



CEU

Administración de Sistemas de Información

Práctica II: Domain Name System (DNS)

Curso 2022-23, Madrid

Profesor: Teodoro Rojo Aladro

Alumna: Ana Fraile

Grado en Ingeniería en Sistemas de Información (2010), Grupo 101



Índice

<i>Introducción</i>	2
<i>Práctico</i>	3
1. Peticiones DNS a servidores locales y remotos	3
Petición DNS de resolución directa con dominio www.google.com y la utilidad <i>dig</i>	3
Petición DNS de resolución inversa con dirección IP 8.8.8.8 y la utilidad <i>dig</i>	4
Proceso iterativo de búsqueda (o +trace de dig).....	5
2. Instalación de Bind 9 en VM1 (Rocky Linux)	6
3. Configuración y mantenimiento de zonas	7
a. Comprobar que el servidor mantiene una caché de últimos accesos realizados	9
b. Creación de zonas primarias.....	10
c. Mantenimiento de zonas primarias.	11
d. Sincronización primaria-secundarias.	13
e. Delegación de un subdominio.	17



Introducción

En esta práctica se ha llevado el manejo del servicio de resolución de nombres DNS Bind, usando este servidor para probar las funciones más comunes presentes, como puede ser la creación y configuración de zonas, la sincronización de servidores maestros y esclavos, y la delegación de subdominios.

Además, se hará uso de dos máquinas virtuales con una distribución diferente en cada una para permitir observar las diferencias y similitudes dependiendo del sistema donde se haya instalado el servicio de Bind.

A la hora de realizar la práctica se han tenido unas consideraciones iniciales: la máquina virtual 1 (VM1) estará levantada con la distribución de Rocky Linux 9.1, y tendrá la dirección IP 192.168.56.2; y la máquina virtual 2 (VM2) estará levantada con la distribución de Ubuntu Server 22.4, y tendrá la dirección IP 192.168.56.100.

Por otro lado, se suponen unos conocimientos iniciales: la utilidad utilizada para realizar peticiones DNS a lo largo de la práctica será *dig*, y tiene dos tipos de resolución con una estructura diferente para los comandos:

- Resolución directa: para obtener una dirección IP a partir de un nombre

```
dig [@servidor] [-t tipo] dominio
```

- Resolución inversa: para obtener el dominio a través de una dirección IP

```
dig [@servidor] -x direcciónIp
```



1. Peticiones DNS a servidores locales y remotos

Comenzamos con la máquina **VM1**. Realizar peticiones DNS utilizando las utilidades *dig* y/o *nslookup*, tanto en resolución directa como inversa, sobre servidores de DNS locales y remotos (servidores de Internet). Llevar a cabo manualmente el proceso iterativo de búsqueda de un recurso de Internet desde los servidores raíz hasta el servidor con autoridad en el dominio a consultar (también puede usar la opción +trace de *dig*).

Petición DNS de resolución directa con dominio www.google.com y la utilidad *dig*

A la hora de realizar la petición a través del servidor local (aquel predeterminado en la configuración de la máquina), se usará la instrucción `dig www.google.com`, tal y como se muestra en la Imagen 1.

```
[[root@server ~]# dig www.google.com

; <>> DiG 9.16.23-RH <>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52774
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.          27      IN      A      74.125.193.99
www.google.com.          27      IN      A      74.125.193.103
www.google.com.          27      IN      A      74.125.193.104
www.google.com.          27      IN      A      74.125.193.105
www.google.com.          27      IN      A      74.125.193.106
www.google.com.          27      IN      A      74.125.193.147

;; Query time: 52 msec
;; SERVER: 10.82.0.129#53(10.82.0.129)
;; WHEN: Fri Mar 03 11:58:35 CET 2023
;; MSG SIZE  rcvd: 139
```

Imagen 1: Dig a servidor local, resolución directa



Por otro lado se pide realizar la petición a través de un servidor remoto, y en este caso se escogió el servidor de DNS de Google (8.8.8.8), usando la instrucción `dig @8.8.8.8 www.google.com`. (ver Imagen 2).

```
[root@server ~]# dig @8.8.8.8 www.google.com

; <>> DiG 9.16.23-RH <>> @8.8.8.8 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19467
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.        105     IN      A      142.250.185.4

;; Query time: 8 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Mar 03 12:07:25 CET 2023
;; MSG SIZE rcvd: 59
```

