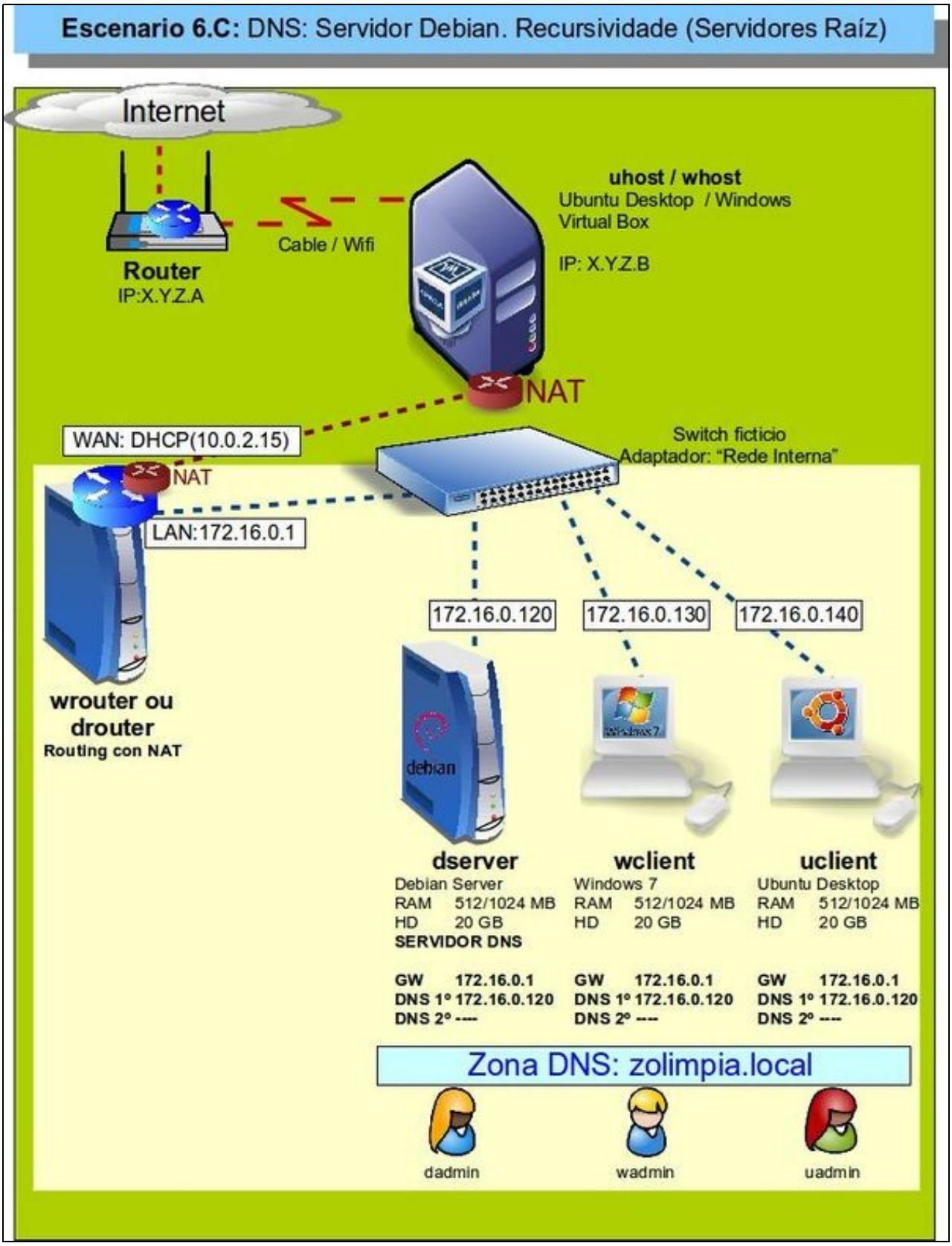
1 Linux: Instalación e configuración do servidor usando recursividade



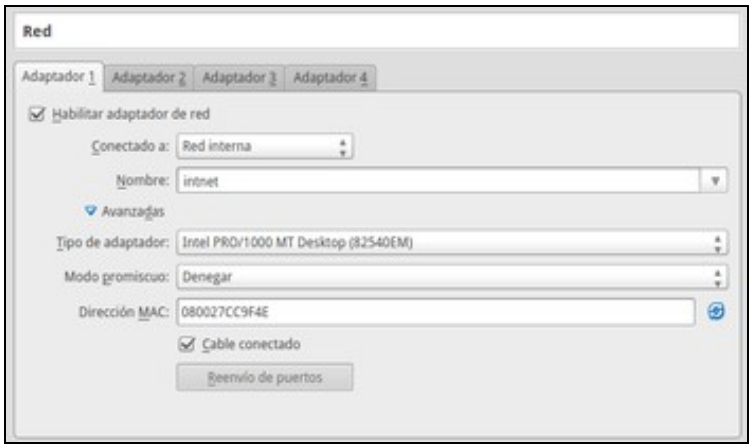
- Visto escenario vaise instalar e configurar o servizo DNS no equipo **dserver**.
- A saída a Internet nas máquinas pódese facer usando a máquina *wrouter* ou *drouter* como router con NAT ou configurando as tarxetas das máquinas en modo de rede NAT.
- O servidor **dserver** terá configurada 2 zonas:
    - Zona de busca directa: **zolimpia.local**

        - Zona de busca inversa: **172.16.0.0**
- Ademais estará configurado para usar **recursividade**.
- Revisar os Conceptos básicos de DNS se non se ten claro algún dos parámetros anteriores.

