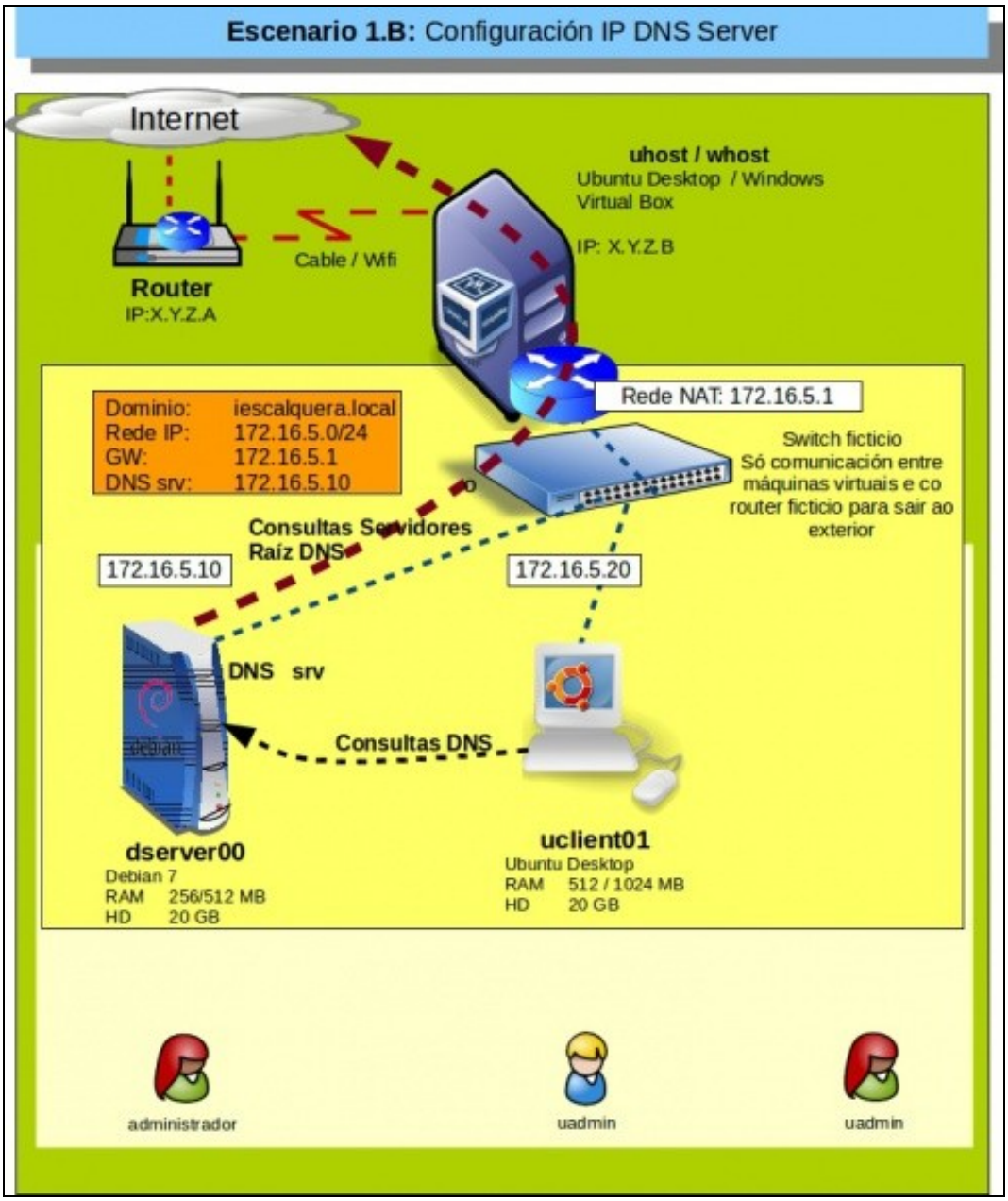
Escenario 1.B - Instalación e configuración do servizo de DNS

Sumario

- 1 Introdución
  - 1.1 Introdución ao servizo DNS
- 2 Introdución ao xestor de servizos systemd
- 3 Instalación e configuración do servizo DNS
- 4 Creación das zonas directa e inversa
- 5 Configuración cliente DNS
  - 5.1 Configuración DNS cliente no servidor dserver00
  - 5.2 Configuración DNS no cliente uclient01
- 6 Instantáneas do escenario 1.B

Introdución

- Neste escenario tratarase de configurar o servidor *dserver00* como servidor de DNS.



