

Práctica 5: Instalar servidor DNS esclavo en Debian

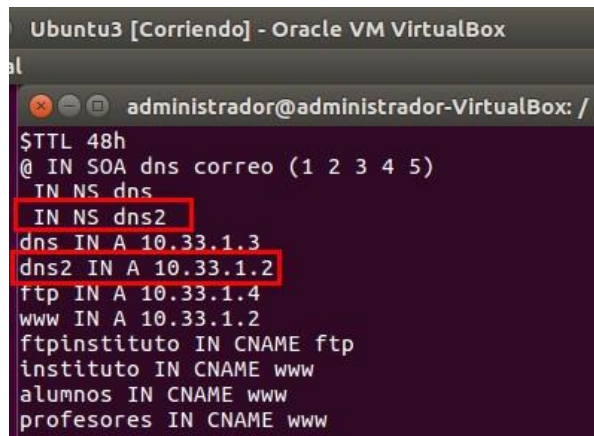
Partiendo de la práctica anterior "Configurar DNS básico", donde ya existe un servidor DNS maestro, añadir al sistema un segundo servidor DNS esclavo en la máquina Debian02.

Deberás comprobar el funcionamiento del servidor esclavo estando apagado el servidor maestro.

Nota 1: Tener en cuenta que para su resolución deberás utilizar el fichero de definición de zona con los registros de recursos más abreviados posible.

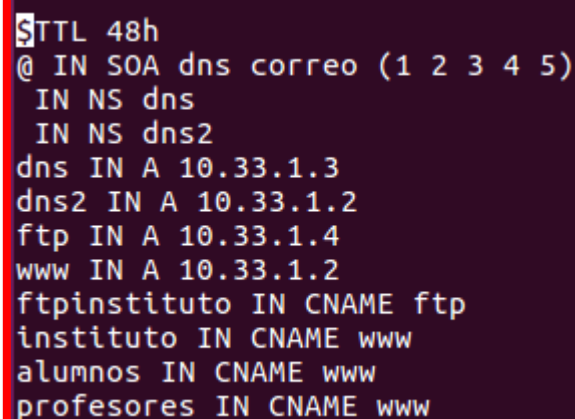
Solución

1º) En el servidor DNS maestro (**ubuntu3**), editamos el fichero de definición de zona del maestro (`var/lib/bind/lin.edu.maestro`) e introducimos algunos cambios necesarios y otros para abreviar su especificación:



```
administrador@administrador-VirtualBox: /
$TTL 48h
@ IN SOA dns correo (1 2 3 4 5)
  IN NS dns
  IN NS dns2
dns IN A 10.33.1.3
dns2 IN A 10.33.1.2
ftp IN A 10.33.1.4
www IN A 10.33.1.2
ftpinstituto IN CNAME ftp
instituto IN CNAME www
alumnos IN CNAME www
profesores IN CNAME www
```

Una vez hechos los cambios, reiniciamos el servicio: `sudo service bind9 restart`




```
$TTL 48h
@ IN SOA dns correo (1 2 3 4 5)
  IN NS dns
  IN NS dns2
dns IN A 10.33.1.3
dns2 IN A 10.33.1.2
ftp IN A 10.33.1.4
www IN A 10.33.1.2
ftpinstituto IN CNAME ftp
instituto IN CNAME www
alumnos IN CNAME www
profesores IN CNAME www
```

2º) Instalamos el servicio DNS en el esclavo (**debian2**):

```
sudo apt-get install bind9
```

3º) También en **debian2** modificamos el valor del servidor DNS al que solicitar resolución como cliente (él mismo, puesto que ahora él también va a ser servidor DNS): _____



```
debian2 [Corriendo] - Oracle VM VirtualBox
GNU nano 3.2 /etc/resolv.conf
nameserver 127.0.0.1
```

