Configuración Servidor DNS Centos 7

Autor: Pablo Andrés Bernabéu Soler

En esta práctica se instalará y configurará un servidor DNS. Para ello, se seguirán los siguientes pasos:

1. Pasos Previos
2. Instalación Servicio DNS (En Centos 7)
3. Configuración del servidor Cache
4. Configuración del servidor principal
5. Configuración con dos servidores: Uno principal y otro esclavo
6. Configuración como servidor secundario, el servidor dnsC en Centos
7. Configuración servidor principal Centos, servidor secundario Windows

1. Pasos Previos

Proceda a usar la instantánea del servidor y cliente en Centros antes de la instalación de cualquier servicio.

1. Indique direccionamiento estático. Para las diferentes tarjetas de red tal como procedió en la práctica de configuración del Servicio DNS.
2. Coloque de momento como DNS los DNS de la UPV.
3. Nombre a la máquina como dnsC.grupoXX.net

Verifique que la tabla de encaminamiento es correcta.

2. Instalación Servicio DNS (En Centos 7)

Una vez cumplimentados los puntos anteriores, procedemos a la instalación del servicio DNS.

Ejecute el comando yum install –y bind bind-utils

A continuación habilitamos e iniciamos el servicio.

```
systemctl enable named
systemctl start named
```

Podemos parar el servicio con *systemctl stop named* o pararlo y reiniciarlo con el comando *systemctl restart named*

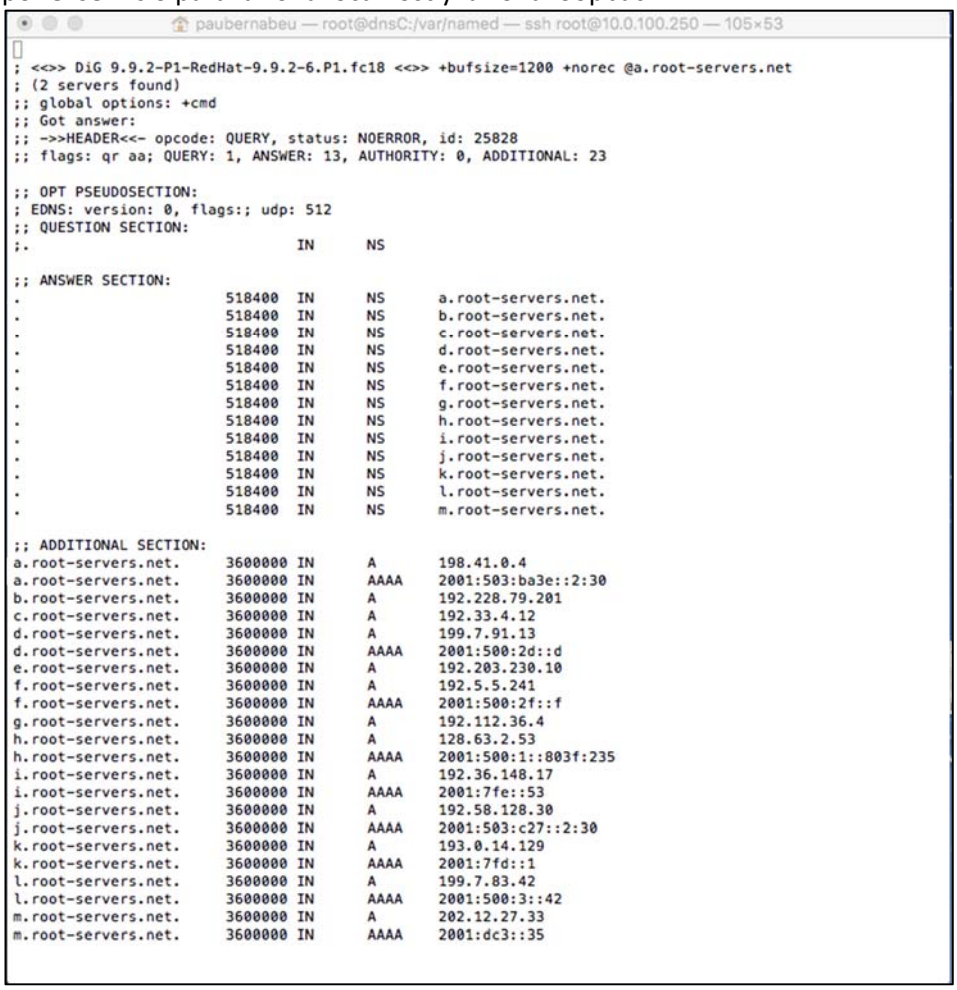
Tras la instalación podemos comprobar que se han creado diferentes directorios y ficheros.