Imagen 2: Dig a servidor remoto, resolución directa

Petición DNS de resolución inversa con dirección IP 8.8.8.8 y la utilidad `dig`

En este caso se realizará una petición al servidor local con la instrucción `dig -x 8.8.8.8 .` (ver Imagen 3)

```
[root@server ~]# dig -x 8.8.8.8

; <>> DiG 9.16.23-RH <>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50385
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.  86079   IN      PTR      dns.google.

;; Query time: 50 msec
;; SERVER: 10.82.0.129#53(10.82.0.129)
;; WHEN: Fri Mar 03 12:37:05 CET 2023
;; MSG SIZE rcvd: 73
```

Imagen 3: Dig a servidor local, resolución inversa



Proceso iterativo de búsqueda (o +trace de dig)

Una opción a la hora de realizar una petición de DNS a dig es +trace, que muestra el proceso que realiza el servidor en cuestión para obtener la respuesta a la petición, recorriendo el camino de servidores NS desde la raíz de las direcciones. Esta opción muestra algunos. Servidores NS en cada nivel de la dirección de dominio a encontrar (., com. ...)(ver Imagen 4)

```
[~]# dig www.google.com +trace
; <>> Dig 9.16.23-9NL <>> www.google.com +trace
;; global options: +cmd
.
.          IN      NS      d.root-servers.net.
.          IN      NS      f.root-servers.net.
.          IN      NS      a.root-servers.net.
.          IN      NS      g.root-servers.net.
.          IN      NS      l.root-servers.net.
.          IN      NS      k.root-servers.net.
.          IN      NS      b.root-servers.net.
.          IN      NS      i.root-servers.net.
.          IN      NS      m.root-servers.net.
.          IN      NS      e.root-servers.net.
.          IN      NS      h.root-servers.net.
.          IN      NS      j.root-servers.net.
.          IN      NS      c.root-servers.net.
83204   IN      RRSIG   NS 8 0 518400 20230316050000 20230304000000 951 . q1fbIDVnAmz1gPjyAKhbR7/EnjoJk3FectHCD9USCYwRU9aNytJ50f +pmhBSkGja68A7Dk1634abzNhYNtY0Xlny59cZutGC0Pp5cuZ
liWVHe 706Hku0lu0DQ2v5KH0PLXh++1xHRSv5FxNLeBx+8oGf2r1N22j+7R wzkAyEBwaYT2Yejfw5n1DBxo4+DM7DboCkRUyDar2ri50RWmf8/t xcF8zJ8ohhW9mfujekDuoofQnj04sM4DRB8Vf2Rw9nsDK1WwYRm P3It+58rlpTDsQ474uOU+M1UO
D/VfKupj/8/UCspixX4CJ01daX/M F1THw==
;; Received 1111 bytes from 10.82.0.129#53110.82.0.129) in 52 ms

com.          IN      NS      e.gtld-servers.net.
com.          IN      NS      b.gtld-servers.net.
com.          IN      NS      j.gtld-servers.net.
com.          IN      NS      m.gtld-servers.net.
com.          IN      NS      i.gtld-servers.net.
com.          IN      NS      f.gtld-servers.net.
com.          IN      NS      a.gtld-servers.net.
com.          IN      NS      g.gtld-servers.net.
com.          IN      NS      h.gtld-servers.net.
com.          IN      NS      l.gtld-servers.net.
com.          IN      NS      k.gtld-servers.net.
com.          IN      NS      c.gtld-servers.net.
com.          IN      NS      d.gtld-servers.net.
com.          IN      DS      38999 9 2 E2DC916f6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C61A5766
com.          IN      RRSIG   DS 8 1 86400 20230316050000 20230304000000 951 . IWKSeSkp5XqgvKAQZ1Q1UvBM74QdCzb3yUMI+roBPJM7PCQ81ghzCZ Zb0MjtmH0sv7GcOsN/pVwE/Q0cIdnD+fK0axq2ppR0LhogK
WMN3as Y1nPjcfalIEZxprAF3kjxA3j9ymcRUB5LqFC0Bhnstto3VjcUtpxmv CR4vEzPgwlm3GTjsylsq5d0m1dpuaqrLygKQyD+lwOE2g+NSTCrwvI 4pdn0k9MmeJaGifZqxB5zC6aok5Q+c5emIa0dLELdRV07PeIoT6CwZ cDH0+Eo+KgZQntq+cJ6+jxmTBf
kdc7sbyt514u9KJ3p6faWrlfa8854 ohs81q==

;; Received 1174 bytes from 192.58.128.30#5311(j.root-servers.net) in 37 ms

google.com.    172800  IN      NS      ns2.google.com.
google.com.    172800  IN      NS      ns1.google.com.
google.com.    172800  IN      NS      ns3.google.com.
google.com.    172800  IN      NS      ns4.google.com.
CKP0QD308174JREF/FEFB84308859IN. 60400 IN NSEC3 9 64000 040020401477CH8N43NS41d4UL665 NS 50A RRSIG DNSKEY NSEC3PARAM
CKP0QD308174JREF/FEFB84308859IN. 60400 IN NSEC3 9 64000 20230304000000 20230304000000 951 com. D1TXUm+Hy65Bbc3raw9wW18LywyS+B3m1d/GpMVTzAUZHtRu0zQogJ db0r520JN/k+Od92Ubb+Lphhea/UeP0/5Is0
0941Peh2X0w6SKUE+h n+j1h874TpkX3m4rzc21fFf+u0YXAx0u0fzN1Fe+xxXku0pHn2D w1SYXXy5/1ppb3hrYn1txqg3kxy931wUP1oPQXQYL8Q==
S84BKCIKBC38P58340AKVNFNKR9059QC.com. 86400 IN NSEC3 1 1 0 - S8ABU064AGOCVW9RJFU06LVC75SLNJS NS DS RRSIG
S84BKCIKBC38P58340AKVNFNKR9059QC.com. 86400 IN RRSIG NSEC3 8 2 86400 20230308060132 20230308060132 36739 com. T0tw8a0lkyHgNOQXKetcAVIZch21Ex7vyZYHz0Yh3n8R/7b0d9hdjL6 7sGPZeEk9grk1Ed0L6rJphJLkwzgMRqjx1wYK
QVbhMhtNz1AYVRZx93 Vws1zbZmipJvz4VSABfp4CCV/fgX1t8mfzbebed+EmV179/TIYwcd0xb oBcBaqDjijMmGIraxIEo/OOp1+Op2gIpwh4yaF70yWuA==

;; Received 84 bytes from 192.48.79.30#5311(gtld-servers.net) in 51 ms

www.google.com. 300   IN      A      172.217.17.4
;; Received 59 bytes from 216.239.32.10#5311(ns1.google.com) in 29 ms
```

