Práctica 4 – Servicio DNS

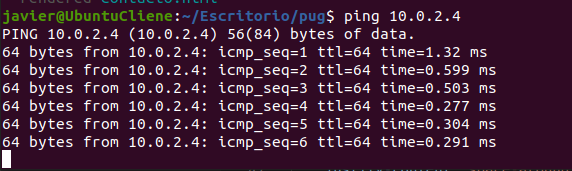
Se trata de que instales un servicio DNS sobre Ubuntu Server, de manera que el cliente Ubuntu resuelva direcciones IP y DNS al estar en la misma Red NAT. También realizarás alguna configuración sobre ellos y en el servicio DHCP de VirtualBox.

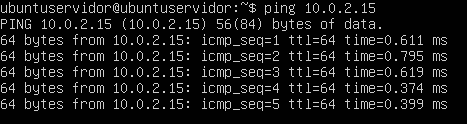
Indicaciones generales:

1. Genera capturas de cada paso.
2. Obtén un documento final <nombre>\_<apellido>\_practica\_<Nº>.**pdf**
3. Súbelo a la plataforma.

**Contenido práctica**

* 1. Tenemos este escenario inicial:
     1. Trabajaremos con un Ubuntu Server y Ubuntu Desktop, que por estar en una Red NAT se integran en un servicio DHCP de VirtualBox.
     2. Las dos VM están conectadas entre sí mediante una red nat.

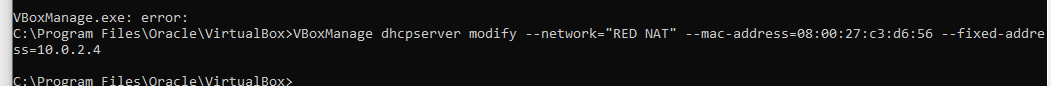


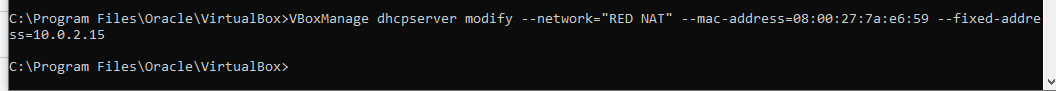


* 1. Es conveniente fijar una IP al servidor. Dado que estamos usando una red nat y no una Red Interna, vamos a usar un comando de VirtualBox que nos permite configurar algunas cuestiones del servicio DHCP interno asociado a la red nat. En particular, asignaremos una IP fija a una VM cuya dirección MAC de su adaptador de red conozcamos, para una cierta red. Ejemplo:

VBoxManage dhcpserver modify --network=RedNat --mac- address=08:00:27:fe:63:80 --fixed-address=10.0.2.7

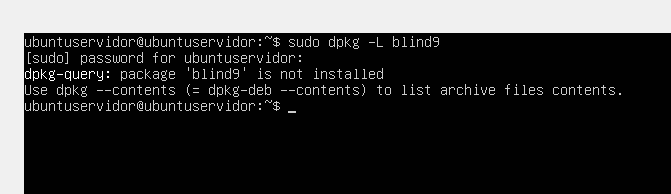
Donde “RedNat” es el nombre de la red nat, “08:00:27:fe:63:80” es la dirección MAC del adaptador de red de nuestro Ubuntu Server y "10.0.2.7" será la IP fija para dicha VM. Este comando hay que lanzarlo con todas las VMs de la red nat apagadas. Con este procedimiento nunca será modificada la IP de Ubuntu Server dentro de nuestra red nat y podemos instalar servicios sin problemas de cambios de IP.

