

Servidor DNS

bind9 & bind9utils

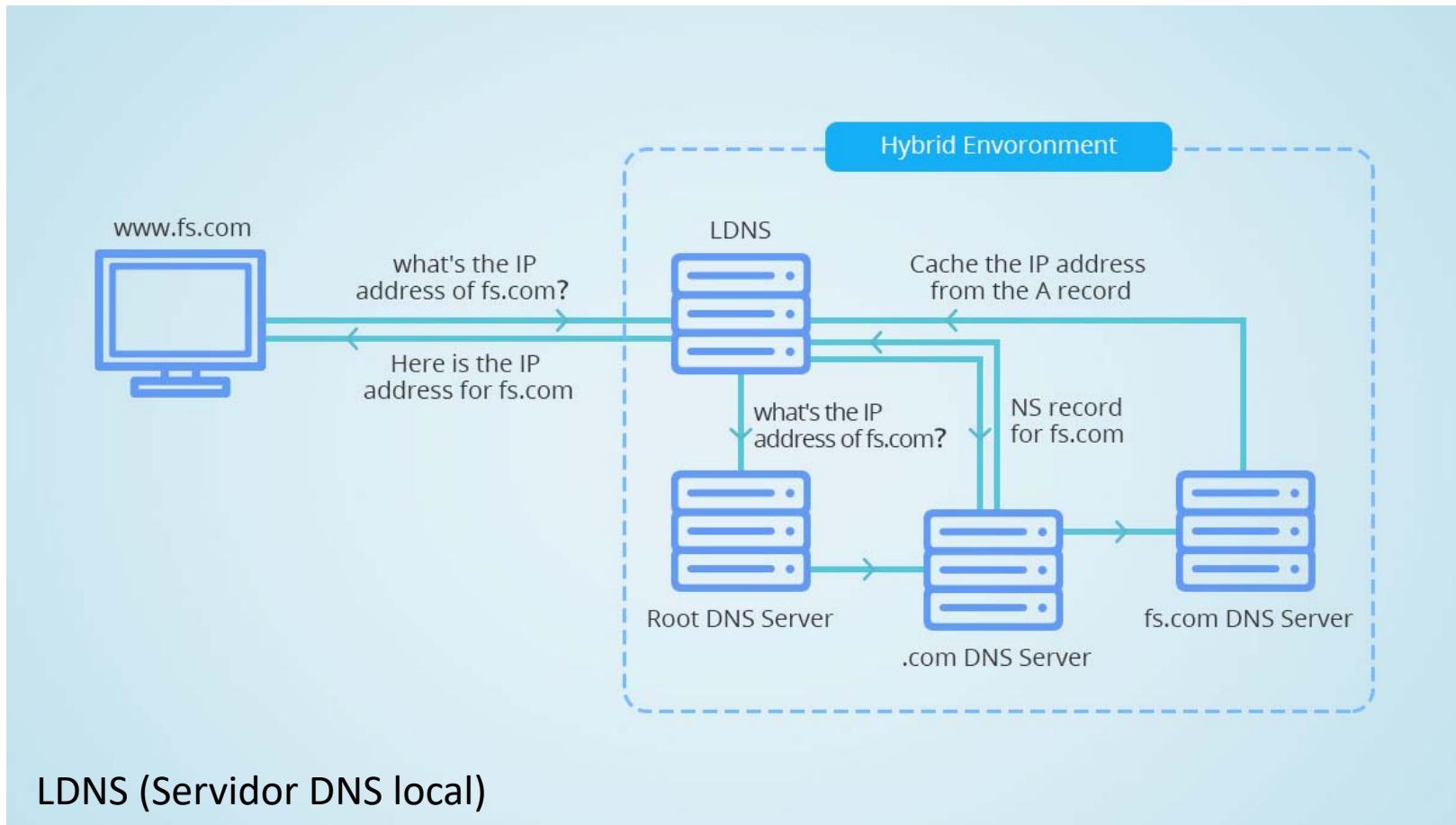
DHCP y DNS

- El DHCP es un protocolo que nos ayuda a asignar dirección IP.
- El DNS se utiliza para convertir el nombre de un sitio web como FS.com a su dirección IP y viceversa.
- Esto garantiza que nuestra computadora encuentre el sitio adecuado, porque una computadora sólo buscar un sitio a través de su dirección IP, en lugar de su nombre de dominio.

¿Cómo funciona el DHCP?



¿Cómo funciona DNS?