Imagen 4: Opción +trace a servidor local, resolución directa



2. Instalación de Bind 9 en VM1 (Rocky Linux)

Instalar el servidor de DNS Bind 9.

Para la instalación de dicho servidor en la máquina de Rocky Linux se hará uso de los paquetes ya predescargados que se encuentran en `/usr/local/src`, estando contenidos en concreto en el directorio `bind`. Tras localizar los paquetes a instalar y encontrándonos en el directorio en cuestión, se usará el gestor de paquetes de este sistema, `rpm`, comenzando la instalación con la instrucción `rpm -ivh *.rpm`. (ver Imagen 5).

```
[root@server ~]# cd /usr/local/src/
[root@server src]# ls
apache bind dhcp-server nagios nfs openssh-server openvpn rpcbind samba shorewall tripwire
[root@server src]# cd bind/
[root@server bind]# ls
bind-9.16.23-5.el9_1.x86_64.rpm bind-dnssec-doc-9.16.23-5.el9_1.noarch.rpm bind-dnssec-utils-9.16.23-5.el9_1.x86_64.rpm
[root@server bind]# rpm -ivh *.rpm
Verifying... #####
Preparing... #####
Actualizando / instalando...
1:bind-dnssec-doc-32:9.16.23-5.el9_1 ##### [ 33%]
2:bind-dnssec-utils-32:9.16.23-5.el9_1 ##### [ 67%]
3:bind-32:9.16.23-5.el9_1 ##### [100%]
```

Imagen 5: Instalación de Bind 9 en Rocky Linux



3. Configuración y mantenimiento de zonas

Configuración del servidor Bind. Estudiar el archivo *named.conf* y el contenido del directorio de configuración de Bind. Arrancar el servicio *named*. El servidor deberá escuchar en el puerto 53/udp de todas las direcciones IP del equipo, y atender peticiones de DNS desde cualquier dirección origen. Trabajará de modo recursivo.

La configuración del servidor Bind en las máquinas Rocky Linux tiene dos ficheros/áreas diferentes: la primera, en el fichero */etc/named.conf*, que guarda la configuración global del servidor, además de la configuración inicial de las diferentes zonas; y la segunda, que se encuentra en el directorio */var/named/*, para poder almacenar la información de recursos de cada zona (ver Imagen 6).

```
[[root@server bind]# cd /var/named/  
[[root@server named]# ls  
  data  dynamic  named.ca  named.empty  named.localhost  named.loopback  slaves
```