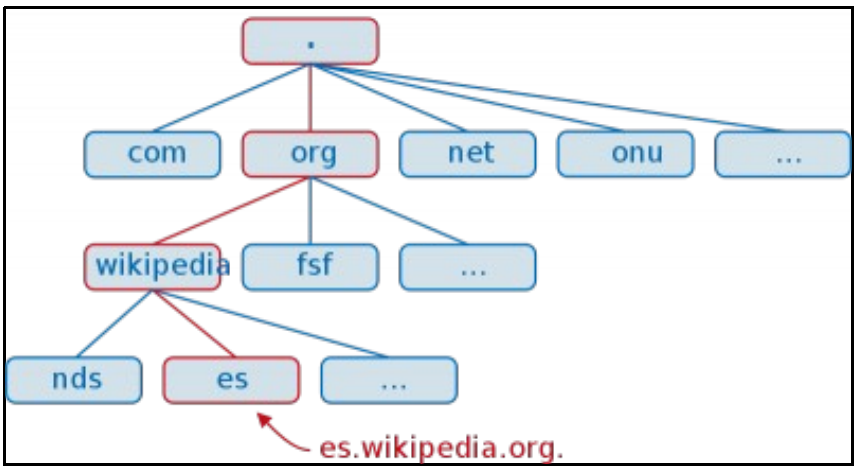
- **dserver00** actuará como servidor DNS de modo que os clientes da rede poderán consultarlle a el polas resolucións de nomes tanto para os do dominio local (*iescalquera.local*) como por nomes do exterior.
- **dserver00** preguntará aos servidores raíz que están no exterior por aqueles nomes de dominio que non xestione el, por exemplo **cesga.es**.
- Nesta ocasión crearemos en **dserver00** a zona de busca directa de DNS **iescalquera.local** e a inversa asociada á rede IP 172.16.5./24.
- A configuración cliente DNS para todo equipo da LAN apuntará á IP deste novo servidor DNS.
- **IMPORTANTE**: para manter a compatibilidade na parte III con SAMBA o nome de dominio non debe exceder os 15 caracteres (Neste caso iescalquera ten 11).

Introdución ao servizo DNS

O Sistema de Nomes de Dominio (*DNS*) é un sistema de nomes xerárquico que nos permite identificar calquera recurso existente nunha rede. Un nome de dominio completo (tamén chamado *FQDN*, *Fully Qualified Domain Name*) consiste en dúas ou máis etiquetas separadas por puntos:

- A etiqueta situada máis ao final é o **dominio de nivel superior** ou *TLD* (*Top Level Domain*) e pode indicar a finalidade do dominio ou o país (como **.org**, **.net**, **.es**, **.pt**, etc.).
- A partir do TLD, as distintas etiquetas que van á esquerda indican distintos **subdominios** de forma xerárquica, uns dentro de outros.
- A etiqueta da situada máis á esquerda (a primeira) indica o nome da máquina.

Por exemplo, como se pode ver na imaxe, o FQDN *es.wikipedia.org* fai referencia á máquina *es* dentro do dominio *wikipedia*, que á súa vez está dentro do dominio *org*. Este último dominio tamén está dentro do dominio ., que é o dominio raíz.



TAMÉN PODES VER...

- Para afondar máis sobre o servizo DNS:
  - Conceptos básicos de DNS do Curso Formación Profesorado: Platega: Simulación de redes locais con máquinas virtuais
  - Do mesmo curso, para ver como configurar DNS en Zentyal ou Windows: Curso Formación Profesorado: Platega: Simulación de redes locais con máquinas virtuais#PARTE V: Servizos básicos das redes locais
  - Os documentos PDF do profesor **Victor Lourido**:
    - Archivo:DNS - Servicios de nombres.pdf
    - Archivo:DNS - Instalación y configuración BIND en Ubuntu.pdf
  - Para conceptos teóricos, punto 9 do seguinte ficheiro PDF: Archivo:Modelo OSI TCP IP.pdf
  - Para Windows, punto 2 do seguinte ficheiro PDF: Archivo:03.- Servizos Internet en 2003.pdf
  - Servizo DNS do profesor Jesús Arribi

Introdución ao xestor de servizos systemd

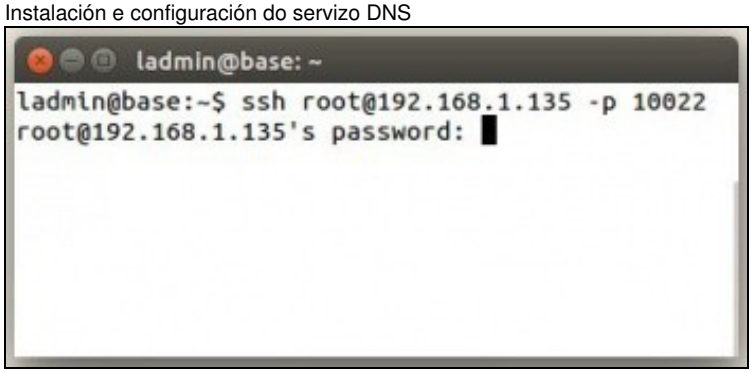
- Debian, dende a versión 8, cambiou o seu xestor de servizos de *SysVinit* a *Systemd*.
- A forma de iniciar/parar/comprobar o estado dun servizo é: **systemctl start/stop/status SERVIZO**
- Segue podéndose usar o formato SysVinit: **service SERVIZO start/stop/status**

- Máis info:
    - https://wiki.archlinux.org/index.php/Systemd_(Espa%C3%B1ol)
    - https://juncotic.com/comandos-sysvinit-vs-comandos-systemd/

