JUNTA DE ANDALUCIA

CONSEJERIA DE EDUCACION
CEP Lora del Río

DNS dinámico

Alberto Molina Coballes, José Domingo Muñoz Rodríguez y José Luis Rodríguez Rodríguez

17 de marzo de 2010

Índice

1. Introducción

Es muy cómodo utilizar DHCP en una red local, pero tiene un inconveniente: no sabemos qué dirección tiene en cada momento un equipo. Una solución para esto es sincronizar el servidor DHCP con el DNS, creando lo que se denomina un servidor DNS dinámico (DDNS). Esta configuración permite que cada vez que se modifique una dirección IP, se registre el cambio en los ficheros que controlan la zona local y, de esta manera, poder acceder a un equipo a través de su nombre.

Vamos a utilizar un mismo equipo como servidor DHCP y DNS, por lo que la comunicación entre estos dos servicios será a través de localhost. Configuraremos incialmente DNS con RNDC, para la sincronización entre los dos servicios a través del puerto 953/tcp.

2. Instalación y configuración de Bind9

```
avatar:~# aptitude install bind9
```

El directorio /etc/bind/ contiene los siguientes ficheros:

```
-rw-r--r-- 1 root root  237 oct  7 23:47 db.0
-rw-r--r-- 1 root root  271 oct  7 23:47 db.127
-rw-r--r-- 1 root root  237 oct  7 23:47 db.255
-rw-r--r-- 1 root root  353 oct  7 23:47 db.empty
-rw-r--r-- 1 root root  270 oct  7 23:47 db.local
-rw-r--r-- 1 root root 2878 oct  7 23:47 db.root
-rw-r--r-- 1 root bind  907 oct  7 23:47 named.conf
-rw-r--r-- 1 root bind  165 oct  7 23:47 named.conf.local
-rw-r--r-- 1 root bind  572 oct  7 23:47 named.conf.options
-rw-r----- 1 bind bind   77 nov 13 13:57 rndc.key
-rw-r--r-- 1 root root 1317 oct  7 23:47 zones.rfc1918
```

Los ficheros named.conf.* eran originalmente sólo uno, ahora se modifican principalmente named.conf.options y named.conf.local, para incluir respectivamente las opciones de bind y la definición de las zonas locales.

El fichero rndc.key contiene una clave para el rndc, que será muy importante en la sincronización con el servidor DHCP:

/etc/bind/rndc.key

```
1 key "rndc-key" {
2 algorithm hmac-md5;
3 secret "S9QTPFn8zklrPHQ7z6XcOA==";
4 };
```

Obviamente la clave cambiará en cada equipo y se genera de forma automática al instalar bind9, aunque es posible generar una nueva clave mediante la instrucción *rndc-confgen*.

Para que bind utilice rndc, hay que incluir las siguientes líneas en alguno de los ficheros named.conf.*:

```
1 include "/etc/bind/rndc.key";
2
3 controls {
4 inet 127.0.0.1 port 953
5 allow { 127.0.0.1; } keys { "rndc-key"; };
6 };
```

de esta manera se permiten actualizaciones de las entradas DNS, pero sólo a quien facilite la clave y sólo desde localhost.

Nota: Conviene aclarar que el demonio de bind9 se denomina named y el usuario que lo ejecuta es *bind* (esto se especifica en el fichero */etc/default/bind9*). Lógicamente el usuario bind deberá tener los permisos pertinentes para actualizar los registros del DNS.