1.1 Sumario

1.2 Configuración previa da MV dserver

- Facer unha instantánea de **dserver** coa MV apagada.



A MV *dserver* xa debera estar configurada do escenario anterior cun único adaptador en modo **Rede interna** ou en modo **Rede NAT** se se quere evitar a necesidade da máquina *router*.

```
root@dserver:~# more /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 172.16.0.120
        netmask 255.255.0.0
        gateway 172.16.0.1
        dns-nameservers 10.0.0.1
root@dserver:~#
```

A configuración mostra a configuración de IP, máscara e porta de enlace do escenario. De momento temos configurado como servidor DNS o que temos na máquina host, neste caso o *10.0.0.1*.

```
root@dserver:~# ping www.google.es -c 1
PING www.google.es (74.125.206.94) 56(84) bytes of data.
64 bytes from wk-in-f94.1e100.net (74.125.206.94): icmp_seq=1 ttl=61 time=46.7 ms

--- www.google.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 46.722/46.722/46.722/0.000 ms
root@dserver:~#
```

E a máquina pode resolver nomes de DNS, como por exemplo *www.google.es*.

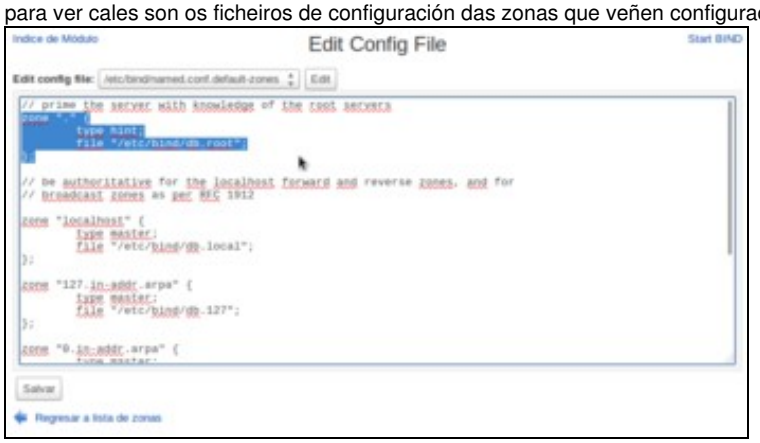
1.3 Instalar o servizo DNS en dserver

- Para comezar, veremos como instalar o servizo de DNS e inicialo coa configuración por defecto, na que resolverá os nomes de Internet por recursividade usando os servidores raíz.

- Instalación do servizo de DNS en Debian
- 

Usando o módulo de **Paquetes de Software**, instalamos o paquete **bind9**.
- 

Rematada a instalación, refrescamos os módulos do Webmin para que apareza dentro da categoría de **Servidores** o módulo de configuración do servidor DNS. Na imaxe podemos ver a páxina inicial do módulo, coas opcións principais. Estas opcións traduciranse en parámetros nos ficheiros de configuración, que podemos ver picando en **Editar ficheiro de configuración**.
- 

Aparecen na parte superior os ficheiros de configuración básicos do servidor DNS. Como podemos ver na imaxe, o ficheiro principal **/etc/bind/named.conf** basicamente o que fai é incluír os outros tres ficheiros. Seleccionamos o ficheiro **/etc/bind/named.conf.default-zones** para ver cales son os ficheiros de configuración das zonas que veñen configuradas por defecto.
- 

Na imaxe podemos ver que hai unha zona co nome ".", que é a zona raíz que permite ao servidor resolver por recursividade usando os servidores raíz. O ficheiro de configuración desa zona está en **/etc/bind/db.root**. Nese ficheiro pódense atopar as referencias aos servidores raíz de Internet.

- 

Pero para que a resolución de nomes por recursividade funcione correctamente, temos que configurar un parámetro que afecta á extensións de seguridade do protocolo DNS, coñecidas como DNSSEC. Estas extensións aumentan a seguridade do servizo de DNS xa que as respostas veñen asinadas para garantir que foron emitidas polos servidores DNS raíz auténticos e non foron modificadas no seu camiño a través da rede, pero requiren unha configuración correcta das chaves para a validación das sinaturas, así que imos desactivar o seu uso para simplificar a instalación do servizo. Picamos en **Verificación de DNSSEC**.

- 

E no parámetro de **Habilitada a validación de respostas DNSSEC?** seleccionamos **Non**. Gardamos os cambios...

- 

E xa podemos iniciar o servidor **bind**, usando a opción da parte superior dereita da páxina.