7º) Modificamos el fichero de configuración de zona local en el esclavo (en **/etc/bind/named.conf.local**) añadimos la zona esclava indicando quién es su maestro):

```

debian2 [Corriendo] - Oracle VM VirtualBox
GNU nano 3.2 /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 "lin.edu" {
    type slave;
    file "/var/lib/bind/lin.edu.esclavo";
    masters {10.83.1.3;};
};

```

4º) Tras reiniciar ambos servidores podemos comprobar cómo se realizó correctamente la transferencia de zona viendo que existe el nuevo fichero `/var/lib/bind/lin.edu.esclavo`, que antes no existía.

```

@^@^@B^@^@^A_+^+^+^@^@^@^@^@^@^@^@^@^@^@^@P^@^A^@F^@^@^@B+^@^@^@^@^A^@^      ^Clin^Cedu
Cdns^Clin^Cedu^@^@N^Ddns2^Clin^Cedu^@^@^@4^@^A^@E^@^@^@B+^@^@^@^@^A^@^Q^Galumnos^Clin^Cedu^@
Cwww^Clin^Cedu^@^@^@^@^@^A^@A^@^@^@B+^@^@^@^@^A^@
Cdns^Clin^Cedu^@^@D
^A^C^@^@^@(^@^A^@A^@^@B+^@^@^@^@^A^@N^Ddns2^Clin^Cedu^@^@D
^A^B^@^@^@^@^@^A^@A^@^@^@B+^@^@^@^@^A^@
Cftp^Clin^Cedu^@^@D
^A^D^@^@^@9^@^A^@E^@^@^@B+^@^@^@^@^A^@V^Lftpinstituto^Clin^Cedu^@^@
Cftp^Clin^Cedu^@^@^@6^@^A^@E^@^@^@B+^@^@^@^@^A^@S_instituto^Clin^Cedu^@^@
Cwww^Clin^Cedu^@^@^@7^@^A^@E^@^@^@B+^@^@^@^@^A^@T
profesores^Clin^Cedu^@^@
Cwww^Clin^Cedu^@^@^@^@^@^A^@A^@^@^@B+^@^@^@^@^A^@
Cwww^Clin^Cedu^@^@D
^A^B

```

**** Si al hacer el "cat" del fichero del esclavo vemos que su formato es "binario" y no vemos su contenido, debemos convertirlo a formato "texto" con el siguiente comando:**

```
named-compilezone -f raw -F text -o example.net.text example.net example.net.raw
* donde example.net.raw es el fichero binario
```

En nuestro caso:

```
named-compilezone -f raw -F text -o lin.edu.esclavo.txt lin.edu lin.edu.esclavo
```

Otra posibilidad es incluir la opción "masterfile-format" en el fichero "named.conf.local" del esclavo:

```
Masterfile-Format Text;
Y hacer lo mismo para cada zona
```

```
zone "lin.edu" {
    type slave;
    file "/var/lib/bind/lin.edu.esclavo";
    masterfile-format text;
    masters {10.33.1.3;};
};
```

Editando el fichero en formato texto:



```
GNU nano 3.2 /var/lib/bind/lin.edu.esclavo
$ORIGIN .
$TTL 172800      ; 2 days
lin.edu          IN SOA  dns.lin.edu. correo.lin.edu. (
                                1      ; serial
                                2      ; refresh (2 seconds)
                                3      ; retry (3 seconds)
                                4      ; expire (4 seconds)
                                5      ; minimum (5 seconds)
                                )
                                NS      dns.lin.edu.
                                NS      dns2.lin.edu.
$ORIGIN lin.edu.
alumnos          CNAME  www
dns               A      10.33.1.3
dns2              A      10.33.1.2
ftp               A      10.33.1.4
ftpinstituto      CNAME  ftp
instituto         CNAME  www
profesores        CNAME  www
www               A      10.33.1.2
```

```
$ORIGIN .
$TTL 172800      ; 2 days
lin.edu          IN SOA  dns.lin.edu. correo.lin.edu. (
                                1      ; serial
                                2      ; refresh (2 seconds)
                                3      ; retry (3 seconds)
                                4      ; expire (4 seconds)
                                5      ; minimum (5 seconds)
                                )
                                NS      dns.lin.edu.
                                NS      dns2.lin.edu.
$ORIGIN lin.edu.
alumnos          CNAME  www
dns               A      10.33.1.3
dns2              A      10.33.1.2
ftp               A      10.33.1.4
ftpinstituto      CNAME  ftp
instituto         CNAME  www
profesores        CNAME  www
www               A      10.33.1.2
```