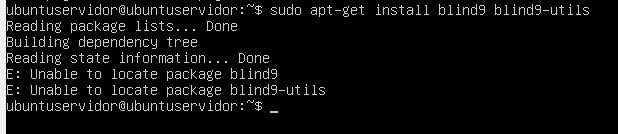


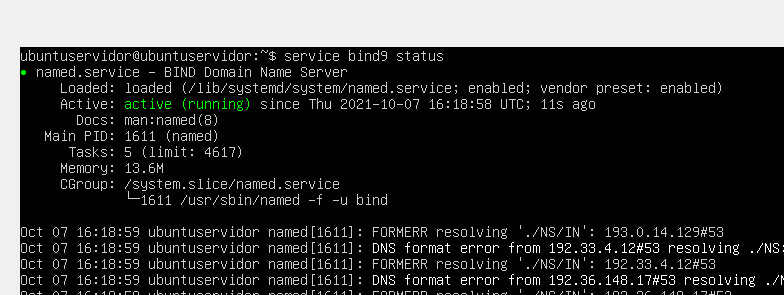


NOTA: podemos realizar lo mismo para el cliente y asignarle la IP 10.0.2.14, por ejemplo.

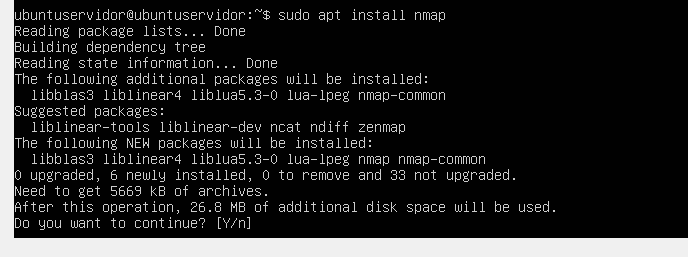
* 1. En el Servidor. Preliminares:
     1. Instala un servicio DNS mediante el paquete Bind9.
        1. Comprueba que no tienes instalado el paquete mediante: **sudo dpkg -L bind9**

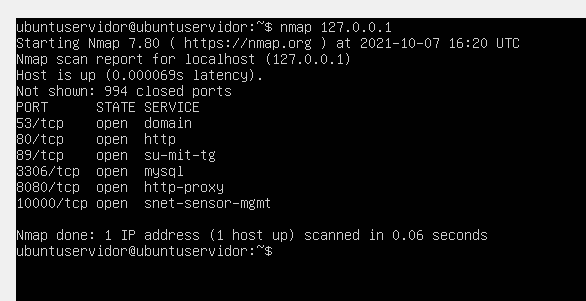


* + - 1. Instalación: **sudo apt-get install bind9 bind9utils**
      2. Para, reinicia y verifica el status del servicio con **service bind9 stop/restart/status** ó **systemctl stop/restart/... bind9**

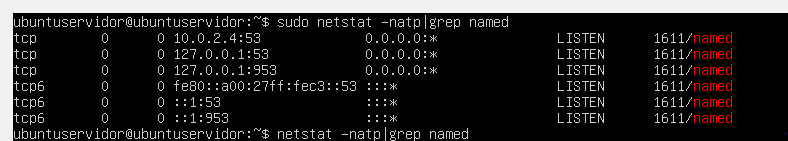


* + - 1. Verifica que el puerto 53 está abierto con nmap (instala el paquete de nmap ni no lo tienes instalado), necesario para que funcione el servicio DNS: nmap 127.0.0.1, que ofrece los puertos abiertos en el servidor.