- No material usaránse as 2 formas de manexar os servizos:
    - As capturas de pantallas que proceden de versións anteriores de Debian usan: service.
    - Aquelas capturas de pantalla que houbo que actualizar usan: systemctl

Instalación e configuración do servizo DNS

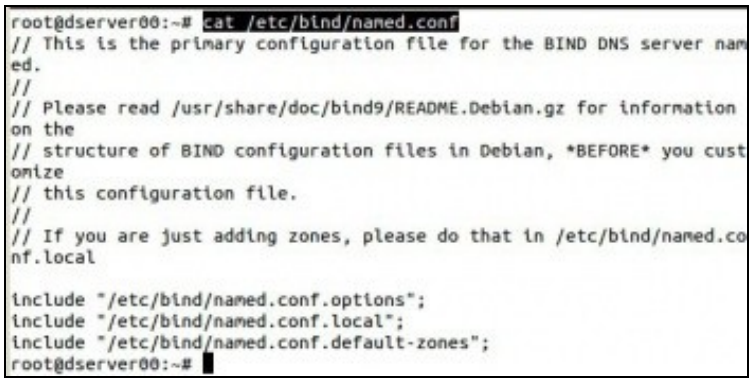
- Para facilitar a configuración do servidor **dserver00** imos conectarnos por ssh/putty dende o equipo real a ese servidor, así poderemos copiar/pegar contidos da web máis facilmente ou copiar configuracións do mesmo servidor ao exterior máis facilmente.
- As pantallas con fondo branco son configuracións no servidor.
- As pantallas con fondo negro son configuracións no cliente.

- Instalación e configuración do servizo DNS
- 

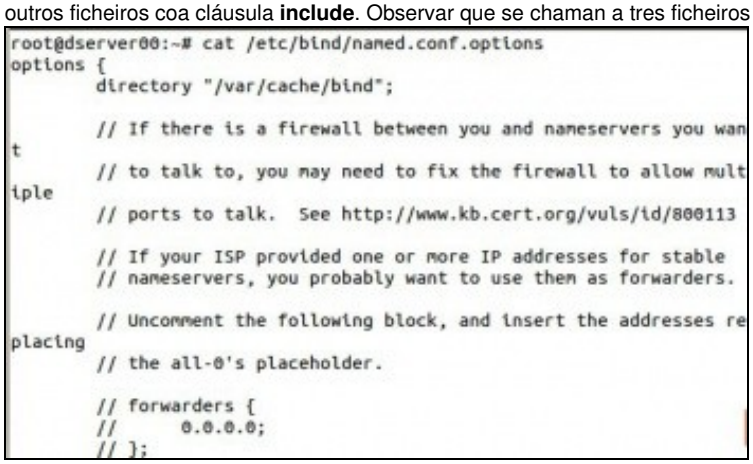
Comezamos conectándonos ao servidor **dserver00** dende o exterior (Equipo físico).
Lembrar que rediriximos os portos en VirtualBox no escenario 1.A, e estamos conectándonos á IP do host real a un porto que nos redirixe ao servidor **dserver00**
Entrar co usuario administrador de dserver00.
Para pasarse a root executar:**su -**
Introducir o contrasinal de root: (abc123.)
- 

Executar **apt-get install bind9** para instalar o servidor DNS.
- 

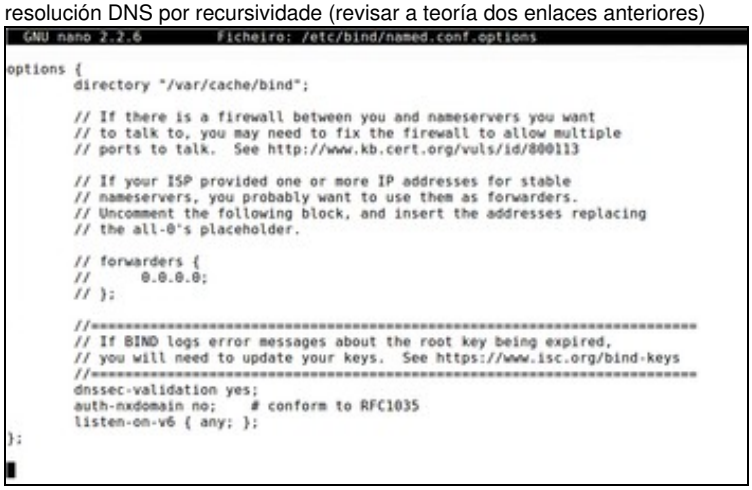
Unha vez instalado o servizo iníciase automaticamente. Agora mesmo xa temos un servidor DNS, calquera equipo que apunte a este equipo na súa configuración cliente DNS xa vai poder resolver nomes de Internet.

- 
```
root@dserver00:~# cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server nam
ed.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information
on the
// structure of BIND configuration files in Debian, *BEFORE* you cust
omize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.co
nf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
root@dserver00:~#
```