El directorio named dentro de /var (/var/named/)

El cual presenta tres directorios /data y /dynamic y slaves. Este último es para guardar los ficheros de zona cuando actúe de DNS secundario o esclavo (slave).

Tenemos además tres ficheros.

En named.ca queda guardada la información de los 13 directorios raíz. En named.empty tenemos un fichero que podemos usar para crear nuestras zonas, así como dos ficheros de configuración usados por el servicio para la zona localhost y la zona loopback.




```
; <<>> DiG 9.9.2-P1-RedHat-9.9.2-6.P1.fc18 <<>> +bufsize=1200 +norec @a.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25828
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 23

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3600000 IN      A       198.41.0.4
a.root-servers.net.     3600000 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3600000 IN      A       192.228.79.201
c.root-servers.net.     3600000 IN      A       192.33.4.12
d.root-servers.net.     3600000 IN      A       199.7.91.13
d.root-servers.net.     3600000 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3600000 IN      A       192.203.230.10
f.root-servers.net.     3600000 IN      A       192.5.5.241
f.root-servers.net.     3600000 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3600000 IN      A       192.112.36.4
h.root-servers.net.     3600000 IN      A       128.63.2.53
h.root-servers.net.     3600000 IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     3600000 IN      A       192.36.148.17
i.root-servers.net.     3600000 IN      AAAA    2001:7fe::53
j.root-servers.net.     3600000 IN      A       192.58.128.30
j.root-servers.net.     3600000 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3600000 IN      A       193.0.14.129
k.root-servers.net.     3600000 IN      AAAA    2001:7fd::1
l.root-servers.net.     3600000 IN      A       199.7.83.42
l.root-servers.net.     3600000 IN      AAAA    2001:500:3::42
m.root-servers.net.     3600000 IN      A       202.12.27.33
m.root-servers.net.     3600000 IN      AAAA    2001:dc3::35
```

Todos estos ficheros son direccionados desde el fichero de configuración.

/etc/named.conf en según qué casos más otros fichero de zona que podemos añadir.

Para poder completar y que nuestro servidor DNS resuelva nombres preguntando a los raíz hemos de proceder del siguiente modo: *vi /etc/named.conf*

paubernabeu — root@dnsC:~ — ssh root@10.0.100.250 — 126×60

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1;10.XX.99.250;}; //<--Añadimos la IP de nuestro servidor DNS 10.X.99.250
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 10.XX.99.0/24;}; //<--Anadimos la red a la que resolvera DNS, podemos colocar 'any'


        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

-- INSERT --
```

Donde le hemos indicado que escuche el puerto 53 en la IP 10.XX.99.250, y que permita preguntar a todos los dispositivos que pertenezcan a la red 10.XX.99.0/24.

Podemos ir añadiendo tantos servidores y redes que consideremos. Si quisiéramos dar respuesta a cualquier red.

```
allow-query {any};
```

Cambie los DNS de la UPV por los DNS propios 10.0.99.250 y 10.0.99.249:

```
[root@dnsC ~]# vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
DNS1=10.0.99.250
DNS2=10.0.99.249
```

Reinicie la red:

```
[root@dnsC ~]# systemctl restart network
```

Verifique que los servidores DNS sean correctos:

```
root@dnsC ~]# vi /etc/resolv.conf


# Generated by NetworkManager
search group0.net
nameserver 10.0.99.250
nameserver 10.0.99.249
```

Reinicie servicio DNS

```
[root@dnsC ~]# systemctl restart named
```

Podemos comprobar que el servicio está en funcionamiento consultando qué procesos el servidor tiene conectados y hacer una búsqueda de la cadena *bind* en la respuesta de la manera siguiente.

