

## Práctica 4. Configuración y Administración de DNS

### 1. Introducción

Es muy importante que antes de empezar esta práctica eliminéis las entradas que habéis ido introduciendo hasta ahora en vuestro archivo `/etc/hosts` (o el correspondiente en Windows) 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.

Máquinas necesarias:

- **DebianDNS:** Será dónde instalemos y configuremos nuestro DNS
- **DebianWeb:** Volveremos a activar la web de la práctica 2.1 (*static-web-example*). **Es un requisito que esto esté funcionando**
- **Máquina anfitriona.** Nuestro Windows

### 2. Instalación servidor DNS en DebianDNS

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 en Ubuntu Server, usaremos los repositorios oficiales. Por ello, podremos instalarlo como cualquier paquete en Ubuntu:

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

#### 2.1 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/named.conf
```

Si lo consultamos veremos lo siguiente:

```
// 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.

### 2.1.1 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:

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

zone "deaw.es" {
    type master;
    file "/etc/bind/db.deaw.es";
};
```

## 2.1.2 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):

```
$TTL 604800
@   IN  SOA  debian.deaw.es. admin.deaw.es. (
        ; Cualquier valor numérico es OK para el serial
        ; pero recomendado el formato: [AñoMesDíaVersion]
        2024112501
        3600
        1800
        604800
        86400
)

      IN  NS  debian.deaw.es.

debian IN  A   192.168.X.X
www    IN  A   192.168.X.X
```

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 (ya sean primarios o secundarios) y los A las IP respectivas.

Donde aparecen las X debéis poner vuestras IP privadas correspondientes, tanto de vuestro servidor DNS como de vuestro servidor web (el que aloja la web estática de la P2.1).

Para comprobar la configuración de la zona de resolución directa:

```
sergio@Debian-DAW:~$ sudo named-checkzone deaw.es /etc/bind/zonas/db.deaw.es
```

```
sudo named-checkconf -z
```

Ahora, si reiniciamos el servicio:

```
sudo systemctl restart bind9
```

Podremos comprobar si nuestro servidor DNS responde a al dominio deaw.es:

```
sergio@Debian-DAW:~$ dig @192.168.1.41 debian.deaw.es

; <<>> DiG 9.20.11-4-Debian <<>> @192.168.1.41 debian.deaw.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58505
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3656d2d56cc0dc480100000068c6ff331ba104f09797d96e (good)
;; QUESTION SECTION:
;debian.deaw.es.                IN      A

;; ANSWER SECTION:
debian.deaw.es.                604800  IN      A      192.168.1.41

;; Query time: 12 msec
;; SERVER: 192.168.1.41#53(192.168.1.41) (UDP)
```

```
sergio@Debian-DAW:~$ dig @192.168.1.41 www.deaw.es

; <<>> DiG 9.20.11-4-Debian <<>> @192.168.1.41 www.deaw.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23136
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 363f1488133a62e30100000068c6ff972a61d6d09ba47561 (good)
;; QUESTION SECTION:
;www.deaw.es.                  IN      A

;; ANSWER SECTION:
www.deaw.es.                  604800  IN      A      192.168.1.43

;; Query time: 0 msec
;; SERVER: 192.168.1.41#53(192.168.1.41) (UDP)
;; WHEN: Sun Sep 14 19:47:03 CEST 2025
```

### 2.1.3 Creación del archivo de zona para 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:

```
zone "deaw.es" {
    type master;
    file "/etc/bind/zonas/db.deaw.es";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zonas/db.1.168.192";
};
```

Y la configuración de la zona de resolución inversa:

```
$TTL 604800
@   IN  SOA debian.deaw.es. admin.deaw.es. (
      2024112501 ; serial [AñoMesDiaVersion]
      3600      ; refresh
      1800      ; retry
      604800    ; expire
      86400     ; minimum

      IN  NS  debian.deaw.es.