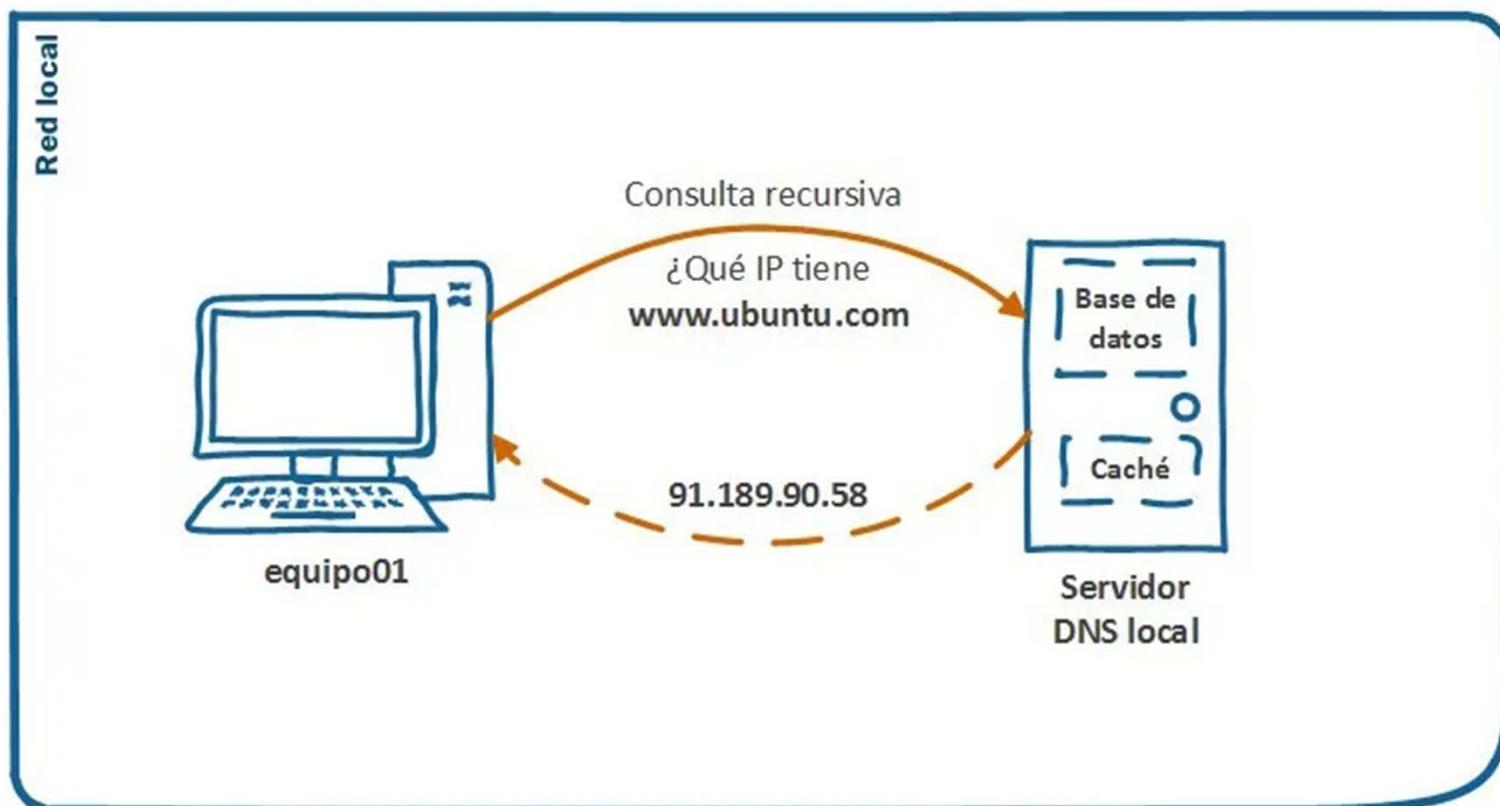
Parámetros	DHCP	DNS
Básico	Un protocolo para asignar una dirección IP al host de forma estática o dinámica.	Un mecanismo de resolución de direcciones.
Protocolos relacionados	UDP	UDP y TCP
Servidor	El servidor DHCP es responsable de asignar las direcciones temporales a la computadora del cliente por un tiempo de arrendamiento, y luego extender el arrendamiento de acuerdo con el requisito.	El servidor DNS es responsable de aceptar las consultas a través del cliente y responder con los resultados.
Metodología de trabajo	Centralizado	Descentralizado
Características	1. Proporciona información adicional, como las direcciones IP del host y la máscara de subred de la computadora. 2. Asigna IP al host por un tiempo de arrendamiento particular 2. Asigna IP al host por un tiempo de arrendamiento particular	1. Convierte nombres simbólicos en direcciones IP y viceversa. 2. Se utiliza para localizar servidores de dominio de directorio activo.
Desventajas	Configuración de dirección IP confiable y administración de red reducida.	Elimina la necesidad de recordar la dirección IP; en cambio, el nombre de dominio se usa para la dirección web.