Imagen 6: Directorio */var/named/*

Para configurar los puertos de escucha del servicio Bind, es necesario modificar el archivo *named.conf*, en este caso eligiendo que para Ipv4 escuche en el puerto 53 para cualquier dirección, dejando los valores restantes tal y como vienen por defecto. (ver Imagen 7)

```
options {  
    listen-on port 53 { any; };  
    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";  
    secroots-file   "/var/named/data/named.secroots";  
    recursing-file  "/var/named/data/named.reCURsing";  
    allow-query     { localhost; };  
  
    /*  
     * 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-validation yes;  
  
    managed-keys-directory "/var/named/dynamic";  
    geoip-directory "/usr/share/GeoIP";  
  
    pid-file "/run/named/named.pid";  
    session-keyfile "/run/named/session.key";  
  
    /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */  
    include "/etc/crypto-policies/back-ends/bind.config";  
};
```

Imagen 7: Modificando *named.conf*



Una vez terminado de configurar el servicio, será necesario iniciar lo con `systemctl start named`, y comprobar que efectivamente se queda escuchando en los puertos deseados con `netstat -untlp`. (ver Imagen 8)

```
[root@server etc]# systemctl start named
[root@server etc]# netstat -untlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 127.0.0.1:53            0.0.0.0:*           LISTEN    24097/named
tcp     0      0 0.0.0.0:22             0.0.0.0:*           LISTEN    751/sshd: /usr/sbin
tcp     0      0 10.0.2.15:53            0.0.0.0:*           LISTEN    24097/named
tcp     0      0 192.168.56.2:53          0.0.0.0:*           LISTEN    24097/named
tcp     0      0 127.0.0.1:953            0.0.0.0:*           LISTEN    24097/named
tcp6    0      0 ::1:53                  ::*:                LISTEN    24097/named
tcp6    0      0 ::::22                 ::*:                LISTEN    751/sshd: /usr/sbin
tcp6    0      0 ::1:953                ::*:                LISTEN    24097/named
udp     0      0 127.0.0.1:323            0.0.0.0:*           LISTEN    736/chrony
udp     0      0 192.168.56.2:53          0.0.0.0:*           LISTEN    24097/named
udp     0      0 10.0.2.15:53            0.0.0.0:*           LISTEN    24097/named
udp     0      0 127.0.0.1:53            0.0.0.0:*           LISTEN    24097/named
udp6    0      0 ::1:323                ::*:                LISTEN    736/chrony
udp6    0      0 ::1:53                  ::*:                LISTEN    24097/named
```

Imagen 8: Iniciar bind



A continuación, realizar distintas configuraciones sobre el servidor Bind y verificar su correcto funcionamiento:

- a. Comprobar que el servidor mantiene una caché de últimos accesos realizados
(para eliminar el contenido de la caché se puede utilizar el comando `rndc flush`)

Hay varias maneras de comprobar que efectivamente el servicio Bind está provisto de una caché:

- Efectuando dos peticiones DNS al mismo recurso en un periodo corto de tiempo y observando que el servidor no necesita volver a buscar la respuesta ya que la almacenará por un periodo de tiempo determinado (ver Imagen 9).

```
[[root@server ~]# rndc flush
[[root@server ~]# dig @localhost www.google.com

; <>> DiG 9.16.23-RH <>> @localhost www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38224
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: a500a43149c95620010000006401d97ceac16dfa7fc96925 (good)
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.          300     IN      A      172.217.17.4
;; Query time: 981 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar 03 12:26:52 CET 2023
;; MSG SIZE  rcvd: 87

[[root@server ~]# dig @localhost www.google.com

; <>> DiG 9.16.23-RH <>> @localhost www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39444
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: afaf7ae1a3d6023c010000006401d9871999037fbd2c2e47 (good)
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.          289     IN      A      172.217.17.4
;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar 03 12:27:03 CET 2023
;; MSG SIZE  rcvd: 87
```

Imagen 9: Mostrar la caché con peticiones seguidas



- Volcando la caché con el comando `rndc dumpdb -cache`. (ver Imagen 10)

```
[[root@server ~]# ls -a /var/named/data/
.  ..  named.run
[[root@server ~]# rndc dumpdb -cache
[[root@server ~]# ls -a /var/named/data/
.  ..  cache_dump.db  named.run
```

Imagen 10: Volcado de cache

- b. **Creación de zonas primarias.** Supondremos un dominio ficticio `miceu.net`, que administra direcciones en el rango `100.10.20.0/24`. Configurar dos zonas primarias para administrar las resoluciones directa e inversa.

