

DNS/BIND

Ivan E. Moore II.
rkrusty@tdyc.com

3 de febrero de 2000

Versión 1.0, 24/10/2000, JEV
Versión 1.1, 07/01/2001, MAV

Resumen

Esta es la traducción al español del capítulo 8 sobre DNS/BIND del Manual Debian de Administración de Redes (<http://www.debian.org/doc/manuals/network-administrator/>). La traducción al español ha sido realizada por David Charro Ripa <dcharro@iname.com>.

(Este artículo ha sido publicado por La Espiral y su versión mas reciente se puede encontrar en <http://www.laespiral.org>¹)

1. Introducción

Bienvenido. El propósito de esta sección es ayudar a configurar BIND en Debian. El documento empezará desde cero y le llevará a un sistema BIND completo y que funcione realmente. Tal y como pidieron algunas personas, he incluido instrucciones sobre cómo configurar un Dominio DNS desde un punto de vista tanto de Servidor Primario como de Servidor Secundario.

Además me he centrado sólo en BIND 8.x, ya que es la versión actual utilizada por Debian y es mucho mejor usarla. Si está usando BIND 4.x, le recomendaría actualizarse.

Por favor, tenga en cuenta que la mayoría de la gente no necesita tener BIND instalado en su sistema. De hecho solo los servidores lo necesitan realmente. De vez en cuando surgen ataques

1

Copyright 1998-2000 Ivan E. Moore II. Este manual es software libre. Puede redistribuirlo y/o modificarlo bajo los términos de la Licencia Pública General de GNU según es publicada por la Free Software Foundation (<http://www.fsf.org>), bien de la versión 2 de dicha Licencia o bien (según su elección) de cualquier versión posterior.

Este manual se distribuye con la esperanza de que sea útil, pero SIN NINGUNA GARANTÍA, incluso sin la garantía MERCANTIL implícita o sin garantizar la CONVENIENCIA PARA UN PROPÓSITO PARTICULAR. Véase la Licencia Pública General de GNU para más detalles.

Debería haber recibido una copia de la Licencia Pública General junto con este manual. Si no ha sido así, escriba a la Free Software Foundation, Inc., en 675 Mass Ave, Cambridge, MA 02139, EEUU. Añada también información sobre cómo contactar con usted mediante correo electrónico y postal.

(“exploits”) que cualquiera puede hacer, desde ataques por denegación de servicio a verdaderas situaciones comprometedoras para el root. La mayoría de los servidores DNS están incorrectamente configurados y acaban en estas situaciones. Si está configurando un sistema doméstico, no necesitará tener instalado BIND. Por favor, piénselo antes de seguir.

NOTA: La versión 8.2.1 de BIND y posteriores tiene una presentación diferente. Todos los ficheros de configuración relacionados con BIND están ahora en `/etc/bind`. Estos incluyen los ficheros de zona.

Por favor, lea 8 para una ayuda avanzada de BIND.

2. Conseguir los ficheros necesarios

Antes de nada, necesitará instalar los ficheros apropiados. Vaya al `dselect` e instale los siguientes ficheros:

Ficheros necesarios:

bind
dnsutils

Ficheros opcionales:

bind-doc
bind-dev
dns-browse
libnet-dns-perl
nslint
dhcp-dns
dnscvsutil

Si usa `apt-get`, entonces basta con ejecutar este comando:

```
apt-get install bind bind-doc dnsutils
```

3. Configurar BIND

3.1. bindconfig

Si ya ha instalado BIND y ha contestado a las preguntas durante la instalación, puede reconfigurar el sistema BIND básico tecleando **bindconfig**. Este programa configura sólo las opciones genéricas básicas. **bindconfig** es lo que ejecuta `dpkg` cuando instala BIND, de modo que lo que vamos a explicar es exactamente lo que se encontrará cuando instale BIND la primera vez. Así es como aparece.