- 

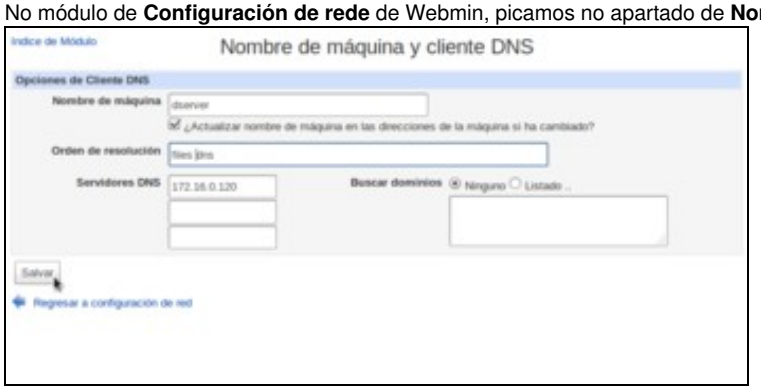
Unha vez iniciado o servizo, vemos que na parte superior aparecen as opcións de deter o servizo e aplicar a configuración. Xa temos o servidor DNS funcionando.

1.4 Configuración do cliente DNS de dserver

- Aínda que *dserver* sexa o servidor de DNS tamén é cliente, e haberá que configurar o cliente DNS para que pregunte, a partir de agora, ao servidor DNS que el mesmo ten instalado.

- 

No módulo de **Configuración de rede** de Webmin, picamos no apartado de **Nome de máquina e cliente DNS**.

- 

Establecemos como orde de resolución **files dns** (para evitar o problema coas resolución dos dominios *.local*). Como servidor de DNS poñemos a súa propia dirección IP: 172.16.0.120.

- ```
root@dserver:/home/dadmin# more /etc/resolv.conf
nameserver 172.16.0.120
Generated by NetworkManager
root@dserver:/home/dadmin# more /etc/nsswitch.conf
/etc/nsswitch.conf
#
Example configuration of GNU Name Service Switch functionality.
If you have the `glibc-doc-reference' and `info' packages installed, try:
`info libc "Name Service Switch"' for information about this file.

passwd: compat
group: compat
shadow: compat
gshadow: files

hosts: files dns
networks: files

protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: nis
```

Observar como agora **/etc/resolv.conf** amosa cal é servidor de DNS ao que realizar as consultas DNS, e o ficheiro **/etc/nsswitch.conf** a orde de resolución.

- ```
root@dserver:/home/dadmin# ping www.google.es -c 1
PING www.google.es (74.125.206.94) 56(84) bytes of data.
64 bytes from wk-in-f94.1e100.net (74.125.206.94): icmp_seq=1 ttl=61 time=40.9 ms

--- www.google.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.950/40.950/40.950/0.000 ms
root@dserver:/home/dadmin#
```

Comprobar que o servidor DNS fai resolucións DNS de equipos do exterior. Isto é grazas aos servidores raíz.

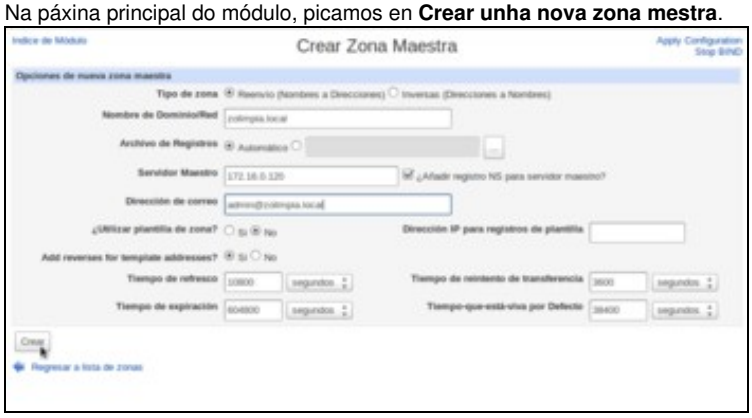
1.5 Configurar zona de busca directa: zolimpia.local

- A continuación vaise crear a zona de busca directa para o dominio **zolimpia.local**, isto é, dado un nome de dominio que se nos diga a IP asociada.

- Configurar unha zona de busca directa

- 

Na páxina principal do módulo, picamos en **Crear unha nova zona mestra**.

- 

Para crear unha zona de busca directa, indicamos como tipo de zona de **Reenvío**. Introducimos o nome da nova zona: **zolimpia.local**, a dirección IP do servidor mestre (que é a de *dserver*) e un enderezo de correo asociada á zona (aínda que non ten que existir realmente ese enderezo). Picamos no botón de **Crear** para crear a zona no ficheiro de configuración do servidor.

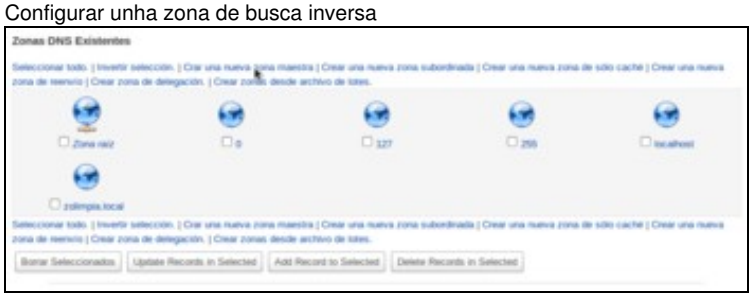
- 

Na imaxe podemos ver a páxina de configuración da zona, que usaremos para dar de alta rexistros dentro da mesma e onde tamén hai apartados para configurar parámetros da zona. Pero antes de crear rexistros, imos ir ao índice do módulo para crear a zona de busca inversa, xa que desta maneira poderemos crear automaticamente os rexistros inversos que permitirán obter o nome de DNS dun equipo desta zona a partir da súa dirección IP.

