El servicio DNS

Sistema de Nombres de Dominios

Siempre que se utiliza un nombre para designar a un servidor, como sucede con *www.debian.org* o *www.una.ac.cr*, éste debe traducirse en la forma de una dirección *IP* única del mismo servidor. Este proceso se conoce como *resolución* y es efectuado gracias al *Domain Name System* (DNS) (o en español, Sistema de Nombres de Dominios).

Este sistema está constituido por una red global de servidores (13 servidores raíz), organizados en un árbol, donde cada servidor contiene una tabla de asociaciones entre los nombres de los servidores y sus respectivas direcciones *IP*.

¿Cómo funciona el DNS?

Supongamos que se pretende contactar el servidor www.google.com. El sistema iniciará una serie de contactos entre otros sistemas diversos, para encontrar cuál es la dirección asociada a la dirección pretendida.

Una versión muy simplificada sería la siguiente: posiblemente, el sistema tendrá que contactar a su servidor de *DNS*, que a su vez, contactará los servidores *DNS* de tope para indagar acerca del dominio "google.com", y enseguida contactar el servidor DNS de google para saber la dirección IP de www.google.com.

Aunque cada investigación o resolución tarda sólo milisegundos, la visualización de una página *web* en un *browser* puede resultar bastante penalizada por este proceso. Especialmente, cuando es posible que varios elementos de la página estén alojados en diversos servidores, cuyas direcciones deban ser resueltas individualmente.

Cache DNS o reenviador de consultas

Objetivo

Aunque las direcciones Internet tengan nombres “legibles” (www.google.com), éstos deben ser traducidos a la dirección *IP* (216.58.219.142) del respectivo servidor. Esa conversión es efectuada realizando una búsqueda en el *DNS* (*Domain Name System*).

Una *cache DNS* guarda localmente los resultados de esa búsqueda para utilización futura, evitando la repetición de búsquedas y aumentando drásticamente la velocidad de respuesta.

La herramienta de mayor uso se denomina BIND.

BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie comenzó a mantenerlo en 1988 mientras trabajaba para la DEC.

Una nueva versión de BIND (BIND 9) fue escrita desde cero en parte para superar las dificultades arquitectónicas presentes anteriormente para auditar el código en las primeras versiones de BIND, y también para incorporar DNSSEC (DNS Security Extensions). BIND 9 incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad. Es comúnmente usado en sistemas GNU/Linux.

Instalación de BIND9

```
root@server:~# apt-get install bind9 bind9-doc dnsutils
```

Configuración

La configuración generada durante la instalación es perfectamente funcional, no requiere modificaciones. Sin embargo, vamos personalizar la instalación en 2 aspectos principales: vamos a definir a cuáles servidores consultará el nuestro para pedir ayuda en la resolución de nombres, si no es posible hacer esto localmente (*forwarders*) y vamos a fortalecer algunos aspectos de seguridad.

Como *forwarders* podemos optar por varias hipótesis: una es utilizar los servidores *DNS* de nuestro proveedor de acceso a Internet.

Otra posibilidad muy interesante es utilizar uno de los diversos servicios públicos de *DNS* disponibles en la actualidad, como:

- ✓ OpenDNS
- ✓ Google Public DNS

Estos servicios prometen suministrar no sólo resoluciones más rápidas, sino también diversos servicios adicionales de seguridad, como filtros de direcciones maliciosos y otros más.

En este caso, utilizaremos los servidores *OpenDNS* (http://www.opendns.com).

Por seguridad sólo serán recibidas conexiones por la interfaz local o por la destinada a la red interna del servidor que se tiene configurado, acá un ejemplo, se debe adaptar a sus escenarios (*listen-on { 127.0.0.1; 192.168.1.100; };*). Así mismo, sólo serán contestados los pedidos de resolución que partan del propio puesto o de la red interna (*allow-query { 127.0.0.1; 192.168.1.0/24; };*). Todos los otros pedidos serán ignorados, para evitar eventuales utilizaciones abusivas de nuestro servidor *DNS* por parte de terceros.

La configuración está guardada en el archivo */etc/bind/named.conf.options*:

/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 {

             // OpenDNS servers

             208.67.222.222;

             208.67.220.220;

                };
```


```
        // Security options

        listen-on port 53 { 127.0.0.1; 192.168.1.100; };

        allow-query { 127.0.0.1; 192.168.1.0/24; };

        allow-recursion { 127.0.0.1; 192.168.1.0/24; };

        allow-transfer { none; };



//========================================================================
====

        // 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 auto;



        auth-nxdomain no;    # conform to RFC1035

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

};
```

Verificar si el archivo de configuración fue correctamente editado:

```
root@server:~# named-checkconf
```

Actualizar el archivo */etc/resolv.conf* para que la resolución de nombres se haga localmente:

/etc/resolv.conf

```
nameserver 127.0.0.1
```

Verificar también que en el archivo */etc/nsswitch.conf* la resolución de nombres pase también por el servicio *DNS*:

/etc/nsswitch.conf

```
# [...]