Para poder administrar un dominio con su propia resolución directa e inversa es necesario crear 2 zonas en el servidor: una primera para guardar recursos relacionados con el dominio (A, AAAA, MX, CNAME...), y una segunda para guardar los recursos PTR de las direcciones dentro del rango a administrar asociadas a un dominio a mantener. (ver Imagen 11).

```
zone "miceu.net" IN {
    type master;
    file "miceu.net.hosts";
};

zone "20.10.100.in-addr.arpa" IN {
    type master;
    file "20.10.100.rev";
};
```

Imagen 11: Creación de zonas VM1



- c. **Mantenimiento de zonas primarias.** Añadir los siguientes registros a las zonas creadas: A (sol, 100.10.20.1), A (luna, .2), A (marte, .4), A (mail, .50), A (ns1, nuestra propia dirección IP), A (www, a las direcciones 100.10.20.200 y 100.10.20.201), NS (ns1), CNAME (servicios ->luna), MX (mail, prioridad 10). Todos los registros de tipo A deben tener asociado su correspondiente registro PTR. Verificar su funcionamiento con el cliente de DNS (*dig* o *nslookup*)

En el caso de la Rocky Linux, el mantenimiento de una zona se lleva a cabo por defecto en el directorio */var/named*, generando un fichero por cada zona. (ver Imagen 12 e Imagen 13)

```
$TTL 10800
miceu.net.      IN SOA ns1.miceu.net. admin.miceu.net. (
                           1           ; serial
                           10800      ; refresh
                           3600       ; retry
                           604800     ; expire
                           38400 )    ; minimum

@          IN   NS    ns1
ns1        IN   A     192.168.56.2
sol        IN   A     100.10.20.1
luna       IN   A     100.10.20.2
marte      IN   A     100.10.20.4
mail       IN   A     100.10.20.50
www        IN   A     100.10.20.200
www        IN   A     100.10.20.201
servicios  IN   CNAME luna
@          IN   MX    10 mail
```

Imagen 12: Mantenimiento miceu.net

```
$TTL 10800
20.10.100.in-addr.arpa. IN SOA ns1.miceu.net. admin.miceu.net. (
                           1           ; serial
                           10800      ; refresh
                           3600       ; retry
                           604800     ; expire
                           38400 )    ; minimum

@          IN   NS    ns1.miceu.net.
1          IN   PTR   sol.miceu.net.
2          IN   PTR   luna.miceu.net.
4          IN   PTR   marte.miceu.net.
50         IN   PTR   mail.miceu.net.
200        IN   PTR   www.miceu.net.
201        IN   PTR   www.miceu.net.
```

Imagen 13: Mantenimiento zona PTR



Para comprobar que ambas zonas se levantaron correctamente se utilizó la utilidad dig con los comandos: dig @localhost luna.miceu.net y dig @localhost -x 100.10.20.50. (ver Imagen 14 e Imagen 15)

```
[root@server named]# systemctl restart named
[root@server named]# dig @localhost luna.miceu.net

; <>> DiG 9.16.23-RH <>> @localhost luna.miceu.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22053
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3209f34ab1066032010000006401e6302c41d5c8fbce8db2 (good)
;; QUESTION SECTION:
;luna.miceu.net.           IN      A

;; ANSWER SECTION:
luna.miceu.net.      10800   IN      A      100.10.20.2

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar  3 13:21:04 CET 2023
;; MSG SIZE  rcvd: 87
```

Imagen 14: Dig luna.miceu.net

```
[root@server named]# dig @localhost -x 100.10.20.50

; <>> DiG 9.16.23-RH <>> @localhost -x 100.10.20.50
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47637
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d989065dfa92acfb010000006401e665a8454ca05375c3d3 (good)
;; QUESTION SECTION:
;50.20.10.100.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
50.20.10.100.in-addr.arpa. 10800 IN      PTR      mail.miceu.net.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar  3 13:21:57 CET 2023
;; MSG SIZE  rcvd: 110
```

Imagen 15: Dig 100.10.20.50



- d. **Sincronización primaria-secundarias.** Vamos a replicar la zona **miceu.net** en otro servidor de DNS secundario. Arrancar la segunda máquina virtual (**VM2**) e instalar nuevamente el servidor Bind 9. A continuación establecer una zona secundaria del dominio **miceu.net**. En el servidor maestro añadir otra entrada NS (**ns2**) apuntando a la dirección IP del nuevo servidor. Configurar en ambos servidores los parámetros que permitirán la transferencia de la zona. Reiniciar ambos servidores y comprobar que el secundario mantiene una copia de la zona. Llevar a cabo algún cambio en la zona maestra incrementando su número de serie. Reiniciar el servidor y verificar que se actualiza la zona secundaria.
Nota: se recomienda configurar la notificación explícita a las secundarias (**notify explicit**) y la directiva **also-notify** con la dirección IP del servidor secundario.