1.6 Crear zona de busca inversa

- Vexamos como crear unha zona de busca inversa.

- Configurar unha zona de busca inversa

- 

No índice do módulo, picamos sobre **Crear unha nova de zona mestra**.

- 

Neste caso, no tipo de zona escolleremos **inversa**. Como nome de rede introducimos o número da rede para a que queremos facer as resolucións inversas , a **172.16**. Como servidor mestre e enderezo de correo, podemos poñer os mesmos que no caso anterior.

- 

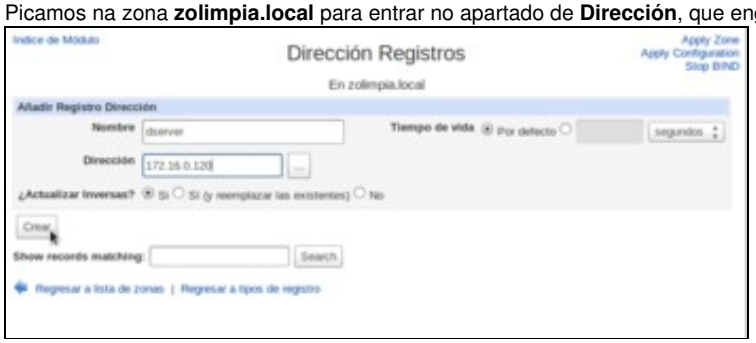
Na páxina de configuración da zona, observamos que neste tipo de zona hai moitos menos tipos de rexistro que na zona de busca directa. En realidade non imos crear manualmente os rexistros nesta zona, xa que faremos que Webmin os cree automaticamente cando creemos os rexistros na zona de busca directa. Por iso, imos ao índice do módulo para crear os rexistros da zona directa.

1.7 Creación de rexistros dentro da zona

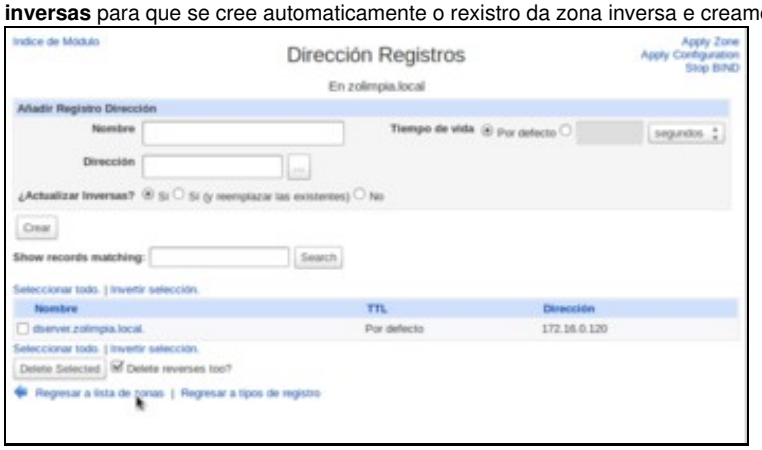
- Neste curso só se vai traballar cos rexistros tipo host (Coñecidos como A) e cos tipo PTR para a resolución inversa. Para afondar no coñecemento dos tipos de rexistro recoméndase: http://es.wikipedia.org/wiki/DNS#Tipos_de_registros_DNS.

- Creación de rexistros nas zonas
- 

Picamos na zona **zolimpia.local** para entrar no apartado de **Dirección**, que engloba os rexistros de tipo *host*.

- 

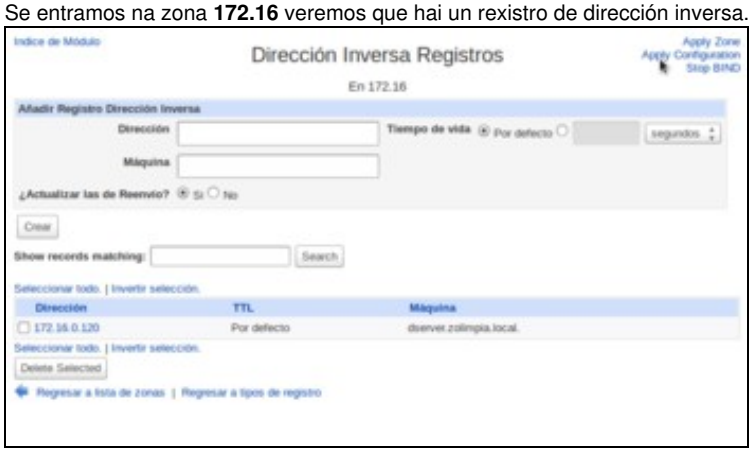
Introducimos como nome o nome do servidor **dserver** e como dirección IP 172.16.0.120. Deixamos marcada a opción de **Actualizar as inversas** para que se cree automaticamente o rexistro da zona inversa e creamos o rexistro.

- 

Podemos ver na táboa o rexistro creado. Imos ao índice do módulo para ver se aparece o rexistro correspondente na zona inversa.