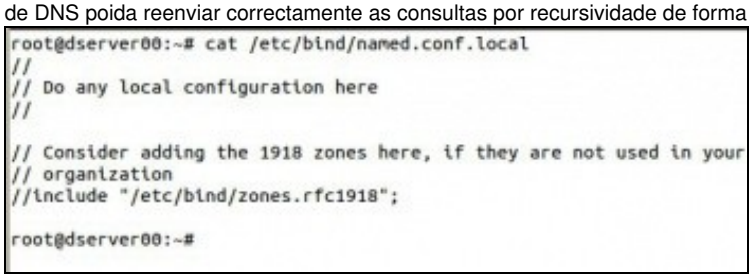
Imos facer unha pequena revisión dos ficheiros de configuración que interveñen na configuración do servizo DNS.
O ficheiro **/etc/bind/named.conf** é o ficheiro principal do servizo. É onde se configuran as zonas de busca ou se chaman a estas a través de outros ficheiros coa cláusula **include**. Observar que se chaman a tres ficheiros que agora pasamos a describir.

- 
```
root@dserver00:~# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you wan
t
        // to talk to, you may need to fix the firewall to allow mult
iple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.

        // Uncomment the following block, and insert the addresses re
placing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };
```

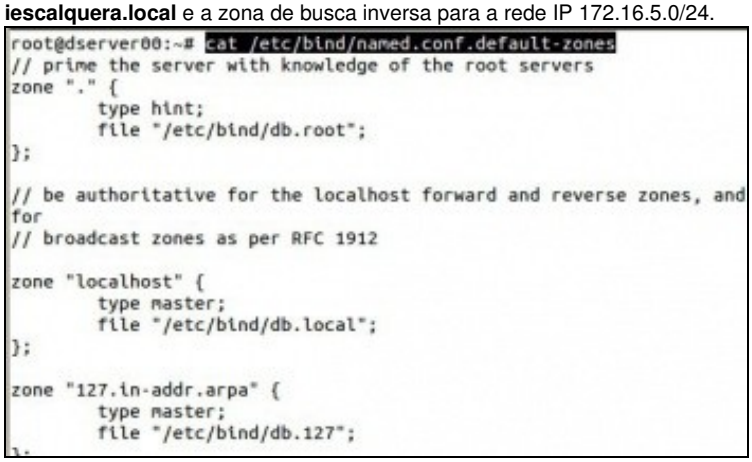
O ficheiro **/etc/bind/named.conf.options** configura, entre outras cousas:
- O directorio onde se vai a ir a buscar por defecto os ficheiros das zonas DNS, neste caso **/var/cache/bind**.
- Os reenviadores aos que preguntar no caso de querer reenviar unha consulta a un/s servidor/es DNS específicos antes que facer resolución DNS por recursividade (revisar a teoría dos enlaces anteriores)

- 
```
 GNU nano 2.2.6        Ficheiro: /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation yes;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

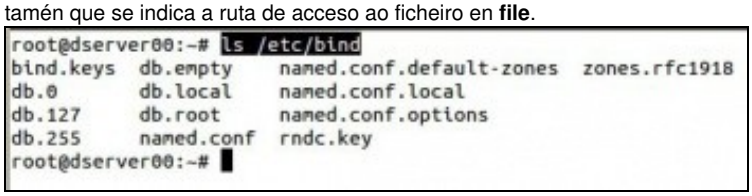
Editamos este ficheiro para modificar o valor do parámetro **dnssec-validation**, para establecer o valor **yes**. Facemos isto para que o servidor de DNS poida reenviar correctamente as consultas por recursividade de forma segura con DNSSEC.

- 
```
root@dserver00:~# cat /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";

root@dserver00:~#
```

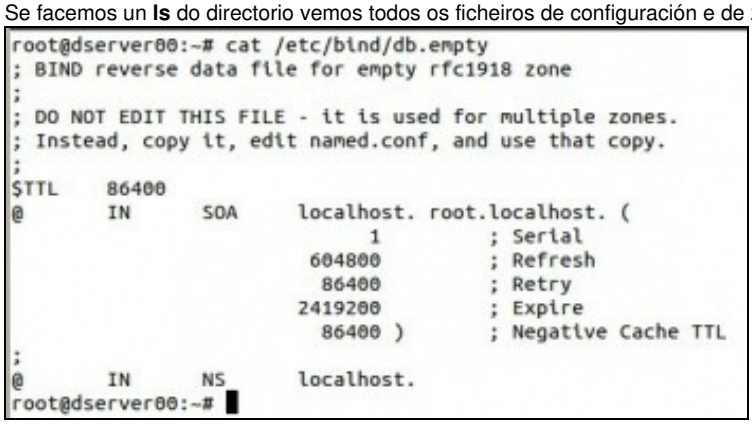
O ficheiro **/etc/bind/named.conf.local** é onde se recomenda que se creen as zonas locais. Aí crearemos a zona de busca directa **iescalquera.local** e a zona de busca inversa para a rede IP 172.16.5.0/24.