2.1. Creación de las zonas locales

Supongamos que queremos resolver las direcciones de nuestra red local, y que pertenecen al dominio *example.com*. Para ello editamos el fichero named.conf.local que inicialmente sólo tiene algunas líneas comentadas e incluimos las siguientes entradas:

/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 "example.com" {
  type master;
  file "db.example";
  allow-update { key "rndc-key"; };
  notify yes;
};

zone "2.168.192.in-addr.arpa" {
  type master;
  file "db.192.168.2";
  allow-update { key "rndc-key"; };
  notify yes;
};
```

Es decir, crearemos dos ficheros que incluirán las entradas para la resolución directa (*db.example*) e inversa (*db.192.168.2*), además se incluye la directiva “allow-update” para que puedan actualizarse las entradas DNS a través de rndc y se indica el nombre de la clave.

Los ficheros *db.example* y *db.192.168.2* se deben crear en el directorio de trabajo, que en este caso es */var/cache/bind*, aunque hay gente que prefiere modificar este directorio por */etc/bind*, en cualquier caso es importante asignar a estos ficheros el usuario y grupo propietario adecuado y los permisos siguientes:

```
-rw-rw-r-- 1 bind bind 313 nov 14 16:25 db.192.168.2
-rw-rw-r-- 1 bind bind 440 nov 14 16:25 db.example
```

Y su contenido podría ser (incluyendo sólo el propio servidor DNS de forma estática, ya que estará fuera del rango de direcciones IP que reparte el servidor DHCP):

/var/cache/bind/db.example

```
$ORIGIN example.com.
$TTL 86400 ; 1 day
@       IN      SOA     avatar   postmaster (
        1 ; serial
        21600 ; refresh (6 hours)
        3600 ; retry (1 hour)
```

```
        604800 ; expire (1 week)
        21600 ; minimum (6 hours)
)
        NS      avatar
avatar  A       192.168.2.1
```

/var/cache/bind/db.192.168.2

```
$ORIGIN 2.168.192.in-addr.arpa.
$TTL 86400 ; 1 day
@       IN      SOA     avatar   postmaster (
        200811131 ; serial
        21600 ; refresh (6 hours)
        3600 ; retry (1 hour)
        604800 ; expire (1 week)
        21600 ; minimum (6 hours)
)
        NS      avatar.example.com.
1       PTR     avatar.example.com.
```

2.2. Prueba de funcionamiento del servidor DNS

Utilizando algún cliente DNS (preferentemente dig), haremos consultas al servidor DNS local y comprobaremos si responde correctamente, por ejemplo:

```
avatar:~$ dig @127.0.0.1 avatar.example.com
```

```
; <> DiG 9.5.0-P2 <> @127.0.0.1 avatar.example.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29030
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;avatar.example.com.          IN        A

;; ANSWER SECTION:
avatar.example.com. 86400 IN    A       192.168.2.1

;; AUTHORITY SECTION:
example.com. 86400      IN      NS      avatar.example.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 17:27:49 2010
;; MSG SIZE  rcvd: 77
```

3. Instalación y configuración de dhcp3-server

```
avatar:~# aptitude install dhcp3-server
```

No se inicia y nos indica que busquemos el motivo en syslog, editamos el fichero */var/log/syslog* y encontramos la línea:

```
dhcpd: Not configured to listen on any interfaces!
```

Editamos el fichero */etc/default/dhcp3-server* y ponemos la interfaz de red por la que avatar debe ofrecer direcciones IP a sus clientes:

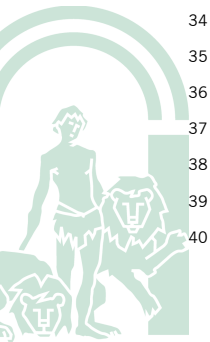
/etc/default/dhcp3-server

```
11 INTERFACES="eth1"
```

Ahora queda definir un rango de direcciones para el servidor DHCP y los parámetros que hay que entregar a los clientes:

/etc/dhcp3/dhcpd.conf