Este programa no existe en las versiones de BIND 8.2.1 y posteriores. Debería reaparecer de nuevo en cualquier momento, pero por ahora ignore estos pasos si usa dichas versiones.

3.1.1. Paso 1

(Ignore este paso si es la primera instalación con `dselect` o con `apt-get`)

```
snowcrash:/var/named# bindconfig
```

It appears that you already have an /etc/named.conf file, suggesting that you have already configured BIND version 8.X at least once. If you proceed, a copy of this file will be saved, but no customizations that you have made to it will be included in the new configuration.

If this means nothing to you, go ahead and proceed with the remainder of the configuration process. If you have customized /etc/named.conf, you probably want to stop now to preserve your customizations.

```
Proceed to configure BIND, ignoring existing /etc/named.conf? [N]
```

3.1.2. Paso 2

```
BIND Configuration
```

```
-----  
By answering the following questions, you can configure BIND for your system.  
If your system has already been configured, the default values will allow you  
to verify your existing configuration.
```

```
Press [ENTER]
```

3.1.3. Paso 3

```
Forwarder Hosts
```

```
-----  
If you are close to a well-connected host or set of hosts which accept  
recursive DNS queries, it would be to your advantage to use them as forwarders  
in order to reduce traffic over links to outside servers.
```

Your DNS server will send all queries not in its cache to the forwarders first. Each forwarder will be asked in turn until an answer is returned or the list is exhausted. If no answer is forthcoming from a forwarder, the server will continue as it would have without the forwarders.

To answer this question, separate each address with a space, or answer 'none' to eliminate all forwarder hosts.

```
Forwarder IP addresses? []
```

Esta opción le permite redirigir cualquier petición DNS a otro servidor DNS. La razón por la que pudiera querer hacer esto es que se encontrara al otro lado de un cortafuegos y no pudiera alcanzar la red exterior directamente. Puede apuntar su servidor para que todas sus búsquedas las haga desde servidores dentro de su red que puedan acceder a la red exterior.

3.1.4. Paso 4

Localhost Entries

With this option, BIND will contain entries for the 'localhost' pseudo-host and its reverse mapping (127.0.0.1). This is recommended.

Enable localhost entries? [Y]

Usted necesita esto. Le permite asociaciones (“mappings”) hacia y desde su servidor local que es 127.0.0.1.

3.1.5. Paso 5

Configuration Complete

Advanced configuration, such as sortlists, xfrnets, limits, and other options can be accomplished by manually editing the /var/named/boot.options configuration file and reloading your nameserver. You may wish to refer to the named(8) man page or review the documentation in /usr/doc/net/named to assist in further customization.

This automatic configuration does not manipulate zone files; you should ensure the proper boot entries are made in /var/named/boot.zones for each primary and secondary zone you are serving. If you leave this file empty, your server will act conveniently as a caching-only name server.

```
Saving old /var/named/boot.options to /var/named/boot.options.old ...
Reading boot.zones ...
Reading boot.options ...
Rotated '/etc/named.conf' at Mon Dec 7 06:34:58 EST 1998.
Reload named now with the new configuration? [Y]
```

Toda su configuración básica ya está completa. Siga adelante y diga sí (“yes”) aquí para que se reinicie BIND.

3.2. *resolv.conf*

/etc/resolv.conf es el fichero que busca Linux para saber cómo debería realizar las búsquedas DNS. El formato es como sigue:

```
domain sudominio.com
search sudominio.com otrosdominios.com
nameserver 192.168.100.1
nameserver 127.0.0.1
```

La primera línea le dice en qué dominio está. Se puede omitir si quiere, pero recomendaría su uso. La segunda es un patrón de búsqueda. También puede omitirse, pero también recomendaría su utilización. Sin ella no podría buscar el nombre de una máquina sin tener que escribir su nombre de dominio completamente calificado, p.e. no podría buscar “beavis”. Debería buscar “beavis.otrodominio.com” (a menos que lo haya especificado en su fichero `/etc/hosts`).