Instalación y configuración del servicio DNS en Ubuntu Server 20.04

- Una consulta es una solicitud de resolución de nombres que se envía a un servidor DNS. Hay dos tipos de consultas:
 - Recursivas
 - Iterativas o no recursivas

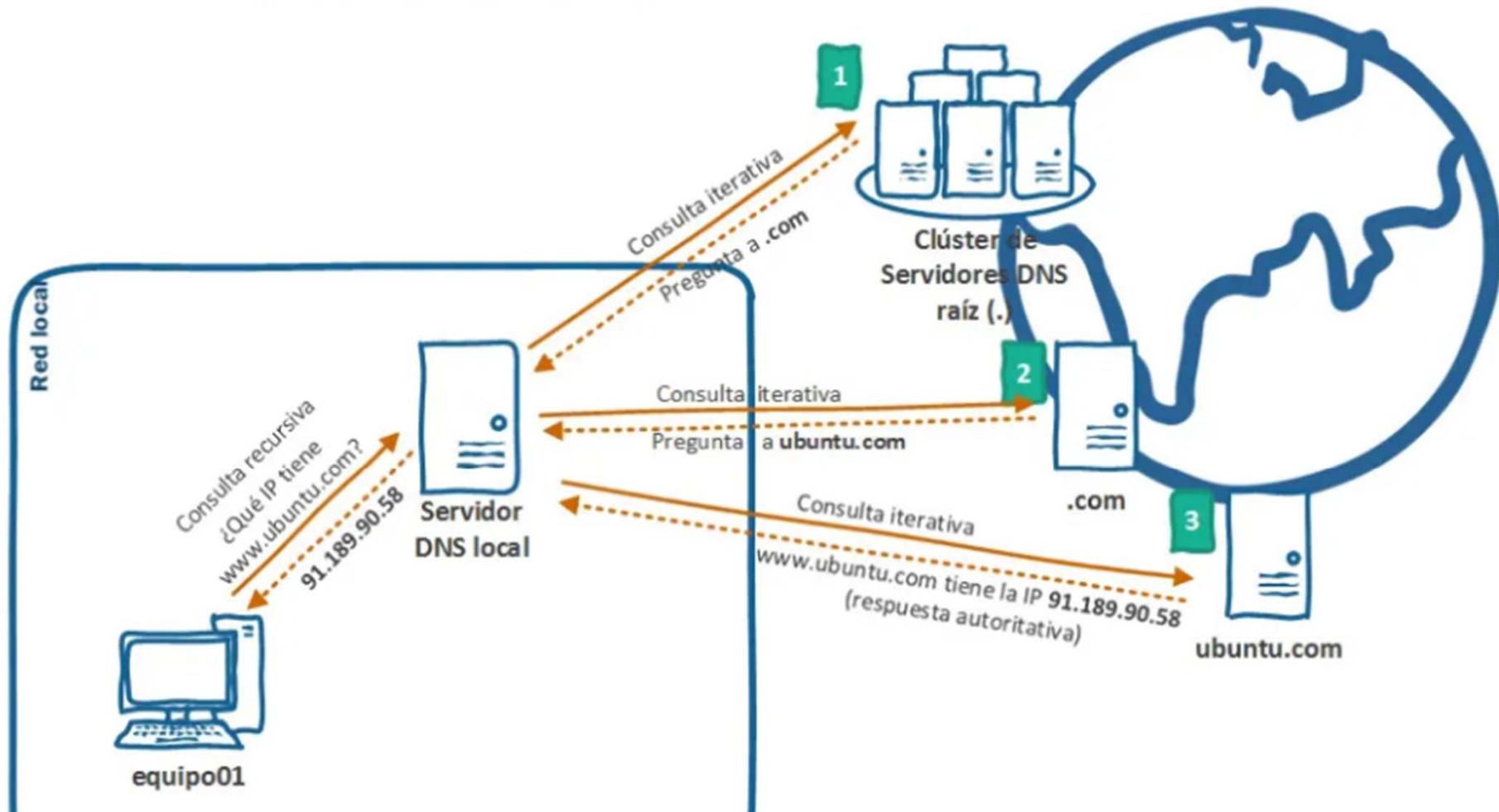
¿Cómo funcionan las consultas recursivas?