- 
```
root@dserver00:~# cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// 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.local";
};

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

O ficheiro **/etc/bind/named.conf.default-zones** é onde o servizo ten xa configuradas unhas zonas por defecto, entre elas a zona raíz chamada punto **"."**. Observar como indica en que ficheiro están almacenados os equipos desa zona raíz. E así coas demais zonas. Fixarse tamén que se indica a ruta de acceso ao ficheiro en **file**.

- 
```
root@dserver00:~# ls /etc/bind
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
root@dserver00:~#
```

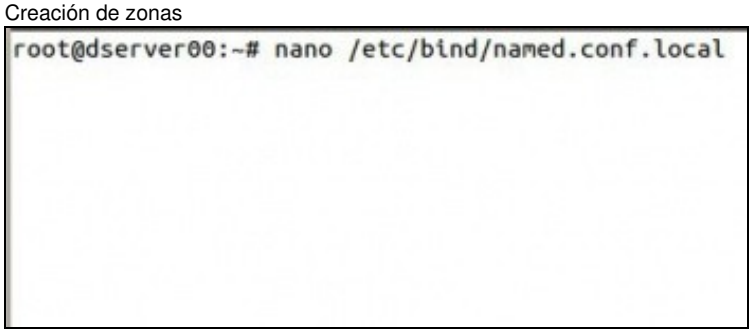
Se facemos un **ls** do directorio vemos todos os ficheiros de configuración e de zonas que aí hai.

- 
```
root@dserver00:~# cat /etc/bind/db.empty
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
root@dserver00:~#
```

Entre eles, o ficheiro de zona **db.empty** que se usa de exemplo para crear outras zonas.

Creación das zonas directa e inversa

- A continuación imos crear dúas zonas:
  - **Directa**: para a resolución dos nomes a IPs dos equipos do dominio **iescalquera.local**.
  - **Inversa**: para a resolución de IPs a nomes de equipos para a rede IP **172.16.5**.

- Creación de zonas
- 
```
root@dserver00:~# nano /etc/bind/named.conf.local
```

Editamos o ficheiro /**etc**/**bind**/**named.conf.local** e ao final deste, ...

- ```
  GNU nano 2.2.6   Ficheiro: /etc/bind/named.conf.local

  zone "iescalquera.local" {
          type master;
          file "db.iescalquera.local";
  };

  zone "5.16.172.in-addr.arpa" {
          type master;
          file "db.172.16.5";
  };
  ```

Creamos as zonas directa e inversa. Observar que non se indica a ruta ao ficheiro onde se van crear os elementos da zona, por tanto este debe estar na ruta especificada anteriormente por defecto: /**var**/**cache**/**bind**. Observar tamén, que toda instrución remata en **";"** . Finalmente observar que o nome da zona inversa é a rede IP ao revés.
Os nomes dos ficheiros **file** poden chamarse como se desexe, o importante é que existan no directorio anterior.

- A continuación amósase ás liñas que se engadiron ao ficheiro:

```
zone "iescalquera.local" {
        type master;
        file "db.iescalquera.local";
};

zone "5.16.172.in-addr.arpa" {
        type master;
        file "db.172.16.5";
};
```

- Creación de zonas
- ```
  -# cp /etc/bind/db.empty /var/cache/bind/db.iescalquera.local
  -# cp /etc/bind/db.empty /var/cache/bind/db.172.16.5
  ```

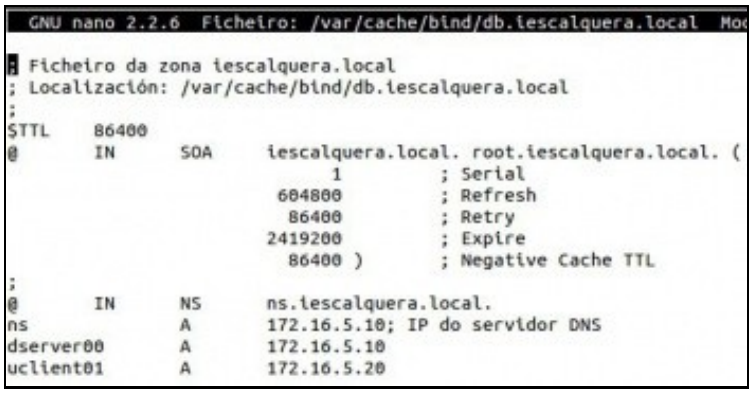
Continuamos copiando o ficheiro **db.empty** á ruta por defecto /**var**/**cache**/**bind** para cada unha das zonas anteriores. Observar que o nome do ficheiro debe coincidir co indicado en **file** nas zonas anteriores.

- ```
  root@dserver00:~# nano /var/cache/bind/db.iescalquera.local
  ```