Las líneas “nameserver” le dicen un orden de búsqueda de servidores DNS. Ya que estamos configurando BIND en su sistema, necesitará cambiar este fichero. Querrá que se parezca más al siguiente:

```
domain sudominio.com
search sudominio.com
nameserver 127.0.0.1
nameserver x.x.x.x
```

Reemplace “sudominio.com” con cualquier dominio que esté usando y sustituya la “x.x.x.x” con un servidor DNS de respaldo que pueda usar. (De este modo, si falla el suyo, aún podrá realizar búsquedas).

Guarde este fichero, y debería haberlo conseguido. Lo que esto le ofrece es la capacidad para buscar información DNS en Internet.

Por favor, diríjase a 5 para informarse sobre cómo preparar un Dominio DNS que funcione.

4. Configuración avanzada

4.1. `named.conf`

`named.conf` es el lugar donde le dice a BIND qué, dónde y cómo. Se trata del fichero de configuración principal de BIND. Antes de BIND 8.x este fichero se llamaba `named.boot`. Más abajo está el fichero `named.conf` que se crea tras la primera instalación de BIND.

```
// generated by named-bootconf.pl

options {
    directory "/var/named";
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
};

//
// Boot file for name server
```

```
//
// type          domain          source          file
zone "." {
    type hint;
    file "named.root";
};

// Zone boot information and daemon options are kept in other files
// (autoincluded from boot.zones)
//
// Name server zone boot file
// See named(8) for syntax and further information
//
// type          domain          source          file
// (autoincluded from boot.options)
//
// Options for name server
// Use 'bindconfig' to automatically configure this file
//
// type          domain          source          file
zone "localhost" {
    type master;
    file "named.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "named.rev-local";
};

// Custom configurations below (will be preserved)
```

El fichero `named.conf` es muy configurable. Simplemente con mirarlo ya se puede intuir cómo añadir un dominio nuevo. Para añadir un dominio nuevo sólo hay que poner al principio de su fichero `named.conf` lo siguiente:

```
zone "nuevodominio.com" {
    type master;
    file "nuevodominio.db";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "192.rev";
};
```

Reemplace “nuevodominio.com” con el nombre del dominio que DNS va a resolver y sustituya “100.168.192.in-addr.arpa” con la subred apropiada para la que llevará a cabo DNS inverso.

Observe el nombre de esta zona de búsqueda inversa: es el número de dirección IP de la red en orden inverso, seguido de `.in-addr.arpa`. Para más información sobre cómo funciona esto, por favor, vaya a la documentación de BIND 8.x situada en `/usr/doc`. (si instaló `bind-doc`) O pruebe con la URL BIND Online Documentation.

En el ejemplo anterior, “type” especifica si es un master o un esclavo de ese dominio. El tipo master quiere decir que su servidor DNS no pedirá a nadie más información sobre ese dominio. Otros sistemas pueden configurarse para realizar transferencias de zona (“zone-transfers”) de ese dominio. La transferencia de zona básicamente significa pasar la información a otro servidor DNS y así ser utilizado para realizar búsquedas DNS. En cambio, si va a extraer la información de otro servidor, necesitará usar el tipo esclavo (“type slave”).

“file” en el ejemplo de arriba especifica el nombre del fichero donde se guarda o se guardará la información. Estos ficheros se encuentran (o deberían encontrarse) por defecto en `/var/named` (a menos que cambie la sentencia “directory” en `/etc/named.conf`).