Para instalar Bind 9 en la máquina Ubuntu se hará uso de su gestor de paquetes, con `apt install bind9`, iniciándose automáticamente el servicio. (ver Imagen 16)

```
[root@server:~# apt install bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils dns-root-data
Suggested packages:
  bind-doc resolvconf
The following NEW packages will be installed:
  bind9 bind9-utils dns-root-data
0 upgraded, 3 newly installed, 0 to remove and 5 not upgraded.
Need to get 407 kB of archives.
After this operation, 1556 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Imagen 16: Instalación Bind 9 en Ubuntu

Una vez instalado Bind 9, para establecer una zona secundaria o esclava de un dominio, habrá que añadir una zona nueva al servidor secundario, y en Ubuntu esto se hace desde el fichero `/etc/bind/named.conf.local`. Al tratarse de una zona secundaria, el tipo de zona será ahora ‘slave’, y tendrá en este caso un solo máster, que será la dirección de la VM1. También se permitirá que la VM1 notifique a la VM2 cuando se reinicie el servicio con `allow-notify (dirección_VM1)`. (ver Imagen 17)

```
//
// 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 "miceu.net" IN {
    type slave;
    file "miceu.net.hosts";
    masters { 192.168.56.2; };
    allow-notify { 192.168.56.2; };
    allow-transfer {none; };
};
```

Imagen 17: Creación zona slave



En el servidor principal (VM1) también será necesario modificar la configuración de la zona de manera que permita al servidor secundario la transferencia de zona (`allow-transfer`), y por comodidad también se ha habilitado la opción de notificar a los servidores secundarios cuando se reinicie el servicio Bind, para que estas puedan comprobar si se reinició por una modificación en la zona (mediante la versión del SOA). (ver Imagen 18)

```
zone "miceu.net" IN {
    type master;
    file "miceu.net.hosts";
    notify explicit;
    also-notify { 192.168.56.100; };
    allow-transfer { 192.168.56.100; };
};

zone "20.10.100.in-addr.arpa" IN {
    type master;
    file "20.10.100.rev";
};
```

Imagen 18: Notificación y transferencia desde master

Por otro lado, en el fichero de mantenimiento de zona en el servidor principal también habrá que añadir la dirección del NS secundario, registrando su recurso NS y A. (ver Imagen 19)

```
$TTL 10800
miceu.net.      IN SOA  ns1.miceu.net. admin.miceu.net. (
                        1           ; serial
                        10800      ; refresh
                        3600       ; retry
                        604800     ; expire
                        38400 )   ; minimum

@          IN      NS      ns1
ns1        IN      A       192.168.56.2
@          IN      NS      ns2
ns2        IN      A       192.168.56.100
sol        IN      A       100.10.20.1
luna       IN      A       100.10.20.2
marte      IN      A       100.10.20.4
mail        IN      A       100.10.20.50
www         IN      A       100.10.20.200
www         IN      A       100.10.20.201
servicios   IN      CNAME  luna
@          IN      MX      10 mail
```

Imagen 19: Añadido NS en master

Tras reiniciar ambos servidores, (ver Imagen 20 e Imagen 21) se puede comprobar, haciendo una petición DNS al servidor secundario (VM2), que este mantiene una copia de la zona, pues su respuesta fue inmediata, es decir, respondió con información propia, y el tiempo que se mantiene la información en la cache es el máximo. (ver Imagen 22)

```
[root@server ~]# vi /etc/named.conf
[root@server ~]# vi /var/named/miceu.net.hosts
[root@server ~]# systemctl restart named
```

Imagen 20: Servidor reiniciado VM1

```
[root@server:/etc/bind# vi named.conf.local
[root@server:/etc/bind# systemctl restart named
Imagen 21: Servidor reiniciado VM2
```



```
[root@server:~# cd /var/cache/bind/
[root@server:/var/cache/bind# ls
managed-keys.bind  managed-keys.bind.jnl  miceu.net.hosts
[root@server:/var/cache/bind# dig @localhost sol.miceu.net

; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @localhost sol.miceu.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61267
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 57e880fb5a82abe301000000640387e7f22fc25e17f77576 (good)
;; QUESTION SECTION:
;sol.miceu.net.          IN      A

;; ANSWER SECTION:
sol.miceu.net.      10800   IN      A       100.10.20.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sat Mar 04 18:03:19 UTC 2023
;; MSG SIZE  rcvd: 86
```

Imagen 22: Dig a VM2

Una vez comprobado el funcionamiento del servidor esclavo, es posible realizar cambios en el servidor principal, y que, tras reiniciar el servicio, la zona secundaria se actualice también. Para ello es necesario ir aumentando la versión del *SOA* tras cada cambio en la zona. En este caso se cambió la dirección IP del recurso sol, actualizando el *SOA* a 2. (ver Imagen 23)

```
$TTL 10800
miceu.net.      IN SOA  ns1.miceu.net. admin.miceu.net. (
                      2           ; serial
                      10800        ; refresh
                      3600         ; retry
                      604800       ; expire
                      38400 )      ; minimum