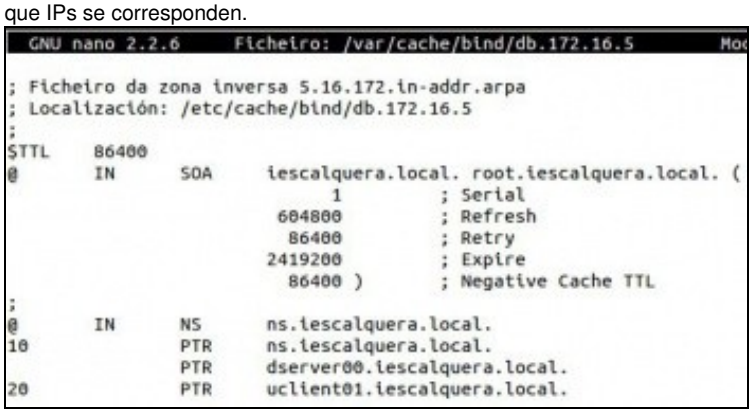
Editamos o ficheiro de busca directa para a zona **iescalquera.local** que se atopa en /**var**/**cache**/**bind**/**db.iescalquera.local**

- ```
  GNU nano 2.2.6  Ficheiro: /var/cache/bind/db.iescalquera.local

  ; BIND reverse data file for empty rfc1918 zone
  ;
  ; DO NOT EDIT THIS FILE - it is used for multiple zones.
  ; Instead, copy it, edit named.conf, and use that copy.
  ;
  $TTL    86400
  @       IN      SOA     localhost. root.localhost. (
                                1         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                            86400 )       ; Negative Cache TTL
  ;
  @       IN      NS      localhost.
  ```

Ten o contido do ficheiro do que foi copiado: **db.empty**.

- 

Configuramos agora a zona como se indica na imaxe para a zona **iescalquera.local**
A continuación ponse o ficheiro en modo texto.
Observar que so substituímos **localhost** por **iescalquera.local** e logo engadimos os rexistros tipo **"A"** para indicar o nome dos equipos con que IPs se corresponden.

- 

Facemos o mesmo coa zona de busca inversa que está no ficheiro /**var**/**cache**/**bind**/**db.172.16.5**. Observar que agora engadimos rexistros **"PTR"** de busca inversa que asocian IPs a nomes. Por exemplo a entrada "10" está asociada aos equipos "ns" e "dserver00" de iescalquera.local, de modo que cando preguntemos por 172.16.5.10 imos obter eses dous posibles nomes de equipo.
Abaixo está o ficheiro de configuración.

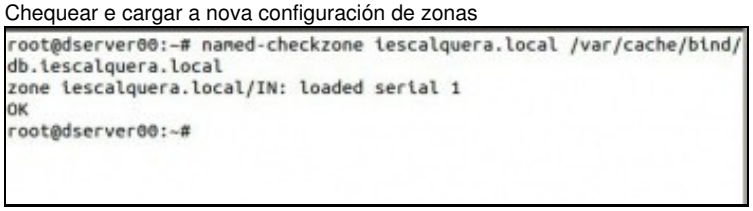
- **Ficheiro de configuración da zona iescalquera.local**: */var/cache/bind/db.iescalquera.local*

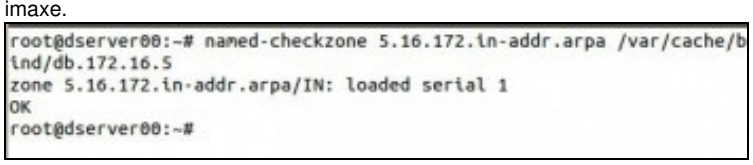
```
$TTL 86400
@       IN SOA  iescalquera.local. root.iescalquera.local. (
                                1          ; serial
                                604800     ; refresh
                                86400      ; retry
                                2419200    ; expire
                                86400      ; minimum
                                )
;
@       IN              NS      ns.iescalquera.local.
ns                      A       172.16.5.10; IP do servidor DNS
dserver00               A       172.16.5.10
uclient01               A       172.16.5.20
```

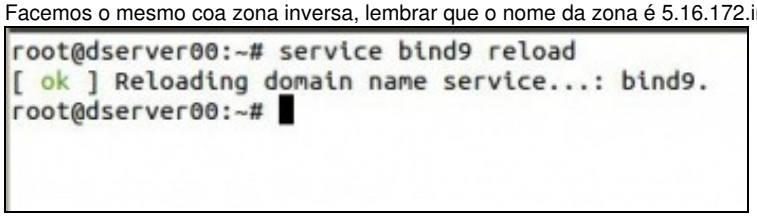
- **Ficheiro de configuración da zona 5.16.172.in-addr.arpa**: */var/cache/bind/db.172.16.5*

```
$TTL 86400
@       IN SOA  iescalquera.local. root.iescalquera.local. (
                                1          ; serial
                                604800     ; refresh
                                86400      ; retry
                                2419200    ; expire
                                86400      ; minimum
                                )
;
@       IN              NS      ns.iescalquera.local.
10                      PTR     ns.iescalquera.local.
                        PTR     dserver00.iescalquera.local.
20                      PTR     uclient01.iescalquera.local.
```

- Agora co comando **named-checkzone** imos comprobar que os ficheiros non teñen erros de sintaxe.

