# Instalación del servidor DNS maestro con Bind9

UT4: Servicio de Nombres de Dominio (DNS)

SERVICIOS EN RED

**dnsmasq** es en realidad un servidor de DNS muy básico, que no permite delegación de zonas o actualización y publicación hacia otros DNSs. Para estas propiedades y otros aspectos como la seguridad necesitamos un servidor DNS profesional y de código abierto, se trata del paquete ***bind9*** de **Internet System Consortium**. Para instalarlo, podemos hacerlo con ***apt*** desde una consola de root:

```
// Instalación del servidor DNS bind
# apt install bind9
```

De esta forma instalaremos los programas necesarios para disponer de un completo servidor DNS con bind. Tan solo será necesario configurarlo y ponerlo en marcha.

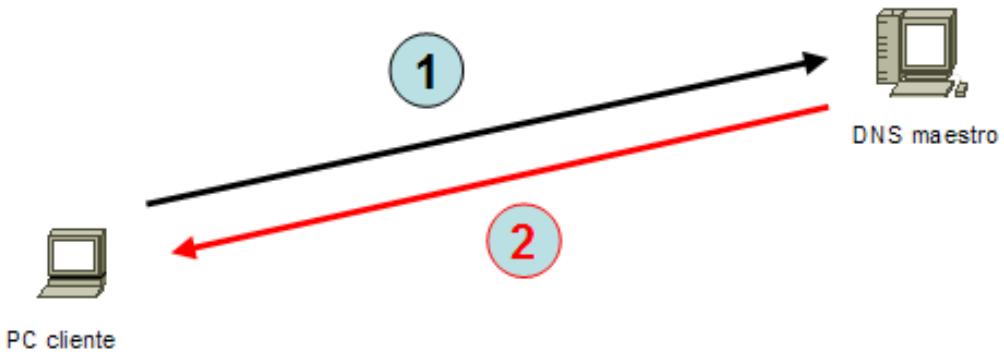
## Configuración del servidor DNS

El servidor DNS bind admite tres modos de funcionamiento:

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

## Servidor DNS maestro

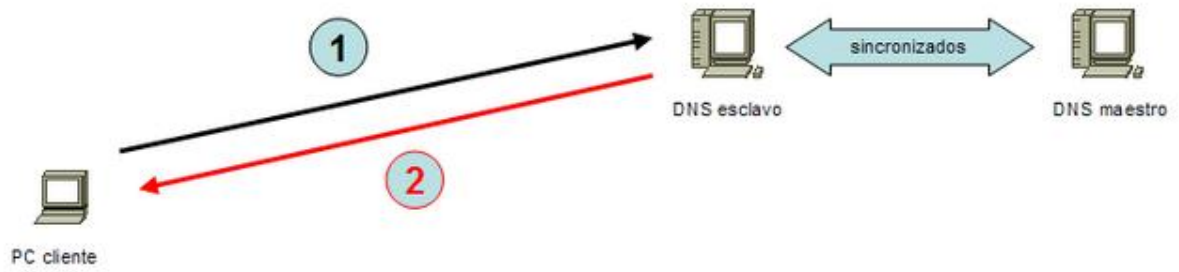
En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.




**Consulta a un DNS maestro**

## Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.




**Consulta a un DNS esclavo**

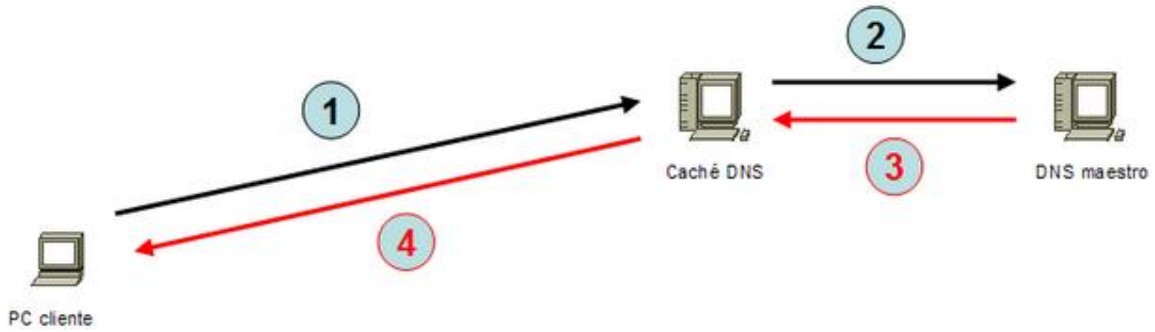
## Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como

nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario. Muchos routers ADSL ofrecen ya este servicio de caché, tan solo hay que activarlo y configurar una o dos IPs de servidores DNS en Internet. En los PCs de nuestra red local podríamos poner como DNS primario la IP de nuestro router y como DNS secundario una IP de un DNS de Internet.




**Consulta a un caché DNS. En caso de fallo, se redirecciona hacia un DNS maestro**

Para configurarlo, tan solo será necesario editar el archivo /etc/bind/named.conf.options y añadir las siguiente líneas:

```
// Configuración como caché DNS
// Añadir IPs de los DNS de nuestro proveedor o de nuestra confianza en /etc/bind/named.conf.options
options {
        max-cache-size 40M;  // Tamaño del caché DNS en Megas
      allow-query-cache { any; };  // Permitir consultas al caché.
        recursion yes;      // valor por defecto, pero es mejor ponerlo para saber que lo hemos tenido en cuenta
};
```

## Archivos de configuración del DNS

El archivo de configuración del DNS es el archivo /etc/bind/named.conf, pero este hace referencia a otros cuantos archivos como por ejemplo:

- Archivo named.conf: Archivo principal de configuración, para zonas públicas.

- Archivo named.conf.options: Opciones genéricas, p.e. *forwarders*
- Archivo named.conf.local: Especificación de zonas privadas (hacia direccionamiento privado RFC1918)
- Archivo db.127:Especificación dirección de retorno (loopback)
- Archivo db.root: DNS de nivel superior
- Otros archivos: db.0, db.255, db.empty, db.local, rndc.conf, rndc.key, zones.rfc1918

## Configuración como servidor de reenvío DNS

Por defecto, al instalar el paquete bind está pre configurado como servidor de reenvío DNS. Tan solo será necesario editar el archivo /etc/bind/named.conf.options y en la sección forwarders añadir las IPs de dos servidores DNS donde redirigir las peticiones DNS:

```
// Configuración como caché DNS
// Añadir IPs de los DNS de nuestro proveedor o de nuestra confianza en /etc/bind/named.conf.options
options {
  forwarders {
    1.1.1.1; 9.9.9.9;
  };
};
```

## Configuración DNS maestro o primario

Por razones de accesibilidad y organizativas, deseamos asignar un nombre a todos los equipos de nuestra red, para lo que instalaremos un servidor DNS privado con un dominio ficticio, por ejemplo '**aula114.org**'. Todos los PCs de nuestra red pertenecerán a dicho dominio ficticio que funcionará solo en nuestra red interna, no en Internet. En tal caso el nombre completo de los PCs terminará con '**aula114.org**', por ejemplo: **equipo12.aula114.org**. Lo ideal en una situación así es disponer de un servidor DNS que sea maestro de nuestro dominio, es decir, maestro del dominio interno '**aula114.org**'.

Nuestro servidor DNS maestro para nuestro dominio ficticio interno 'aula114.org' será capaz de resolver peticiones internas de nombres de este dominio, tanto de forma directa como de forma inversa, es decir, si recibe una consulta acerca de quién es **equipo12.aula114.org** deberá devolver su IP, pongamos por ejemplo 192.168.114.212. Si la consulta es una consulta DNS inversa acerca de quién es 192.168.114.212, deberá responder **equipo12.aula114.org**. Por ello deberemos añadir en el archivo **/etc/bind/named.conf.local** la especificación de maestro para el dominio y para la resolución inversa, por ejemplo:

```
// Añadir en /etc/bind/named.conf.local
// Archivo para búsquedas directas
zone "aula114.org" {
  type master;
  file "db.aula114.org";     // Debe estar en /var/cache/bind/
  allow-update { none; };
};

// Archivo para búsquedas inversas
zone "114.168.192.in-addr.arpa" {
  type master;
  file "114.168.192.rev";
  allow-update { none; };
};
```

Evidentemente será necesario crear los archivos **db.aula114.org** y **114.168.192.rev** en **/var/cache/bind** que especificarán la asociación entre nombres y direcciones IP de nuestra red en un sentido y en otro respectivamente.