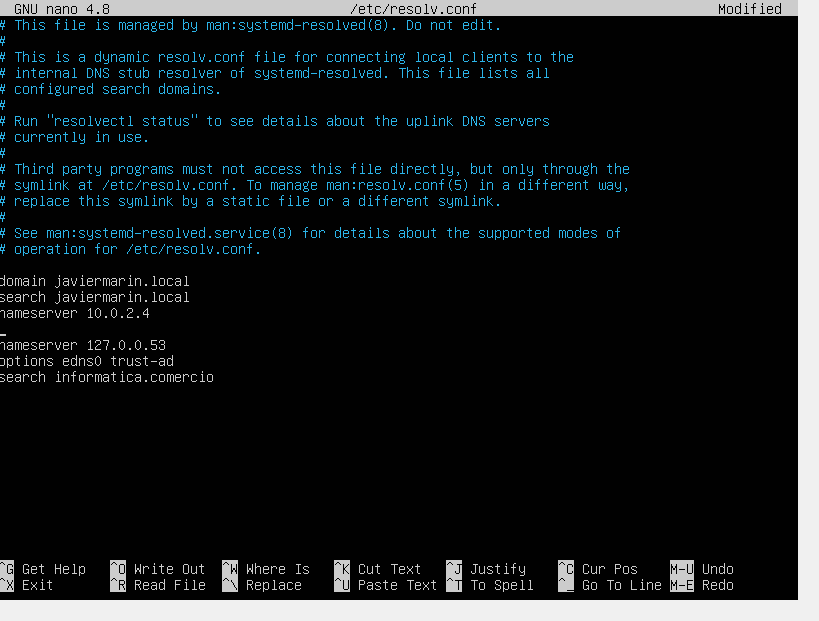


* + - 1. Emplea este comando con el servicio named, que hace referencia a servicios DNS exclusivamente: netstat -natp | grep named



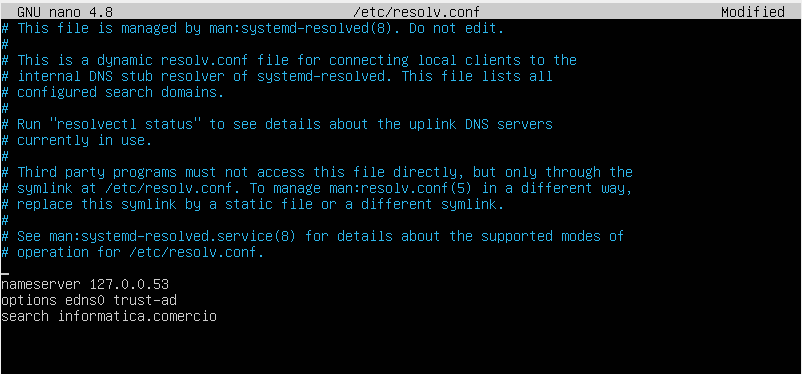
* + 1. Configura /etc/resolv.conf para indicar qué IP resuelve las direcciones DNS:

domain <nombreapellidos>.local search <nombreapellidos>.local nameserver IPSERVIDOR

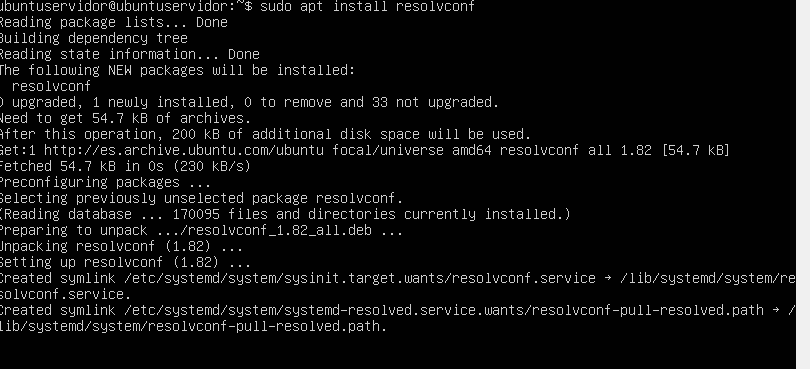


PD: /etc/resolv.conf puede resetearse al reiniciar cada vez la VM, es conveniente que tengáis una copia de resolv.conf en vuestro directorio home y que lo machaquéis si observáis esa circunstancia. Otra solución, persistente, es, extraída de https://[www.ricmedia.com/set-permanent-dns-nameservers-ubuntu-](http://www.ricmedia.com/set-permanent-dns-nameservers-ubuntu-) debian-resolv-conf/

