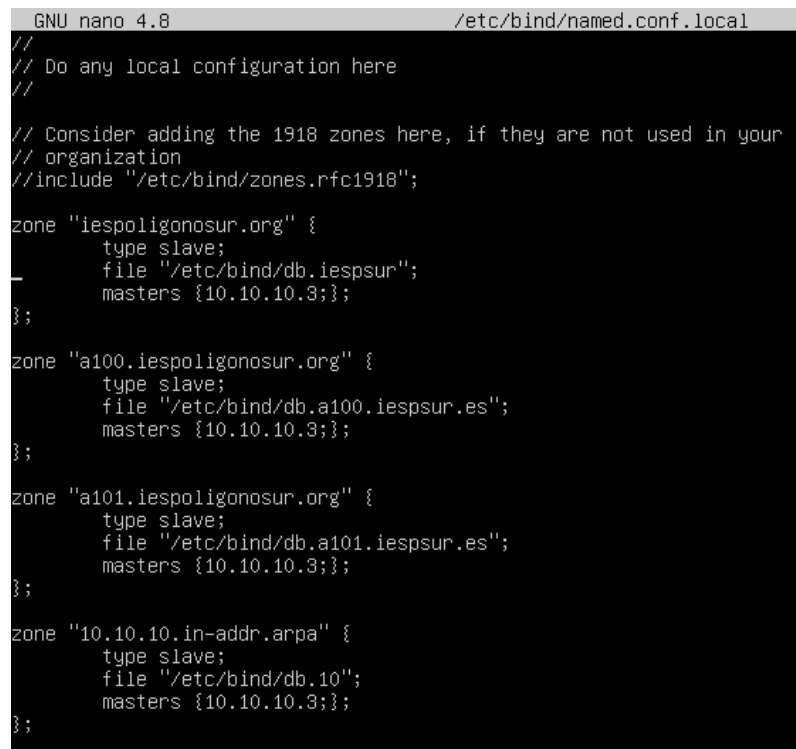
Si a nivel global establecemos *notify no*, dentro de una zona concreta podemos sobrescribirlo con la sentencia *also-notify*, permitiendo mensajes NOTIFY para dicha zona. También, si a nivel global ponemos un *also-notify*, y en una zona escribimos *notify no*, desactivaremos los mensajes NOTIFY solo para esa zona.

El mensaje NOTIFY en realidad no indica que la zona haya cambiado, sino que puede que haya cambiado. El receptor del mensaje lo que hará es solicitar el RR SOA y a través del número de serie sabrá si ha cambiado o no.

Si, por ejemplo, quisiéramos desactivar los mensajes NOTIFY en un servidor que solo tuviera zonas slave, en la cláusula *options* escribiríamos:

`notify no;`

¿Y el servidor secundario? ¿De qué manera se configuraría su archivo `named.conf.local`. Pues más o menos del siguiente modo:



```
GNU nano 4.8 /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 "iespoligonosur.org" {
    type slave;
    file "/etc/bind/db.iespsur";
    masters {10.10.10.3;};
};

zone "a100.iespoligonosur.org" {
    type slave;
    file "/etc/bind/db.a100.iespsur.es";
    masters {10.10.10.3;};
};

zone "a101.iespoligonosur.org" {
    type slave;
    file "/etc/bind/db.a101.iespsur.es";
    masters {10.10.10.3;};
};

zone "10.10.10.in-addr.arpa" {
    type slave;
    file "/etc/bind/db.10";
    masters {10.10.10.3;};
};
```

Solo cambiaríamos el `type`, que pasaría a ser `slave` (esclavo), y debajo de `file` añadimos `masters` seguido de la ip del dns primario.

## 2. Temporizador en el registro SOA

Como ya sabemos, cada zona cuenta con su propio archivo de configuración donde indicamos los dns existentes y los hijos que nacen de su zona.

```

GNU nano 4.8                                db.iespsur
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dns1.iespoligonosur.org. info.iespsur.es. (
                        5      ; Serial
                        60     ; Refresh
                        30     ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       dns1.iespoligonosur.org.
dns1      IN      A        10.10.10.3
www       IN      A        10.10.10.2
david     IN      A        10.10.10.18
dns2.iespoligonosur.org. IN      A        10.10.10.4
;@        IN      AAAA     ::1

```

En el registro SOA, donde especificamos el servidor primario, aparecen una serie de numeraciones que hacen alusión a los tiempos de refresco, reintento y expiración.

- **Refresh**

Indica el intervalo de tiempo tras el cual un servidor esclavo intentará actualizarse con la zona del servidor maestro. En este caso, le he dado sesenta segundos.