Una consulta recursiva es aquella realizada a un servidor DNS, en la que el cliente solicita al servidor que le proporcione una respuesta completa a la consulta. El servidor DNS comprueba las zonas de búsquedas y la caché para proporcionar una respuesta a la consulta.



¿Cómo funcionan las consultas iterativas?

Una consulta iterativa es aquella efectuada a un servidor DNS en la que el cliente solicita la mejor respuesta que el servidor DNS pueda proporcionar sin buscar ayuda adicional de otros servidores DNS. El resultado de una consulta iterativa suele ser una referencia a otro servidor DNS de nivel inferior en el árbol DNS.

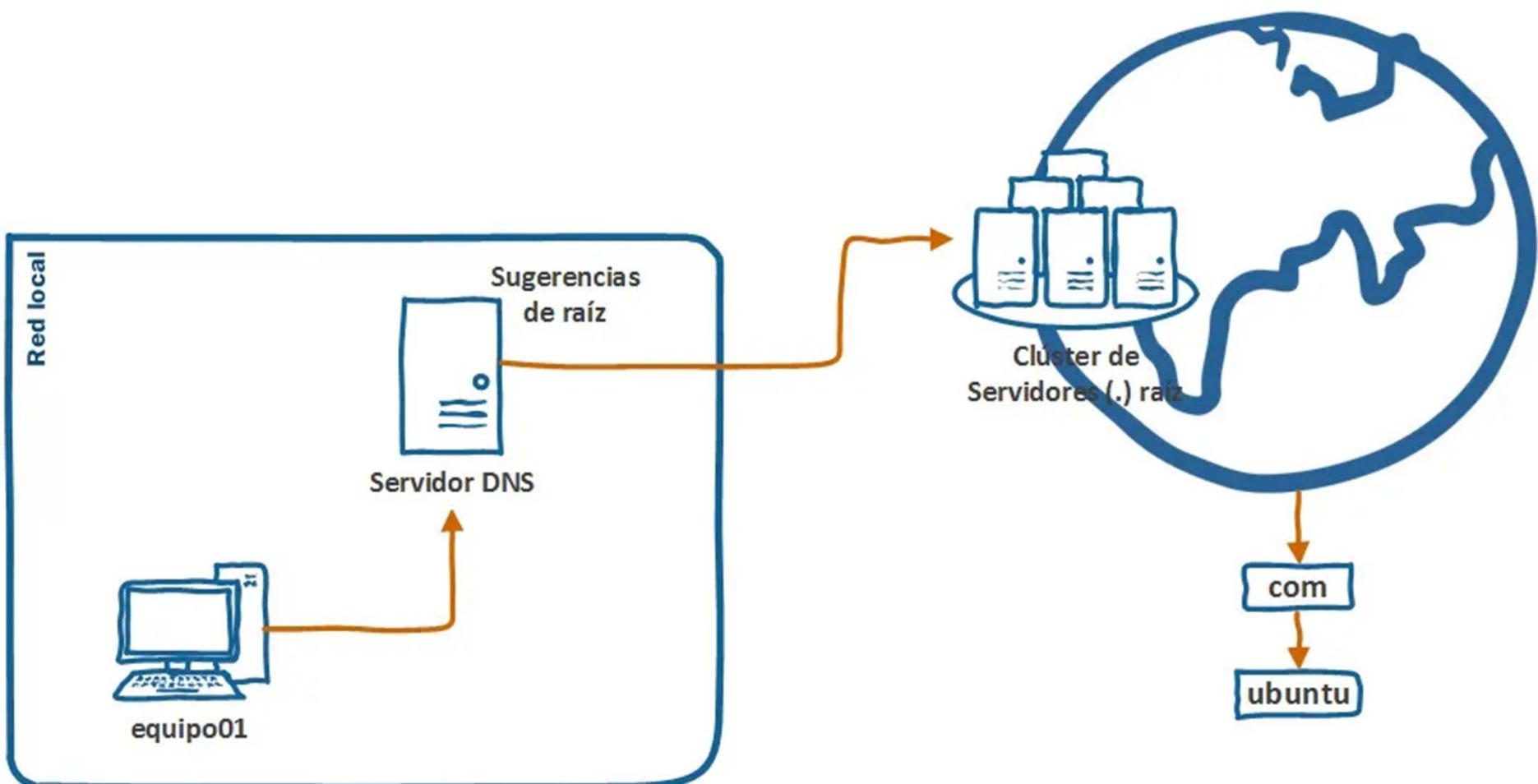


Servidores DNS

- Si un servidor DNS es autoritativo en el espacio de nombres de la consulta: comprobará la caché, comprobará las zonas existentes (base de datos) y devolverá la dirección IP solicitada.
- Si un servidor DNS no es autoritativo en el espacio de nombres de la consulta, realizará una de las siguientes acciones:
 - Utilizar sugerencias raíz (root hints) para encontrar una respuesta a la consulta.
 - Reenviar la consulta que no puede resolverse a un servidor específico denominado Forwarder (Reenviador).