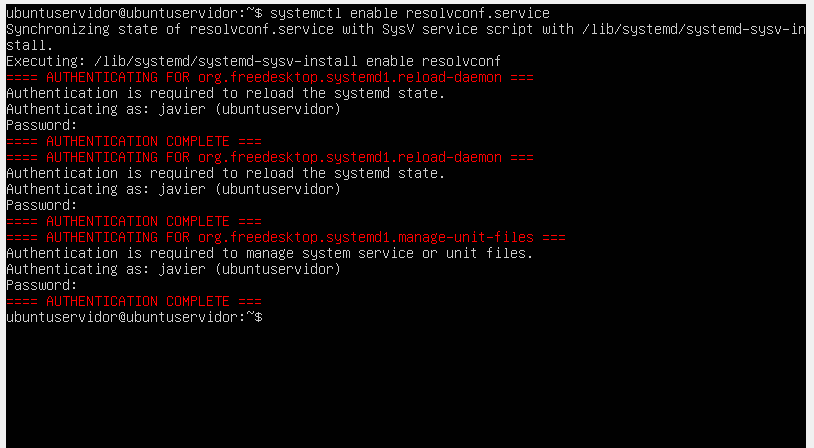
* 1. Eliminamos las líneas indicadas en C) b y lo dejamos vacío.



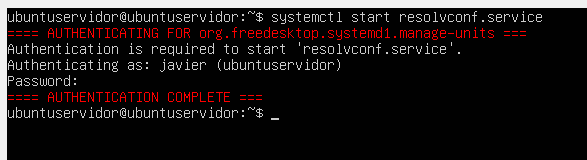
* 1. apt install resolvconf



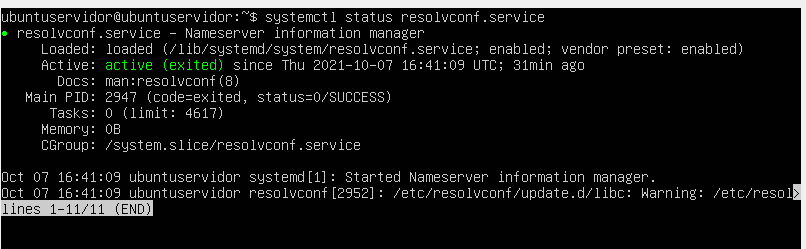
* 1. systemctl enable resolvconf.service



* 1. systemctl start resolvconf.service

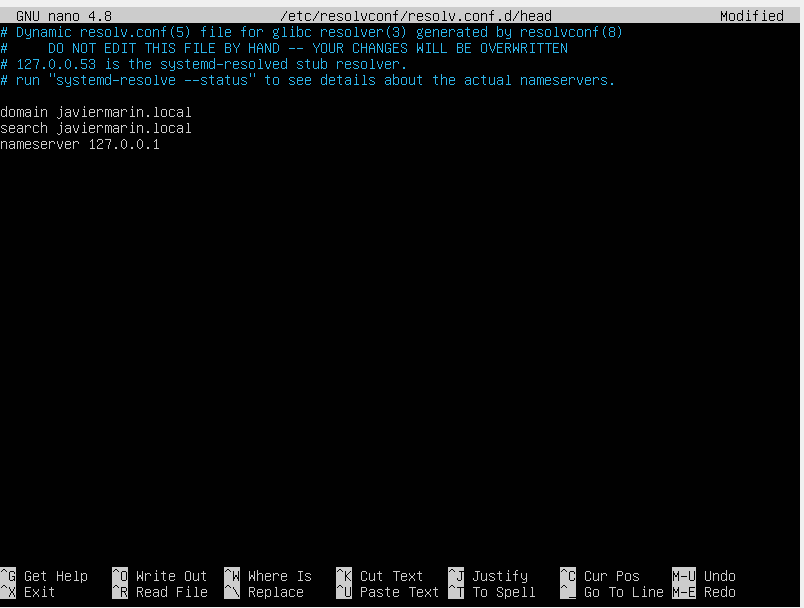


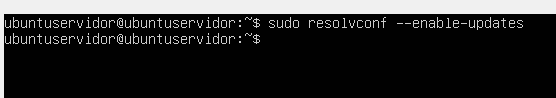
* 1. systemctl status resolvconf.service



* 1. Edita /etc/resolvconf/resolv.conf.d/head y agrega:

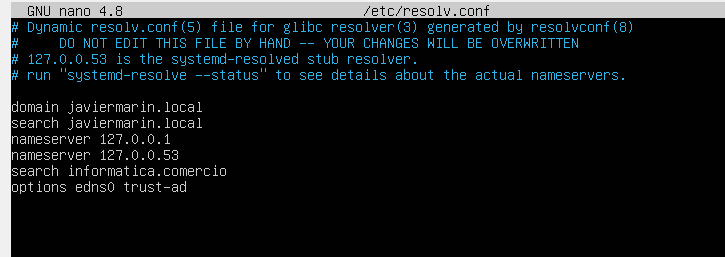
domain <nombreapellidos>.local search <nombreapellidos>.local nameserver IPSERVIDOR