- 

Se entramos na zona **172.16** veremos que hai un rexistro de dirección inversa. Picamos sobre **Dirección inversa** para velo.

- 

Comprobamos que o rexistro creado é o inverso ao que creamos na zona directa. É importante ter en conta que aínda que todos os cambios estean realizados nos ficheiros de configuración, aínda non son efectivos no servizo de DNS. Picamos sobre a opción de **Aplicar configuración** para facer efectivas as novas zonas e os rexistros creados.

- ```
root@dserver:/home/dadmin# ping dserver.zolimpia.local -c 1
PING dserver.zolimpia.local (172.16.0.120) 56(84) bytes of data.
64 bytes from dserver.zolimpia.local (172.16.0.120): icmp_seq=1 ttl=64 time=0.035 ms

--- dserver.zolimpia.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.035/0.035/0.035/0.000 ms
```

Comprobación dende *dserver* da resolución directa.
```

-
```
root@dserver:/home/dadmin# dig -x 172.16.0.120

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> -x 172.16.0.120
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22515
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

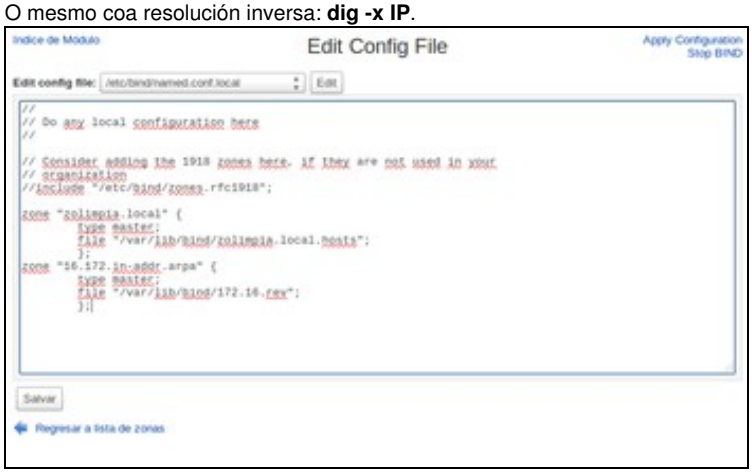
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;120.0.16.172.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
120.0.16.172.in-addr.arpa. 38400 IN     PTR     dserver.zolimpia.local.

;; AUTHORITY SECTION:
16.172.in-addr.arpa.    38400   IN      NS      172.16.0.120.

;; Query time: 2 msec
;; SERVER: 172.16.0.120#53(172.16.0.120)
;; WHEN: Mon Mar 28 14:04:18 CEST 2016
;; MSG SIZE  rcvd: 116
```

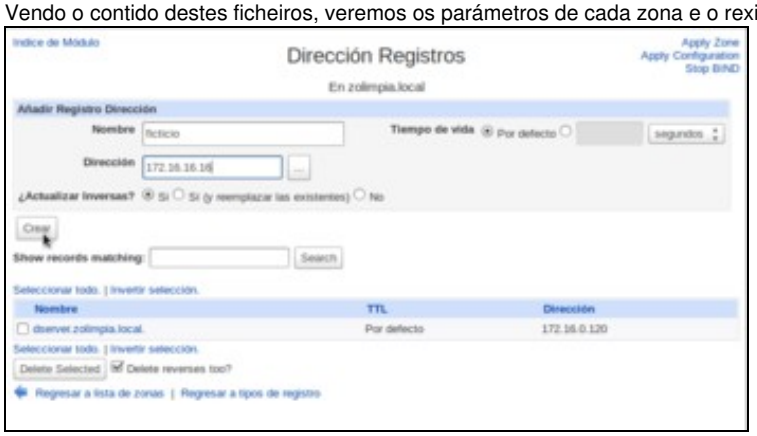
O mesmo coa resolución inversa: **dig -x IP**.

- 

Podemos observar que no ficheiro de configuración **/etc/bind/named.conf.local** se crearon as dúas zonas, e cales son os ficheiros que conteñen a información das mesmas.