NOTA: el dueño de los ficheros de zona debe ser bind:bind, se cambia con:

*chown bind:bind nombre_de_fichero*

## Archivo de zona de búsqueda directa

Supongamos que en nuestra red local tenemos un aula con 11 PCs con IPs que van desde la 192.168.115.101 hasta 192.168.115.110 y cuyos nombres van desde equipo01 hasta equipo10, luego un servidor web (ubuntuserver00) que además es servidor DNS con la IP 192.168.115.111. El archivo de configuración DNS de nuestro dominio podría ser así:

```
;  Archivo db.aula114.org
;
; BIND data file for aula114.org
;
$TTL    1D
@ IN SOA server.aula114.org. root.aula114.org. (
        2019112101 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

; Servidores DNS del dominio
        IN      NS      server.aula114.org.

; Correo
        IN      MX 10   mx1.aula114.org.

; Directas
server IN A 192.168.114.200
equipo01 IN A 192.168.114.201
equipo02 IN A 192.168.114.202


; Alias o sinónimo
dns IN CNAME server
smtp IN CNAME server
eq1 IN CNAME equipo01
```

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y períodos de actuación). Las dos siguientes líneas indican quién es el servidor primario (NS = Name Server) . Las siguientes líneas especifican las IPs de los distintos PCs componentes del dominio (A = Address).

Si olvidamos algún punto y coma, dará errores y no funcionará correctamente. Para revisar los archivos disponemos de los comandos **named-checkconf** y **named-checkzone** que analizan que esté correcta la sintaxis de los mismos.

También se puede consultar el archivo de **logs del sistema** para comprobar si existe algún error:

```
# cat /var/log/syslog | grep named
# journalctl -u named.service
```

Para comprobar que el archivo de resolución directa está correctamente, se debe ejecutar:

```
named-checkzone aula114.org. /var/cache/bind/db.aula114.org
```

Y la salida que se obtiene es:

```
zone aula114.org/IN: loaded serial 2018100801
OK
```

## Archivo de zona de búsqueda inversa

Para poder realizar consultas inversas (de IP a nombre) será necesario crear el siguiente archivo:

```
;
; BIND reverse data file for 192.168.114.0
;
$TTL    1D
@ IN SOA 114.168.192.in-addr.arpa. root.aula114.org. (
        2018100801 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

        IN      NS      server.aula114.org.

10  IN PTR profesor.aula114.org.

12 IN PTR equipo02.aula114.org.
210 IN PTR mail.aula114.org.
200 IN PTR www.aula114.org.
```

Para comprobar que el archivo de zona inversa está correctamente, se debe ejecutar:

```
named-checkzone                    114.168.192.in-addr.arpa.
/var/cache/bind/114.168.192.rev
```

La salida que nos devuelve la línea anterior será:

```
zone 114.168.192.in-addr.arpa/IN: loaded serial 2018100801
OK
```

Una vez configurado nuestro servidor DNS, debemos indicar a nuestro servidor Linux que el servidor DNS es él mismo, modificando en las líneas necesarias el archivo **/etc/network/interfaces**.

```
// Indicamos que nosotros mismos somos servidores DNS
// y por defecto buscamos en nuestro dominio
// Editar /etc/network/interfaces del servidor DNS
dns-nameservers 127.0.0.1
dns-search aula114.org

// Editar /etc/resolvconf/resolv.conf.d/head y fijar dominio
domain aula114.org
```

En el resto de PCs de la red, indicaremos que el servidor DNS es 192.168.114.200

```
// En los clientes de la red indicamos quién es el DNS
// Editar /etc/network/interfaces del resto de PCs de la red
....
dns-nameserver 192.168.114.200
dns-search aula114.org
```

Tan solo nos faltará poner en marcha nuestro servidor de nombres ejecutando en el servidor el script de inicio correspondiente:

```
// Arranque del servidor DNS
# systemctl restart bind9
```

## Comprobaciones desde el cliente

Disponemos de tres comandos para realizarlas: el comando ***host***, el comando ***dig*** o el comando ***nslookup.*** Con ellos puedo hacer cualquier consulta de prueba.

