

Instalación y configuración del servidor DNS Bind

Luis Llorente Campo
Universidad de León, España

luisllorente@luisllorente.com

Este documento muestra cómo instalar y configurar el servidor dns Bind (<http://www.isc.org/products/BIND/>). Todo el proceso está pensado para la distribución Debian GNU/Linux. Pretende ser una guía que muestre el proceso de una forma genérica, teniendo que ser adaptado el proceso para cada situación específica.

Introducción

Se ha elegido el servidor dns Bind (<http://www.isc.org/products/BIND/>) por ser el más utilizado en el mundo y que dispone de muy abundante documentación sobre su configuración, contando además con características avanzadas como:

- Zonas firmadas (DNSSEC)
- Peticiones firmadas (TSIG)
- Soporte para IPv6
- Soporte de vistas (diferenciación de la respuesta según el origen)

que podrán ser puestas en marcha en un futuro si fuese necesario.

Instalación

Necesitamos instalar el paquete bind, y opcionalmente (aunque muy recomendable), la documentación del servidor, que se encuentra en el paquete bind-doc.

Para ello, ejecutaremos como es habitual en Debian el comando:

```
# apt-get install bind bind-doc
```

Una vez finalizada la instalación, pasaremos a configurar los distintos parámetros del servidor de nombres.

Configuración

El fichero de configuración es:

- /etc/bind/named.conf

Veremos cómo configurar el servidor para que los ordenadores de nuestra red local puedan resolver nombres de ordenadores conectados a Internet. También veremos cómo crear la configuración para poder asignar nombres a los ordenadores de la red local y de esta forma poder acceder a ellos más fácilmente.

Servidor

Debido a problemas burocráticos/administrativos, parte de lo que se esperaba hacer con el servidor DNS no se puede realizar. En concreto la parte relativa a tener un dominio propio para la Unidad de Imagen. Esto es debido a que no es posible alojar un dominio externo en la red RedIris.

Por este motivo, sólo se podrá utilizar el servidor DNS en la red local. Se configurará de modo que cachee las peticiones de los clientes para aumentar el rendimiento. Sólo podrán acceder a él los ordenadores situados en nuestra red local.

Para ello, en el fichero de configuración definiremos una lista de control de acceso (ACL) que estará compuesta por nuestra red local y el propio ordenador que hace de servidor:

```
acl miacl {
192.168.1.0/24;
127.0.0.1;
};
```

En la sección de opciones (options) diremos que sólo permitiremos hacer consultas, transferencias y escuchar en la ACL definida:

```
allow-transfer {
miacl;
};

allow-query {
miacl;
};

listen-on {
miacl;
};
```

Por último, configuraremos el servidor para que haga las peticiones a los servidores DNS de la universidad (así mejoramos la velocidad):

```
forwarders {
193.146.96.2;
193.146.96.3;
};
```

Con todo esto, ya tenemos el servidor listo para resolver nombres desde nuestra red local.

Nombres en la red local

Para poder resolver los nombres de los ordenadores de nuestra red local, deberemos crear dos zonas: una para la resolución directa y otra para la resolución inversa.

Nuestros ordenadores tendrán como nombre XXXXX.uimagen.iaf, por lo que la zona se llamará "uimagen.iaf". Y ya que se encuentran situados en el rango de IPs 192.168.1.x, la zona inversa deberá tener el nombre "1.168.192.in-addr.arpa". Añadiremos al fichero de configuración estas dos zonas de la siguiente forma:

```
zone "uimagen.iaf" {
    type master;
    file "/etc/bind/db.uimagen.iaf";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/rev.192.168.1";
};
```

Los ficheros:

- /etc/bind/db.uimagen.iaf
- /etc/bind/rev.192.168.1

almacenarán los datos de nuestros ordenadores. En el siguiente apartado veremos un ejemplo de estos dos ficheros.

Ejemplos de ficheros de configuración de Bind

Estos son los ficheros completos de configuración de uno de los servidores dns que hemos configurado. Se incluyen los comentarios originales para una mejor comprensión del significado de algunas de las directivas de configuración.

/etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//

acl miacl {
    192.168.1.0/24;
    127.0.0.1;
};

options {
```

```
directory "/var/cache/bind";

// 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 and later use an unprivileged
// port by default.

// query-source address * port 53;

// 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 {
193.146.96.2;
193.146.96.3;
};

allow-transfer {
miacl;
};

allow-query {
miacl;
};

listen-on {
miacl;
};

// reduce log verbosity on issues outside our control
logging {
category lame-servers { null; };
category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};
```

```
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

// add entries for other zones below here

zone "uimagen.iaf" {
    type master;
    file "/etc/bind/db.uimagen.iaf";
};

zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/rev.192.168.1";
};
```

/etc/bind/db.uimagen.iaf

```
;
; BIND data file for uimagen.iaf.
;
@      IN      SOA      uimagen.iaf. root.uimagen.iaf. (
                                2001131102; Serial
                                604800   ; Refresh
                                86400    ; Retry
                                2419200  ; Expire
                                604800 ) ; Default TTL
;
                                IN      NS      dns.uimagen.iaf.
;
www    IN      A       192.168.1.1
dns    IN      A       192.168.1.1
dns2   IN      A       192.168.1.2
ftp    IN      A       192.168.1.1
cancerbero  IN    A       192.168.1.1
sanpedro  IN    A       192.168.1.2
```

/etc/bind/rev.192.168.1

```
;
; BIND reverse data file for 192.168.1.0
;
@      IN      SOA      uimagen.iaf. root.uimagen.iaf. (
                        2001131102; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Default TTL
;
      IN NS     dns.uimagen.iaf.
      IN NS     dns2.uimagen.iaf.
1     IN PTR    www.uimagen.iaf.
1     IN PTR    ftp.uimagen.iaf.
1     IN PTR    dns.uimagen.iaf.
2     IN PTR    dns2.uimagen.iaf.
1     IN PTR    cancerbero.uimagen.iaf.
2     IN PTR    sanpedro.uimagen.iaf.
```

Prueba

Una vez esté todo configurado, pondremos en marcha el servidor mediante el comando:

```
# /etc/init.d/bind restart
```

A partir de este momento, podremos utilizar el servidor de nombres desde cualquier cliente conectado a nuestra red local. Una vez esté configurado el cliente para que coja como servidor DNS el que acabamos de configurar, podremos hacer alguna prueba ejecutando por ejemplo un **ping** a un sitio remoto:

```
ping www.google.com
```

Deberíamos ver cómo es capaz de resolver el nombre www.google.com y realizar el **ping**.

Para comprobar el funcionamiento del DNS en nuestra red local, haremos el **ping** a un equipo de la red local:

```
ping cancerbero.uimagen.iaf
```

Y al igual que el caso anterior, deberíamos ver cómo resuelve el nombre a una IP (en este caso la 192.168.1.1) y realiza el correspondiente **ping**.

Importante: No debemos olvidar que si se realiza alguna modificación a los ficheros de configuración del servidor, deberemos reiniciarlo para que lea la nueva configuración.

Más información

Se recomienda la lectura de toda la documentación que acompaña al servidor, siendo ésta una lectura muy útil, ya que la gestión de un servidor DNS no es una tarea sencilla.

Dicha documentación se encuentra en el directorio `/usr/share/doc/bind/`, e incluye también varios RFCs relativos al servicio DNS.

Otra fuente de información puede ser la página web oficial: <http://www.isc.org/products/BIND/>, en la cual existen enlaces a varias listas de correo y otras páginas web con recursos sobre este tema.

Sobre este documento

Se otorga permiso para copiar, distribuir y/o modificar este documento bajo los términos de la Licencia de Documentación Libre GNU, versión 1.1 o cualquier versión posterior publicada por la Free Software Foundation. Puedes consultar una copia de la licencia en <http://www.gnu.org/copyleft/fdl.html> (<http://www.gnu.org/copyleft/fdl.html>)

Este documento ha sido escrito en formato XML utilizando la DTD de DocBook (<http://www.docbook.org>). Mediante este sistema, puede ser fácilmente transformado a múltiples formatos (HTML, TXT, PDF, PostScript, LaTeX, DVI, ...). Se recomienda su utilización como herramienta de documentación potente y libre.