Práctica 4

DNS: Sistema de Nombres de Dominio

En esta práctica aprenderemos a configurar un servidor DNS, tanto para la resolución directa como la inversa. Emplearemos el servidor de nombres más utilizado en Internet: `bind9`, del *Internet System Consortium, ISC*.

4.1. Configuración básica

Crearemos la topología de máquinas virtuales mostrada en la figura 4.1. La máquina `uml1` será nuestro

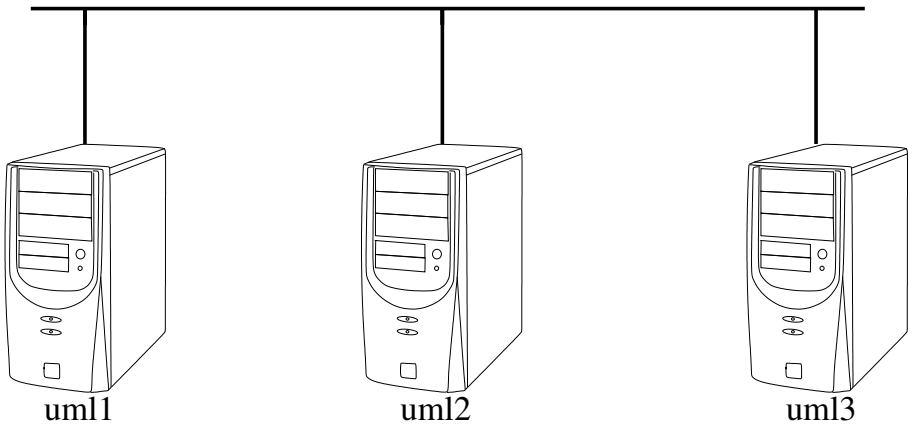

Figura 4.1: Topología de la práctica de DNS

servidor primario, la máquina `uml2` será un servidor secundario, y `uml3` actuará como cliente.

4.1.1. Servidor primario

Comenzaremos configurando un servidor primario en la máquina `uml1` para la zona `ar.fdi.ucm.es`, como se muestra en la figura 4.2.

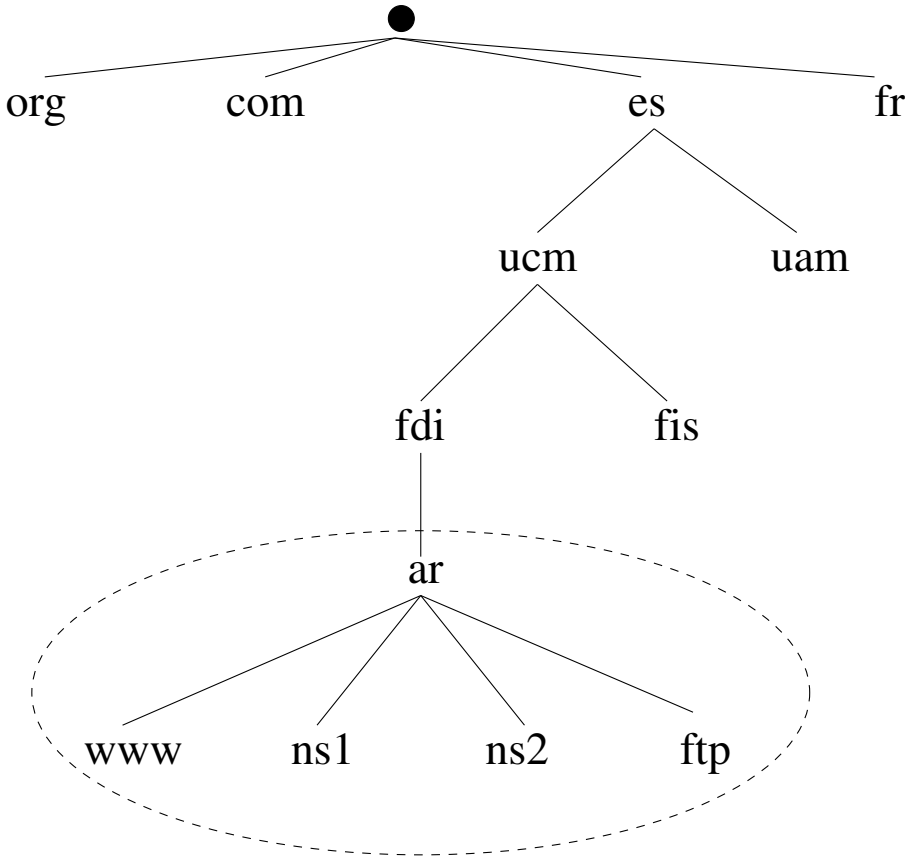

FIGURA 4.2: Zona DNS

Los archivos de configuración se encuentran en el directorio `/etc/bind/`. Comprobar el contenido de los ficheros `/etc/bind/named.conf`, `/etc/bind/named.conf.options` y `/etc/bind/named.conf.default-zones`. En este último se definen varias zonas importantes, como por ejemplo la zona "raíz" (es decir, "."), de tipo `hint`. Estudiar el contenido del archivo `/etc/bind/db.root`, donde se encuentran definidos los servidores de nombres raíz.

