Práctica DNS: Configuración de un servidor

Tabla de Contenido

Es muy importante que antes de empezar esta práctica eliminéis las entradas que podais haber ido introduciendo hasta ahora en vuestro archivo `/etc/hosts` para asegurarnos que realmente la resolución de nombres va a nuestro servidor DNS. Si no hacéis esto, resolverá los nombres, pensaréis que está bien pero en realidad estará mal.

1. Instalación de servidor DNS

Bind es el estándar de facto para servidores DNS. Es una herramienta de software libre y se distribuye con la mayoría de plataformas Unix y Linux, donde también se le conoce con el sobrenombre de named (name daemon). **Bind9** es la versión recomendada para usarse y es la que emplearemos.

Para instalar el servidor DNS, usaremos los repositorios oficiales. Por ello, podremos instalarlo como cualquier paquete:

```
sudo apt-get install bind9 bind9utils bind9-doc
```

2. Configuración del servidor

Puesto que en clase sólo vamos a utilizar IPv4, vamos a decírselo a Bind, en su archivo general de configuración. Este archivo `named` se encuentra en el directorio:

```
/etc/default
```

Y para indicarle que sólo use IPv4, debemos modificar la línea siguiente con el texto resaltado:

```
OPTIONS = "-u bind -4"
```

El archivo de configuración principal `named.conf` de Bind está en el directorio:

```
/etc/bind
```

Si lo consultamos veremos lo siguiente:

Ejemplo 1. Fichero `/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";
```

Este archivo sirve simplemente para aglutinar o agrupar a los archivos de configuración que usaremos. Estos 3 *includes* hacen referencia a los 3 diferentes archivos donde deberemos realizar la verdadera configuración, ubicados en el mismo directorio.

2.1. configuración `named.conf.options`

Es una buena práctica que hagáis siempre una copia de seguridad de un archivo de configuración cada vez que vayáis a realizar algún cambio:

```
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.backup
```

Ahora editaremos el archivo `named.conf.options` e incluiremos los siguientes contenidos:

- Por motivos de seguridad, vamos a incluir una lista de acceso para que sólo puedan hacer consultas recursivas al servidor aquellos hosts que nosotros decidamos.

  En nuestro caso, los hosts confiables serán los de la red `192.168.X.0/24` (donde la `X` depende de

vuestra red). Así pues, justo antes del bloque `options {⋯}`, al principio del archivo, añadiremos algo así:

Ejemplo 2. Fichero `/etc/bind/named.conf.options`

```
acl confiables {
    192.168.X.0/24;
};

options {
        directory "/var/cache/bind"; ①

        // forwarders {
        //   0.0.0.0;
        // };

        allow-transfer { none; }; ②

    listen-on port 53 { 192.168.X.Y; }; ③

        recursion yes; ④
        allow-recursion { confiables; }; ⑤

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation yes; ⑥

        // listen-on-v6 { any; }; ⑦
};
```

① Si nos fijamos el servidor por defecto ya viene configurado para ser un DNS caché. El directorio donde se cachearán o guardarán las zonas es `/var/cache/bind`.

② No permitir transferencia de zonas a nadie, de momento

③ Configurar el servidor para que escuche consultas DNS en el puerto `53` (por defecto DNS utiliza puerto `53/UDP`) y en la IP de su interfaz de la red privada. Deberéis colocar la IP de la interfaz de vuestro servidor, puesto que resolverá las consultas DNS del cliente/s de esa red.

④ Permitir las consultas recursivas, ya que en el primer punto ya le hemos dicho que sólo puedan hacerlas los hosts de la ACL.

⑤ Que sólo se permitan las consultas recursivas a los hosts que hemos decidido en la lista de acceso anterior

⑥ Habilitaremos o deshabilitaremos *dnssec*.

⑦ Además, vamos a comentar la línea que `listen-on-v6 { any; };` puesto que no vamos a responder a consultas de IPv6. Para comentarla basta añadir al principio de la línea dos barras

`//`. También podría hacerse con una almohadilla pero aparecería resaltado con color ya que estos comentarios los suele utilizar el administrador para aclarar algún aspecto de la configuración.

Podemos comprobar si nuestra configuración es correcta con el comando:

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

Si hay algún error, nos lo hará saber. En caso contrario, nos devuelve a la línea de comandos.

Reiniciamos el servidor y comprobamos su estado:

```
systemctl restart named
systemctl status named
```

2.2. Configuración `named.conf.local`

En este archivo configuraremos aspectos relativos a nuestras zonas. Vamos a declarar la zona `deaw.es`. Por ahora simplemente indicaremos que el servidor DNS es maestro para esta zona y donde estará ubicado el archivo de zona que crearemos más adelante:

Ejemplo 3. Fichero `/etc/bind/named.conf.local`

```
/
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "deaw.es" {
     type master;
     file "/var/lib/bind/deaw.es.dns";
};
```

2.3. Creación del archivo de zona

Vamos a crear el archivo de zona de resolución directa justo en el directorio que hemos indicado antes y con el mismo nombre que hemos indicado antes.

El contenido será algo así (procurad respetar el formato):

Ejemplo 4. Fichero /var/lib/bind/deaw.es.dns