Por defecto BIND no está configurado con mucha seguridad y cualquiera puede extraer su información remotamente. Para controlar quién puede realizar transferencias de zona y así extraer información de su servidor, añada esta línea a su fichero `named.conf`:

```
allow-transfer "192.168.100.1"; /* this line */
```

Esta línea va dentro de la sección de opciones como por ejemplo:

```
options {
    directory "/var/named";
    allow-transfer "192.168.100.1";
};
```

Sustituya 192.168.100.1 con la dirección IP de aquellos servidores que quiera que sean capaces de realizar transferencias de zona de su servidor. NOTA: Esto no quiere decir que las personas no listadas aquí no sean capaces de hacer búsquedas de nombres de servidores en su servidor. Sólo significa que ellos tienen que conocer lo que están buscando. Tienen que saber un nombre o una dirección IP para hacer una búsqueda. No podrán extraer todos los datos guardados en sus ficheros de base de datos.

4.2. Archivos de zona

Los archivos de zona (o archivos de base de datos) son el corazón de su sistema BIND. Aquí está toda la información sobre qué nombre de host se asocia con qué dirección IP.

4.2.1. Archivos de zonas de dominio

Aquí tenemos un ejemplo para un fichero de dominio de `sudominio.com`. Por favor observe que se trata de un ejemplo muy genérico y que existen más características que se pueden incluir. Vaya a la documentación de BIND para obtener más ayuda de estas características.

```
;
; BIND data file for sudominio.com
;
@      IN      SOA      sudominio.com. root.sudominio.com. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Default TTL

      IN NS      dns.sudominio.com.
IN MX 10 mail.sudominio.com.

www  IN A 192.168.100.5
dns  IN A 192.168.100.10
mail IN A 192.168.100.20
```

Cualquier línea que comience con “;” (punto y coma) es un comentario y será ignorado por BIND. Las primeras 6 líneas son de configuración de la zona. Estas líneas dicen cuál es la zona (sudominio.com), quién es el responsable (root.sudominio.com, que es equivalente a root@sudominio.com) y alguna otra cosa más. Estas otras cosas incluyen un número de serie que nos dé una pista de cuándo se ha actualizado, cada cuánto actualizar la base de datos, cada cuánto reintentar una transferencia de zona, cuándo caduca la información de zona y un tiempo de vida por defecto. ***IMPORTANTE*** En el momento en que haga cambios a los ficheros de zona, debe incrementar el número de serie. Si no lo hace, puede haber problemas, sobre todo si es un servidor primario proporcionando información a sitios secundarios. La mayoría de esta información sólo se usa si tiene sistemas tanto maestros como esclavos.

Las dos líneas siguientes le dicen quién es el servidor DNS primario y quién debería coger el correo en este dominio. Puede tener múltiples líneas de cada uno de estos. Para añadir más servidores DNS tan solo hay que repetir exactamente lo que está listado, cambiando el servidor dns.sudominio.com por otro servidor DNS. Para añadir otro servidor de correo, haga lo mismo salvo que tiene un campo extra. El “10” en la línea MX establece la prioridad, los números bajos son los primeros. Esto quiere decir que, si tiene 2 líneas MX, una con 10 y la otra con 20, intentará enviar el correo a la lista MX con la prioridad 10 y si falla irá a la lista MX con la prioridad 20.

El resto del fichero de zona relaciona todas sus computadoras e IPs. Para más información de otras características y configuración de esta información pruebe con la documentación de BIND.

4.2.2. Ficheros inversos

Los ficheros de búsqueda inversa son casi iguales a los ficheros de dominio, pero con algunos pequeños cambios. Aquí hay un ejemplo de un fichero de búsqueda inversa.

```
;
; BIND reverse data file for 192.168.100.0
```

```
;  
@      IN      SOA      sudominio.com. root.sudominio.com. (  
                                1          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Default TTL  
;  
      IN      NS       dns.sudominio.com.  
  
5 IN PTR www.sudominio.com.  
10 IN PTR dns.sudominio.com.  
20 IN PTR mail.sudominio.com.
```

La primera sección de este fichero es exactamente la misma que la primera sección de los ficheros de zona de dominio. La sección de abajo es la diferente. Aquí estamos listando primero la última parte de la dirección IP y por tanto el nombre del puesto al final.

