Índice

1. Introducción

Normalmente, al registrar un **dominio en Internet**, la empresa o Agente registrador, además de realizar el registro, nos proporciona el servicio de **servidor maestro**. Esto es, cualquier dato referente a nuestro dominio tendrá que ser buscado en el servidor que se nos facilita. De esta forma, las empresas que nos registran el dominio nos facilitan el acceso remoto al servidor maestro para poder introducir los registros de recursos (RR) que necesitemos, para ese dominio.

Si tengo un servidor de aplicaciones en una IP fija XXX.XXX.XXX.XXX y quiero responda a ***www.mi_dominio.com,*** *tengo que incluir el registros de recursos de tipo A correspondiente en el servidor maestro.*

En esta práctica se instalará y configurará un servidor de nombres (**bind9**) en un máquina **virtual Ubuntu** que actuará como servidor maestro de una zona local y se definirá una estructura de dominios y subdominios mediante la definición de los registros de recursos correspondendientes.

2. Servidor DNS Bind9

BIND (*Berkeley Internet Name Domain*) Es el servidor DNS utilizando más

frecuentemente, sobre todo en sistemas operativos tipo Unix. De hecho, se trata de un *estándar de facto*. Actualmente, podemos encontrar **2**

versiones de BIND. BIND y BIND 9 (release 9 de Bind). BIND 9 fue reescrito desde cero para mejorar BIND y para añadir nuevas funcionalidades y soporte para DNSSEC (DNS Security Extensions). Las versiones antiguas de BIND, al igual que ocurre con otros programas, como sendmail, son conocidos por su gran número de vulnerabilidades por lo que es recomendable el uso de del servidor **Bind 9**.

2.1 Instalación del servicio

Las instalación del servicio se llevará a cabo a partir del gestor de paquetes **synaptic**.
Los paquetes a instalar son ***bind9*** *y* ***bind9-doc.***

```
$ sudo apt install bind9 bind9-doc dnsutils
```

Una vez, instalado podemos gestionar el demonio **bind9** utilizando el comando `systemctl` o su correspondiente `service`.

`systemctl [start|stop|restart] bind9`	`service bind9 [start|stop|restart]`

Si no configuramos nada más, por defecto nuestro servidor DNS funcionará como un servidor de nombres ***caché****.*

2.2 Estructura de directorios.

Los ficheros de configuración del daemon bind (siguiendo los estándares de Debian GNU/Linux) se encuentran bajo la carpeta `/etc/bind`.

Los ficheros más importantes implicados son:

- `db.root` : fichero donde están las direcciones IP de los **servers root** que contienen información sobre los nombres de dominio de nivel superior o TLD's.
- `db.local`: archivo de configuración DNS de la **zona localhost.**
- `named.conf`: archivo de configuración principal desde el cual se llevará a cabo la inclusión de todos los demás.
- `named.conf.options`: archivo de especificación de opciones extra. Un ejemplo de uso puede ser la configuración de un **servidor DNS** de nombres al que queremos reenviar **(forwarder)** las peticiones que no se encuentran de forma local en nuestro servidor.

- `named.conf.local`: archivo de especificación/configuración de las zonas que maneja el servidor.
- `named.conf.default-zones`: Este archivo contiene las referencias a las zonas que el sistema crea por defecto. A continuación se detallan las principales:
  - **Zona "." o zona raíz:** Hace referencia al fichero `/etc/bind/db.root` donde se encuentran los registros de recursos de los 13 servidores DNS raíz. Que utilizará el servidor cuando no encuentre el dominio solicitado en caché.
  - **Zona de localhost y su resolución inversa** 127.0.0.0 (127.in-addr.arpa). Hacen referencia a los archivos/etc/bind/db.local y /etc/bind/db.127, respectivamente. Nos proporciona la resolución del nombre de máquina localhost.
  - **Zona de resolución inversa de difusión o broadcast** (255.in-addr.arpa). Hace referencia al archivo/etc/bind/db.255.

Puedes consultar más información sobre la configuración del servicio DNS en la documentación oficial para ubuntu.

Ejercicio 1 (1 punto)

Instala el servidor **Bind9**, edita el fichero `/etc/bind/named.conf.options` y configura como servidor de reenvío el servidor DNS abierto de google (ip -> 8.8.8.8), para las zonas que no administre nuestro servidor:

```
forwarders {
    8.8.8.8;
};
```

Comprueba que tu DNS está funcionando **como caché**. Para ello, realiza resoluciones de nombres de dominio de Internet con el comando dig, y comprueba el tiempo que tardan. ¿Qué debe ocurrir si nuestro DNS está funcionando como caché?

2.3 Configuración del Servidor Maestro

En primer lugar debemos tener claro qué tipo de servidor queremos configurar. Tenemos:

- **Primary masters:** Lee el archivo de zona de un fichero del propio servidor.

