Índice

SA05-AQ5.1 – Instalación y configuración de un servidor DNS primario. Bind9

1. Introducción

Normalmente, al registrar un **dominio en Internet**, la empresa o Agente registrador además de realizar el registro nos proporciona un **servidor DNS** que actuará como **servidor maestro** para la **nueva zona** que acabamos de crear. Esto es, que cualquier nuevo registro dentro de la zona a la que hace referencia el dominio comprado tendrá que ser añadido en este servidor. 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.

*Si tengo un servidor de aplicaciones en una IP fija XXX.XXX.XXX.XXX y quiero que responda a **www.mi_dominio.com,** tendré que comprar el dominio **mi_dominio.com** e incluir un registro de recursos de tipo A en el servidor maestro que nos proporciona el proveedor.*

En esta práctica se instalará y configurará un servidor de nombres maestros (**bind9**) en un maquina **virtual Ubuntu** que actuará como servidor maestro de una zona local y se añadirán registro para las diferentes aplicaciones configuradas en las practicas anteriores.

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 *standard 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

La 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]`

Como se ha comentado anteriormente, 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 extras. Un ejemplo de uso puede ser la configuración de un **servidores dns** de nombres al que queremos reenviar **(forwarders)** 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

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

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

→ Comprueba que tu dns está funcionando **como caché,** para ello, realiza resoluciones de nombres de dominio de Internet y comprueba el tiempo que tardan. ¿Qué debe ocurrir si nuestro dns está funcionando como caché?

Recuerda abrir **el puerto 53** en el **firewall del servidor** para realizar peticiones desde la **red interna**

Si te encuentras dentro del **centro educativo**, será necesario que desactives la validación del DNS mediante la siguiente directiva `dnssec-validation no;`

2.3 Configuración del Servidor Maestro

En primer lugar debemos tener claro qué tipo de servidor queremos configurar. Como se ha comentado en clase 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 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 sólo hay que mantener un archivo de zona en el servidor primario y todos los demás servidores secundarios se sincronizan con este.

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

queramos 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.local
      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. (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 registro **SOA** nos proporciona información sobre la zona que estamos configurando. En él, se especifica que el servidor de nombres primario para la zona es el servidor `ns1.ddaw.lan.`

La parte indicada en la tabla anterior como **Registro de recursos**, posee una entrada por cada uno de los subdominios y/o recursos que necesitamos configurar.

En la **primera y segunda** línea indicamos que los servidor de nombres para la zona 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 ya que en esta práctica solo vamos a configurar un servidor de nombres).*

Debemos tener en cuenta que, con los datos analizados, los servidores de nombres `ns1` y `ns2` todavía no tienen asignada la ip que indica el host donde 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 linea** 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 sub-dominio nos enviará directamente al host con la ip `172.16.211.1`.

Ejercicio 2

→ Para revisar que los archivos están bien configurados puedes ayudarte de los comandos **named-checkconf** y **named-checkzone**. Busca información sobre como se utilizarlos y la función que realiza cada uno de ellos.

Ejercicio 3

→ Crea una nueva instancia en AWS, etiquétala con el nombre **ud5-a2-dns** y asígnale una dirección IP elástica.

→ Instala un servidor **DNS bind9,** y añade una zona directa para el dominio `grupoX.ddaw.es` . Deberá contener, como mínimo, registros de recursos para siguientes host:

- Un registro para cada uno de los siguientes servidores de aplicaciones:
  - `app1.grupoX.ddaw.es` → 172.16.224.21

- `app2.grupoX.ddaw.es` → 172.16.224.22
- `app3.grupoX.ddaw.es` → 172.16.224.23

2. Un registro para el servidor de correo `mail.grupoX.ddaw.es` que corresponderá al host 172.16.224.24.

3. Un registro de tipo TXT que nos permita insertar texto para verificar ante un tercero que el dominio nos pertenece. El texto asociado que debe aparecer es "google-site-verification=qW2WOnmUMDHWaF-2Tgfyzmwyk2BqWg4dghWqvW0PY8c8"

4. Asocia el subdominio `www.grupoX.ddaw.es` a una de las aplicaciones configuradas en el punto 1. Deberás hacerlo mediante un nombre de canónico.

Comprueba el correcto funcionamiento de cada uno de los registros. Recuerda que como las máquinas con las IP's anteriores no existen deberas probarlo con uno de los clientes DNS vistos en la actividad 1.

Tras la las diferentes pruebas que vayamos realizando durante la configuración del servicio, podría ser necesario, eliminar la cache, para ello haremos uso de la **herramienta rndc,** que nos permite **gestionar el servidor dns** mediante línea de comandos

```
$sudo rndc flush
$sudo rndc reload
```

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.