Aquí tiene que fijarse en dos detalles. Debe usar el nombre de dominio completamente cualificado y poner un punto al final de él. Estas 2 observaciones son importantes y el comportamiento será extraño de no hacerlo así. Otra posibilidad es usar “\$ORIGIN”, que es el nombre de dominio que se añade automáticamente a todos los nombres que no acaban en punto. El origen puede cambiarse el fichero db con \$ORIGIN. No olvide el punto final de \$ORIGIN.²

```
$ORIGIN sudominio.com.
```

5. Configurar un servidor primario de DNS

En el Servidor Primario de DNS es donde están las copias maestras de sus archivos DNS. Puede ser un solo sistema u otros servidores (Secundarios) pueden trabajar con él, llevando a cabo transferencias de zona. Una transferencia de zona es sólo eso, traspasar los archivos de zona de un sistema a otro. Así es como un servidor primario distribuye su información de zona a otros servidores.

Esta sección trata sobre cómo configurar su sistema Debian como servidor primario de DNS. Crearemos un dominio falso y configuraremos BIND para funcionar con ese dominio.

5.1. Preparación

Lo que haremos aquí sera crear un nuevo dominio. Para nuestros propósitos utilizaremos foo.org. En esta sección, prepararemos su sistema Debian para ser un servidor primario de foo.org.

Para una mejor comprensión del funcionamiento de todo esto, usaremos los siguientes servidores con sus correspondientes IP para los ejemplos.

² Paul Albitz, Cricket Liu: DNS and BIND, O'Reilly & Accosiates, Inc, 1a edic. julio 1994, pag. 136

```
www.foo.org = 192.168.100.10
news.foo.org = 192.168.100.20
mail.foo.org = 192.168.100.30
dns.foo.org = 192.168.100.40
dns2.foo.org = 192.168.100.50
```

Utilizando esto en nuestro ejemplo, dns.foo.org representará su servidor Debian. dns2.foo.org será usado 6. También habrá observado que estamos utilizando la subred 192.168.100.x. Para nuestros ejemplos aquí, también seremos maestro para esta subred.

5.2. Configurar BIND para su nuevo Dominio DNS

Ahora a configurar BIND. Como se muestra en 4, configurar BIND es bastante sencillo. De nuevo, no vamos a tratar ninguna configuración avanzada pero si desea ayuda, por favor, pruebe con BIND 8.0 Online Documentation.

5.2.1. archivos de zona

Primero necesitamos crear dos archivos. Uno para su dominio foo.org y otro para su subred 192.168.100.x. Empecemos con el archivo del dominio foo.org. Necesita crear un archivo llamado foo.db en /var/named. (Este archivo puede llamarse como quiera, pero lo hacemos así por el ejemplo). El archivo debería parecerse a algo como esto:

```
;
; BIND data file for foo.db
; /var/named/foo.db
;
@      IN      SOA      foo.org. root.foo.org. (
                        1998121401      ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200         ; Expire
                        604800 )        ; Default TTL

      IN NS      dns.foo.org.

      IN MX 10   mail.foo.org.

www  IN A 192.168.100.10
news IN A 192.168.100.20
mail IN A 192.168.100.30
dns  IN A 192.168.100.40
dns2 IN A 192.168.100.50
```

Observe, en el ejemplo anterior, que usamos como serie 1998121401. La razón principal por la que lo hacemos es tener una pista de cuándo fue modificado por última vez el archivo. Nos dice

que el archivo fue modificado por ultima vez el 14-12-1998 y que fue la primera vez en ese día. No hace falta que lo haga así, pero necesitará estar seguro de que aumenta la serie cada vez que lo modifica. (Especialmente si tiene Secundarios).