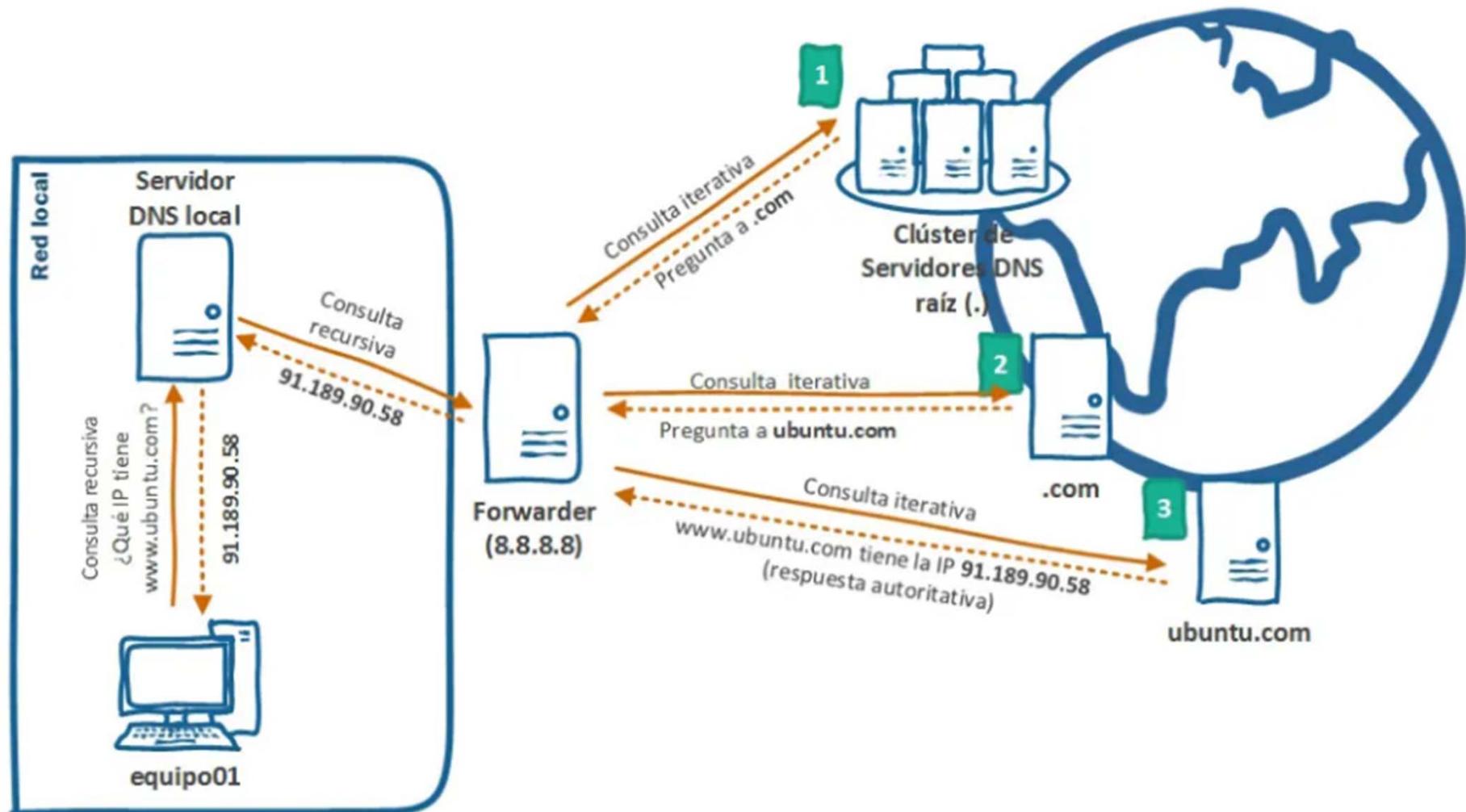
¿Cómo funciona Root hints (sugerencias de raíz)?

