

SISTEMAS MICROINFORMÁTICOS Y REDES (SERVICIOS DE RED)

Ejercicio: Práctica 5.3 DNS (Configuración del servicio DNS servidor con Zentyal)

Introducción.

En la práctica instalaremos y configuraremos un servidor DNS con **bind** utilizando **Zentyal** como **interfaz de administración**. En la práctica ensayaremos diferentes configuraciones y modos de funcionamiento.

Al utilizar esta herramienta gráfica, prácticamente no necesitaremos escribir y modificar los ficheros de configuración directamente, pero debemos conocer la sintaxis y el funcionamiento de las principales directivas, por lo que en la práctica se hará hincapié en la inspección de dichos ficheros y el significado de los distintos parámetros e instrucciones.

Escenario.

El punto de partida será nuestra máquina virtual con **Ubuntu 20.04 Server** y **Zentyal 7.0** instalado con el perfil de infraestructura de la práctica anterior.

Para realizar las pruebas necesitaremos dos máquinas virtuales más con **Windows10** y **Ubuntu 20.04 Desktop**, que actuarán como **clientes**. Ambos clientes se configurarán con **una única tarjeta de red** en modo “sólo anfitrión”.

He usado la tarjeta de red en modo red interna, que la configuración con el modo sólo anfitrión me estaba dando muchos errores. La funcionalidad es la misma así que espero que no tenga mucha importancia.

NOTA: No será necesario tener ambos clientes arrancados simultáneamente, ya que los correspondientes ejercicios se realizan de forma alternativa.

Para el últimos apartado de la práctica necesitaremos una segunda máquina virtual **Ubuntu Server 20.04** pero **sin Zentyal** (que puede funcionar con sólo **512 MB de RAM**).

En este último apartado si **será necesario** tener **3** máquinas virtuales simultáneas (que supondrán un consumo máximo de **2,5 GB de RAM**).

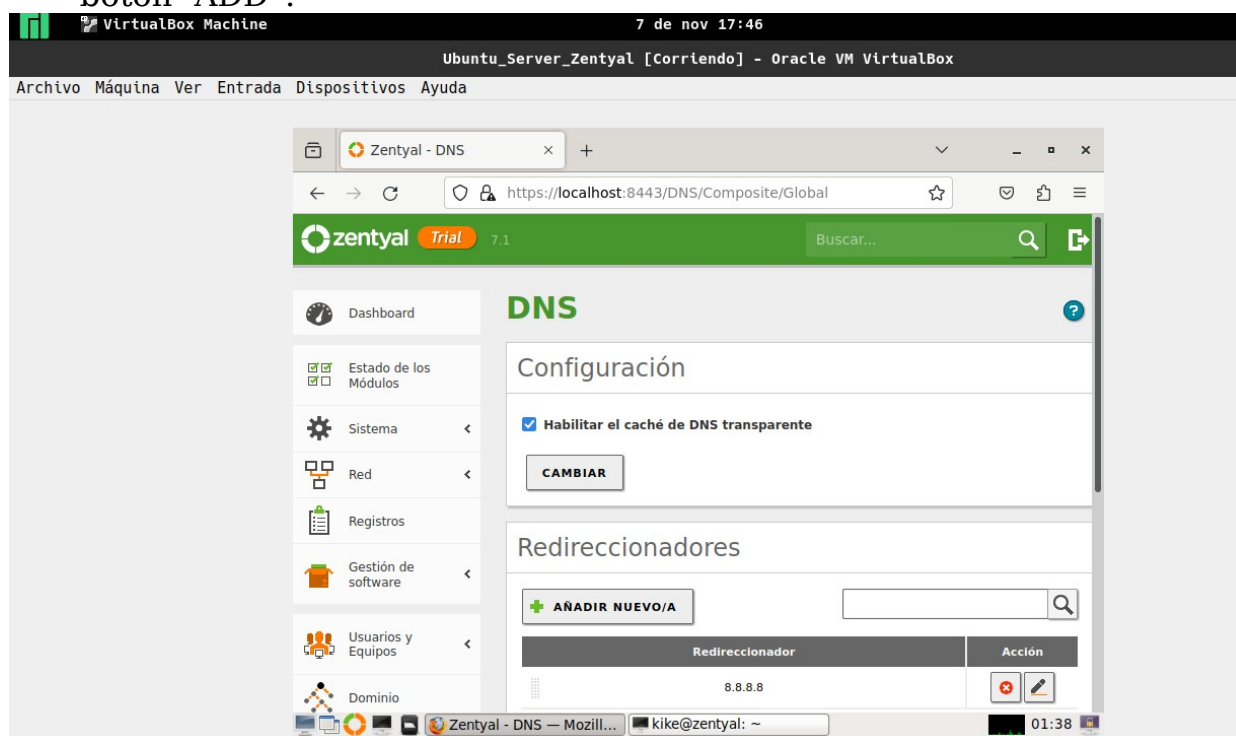
2 Servidor cache en modo proxy ("forwarding").

Podemos configurar el servidor cache para que reenvíe las peticiones a otro servidor DNS en lugar de atacar directamente a los root-servers.

Para eso se utiliza la opción de configuración "forwarders o redireccionadores".

Como ejemplo configuraremos nuestro servidor para redirigir las peticiones al servidor DNS de google:

1. introducimos la IP 8.8.8.8 en el campo Forwarder y pulsamos el botón "ADD".