Ahora necesita crear su archivo de la subred 192.168.100.x. Cree un archivo llamado `192.168.100.db` en `/var/named`. Se parecerá necesariamente a algo como lo siguiente:

```
;
; BIND reverse data file for 192.168.100.0
; /var/named/192.168.100.db
;
@      IN      SOA      foo.org. root.foo.org. (
                                1998121401      ; Serial
                                604800          ; Refresh
                                86400           ; Retry
                                2419200         ; Expire
                                604800 )        ; Default TTL

      IN      NS       dns.foo.org.

10 IN PTR www.foo.org.
20 IN PTR news.foo.org.
30 IN PTR mail.foo.org.
40 IN PTR dns.foo.org.
50 IN PTR dns2.foo.org.
```

Por favor, tanga en cuenta el (.) al final de cada nombre de puesto. (ej. `www.foo.org.`) El punto DEBE estar allí, pues de otra manera BIND no leerá correctamente su zona.

5.2.2. `named.conf`

Ahora necesitamos añadir su nuevo dominio al archivo de configuración de BIND. Adelante, edite su archivo `/etc/named.conf` y añada las siguientes líneas al final.

```
zone "foo.org" {
    type master;
    file "foo.db";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "192.168.100.rev";
};
```

Guarde ese fichero y lo habrá hecho. Todo lo que tiene que hacer ahora es ejecutar `/etc/init.d/bind reload` y probarlo. Para ayuda sobre cómo comprobar BIND, por favor, revise 7.

6. Configurar un Servidor DNS Secundario

Un Servidor DNS Secundario es básicamente un servidor de respaldo. No mantiene las versiones maestras de la información de zona, sino copias. La mayoría de los sitios usan servidores Secundarios en ubicaciones remotas o para disminuir el trabajo del servidor Primario. El servidor Secundario realiza transferencias de zona en tiempos acordados, haciendo seguro que tenga las versiones más actualizadas de la información de zona.

6.1. Preparación

La gran diferencia al preparar un servidor Primario y otro Secundario es que sus archivos de zona ya están contruidos. Los únicos cambios que tiene que hacer es decirle a BIND en ambos sistemas que este servidor es uno Secundario y realizar las transferencias de zona.

6.2. Configurar BIND como un Servidor Secundario para su nuevo Dominio DNS

6.2.1. Cambios al Servidor Primario

Primero tenemos que hacer cambios a su servidor Primario de modo que conozca a su nuevo servidor Secundario. En el Primario, edite su archivo de dominio `foo.db` y añádale la siguiente línea: (Nota: aquí se muestra el archivo completo.)

```
;  
; BIND data file for foo.db  
; /var/named/foo.db  
;  
@      IN      SOA      foo.org. root.foo.org. (  
                1998121401      ; Serial  
                604800      ; Refresh  
                86400      ; Retry  
                2419200      ; Expire  
                604800 )      ; Default TTL  
  
                IN      NS      dns.foo.org.  
IN NS dns2.foo.org. ; ADD THIS LINE ***  
  
                IN      MX 10 mail.foo.org.  
  
www     IN      A      192.168.100.10  
news    IN      A      192.168.100.20  
mail    IN      A      192.168.100.30  
dns     IN      A      192.168.100.40  
dns2    IN      A      192.168.100.50
```

Ahora edite su archivo `/var/named/192.168.100.db` y haga lo mismo.

```

;
; BIND reverse data file for 192.168.100.0
; /var/named/192.168.100.db
;
@      IN      SOA      foo.org. root.foo.org. (
                                1998121401      ; Serial
                                604800          ; Refresh
                                86400           ; Retry
                                2419200        ; Expire
                                604800 )        ; Default TTL

      IN      NS       dns.foo.org.
IN NS dns2.foo.org. ; ADD THIS LINE ***

10     IN      PTR     www.foo.org.
20     IN      PTR     news.foo.org.
30     IN      PTR     mail.foo.org.
40     IN      PTR     dns.foo.org.
50     IN      PTR     dns2.foo.org.

