Servidor DNS Linux Debian bind9

Índice

1. Instalación servidor DNS Linux Debian

Como en casi todos los servicios provenientes del software libre, existen múltiples opciones de software para cada uno de los servicios, en nuestro caso, y como norma general, utilizaremos aquellos más implantados en Internet y en las empresas. En el caso del servicio DNS estaríamos hablando de bind9.

Para su instalación ejecutaremos el comando **apt-get install bind9**.

Tras la instalación, debemos tener en cuenta que la configuración y administración general del servidor DNS bind9 se realiza mediante el fichero de configuración **/etc/bind/named.conf**.

Ampliación de conocimientos: Existen aplicaciones gráficas, basadas en servidores web, que nos permiten su administración, como por ejemplo webmin (sobre Apache).

```
servicios@debian:~$ cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

La instalación por defecto permite un funcionamiento de servidor DNS caché, saliendo a resolver a Internet consultando a los servidores TNS y almacenando las resoluciones para posteriores peticiones de clientes.

Una vez realizada la instalación podemos comprobar su funcionamiento mediante los comandos nslookup y dig.

nslookup.- Entre otras informaciones, podemos obtener la dirección IP del nombre DNS, tipo de respuesta (autorizada no autorizada), alias, etc.

dig.- Entre otras informaciones, podemos obtener la dirección IP del nombre DNS, tiempo empleado en la resolución de la consulta DNS, tiempo de vida de la resolución en la caché.

Una vez instalado el servicio DNS, como casi todos los servicios, se puede reiniciar, parar y arrancar desde línea de comando mediante:

service bind9 start.- Arranca el servicio.

service bind9 stop.- Para el servicio.

service bind9 restart.- Reinicia el servicio.

Para los administradores DNS noveles, la causa más común de fallo son los errores de sintaxis. Es muy importante colocar correctamente todas las llaves, los puntos, los puntos y coma, las comillas, etc, ya que en caso contrario el servicio DNS no arrancará o no funcionará correctamente.

Para corregir este tipo de errores existe una herramienta administrativa diseñada para comprobar la correcta configuración sintáctica del archivo. Para su utilización ejecutaremos el comando:

named-checkconf nombre_de_fichero

El fichero al que hace referencia puede ser cualquiera de los ficheros de configuración de bind9.

Ejemplos:

named-checkconf /etc/bind/named.conf

named-checkconf /etc/bind/named.conf.options

named-checkconf /etc/bind/named.conf.local

named-checkconf /etc/bind/named.conf.default-zones

2. Ficheros de configuración

En la instalación por defecto el fichero **named.conf** está formado por otros tres ficheros de configuración que se añaden a él mediante la sentendia **include**.

Sentencia **include**.- El contenido del fichero al que hace referencia se añadirá al fichero contenedor (**named.conf**) en la posición en la que aparezca dicha sentencia. Pueden aparecer tantas sentencias **include** como deseemos.

La forma general es:

include "nombre_de_fichero";

Hoy en día, por motivos organizativos, en lugar de añadir información al fichero **named.conf** de forma indiscriminada, se utilizan los ficheros añadidos mediante la sentencia **include** para dividir de forma más clara su contenido. Cada uno de ellos tiene una función básica que se puede intuir fácilmente por su nombre, siendo estas:

include "/etc/bind/named.conf.options"; → Opciones generales de configuración que se aplicarán a todo el servidor DNS.

include "/etc/bind/named.conf.local"; → Configuraciones DNS locales (zonas del usuario).

include "/etc/bind/named.conf.default-zones"; → Configuraciones DNS caché (zonas por defecto).

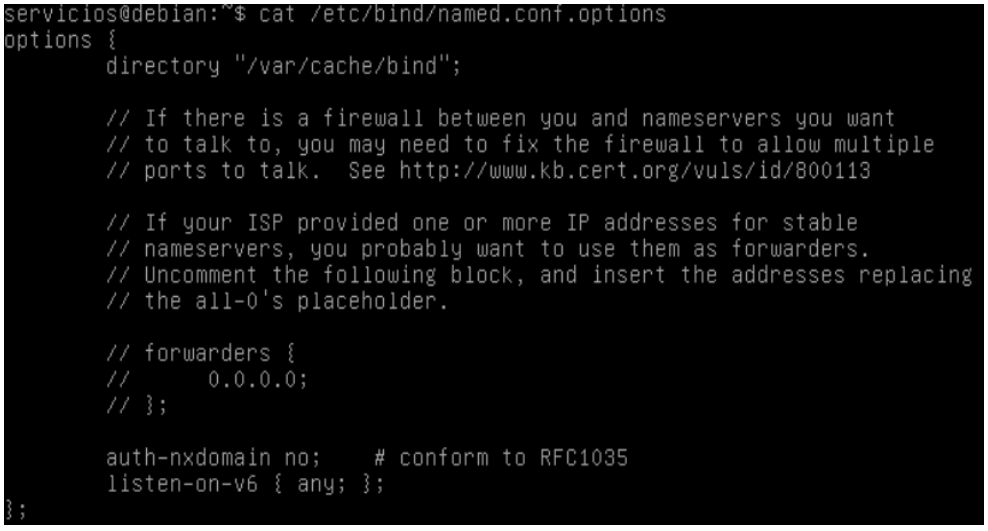
Nota: Siempre que modifiquemos cualquier fichero de configuración del sistema es importante realizar una copia de seguridad previa a los cambios, así como documentar dichos cambios mediante comentarios dentro del propio fichero.

2.1. Fichero named.conf.options

Su función es contener la sentencia **options**, utilizada para añadir a la configuración del servicio DNS una serie de características globales, es decir, se aplicarán a todas las zonas del servidor, tanto a las de defecto como a las añadidas por el administrador.

Sentencia **options**.- Tiene como función establecer valores a distintas opciones configurables del servidor DNS en general. La forma general es:

```
options{
  parametro1 valor1;
  …
  parametron valorn;
};
```



El contenido inicial habilita la utilización del directorio **/var/cache/bind** por compatibilidad con versiones anteriores, así como la utilización de IPv6 y otras opciones.

2.2. Fichero named.conf.local

Por defecto está vacío. Su función es contener la configuración de cada una de las zonas locales gestionadas por el servidor DNS y para ello utilizará sentencias **zone**.

Sentencia **zone**.- Establece la configuración de cada zona y el tipo de servidor DNS para dicha zona. La forma general básica es:

```
zone "nombre_de_dominio"{
   type tipo_zona;
   file "nom_fichero_def_zona";
};
```

Debe aparecer una sentencia **zone** por cada zona controlada por el servidor, por lo que pueden existir uno o varias sentencias tipo **zone** en el fichero **named.conf**.

- ***"nombre_de_dominio":*** *Nombre del dominio local a administrar.* Nota: La zona caché para acceder a Internet debe tener como nombre_de_dominio el valor ".".

- El parámetro **type** indicará el tipo de zona que controlará el servidor. Los tipos de zona básicos son:

  type master.- Hace referencia a una zona maestra.

  type slave.- Hace referencia a una zona esclava.

  type hint*.- Zona caché (lo veremos en el siguiente apartado).*

  Se debe tener en cuenta que pueden existir varias zonas dentro de un servidor, siendo estas del mismo tipo, de distinto o una mezcla de ambas.

- **file "nom_fichero_def_zona":** Nombre del fichero que contendrá los registros de recursos para la definición y gestión de la zona. Debería tener un nombre representativo.

  Nota: Aunque es posible configurarlo de otra manera, previo al nombre del fichero de definición de zona se debe especificar el directorio donde se encuentra, que en el caso de las zonas locales suele ser **/var/lib/bind/**.

Ejemplo zona local:

```
zone "lin.edu"{
   type master;
   file "/var/lib/bind/lin.edu.maestro";
};
```

La zona caché por defecto está definida en el fichero named.conf.default-zones y lo veremos en el siguiente apartado.

2.3. Fichero named.conf.default-zones

Contiene las sentencias **zone** de las zonas por defecto, es decir, de la **zona caché**, la **zona localhost** y las **zonas de resolución inversa** de localhost. No se debe modificar su contenido para no interferir con las resoluciones caché, resoluciones sobre Internet y consultas con los TNS.

3. Configuración básica de zona

La configuración básica más sencilla es un servidor DNS maestro sobre un dominio local, en el que se resolverá sobre los nombres de dominio de los equipo locales.

Supuesto el dominio ***lin.edu***, en el fichero ***named.conf.local*** deberíamos incluir:

```
zone "lin.edu"{
   type master;
   file "/var/lib/bind/lin.edu.maestro";
};
```

El fichero indicado en la opción *file* contendrá una serie de directivas y los registros de recursos necesarios para su gestión, recibiendo el nombre de **fichero de definición de zona**, es decir, en nuestro ejemplo, el **fichero de definición** de la zona lin.edu es /var/lib/bind/lin.edu.maestro.

3.1. Ficheros de definición de zona

El fichero de configuración de cada zona definida en el fichero de configuración local de bind9 (**named.conf.local**) puede almacenarse donde se desee, aunque normalmente lo encontraremos en **/var/lib/bind**.

El nombre a utilizar, una vez más, será el deseado, pero deberíamos utilizar un nombre que nos recuerde la zona a la que hace referencia, por ejemplo, podríamos utilizar la forma **nombre_dominio.maestro** para una zona maestra, **nombre_dominio.esclavo** para un servidor secundario, etc.

En este tipo de ficheros se encuentran dos elementos bien diferenciados, siendo el primero las directivas y el segundo los registros de recursos.

a) Directivas:

Las directivas están precedidas de del carácter (**$**) y son principalmente tres:

- ***$TTL valor_con_opción****.- Especifica el tiempo de vida (**T**ime **T**o **L**ive) por defecto de los registros de recursos en los servidores tipo caché. El valor del tiempo debe ir seguido (sin espacio en blanco) de la opción, que hace referencia a la unidad de medida temporal, pudiendo ser: s (segundos), m (minutos), h (horas), d (dias) y w (semanas).*

  Nota: También es posible indicar el TTL en la definición del registro de recursos SOA de la zona en cuestión.

  Ejemplo: ***$TTL 48h***

• *$**ORIGIN nombre_dominio.**.-* Establece el nombre de dominio por omisión, es decir, especifica el nombre de dominio que se añadirá a los nombres de los equipos que no finalizan en el carácter punto (**.**). No es necesario incluirla en el fichero de definición de zona, ya que por defecto toma el nombre de la zona finalizado en punto.

Ejemplo:

```
$ORIGIN lin.edu.
...
ftp IN A 172.26.25.50 → Equivale a ftp.lin.edu. IN A 172.26.25.50
```

Nota: En algunos casos de configuración avanzada se puede mezclar la opción por defecto con $ORIGIN buscando un efecto concreto como en el ejemplo del $INCLUDE.

• *$**INCLUDE nombre_fichero**.- El contenido del fichero indicado se incluye en la posición en la que aparezca la directiva.*

Ejemplo: Declaración de la zona lin.edu

```
...
ftp IN A 172.26.25.50
$INCLUDE /var/lib/bind/aula110
www IN A 172.26.25.100
...
```

Contenido del fichero aula110:

```
$ORIGIN aula110.lin.edu.
pc100 IN A 172.26.110.100
pc101 IN A 172.26.110.101
pc102 IN A 172.26.25.102
```

El resultado final conjunto de los $ORIGIN e $INCLUDE equivale a:

```
...
ftp.lin.edu.  IN A 172.26.25.50
pc100.aula110.lin.edu. IN A 172.26.110.100
pc101.aula110.lin.edu. IN A 172.26.110.101
pc102.aula110.lin.edu. IN A 172.26.25.102
www.lin.edu. IN A 172.26.25.100
(añadido por defecto por el nombre de la zona)
(añadido por $ORIGIN)
```

3.2. Registros de recursos

De entre las distintas opciones de configuración de registros de recursos estudiaremos las más importantes (SOA, NS, A y CNAME).

- **Registro SOA.-** (Start of Authority) Define una zona de autoridad. Es obligatorio al describir la zona maestra y es el primer registro de recursos que deberá aparecer. En él se definirán una serie de parámetros referentes a la relación entre el servidor maestro y el esclavo. Su sintaxis es:

nombre_dominio. IN SOA servidor. responsable. (parámetros)

Donde:

nombre_dominio.: Indica el nombre de dominio que se va a resolver. Si coincide con el indicado en la sentencia **zone** puede sustituirse por el carácter @.

IN: Hace referencia a un registro de recursos de **IN**ternet. Existen otras opciones que no estudiaremos aquí.

SOA: **S**tart **O**f **A**utority. Indica que el registro de recursos hace referencia al servidor maestro de la zona y sus opciones de configuración.

servidor.: Nombre de host del equipo que hace de DNS o nombre FQDN de dicho equipo en el dominio. En general, cuando sea necesario hacer referencia a un equipo, lo más correcto sería utilizar su nombre FQDN abreviado (sin finalizar en punto y sin el dominio), puesto que tenemos un servidor DNS para resolver.

responsable.: Cuenta de correo del responsable del DNS. La separación entre el usuario de correo y su dominio se realiza mediante el carácter punto (“.”) y cuando se utilice dicha información para establecer una conexión por correo electrónico se tomará como el carácter arroba (“@”).

parámetros: Son valores de sincronización con el esclavo. Hacen referencia a valores para el servidor esclavo y al tiempo de vida de los registros en el cache. Son varios y deben especificarse en un orden concreto y separados unos de otros por un espacio como mínimo. Aunque no exista un servidor esclavo deberán escribirse, aunque no se tomarán en cuenta, por lo que en estos casos podemos especificar (1 2 3 4 5). Los valores concretos de los parámetros los veremos cuando veamos los servidores esclavos.

Ejemplo:

lin.edu. IN SOA dns. correo.lin.edu. (1 2 3 4 5)

Se debe tener en cuenta que, como la sentencia **zone** y el nombre de dominio coinciden, lo anterior se podría haber escrito de forma resumida:

@ IN SOA dns. correo.lin.edu. (1 2 3 4 5)

Además, como podemos utilizar el nombre FQDN podríamos haberlo escrito como:

lin.edu. IN SOA dns.lin.edu. correo.lin.edu. (1 2 3 4 5)

También: **@ IN SOA dns correo (1 2 3 4 5)** → Teniendo en cuenta que deberá existir un registro **A** para el nombre **dns.**

- Registro NS.- Registro que identifica al servidor DNS con posibilidad de resolver sobre la zona. Deberá existir uno como mínimo, aunque también es posible que existan otros servidores con autoridad para la misma zona (secundarios o esclavos). Su sintaxis es:

nombre_dominio. IN NS servidor_autorizado.

Donde:

nombre_dominio.: Indica el nombre de dominio sobre el que se tiene autoridad. Puede no especificarse cuando el nombre de dominio coincide con el especificado en named.conf.local como nombre de zona.

servidor_autorizado.: Está formado por el nombre de equipo, teniendo en cuenta que lo más correcto sería utilizar su nombre FQDN abreviado (sin finalizar en punto y sin el dominio).

Ejemplo:

lin.edu. IN NS dns.

También: **lin.edu. IN NS dns.lin.edu.**

Como a los nombres que no finalizan en punto se les añade por defecto el nombre de la zona, podríamos resumirlo en: **IN NS dns ¿con @?**

- Registro A.- Identifica un equipo con un nombre de dominio asociado a una dirección IP.

Su sintaxis es:

nombre_equipo. IN A dirección_IP

Donde:

nombre_equipo.: Es el nombre del equipo al que asociaremos una dirección IP. Puede finalizar en un punto y ser un nombre FQDN dentro del dominio o no finalizar en punto y estar formado sólo por el nombre de equipo, teniendo en cuenta que en este caso, el servidor DNS añadirá automáticamente el nombre de la zona al nombre de equipo.

Ejemplo:

dns.lin.edu. IN A 172.26.25.15

Podríamos haberlo escrito como: **dns IN A 172.26.25.15** (.lin.edu. se añadirá por defecto extraído del nombre de zona, aunque también se puede añadir por $ORIGIN)

- Registro CNAME.- Sirve para crear alias a equipos cuyo nombre ya se ha definido y cuyo registro tipo **A** debe estar definido previamente. Igual que en el caso anterior se puede especificar el FQDN o abreviarlo. Su sintaxis es:

alias. IN CNAME nombre_equipo.

Donde:

alias.: Es el nuevo nombre de equipo con el que queremos referirnos a *nombre_equipo.*, del que previamente debe existir un registro tipo **A**.

Ejemplo:

ftp.lin.edu. IN A 172.26.25.16

…

srvftp.lin.edu. IN CNAME ftp.lin.edu.

También:

ftp IN A 172.26.25.16

…

srvftp IN CNAME ftp *(.lin.edu. se añadirá por defecto extraído del nombre de zona, aunque también se puede añadir por $ORIGIN)*

De forma parecida al caso de los ficheros de configuración, podremos verificar la integridad del contenido de los **ficheros de definición de zona**.

Existe otra herramienta administrativa para dicha comprobación que podremos utilizar mediante el comando:

named-checkzone nombre_dominio nombre_de_fichero_zona

Ejemplo: **named-checkzone lin.edu /var/lib/bind/lin.edu.maestro**

4. Configuraciones avanzadas

Como se estudió en la teoría, con los servidores DNS se pueden hacer múltiples configuraciones y combinaciones. Veremos ahora algunas de ellas:

4.1 Servidor DNS esclavo (secundario)

Se trata de un servidor copia de respaldo del servidor maestro (principal) capaz de resolver sobre su/s mismo/s dominio/s si el maestro no está disponible.

Se pueden crear tantos servidores DNS esclavos de un mismo dominio como queramos.

Además, podremos administrar que tras un cambio en el servidor maestro se informe inmediatamente a su/s esclavo/s (transferencia de zona) o se espere un determinado tiempo configurable.

Para crear un servidor esclavo debemos tener otro ordenador, distinto del servidor maestro, que realice dicho trabajo (En nuestro caso utilizaremos otra máquina virtual importada y cambiada su MAC durante la importación.

Se deben añadir algunos cambios en el servidor maestro y posteriormente configurar el nuevo servidor esclavo:

- En el **maestro**, en su fichero de definición de zona (*/etc/bind/named.conf.local*), debemos añadir un nuevo registro de recursos **NS** (uno por cada servidor esclavo) para especificar un nuevo servidor DNS con capacidad de resolver sobre la zona, así como el registro **A** del nuevo servidor DNS esclavo.

  Ejemplo:

…

IN NS dns

IN NS dns2 //servicor esclavo

…

dns2 IN A 172.26.25.103

...

- En el servidor **esclavo**, en su fichero de configuración local (/etc/bind/named.conf.local) se deberá crear una zona para el mismo dominio pero tipo esclavo (**type slave**), añadiendo una línea de configuración que indique cuál es el equipo maestro del dominio y especificando su fichero de configuración de zona que recibirá los datos de la transferencia de zona:

  Ejemplo:

  zone "lin.edu"{

  type slave;

  file "/var/lib/bind/lin.edu.esclavo";

  masters {172.26.25.100;};

  };

- A diferencia del servidor DNS maestro, el fichero de definición de zona con los registros de recursos no es necesario crearlo, puesto que se realiza la **transferencia de zona** desde el maestro, es decir, al arrancar el servidor DNS esclavo se pondrá en contacto con el maestro y se descargará la última y nueva versión del fichero con los registros de recursos del maestro copiándolo en la carpeta y nombre especificado en el esclavo (**/var/lib/bind/lin.edu.esclavo**), por lo que en este momento, si reiniciamos el servicio DNS en ambos servidores ya estarían funcionando y resolviendo maestro y esclavo para un mismo dominio.

Sincronización de los servidores DNS maestro y esclavo

Sobre los parámetros que nos veíamos obligados a especificar en la creación del servidor maestro y cuya funcionalidad es la sincronización con el esclavo (1 2 3 4 5), es ahora cuando trabajaremos con ellos, puesto que tenemos un servidor esclavo.

Cada uno de dichos cinco valores numéricos se expresan en **segundos**, tienen una funcionalidad y se deben especificar en este mismo orden concreto. Para estudiarlos utilizaremos el ejemplo:

```
lin.edu                 IN SOA  dns.lin.edu. correo.lin.edu. (
                                1          ; serial
                                2          ; refresh (2 seconds)
                                3          ; retry (3 seconds)
                                4          ; expire (4 seconds)
                                5          ; minimum (5 seconds)
                                )
```

serial → Numero de serie: Se utiliza para verificar los cambios en el fichero de definición de zona con el siguiente modo de funcionamiento: El administrador deberá aumentarlo en una unidad tras cada cambio del contenido del fichero. En caso de existir servidor DNS esclavo, mediante una solicitud al maestro, accederá a este valor y en caso de ser mayor del que tenga almacenado procederá con la actualización de su información de la zona (transferencia de zona). A nivel profesional se suele utilizar el valor **año_mes_dia_versión** con el formato **aaaammddvv**.

> Ejemplo: Si la segunda y última modificación se realizó el 1 de septiembre de 2012 especificaríamos el valor **2012090102**.

refresh → Periodo de refresco.- Indica el *tiempo en segundos que deben esperar los servidores esclavos en conectar con el maestro para ver si existe una actualización de la zona*. Se debe tener en cuenta que el tiempo de refresco se puede ver alterado por el parámetro **notify**.

> Ejemplo: Para indicar a los servidores esclavos que consulten con el maestro cada media hora (30 x 60 = 1800) por si existe una nueva versión de la zona especificaríamos el valor **1800**.

retry → Frecuencia de reintentos.- Indica el tiempo en segundos que deberá esperar el servidor esclavo en caso de que el maestro no contestara a su solicitud de verificación de zona una vez transcurrido el periodo de refresco, para volver a preguntar.

> Ejemplo: Supongamos que en caso de caída del maestro queremos que el esclavo realice un nuevo intento de conexión cada minuto, por lo que especificaremos el valor **60**.

expire → Tiempo de expiración.- Tiempo máximo que mantendrá el servidor esclavo la información sobre la zona sin tener conexión con el maestro. Trascurrido dicho tiempo la información sobre la zona se perderá.

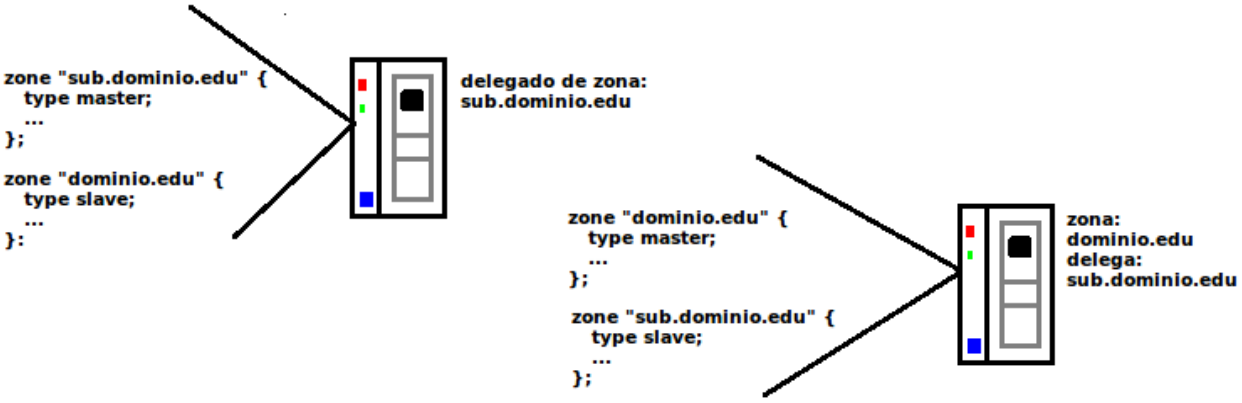
> Ejemplo: Supongamos que deseamos que el servidor esclavo mantenga la información sobre la zona 1 día sin conexión con el maestro (24 x 60 x 60 = 86400), en dicho caso especificaremos el valor **86400**.

minimum → TTL mínimo.- Tiene la misma función que la directiva $TTL. El valor mínimo admitido de TTL es de 30 minutos (si se indica uno menor se ignorará), aunque se deberá expresar en segundos. Ejemplo: Supongamos que se desea mantener los registros del servidor caché un total de media hora (45 x 60), con lo que deberíamos especificar el valor **2700**.

4.2. Delegación de zona

Una delegación de zona consiste en **ceder la gestión y administración de un dominio o una parte del dominio a otro servidor maestro**.

Si deseamos (de forma opcional) que las zonas principales y delegadas sean respondidas por cualquier servidor del dominio, tanto principal como delegado, se deberá añadir el servidor de la zona delegada como esclavo de la zona principal y viceversa, es decir, el servidor delegado deberá añadir como servidor esclavo para su zona delegada al principal.



Las configuraciones de las zonas delegadas son exactamente igual que las zonas autorizadas, teniendo en cuenta que en algunos casos utilizaremos como zona un subdominio del dominio principal.

5. Opciones avanzadas de servidor DNS.

Existe una multitud de parámetros que podemos incluir en la sentencia **options**, (named.conf.options), con lo que se aplicarán a todas las zonas del servidor o de forma individual en cada sentencia **zone** (named.conf.local), en cuyo caso se aplicará sólo a dicha zona y siendo esta última la manera más común de configuración.

Cuando las opciones que se aplican dentro de una sentencia **zone** entran en conflicto con las globales, la prioridad de cada zona es superior a la global, es decir, se aplican las opciones indicadas en la zona.

Entre estas opciones podemos encontrar:

- **directory "path".**- Su función es indicar el directorio de trabajo del servidor DNS. En caso de aparecer permitirá escribir el resto de las rutas hasta los ficheros de trabajo de forma relativa, ya que el sistema operativo tomará el resto de la ruta, hasta hacerla absoluta de dicho valor de path. En caso de aparecer dicho parámetro suele ser el primero.

Ejemplo en sentencia options:

```
options{
  directory "/var/lib/bind";
  ...
};
```

Ejemplo en sentencia zone:

```
zone "lin.edu"{
  directory "/var/lib/bind";
  type master;
```

```
  file "lin.edu.maestro";
};
```

- **port num_puerto**.- Especifica el número de puerto por el que el servidor DNS recibe y envía el tráfico causado. Puede no especificarse este parámetro, en cuyo caso, el valor por defecto es el puerto 53. Nota: Se recomienda no cambiarlo.

Ejemplo:

```
options{
  …;
  port 53;
  …;
};
```

- **allow-query {id_red1; id_red2; …; id_redn;}**.- Especifica los equipos a los que se les permite hacer consultas a ese servidor DNS, es decir, se permite la consulta si el equipo pertenece a una de las redes indicadas. Se puede especificar una red, una lista de ellas, una subred, una IP concreta, etc. Nota: Fijarse en que se debe incluir una lista de direcciones IP separadas por el carácter punto y coma, incluso para el último valor de la lista.

También es posible utilizar la sentencia **acl (ac**cess **l**ist o lista de acceso**)**, para indicar las redes permitidas. Para indicarlo deberemos expresar la palabra clave **acl**, seguida del nombre de la lista de acceso entre comillas dobles y para finalizar especificaremos las redes entre llaves y separadas por punto y coma, con un punto y coma al final. La sentencia **acl** deberá aparecer definida fuera y antes de **options** o **zone**.

Ejemplo 1:

```
options{
  …;
  allow-query {172.26.0.0/16; 192.168.1.0/24;};
  …;
};
```

Ejemplo 2:

```
acl "clientesdns" {172.26.0.0/16; 192.168.1.0/24;};
options{
  …;
  allow-query {"clientesdns";};
  …;
};
```

- **notify *yes* | explicit | no**.- Permite configurar las notificaciones a realizar sobre los servidores esclavos cuando se produce algún tipo de modificación sobre la zona que controla. Se debe elegir una y sólo una de las tres y la opción por defecto es **yes**, es decir, al producirse algún cambio se envían mensajes de notificación a aquellos

servidores con los registros de recursos NS de la zona que controlan, por lo que los servidores esclavos no necesitarán esperar al tiempo de refresco para su actualización. En caso de especificar el valor **no**, no se enviarán dichas notificaciones y los servidores esclavos deberán esperar a que se cumplan su tiempo de refresco para conectarse y verificar si existen cambios. En caso de asignarle el valor **explicit**, únicamente serán enviadas notificaciones a los servidores recogidos en el parámetro **also-notify**.