```
;
; deaw.es
;
$TTL    86400
@   IN  SOA debian.deaw.es. admin.deaw.es. (
                  1     ; Serial ①
               3600     ; Refresh
               1800     ; Retry
             604800     ; Expire
              86400 )   ; Negative Cache TTL
;
@       IN  NS      debian.deaw.es.
debian.deaw.es. IN  A       192.168.X.X
```

① Cualquier valor númerico es correcto para el serial, pero se recomienda AñoMesDiaVersion

Recordad de teoría que los registros `SOA` son para detallar aspectos de la zona autoritativa, los `NS` para indicar los servidores DNS de la zona y los `A` las IPs respectivas.

Donde aparecen las `X` debéis poner vuestras IPs correspondientes, tanto de vuestro servidor como de vuestro cliente.

2.4. Zona para la resolución inversa

Recordad que deben existir ambos archivos de zona, uno para la resolución directa y otro para la inversa. Vamos pues a crear el archivo de zona inversa.

En primer lugar, debemos añadir las líneas correspondientes a esta zona inversa en el archivo `named.conf.local`, igual que hemos hecho antes con la zona de resolución directa:

Ejemplo 5. Fichero `/etc/bind/named.conf.local`

```
/
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "deaw.es" {
     type master;
     file "/var/lib/bind/deaw.es.dns";
};
```

```
zone "X.168.192.in-addr.arpa" {
     type master;
     file "/var/lib/bind/deaw.es.rev";
};
```

Donde la X es el tercer byte de vuestra red.

Y la configuración de la zona de resolución inversa:

Ejemplo 6. Fichero /var/lib/bind/deaw.es.rev

```
;
; X.168.192
;
$TTL    86400
@   IN  SOA debian.deaw.es. admin.deaw.es. (
                  1     ; Serial ①
               3600     ; Refresh
               1800     ; Retry
             604800     ; Expire
              86400 )   ; Negative Cache TTL
;
@       IN  NS      debian.deaw.es.
Y               IN  PTR     debian.deaw.es. ①
```

① En Y poner el último octeto de la IP del equipo.

Podemos comprobar que la configuración de las zonas es correcta con el comando adecuado.

2.5. Comprobación de las configuraciones

Para comprobar la configuración de la zona de resolución directa:

```
named-checkzone deaw.es. /var/lib/bind/deaw.es.dns
```

Y para comprobar la configuración de la zona de resolución inversa:

```
named-checkzone X.168.192.in-addr.arpa. /var/lib/bind/deaw.es.rev
```

Si todo está bien, devolverá OK. En caso de haber algún error, nos informará de ello.

Reiniciamos el servicio y comprobamos el estado. Debemos ver una línea parecida a:

```
Nov 20 17:56:54 deaw named[28234]: zone X.168.192.in-addr.arpa/IN: loaded serial
```

```
Nov 20 17:56:54 deaw named[28234]: zone deaw.es/IN: loaded serial
```

Es muy importante que el cliente esté configurado para usar como servidor DNS el que acabamos de instalar y configurar. Ya sea Windows, ya sea Linux, debéis cambiar vuestra configuración de red para que la máquina con la que hagáis las pruebas utilice este servidor DNS como el principal.

2.6. Comprobación de las resoluciones y de las consultas

Podemos comprobar desde los clientes, con `dig` o `nslookup` las resoluciones directas e inversas:

3. Comprobación usando *dig*

Comprobaremos la configuración preguntando al servidor directamente `@192.168.X.Y` o sin la arroba, si tenemos configurado el servidor DNS `debian` como servidor primario de nuestro cliente.

Ejemplo 7. Salida de la comprobación

```
$ dig @192.168.X.Y debian.deaw.es

; <<>> DiG 9.18.19 <<>> @192.168.X.Y debian.deaw.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16838
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1a0b5e79b553b491010000006559c73fc2ae930060cd8bec (good)
;; QUESTION SECTION:
;debian.deaw.es.            IN  A

;; ANSWER SECTION:
debian.deaw.es.     86400   IN  A   192.168.X.Y ①

;; Query time: 0 msec
;; SERVER: 192.168.X.Y#53(192.168.X.Y) (UDP) ②
;; WHEN: Sun Nov 19 09:28:47 CET 2023
;; MSG SIZE  rcvd: 87
```

① Respuesta correcta

② Servidor al que le hemos hecho la pregunta

4. Comprobación usando *nslookup*

Ejemplo 8. Salida de la comprobación con `nslookup`

```
$ nslookup debian.deaw.es 192.168.X.Y
Server:     192.168.X.Y ①
Address:    192.168.X.Y#53

Name:   debian.deaw.es
Address: 192.168.X.Y ②
```

① Servidor al que pregunto

② Respuesta

5. Cuestiones finales

1. ¿Qué pasará si un cliente de una red diferente a la tuya intenta hacer uso de tu DNS de alguna manera, le funcionará? ¿Por qué, en qué parte de la configuración puede verse?
2. Por qué tenemos que permitir las consultas recursivas en la configuración?
3. El servidor DNS que acabáis de montar, ¿es autoritativo?¿Por qué?
4. ¿Dónde podemos encontrar la directiva `$ORIGIN` y para qué sirve?
5. ¿Una zona es idéntico a un dominio?
6. ¿Pueden editarse los archivos de zona de un servidor esclavo/secundario?
7. ¿Por qué podría querer tener más de un servidor esclavo para una misma zona?
8. ¿Cuántos servidores raíz existen?
9. ¿Qué es una consulta iterativa de referencia?
10. En una resolución inversa, ¿a qué nombre se mapearía la dirección IP `172.16.34.56`?

6. Evaluación

Criterio	Puntuación
Configuración correcta del servidor y zona DNS	**3 puntos**
Evidencias de las comprobaciones del correcto funcionamento	**2 puntos**
Se ha utilizado SSH	**0.5 puntos**
Introducción de IPs de ejercicios anteriores para la resolución DNS	**1**
Cuestiones finales	**2.5 puntos**

Criterio	Puntuación
Se ha prestado especial atención al formato del documento, utilizando la plantilla actualizada y haciendo un correcto uso del lenguaje técnico	**1 punto**