INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR DNS EN SO LINUX

1. Para empezar, es necesario tener conexión a Internet desde la máquina y tener configurados correctamente los repositorios que se encuentran localizados en la ruta */etc/apt/source.list*. A partir de aquí se ejecutan los comandos **(en modo root)**:

```
apt-get update
apt-get upgrade.
```

   a. *update*: actualiza la lista de paquetes disponibles y versiones, pero no actualiza ningún paquete. Esta lista se selecciona de los servidores con repositorios que se definen en el *source.list*.
   b. *upgrade*: instalará las nuevas versiones respetando la configuración del software, cuando sea posible.

2. Una vez actualizados los repositorios, comenzamos la instalación de bind9 y de sus utilidades, y ello se realiza a partir del siguiente comando (entrando como usuario root):

```
apt-get install bind9
```

3. Posteriormente, se puede comprobar que el servicio DNS (bind9) se ha instalado correctamente. Para ello se usan los siguientes comandos:

```
systemctl start named
systemctl | grep running
```

   También podemos comprobarlo mediante los comandos:

```
service named start
service named status
```

4. Una vez comprobado que el servicio está correcto, se está en disposición de configurar nuestro servidor DNS. En la carpeta bind tienes todos los archivos necesarios de configuración. El primer fichero que lee el servicio bind9 es el *named.conf*. No es necesario modificar nada en principio. Para verlo podemos ejecutar:

```
cat /etc/bind/named.conf
```

Este fichero incluye tres ficheros importantes que va a leer el servicio bind9, que son los siguientes:

> *named.conf.options*: en este primer fichero se define la caché de nuestro DNS, y la configuración genérica del servidor, como puede ser la transferencia de zonas, forwarders, etc. La configuración más importante de este fichero son los forwarders (reenviadores), ya que es necesario configurarlos para que cuando un cliente realice una consulta DNS y no encuentre la respuesta en local, la respuesta se pueda encontrar en Internet, como puede ser el nombre de un servidor, un sitio web, un servidor de correo, etc. Por lo general, son los servidores DNS de nuestro ISP, Google, Telefónica, etc. Se puede poner por ejemplo el DNS de Google, 8.8.8.8.

> *named.conf.local*: este fichero es tan importante como el anterior, y es donde se definen las zonas de búsqueda directa e inversas. Como ejemplo se va a localizar un dominio denominado www.prueba.com , y los ficheros para la zona directa e inversa son respectivamente *prueba.local* y *prueba.127*, para seguir una nomenclatura. Las zonas en un principio son de tipo master (recordamos que las zonas pueden ser de tres tipos: máster, slave y cache).

> *named.conf.default-zones*: es un fichero donde se definen las zonas por defecto. La inclusión de este fichero se puede comentar. Realmente donde se definen las zonas nuevas es en el fichero named.conf.local.

5. Ahora vamos a configurar el servidor. En la carpeta bind están los archivos necesarios. Con el comando ls y la opción -l puedes listar todos los archivos con algunos detalles:

```
ls -l /etc/bind
```

6. Continuamos con los archivos de configuración. Vamos a añadir un reenviador (forwarders) al archivo *named.conf.options*. Editamos y añadimos la siguiente línea de código:

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

7. Como hemos comentado antes, vamos a tomar como ejemplo la localización de un dominio denominado www.prueba.com. Para ello editamos el archivo *named.conf.local*:

```
//Búsqueda directa
zone "prueba.com"{
type master;
file "/etc/bind/prueba.local";
};

//Búsqueda inversa
zone "2.0.10.in-addr.arpa"{
type master;
file "/etc/bind/prueba.127";
};
```

8. Los siguientes archivos para configurar son prueba.local y prueba.127. Tales ficheros nos permitirán definir los registros DNS, que posteriormente se van a resolver para dar respuesta a las peticiones de nuestros clientes DNS. Deberemos tener permisos de super usuario (root) para crear el archivo en la carpeta /etc/bind. Podemos tomar y hacer una copia del archivo *"db.local"* y guardarlo con el nombre de *"prueba.local"*. El archivo debe quedar como el de la imagen:

```
┌──(root㉿kali)-[/etc/bind]
└─# cat prueba.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     prueba.com. root.prueba.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      prueba.com.
@       IN      A       10.0.2.15
dns     IN      A       10.0.2.15
server2003 IN    A      10.0.2.20
www     IN      CNAME    prueba.com.
```

Se va a detallar a continuación las diferentes opciones que posee el fichero de zona directa:

> *$TTL (Time to Live)*: indica la duración en segundos que se conservarán los datos en memoria caché.