-
```
root@dserver:/home/dadmin# more /var/lib/bind/zolimpia.local.hosts
$ttl 38400
zolimpia.local. IN      SOA     172.16.0.120. admin.zolimpia.local. (
                        1459166079
                        10800
                        3600
                        604800
                        38400 )
zolimpia.local. IN      NS      172.16.0.120.
dserver.zolimpia.local. IN      A       172.16.0.120
root@dserver:/home/dadmin#
root@dserver:/home/dadmin#
root@dserver:/home/dadmin# more /var/lib/bind/172.16.rev
$ttl 38400
16.172.in-addr.arpa.    IN      SOA     172.16.0.120. admin.zolimpia.local. (
                        1459166326
                        10800
                        3600
                        604800
                        38400 )
16.172.in-addr.arpa.    IN      NS      172.16.0.120.
120.0.16.172.in-addr.arpa.      IN      PTR     dserver.zolimpia.local.
```

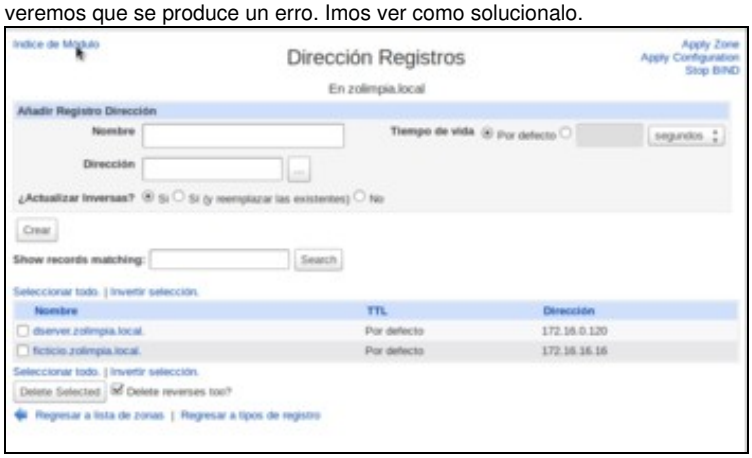
Vendo o contido destes ficheiros, veremos os parámetros de cada zona e o rexistro creado en cada unha.

- 

Imos dar de alta o equipo **ficticio** na zona **zolimpia.local** (172.16.16.16)

- 

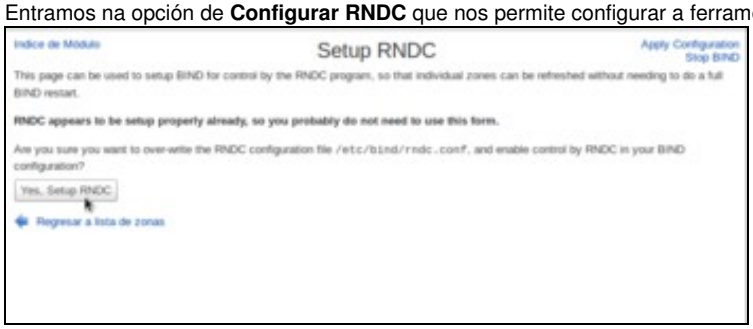
Co rexistro creado, en lugar de picar sobre *Aplicar configuración*, sería máis interesante usar a opción de *Aplicar zona* que aplicar os cambios da zona sen ter que reiniciar o servidor (xa que isto deixa momentaneamente sen servizo aos clientes). Pero se intentamos usar esta opción veremos que se produce un erro. Imos ver como solucionalo.

- 

Imos ao índice do módulo.

- 

Entramos na opción de **Configurar RNDC** que nos permite configurar a ferramenta rndc para executar operacións sobre o servidor DNS.

- 

Webmin nos permite configurar automaticamente a ferramenta picando o botón de **Si, configurar RNDC**.

- 

Podemos comprobar que agora xa podemos aplicar os cambios na zona de busca directa, e na zona de busca inversa.

- ```
  root@dserver:/home/dadmin# ping ficticio.zolimpia.local -c 1
  PING ficticio.zolimpia.local (172.16.16.16) 56(84) bytes of data.
  From dserver.zolimpia.local (172.16.0.120) icmp_seq=1 Destination Host Unreachable

  --- ficticio.zolimpia.local ping statistics ---
  1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

  root@dserver:/home/dadmin#
  ```

Comprobación dende *dserver* da resolución directa. Ollo que aínda que ninguén responda ao PING o servidor DNS está funcionando ao realizar a resolución. O que que pasa que non hai ningún equipo con esa IP.

- ```
  root@dserver:/home/dadmin# dig -x 172.16.16.16

  ; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> -x 172.16.16.16
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21799
  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 4096
  ;; QUESTION SECTION:
  ;16.16.16.172.in-addr.arpa.     IN      PTR

  ;; ANSWER SECTION:
  16.16.16.172.in-addr.arpa. 38400 IN     PTR     ficticio.zolimpia.local.

  ;; AUTHORITY SECTION:
  16.172.in-addr.arpa.    38400   IN      NS      172.16.0.120.

  ;; Query time: 2 msec
  ;; SERVER: 172.16.0.120#53(172.16.0.120)
  ;; WHEN: Mon Mar 28 14:12:03 CEST 2016
  ;; MSG SIZE  rcvd: 117
  ```

O mesmo coa resolución inversa: **dig -x** (Ollo, para que esta resolución funcione hai que ter aplicado os cambios na zona de busca inversa).

- ```
  root@dserver:/home/dadmin# ping dserver -c 1
  PING dserver (127.0.1.1) 56(84) bytes of data.
  64 bytes from dserver (127.0.1.1): icmp_seq=1 ttl=64 time=0.065 ms

  --- dserver ping statistics ---
  1 packets transmitted, 1 received, 0% packet loss, time 0ms
  rtt min/avg/max/mdev = 0.065/0.065/0.065/0.000 ms
  root@dserver:/home/dadmin#
  ```

Xa vimos que se facemos ping ao nome do servidor de DNS co seu nome de dominio o servidor DNS indícanos que ten IP 172.16.0.120. Pero que pasa se se fai ping só ao propio nome do servidor: *dserver*?. Se se pregunta polo nome a secas, faise a resolución correctamente, pero ... de 127.0.1.1. De onde sae iso?...