2. Al volver a la página de configuración del DNS comprobaremos ahora aparece la lista de forwarders.

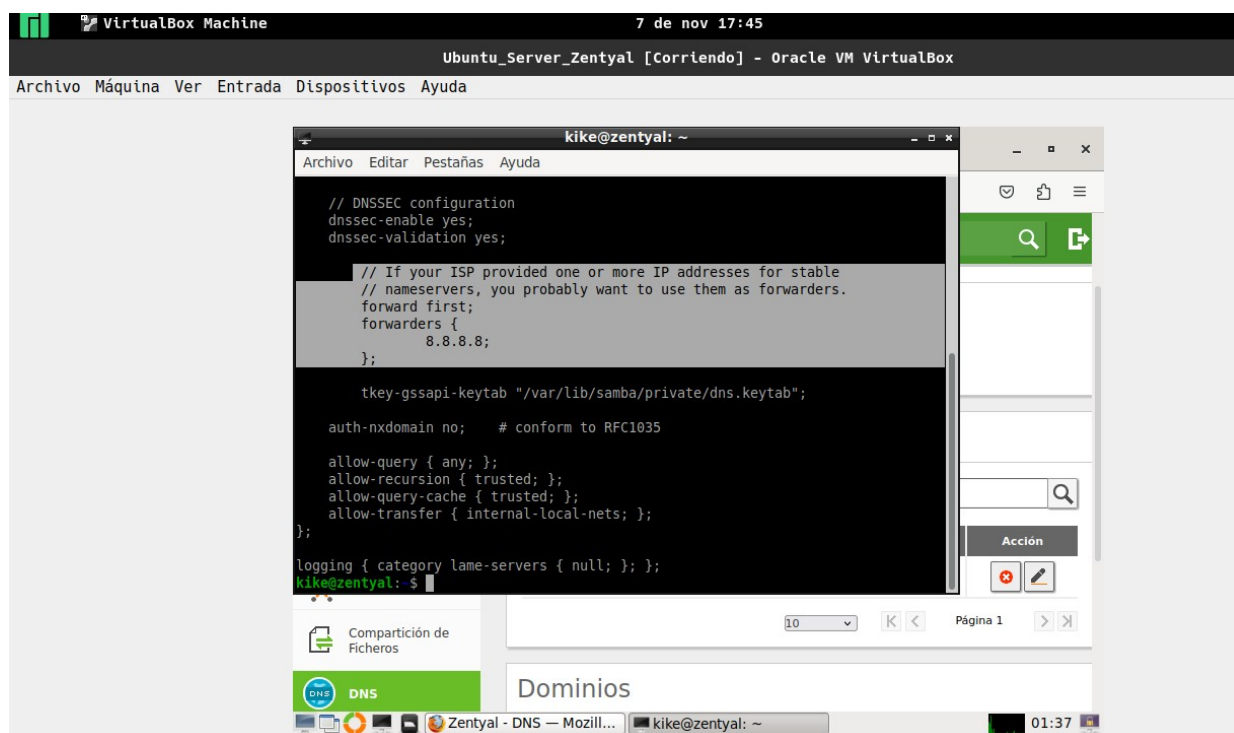
3. Se iluminará la opción "Save changes" en la parte superior de la página. Pulsaremos sobre ella y después se nos pedirá confirmación con un mensaje que advierte que los cambios en las configuraciones de red podrían afectar al acceso a la interfaz web de administración.

Tras unos instantes estarán grabados todos los cambios y reiniciados los servicios.

Ejercicio 2.1: Busca qué opción nueva de configuración está indicando que se use 8.8.8.8 como forwarder. Indica cual es exactamente la directiva y en qué fichero de configuración del bind se encuentra.

Entra dentro de la carpeta bind (usando el comando el cd) y busca en que archivos se ha añadido la opción de forwarders (usa los comandos ls y grep para encontrar la localización vistos en la práctica anterior y nano para ver el contenido).

Se ha añadido en la carpeta named.conf.options



Ejercicio 2.2: Repetir las consultas del ejercicio 1.5 de la primera parte de la práctica para comprobar que nuestro DNS sigue funcionando. Observad si hay diferencias de tiempo significativas respecto del caso anterior.

Justifica razonadamente los resultados obtenidos.

Pruebas	ausiasmarch.net	superdeporte.es	europarl.europa.eu	microsoft.com
1	48 msec	24 msec	28 msec	36 msec
2	32 msec	20 msec	0 msec	0 msec
3	0 msec	0 msec	0 msec	4 msec

Si que hay diferencias, los tiempos ahora son incluso de menor tiempo. Las consultas son más rápidas y supongo que será porque nuestro servidos DNS se quedará las consultas en la cache y después podrá resolver las consultas muchísimo más rápidas ya que nuestro servidor DNS está en nuestra misma red.

3 Servidor autoritario (maestro)

Vamos a configurar ahora el servidor para que sea autoritario para un dominio propio.

El nombre de nuestro dominio DNS de prueba será el siguiente: **smr.lan**

La información que debe contener el dominio se resume en las siguientes tablas:

Tabla 3.a Registros de tipo A y CNAME

HOSTNAME	IP	ALIAS
server	172.20.10.10	Zentyal, www, ns
ubuntu	172.20.10.20	linux, desktop
windows	172.20.10.30	win10
anfitrión	172.20.10.1	real
mail	64.233.164.27	

Tabla 3.b Otros registros:

TIPO	HOSTNAME / IP
NS	server
MX (prioridad 10)	mail
MX (prioridad 20)	alt2.aspmx.l.google.com

Veamos ahora como crear el dominio y empezar a añadir registros.

Tomaremos como ejemplo para las capturas el dominio '**smrsemi.lan**'

3.1 Crear el dominio

Desde **dashboard**, seleccionamos la opción **DNS** del menú y pulsamos en **"add new"** bajo la etiqueta **"Domains"**.