- Chequear e cargar a nova configuración de zonas
- 

  Executamos o comando pasándolle o nome da zona e o ficheiro no que se atopa. Se todo vai ben debemos obter unha mensaxe como a da imaxe.
- 

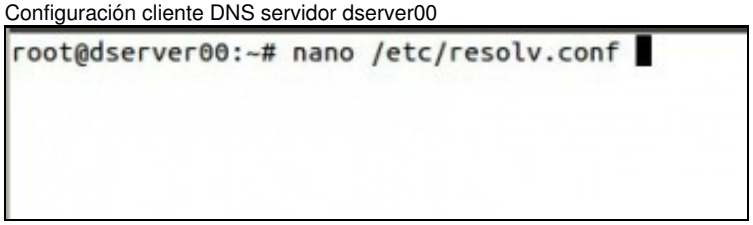
  Facemos o mesmo coa zona inversa, lembrar que o nome da zona é 5.16.172.in-addr.arpa, isto é a Rede IP ao revés.
- 

  Unha vez comprobadas as zonas só resta cargalas no servizo DNS. Para iso non é preciso reiniciar o servizo senón que facemos **reload** para que cargue as novas zonas.
  Se o servizo non está activo executar:**service bind9 start**

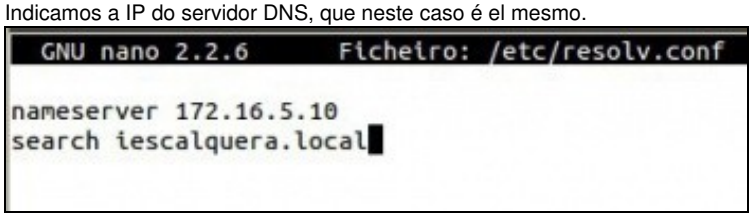
Configuración cliente DNS

Configuración DNS cliente no servidor dserver00

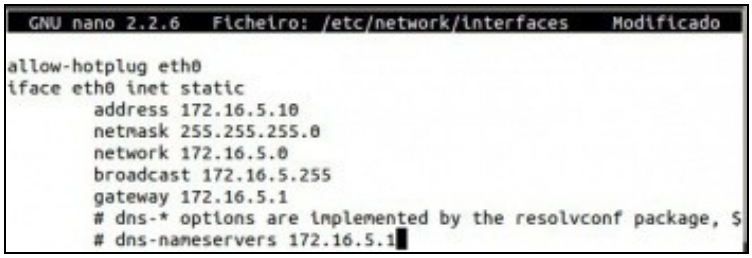
- O servidor DNS, **dserver00**, tamén é un cliente DNS pois os programas que se conecten a Internet precisan pasar nomes de dominio a IPs.
- Por tanto imos configurar a parte cliente DNS do servidor **dserver00**

- Configuración cliente DNS servidor dserver00
- 

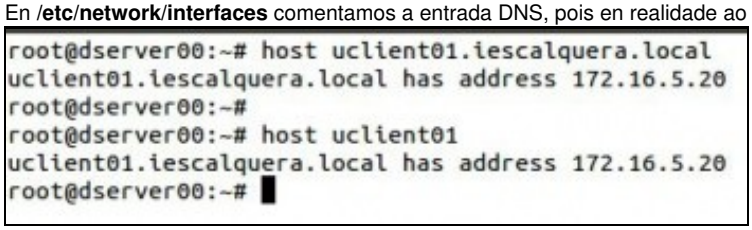
  Editamos o ficheiro /**etc**/**resolv.conf**.
- 

  Indicamos a IP do servidor DNS, que neste caso é el mesmo.
- 

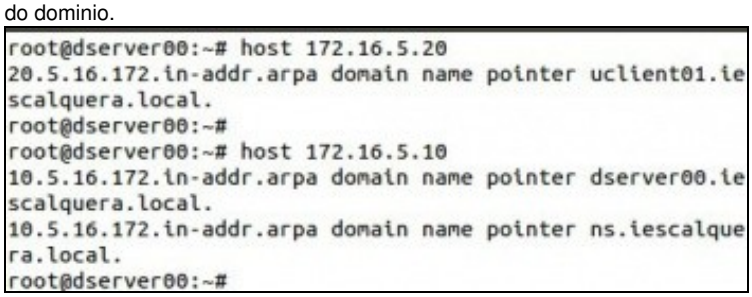
Indicamos tamén o sufixo DNS (ou dominios de busca) **iescalquera.local**. Deste xeito se desexamos conectarnos dende ao servidor ao equipo **uclient01.iescalquera.local**, so precisamos indicar o nome **uclient01** e el engadiralle o sufixo **iescalquera.local** de modo automático.

- 

En /**etc**/**network**/**interfaces** comentamos a entrada DNS, pois en realidade ao ter o ficheiro resolv.conf esta non ten efecto.

- 

Comprobamos con **host** que podemos facer **Resolucións directas** (de nomes a IPs), tanto:
-do nome de equipo co dominio completo,
-como só co nome de equipo. Fixarse que como grazas ao sufixo DNS da cláusula **search** do ficheiro /**etc**/**resolv.conf** se completa o nome do dominio.