```
Ejemplo:
options{
  …;
  notify yes;
  …;
};
```

- **also-notify** {ip_servidor_esclavo1; ip_servidor:esclavo2; …;}.- Permite indicar los servidores esclavos a los que se enviará notificación cuando se produce un cambio en la zona maestra y está configurado el valor **notify** a **explicit**. Nota: Fijarse en que se debe incluir una lista de direcciones IP separadas por el carácter punto y coma, incluso para el último valor de la lista. No tiene sentido sin el parámetro **notify explicit**.

Ejemplo:

```
options{
  …;
  notify explicit;
  also-notify {172.26.25.50; 172.26.25.30;};
  …;
};
```

- **forward *first* | only.**- Su función es indicar el servidor DNS al que se realizará un reenvío de la consulta DNS no satisfecha si fuera necesario. Es decir, si este servidor DNS no puede dar respuesta a la consulta, dicha consulta se reeenviará al servidor DNS indicado en el parámetro "forwareders". La opción por defecto es **first**, lo que provoca que, en caso de ser necesario, pregunte por orden a los servidores indicados en la lista de **forwarders** y si no se termina de resolver la consulta terminará por preguntar a los servidores TNS. En caso de especificar **only** únicamente preguntara a los servidores de la lista de **forwarders** y si no responden no podrá hacer la resolución. No tiene sentido sin el parámetro forwarders.

Ejemplo:

```
options{
   …;
  forward first;
  …;
};
```

- **forwarders {ip_servidor_reenvio1, ip_servidor_reenvio2, ...;}**. Su función es indicar los servidores a los que preguntar en caso de ser necesario. Nota:

Fijarse en que se debe incluir una lista de direcciones IP separadas por el carácter punto y coma, incluso para el último valor de la lista. No tiene sentido sin el parámetro forward.

Ejemplo:

```
options{
  …;
  forward first;
  forwarders {172.26.25.99; 172.26.25.66;};
  …;
};
```

6. Configuración de la resolución inversa.

En principio deberá existir una zona de resolución inversa como mínimo por cada una de las zonas de resolución directa del maestro. De forma análoga a las zonas directas, se deberá especificar su valor en el fichero de configuración de zona y sus registros de recursos en su fichero de definición de zona.

Ejemplo zona local y zona inversa en el fichero de configuración de zona:

```
zone "lin.edu"{
  type master;
  file "/var/lib/bind/lin.edu.maestro";
};
zone "26.172.in-addr.arpa" {
  type master;
  file "lin.edu.maestro.inversa";
};
```

Teniendo en cuenta que en el **fichero de definición de zona** directa *lin.edu.maestro* tenemos:

```
$TTL 48h
@ IN SOA dns correo (1 2 3 4 5)
 IN NS dns
dns IN A 172.26.25.100
ftp IN A 172.26.25.101
www IN A 172.26.25.102
ftpvillablanca IN CNAME ftp
villablanca IN CNAME www
```

```
alumnos IN CNAME www
profesores IN CNAME www
```

En el fichero **lin.edu.maestro.inversa** deberíamos tener, además de los registros de inicio de autoridad y de servidor de nombres, un registro de resolución inversa para todos y cada uno de los registros de dirección (**A**) de la zona maestra directa, no siendo necesario su especificación para los alias, aunque también se podrían añadir.

```
$TTL 48h
@ IN SOA dns.lin.edu. correo.lin.edu. (1 2 3 4 5)
    IN NS dns.lin.edu.
100.25 IN PTR dns.lin.edu.
101.25 IN PTR ftp.lin.edu.
102.25 IN PTR www.lin.edu.
```

Si añadiéramos los alias:

```
101.25 IN PTR ftpvillablanca.lin.edu.
102.25 IN PTR villablanca.lin.edu.
102.25 IN PTR alumnos.lin.edu.
102.25 IN PTR profesores.lin.edu.
```

MUY IMPORTANTE: Se debe tener en cuenta que se deberá especificar el nombre de equipo en su versión completa del FQDN, puesto que si no se incluye el dominio y se deja sin punto añadiría el nombre de la zona que es 26.172.in-addr.arpa.

Para comprobar la integridad del fichero de zona inversa ejecutamos el comando:

named-checkzone 26.172.in-addr.arpa /var/lib/bind/lin.edu.maestro.rev

Sólo falta reiniciar el servicio DNS comprobar las resoluciones directas e inversas, por ejemplo mediante **nslookup**.