```
[root@dnsC ~]# ps -aef | grep named

named  4741     1  0 20:43 ?   00:00:00 /usr/sbin/named -u named
root   4791  4774  0 20:48 pts/0   00:00:00 grep --color=auto named
```

En caso que el servicio no respondiera a una orden de parada, se podría matar con la orden kill-9 y el número del proceso asociado.

```
[root@dnsC ~]# kill -9 4741
```

Si lo matamos volvemos a iniciar el servicio DNS

Probamos que funciona haciendo ping wwww.google.es

Otra comprobación que se puede hacer es consultar cuales son los puertos que el servidor gestiona. Para que la consulta sea más clara se puede parametrizar que la orden muestre cual es el proceso que gestiona el puerto y que indique el número del mismo.

Previamente instalaremos:

```
[root@dnsC ~]# yum install netstat
```

Ejecutamos:

```
root@dnsC ~]# netstat -pan |more
```

```
Proto Recv-Q Send-Q  Local Address      Foreign Address     State       PID/Program name
tcp   0      0       10.0.99.250:53     0.0.0.0:*           LISTEN      2511/named
tcp   0      0       127.0.0.1:53       0.0.0.0:*           LISTEN      2511/named
tcp   0      0       10.0.100.250:22    0.0.0.0:*           LISTEN      1292/sshd
tcp   0      0       127.0.0.1:953      0.0.0.0:*           LISTEN      2511/named
tcp   0      0       127.0.0.1:25       0.0.0.0:*           LISTEN      2453/master
tcp   0      0       10.0.100.250:22    0.0.100.100:49225   ESTABLISHED 2478/sshd:root@pts
tcp6  0      0 ::1:53                  :::*                LISTEN      2511/named
tcp6  0      0 ::1:953                 :::*                LISTEN      2511/named
udp   0      0       10.0.99.250:53     0.0.0.0:*                       2511/named
udp   0      0       127.0.0.1:53       0.0.0.0:*                       2511/named
udp6  0      0 ::1:53                  :::*                            2511/named
```

Recordad: En este caso el servidor DNS consulta a los servidores RAIZ, tanto para la resolución directa como inversa.

3. Configuración del servidor Cache

Para que un servidor DNS funcione como cache hay que configurar que servidores hemos de consultar, denominados reenviadores (forwarders). Esta información nuevamente la hemos de indicar en: /etc/named.conf

Abrimos el fichero e indicamos los servidores DNS de la UPV: 158.42.250.65; 158.42.250.195 y el de google 8.8.8.8 por ejemplo, para ello añadimos la línea forwarders {158.42.250.65; 158.42.250.195; 8.8.8.8;};

Además le podemos añadir la línea para que solo solicite información a los reenviadores. **forward only;**

```
options {
        listen-on port 53 { 127.0.0.1;10.0.99.250;};
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 10.0.99.0/24;};
        forwarders {158.42.250.65; 158.42.250.195; 8.8.8.8;};
        forward only;
…
};
```

Para verificar que consulta a los renviadores podemos comentar la zone "." en el fichero de configuración del servicio. Para comenta /*…*/

```
/*zone "." IN {
        type hint;
        file "named.ca";
};*/
```

Guardamos y reiniciamos el servicio,

Y hacemos ping a www.google.com, por ejemplo y deberemos obtener respuesta.

Vamos a comprobar ahora el funcionamiento del sistema desde el cliente: Abrimos la máquina cliente de Centos, que ya tenemos creada, verificamos tiene IP y que los servidores DNS son 10.XX.99.250 y 10.XX.99.249.

Introducimos la orden nslookup, si no está disponible instalamos bind-utils