Root hints es un registro de recursos DNS almacenado en un servidor DNS que indica las direcciones IP de los servidores DNS raíz.



¿Cómo funcionan los forwarders (reenviadores)?

Un reenviador es un servidor DNS designado por otros servidores DNS internos para reenviar consultas y resolver nombres de dominios externos o fuera del sitio.



Servidor DNS

- Se Implementará un **Servidor DNS** de tipo **master** con zonas directa e inversa para la resolución de nombres en nuestra red local, de la cual será **autoritativo** con **forwarders** para las consultas externas.
- Instalar los paquetes **bind9** y **bind9utils**.

```
sudo apt install bind9 bind9utils
```

Servidor DNS

- El primer fichero a editar será `/etc/bind/named.conf.local`. En él definiremos las zonas, directa e inversa, para el dominio `midominio.local` haciendo uso de la cláusula `zone`. Cada bloque de zona incluirá de qué tipo será la zona y el fichero en el que estarán definidas, para cada zona, las características, propiedades y entidades del dominio.

Servidor DNS

```
GNU nano 4.8                               /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";

// Fichero para búsquedas directas
zone "midominio.local" {
    type master;
    file "/etc/bind/db.midominio.local";
};

// Fichero para búsquedas inversas
zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.168.192";
};
```

Servidor DNS

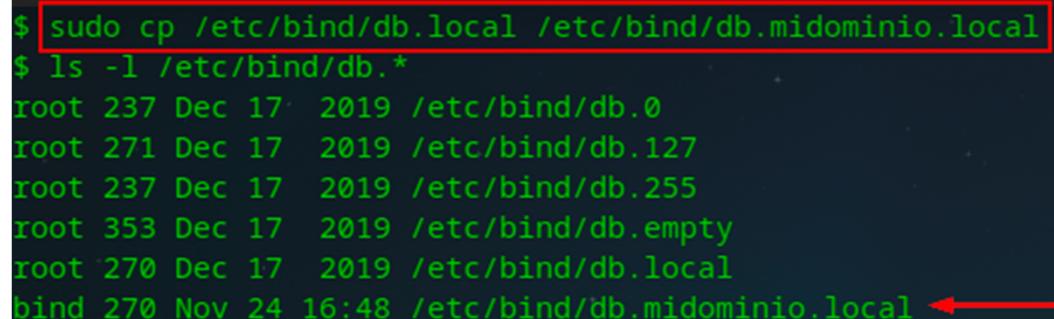
- Una vez definidas las zonas, vamos a comprobar que la configuración sea correcta y no hayamos cometido errores en la sintaxis del fichero. Usaremos el comando named-checkconf. Si tras lanzar el comando no nos devuelve nada, significará que no se han encontrado errores.

```
$ sudo named-checkconf /etc/bind/named.conf.local  
$
```

Servidor DNS

- Crear los ficheros de zona que hemos indicado anteriormente en la configuración. Para su creación vamos a tomar como plantillas ficheros de zonas que se crean al instalar el paquete bind9 y los editaremos. Para la zona directa crearemos el fichero /etc/bind/db.midominio.local.

```
$ sudo cp /etc/bind/db.local /etc/bind/db.midominio.local
$ ls -l /etc/bind/db.*
```



```
root 237 Dec 17 2019 /etc/bind/db.0
root 271 Dec 17 2019 /etc/bind/db.127
root 237 Dec 17 2019 /etc/bind/db.255
root 353 Dec 17 2019 /etc/bind/db.empty
root 270 Dec 17 2019 /etc/bind/db.local
bind 270 Nov 24 16:48 /etc/bind/db.midominio.local ←
```

Servidor DNS

- Una vez creado el fichero lo editaremos y cambiaremos/añadiremos el nombre del dominio y las entidades por las nuestras. También debemos cambiar la cláusula Serial cada vez que editemos nuestros ficheros de zona, esto es una forma de llevar un control de versiones. Por ejemplo, una numeración del tipo YYMMDDVV (año mes día versión).