Introduciremos el nombre de nuestro **dominio (smr.lan)** y pulsaremos el botón **ADD**.

El dominio se mostrará ahora en la lista de dominios.

La descripción de las principales opciones es la siguiente:

- **Domain IP Addresses (Direcciones IP del dominio):** permite asociar una o más Ips directamente al nombre de dominio (no a un host del dominio).

La acción por defecto de Zentyal al crear el dominio, es añadir automáticamente todas las direcciones IP del servidor a esta lista.

- **Hostnames (Nombres de máquinas):** permite definir cuantos nombres (**registros A**) queramos dentro del dominio. Zentyal configurará automáticamente la resolución inversa. Estos nombres los asociaremos con una o más Ips.

En esta opción también pueden definirse **alias (registros CNAME)**.

A la hora de añadir máquinas o alias de estas al dominio, se da por supuesto el nombre de dominio, por ejemplo, para añadir el nombre '**www.smr.lan**' escribiremos simplemente '**www**', no el nombre completo '**www.smr.lan**'.

Zentyal, como acción por defecto, crea un **registro de tipo A** con el nombre '**server**', y le asigna todas las IPs del servidor.

- **Mail Exchangers (servidores de correo)**: son los encargados de recibir los mensajes de mail para el dominio (**registros MX**). **Podremos elegir entre los registros de tipo A** previamente definidos dentro del dominio **o bien uno externo**. Asignaremos también una preferencia, que determina el orden en el otros servidores elegirán a quien entregan el correo.

- **Name Servers (Servidores de nombres)**: permite configurar la lista de servidores DNS autoritarios para el dominio (**registros NS**). Al igual que los **MX**, **elegiremos entre los registros de tipo A** previamente definidos dentro del dominio **o un nombre externo**.

En este punto, **la acción por defecto de Zentyal** para los dominios nuevos es **asociar un registro NS al nombre 'server'** creado también automáticamente.

Nota: Para que el dominio sea válido debe existir al menos un **registro NS** (aunque preferiblemente deberían ser dos). Esto implica que no debemos borrar este registro automático sin haber creado previamente otro **registro NS** válido.

Nota: La asignación de **TODAS las IPs internas y externas** tanto como direcciones asociadas al dominio como al registro de tipo **A 'server'** generan un efecto 'round robin' entre redes diferentes que puede generar problemas en algunos contextos.

Para trabajar sólo con las IPs de la red interna de Zentyal (la red solo anfitrión), vamos a **eliminar la IP externa** del dominio:

Hacemos clic sobre el botón de configurar las Ips asociadas al dominio.

Sólo dejaremos la IP de la red interna (192.168.56.200) de manera que localizamos la IP externa (**NAT o bridge**) y hacemos clic en su correspondiente botón de **borrar**:

Por último, para grabar los cambios, usaremos el botón "**Save Changes**" y confirmaremos.

Vamos a eliminar también la IP externa en la lista de IPs asociadas al nombre de hosts 'server', accediendo a Hostnames → server

Desde allí procederemos de forma análoga para dejar sólo la IP

interna.

Recuerda finalmente grabar los cambios.

3.3 Creación del registro 'anfitrion'.

A modo de **ejemplo**, vamos a detallar los pasos para crear el **registro A y los CNAMEs** asociados al nombre '**anfitrion**', el resto de los registros de las tablas **3.a** y **3.b** se dejarán como **ejercicio** para el alumno.

Accedemos de nuevo a 'Hostnames' y después pulsamos el botón 'ADD NEW'.

Escribimos 'anfitrion' como hostname y pulsamos en ADD

'anfitrion' aparecera ahora en la lista de hosts. Haremos clic en el botón de su configuración de Ips.

Aparecerá la lista (vacía) de IPs y pulsaremos el botón "ADD NEW".