```
[root@client ~]# yum install dns-utils
```

Ya podremos usar el comando nslookup. Si bien, ya podemos usar comando específico de *Red Hat 7* getent con la opción hosts:

```
[root@client ~]# getent hosts www.google.com
```

2a00:1450:4003:806::2004 www.google.com

Si observamos nos da sólo una IP y en este caso la IPv6, podemos forzar a que me dé todas las posibles IP relacionados con dicho DNS que sean IPV4

```
[root@client ~]# getent ahostsv4 www.google.com
216.58.201.132  STREAM www.google.com
216.58.201.132  DGRAM
216.58.201.132  RAW
```

O todas, tanto de IPv4, como de IPv6

```
[root@client ~]# getent ahosts www.google.com
216.58.214.164  STREAM www.google.com
216.58.214.164  DGRAM
216.58.214.164  RAW
2a00:1450:4003:806::2004 STREAM
2a00:1450:4003:806::2004 DGRAM
2a00:1450:4003:806::2004 RAW
```

Si usamos nslookup (conviene ir usando los nuevos comandos de red Hat 7). Si usamos la orden server nos indica los servidores DNS actualmente configurados (recordad el servidor Windos2012, está apagado).

```
[root@client ~]# nslookup
> server
Default server: 10.0.99.250
Address: 10.0.99.250#53
Default server: 10.0.99.249
Address: 10.0.99.249#53
>
```

Preguntamos por www.google.com,

```
> www.google.com
Server:         10.0.99.250
Address:  10.0.99.250#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.210.132
>
```

La respuesta es no autoritativa, porque nuestro servidor no tiene autoridad sobre la base de datos del dominio consultado.

Como ya hemos comprobado vamos a quitar comentario a que en caso de fallo de los reenviadores acceda a los servidores DNS raíz.

[root@dnsC /]# vi /etc/named.conf

Descomentamos, quitamos /* y */

/*zone "." IN { type hint; file "named.ca"; };*/	**zone "." IN {** **type hint;** **file "named.ca";** **};**

Guardamos y reiniciamos el servicio:

[root@dnsC /]# systemctl restart named

4. Configuración del servidor principal

En este punto configuramos el servidor denominado dnsC como un servidor principal del dominio grupoXX.net (en este caso grupo0.net)

El primer paso consiste en indicar que este es un servidor principal y donde se ha aguardado la configuración del dominio de zona.

Abrimos el fichero *named.conf*

[root@dnsC /]# vi /etc/named.conf

Este fichero nos indica donde debemos guardar el fichero de configuración de zona, en concreto en lo que nos indica en la línea indicada, podemos dejarlo en subdirectorios a partir de esta referencia.

directory "/var/named";

Tal como vimos en el punto 2 de la presenta práctica. Pero es una buena práctica no añadir nada en este fichero sobre la configuración de las zonas. Si observamos al final del mismo nos aparece.

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

Por tanto tenemos incluido un fichero específico de zonas. Podríamos crear uno y con la directiva include añadirlo a namend.conf. Y ese fichero establecer la zona del servidor principal.

En nuestro cado vamos a añadir la zona directa e inversa en el fichero

/etc/named.rfc1912.zones

Abrimos pues el fichero, vi /etc/named.rfc1912.zones

Al final del mismo añadimos la zona de resolución directa que llamaremos grupoXX.net y la zona de resolución inversa que llamaremos 99.XX.10.in-addr.arpa sobre la que vamos a ser maestros,

con el comando type. Con el comando file indicamos qué nombre van a tener los ficheros de zona respectivamente:

```
//Add zones
zone "grupo0.net" IN{
        type master;
        file "named.grupo0.net";
        allow-update {none;};
};
zone "99.0.10.in-addr.arpa" IN {
        type master;
        file "named.99.0.10";
        allow-update {none;};
};
```

Guardamos.

Podemos chequear que no hay errores en el fichero named.rfc1912.zones usando el comando named-checkconf. Si nos no devuelve ningún mensaje es que todo está correcto.