Nuestros archivos de definición de zona se llamarán `db.ar.fdi.ucm.es` para la zona directa y `db.192.168.1` para la inversa. Aunque según la directiva `directory` del archivo `named.conf.options` deberían estar en `/var/cache/bind`, nosotros los ubicaremos también en `/etc/bind` pero haciendo referencia a la ruta completa en los archivos de configuración. Precisamente, el archivo de configuración que debemos modificar es el `named.conf.local`, para que muestre algo parecido a lo siguiente:

```
zone "ar.fdi.ucm.es" IN {
        type master;
        file "/etc/bind/db.ar.fdi.ucm.es";
        allow-query {any;};
};
```

Con esto estamos diciendo que nuestro servidor es el primario ("`master`") de la zona, que el archivo de definición de zona es `/etc/bind/db.ar.fdi.ucm.es` (si no especificáramos la ruta completa debería estar ubicado en `/var/cache/bind`), y que además permitimos consultas referidas a esta zona por parte de cualquier máquina de Internet. Más adelante veremos cómo establecer también qué máquinas tienen permiso para realizar una copia completa del archivo de zona, que serán, normalmente, sólo los servidores secundarios.

Ahora debemos crear el archivo `db.ar.fdi.ucm.es` con los datos de la zona:

```
$TTL 3600

@  IN  SOA ns1.ar.fdi.ucm.es. dnsadmin.ar.fdi.ucm.es. (
        2018022201 ; Número de serie
        43200 ; Sincro
        3600 ; Reintentos
        604800 ; Expire
        1800; negative caching
)
; Servidores autoritativos
        IN NS   ns1 ; primario
        IN NS   ns2 ; secundario
        IN NS   ns3 ; secundario

; Direcciones
ns1     IN A 192.168.1.1
        IN AAAA 2001:db8:1180::1
ns2     IN A 192.168.1.2
        IN AAAA 2001:db8:1180::2
ns3     IN A 172.16.4.1 ; externo a la red local

deimos  IN A 192.168.1.5
fobos   IN A 192.168.1.27
marte   IN A 192.168.1.22
```

Modificar el archivo anterior para añadir los siguientes registros:

- El nombre `www.ar.fdi.ucm.es.` en las direcciones `192.168.27.4` y `2001:db8:27::4`
- El nombre `ftp.ar.fdi.ucm.es.` en las direcciones `192.168.1.2` y `2001:db8:1180::2`
- El nombre `ftp.ar.fdi.ucm.es.` como *alias* (registro `CNAME`) de `www.ar.fdi.ucm.es.`

Podemos comprobar la configuración de bind9 mediante la orden `named-checkconf` y la definición de la zona mediante `named-checkzone`. Estudiar su uso en las páginas de manual (`man named-checkconf`

y `man named-checkzone`. Una vez que esté configurado, reiniciamos el servicio con `systemctl restart bind9`.

Desde la máquina `uml3`, que actuará como cliente, podemos comprobar el funcionamiento del servidor DNS mediante las órdenes `host` y `dig`. Por ejemplo:

```
host www.ar.fdi.ucm.es 192.168.1.1
dig @192.168.1.1 www.ar.fdi.ucm.es
```

Estudiar el funcionamiento de ambas órdenes en las páginas del manual.

4.1.2. Servidor secundario

En la máquina `uml2` configuraremos un servidor secundario. Para ello, en el archivo `/etc/bind/named.conf.local` hay que añadir lo siguiente:

```
zone "ar.fdi.ucm.es" IN {
        type slave;
        file "db.ar.fdi.ucm.es";
        masters {192.168.1.1; 2001:db8:1180::1;};
};
```

En el servidor primario debemos permitir la transferencia de zona desde este servidor, por lo que debemos añadir la directiva "`allow-transfer {192.168.1.2; 2001:db8:1180::2;};`" (sin las comillas) a la definición de zona en `named.conf.local` de `uml1`. En general, aquí debemos añadir las direcciones IP (tanto IPv4 como IPv6) de todos los servidores secundarios.

4.1.3. Cliente

El cliente `uml3` necesita saber las direcciones IP de los servidores de nombre predeterminados. Esta información la puede obtener de manera dinámica mediante DHCP, como se vio en la práctica 5, o bien de manera estática, modificando el archivo `/etc/resolv.conf` de la siguiente manera:

```
search ar.fdi.ucm.es
nameserver 192.168.1.1
nameserver 2001:db8:1180::1
nameserver 192.168.1.2
```

Comprobar que ahora no es necesario especificar la dirección IP del servidor DNS al utilizar las órdenes `host` y `dig`.

4.2. Resolución inversa

Añadiremos ahora la zona de resolución inversa para las direcciones IPv4 de nuestra red. En el servidor primario, modificamos el fichero `named.conf.local` con la definición de la zona:

```
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/db.192.168.1";
        allow-query {any;};
        allow-transfer {192.168.1.2; 2001:db8:1180::2; 172.16.4.1;};
};
```

Editamos el archivo `db.192.168.1` para que contenga la información adecuada:

```
$TTL 3600;

@       IN      SOA ns1.ar.fdi.ucm.es. dnsadmin.ar.fdi.ucm.es. (
                2018022203 ; Número de serie
                43200 ; Sincro
                3600 ; Reintentos
                604800 ; Expire
                86400; negative caching
)

; Servidores autoritativos
        IN      NS ns1.ar.fdi.ucm.es.
        IN      NS ns2.ar.fdi.ucm.es.
        IN      NS otroservidor.ejemplo.org.

; Nombres
1       IN      PTR ns1.ar.fdi.ucm.es.
2       IN      PTR ns2.ar.fdi.ucm.es.
5       IN      PTR deimos.ar.fdi.um.es.
```

Completar con los registros `PTR` que faltan.

En el servidor secundario, añadir la nueva zona en el archivo `named.conf.local`.

Una vez reiniciados los servidores, comprobar su funcionamiento desde la máquina cliente:

```
host 192.168.1.5
dig -t PTR 5.1.168.192.in-addr.arpa
dig -x 192.168.1.5
```