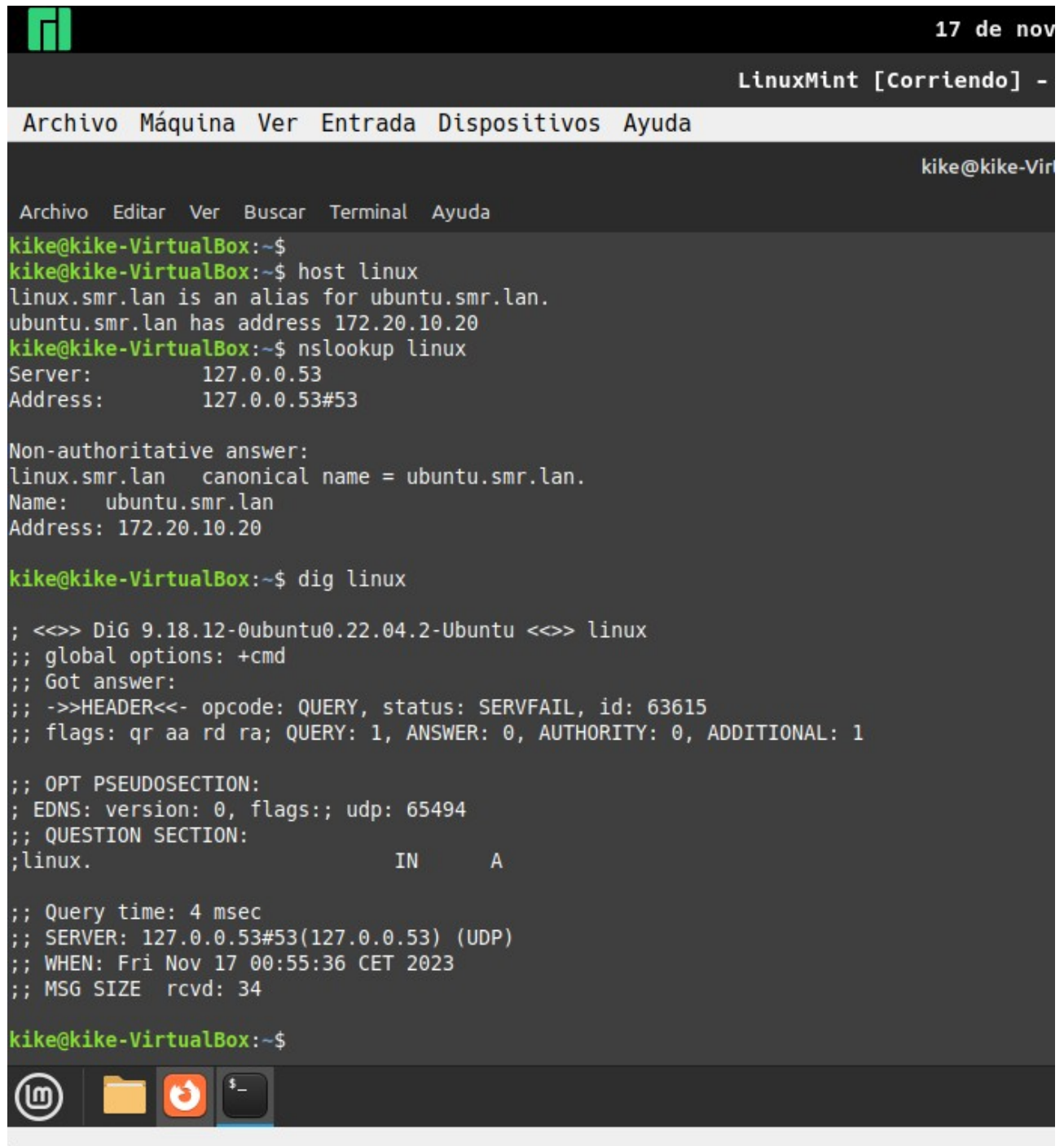
Introducimos la IP (192.168.56.1) y hacemos clic en "ADD"

Comprobaremos que al IP se ha introducido correctamente y aparece en la lista. Volveremos ahora a la lista de 'Host names' para introducir los alias.

Por último, guardaremos los cambios.

Ejercicios 3: Introduce todos los **registros** de las tablas **3.a** y **3.b**.
Accede por **ssh** al servidor y realiza los siguientes ejercicios:

3.1 Utiliza indistintamente los comandos **host**, **dig** o **nslookup** para probar que pueden resolverse los **FQDNs** de los nombres definidos en las tablas **3.a** y **3.b** Como resultado.



```
17 de nov
LinuxMint [Corriendo] -
Archivo Máquina Ver Entrada Dispositivos Ayuda
kike@kike-VirtualBox:~$
kike@kike-VirtualBox:~$ host linux
linux.smr.lan is an alias for ubuntu.smr.lan.
ubuntu.smr.lan has address 172.20.10.20
kike@kike-VirtualBox:~$ nslookup linux
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
linux.smr.lan canonical name = ubuntu.smr.lan.
Name:   ubuntu.smr.lan
Address: 172.20.10.20

kike@kike-VirtualBox:~$ dig linux

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> linux
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 63615
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;linux.                IN      A

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Nov 17 00:55:36 CET 2023
;; MSG SIZE rcvd: 34

kike@kike-VirtualBox:~$
```