- **Secondary masters o slave:** Lee el archivo de zona del master server que tiene autoridad en la zona. También son conocidos como servidores esclavos. El proceso de conexión del **servidor secundario** al principal para obtener la información de la zona se llama **transferencia de zona** (zone transfer). No obstante, debemos tener claro que tanto el servidor primario como el secundario o secundarios son servidores autorizados de la zona. Esta relación facilita la gestión de la zona ya que solo hay que mantener un archivo de zona en el servidor primario y todos los demás servidores secundarios se sincronizan con éste.

> En esta práctica nos centraremos en la la configuración de un **servidor DNS** primario

2.3.1 Sintaxis

Antes de configurar las zonas deberemos tener en cuenta una serie de consideraciones a nivel de sintaxis de los ficheros de zona:

$TTL	Establece el tiempo de vida por defecto. Cada zona puede sobrescribir este valor.
@	Se puede utilizar para referirse a nombre de dominio base de la zona que estamos configurando
;	Permite insertar comentarios en el fichero de configuración de la zona

2.3.2 Ficheros de zona

El primer paso **para la definición de una nueva zona** en el servidor, es la creación de un archivo de zona. Debemos tener en cuenta que cada uno de los dominios que compremos y queremos albergar, dispondrá de su propio archivo de zona. En lo que sigue supondremos que el dominio que queremos configurar es `ddaw.lan` y que las direcciones IP asignadas de la red son **`172.16.211.0/24`.**

Creación de zona de búsqueda directa

1. Para la configuración de una zona, deberemos declararla en el fichero `named.conf.local` del servidor. Para ello editamos el fichero e incluimos las siguientes líneas:

/etc/bind/named.conf.local

```
zone "ddaw.lan" in  { //La zona es ddaw.lan
      type master; //Este servidor será primario para la zona
      file "/etc/bind/db.ddaw.lan"; //fichero de registros de zona
};
```

2. Seguidamente crearemos el fichero de registros de zona `db.ddaw.lan` en el directorio `/etc/bind` que representará la base de datos para la zona del dominio que vamos configurar. En él definiremos todos los registros de recursos de los subdominios que queramos resolver en nuestra zona. Esto es, si tenemos un servidor web que está en la IP 172.16.211.1, y queremos acceder mediante el nombre de dominio www.ddaw.lan incluiremos un nuevo registro en el archivo de zona. (Podemos tomar como base el fichero que representa la zona local `etc/bind/db.local`)

db.ddaw.lan

```
$TTL    604800
@       IN      SOA     ns1.ddaw.lan. admin.ddaw.lan. (
                         1          ; Serial
                         604800     ; Refresh
                         86400      ; Retry
                         2419200    ; Expire
                         604800 )   ; Negative Cache TTL
;
@       IN      NS      ns1.ddaw.lan.
@       IN      NS      ns2.ddaw.lan.
ns1     IN      A       172.16.211.2
ns2     IN      A       172.16.211.3
www     IN      A       172.16.211.1
@       IN      MX  1   mail.ddaw.lan.
mail    IN      A       172.16.211.10
```

Registro SOA

Registros de Recursos

El símbolo **@** es equivalente a definir **el nombre de dominio** principal de la zona que estamos configurando, en este caso `ddaw.lan.`

Si al definir un **nombre de dominio,** éste **no acaba en "."** automaticamente se le **añadirá la parte del dominio principal** de la zona que estamos configurando. En

el ejemplo **ns1 equivale a** definir `ns1.ddaw.lan.`

La **primera definición** que podemos ver en el archivo de zona anterior, es un registro de tipo **SOA**. Éste nos proporciona información sobre la zona (ddaw.lan.) que estamos configurando. En él se especifica que **el servidor de nombres primario** para la zona es el servidor `ns.ddaw.lan.` y que el email del responsable es admin.ddaw.lan (admin@ddaw.lan).

A continuación se definen una serie de entradas, llamadas **Registro de recursos**, cada una de estas entradas nos permiten asociar subdominios de la zona que tienen la forma **xxx**.ddaw.lan. con las direcciones IP de cada uno de ellos.

En la **primera** línea indicamos que disponemos de **2 servidores de nombres** para el dominio que hemos comprado (zona), estos son `ns1.ddaw.lan.` y `ns2.ddaw.lan.` De ellos, tal y como **indicaba el registro SOA**, **el servidor primario** es `ns1.ddaw.lan.` *(Nótese que el servidor `ns2.ddaw.lan` se indica a modo de ejemplo).*

No obstante, los servidores de nombres `ns1` y `ns2` todavía **no tienen asignada ninguna IP** de la máquina en la que se encuentran, para ello **tenemos** que **crear un registro de tipo A** para cada uno de ellos. En el ejemplo (**líneas 3 y 4**) se indica que los servidores de nombres se encuentran en las ip's `172.16.211.2` y `172.16.211.3`

En la **quinta línea** se esta indicando que el subdominio `www.ddaw.lan.` corresponde a la ip `172.16.211.1`, Es decir, que cuando accedemos desde el navegador a ese subdominio nos enviará directamente al host con la ip `172.16.211.1`.