- ```
  root@dserver:/home/dadmin# cat /etc/hosts
  127.0.0.1       localhost
  127.0.1.1       dserver

  # The following lines are desirable for IPv6 capable hosts
  ::1     localhost ip6-localhost ip6-loopback
  ff02::1 ip6-allnodes
  ff02::2 ip6-allrouters
  root@dserver:/home/dadmin#
  ```

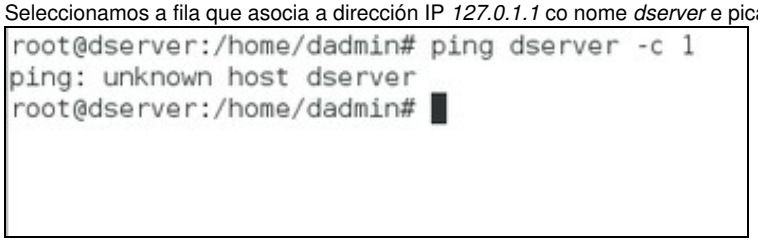
Do ficheiro de **hosts** local (*/etc/hosts*).

- 

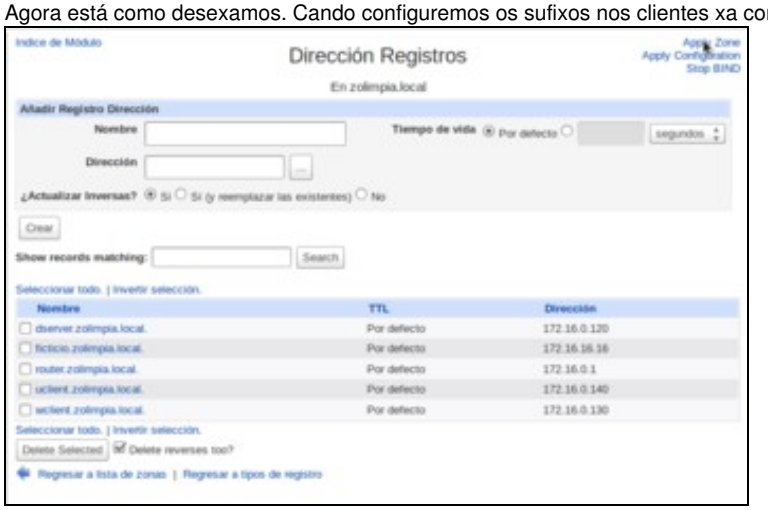
Podemos ver e modificar o contido do ficheiro dende o módulo de **Configuración de rede** do Webmin, no apartado de **Direccións de máquina**.

- 

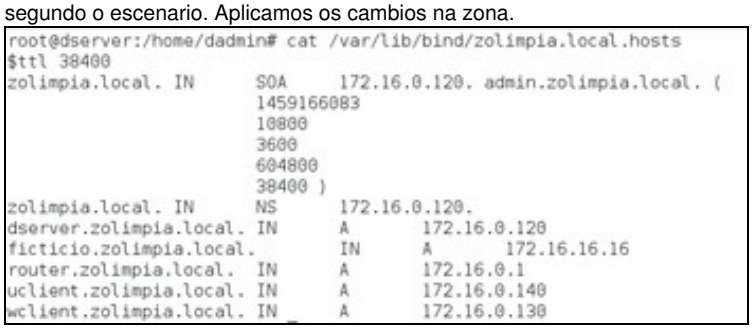
Seleccionamos a fila que asocia a dirección IP *127.0.1.1* co nome *dserver* e picamos en **Borrar as direccións de máquina seleccionadas**.

- 

Agora está como desexamos. Cando configuremos os sufixos nos clientes xa comprobaremos que isto vai resolver.

- 

Ben, agora procedamos a dar de alta na zona de busca directa os rexistros asociados a *wclient* e *uclient* coas súas IPs correspondentes, segundo o escenario. Aplicamos os cambios na zona.

- 

Na imaxe móstrase o ficheiro de configuración de busca directa: **/var/lib/bind/zolimpia.local.hosts**, cos rexistros creados.

- ```
  root@dserver:/home/dadmin# cat /var/lib/bind/172.16.rev
  $ttl 38400
  16.172.in-addr.arpa.    IN      SOA     172.16.0.120. admin.zolimpia.local. (
                          1459166330
                          10800
                          3600
                          604800
                          38400 )
  16.172.in-addr.arpa.    IN      NS      172.16.0.120.
  120.0.16.172.in-addr.arpa.      IN      PTR     dserver.zolimpia.local.
  16.16.16.172.in-addr.arpa.      IN      PTR     ficticio.zolimpia.local.
  1.0.16.172.in-addr.arpa.        IN      PTR     router.zolimpia.local.
  140.0.16.172.in-addr.arpa.      IN      PTR     uclient.zolimpia.local.
  130.0.16.172.in-addr.arpa.      IN      PTR     wclient.zolimpia.local.
  ```

  E nesta podemos ver o ficheiro da zona de busca inversa.
- ```
  root@dserver:/home/dadmin# ping uclient.zolimpia.local -c 1
  PING uclient.zolimpia.local (172.16.0.140) 56(84) bytes of data.
  From dserver.zolimpia.local (172.16.0.120) icmp_seq=1 Destination Host Unreachable