@           IN      NS      ns1
ns1         IN      A       192.168.56.2
@           IN      NS      ns2
ns2         IN      A       100.10.20.5
sol         IN      A       100.10.20.5
luna        IN      A       100.10.20.2
marте       IN      A       100.10.20.4
mail        IN      A       100.10.20.50
www         IN      A       100.10.20.200
www         IN      A       100.10.20.201
servicios   IN      CNAME  luna
@           IN      MX      10 mail
```

Imagen 23: Cambio en la zona VM1



Tras reiniciar el servidor y realizar una nueva petición de este servicio al servidor secundario, efectivamente se ha actualizado la dirección IP del recurso sol.miceu.net. (ver Imagen 24)

```
[root@server:/var/cache/bind# dig @localhost sol.miceu.net
; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @localhost sol.miceu.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20989
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cd88f0b37bd6f3810100000640388545853bd4db9a81ac3 (good)
;; QUESTION SECTION:
;sol.miceu.net.          IN      A
;;
;; ANSWER SECTION:
sol.miceu.net.      10800   IN      A      100.10.20.5
;;
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sat Mar 04 18:05:08 UTC 2023
;; MSG SIZE  rcvd: 86
```

Imagen 24: Cambio en servidor secundario



e. Delegación de un subdominio. Crear una nueva zona maestra `mispruebas.com` en el servidor **VM2**. Vamos a configurar la delegación de un subdominio (por ejemplo, `madrid.mispruebas.com`), cuya zona maestra se ubicará en el otro servidor de DNS (**VM1**). Para hacer las pruebas añadir algún registro A en el nuevo subdominio y verificar que una petición de resolución dirigida al servidor VM2 y relativa al subdominio, es reenviada y resuelta en el servidor VM1. Comprobar igualmente el efecto de la directiva `recursión yes|no` en el comportamiento del servidor que aloja el dominio principal (VM2).

A la hora de configurar la delegación de subdominios es conveniente trabajar del subdominio más específico (`madrid.mispruebas.com`), al dominio que engloba todo el resto de subdominios (`mispruebas.com`). Para ello se comenzó creando la zona `madrid.mispruebas.com` en la VM1, modificando los ficheros: `/etc/named.conf` y `/var/named/madrid.mispruebas.com.hosts`.

En el fichero `named.conf` se añadió la sentencia de creación de una nueva zona, complementándola con la dirección de la VM2 (contenedora del dominio principal) en la opción de `allow-query`, tal y como se muestra en la Imagen 25.

```
zone "madrid.mispruebas.com" IN {
    type master;
    file "madrid.mispruebas.com.hosts";
    allow-query {localhost;192.168.56.100; };
};
```

Imagen 25: Creación subdominio, VM1

Si no se hubiese añadido esta opción, la VM2 no sería capaz que pedirle información relacionada con la zona, ya que por defecto en la máquina Rocky Linux mantiene que nada más pueden realizar ella misma puede realizar consultas al servidor. Uno se da cuenta de que esta opción no está habilitada si se realiza una petición de DNS a un recurso del dominio y el estado de la consulta aparece como denegado. (ver Imagen 26)

```
[root@server:~# dig @192.168.56.2 chamartin.madrid.mispruebas.com
; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @192.168.56.2 chamartin.madrid.mispruebas.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: REFUSED, id: 56343
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2ffc77a34527a10d0100000640877b55aa9dc132c297397 (good)
;; QUESTION SECTION:
;chamartin.madrid.mispruebas.com. IN      A

;; Query time: 8 msec
;; SERVER: 192.168.56.2#53(192.168.56.2) (UDP)
;; WHEN: Wed Mar 08 11:55:33 UTC 2023
;; MSG SIZE  rcvd: 88
```

Imagen 26: Dig con status refused, VM2 a VM1



Por otro lado, en el fichero `madrid.mispruebas.com.hosts` se configuró la información de los recursos relacionados con la zona, que en este caso es la dirección Chamartín. `madrid.mispruebas.com`, con dirección IP 200.1.1.1 (recurso tipo A), junto con la propia dirección de la VM1 como servidor de la zona. (ver Imagen 27)

```
$TTL 10800
madrid.mispruebas.com.      IN SOA ns1.madrid.mispruebas.com. admin.madrid.mispruebas.com. (
                                1           ; serial
                                10800      ; refresh
                                3600       ; retry
                                604800     ; expire
                                38400 )    ; minimum