* 1. resolvconf --enable-updates
  2. resolvconf -u



Si editamos ahora /etc/resolv.conf, deberíamos ver en las primeras líneas lo indicado en b.5), quedando persistente ante reboot y ante cambios de configuración de la red.

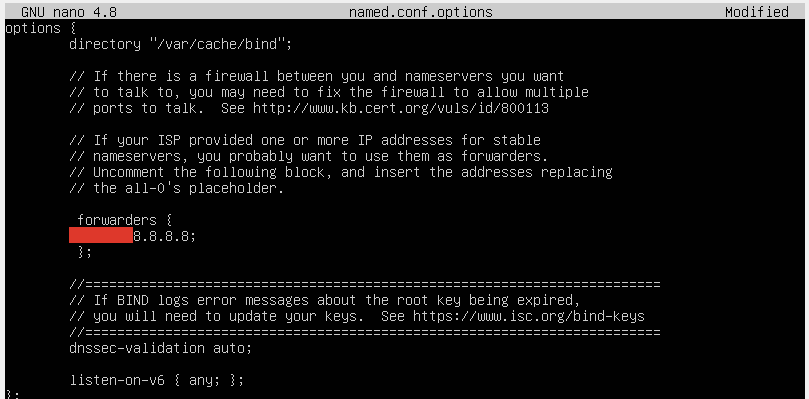


* 1. Configuración de zonas directas e indirectas:
     1. Acude a /etc/bind
     2. Explica qué significan los archivos que empiezan por db y los archivos que empiezan por named. Qué sentido tienen y para qué se usan.

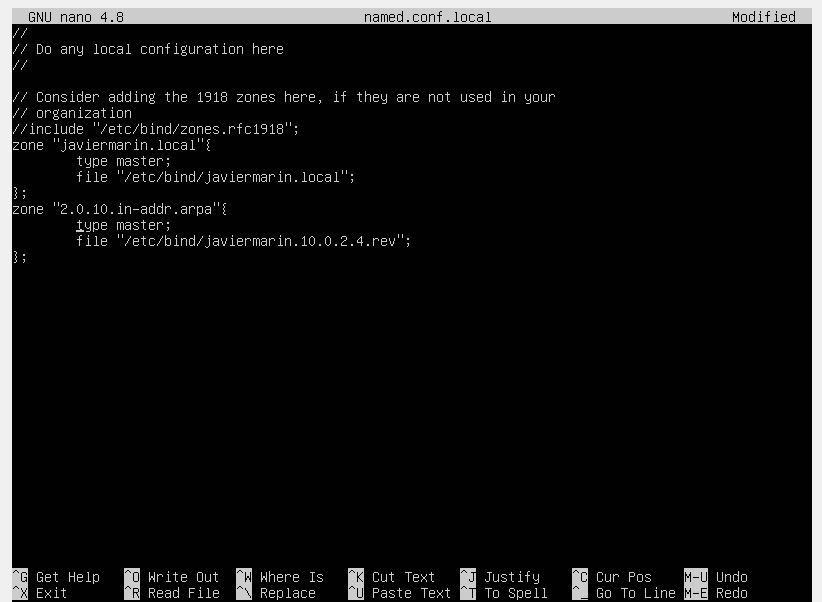
**DB**: El fichero db. local es un fichero de zona que va a permitir resolver el nombre localhost a la dirección de loopback 127.0.0.1

**NAMED:** Un fichero muy pequeño que contiene punteros a ficheros con informacion de zonas y a otros servidores de nombres.

* + 1. Modificamos el archivo named.conf.options para configurar el reenviador que resolverá direcciones externas. Indica el DNS de Google en forwarders. Ello nos resolverá IPs externas a nuestra red local.