```
root@dnsC /]# named-checkconf /etc/named.rfc1912.zones
[root@dnsC /]#
```

Recordad que debéis comentar las líneas los reenviadores en para que deje de ser un servidor caché en el fichero named.conf

Como hemos señalado anteriormente, en el fichero /etc/named.conf se pueden definir directamente las zonas para las que nuestro servidor va ser autorizado.

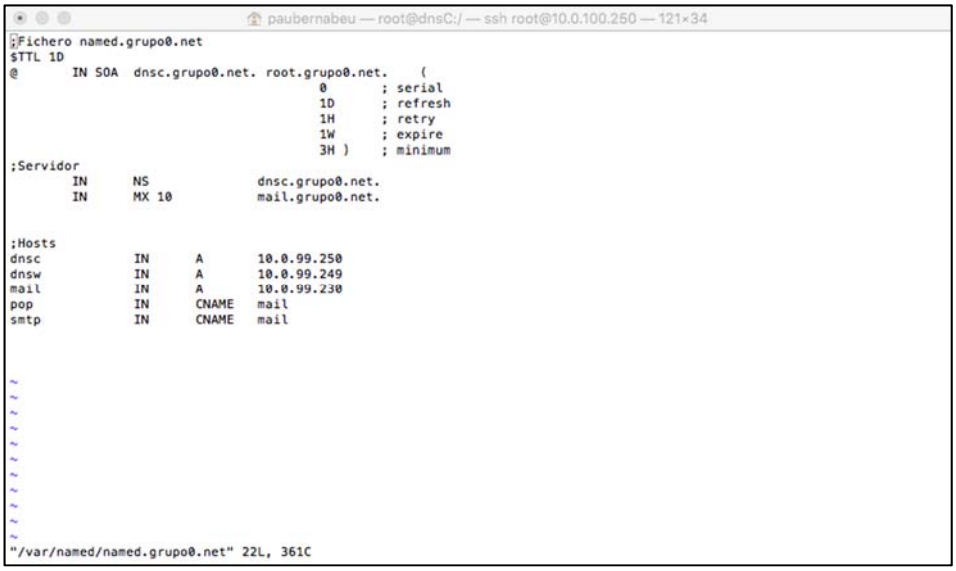
Sabemos además que el servidor va a consultar los ficheros de zona en /var/named por defecto. De modo que es allí donde tenemos que crear estos ficheros.

Para crear los ficheros de zona podemos valernos de la plantilla named.localhost y editarla:

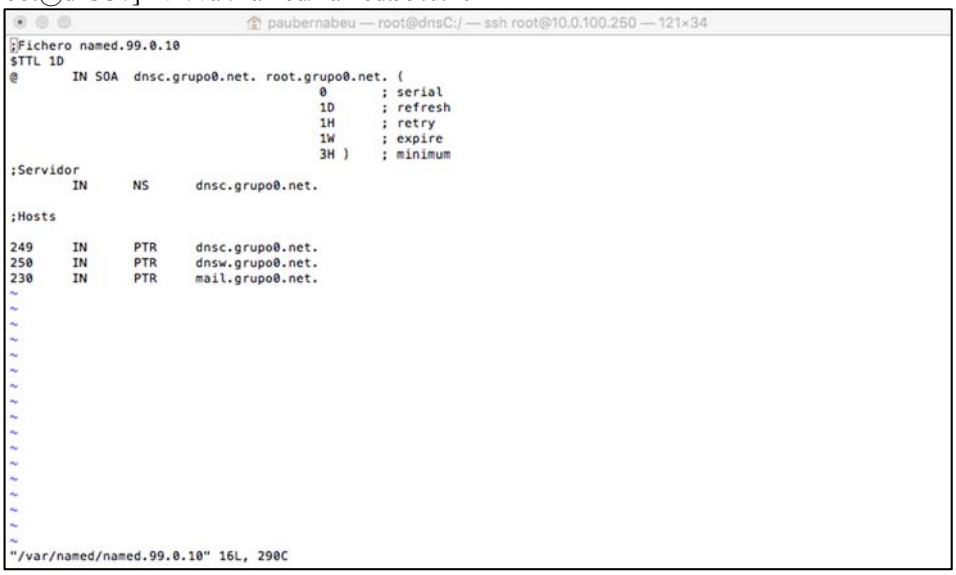
```
[root@dnsC/]# cp /var/named/named.localhost /var/named/named.grupo0.net
[root@dnsC/]# cp /var/named/named.localhost /var/named/named.99.0.10
```

Nuestros ficheros de zona para la resolución directa e inversa quedarían de la siguiente forma:

```
[root@dnsC /]# vi /var/named/named.grupo0.net
```



[root@dnsC /]# vi /var/named/named.99.0.10



Comprobaremos no tenemos errores en los ficheros de zona, usando el comando named-checkzone

```
[root@dnsC /]# named-checkzone grupo0.net /var/named/named.grupo0.net
zone grupo0.net/IN: loaded serial 0
OK
[root@dnsC /]# named-checkzone 99.0.10.in-addr.arpa  /var/named/named.grupo0.net
zone 99.0.10.in-addr.arpa/IN: loaded serial 0
OK
[root@dnsC /]#
```

Como hemos creado los ficheros de zona con el usuario root tenenos que cambiarle el propietario y el grupo para que el servidor pueda tener acceso a ellos.

```
[root@dnsC /]# chown named:named /var/named/named.grupo0.net
[root@dnsC /]# chown named:named /var/named/named.99.0.10
```

Iniciamos o reiniciamos el servicio:

[root@dnsC /]# systemctl restart named

Y establecemos que se inicie cuando se encienda la máquina chkconfig named on

En nuestro caso no tenemos activado el firewall, pero si fuese así, deberíamos de darle permiso en el firewall para la conexión a los puertos 53 tcp y udp y que añadiese el servicio DNS.

Lo veremos más adelante.

Verificación del funcionamiento

Abrimos la máquina cliente Centos, y ejecutamos el comando getent hosts:

```
[root@client ~]# getent hosts dnsC.grupo0.net dnsW.grupo0.net mail.grupo0.net
10.0.99.250     dnsC.grupo0.net
10.0.99.249     dnsW.grupo0.net
10.0.99.230     mail.grupo0.net
```

Observamos que nos indica las direcciones IP a partir de los nombres.

Para verificar la resolución inversa ejecutamos:

```
[root@client ~]# getent hosts 10.0.99.250 10.0.99.249 10.0.99.230
10.0.99.250     dnsw.grupo0.net
10.0.99.249     dnsc.grupo0.net
10.0.99.230     mail.grupo0.net
```

Comprobamos resuelve nombres fuera de la zona, tanto de forma directa como indirecta.

```
[root@client ~]# getent hosts www.upv.es
158.42.4.23     ias.cc.upv.es www.upv.es

[root@client ~]# getent hosts 158.42.4.23
158.42.4.23     ias.cc.upv.es
```

Podemos usar la orden dig. Con esta orden podemos obtener más detalle en las consultas (aparecen los servidores DNS del dominio (registro NS).

```
[root@client ~]# dig dnsc.grupo0.net

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> dnsc.grupo0.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23841
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnsc.grupo0.net.               IN      A

;; ANSWER SECTION:
dnsc.grupo0.net.        86400   IN      A       10.0.99.250

;; AUTHORITY SECTION:
grupo0.net.             86400   IN      NS      dnsc.grupo0.net.

;; Query time: 0 msec
;; SERVER: 10.0.99.250#53(10.0.99.250)
;; WHEN: sáb jul 23 15:04:49 CEST 2016
;; MSG SIZE  rcvd: 74
```

Añade a la zona el servidor DNS dnsW.grupoXX.net y verifica que aparece al realizar la consulta DIG. Deberías obtener ahora:

```
[root@client ~]# dig dnsc.grupo0.net

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> dnsc.grupo0.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54556
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnsc.grupo0.net.               IN      A

;; ANSWER SECTION:
dnsc.grupo0.net.        86400   IN      A       10.0.99.250

;; AUTHORITY SECTION:
grupo0.net.             86400   IN      NS      dnsc.grupo0.net.
grupo0.net.             86400   IN      NS      dnsW.grupo0.net.