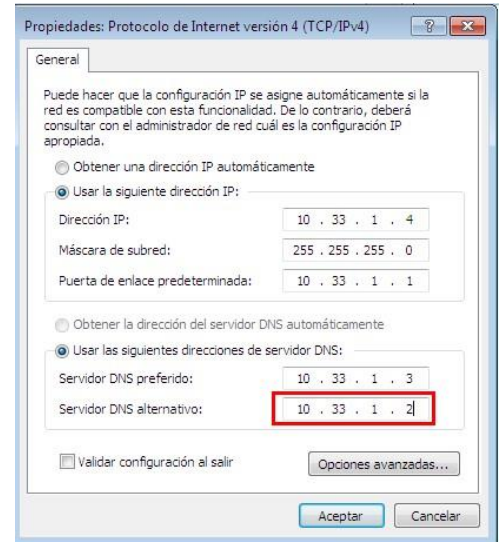
5º) Con el servidor DNS esclavo en marcha, **apagamos el maestro (ubuntu3)** y desde un cliente (por ejemplo, windows4) que tenga como primer DNS el maestro y como segundo DNS el esclavo, será capaz de enviar solicitudes de resolución DNS hasta el esclavo y ser respondidas correctamente.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\adminW7Base>ping www.lin.edu

Haciendo ping a www.lin.edu [10.33.1.21] con 32 bytes de datos:
Respuesta desde 10.33.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.33.1.2: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 10.33.1.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
```



```
Estadísticas de ping para 10.33.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\adminW7Base>ping ftp.lin.edu

Haciendo ping a ftp.lin.edu [10.33.1.41] con 32 bytes de datos:
Respuesta desde 10.33.1.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.33.1.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.33.1.4: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.33.1.4: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.33.1.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ubuntu1:

- Cuando tenemos los DNS configurados en la interfaz gráfica (pero no en */etc/resolv.conf*), funciona bien, coge el DNS esclavo, pero al hacer nslookup o dig dice que el servidor DNS es 127.0.0.1 (lo que pone en resolv)



```
administrador@ubuntu1:~$ nslookup www.lin.edu
Server:      127.0.1.1
Address:     127.0.1.1#53

Name:   www.lin.edu
Address: 10.33.1.2
```

```
administrador@administrador-VirtualBox:~$ nslookup www.lin.edu
Server:      127.0.1.1
Address:     127.0.1.1#53

Name:   www.lin.edu
Address: 10.33.1.2
```

- En cambio, si ponemos los dos DNS (maestro y esclavo) en */etc/resolv.conf*, sí indica su IP con nslookup.

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.33.1.3
nameserver 10.33.1.2
```

```
administrador@ubuntu1:~$ nslookup ftp.lin.edu
Server:      10.33.1.2
Address:     10.33.1.2#53

Name:   ftp.lin.edu
Address: 10.33.1.4
```

```
administrador@administrador-VirtualBox:~$ nslookup ftp.lin.edu
Server:      127.0.1.1
Address:     127.0.1.1#53

Name:   ftp.lin.edu
Address: 10.33.1.4
```

Windows4:

- Si el maestro no está arrancado, el comando "nslookup" no devuelve la IP del servidor DNS (aunque sí hace la resolución). Si definimos primero el DNS esclavo sí.

```
C:\Users\adminW7Base>nslookup www.lin.edu
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 10.33.1.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
```

```
C:\Users\adminW7Base>nslookup www.lin.edu
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 10.33.1.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
```