; ----- PTRs de tu red -----
41 IN  PTR  debian.deaw.es.
43 IN  PTR  www.deaw.es.
```

Para comprobar la configuración de la zona de resolución inversa:

```
sergio@Debian-DAW:~$ sudo named-checkzone 1.168.192.-in-addr.arpa /etc/bind/zonas/db.1.168.192
zone 1.168.192.-in-addr.arpa/IN: loaded serial 2024112501
OK
```

```
sudo named-checkconf -z
```

Ahora, si reiniciamos el servicio:

```
sudo systemctl restart bind9
```

Podremos comprobar si nuestro servidor DNS resuelve la zona inversa:

```
sergio@Debian-DAW:~$ dig @192.168.1.41 -x 192.168.1.41

; <<>> DiG 9.20.11-4-Debian <<>> @192.168.1.41 -x 192.168.1.41
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22006
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7c6e3392a7229e500100000068c703f6dfca00059ef07f42 (good)
;; QUESTION SECTION:
;41.1.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
41.1.168.192.in-addr.arpa. 604800 IN      PTR      debian.deaw.es.

;; Query time: 0 msec
```



```
sergio@Debian-DAW:~$ dig @192.168.1.41 -x 192.168.1.43

; <<>> DiG 9.20.11-4-Debian <<>> @192.168.1.41 -x 192.168.1.43
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36151
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

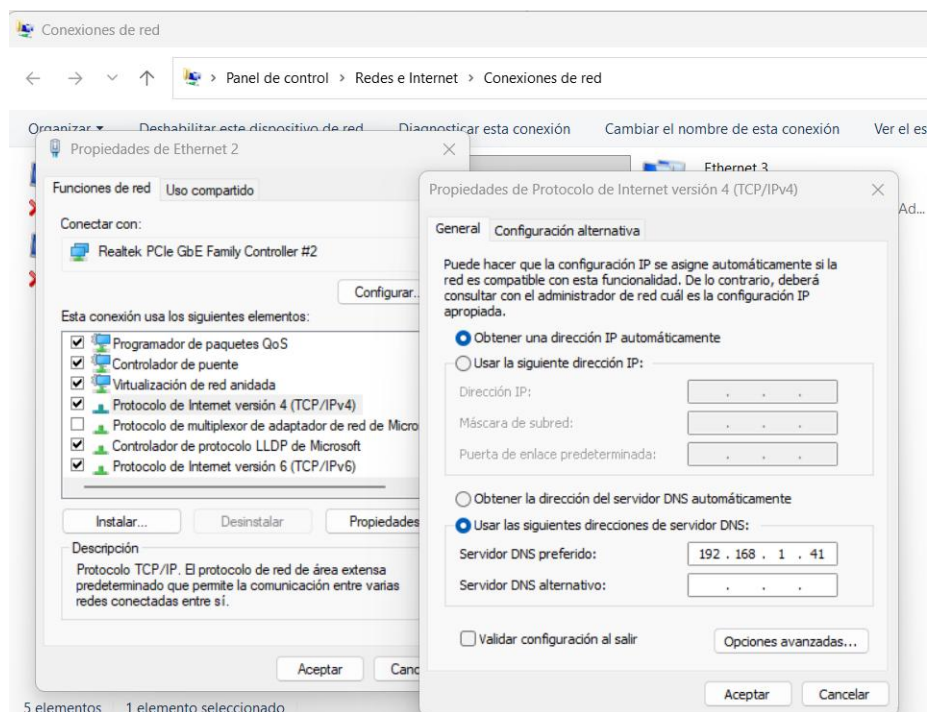
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7b6486c467869df20100000068c70430605b27dece1bb136 (good)
;; QUESTION SECTION:
;43.1.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
43.1.168.192.in-addr.arpa. 604800 IN      PTR      www.deaw.es.

;; Query time: 4 msec
;; SERVER: 192.168.1.41#53(192.168.1.41) (UDP)
;; WHEN: Sun Sep 14 20:06:40 CEST 2025
;; MSG SIZE rcvd: 107
```

### 3. Configuración DNS de nuestro anfitrión

Es muy importante que el cliente esté configurado para usar como servidor DNS el que acabamos de instalar y configurar. Debéis cambiar vuestra configuración de red para que la máquina con la que hagáis las pruebas utilice este servidor DNS como el principal:



Ahora deberíais poder navegar por Internet, pero el servidor DNS que usará será vuestro servidor Debian. Además, podréis validarlo desde vuestro anfitrión de la siguiente forma:



```
C:\Users\Sergio>nslookup www.deaw.es
Servidor:  debian.deaw.es
Address:  192.168.1.41