;; ADDITIONAL SECTION:
dnsW.grupo0.net.        86400   IN      A       10.0.99.249

;; Query time: 0 msec
;; SERVER: 10.0.99.250#53(10.0.99.250)
;; WHEN: sáb jul 23 15:09:44 CEST 2016
;; MSG SIZE  rcvd: 109
```

Podemos usar una consulta externa:

```
[root@client ~]# dig www.upv.es

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> www.upv.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38923
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.upv.es.                    IN      A

;; ANSWER SECTION:
www.upv.es.             3600    IN      CNAME   ias.cc.upv.es.
ias.cc.upv.es.          3600    IN      A       158.42.4.23

;; AUTHORITY SECTION:
upv.es.                 86400   IN      NS      mirzam.ccc.upv.es.
upv.es.                 86400   IN      NS      vega.cc.upv.es.
upv.es.                 86400   IN      NS      sun.rediris.es.
upv.es.                 86400   IN      NS      chico.rediris.es.

;; ADDITIONAL SECTION:
vega.cc.upv.es.         86400   IN      A       158.42.4.1
chico.rediris.es.       86400   IN      A       130.206.1.3
mirzam.ccc.upv.es.      86400   IN      A       158.42.1.5
sun.rediris.es.         86400   IN      A       130.206.1.2

;; Query time: 263 msec
;; SERVER: 10.0.99.250#53(10.0.99.250)
;; WHEN: sáb jul 23 15:11:49 CEST 2016
;; MSG SIZE  rcvd: 230
```

Para consultar los registros MX del dominio, ejecutamos

```
[root@client ~]# dig mx grupo0.net

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> mx grupo0.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39338
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grupo0.net.                    IN      MX

;; ANSWER SECTION:
grupo0.net.             86400   IN      MX      10 mail.grupo0.net.

;; AUTHORITY SECTION:
grupo0.net.             86400   IN      NS      dnsW.grupo0.net.
grupo0.net.             86400   IN      NS      dnsc.grupo0.net.

;; ADDITIONAL SECTION:
mail.grupo0.net.        86400   IN      A       10.0.99.230
dnsc.grupo0.net.        86400   IN      A       10.0.99.250
dnsW.grupo0.net.        86400   IN      A       10.0.99.249

;; Query time: 0 msec
;; SERVER: 10.0.99.250#53(10.0.99.250)
;; WHEN: sáb jul 23 15:14:25 CEST 2016
;; MSG SIZE  rcvd: 146
```

5. Configuración con dos servidores: Uno principal y otro esclavo

En este campo se configurará este servidor denominado dnsC como servidor secundario del dominio grupoXX.net.

En esta tarea hemos de tener en cuenta que el servidor dnsW será el servidor principal maestro (master), y el dnsC tendrá la categoría de esclavo (salve). La base de datos se configura en el

maestro y el esclavo accede a esta base copiándola en el servidor local. Cada vez que hay un cambio en el maestro (modificación del *serial*), la máquina esclavo actualiza su base de datos.

El primer paso es indicar en el servidor principal dnsW que hay un servidor secundario a fin de darle permisos de compartición de la base de datos. Hemos de indicarle que está permitida la transferencia a servidores secundarios denominados esclavos (*slaves*).

Id al punto 8, de la práctica Configuración de Servidor DNS en Windows 2012 r2 para proceder.

6. Configuración como servidor secundario, el servidor dnsC en Centos

Hemos de indicar en este servidor que es del tipo esclavo, donde guardar la base de datos reciba del principal e indicarle cuál es el servidor principal.

Abrimos pues el fichero /etc/named.rfc1912.zones y configuramos dichas opciones para la zona directa como indirecta. Vamos pues a reescribir las zonas “grupo0.net” y “99.0.10.in-addr.arpa”