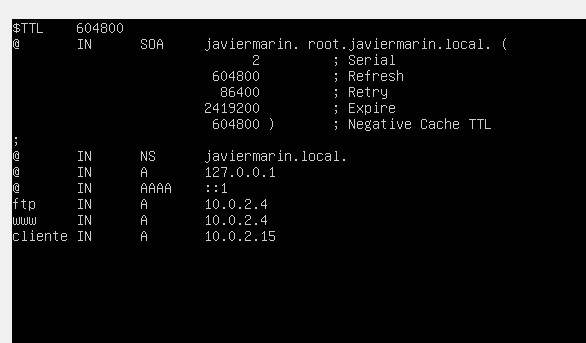
* + 1. Edita named.conf.local. Vamos a crear una zona DNS Maestra y vamos agregar la zona de dominio <nombreyapellidos>.local. Para ello agrega una zona directa e indirecta. Apóyate en los apuntes y no olvides poner ; al cierre de las llaves.



* + 1. Verifica que los archivos de configuración están bien escritos mediante named-checkconf.

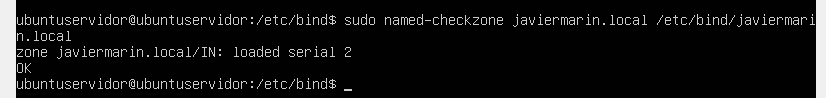


* 1. Crea la base de datos de la zona directa:
     1. Genera <nombreyapellidos>.local (apóyate en db.local)
     2. Edita el nuevo archivo y asocia los nombres de las máquinas y sus IPs:
        1. ftp.<nombreyapellidos>.local -> IPSERVIDOR
        2. [www.](http://www/)<nombreyapellidos>.local -> IPSERVIDOR
        3. cliente.<nombreyapellidos>.local -> IPCLIENTE



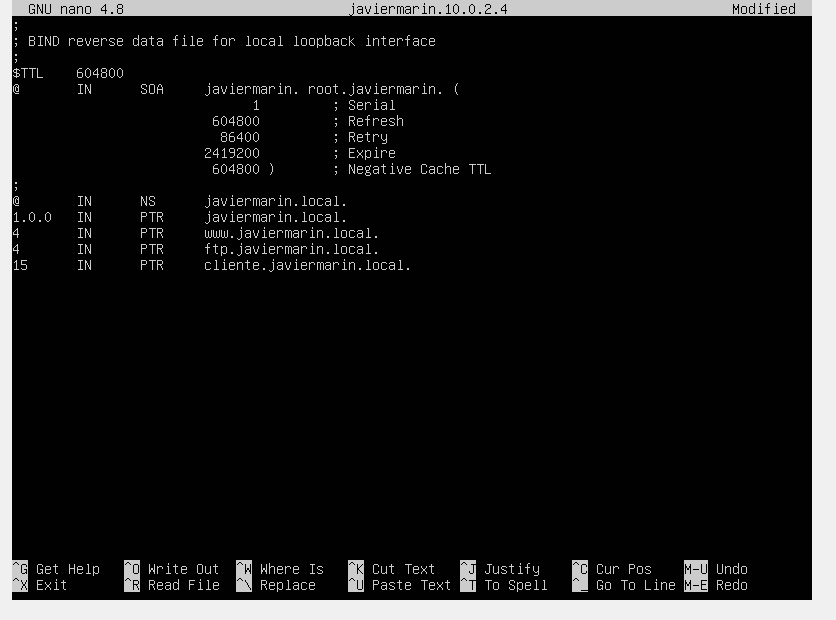
* + 1. Utiliza el comando named-checkzone <nombreyapellidos>.local

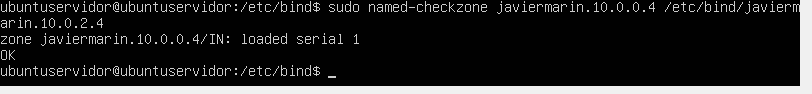
/etc/bind/<nombreyapellidos>.local para verificar que no hay errores en el archivo