Nombre:   www.deaw.es
Address:  192.168.1.43

C:\Users\Sergio>nslookup debian.deaw.es
Servidor:  debian.deaw.es
Address:  192.168.1.41

Nombre:   debian.deaw.es
Address:  192.168.1.41
```

```
C:\Users\Sergio>nslookup -type=PTR 192.168.1.41
Servidor:  debian.deaw.es
Address:  192.168.1.41

41.1.168.192.in-addr.arpa      name = debian.deaw.es
```

Del mismo modo, ahora deberíais poder usar vuestro DNS para poder ver la página web de la otra máquina virtual (en vuestro caso se tiene que ver la web de la Práctica 2.1):

http://www.deaw.es

V Imprimir BALMIS Bibliografía IA Doctorado Khipu Hub BD Bibliografía Formación O

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

## 4. 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 (ACL) para que sólo puedan hacer consultas al servidor aquellos hosts que nosotros decidamos (los de nuestra red), en mi caso la red 192.168.1.0/24
- 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.
- Que sólo se permitan las consultas y consultas caché a los hosts que hemos decidido en la lista de acceso anterior
- Permitir las consultas recursivas (, ya que en el primer punto ya le hemos dicho que sólo puedan hacerlas los hosts de la ACL.
- No permitir transferencia de zonas a nadie, de momento
- 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 vuestra Debian**, puesto que resolverá las consultas DNS del cliente/s de esa red.
- Poner como reenviadores los servidores DNS de Cloudflare (1.1.1.1) y Google (8.8.8.8) y, además, con preferencia respecto a las consultas recursivas.

```
acl "conf" {
    127.0.0.1;          // localhost
    192.168.1.0/24;    // tu red local
};

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

    // Activamos recursion (resolver para clientes autorizados)
    recursion yes;
    allow-recursion {conf;};

    allow-query {conf;};
    allow-query-cache {conf;};

    // Usar reenviadores (forwarders) para Internet
    forwarders {
        1.1.1.1;    // Cloudflare
        8.8.8.8;    // Google
    };
    forward first; // primero intenta forwarders, si fallan → resolución raíz

    allow-transfer {none;};

    // Escuchar solo en interfaces locales y LAN
    listen-on {127.0.0.1; 192.168.1.41; };
    listen-on-v6 { none; };

    dnssec-validation auto;
    auth-nxdomain no;
};
```

Podemos comprobar si nuestra configuración es correcta con el comando:

```
sudo named-checkconf
```

## TAREAS

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? Teniendo nuestro anfitrión configurado como servidor DNS nuestro Debian, ¿qué pasa si desactivo la recursión y los *forwarders*? Compruébalo.
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 lo mismo que 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?
10. En el caso de nuestro servidor DNS, ¿qué quiere decir que haga una llamada recursiva (ponme un ejemplo)? ¿Y cuando la hace a través de los *forwarders*? ¿Qué diferencia hay?
11. Completa el archivo de zona de deaw.es añadiendo registros para que el dominio funcione como si fuese una pequeña empresa. Para ello, incluye lo siguiente:

Registros A:

- mail.deaw.es apuntando al servidor de correo (IP diferente a la de la web).
- ftp.deaw.es apuntando a un servidor propio de FTP.
- vpn.deaw.es para el acceso remoto.

Un registro CNAME:

- intranet.deaw.es que sea un alias de debian.deaw.es.

Un registro MX (debes crear su registro A correspondiente):

- Define el servidor de correo principal (mail.deaw.es) con prioridad 10.
- Opcionalmente, un secundario (backupmail.deaw.es) con prioridad 20.

12. Completa el archivo de zona inversa correspondiente para tu red 192.168.X.0/24 (ajusta la X al número de tu red). En él deben aparecer los registros PTR que hagan coincidir con la zona directa. Concretamente: mail.deaw.es, ftp.deaw.es., vpn.deaw.es., backupmail.deaw.es.

Documenta y graba toda la práctica con las capturas de pantalla correspondientes de cada configuración y comprobación.

En el vídeo muestra que puedes navegar usando tu servidor DNS, así como pruebas en las que se vea que resuelve correctamente dominios de zona directa e inversa (con pruebas de los ejercicios 12 y 13). Además, muestra los archivos de configuración.