3.2 Utiliza el comando **nslookup** para obtener el **servidor** (o **servidores**) de **correo** de nuestro dominio.

```
17 de nov 01:09
LinuxMint [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kike@kike-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
kike@kike-VirtualBox:~$ nslookup type=MX mail
;; communications error to 64.233.164.27#53: timed out
;; communications error to 64.233.164.27#53: timed out
;; communications error to 64.233.164.27#53: timed out
;; no servers could be reached

kike@kike-VirtualBox:~$ nslookup mail
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   mail.smr.lan
Address: 64.233.164.27

kike@kike-VirtualBox:~$
```

```
17 de nov 01:07
Ubuntu_Server_Zentyal [Corriendo] - Oracle VM VirtualBox
Dispositivos Ayuda
kike@zentyal: ~
Archivo Editar Pestañas Ayuda
kike@zentyal:~$ dig alt2aspmx.l.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> alt2aspmx.l.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64350
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

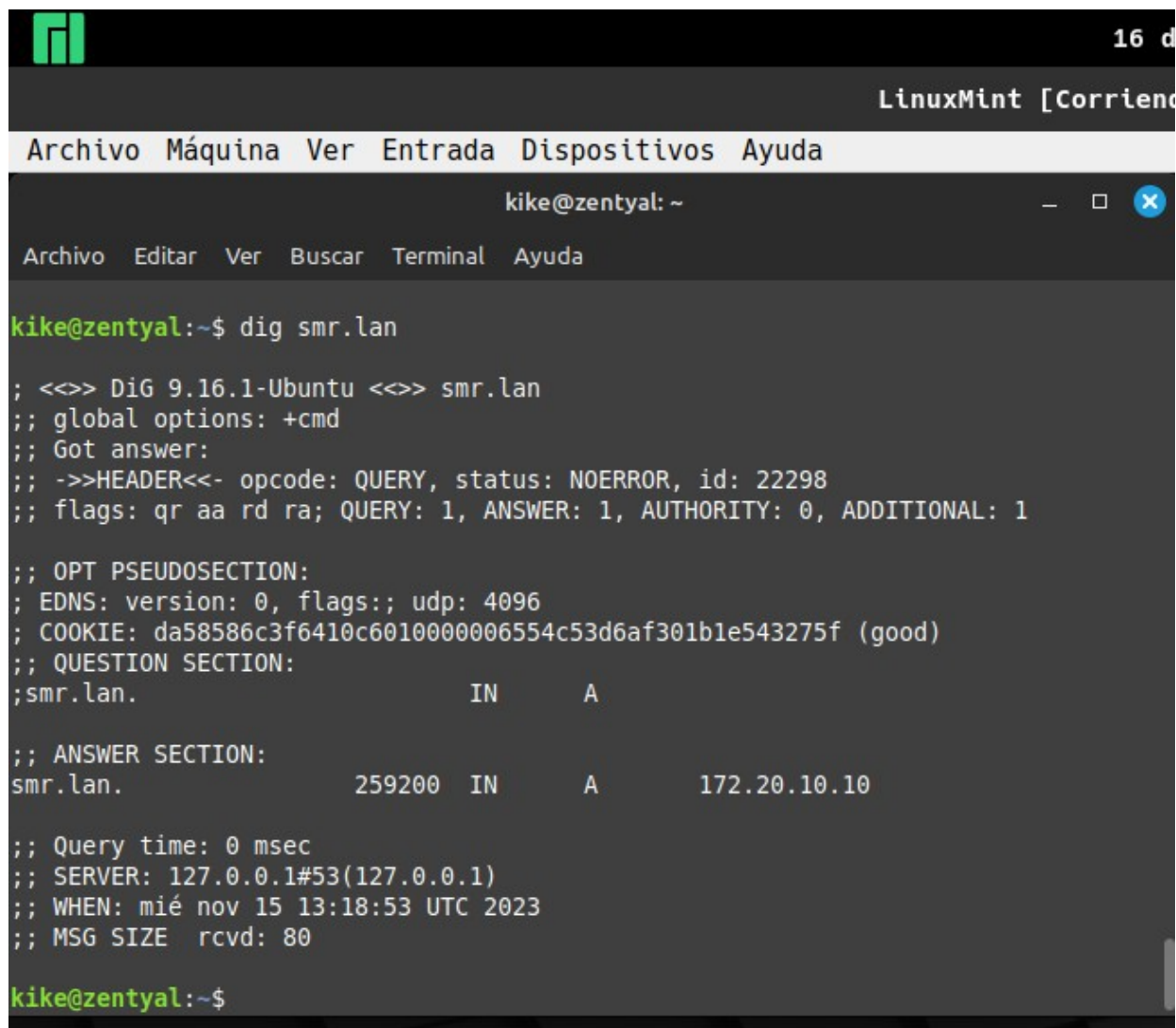
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6347237449c8e7d8010000006554d451d4bdbc39babac0a1 (good)
;; QUESTION SECTION:
;alt2aspmx.l.google.com.      IN      A

;; AUTHORITY SECTION:
l.google.com.                5      IN      SOA     ns1.google.com. dns-admin.google.com. 5
0 900 1800 60

;; Query time: 40 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié nov 15 14:23:13 UTC 2023
;; MSG SIZE rcvd: 139

kike@zentyal:~$
```


3.3 Usando dig, adjunta una captura donde se obtenga la lista de servidores DNS de nuestro dominio.



```
kike@zentyal:~$ dig smr.lan

; <<>> DiG 9.16.1-Ubuntu <<>> smr.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22298
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

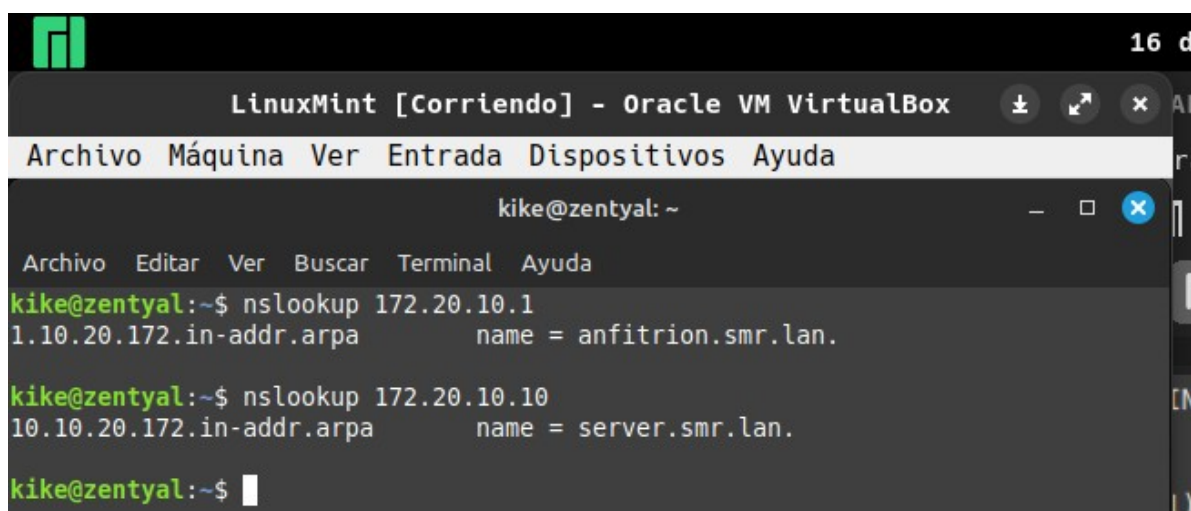
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: da58586c3f6410c6010000006554c53d6af301b1e543275f (good)
;; QUESTION SECTION:
;smr.lan.                IN      A

;; ANSWER SECTION:
smr.lan.                259200  IN      A      172.20.10.10

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié nov 15 13:18:53 UTC 2023
;; MSG SIZE rcvd: 80

kike@zentyal:~$
```