Comando host:

```
root@equipo00:/home/usuario# host equipo01
equipo01.aula114.org has address 192.168.114.201
```

Comando dig:

```
root@equipo00:/home/usuario# dig equipo07

; <<>> DiG 9.10.3-P4-Ubuntu <<>> equipo07
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 29906
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;equipo07.                      IN   A

;; AUTHORITY SECTION:
.               10800     IN   SOA  a.root-servers.net.
nstld.verisign-grs.com. 2017012301 1800 900 604800 86400

;; Query time: 27 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jan 23 23:47:13 CET 2017
;; MSG SIZE  rcvd: 112
```

Comando nslookup:

```
root@equipo00:/home/usuario# nslookup 192.168.1.204
Server:         127.0.0.1
Address:   127.0.0.1#53

204.114.168.192.in-addr.arpa     name = equipo04.aula114.org.
```

```
root@equipo00:/home/usuario# nslookup equipo04
Server:         127.0.0.1
Address:   127.0.0.1#53

Name: equipo04.aula114.org
Address: 192.168.114.204
```

## Configuración DNS esclavo

Si deseamos configurar nuestro servidor DNS para que actúe como esclavo de un servidor DNS maestro, la configuración es mucho más sencilla que en el caso anterior ya que únicamente será necesario indicar en el DNS esclavo quién es el servidor DNS maestro, y en el DNS maestro, la IP del DNS esclavo.

Es importante que el DNS esclavo tenga como DNS configurado el DNS maestro.

Ejemplo, supongamos que el nombre del DNS maestro es dns.aula114.org (IP 192.168.aula.x1) y que el nombre del DNS esclavo es dns2.aula114.org. En el archivo 'db.aula114.org de zona de búsqueda directa añadiremos la línea del segundo dns justo debajo de donde está la del primero:

```
// Añadir línea en db.aula114.org del maestro
....
     IN NS dns.aula114.org.
     IN NS dns2.aula114.org. // Nueva línea

dns2 IN A 10.2.13.240
....
```

**De esta forma indicaremos que existen más servidores DNS para dicha zona. Lo mismo haremos en el archivo '114.168.192.rev' de la zona inversa:**

```
// Añadir línea en 114.168.192.rev del maestro
....
     IN NS dns.aula114.org.
     IN NS dns2.aula114.org. // Nueva línea
dns2 IN A 10.2.13.240
....
```

En el archivo /etc/bind/named.conf.local del servidor DNS esclavo debemos indicar que se trata de un servidor esclavo y también debemos indicar quién es el maestro:

```
// Añadir en /etc/bind/named.conf.local del esclavo
zone "aula114.org" {
  type slave;
```

```
  file "db.aula114.org";
  masters { ip_del_maestro; };
  allow-notify { ip_del_maestro; };
};
zone "114.168.192.in-addr.arpa" {
  type slave;
  file "114.168.192.rev";
  masters { 192.168.114.200; };
  allow-notify { 192.168.114.200; };
};
```

En el archivo /etc/bind/named.conf.local del servidor DNS maestro podemos utilizar allow-notify para mantener los DNS sincronizados. Con alow-notify pasamos los cambios de zonas en el maestro al esclavo:

```
// Archivo /etc/bind/named.conf.local del maestro
zone "aula114.org" {
  type master;
  file "db.aula114.org";
  allow-transfer { ip_del_esclavo; };
  also-notify { ip_del_esclavo; };
};

zone "114.168.192.in-addr.arpa" {
  type master;
  file "114.168.192.rev";
  allow-transfer { ip_del_esclavo; };
  also-notify { ip_del_esclavo; };
};
```

De esta forma dispondremos en la red de un servidor DNS esclavo que podrá satisfacer las peticiones DNS al igual que lo haría el maestro. Es interesante si el número de peticiones es muy elevado y se requiere distribuir la carga entre los dos servidores, o si deseamos disponer de servicio DNS de alta disponibilidad de forma que aunque el servidor maestro deje de funcionar, el servidor esclavo podrá seguir ofreciendo el servicio.