Servidor DNS

```
GNU nano 4.8                               /etc/bind/db.midominio.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     midominio.local. root.midominio.local. (
                      2020112600          ; Serial
                           604800            ; Refresh
                           86400             ; Retry
                          2419200            ; Expire
                           604800 )           ; Negative Cache TTL
;
@      IN      NS      dns.midominio.local.
dns   IN      A       192.168.10.10
pc01  IN      A       192.168.10.21
pc02  IN      A       192.168.10.22
```

Servidor DNS

- Se crea el fichero de zona inversa.

```
$ sudo cp /etc/bind/db.127 /etc/bind/db.10.168.192
$ ls -l /etc/bind/db.*
root 237 Dec 17 2019 /etc/bind/db.0
bind 271 Nov 26 17:15 /etc/bind/db.10.168.192 ←
root 271 Dec 17 2019 /etc/bind/db.127
root 237 Dec 17 2019 /etc/bind/db.255
root 353 Dec 17 2019 /etc/bind/db.empty
root 270 Dec 17 2019 /etc/bind/db.local
bind 548 Nov 26 17:08 /etc/bind/db.midominio.local
```

Servidor DNS

- Una vez creado el fichero lo editaremos y cambiaremos/añadiremos el nombre del dominio y las entidades por las nuestras. No olvidar modificar el Serial.

```
GNU nano 4.8                               /etc/bind/db.10.168.192
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     midominio.local. root.midominio.local. (
                      2020112600      ; Serial
                           604800      ; Refresh
                           86400       ; Retry
                          2419200     ; Expire
                           604800 )    ; Negative Cache TTL
;
@       IN      NS      dns.
10      IN      PTR     dns.midominio.local.
21      IN      PTR     pc01.midominio.local.
22      IN      PTR     pc02.midominio.local.
```

Servidor DNS

- Lo siguiente es comprobar que la configuración de los ficheros de zonas la hemos realizado correctamente y no hayamos cometido errores en la sintaxis del fichero. El comando que vamos a usar para comprobar los ficheros de zonas es named-checkzone seguido del nombre de la zona y del fichero en cuestión. Sabremos que todo está correctamente configurado si obtenemos un OK como respuesta.

Servidor DNS

```
juanapc@pandora:~$ sudo named-checkzone midominio.local /etc/bind/db.midominio.local ←
zone midominio.local/IN: loaded serial 2020112600
OK
juanapc@pandora:~$ sudo named-checkzone 10.168.192.in-addr.arpa /etc/bind/db.10.168.192
zone 10.168.192.in-addr.arpa/IN: loaded serial 2020112600
OK
```

Servidor DNS

- El siguiente paso es editar el fichero `/etc/bind/named.conf.options` donde crearemos una lista de acceso para restringir quien puede realizar las consultas a nuestro servidor DNS e indicaremos un par de servidores forwarders donde delegará nuestro servidor DNS local cuando no pueda resolver alguna consulta.

Servidor DNS

```
GNU nano 4.8                               /etc/bind/named.conf.options

acl safeclients {
    localhost;
    localnets;
};

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.

    allow-query { any; };
    allow-recursion { safeclients; };
    allow-query-cache { safeclients; };

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

//=====

```

Servidor DNS

- Antes de poner nuestro servicio en marcha vamos a modificar el fichero `/etc/default/named` donde especificaremos un argumento para el usuario bind. Este usuario se crea automáticamente al realizar la instalación del servicio bind9. El argumento a indicar es `-4`, con él forzamos el uso de IPv4 siempre y así evitaremos mensajes de error de red inalcanzable por direccionamiento IPv6.

Servidor DNS

```
GNU nano 4.8                               /etc/default/named
#
# run resolvconf?
RESOLVCONF=no
+
# startup options for the server
OPTIONS="-u bind -4"
```



Servidor DNS

- Solo queda reiniciar el servicio bind9 y comprobar que esté corriendo correctamente.

```
juanapc@pandora:~$ sudo service bind9 restart ←
juanapc@pandora:~$ sudo service bind9 status ←
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2020-11-26 17:31:51 UTC; 4s ago
    Docs: man:named(8)
   Main PID: 1913 (named)
     Tasks: 8 (limit: 2282)
    Memory: 15.5M
      CGroup: /system.slice/named.service
              └─1913 /usr/sbin/named -f -u bind -4

Nov 26 17:31:51 pandora named[1913]: zone localhost/IN: loaded serial 2
Nov 26 17:31:51 pandora named[1913]: zone 255.in-addr.arpa/IN: loaded serial 1
Nov 26 17:31:51 pandora named[1913]: zone 10.168.192.in-addr.arpa/IN: loaded serial 2020112600
Nov 26 17:31:51 pandora named[1913]: zone midominio.local/IN: loaded serial 2020112600
Nov 26 17:31:51 pandora named[1913]: all zones loaded
Nov 26 17:31:51 pandora named[1913]: running
Nov 26 17:31:51 pandora named[1913]: zone 10.168.192.in-addr.arpa/IN: sending notifies (serial 2020112600)
Nov 26 17:31:51 pandora named[1913]: zone midominio.local/IN: sending notifies (serial 2020112600)
Nov 26 17:31:51 pandora named[1913]: managed-keys-zone: Key 20326 for zone . is now trusted (accepting)
```