3.4 Utiliza **nslookup** para comprobar la **resolución inversa** de las IPs **172.20.10.1** y **172.20.10.10**.



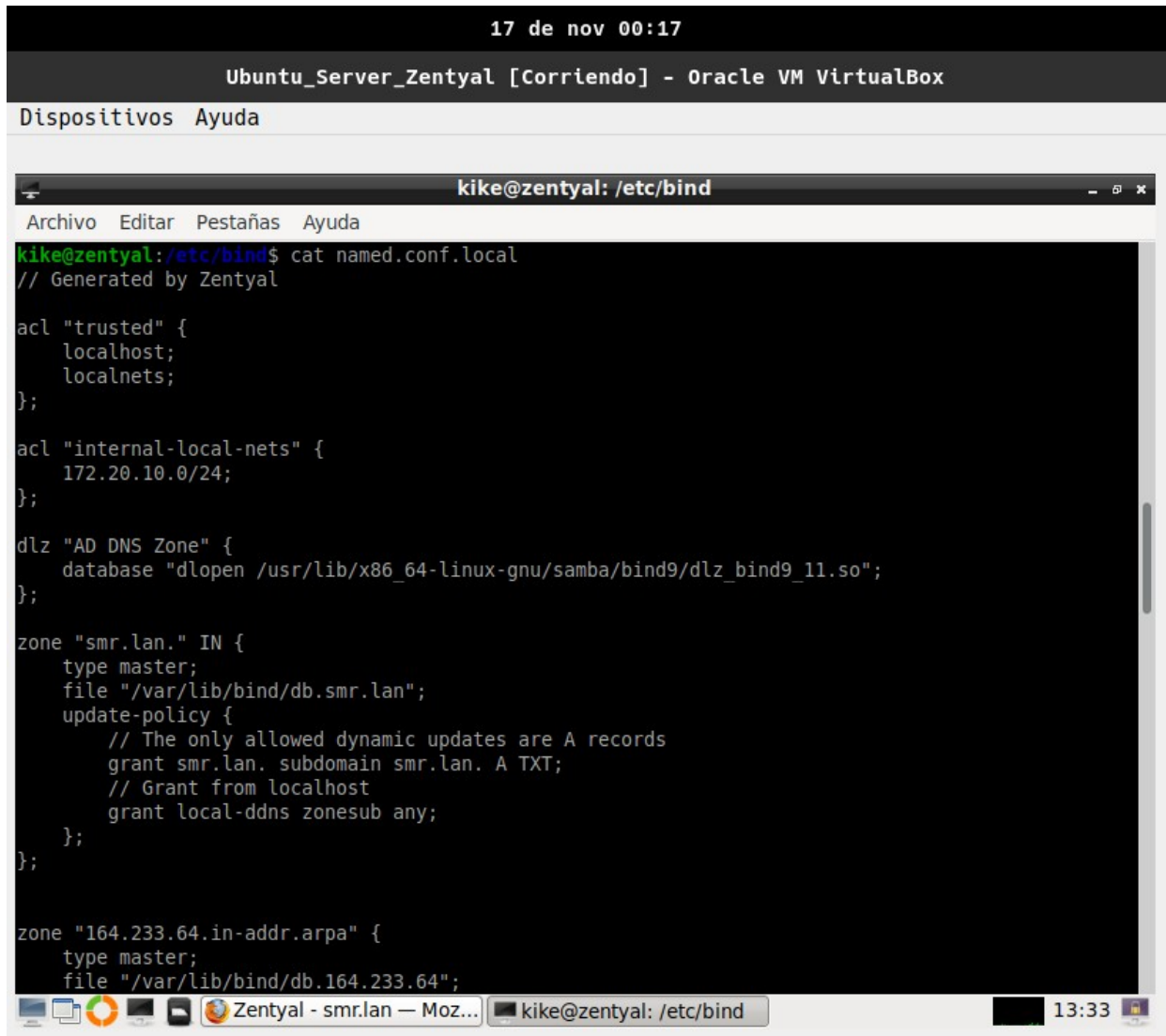
```
kike@zentyal:~$ nslookup 172.20.10.1
1.10.20.172.in-addr.arpa      name = anfitrion.smr.lan.

kike@zentyal:~$ nslookup 172.20.10.10
10.10.20.172.in-addr.arpa     name = server.smr.lan.

kike@zentyal:~$
```

5 Inspecciona el directorio **/etc/bind/** e indica que fichero o ficheros se han creado para nuestra zona. Adjunta también el contenido completo del **fichero de zona**.