Cada vez que hagamos un cambio en los archivos **db.aula114.org** y **114.168.192.rev** del maestro, debemos acordarnos de actualizar el parámetro serial (incrementar en una unidad) para que los dns dependientes del maestro sepan que ha cambiado y actualicen su información para mantenerse perfectamente sincronizados.

# Servidor DNS Delegado [the pro and easy way by Andrés G.P.] (Subdominios)

Si deseamos delegar una subzona (subdominio) debemos configurar nuestro servidor DNS maestro para que delegue dicha zona a otro servidor DNS que será la autoridad (SOA) para dicha subzona.

Los archivos a configurar modificar son:

```
// Archivo /etc/bind/named.conf.local del dns delegado
zone "s.aula114.org" {
  type master;
  file "db.s.aula114.org";
};

// Se podrían resolver más zonas directas o inversas en este fichero
```

```
// Archivo db.aula114.org del DNS MAESTRO
// nos vamos a la parte NS del fichero y añadimos

@       IN      NS      dns.aula114.org.
s       IN      NS      delegado01.s.aula114.org.
delegado01.s    IN      A       192.168.114.240
```

```
//  Archivo db.s.aula114.org del DNS Delegado
$TTL    1D
@ IN SOA delegado01.s.aula114.org. root.s.aula114.org. (
        2022110301 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL
; Servidores DNS del subdominio
        IN      NS      delegado01.s.aula114.org.
;Correo
        IN      MX 5     correo1
        IN      MX 10    correo2
```

```
; Directas
delegado01      IN A 192.168.114.200
www             IN A 172.16.40.40
correo1         IN A 172.16.40.11
correo2         IN A 172.16.40.12
ldap            IN A 172.16.40.13


; Alias o sinonimo
dns IN CNAME www
web IN CNAME www
m1 IN CNAME correo1
m2 IN CNAME correo2
```

Hay que reiniciar los 3 DNSs y hacer las consultas DNS de la zona y la subzona al DNS maestro. Si se definen inversas en el DNS delegado, las consultas hay que hacerlas al delegado para esa zona inversa.

## Autoarranque, arranque y parada del servidor DNS

El servidor DNS, en contenedores, dispone de un script de arranque y parada en la carpeta ***/etc/init.d***. En las versiones cloud y server oficiales, tenemos disponible la utilidad ***systemctl:***

```
// Arranque del servidor DNS
sudo systemctl start named.service
sudo /etc/init.d/bind9 start
// Parada del servidor DNS
sudo systemctl stop named.service
sudo /etc/init.d/bind9 stop
// Reinicio del servidor DNS
sudo systemctl restart named.service
sudo /etc/init.d/bind9 restart
// Habilitar al arranque del servidor DNS
sudo systemctl enable named.service
// Deshabilitar al arranque del servidor DNS
sudo systemctl disable named.service
```

```
// Comprobar si se iniciará al arranque del servidor DNS
sudo systemctl is-enabled named.service
```

**ANEXO**

**Ficheros de configuración de Nombre y sufijo DNS de la máquina**

```
diego@DnsDJFR:~$ cat /etc/hostname
DnsDJFR
diego@DnsDJFR:~$ cat /etc/hosts
127.0.0.1       localhost
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
# --- BEGIN PVE ---
172.16.200.29 DnsDJFR.institutodh.net DnsDJFR
# --- END PVE ---
diego@DnsDJFR:~$ cat /etc/resolv.conf
# --- BEGIN PVE ---
search institutodh.net
nameserver 172.16.200.29
# --- END PVE ---
```

# Servidor DNS Delegado [the hard and fool way] (Subdominios)

Si deseamos delegar una subzona (subdominio) debemos configurar nuestro servidor DNS maestro para que actúe como esclavo de la subzona e informar de la delegación en el archivo de Registro de Recursos de la zona en la que se va a producir la delegación.