* 1. Crea la base de datos de la zona indirecta:
     1. La nomenclatura es <nombreyapellidos>.IPSERVIDOR (apóyate en db.127)
     2. Edita el nuevo archivo y asocia los nombres de las máquinas y sus IPs.
     3. Utiliza el comando named-checkzone

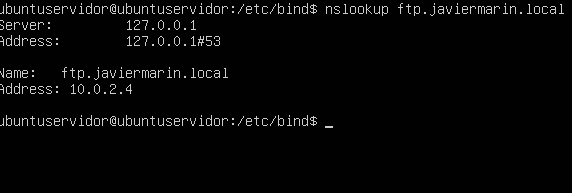
/etc/bind/<nombreyapellidos>.IPSERVIDOR para verificar que no hay errores en el archivo.



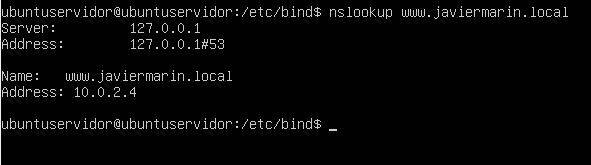


* 1. Verifica que el servicio DNS resuelve correctamente de forma directa e indirecta:

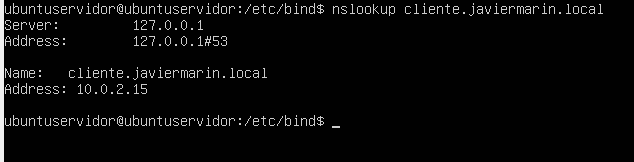
nslookup ftp.<nombreyapellidos>.local

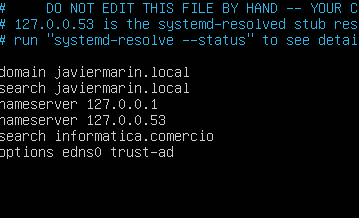


nslookup [www.](http://www/)<nombreyapellidos>.local

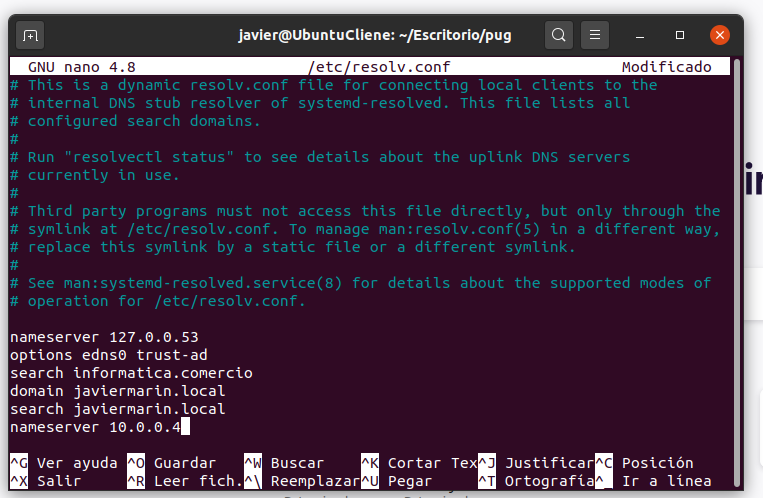


nslookup cliente.<nombreyapellidos>.local



* 1. Verifica en los clientes Ubuntu que pueden resolver las anteriores direcciones de la red local. Para ello:
     1. nano /etc/resolv.conf
     2. Indica que el servidor DNS está en la máquina de IP fija y que va buscar en la zona indicada:

domain <nombreapellidos>.local search <nombreapellidos>.local nameserver IPSERVIDOR



* + 1. Guarda el archivo y verifica que el cliente resuelve bien las siguientes direcciones:

REPETIR LO HECHO EN LA MAQUINA SERVIDO CON RESOLVCONF (INSTALAR Y CONFIGURAR)

nslookup ftp.<nombreyapellidos>.local nslookup [www.](http://www/)<nombreyapellidos>.local nslookup cliente.<nombreyapellidos>.local

* 1. Abre el navegador web en el cliente y ejecuta [www.](http://www/)<nombreapellidos>.local y verifica que ves el punto de entrada de Apache.