Tenemos el archivo **named.conf.local** y se nos ha creado también el archivo **named.conf.default-zones**



The screenshot shows a terminal window titled "kike@zentyal: /etc/bind". The terminal output is as follows:

```
17 de nov 00:17
Ubuntu_Server_Zentyal [Corriendo] - Oracle VM VirtualBox
Dispositivos Ayuda

kike@zentyal: /etc/bind
Archivo Editar Pestañas Ayuda
kike@zentyal:/etc/bind$ cat named.conf.local
// Generated by Zentyal

acl "trusted" {
    localhost;
    localnets;
};

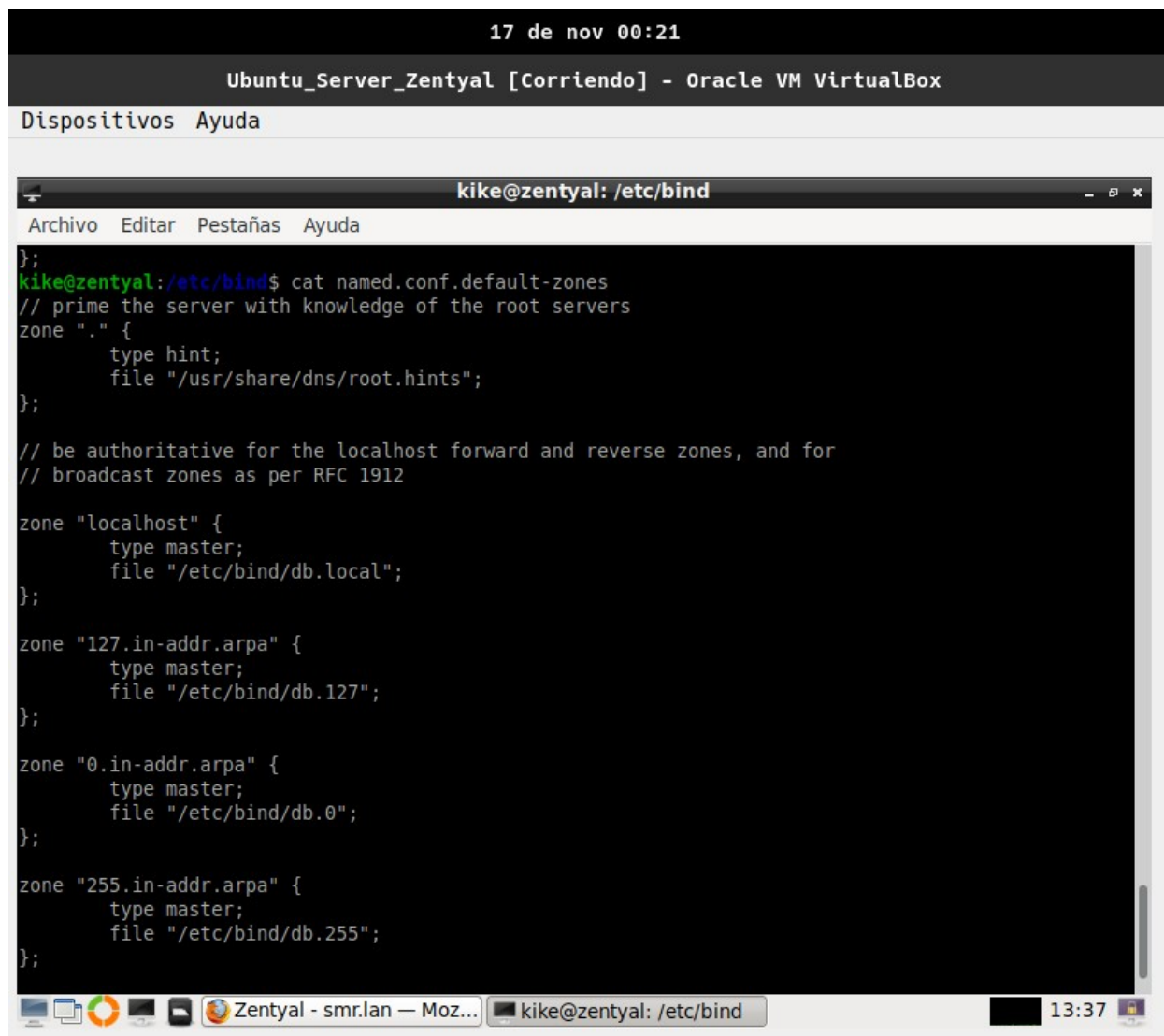
acl "internal-local-nets" {
    172.20.10.0/24;
};

dlz "AD DNS Zone" {
    database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_11.so";
};

zone "smr.lan." IN {
    type master;
    file "/var/lib/bind/db.smr.lan";
    update-policy {
        // The only allowed dynamic updates are A records
        grant smr.lan. subdomain smr.lan. A TXT;
        // Grant from localhost
        grant local-ddns zonesub any;
    };
};

zone "164.233.64.in-addr.arpa" {
    type master;
    file "/var/lib/bind/db.164.233.64";
```