- 

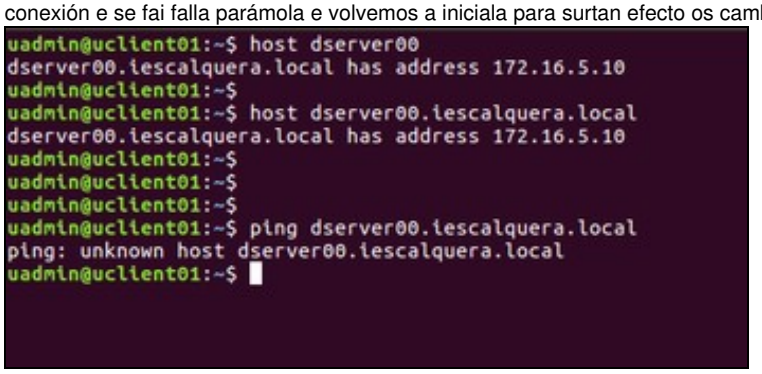
Facemos o mesmo con **host** para comprobar as **resolucións inversas** (de IPs a nomes de dominio).
Observar como para IP 172.16.5.10 obtemos dous nomes de dominio.

Configuración DNS no cliente uclient01

- Agora tócalle a quenda ao equipo Ubuntu: **uclient01**.

- IP do servidor
- 

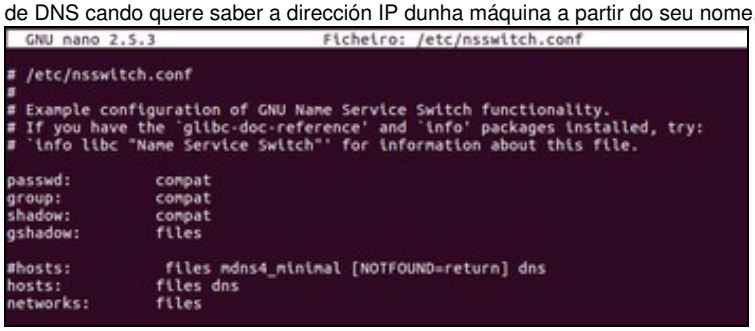
Editamos a conexión activa do cliente Ubuntu. Cambiamos o servidor DNS e engadimos o sufixo DNS no dominio de busca. Gardamos a conexión e se fai falla parámola e volvemos a iniciala para surtan efecto os cambios.

- 

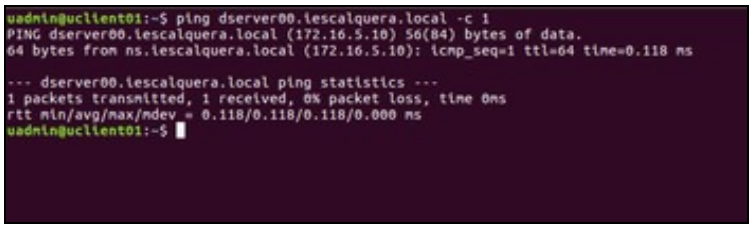
Se probamos agora o funcionamento do servidor de DNS dende os equipos clientes, observaremos un comportamento un tanto raro: Co comando *host* obteremos correctamente a dirección IP dos equipos do noso dominio, pero non funcionará se intentamos conectarnos a eles usando por exemplo o comando *ping*. O problema está na configuración do ficheiro */etc/nsswitch.conf* e un servizo chamado Avahi que non funciona correctamente se se usa o dominio *.local*.

- 

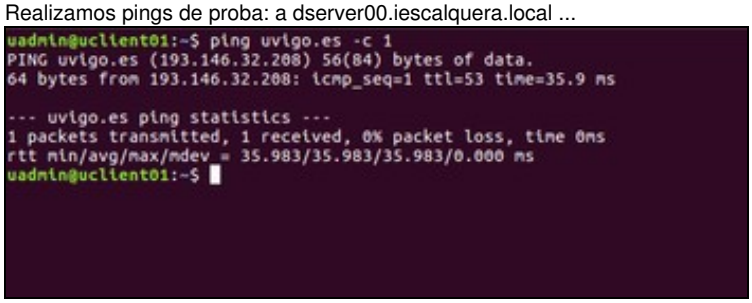
En */etc/nsswitch.conf* indícaselle ao sistema que servizos ten que usar para buscar os usuarios, grupos, máquinas, etc. Se editamos este ficheiro no cliente, veremos que na liña de *hosts* fai uso dun servizo *mdns4_minimal*, que é o que impide que o equipo consulte ao servidor de DNS cando quere saber a dirección IP dunha máquina a partir do seu nome.

- 

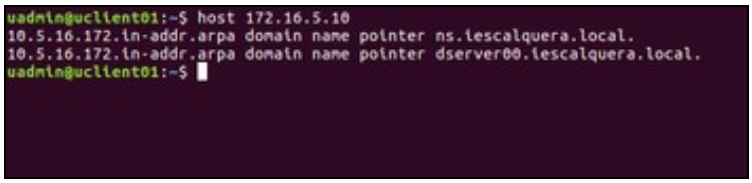
Modificamos a entrada **hosts** a **files dns**

- 

Realizamos pings de proba: a dserver00.iescalquera.local ...

- 

... ao exterior.

- 

Con **host** miramos resolucións inversas.

Instantáneas do escenario 1.B

- Ao igual que se fixo no escenario 1.A imos crear unha instantánea no servidor *dserver00* e no cliente *uclient01*. Nunca se sabe se precisaremos volver atrás.

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