@          IN      NS      ns1
ns1        IN      A       192.168.56.2
chamartin  IN      A       200.1.1.1
```

Imagen 27: Mantenimiento subdominio, VM1

Hasta aquí, la configuración de la zona se podría asemejar a la de cualquier otro dominio, obviando el incluir el `allow-query`. Y a pesar de que la creación de la zona/dominio principal en la VM2 se realizará igual que para el resto de zonas, añadiéndolas al fichero `/etc/bind/named.conf.local` (ver Imagen 28), desde el dominio principal (VM2) sí que será importante añadir a la zona un nuevo NS para la dirección `madrid.mispruebas.com` que apunte al servidor donde se aloja el subdominio (VM1). (ver Imagen 29)

```
zone "mispruebas.com" IN {
    type master;
    file "mispruebas.com.hosts";
};
```

Imagen 28: Creación dominio principal, VM2

```
$TTL 10800
mispruebas.com.      IN SOA ns1.mispruebas.com. admin.mispruebas.com. (
                                1           ; serial
                                10800      ; refresh
                                3600       ; retry
                                604800     ; expire
                                38400 )    ; minimum

@          IN      NS      ns1
ns1        IN      A       192.168.56.100
madrid     IN      NS      ns1.madrid
ns1.madrid IN      A       192.168.56.2
```

Imagen 29: Mantenimiento dominio principal, VM2



Creados ambos el subdominio y el dominio, es preciso comprobar el correcto funcionamiento del sistema, posiblemente a través de peticiones DNS. Observando también las diferencias entre un servidor recursivo y uno sin esa función.

Estando en una primera instancia configurado el servidor de la VM2 de manera recursiva, al realizar una petición al recurso `chamartin.madrid.mispruebas.com` se observa que este es capaz de obtener su dirección IP tras leer la información del NS dónde se encuentra alojada la zona. (ver Imagen 30)

```
[root@server:~# dig @localhost chamartin.madrid.mispruebas.com
; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @localhost chamartin.madrid.mispruebas.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 25344
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: cefd2b3befb5447d010000006408816a8099db144ee28155 (good)
;; QUESTION SECTION:
;chamartin.madrid.mispruebas.com. IN      A
;;
;; ANSWER SECTION:
chamartin.madrid.mispruebas.com. 10800 IN A      200.1.1.1
;;
;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Wed Mar 08 12:36:58 UTC 2023
;; MSG SIZE rcvd: 104
```

Imagen 30: Dig recursivo `chamartin`, VM2

Para poder observar el funcionamiento del servidor de la VM2 en estado no recursivo es necesario modificar el parámetro de `recursion` en el fichero `/etc/bind/named.conf.options` y dejarlo con su valor en `no`. (ver Imagen 31)

```
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 {
    //     0.0.0.0;
    // };

    //========================================================================
    // 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;

    listen-on-v6 { any; };

    recursion no;
};
```

Imagen 31: Cambio de `recursion`, VM2



Tras guardar los cambios del fichero y reiniciar el servicio de *named*, ya es posible observar las diferencias en la respuesta a las consultas de DNS, en este caso nada más devolvió la dirección IP del NS donde se encuentra alojada la zona `madrid.mispruebas.com`, y tuvimos que ir manualmente a obtener la dirección IP del dominio `chamartin.madrid.com`, realizando la consulta a la dirección obtenida del servidor NS. (ver Imagen 32)

```
[root@server:/etc/bind# vi named.conf.options
[root@server:/etc/bind# systemctl restart named
[root@server:/etc/bind# dig @localhost chamartin.madrid.mispruebas.com

; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @localhost chamartin.madrid.mispruebas.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52679
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: dad306820c419ebd01000006403a2180e4838bcf9f353cd (good)
;; QUESTION SECTION:
;chamartin.madrid.mispruebas.com. IN      A

;; AUTHORITY SECTION:
madrid.mispruebas.com. 10800    IN      NS      ns1.madrid.mispruebas.com.

;; ADDITIONAL SECTION:
ns1.madrid.mispruebas.com. 10800 IN      A      192.168.56.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sat Mar 04 19:55:04 UTC 2023
;; MSG SIZE  rcvd: 122

[root@server:/etc/bind# dig @192.168.56.2 chamartin.madrid.mispruebas.com

; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> @192.168.56.2 chamartin.madrid.mispruebas.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51088
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 404b91416d26de3701000006403a238b3b7e9face9242a4 (good)
;; QUESTION SECTION:
;chamartin.madrid.mispruebas.com. IN      A

;; ANSWER SECTION:
chamartin.madrid.mispruebas.com. 10800 IN A      200.1.1.1

;; Query time: 0 msec
;; SERVER: 192.168.56.2#53(192.168.56.2) (UDP)
;; WHEN: Sat Mar 04 19:55:36 UTC 2023
;; MSG SIZE  rcvd: 104
```

Imagen 32: Dig no recursivo chamartin, VM2-VM1