- **Retry**

Indica el intervalo de tiempo entre reintentos del servidor esclavo, para cuando la conexión con el servidor maestro tras el tiempo de refresco ha fallado. En este caso, le he dado treinta segundos.

- **Expire**

Indica el intervalo de tiempo que el servidor esclavo estará haciendo reintentos de conexión con el servidor maestro porque este no contesta. Hasta que no pase este tiempo, aunque el servidor esclavo no se pueda actualizar, responde a las consultas de forma autoritaria, pero llegado el momento de expiración, deja de contestar a las consultas de la zona que no ha podido actualizarse.

Para probar la conexión existente entre el servidor maestro y el esclavo, he cambiado el serial, de 2 a 5, y he añadido un nuevo hijo, david, así como su ip. Una vez hecho esto, veremos como el serial de la zona iespoligonosur.org, la que acabo de editar, se ha modificado haciendo uso del comando `cat /var/log/syslog | grep serial`.

```

Oct 26 13:49:34 usuario named[1204]: zone localhost/IN: loaded serial 2
Oct 26 13:49:34 usuario named[1204]: zone a100.iespoligonosur.org/IN: transferred serial 2
Oct 26 13:49:34 usuario named[1204]: zone a100.iespoligonosur.org/IN: sending notifies (serial 2)
Oct 26 13:49:34 usuario named[1204]: zone 10.10.10.in-addr.arpa/IN: transferred serial 2
Oct 26 13:49:34 usuario named[1204]: zone a101.iespoligonosur.org/IN: transferred serial 2
Oct 26 13:49:34 usuario named[1204]: zone a101.iespoligonosur.org/IN: sending notifies (serial 2)
Oct 26 13:49:34 usuario named[1204]: zone iespoligonosur.org/IN: transferred serial 5
Oct 26 13:49:34 usuario named[1204]: zone 168.192.in-addr.arpa/IN: transferred serial 2
Oct 26 13:49:34 usuario named[1204]: zone 168.192.in-addr.arpa/IN: sending notifies (serial 2)

```

No solo eso, si voy al servidor secundario y mediante el comando `dig` trato de dar con `david.iespoligonosur.org`, recibiré la correspondiente respuesta:

```

usuario@usuario:/etc/bind$ dig @10.10.10.4 david.iespoligonosur.org
; <<> DiG 9.16.1-Ubuntu <<> @10.10.10.4 david.iespoligonosur.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2758
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 675c68276dc2d6810100000063593de0e5817bc288351f41 (good)
;; QUESTION SECTION:
;david.iespoligonosur.org.      IN      A

;; ANSWER SECTION:
david.iespoligonosur.org. 604800 IN      A      10.10.10.18

;; Query time: 0 msec
;; SERVER: 10.10.10.4#53(10.10.10.4)
;; WHEN: mié oct 26 14:02:08 UTC 2022
;; MSG SIZE rcvd: 97

```

Como ha quedado comprobado, automáticamente el servidor secundario recibe la transferencia del primario, de su maestro.

### 3. Notificaciones

En el primer apartado, ya vimos algunas, pero en este punto vamos a hablar de otras directivas relacionadas con las notificaciones que interesa conocer:

- **Allow-notify**

Se aplica solamente a las zonas esclavas, y sirve para especificar las direcciones IP de los servidores de los que se aceptarán mensajes NOTIFY, e implícitamente de los que se actualizarán las zonas. Por defecto, solo se actualizarán zonas de aquellos servidores especificados en la sentencia *masters*.

- **Also-notify**

Se utiliza para especificar los servidores a los que se les enviarán mensajes NOTIFY cuando la zona maestra sea recargada. Puede ir dentro de las cláusulas *options*, *zone* y *view*. Su sintaxis simplificada en una zona es la siguiente:

```

zone "iespoligonosur.org" {
    type master;
    file "/etc/bind/db.iespsur";
    allow-transfer {10.10.10.4;};
    also-notify {10.10.10.5;};
    notify no;
};

```

Como puede apreciarse, se coloca justo debajo de `allow-transfer`, pues `allow-transfer` permite la transferencia y con `also-notify` podemos añadir un servidor secundario adicional dando su ip.

Por defecto los mensajes NOTIFY se envían a los servidores que constan en los RR NS de cada zona, y con *also-notify* se pueden especificar otros servidores.

- **Directiva acl**

Permite añadir las ip a las cuales voy a permitir la transferencia. Por ejemplo:

acl secundarios { 10.10.10.4; 10.10.10.5; }, y en allow transfer en lugar de poner la ip pongo directamente { secundarios; }, tal y como ya habíamos nombrado con acl.