Finalmente, en la última línea se indica que el servidor de correo para el dominio `ddaw.lan` es `mail.ddaw.lan.`

Una vez **configurada la zona**, comprobaremos que ha sido definida correctamente mediante la orden $ named-checkzone.

```
ddaw@ubuntuserver:/etc/bind$ sudo named-checkzone ddaw.lan
/etc/bind/db.ddaw.lan
zone ddaw.lan/IN: loaded serial 1
OK
```

A continuación reiniciaremos el servidor:

```
ddaw@ubuntuserver:/etc/bind$ sudo service bind9 restart
```

y **comprobaremos si el servidor de nombres** que acabamos de configurar es capaz de **proporcionarnos la IP** de alguno de los registros de recursos (dominios) que acabamos de configurar. En este caso, y considerando que el servidor de nombres está en la ip 127.0.0.1, **utilizaremos el cliente DNS dig**, para preguntar por el registro `www.ddaw.lan`.

```
ddaw@ubuntuserver:/etc/bind$ dig @127.0.0.1 www.ddaw.lan

; <<>> DiG 9.16.1-Ubuntu <<>> @127.0.0.1 www.ddaw.lan
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27965
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 326a59fb3ab5f69601000000601dc5934e41734d0300ef61 (good)
;; QUESTION SECTION:
;www.ddaw.lan.                  IN     A

;; ANSWER SECTION:
www.ddaw.lan.       86400      IN     A      172.16.39.31

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Feb 05 22:24:19 UTC 2021
;; MSG SIZE  rcvd: 85
```

Creación de zona de búsqueda inversa

Hasta el momento hemos configurado la zona para la traducción de nombres de dominio en direcciones IP. Para terminar de configurar correctamente la zona, deberemos configurar la **resolución inversa**, que nos permitirá llevar a cabo la traducción de direcciones IP en nombres de dominio.

1. Al igual que en caso anterior, damos de alta una nueva zona el archivo `named.conf.local`, dentro del dominio especial `in-addr.arpa` y que corresponde a la red `172.16.211.0/24`

/etc/bind/named.conf.local

```
zone "211.16.172.in-addr.arpa" in  {
        type master;
        file "/etc/bind/db.211.16.172
};
```

2. Creamos el fichero `db.211.16.172` en el directorio `/etc/bind` y damos de alta los registros de recursos que necesitemos.

db.211.16.172

```
$TTL    604800
@       IN      SOA     ns1.ddaw.lan. admin.ddaw.lan. (
                         1          ; Serial
                         604800     ; Refresh
                         86400      ; Retry
                         2419200    ; Expire
                         604800 )   ; Negative Cache TTL
;
@       IN      NS      ns1.ddaw.lan.
@       IN      NS      ns2.ddaw.lan.
1       IN      PTR     www.ddaw.lan.
10      IN      PTR     mail.ddaw.lan.
2       IN      PTR     ns1.ddaw.lan.
3       IN      PTR     ns2.ddaw.lan.
```

Registro SOA

Registros de Recursos

La primera parte del fichero no varía respecto a la configuración del fichero de la zona directa. No obstante, como se ve en las **líneas 3 y 4** de la zona marcada como **registro de recursos**, estamos configurando 2 registros para que cuando se pregunte por la IP del servidor `172.16.211.1`, el servidor DNS devuelva el dominio `www.ddaw.lan` y cuando se pregunte por la ip `172.16.211.10` se devuelva el dominio `mail.ddaw.lan`.

Debemos tener en cuenta que solo se indica el último octeto de la ip `172.16.211.10` ja se está configurando la zona inversa `172.16.211`.

Ejercicio 2 (1 punto)

1. Investiga la funcionalidad que proporcionan las zonas de búsqueda inversa. Cita un ejemplo de aplicación y/o servicio que haga uso de ellas, y para qué lo utiliza. (**0.5 puntos**)

2. Para revisar que los archivos están bien configurados puedes ayudarte de los

comandos **named-checkconf** y **named-checkzone**. Busca información sobre como se utilizan y la función que realiza cada uno de ellos. (**0.5 puntos**)

3. Bibliografía / Webgrafía

- Instalación y configuración de un servidor DNS. "https://help.ubuntu.com/lts/serverguide/dns-configuration.html". Ubuntu.com
- Instalación y configuración de un servidor DNS de cache y reenvío. "https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-caching-or-forwarding-dns-server-on-ubuntu-16-04". Digital Ocean.
- Instalación y configuración de un servidor DNS en una red privada. "https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04." Digital Ocean.