```

Lo que consigue al añadir la nueva línea IN NS es decirle a BIND que dns2.foo.org también es un servidor DNS autorizado para foo.org y la subred 192.168.100.x. Con BIND 8.x esto también le dice a BIND que en cualquier momento que se haga un cambio a los archivos de zona, debe notificar a dns2.foo.org que se ha hecho un cambio de modo que dns2.foo.org pueda hacer una transferencia de zona.

Por favor, note que si ha configurado su servidor Primario solamente para permitir transferencias de zona desde anfitriones específicos, necesitará estar seguro de que dns2.foo.org está incluido en esa lista. (opción `allows-transfer` en `/etc/named.conf`.)

Puede volver a cargar BIND en su servidor Primario. (`/etc/init.d/bind reload`)

6.2.2. named.conf

Ahora necesita añadir información a su archivo `/etc/named.conf` en su servidor Secundario. Añada las siguientes líneas al final de `/etc/named.conf`:

```

zone "foo.org" {
    type slave;
    file "foo.db";
masters {
192.168.100.40;
};
};

zone "100.168.192.in-addr.arpa" {
    type slave;
    file "192.168.100.db";
masters {
192.168.100.40;
};
};

```

```
};  
};
```

Lo anterior le indica a BIND que su servidor es un esclavo (Secundario) de foo.org y la subred 192.168.100.x. También le dice a BIND que necesita para conseguir la información de zona (foo.db y 182.168.100.db) de 192.168.100.40, el cual es dns.foo.org.

6.2.3. Archivos de zona

Como se trata de un servidor Secundario, no hay necesidad de hacer nada con los archivos de zona. ¡PREMIO! Todo funcionará mientras tenga correctamente configurado su servidor Primario y su archivo named.conf esté configurado adecuadamente.

Lo ha conseguido. Cargue de nuevo su BIND y pruébelo. `/etc/init.d/bind reload`

6.2.4. Información

Ahora, cada vez que se modifiquen los archivos de zona del sitio del Primario y se incremente el número de serie, BIND enviará una notificación a todos los Secundarios (cualquier servidor en el archivo de zona con un registro IN NS) avisando que se ha hecho un cambio. Entonces el BIND de cada uno de estos servidores comparará sus propios archivos de zona para ver si tiene la misma versión o no. Si la versión que el Primario ha notificado es más reciente, entonces llevará a cabo una transferencia de zona y obtendrá la nueva versión.

Si todo está configurado adecuadamente, nunca necesitará hacer cambios en su servidor Secundario salvo para actualizar el propio BIND. Todos los cambios a partir de aquí se harán en el servidor Primario. La excepción es si se añade una nueva zona en el primario, tendrá que añadirla a los Secundarios también si quiere que sean Secundarios de la nueva zona.

7. Probarlo todo

Las pruebas son la parte fácil. Si ha seguido las directivas escritas aquí, todo funcionará. Lo primero que necesita antes de poder probar propiamente es cargar de nuevo la base de datos.

```
/etc/init.d/bind reload
```

Entonces debe seguir adelante, ejecutar **nslookup** y hacer algunas consultas

```
snowcrash:~# nslookup  
Default Server: localhost  
Address: 127.0.0.1
```

```
>
```

Cuando ejecute **nslookup**, debería parecerse al ejemplo anterior a menos que haya creado su propio dominio y esté usando una dirección IP diferente de 127.0.0.1. Debería poder escribir `www.debian.org` y, tras pensárselo un poco, devolverle la dirección IP de `www.debian.org`.

Si está siguiendo estas instrucciones para configurar un nuevo dominio, su **nslookup** se parecería más a esto:

```
snowcrash:~# nslookup
Default Server:  dns.foo.org
Address:  192.168.100.40
```

>

Ahora podría buscar cada uno de los puestos que añadimos a sus archivos de zona. (`www.foo.org`, `mail.foo.org`, etc...)

8. Dónde conseguir ayuda de BIND

Los siguientes sitios son buenas fuentes de ayuda para BIND:

- [ISC's BIND Site](#)
- [BIND Documentation Online](#)
- [Linux DNS HOWTO](#)