  --- uclient.zolimpia.local ping statistics ---
  1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

  root@dserver:/home/dadmin#
  ```

  A estas alturas **uclient** aínda está apagado e non configurado, co cal se dende *dserver* se fai un ping a *uclient.zolimpia.local* o servidor DNS resolverá correctamente pero non se obtén resposta porque está apagado.
- ```
  root@dserver:/home/dadmin# dig -x 172.16.0.140

  ; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> -x 172.16.0.140
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 56627
  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 4096
  ;; QUESTION SECTION:
  ;140.0.16.172.in-addr.arpa.     IN      PTR

  ;; AUTHORITY SECTION:
  16.172.in-addr.arpa.    38400   IN      SOA     172.16.0.120. admin.zolimpia.local. 1459166327 10800 3600 6
  04800 38400

  ;; Query time: 14 msec
  ;; SERVER: 172.16.0.120#53(172.16.0.120)
  ;; WHEN: Mon Mar 28 14:21:59 CEST 2016
  ;; MSG SIZE  rcvd: 122
  ```

  Pero se intentamos facer a resolución inversa, non obtemos o nome de *uclient*. Por que? Se só aplicamos os cambios na zona de busca directa, o rexistro da zona inversa non está activo, aínda que xa estea no ficheiro de configuración.
- 

  Se entramos na zona de busca inversa e aplicamos a zona...
- ```
  root@dserver:/home/dadmin# dig -x 172.16.0.140

  ; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> -x 172.16.0.140
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45511
  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 4096
  ;; QUESTION SECTION:
  ;140.0.16.172.in-addr.arpa.     IN      PTR

  ;; ANSWER SECTION:
  140.0.16.172.in-addr.arpa. 38400 IN     PTR     uclient.zolimpia.local.

  ;; AUTHORITY SECTION:
  16.172.in-addr.arpa.    38400   IN      NS      172.16.0.120.

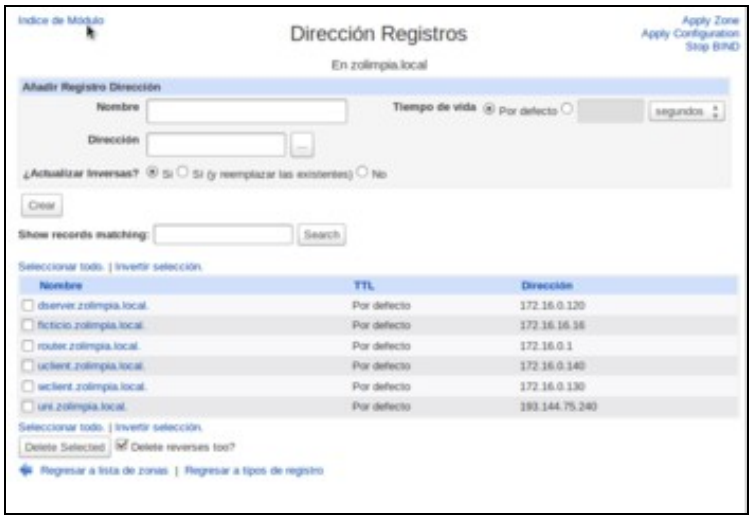
  ;; Query time: 0 msec
  ;; SERVER: 172.16.0.120#53(172.16.0.120)
  ;; WHEN: Mon Mar 28 14:23:01 CEST 2016
  ;; MSG SIZE  rcvd: 116
  ```

A resolución inversa tamén funcionaría correctamente.

1.7.1 Creación de rexistros con asociacións a IPs fóra da LAN

- Nesta ocasión vaise facer unha asociación dun nome de dominio de **zolimpia.local** cunha IP dun servidor que non está na LAN. Neste caso facendo un **ping a www.usc.es** obtense a IP: 193.144.75.240

- Crear rexistros para IPs externas
- 

Crear un rexistro na zona de busca directa **zolimpia.local** chamado **uni** e coa IP: 193.144.75.240. Marcamos a opción de actualizar as inversas.
- 

Na imaxe vemos o rexistro creado, pero se imos ao índice do módulo...
- 

Vemos que non se puido crear o rexistro inverso, xa que non hai ningunha zona de busca inversa que comece por 193. Comprobamos así que Webmin só crea os rexistros inversos se atopa unha zona de busca inversa na que crealos.

- ```
  root@dserver:/home/dadmin# ping uni.zolimpia.local -c 1
  PING uni.zolimpia.local (193.144.75.240) 56(84) bytes of data.

  --- uni.zolimpia.local ping statistics ---
  1 packets transmitted, 0 received, 100% packet loss, time 0ms

  root@dserver:/home/dadmin#
  ```

Comprobar que o servidor resolve correctamente. O servidor da USC non responde aos pings porque ou ben está configurado ou ben hai un FW configurado para que non responda ao tráfico ICMP (ping).

- 

Pero se nun navegador en *dserver* indicamos a URL **uni.zolimpia.local**, aí está a páxina da Universidade. Pero ollo!!, isto é porque o servidor web da USC non está configurado para que haxa que poñerlle exactamente *www.usc.es* para que funcione. Isto podería non funcionar con outros servidores web que estean configurados para responder só ao seu nome de DNS.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez --
  ```