hosts:    files dns

# [...]
```

Reiniciar el servicio *DNS*:

```
root@server:~#  /etc/init.d/bind9 restart
```

Verificación

Para verificar la configuración, debe buscar la dirección IP de cualquier sitio en internet. El servidor *DNS* deberá mostrar nuestra dirección (*127.0.0.1*) y las direcciones *IP* del sitio buscado, se mostrarán de forma correcta:

```
root@server:~# nslookup www.debian.org

Server:         127.0.0.1

Address:        127.0.0.1#53



Non-authoritative answer:
```


```
Name:   www.debian.org

Addresses:

          2001:4f8:1:c::15

          2605:bc80:3010:b00:0:deb:166:202

          128.31.0.62

          149.20.4.15

          140.211.166.202
```

El proceso inverso, es decir, buscar un nombre a partir de una dirección *IP*, también debe funcionar:

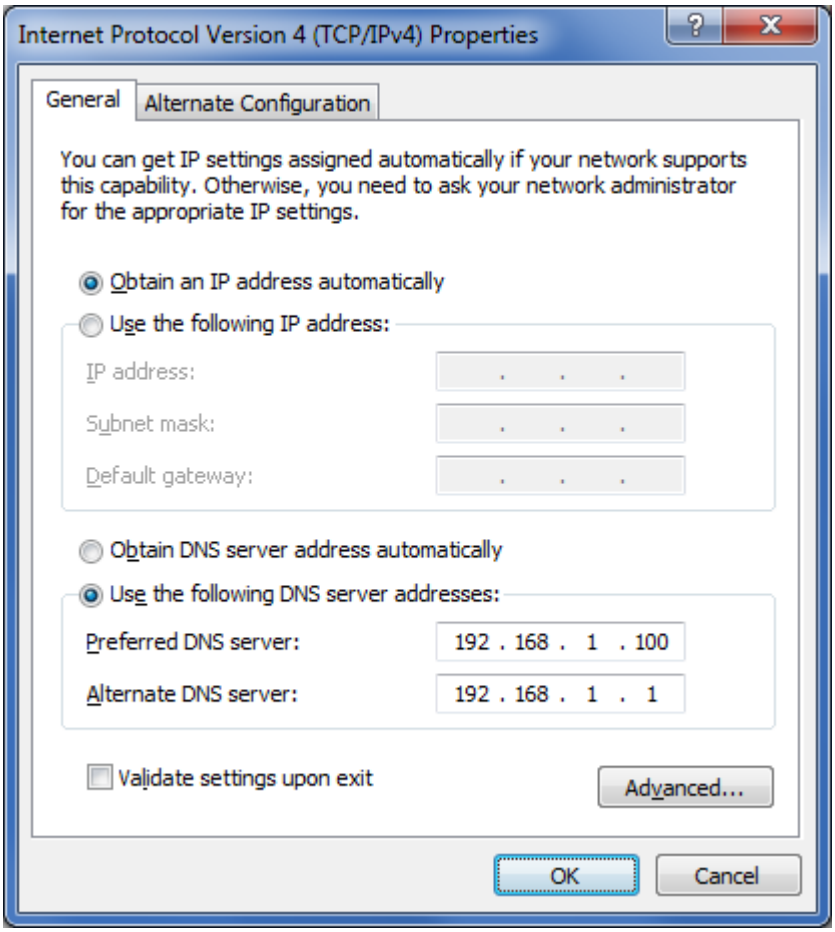
```
root@server:~# nslookup 5.153.231.4

Server:         127.0.0.1

Address:        127.0.0.1#53



Non-authoritative answer:

4.231.153.5.in-addr.arpa        name = senfter.debian.org.



Authoritative answers can be found from:

.       nameserver = j.root-servers.net.

.       nameserver = d.root-servers.net.

.       nameserver = a.root-servers.net.
```


```
.       nameserver = k.root-servers.net.

.       nameserver = e.root-servers.net.

.       nameserver = i.root-servers.net.

.       nameserver = l.root-servers.net.

.       nameserver = h.root-servers.net.

.       nameserver = b.root-servers.net.

.       nameserver = f.root-servers.net.

.       nameserver = g.root-servers.net.

.       nameserver = m.root-servers.net.

.       nameserver = c.root-servers.net.
```

Configuración de los clientes

Windows

Para los sistemas Windows, debe indicar, las propiedades del protocolo de Internet (*TCP(IP)*) de conexión de red, y debe determinar la dirección de nuestro servidor *DNS* (*192.168.1.100*) o (sea el caso de su servidor o máquina virtual)como servidor *DNS* preferido.



Linux

Para los sistemas Linux, se debe editar el archivo */etc/resolv.conf* para substituir o añadir el *nameserver* con la dirección *IP* de nuestro servidor:

```
# [...]

nameserver 192.168.1.100

# [...]
```

Sitios web consultados

- ISC Bind
- Wikipedia: Domain Name System
- Linux Home Networking: Quick HOWTO: Ch18 Configuring DNS
- DNS Howto, 3. A resolving, caching name server
- Securing Debian Manual
- OpenDNS
- Google Public DNS