```
zone "grupo0.net" IN{
        type slave; //Ahora le indicamos es esclavo
        file "slaves/named.grupo0.net"; //donde guardará la BBDD
                                                                    //reciba del principal
        masters{
                10.0.99.249;//Indicamos IP del Servidor Principal
        };
};

zone "99.0.10.in-addr.arpa" IN {
        type slave; //Ahora le indicamos es esclavo.
        file "slaves/named.99.0.10";//donde guardará la BBDD
                                                                    //reciba del principal
        masters{
                10.0.99.249; ;//Indicamos IP del Servidor Principal
        };
};
```

Reiniciamos el servicio. Y si todo ha ido bien, en la carpeta /var/named/slaves. Nos aparecen las BBDD enviadas por el servidor principal.

```
[root@dnsC /]# cd /var/named/slaves/
[root@dnsC slaves]# ls
named.99.0.10  named.grupo0.net
[root@dnsC slaves]#
```

Que si los abrimos nos muestran un resultado ininteligible:

7. Configuración servidor principal Centos, servidor secundario Windows

Si hubiésemos deseado hacer el principal a el Servidor de Centos y el de Windows como secundario, el procedimiento sería.

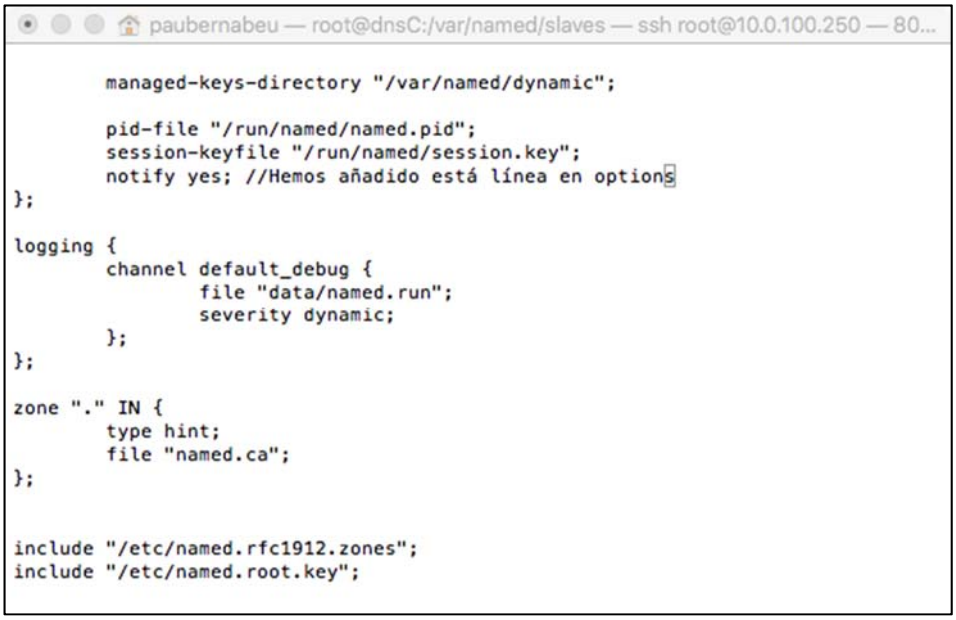
Indicar que el servidor principal es dnsc.

Le indicamos en la zona descrita en etc/named.rfc1912.zones que es maestro, donde está la base de datos que deberá transferir al secundario e indicarle la IP del servidor secundario.

```
zone "grupo0.net" IN{
        type master;
        file "named.grupo0.net";
        allow-transfer{
                10.0.99.250;
        };
};

zone "99.0.10.in-addr.arpa" IN {
        type master;
        file "named.99.0.10";
        allow-transfer{
                10.0.99.250;
        };
};
```

Como hemos hecho para el caso anterior, es recomendable que el servidor principal notifique al secundario los cambios en sus registros. Para ello en el fichero de configuración etc/named.conf, añadimos dentro de options, la línea notify yes.



Ahora id a la Practica “Configuración Servidor DNS Windows 2012 r2” para configurarlo como secundario. (punto 9)