Servidor DNS

- Ahora editaremos la configuración de red de nuestro Ubuntu Server para indicarle que él mismo, es el servidor DNS que tendrá que consultar para la resolución de nombres. Ubuntu Server 20.04 se hace uso de netplan.

```
GNU nano 4.8                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      gateway4: 192.168.10.1
      nameservers:
        addresses: [192.168.10.10] ←
        search: [midominio.local] ←
version: 2
```

Servidor DNS

- Una vez editada la configuración de red, lanzamos la instrucción sudo netplan apply para que los cambios surtan efecto.

```
~$ sudo netplan apply
```

Servidor DNS

- Primeas pruebas con **nslookup** para comprobar si el servidor DNS está resolviendo correctamente los nombres y las IPs.

```
juanapc@pandora:~$ nslookup pc01
Server:      127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer: ← X
Name:  pc01.midominio.local
Address: 192.168.10.21
```

Servidor DNS

- Si consultamos el fichero `/etc/resolv.conf` donde debería aparecer como nameserver la IP de nuestro servidor (`localhost`), veremos que nos aparece la dirección de loopback `127.0.0.53` la cual nosotros no hemos indicado en el fichero de configuración de la red. Además, si le hacemos un `ls -l`, podemos observar que se trata de un enlace simbólico a otro fichero de configuración.

Servidor DNS

```
juanapc@pandora:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search midominio.local

juanapc@pandora:~$ ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 Jul 31 16:28 /etc/resolv.conf -> ../../run/systemd/resolve/stub
```

Servidor DNS

- Systemd tiene su propia implementación de resolución de nombres: `systemd-resolved`. Además de implementar un resolver, añade características adicionales tales como caché DNS y validación DNSSEC.
- Por defecto, las aplicaciones hacen uso del resolver de `systemd-resolved` que escucha en la interfaz de loopback en la dirección 127.0.0.53. Este es el motivo por el cual las respuestas a nuestras consultas a pc01 y pc02 son, de momento, no autoritativas, ya que nos está respondiendo el resolver de `systemd-resolved` que a su vez obtiene la respuesta de nuestro resolver (`bind9`).

Servidor DNS

- ¿Cómo podemos desactivar systemd-resolved y que las aplicaciones consulten nuestro resolver directamente? Existen 4 modos de implementación de systemd-resolved. Es decir, existen 4 ficheros de configuración, 1 por cada modo de implementación de systemd-resolved.

```
$ ls -l /run/systemd/resolve/stub-resolv.conf 1
$ ls -l /usr/lib/systemd/resolv.conf 2
$ ls -l /run/systemd/resolve/resolv.conf 3
$ ls -l /etc/resolv.conf 4
```

Servidor DNS

- Para que todo funcione como antes de systemd y las aplicaciones consulten nuestro resolver directamente, debemos cambiar el enlace simbólico de /etc/resolv.conf y apuntarlo al siguiente fichero /run/systemd/resolve/resolv.conf

```
ls -l /etc/resolv.conf
oot 39 Jul 31 16:28 /etc/resolv.conf -> ../../run/systemd/resolve/stub-resol

sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf

ls -l /etc/resolv.conf
oot 32 Nov 26 18:33 /etc/resolv.conf -> /run/systemd/resolve/resolv.conf
```



Servidor DNS

- Una vez modificado el enlace simbólico vamos a comprobar el nuevo contenido de /etc/resolv.conf y veremos como, ahora si, aparece como nameserver la IP de nuestro servidor.

```
juanapc@pandora:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.10.10 ←
search midominio.local ←
```

Servidor DNS

- Realizamos las mismas pruebas con nslookup que realizamos anteriormente y comprobaremos el resultado de las consultas.

```
juanapc@pandora:~$ nslookup pc01
Server:      192.168.10.10
Address:     192.168.10.10#53
                ✓
Name:   pc01.midominio.local
Address: 192.168.10.21
```

```
juanapc@pandora:~$ nslookup 192.168.10.21
21.10.168.192.in-addr.arpa      name = pc01.midominio.local..
```

Referencias

- <https://blog.sysdual.com/installacion-y- configuracion-del-servicio-dns-en-ubuntu-server- 20-04/>
- <https://community.fs.com/es/blog/dhcp-and-dns- difference.html>