The terminal window has a menu bar with "Archivo", "Editar", "Pestañas", and "Ayuda". The bottom status bar shows the window title "Zentyal - smr.lan — Moz...", the user and directory "kike@zentyal: /etc/bind", and the time "13:33".



```
17 de nov 00:21
Ubuntu_Server_Zentyal [Corriendo] - Oracle VM VirtualBox
Dispositivos Ayuda

kike@zentyal: /etc/bind
Archivo Editar Pestañas Ayuda

kike@zentyal:/etc/bind$ cat named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.localhost";
};

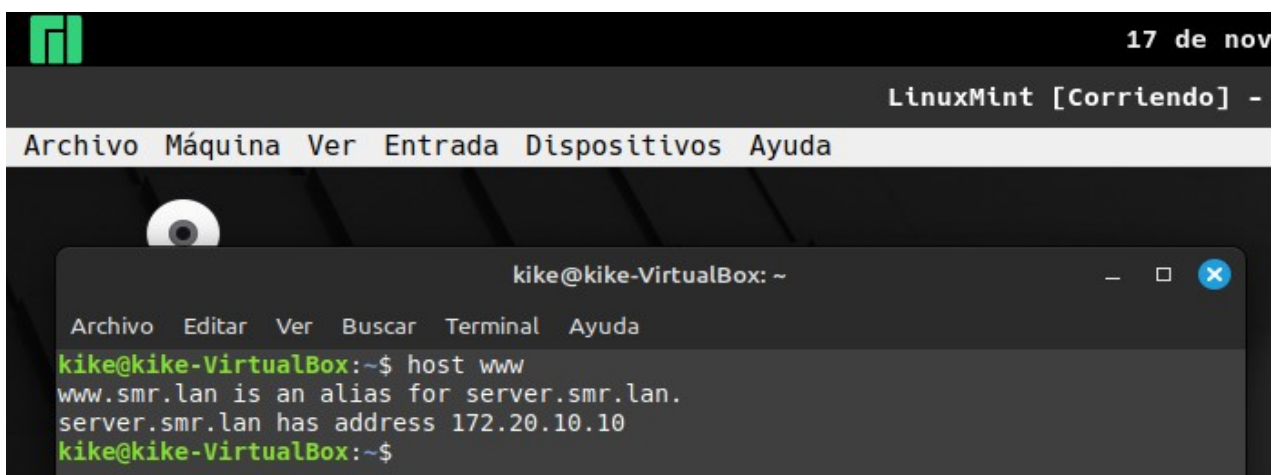
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

3.6 Arranca el cliente **Ubuntu Desktop**. Configura la red con la IP: **172.20.10.20/24**. Como **gateway** y **servidor DNS** utiliza la IP interna del **servidor Zentyal**.

Comprueba con **dig** que puedes resolver el **FQDN** correspondiente al nombre de host **"www"**, adjunta una captura.



```
17 de nov
LinuxMint [Corriendo] -
Archivo Máquina Ver Entrada Dispositivos Ayuda

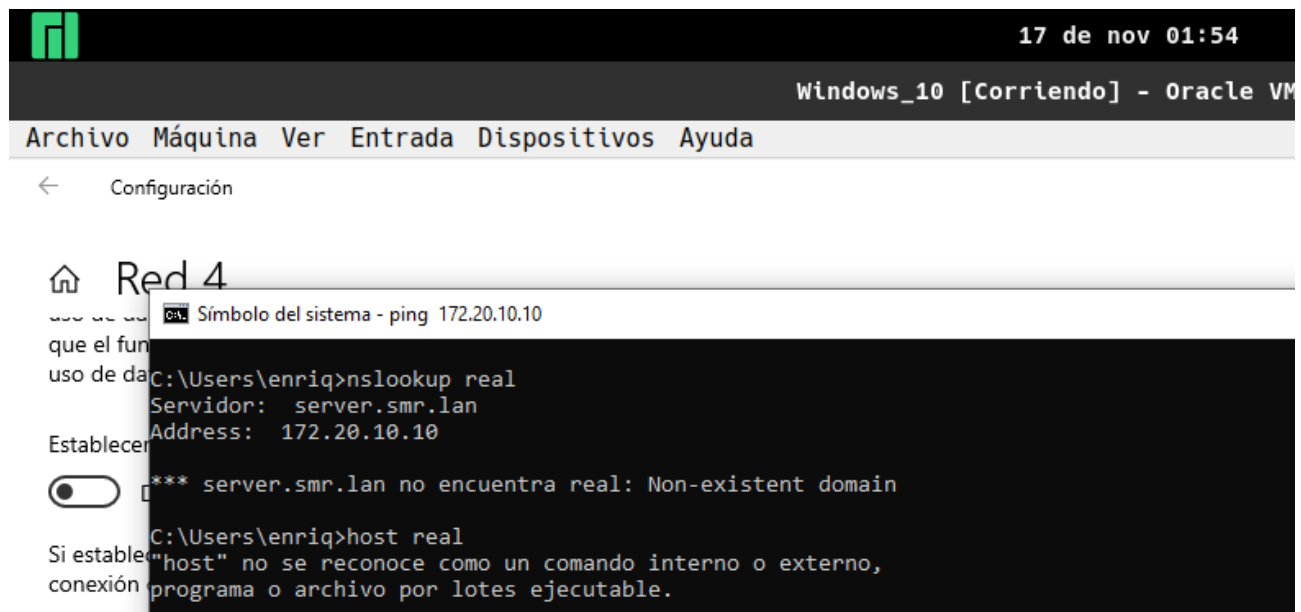
kike@kike-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda

kike@kike-VirtualBox:~$ host www
www.smr.lan is an alias for server.smr.lan.
server.smr.lan has address 172.20.10.10
kike@kike-VirtualBox:~$
```

3.7 Arranca el cliente Windows 10. Configura al red manualmente con la IP: **172.20.10.30/24**. Como **gateway** y **servidor DNS** utiliza la **IP interna del servidor Zentyal**.

Comprueba con **nslookup** que puedes resolver el **FQDN** correspondiente al nombre de host **"real"**, adjunta una captura.

Tengo muchos problemas con las MV windows, te pongo esta captura pero se me apagaba la máquina cada vez que la encendía. El servidor va bien y la conexión entre MVs están bien configurada.



The screenshot shows a virtual machine window titled "Windows_10 [Corriendo] - Oracle VM". The interface includes a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu is a "Configuración" (Configuration) window. On the left, under "Red 4" (Network 4), there is a toggle switch for "Símbolo del sistema - ping 172.20.10.10" which is currently turned off. The main area of the configuration window shows a command prompt with the following text:

```
C:\Users\enriq>nslookup real
Servidor:  server.smr.lan
Address:  172.20.10.10

*** server.smr.lan no encuentra real: Non-existent domain

C:\Users\enriq>host real
"host" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
```