```
1  ##################################################
2  # Líneas para la actualización del servidor DNS:
3
4  server-identifier       avatar;
5  ddns-updates            on;
6  ddns-update-style       interim;
7  ddns-domainname         "example.com.";
8  ddns-rev-domainname     "in-addr.arpa.";
9  deny                    client-updates;
10
11 include                 "/etc/bind/rndc.key";
12
13 zone example.com. {
14 primary 127.0.0.1;
15 key rndc-key;
16 }
17
18 zone 2.168.192.in-addr.arpa. {
19 primary 127.0.0.1;
20 key rndc-key;
21 }
22
23 ##################################################
24 # Configuración general del servidor DHCP
25
26 default-lease-time 3600;
27 max-lease-time 86400;
28 authoritative;
29
30 ##################################################
31 # Se reparten las direcciones 192.168.2.2-192.168.2.127
32 # entre los clientes:
33
34 subnet 192.168.2.0 netmask 255.255.255.0 {
35   range 192.168.2.2 192.168.2.127;
36   option routers 192.168.2.1;
37   option domain-name "example.com.";
38   option domain-name-servers 192.168.2.1;
39   option broadcast-address 192.168.2.255;
40 }
```



4. Puesta en marcha de los servicios

Lo primero que haremos será parar ambos servidores y vaciar los ficheros de peticiones dhcp que se pudiesen haber generado:

```
avatar:~# /etc/init.d/bind9 stop
avatar:~# /etc/init.d/dhcp3-server stop
avatar:~# echo "" > /var/lib/dhcp3/dhcpd.leases
avatar:~# echo "" > /var/lib/dhcp3/dhcpd.leases~
```

Ponemos en marcha de nuevo los dos servidores y realizamos una petición DHCP desde un cliente de la red, abrimos el fichero /var/log/syslog y si todo va bien nos aparecerán líneas como:

```
avatar dhcpd: DHCPDISCOVER from 00:11:09:60:c6:ec via eth2
avatar dhcpd: DHCPOFFER on 192.168.2.2 to 00:11:09:60:c6:ec (cliente) via eth2
avatar named[4596]: client 127.0.0.1#51880: signer "rndc-key" approved
avatar named[4596]: client 127.0.0.1#51880: updating zone 'example.com/IN': adding an RR at cl...
avatar named[4596]: client 127.0.0.1#51880: updating zone 'example.com/IN': adding an RR at 'c...
avatar named[4596]: journal file db.example.jnl does not exist, creating it
avatar dhcpd: Added new forward map from cliente.example.com. to 192.168.2.2
avatar named[4596]: client 127.0.0.1#39603: signer "rndc-key" approved
avatar named[4596]: client 127.0.0.1#39603: updating zone '2.168.192.in-addr.arpa/IN': deleti...
avatar named[4596]: client 127.0.0.1#39603: updating zone '2.168.192.in-addr.arpa/IN': adding...
avatar named[4596]: journal file db.192.168.2.jnl does not exist, creating it
avatar named[4596]: zone 2.168.192.in-addr.arpa/IN: sending notifies (serial 200811133)
avatar dhcpd: added reverse map from 2.2.168.192.in-addr.arpa. to cliente.example.com.
avatar dhcpd: DHCPREQUEST for 192.168.2.2 (127.0.1.1) from 00:11:09:60:c6:ec (cliente) via eth2
avatar dhcpd: DHCPACK on 192.168.2.2 to 00:1d:09:60:c6:ec (cliente) via eth2
```

También podemos comprobar que se han creado dos nuevos ficheros en el directorio de trabajo de bind:

```
-rw-r--r-- 1 bind bind 844 nov 14 18:08 db.192.168.2.jnl
-rw-r--r-- 1 bind bind 911 nov 14 18:08 db.dominio.jnl
```

5. Configuración de los clientes DHCP

El principal requisito que debe cumplir un cliente DHCP para funcionar en este entorno es que debe enviar el nombre del host (hostname) en la petición inicial. El cliente más habitual en las distribuciones linux es dhcp3-client, que no viene configurado inicialmente para enviar el hostname. Para solucionar esto editamos el fichero /etc/dhcp3/dhclient.conf e incluimos la línea:

/etc/dhcp3/dhclient.conf

```
16 send host-name cliente;
```

donde hay que sustituir en cada caso *cliente* por el nombre del equipo.