> *Nombre Zona*: FQDN[1] de la zona administrada por este archivo, los nombres de zona deben acabar en punto, de lo contrario dará error en el chequeo de los archivos. Usualmente se pone @ para no cargar demasiado al archivo. Es necesario declarar el registro NS y A para que la zona conozca tanto el dominio como la IP del servidor DNS que suministra la zona.

> *IN*: esta opción es obsoleta pero es la única que se puede usar hasta la fecha. Es la clase de Internet.

> *SOA (Start of Authority)*: registro obligatorio para indicar que el servidor actual es el propietario y legítimo de esta zona.

> *Serial*: número de serie del archivo, se usa cuando la zona se replica a otros servidores.

> *Refresh*: valor numérico que se utiliza cuando la zona se replica a un servidor esclavo, y el intervalo con el que se comprueba la validez.

> *Retry*: es un valor numérico que indica el tiempo que pasa hasta que contacta el servidor esclavo con el servidor maestro.

> *Expire*: es otro valor numérico que indica cuántos segundos como máximo el servidor retendrá los registros antes de expirarlos.

---

[1] Un ***FQDN*** (sigla en inglés de ***fully qualified domain name***) es un nombre de dominio completo que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo. Por ejemplo, dada la computadora llamada «serv1» y el nombre de dominio «bar.com.», el FQDN será «serv1.bar.com.» (Fuente: Wikipedia).

> *Negative*: indica cuánto tiempo el servidor debe conservar en su caché la respuesta negativa.

> *NS*: registro que indica cual es el servidor de nombres para esta zona.

El fichero prueba.127 sería de la siguiente forma:

```
┌──(root㉿kali)-[/etc/bind]
└─# cat prueba.127
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     prueba.com. root.prueba.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      prueba.com.
15      IN      PTR     prueba.com.
20      IN      PTR     server2003.prueba.com.
```

Si se observa el fichero anterior, se comprobará que las opciones son prácticamente las mismas, salvo la diferencia a la hora de declarar los registros, ya que estamos en una zona inversa, entonces la declaración de un registro sería de la forma 10 IN PTR prueba.com.

El número 10 sería el último byte de la dirección IP del dominio. *IN* para declarar un registro y la opción nueva es la siguiente:

> *PTR*: crea la correspondencia de un nombre con una dirección IP. Además, de *SOA* y *NS*, son los únicos registros que se encuentran en las zonas inversas.

9. El siguiente fichero que es necesario configurar es resolv.conf, que nos permitirá decirle quiénes son los servidores DNS, el dominio de nuestro servidor y dónde es necesario realizar la búsqueda. Por lo tanto, la configuración de nuestro fichero se ve a continuación:

```
┌──(root㉿kali)-[/etc]
└─# cat resolv.conf
# Generated by NetworkManager
domain prueba.com
search prueba.com
nameserver 10.0.2.15
```

10. A continuación, se va a comprobar que el DNS está funcionando correctamente con los registros que hemos declarado.
    iniciamos el servicio con:

```
service named start
```

11. Las pruebas se pueden hacer con varios comandos de cliente DNS, como pueden ser ***nslookup***, ***dig*** o ***host***. En nuestro caso, vamos a usar dos comandos ***nslookup*** y ***dig*** para que se observen las distintas opciones, una más breve y otra más extensa.

Con el comando **dig** y consultando zona directa prueba.com el resultado sería el siguiente:

El resultado de la ejecución del comando dig acompañado del dominio prueba.com noss da como resultado:

- La pregunta es qué IP tiene el dominio prueba.com y como respuesta primera es el registro tipo A 10.0.2.15
- Como segunda opción de sección es el registro NS de dominio principal prueba.com.
- Además, esta consulta da otros datos más: cuándo se ha realizado la consulta, el tamaño del mensaje, el tiempo que ha tardado, el servidor que ha respondido a la consulta.

Con el comando dig y consultando zona inversa 10.0.2.15 el resultado sería el siguiente:

Para concluir, se van a detallar dos comandos que nos permiten chequear sintácticamente los ficheros que se han creado anteriormente, como son los siguientes: *named.conf, named.conf.options, named.conf.local, prueba.local, prueba.127*.

Comando	Descripción	Sintaxis

`named-checkconf`	Detecta posibles errores sintácticos en los ficheros de configuración named.	`named-checkconf` **`fichero_configuración`**
`named-checkzone`	Detecta posibles errores sintácticos en los ficheros de configuración de zona	`named-checkzone` **`nombre_dominio`** **`fichero_de_zona`**