Los archivos a configurar modificar son:

```
// Archivo /etc/bind/named.conf.local del maestro
zone "aula114.org" {
  type master;
  file "db.aula114.org";
  allow-transfer { ip_del_esclavo; };
  also-notify { ip_del_esclavo; };
};

zone "s.aula114.org" {
  type slave;
  file "db.s.aula114.org";
  masters { ip_del_dnsdelegado; };
  allow-notify { ip_del_dnsdelegado; };
};


zone "114.168.192.in-addr.arpa" {
  type master;
  file "114.168.192.rev";
  allow-transfer { ip_del_esclavo; };
  also-notify { ip_del_esclavo; };
};


// Archivo /etc/bind/named.conf.local del dns delegado
zone "s.aula114.org" {
  type master;
  file "db.s.aula114.org";
  allow-transfer { ip_del_dnsMaestro; };
  also-notify { ip_del_DnsMaestro; };
```

```
};

// Se podrían resolver más zonas inversas en este fichero
```

// Archivo db.aula114.org del **DNS MAESTRO**

```
// nos vamos al final del fichero y añadimos
$ORIGIN s.aula114.org.
@       IN      NS      delegado01.s.aula114.org.
        IN      NS      dns.aula114.org.
delegado01      IN      A       192.168.114.240
```

// Archivo db.s.aula114.org del **DNS Delegado**

```
$TTL    1D
@ IN SOA delegado01.s.aula114.org. root.s.aula114.org. (
        2022110301 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL
; Servidores DNS del subdominio
        IN      NS      delegado01.s.aula114.org.
        IN      NS      dns.aula114.org.
;Correo
        IN      MX 5     correo1
        IN      MX 10    correo2


; Directas
delegado01      IN A 192.168.114.200
www             IN A 172.16.40.40
correo1         IN A 172.16.40.11
correo2         IN A 172.16.40.12
ldap            IN A 172.16.40.13
```

```
; Alias o sinonimo
dns IN CNAME www
web IN CNAME www
m1 IN CNAME correo1
m2 IN CNAME correo2
```

Hay que reiniciar los 3 DNSs y hacer las consultas DNS de la zona y la subzona al DNS maestro. Si se definen inversas en el DNS delegado, las consultas hay que hacerlas al delegado para esa zona inversa.

## Autoarranque, arranque y parada del servidor DNS

El servidor DNS, en contenedores, dispone de un script de arranque y parada en la carpeta ***/etc/init.d***. En las versiones cloud y server oficiales, tenemos disponible la utilidad ***systemctl:***

```
// Arranque del servidor DNS
sudo systemctl start named.service
sudo /etc/init.d/bind9 start
// Parada del servidor DNS
sudo systemctl stop named.service
sudo /etc/init.d/bind9 stop
// Reinicio del servidor DNS
sudo systemctl restart named.service
sudo /etc/init.d/bind9 restart
// Habilitar al arranque del servidor DNS
sudo systemctl enable named.service
// Deshabilitar al arranque del servidor DNS
sudo systemctl disable named.service
// Comprobar si se iniciará al arranque del servidor DNS
sudo systemctl is-enabled named.service
```

**ANEXO**

**Ficheros de configuración de Nombre y sufijo DNS de la máquina**

```
diego@DnsDJFR:~$ cat /etc/hostname
DnsDJFR
diego@DnsDJFR:~$ cat /etc/hosts
127.0.0.1       localhost
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
# --- BEGIN PVE ---
172.16.200.29 DnsDJFR.institutodh.net DnsDJFR
# --- END PVE ---
diego@DnsDJFR:~$ cat /etc/resolv.conf
# --- BEGIN PVE ---
search institutodh.net
nameserver 172.16.200.29
# --- END PVE ---
```